LINKSYS®

A Division of Cisco Systems, Inc.

ADSL2 Gateway

with 4-Port Switch

User Guide

WIRED

Model No. **AG241**

Cisco Systems

Copyright and Trademarks

How to Use this Guide

Your Guide to the ADSL2 Gateway with 4-Port Switch 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

Chapter 1: Introduction 1
Welcome 1
What's in this Guide? 2
Chapter 2: Planning Your Network 4
The Gateway's Functions 4
IP Addresses 4
What is a VPN? 5
Why do I need a VPN? 6
Chapter 3: Getting to Know the ADSL2 Gateway with 4-Port Switch 8
The Back Panel 8
The Front Panel 9
Chapter 4: Connecting the ADSL2 Gateway with 4-Port Switch 10
Overview 10
Wired Connection to a Computer 11
Wireless Connection to a Computer 12
Chapter 5: Configuring the Gateway 13
Overview 13
How to Access the Web-based Utility 15
The Setup Tab 15
The Security Tab 22
The Access Restrictions Tab 27
The Applications and Gaming Tab 29
The Administration Tab 32
The Status Tab 37
Common Problems and Solutions 39
Frequently Asked Questions 47
Introduction 53
Environment 53
How to Establish a Secure IPSec Tunnel 54
Windows 98 or Me Instructions 64
Windows 2000 or XP Instructions 65

List of Figures

Figure 2-1: Network 4
Figure 2-2: Computer-to-VPN Gateway 6
Figure 2-3: VPN Gateway-to-VPN Gateway 7
Figure 3-1: Back Panel 8
Figure 3-2: Front Panel 9
Figure 4-1: Ethernet Connection 11
Figure 4-2: ADSL Connection 11
Figure 4-3: Power Connection 11
Figure 5-1: Password Screen 15
Figure 5-2: Basic Setup Tab 15
Figure 5-3: Dynamic IP 16
Figure 5-4: Static IP 16
Figure 5-5: IPoA 17
Figure 5-6: RFC 2516 PPPoE 17
Figure 5-7: RFC 2364 PPPoA 18
Figure 5-8: Bridged Mode Only 18
Figure 5-9: Optional Settings 19
Figure 5-10: DynDNS.org 20
Figure 5-11: TZO.com 20
Figure 5-12: Advanced Routing 21
Figure 5-13: Advanced Wireless Settings 22
Figure 5-14: Firewall 23
Figure 5-15: VPN 24
Figure 5-16: VPN Settings Summary 24
Figure 5-17: Manual Key Management 25
Figure 5-18: System Log 25
Figure 5-19: Advanced VPN Tunnel Setup 26
Figure 5-20: Internet Access 27

Figure 5-21: Internet Policy Summary 27
Figure 5-22: List of PCs 28
Figure 5-23: Port Services 28
Figure 5-24: Single Port Forwarding 29
Figure 5-25: Port Range Forwarding 29
Figure 5-26: Port Triggering 30
Figure 5-27: DMZ 30
Figure 5-28: QOS 31
Figure 5-29: Management 32
Figure 5-30: Reporting 33
Figure 5-31: System Log 33
Figure 5-32: Ping Test 34
Figure 5-33: Backup&Restore 34
Figure 5-34: Factory Defaults 35
Figure 5-35: Firmware Upgrade 35
Figure 5-36: Reboot 36
Figure 5-37: Status 37
Figure 5-38: Local Network 37
Figure 5-39: DHCP Clients Table 37
Figure 5-40: DSL Connection 38
Figure B-1: Local Security Screen 54
Figure B-2: Rules Tab 54
Figure B-3: IP Filter List Tab 54
Figure B-4: IP Filter LIst 55
Figure B-5: Filters Properties 55
Figure B-6: New Rule Properties 55
Figure B-7: IP Filter List 56
Figure B-8: Filters Properties 56
Figure B-9: New Rule Properties 56
Figure B-10: IP Filter List Tab 57

Figure B-11: Filter Acton Tab 57
Figure B-12: Security Methods Tab 57
Figure B-13: Authentication Methods 58
Figure B-14: Preshared Key 58
Figure B-15: New Preshared Key 58
Figure B-16: Tunnel Setting Tab 59
Figure B-17: Connection Type Tab 59
Figure B-18: Properties Screen 59
Figure B-19: IP Filter List Tab 60
Figure B-20: Filter Action Tab 60
Figure B-21: Authentication Methods Tab 60
Figure B-22: Preshared Key 61
Figure B-23: New Preshared Key 61
Figure B-24: Tunnel Setting Tab 61
Figure B-25: Connection Type 62
Figure B-26: Rules 62
Figure B-27: Local Computer 62
Figure B-28: VPN Tab 63
Figure C-1: IP Configuration Screen 64
Figure C-2: MAC Address/Adapter Address 64
Figure C-3: MAC Address/Physical Address 65
Figure D-1: Upgrade Firmware 66

Chapter 1: Introduction

Welcome

The Linksys ADSL2 Gateway with 4-Port Switch is the all-in-one solution for Internet connectivity in your home. The ADSL Modem function gives you a blazing fast connection to the Internet, far faster than a dial-up, and without tying up your phone line.

Connect your computers to the Gateway via the built-in 4-port 10/100 Ethernet Switch to jump start your home network. You can share files, printers, hard drive space and other resources, or play head-to-head computer games. Attach four computers directly, or connect more hubs and switches to create as big a network as you need. The Gateway ties it all together and lets your whole network share that high-speed Internet connection.

To protect your data and privacy, the ADSL2 Gateway with 4-Port Switch features an advanced firewall to keep Internet intruders and attackers out. Wireless transmissions can be protected by powerful data encryption. Safeguard your family with Parental Control features like Internet Access Time Limits and Key Word Blocking. Configuration is a snap with any web browser.

With the Linksys ADSL2 Gateway with 4-Port Switch at the heart of your home network, you're connected to the future.

What's in this Guide?

This user guide covers the steps for setting up and using the ADSL2 Gateway with 4-Port Switch.

- Chapter 1: Introduction
  This chapter describes the ADSL2 Gateway with 4-Port Switch ADSL2 Gateway with 4-Port Switch applications and this User Guide.

- Chapter 2: Planning Your Network
  This chapter describes the basics of networking.

- Chapter 3: Getting to Know the ADSL2 Gateway with 4-Port Switch
  This chapter describes the physical features of the Gateway.

- Chapter 4: Connecting the ADSL2 Gateway with 4-Port Switch
  This chapter instructs you on how to connect the Gateway to your network.

- Chapter 5: Configuring the Gateway
  This chapter explains how to use the Web-Based Utility to configure the settings on the Gateway.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the ADSL2 Gateway with 4-Port Switch.

- Appendix B: Configuring IPSec between a Windows 2000 Computer and the Gateway
  This appendix instructs you on how to establish a secure IPSec tunnel using preshared keys to join a private network inside the VPN Gateway and a Windows 2000 or XP computer.

- Appendix C: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on your Gateway if you should need to do so.

- Appendix D: Finding the MAC Address and IP Address for your Ethernet Adapter.
  This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Gateway.

- Appendix E: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

- Appendix F: Specifications
  This appendix provides the technical specifications for the Gateway.

- 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.

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.

***LAN**: the computers and networking products that make up your local network*

NOTE: Since the Gateway is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Gateway uses NAT technology, the only IP address that can be seen from the Internet for your network is the Gateway's Internet IP address. However, even this Internet IP address can be blocked, so that the Gateway and network seem invisible to the Internet—see the Block WAN Requests description under Security in "Chapter 5: Configuring the Gateway."

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 5: Configuring the Gateway."

What is a VPN?

A VPN, or Virtual Private Network, is a connection between two endpoints - a VPN Gateway, for instance - in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks.

This is done by creating a "tunnel". A VPN tunnel connects the two computers or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques - IPSec, short for IP Security - the VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices,

telecommuters, and/or professionals on the road (travelers can connect to a VPN Gateway using any computer with VPN client software that supports IPSec, such as SSH Sentinel.)

There are two basic ways to create a VPN connection:

- VPN Gateway to VPN Gateway
- Computer (using VPN client software that supports IPSec) to VPN Gateway

The VPN Gateway creates a "tunnel" or channel between two endpoints, so that data transmissions between them are secure. A computer with VPN client software that supports IPSec can be one of the two endpoints. Any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN Gateway to create a VPN tunnel using IPSec (refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP computer and the VPN Gateway"). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

Computer (using VPN client software that supports IPSec) to VPN Gateway

The following is an example of a computer-to-VPN Gateway VPN. (See Figure 2-2.) In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software that supports IPSec and connects to the VPN Gateway at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected.

VPN Gateway to VPN Gateway

An example of a VPN Gateway-to-VPN Gateway VPN would be as follows. (See Figure 2-3.) At home, a telecommuter uses his VPN Gateway for his always-on Internet connection. His Gateway is configured with his office's VPN settings. When he connects to his office's Gateway, the two Gateways create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected.

For additional information and instructions about creating your own VPN, please visit Linksys's international website at www.linksys.com/international or refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP computer and the VPN Gateway."

Why do I need a VPN?

Computer networking provides a flexibility not available when using a paper-based system. With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to

Figure 2-2: Computer-to-VPN Gateway

IMPORTANT: You must have at least one VPN Gateway on one end of the VPN tunnel. At the other end of the VPN tunnel, you must have a second VPN Gateway or a computer with VPN client software that supports IPSec.

protect data inside of a local network. But what do you do once information is sent outside of your local network, when emails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected?

That is when a VPN can help. VPNs secure data moving outside of your network as if it were still within that network.

When data is sent out across the Internet from your computer, it is always open to attacks. You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network - when you send data to someone via email or communicate with an individual over the Internet - the firewall will no longer protect that data.

At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows:

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

2) Data Sniffing

Data “sniffing” is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

3) Man in the Middle Attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a “man in the middle” attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That's a long way to go for unsecured data and this is when a VPN serves its purpose.

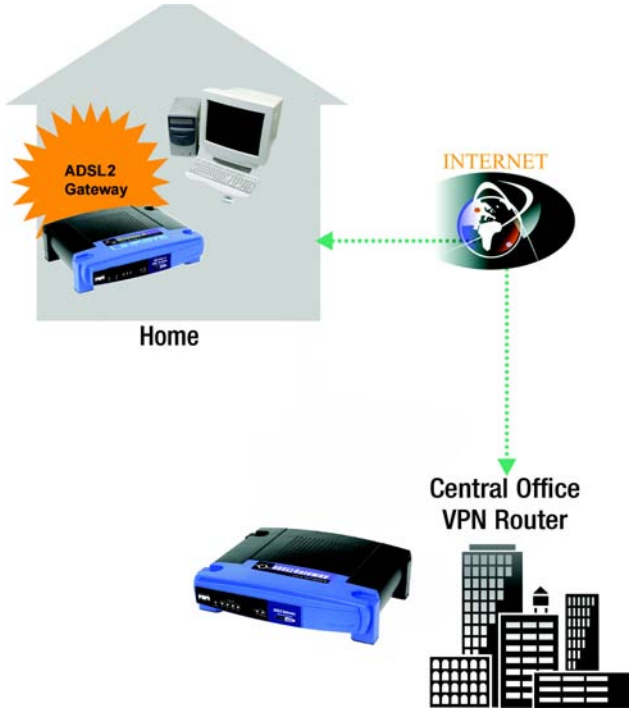


Figure 2-3: VPN Gateway-to-VPN Gateway

Chapter 3: Getting to Know the ADSL2 Gateway with 4-Port Switch

The Back Panel

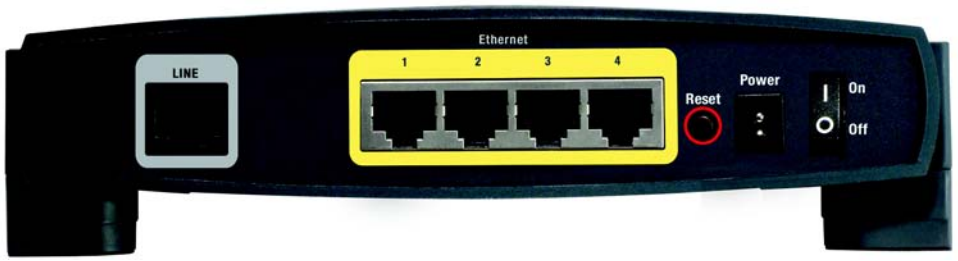


Figure 3-1: Back Panel

The Gateway's ports, where a network cable is connected, are located on the back panel. The Gateway's buttons are also located on the back panel.

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

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

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

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

On/Off Switch This switch is used to turn the Gateway on or off.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys international website at www.linksys.com/international for more information about products that work with the Gateway.

Important: Resetting the Gateway to factory defaults will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Gateway if you want to retain these settings.

The Front Panel

The Gateway's LEDs, where information about network activity is displayed, are located on the front panel.

Figure 3-2: Front Panel

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

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

DSL Green. The **DSL** LED lights up whenever there is a successful DSL connection. The LED blinks while establishing the ADSL connection.

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

Chapter 4: Connecting the ADSL2 Gateway with 4-Port Switch

Overview

The Gateway's setup consists of more than simply plugging hardware together. You will have to configure your networked computers to accept the IP addresses that the Gateway assigns them (if applicable), and you will also have to configure the Gateway with setting(s) provided by your Internet Service Provider (ISP).

The installation technician from your ISP should have left the setup information for your modem with you after installing your broadband connection. If not, you can call your ISP to request that data.

After you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Gateway.

Connection to a Computer

1. Before you begin, make sure that all of your network's hardware is powered off, including the Gateway and all computers.
2. Connect one end of an Ethernet network cable to one of the Ethernet ports (labeled 1-4) on the back of the Gateway (see Figure 4-1), and the other end to an Ethernet port on a computer.
3. Repeat this step to connect more computers, a switch, or other network devices to the Gateway.

Figure 4-1: Ethernet Connection

NOTE: A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.

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

For countries that do **not** have phone jacks with RJ-11 connectors (e.g. France, Sweden, Switzerland, United Kingdom, etc.), except for ISDN users, the microfilter has to be used between the modem and the wall jack, because the microfilter will have the RJ-11 connector.

Annex B users (E1 and DE versions of the Gateway) must use the included special cable to connect the gateway to the wall jack (RJ-45 to RJ-12). If you require splitters or special jacks, please contact your service provider.

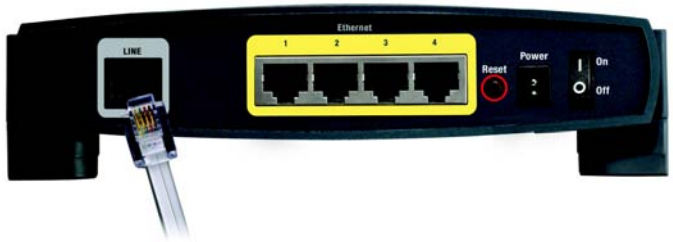


Figure 4-2: ADSL Connection

4. Connect a phone cable from the Line port on the Gateway's back panel (see Figure 4-2) to the wall jack of the ADSL line. A small device called a microfilter may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.

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

5. Connect the power adapter to the Gateway's Power port (see Figure 4-3), and then plug the power adapter into a power outlet. Turn the On/Off switch to On.

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

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

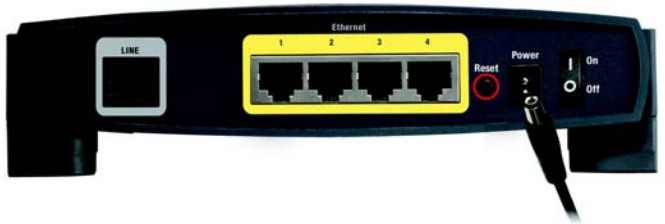


Figure 4-3: Power Connection

The Gateway's hardware installation is now complete.

Go to "Chapter 5: Configuring the Gateway."

NOTE: You should always change the SSID from its default, linksys, and enable WEP encryption.

Chapter 5: Configuring the Gateway

Overview

Follow the steps in this chapter and use the Gateway's web-based utility to configure the Gateway. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Gateway. For a basic network setup, most users only have to use the following screens of the Utility:

- Basic Setup. On the Basic Setup screen, enter the settings provided by your ISP.
- Management. Click the **Administration** tab and then the **Management** tab. The Gateway's default username and password is admin. To secure the Gateway, change the Password from its default.

There are six main tabs: Setup, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

Setup

- Basic Setup. Enter the Internet connection and network settings on this screen.
- DDNS. To enable the Gateway's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.
- Advanced Routing. On this screen, you can alter Dynamic Routing, and Static Routing configurations.

Security

- Firewall. This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests.
- VPN. To enable or disable IPSec and/or PPTP Pass-through, and set up VPN tunnels, use this screen.

Access Restrictions

- Internet Access. This screen allows you to prevent or permit only certain users from attaching to your network.

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 password through the Administration tab.

Applications & Gaming

- Single Port Forwarding. Use this screen to set up common services or applications on your network.
- Port Range Forwarding. To set up public services or other specialized Internet applications on your network, click this tab.
- Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, click this tab.
- DMZ. To allow one local user to be exposed to the Internet for use of special-purpose services, use this screen.
- QoS. QoS ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as Internet phone calls or videoconferencing.

Administration

- Management. On this screen, alter Gateway access privileges, SNMP, UPnP, and WT-82 settings.
- Reporting. If you want to view or save activity logs, click this tab.
- Diagnostics. Use this screen to do a Ping Test.
- Backup&Restore. The Backup&Restore tab allows you to back up and restore the Gateway's configuration file.
- Factory Defaults. If you want to restore the Gateway's factory defaults, use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Gateway's firmware.
- Reboot. This tab allows you to do a soft or hard reboot of your Gateway.

Status

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

How to Access the Web-based Utility

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

A password request page, shown in Figure 5-1 will appear. (non-Windows XP users will see a similar screen.) Enter **admin** (the default user name) in the User Name field, and enter **admin** (the default password) in the Password field. Then click the **OK** button.

Figure 5-1: Password Screen

The Setup Tab

The Basic Setup Tab

The first screen that appears is the Basic Setup tab. This tab allows you to change the Gateway's general settings. Change these settings as described here and click the **Save Settings** button to save your changes or **Cancel Changes** to cancel your changes.

Internet Setup

- PVC Connection. Select a PVC connection number from the drop-down menu. Then, select the **Enable Now** to enable the connection.
- VC Settings. Virtual Circuits (VPI and VCI): These fields consist of two items: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
  - Multiplexing: Select **LLC** or **VC** , depending on your ISP.
  - QOS Type: Select from the drop-down menu: **CBR**, Continuous Bit Rate to specify fixed bandwidth for voice or data traffic; **UBR**, Unspecific Bit Rate for application that are none-time sensitive, such as email; or **VBR**, Variable Bite Rate for Bursty traffic and bandwidth sharing with other application.
  - Pcr Rate: Peak Cell Rate, divide the DSL line rate by 424 to find the PCR to get the maximum rate the sender can send cells. Enter the rate in the field (if required by your service provider).
  - Scr Rate: Sustain Cell Rate, sets the average cell rate that can be transmitted. SCR normally less than PCR. Enter the rate in the field (if required by your service provider).
  - Autodetect: Select **Enable** to have the settings automatically entered or **Disable** to enter the values manually.
  - Virtual Circuit: Enter the VPI and VCi ranges in the fields.

Figure 5-2: Basic Setup Tab

- Internet Connection Type. The Gateway supports five Encapsulations: RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA, and Bridged Mode Only. Each Basic Setup screen and available features will differ depending on what type of encapsulation you select.

RFC 1483 Bridged

Dynamic IP

IP Settings. Select **Obtain an IP Address Automatically** if your ISP says you are connecting through a dynamic IP address.

Static IP

If you are required to use a permanent (static) IP address to connect to the Internet, then select **Use the following IP Address**.

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

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

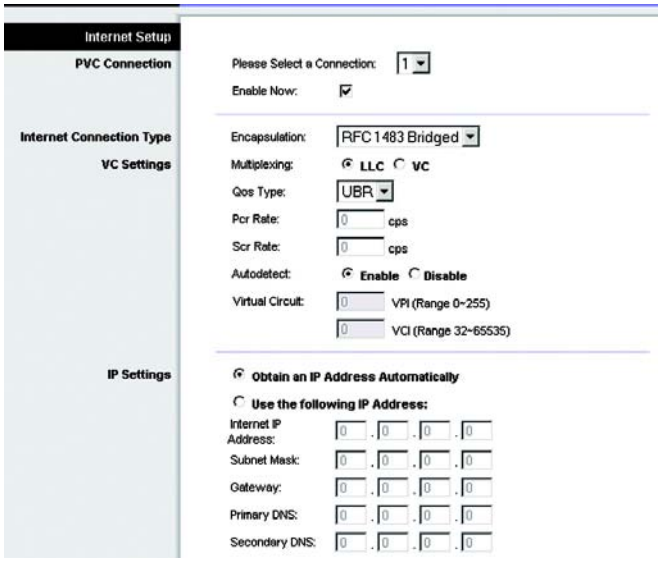


Figure 5-3: Dynamic IP

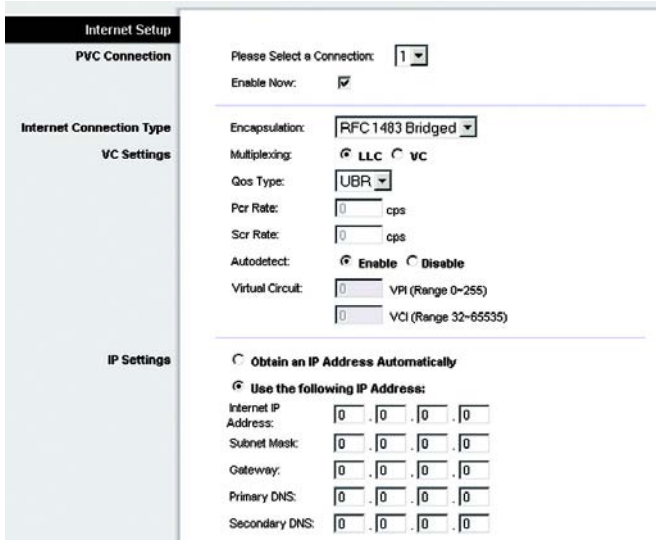


Figure 5-4: Static IP

IPoA

If you are required to use RFC 1577 IPoA (Classical IP over ATM), then select **IPoA**.

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

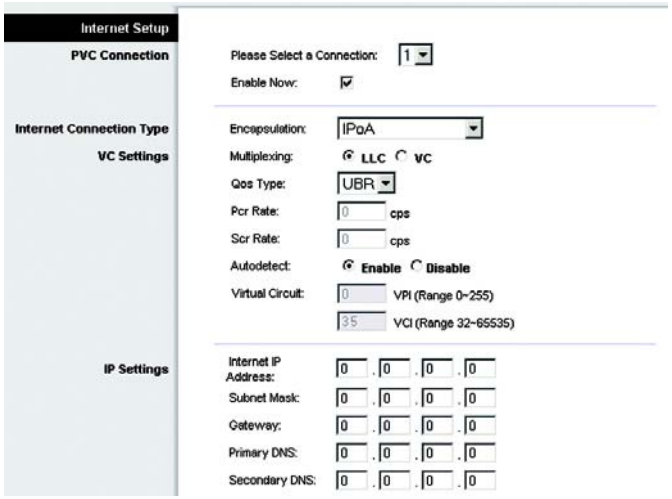


Figure 5-5: IPoA

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.

- Service Name. Enter the name of your PPPoE service in the field.
- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Gateway to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive: Redial Period. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the Gateway to check the Internet connection. The default Redial Period is 30 seconds.

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

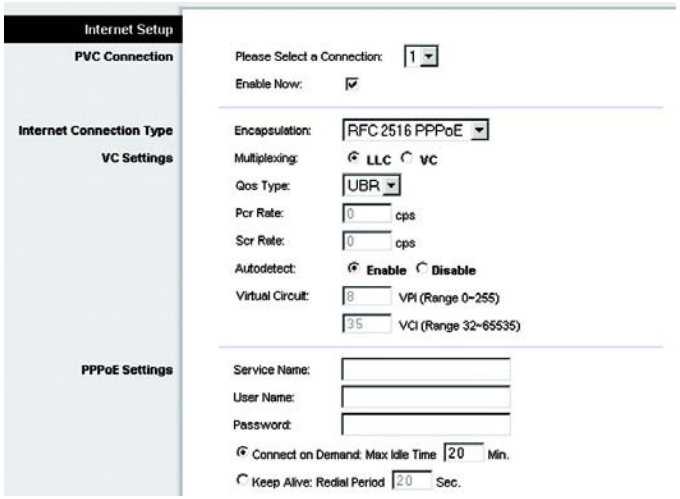


Figure 5-6: RFC 2516 PPPoE

RFC 2364 PPPoA

Some DSL-based ISPs use PPPoA (Point-to-Point Protocol over ATM) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoA. If they do, you will have to enable PPPoA.

- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Gateway to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive Option: Redial Period. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the Gateway to check the Internet connection. The default Redial Period is 30 seconds.

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

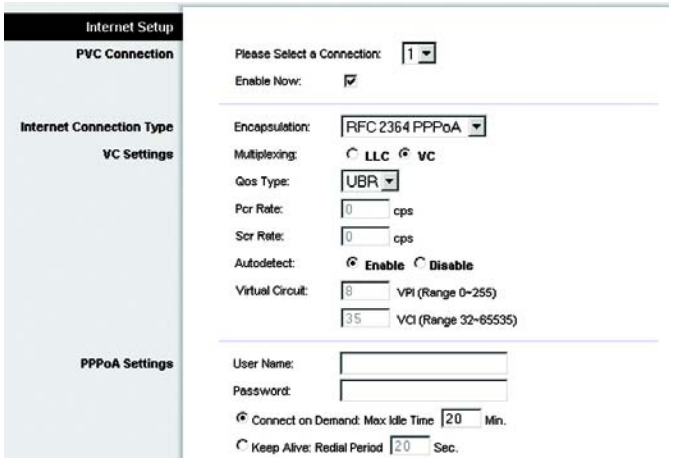


Figure 5-7: RFC 2364 PPPoA

Bridged Mode Only

If you are using your Gateway as a bridge, which makes the Gateway act like a standalone modem, select **Bridged Mode Only**. All NAT and routing is disabled in this mode.

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

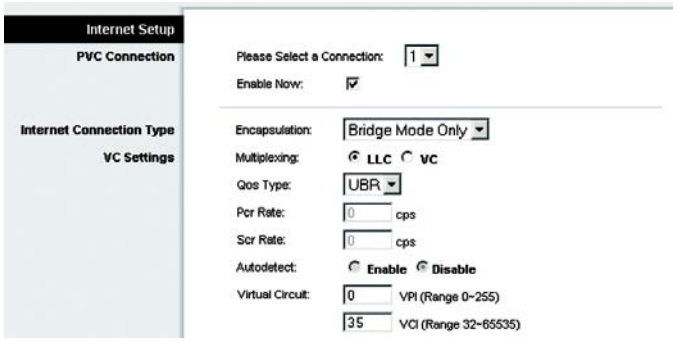


Figure 5-8: Bridged Mode Only

Optional Settings (Required by some ISPs)

- Host Name and Domain Name. These fields allow you to supply a host and domain name for the Gateway. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.
- MTU. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Manual** and enter the value desired in the *Size* field. It is recommended that you leave this value in the 1200 to 1500 range. By default, MTU is configured automatically.

Network Setup

- Router IP. The values for the Gateway's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.
  - Local IP Address. The default value is 192.168.1.1.
  - Subnet Mask. The default value is 255.255.255.0.
- Network Address Server Settings (DHCP). A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, it is highly recommended that you leave the Gateway enabled as a DHCP server.
  - DHCP Relay Server. If you enable the Local DHCP Server or DHCP Relay for the Local DHCP server, enter the IP address for the DHCP server in the fields.
  - AutoDetect LAN DHCP Server.
  - Starting IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, because the default IP address for the Gateway is 192.168.1.1.
  - Maximum Number of DHCP Users. Enter the maximum number of users/clients that can obtain an IP address. The number will vary depending on the starting IP address entered.
  - Client Lease Time. The Client Lease Time is the amount of time a network user will be allowed connection to the Gateway with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.
  - Static DNS 1-3. The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You

Figure 5-9: Optional Settings

can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

- WINS. The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.
- Time Setting. This is where you set the time zone for your Gateway. Select your time zone from the drop-down menu. If desired, check the **Automatically adjust clock for daylight saving changes**.

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

The DDNS Tab

The Gateway offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Gateway.

Before you can use this feature, you need to sign up for DDNS service at DynDNS.org.

DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** in the drop-down menu. (See Figure 5-10.) To disable DDNS Service, select **Disabled**.

DynDNS.org

- User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
- Internet IP Address. The Gateway's current Internet IP Address is displayed here. Because it is dynamic, it will change.
- Status. The status of the DDNS service connection is displayed here.

TZO.com

- Email Address, Password, and Domain Name. Enter the Email Address, TZO Password Key, and Domain Name of the service you set up with TZO.

Figure 5-10: DynDNS.org

Figure 5-11: TZO.com

- Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change.
- Status. The status of the DDNS service connection is displayed here.

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

Advanced Routing Tab

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

Advanced Routing

- Operating Mode. NAT is a security feature that is enabled by default. It enables the Gateway to translate IP addresses of your local area network to a different IP address for the Internet. To disable NAT, click the **Disabled** radio button.
- Dynamic Routing. With Dynamic Routing you can enable the Gateway to automatically adjust to physical changes in the network's layout. The Gateway, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other Gateways on the network. To enable RIP, click **Enabled**. To disable RIP, click **Disabled**.
  - Transmit RIP Version. To transmit RIP messages, select the protocol you want: **RIP1, RIP1-Compatible, or RIP2**.
  - Receive RIP Version. To receive RIP messages, select the protocol you want: **RIP1** or **RIP2**.
- Static Routing. If the Gateway is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, change the following settings:
  - Select set number. Select the number of the static route from the drop-down menu. The Gateway supports up to 20 static route entries. If you need to delete a route, after selecting the entry, click the **Delete This Entry** button.
  - Destination IP Address. The Destination IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0.

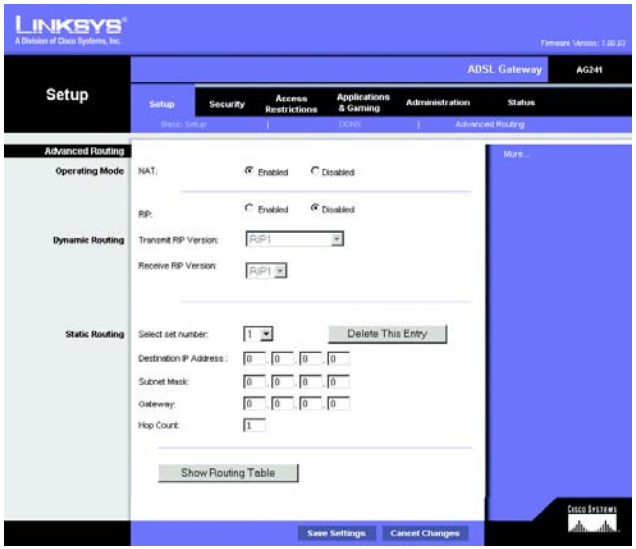


Figure 5-12: Advanced Routing

- Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.
- Hop Count. Hop Count is the number of hops to each node until the destination is reached (16 hops maximum). Enter the Hop Count in the field.

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

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

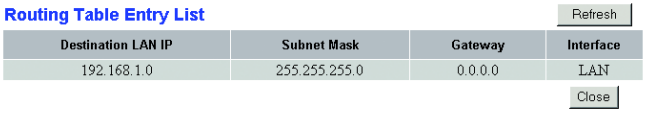


Figure 5-13: Advanced Wireless Settings

The Security Tab

Firewall

When you click the Security tab, you will see the Firewall screen. This screen contains Filters and the option to Block WAN Requests. Filters block specific Internet data types and block anonymous Internet requests. To add Firewall Protection, click **Enable**. If you do not want Firewall Protection, click **Disable**.

Additional Filters

- Filter Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enabled**.
- Filter Cookies. A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click **Enabled**.
- Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java Applet filtering, click **Enabled**.
- Filter ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click **Enabled**.

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.

Figure 5-14: Firewall

VPN

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. The VPN screen allows you to configure your VPN settings to make your network more secure.

VPN Passthrough

- IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enable** button. To disable IPSec Passthrough, click the **Disable** button.
- PPTP Passthrough. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enable** button. To disable PPTP Passthrough, click the **Disable** button.
- L2TP Passthrough. Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used to enable the operation of a VPN over the Internet.To allow L2TP Passthrough, click the **Enable** button. To disable L2TP Passthrough, click the **Disable** button.

IPSec VPN Tunnel

The VPN Gateway creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

- To establish this tunnel, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. It is possible to create up to five simultaneous tunnels. Then click **Enabled** to enable the IPSec VPN tunnel. Once the tunnel is enabled, enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify

multiple tunnels and does not have to match the name used at the other end of the tunnel. To delete a tunnel entry, select the tunnel, then click **Delete**. To view a summary of the settings, click **Summary**.

- Local Secure Group and Remote Secure Group. The Local Secure Group is the computer(s) on your LAN that can access the tunnel. The Remote Secure Group is the computer(s) on the remote end of the tunnel that can access the tunnel. These computers can be specified by a Subnet, specific IP address, or range.

- Local Security Gateway.

- Remote Security Gateway. The Remote Security Gateway is the VPN device, such as a second VPN Gateway, on the remote end of the VPN tunnel. Enter the IP Address or Domain of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Gateway, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Gateway, but the IP Address of the remote VPN Gateway or device with which you wish to communicate. If you enter an IP address, only the specific IP Address will be able to acess the tunnel. If you select **Any**, any IP Address can access the tunnel.

- Encryption. Using Encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable. In Figure 5-19, DES (which is the default) has been selected.

- Authentication. Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, if the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication. In the Manual Key Management screen, MD5 (the default) has been selected.

- Key Management. Select **Auto (IKE)** or **Manual** from the drop-down menu. The two methods are described below.
  Auto (IKE)
  Select **Auto (IKE)** and enter a series of numbers or letters in the Pre-shared Key field. Based on this word, which MUST be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may select to have the key expire at the end of a time period. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure.

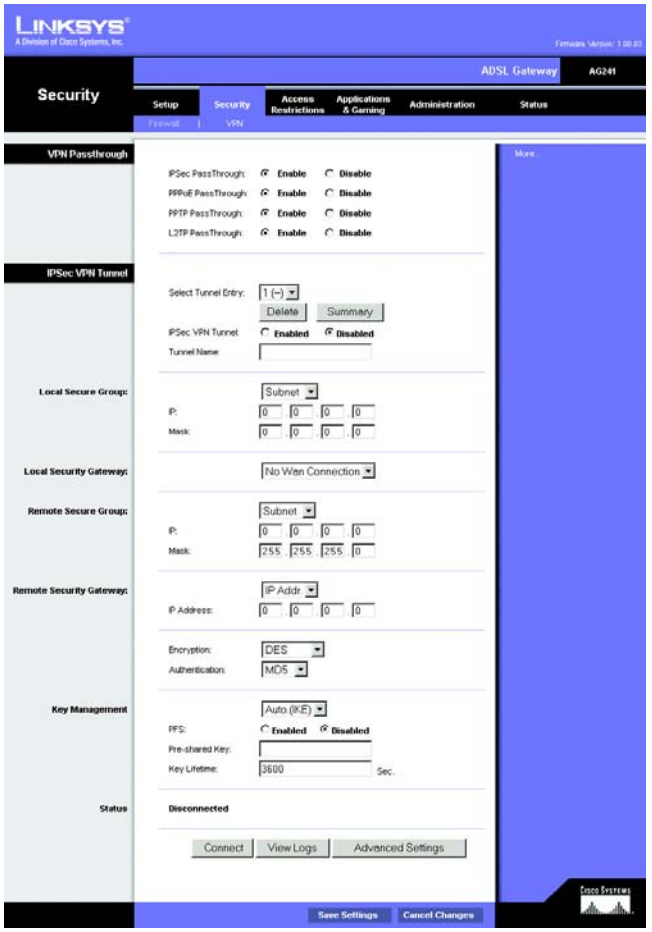


Figure 5-15: VPN

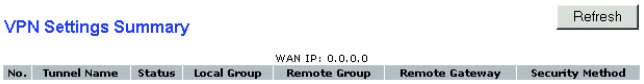


Figure 5-16: VPN Settings Summary

Manual

Select **Manual,** then select the Encryption Algorithm from the drop-down menu. Enter the Encryption Key in the field (if you chose DES for your Encryption Algorithm, enter 16 hexadecimal characters, if you chose 3DES, enter 48 hexadecimal characters). Select the Authentication Algorithm from the drop-down menu. Enter the Authentication Key in the field (if you chose MD5 for your Authentication Algorithm, enter 32 hexadecimal characters, if you chose SHA1, enter 40 hexadecimal characters). Enter the Inbound and Outbound SPIs in the respective fields.

- Status. The status of the connection is shown.

Click the **Connect** button to connect your VPN tunnel. Click **View Logs** to view system, UPnP, VPN, firewall, access, or all logs.Click the **Advanced Settings** button and the Advanced IPSec VPN Tunnel Setup screen will appear.

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

Advanced VPN Tunnel Setup

From the Advanced IPSec VPN Tunnel Setup screen you can adjust the settings for specific VPN tunnels.

Phase 1

- Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.
- Operation Mode. There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Gateway will accept both Main and Aggressive requests from the remote VPN device.
- Encryption. Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.
- Authentication. Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.
- Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

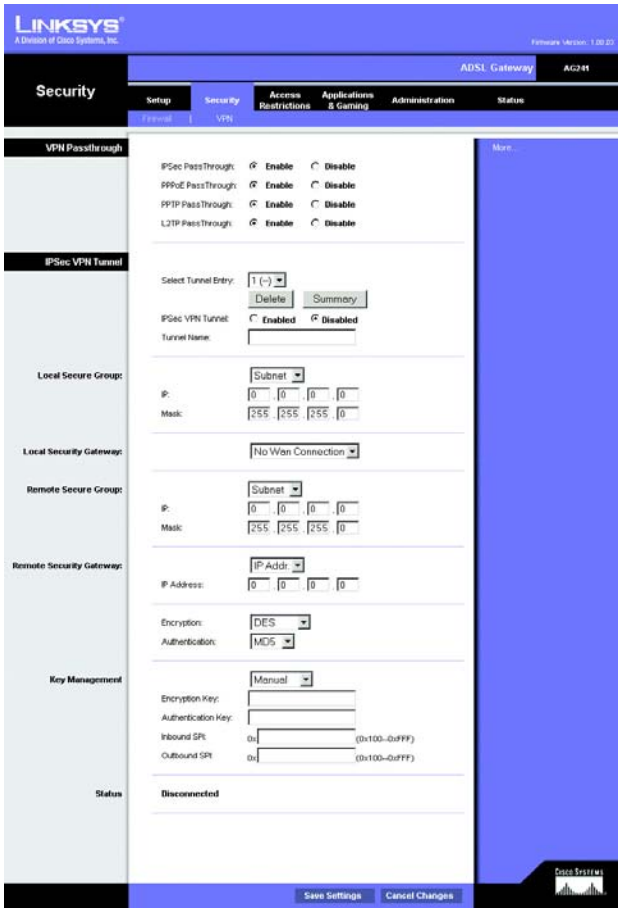


Figure 5-17: Manual Key Management

Figure 5-18: System Log

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

Phase 2

- Encryption. The encryption method selected in Phase 1 will be displayed.
- Authentication. The authentication method selected in Phase 1 will be displayed.
- PFS. The status of PFS will be displayed.
- Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.
- Key Life Time. In the Key Lifetime field, you may select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Other Setting

- NetBIOS broadcast. Check the box next to NetBIOS broadcast to enable NetBIOS traffic to pass through the VPN tunnel.
- Anti-replay. Check the box next to Anti-replay to enable the Anti-replay protection. This feature keeps track of sequence numbers as packets arrive, ensuring security at the IP packet-level.
- Keep-Alive. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection.
- Check this box to block unauthorized IP addresses. Enter in the field to specify how many times IKE must fail before blocking that unauthorized IP address. Enter the length of time that you specify (in seconds) in the field.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. For further help on this tab, click the **Help** button.

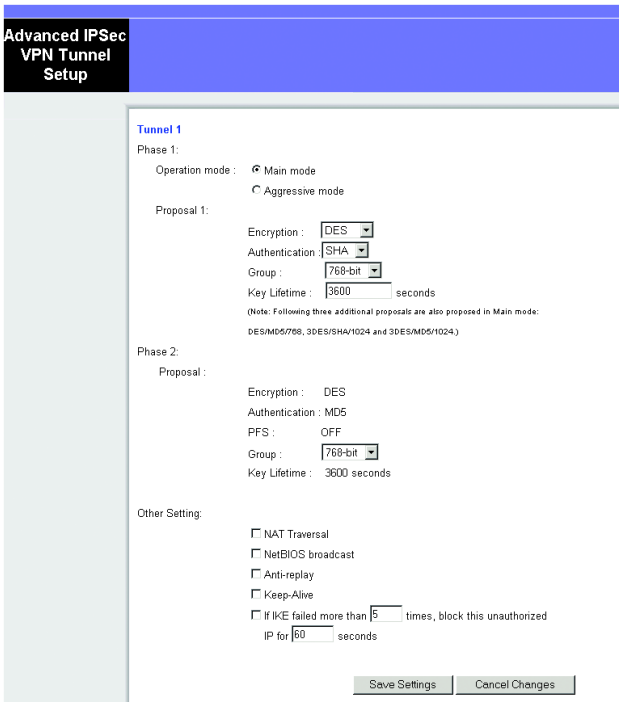


Figure 5-19: Advanced VPN Tunnel Setup

The Access Restrictions Tab

Internet Access

The Access Restrictions tab allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific computers and set up filters by using network port numbers.

- Internet Access Policy. Multiple Filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the **Delete** button. To see a summary of all Policies, click the **Summary** button.

  The summaries are listed on this screen with their name and settings. To return to the Filters tab, click the **Close** button.

- Enter Policy Name. Policies are created from the fields presented here.

  To create an Internet Access policy:

1. Enter a Policy Name in the field provided. Select **Internet Access** as the Policy Type.

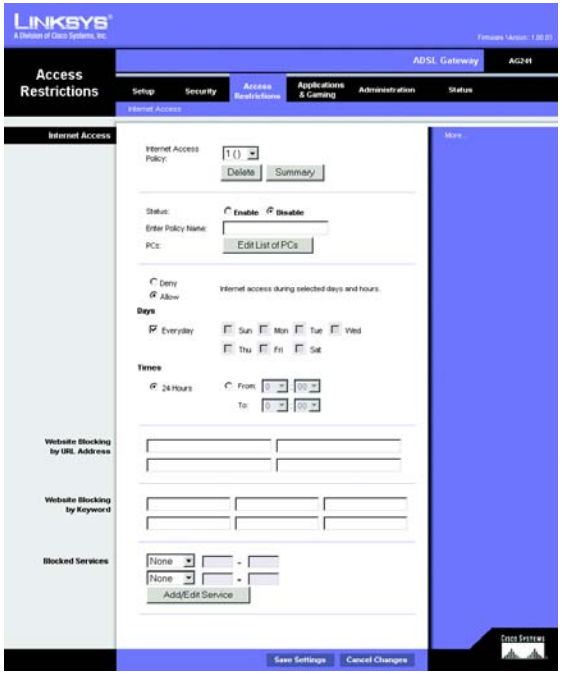


Figure 5-20: Internet Access

2. Click the **Edit List of PCs** button. This will open the List of PCs screen. From this screen, you can enter the IP address or MAC address of any computer to which this policy will apply. You can even enter ranges of computers by IP address. Click the **Save Settings** button to save your settings, the **Cancel Changes** button to undo any changes and return to the Filters tab.

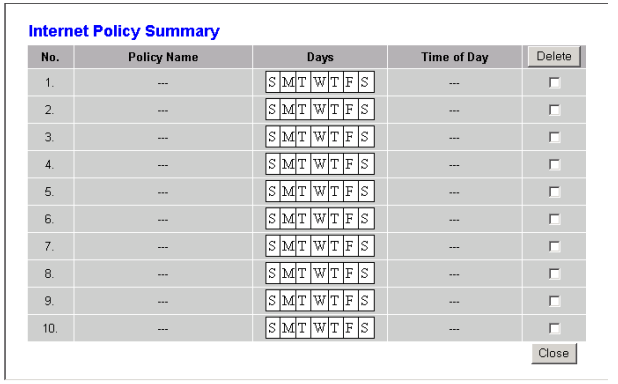


Figure 5-21: Internet Policy Summary

3. If you wish to Deny or Allow Internet access for those computers you listed on the List of PCs screen, click the option.

4. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services. If a service isn't listed, you can click the **Add/ Edit Service** button to open the Port Services screen and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service.

5. By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered.

6. Click the **Save Settings** button to activate the policy.

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Website Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Website Blocking by Keyword fields.

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

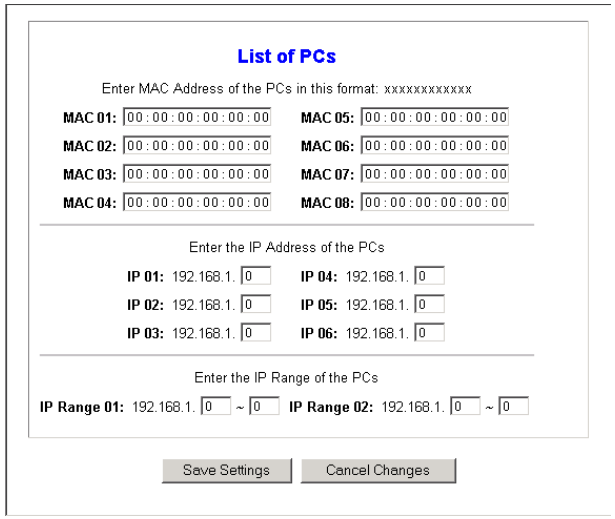


Figure 5-22: List of PCs

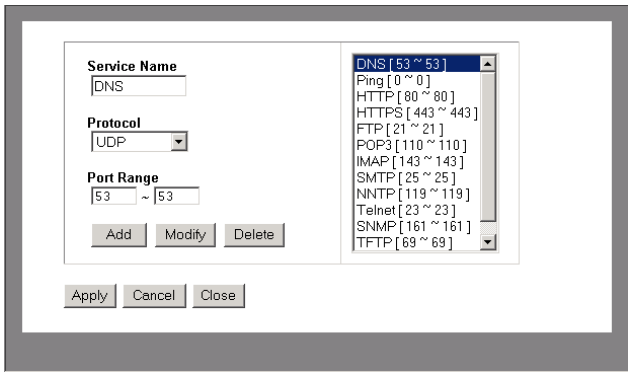


Figure 5-23: Port Services

The Applications and Gaming Tab

Single Port Forwarding

The Single Port Forwarding screen provides options for customization of port services for common applications.

When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Choose or enter the Application in the field. Then, enter the External and Internal Port numbers in the fields. Select the type of protocol you wish to use for each application: **TCP** or **UDP**. Enter the IP Address in the field. Click **Enabled** to enable Forwarding for the chosen application.

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

Figure 5-24: Single Port Forwarding

Port Range Forwarding

The Port Forwarding screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- Application. Enter the name you wish to give each application.
- Start and End. Enter the starting and ending numbers of the port you wish to forward.
- TCP UDP. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address and Click **Enabled**.

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

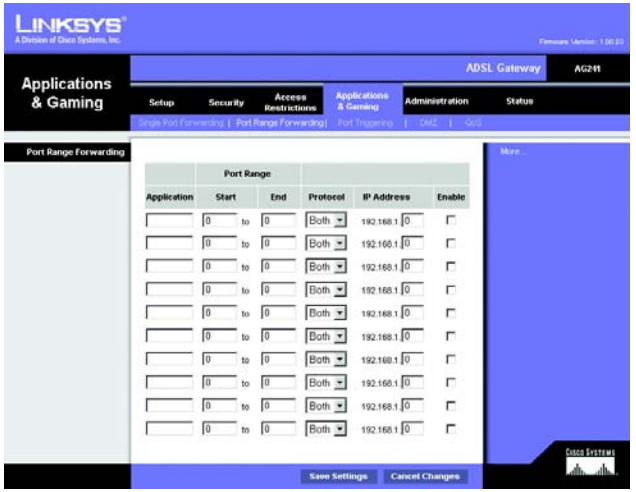


Figure 5-25: Port Range Forwarding

Port Triggering

Port Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Gateway will watch outgoing data for specific port numbers. The Gateway will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Gateway, the data is pulled back to the proper computer by way of IP address and port mapping rules.

- Application. Enter the name you wish to give each application.
- Start Port and End Port. Enter the starting and ending Triggered Range numbers and the Incoming Forwarded Range numbers of the port you wish to forward.

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

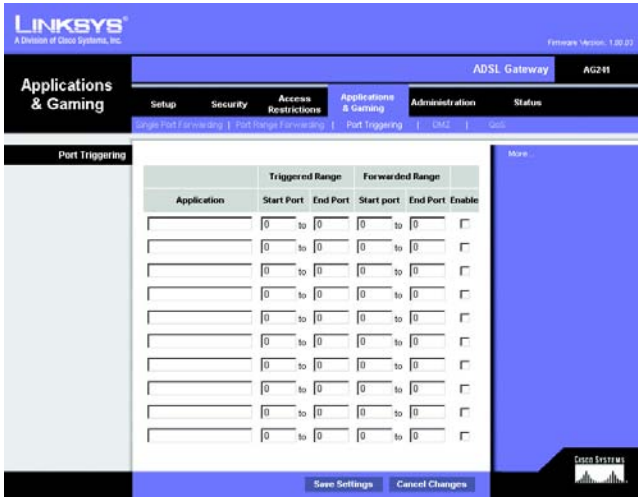


Figure 5-26: Port Triggering

DMZ

The DMZ screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing through DMZ Hosting. DMZ hosting forwards all the ports for one computer at the same time, which differs from Port Range Forwarding, which can only forward a maximum of 10 ranges of ports.

- DMZ Hosting. This feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enabled**. To disable DMZ , select **Disabled**.
- DMZ Host IP Address. To expose one computer, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter."

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

Figure 5-27: DMZ

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.

Application-based QoS

Application-based QoS manages information as it is transmitted and received. Depending on the settings of the *QoS* screen, this feature will assign information a high or low priority for the five preset applications and three additional applications that you specify.

Enable/Disable. To use application-based QoS, select **Enable**. Otherwise, keep the default, **Disable**.

High priority/Medium priority/Low priority. For each application, select **High priority** (traffic on this queue shares 60% of the total bandwidth), **Medium priority** (traffic on this queue shares 18% of the total bandwidth), or **Low priority** (traffic on this queue shares 1% of the total bandwidth).

FTP (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

HTTP (HyperText Transport Protocol). The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

SMTP (Simple Mail Transfer Protocol). The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

POP3 (Post Office Protocol 3). A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

Specific Port#. You can add three additional applications by entering their respective port numbers in the *Specific Port#* fields.

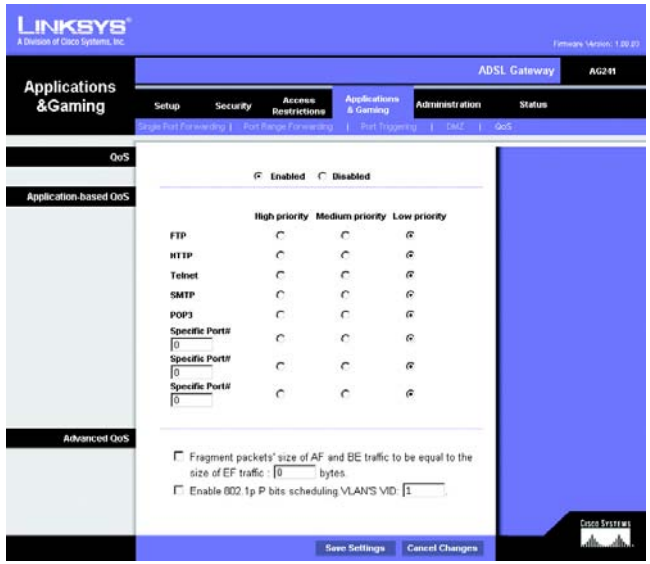


Figure 5-28: QOS

Advanced QoS

This setting allows you to specify traffic queue priority.

Fragment packet's size of AF and BE traffic to be equal to the size of EF traffic. Select this option to fragmentize the packet sizes for AF (Assured Forwarding) and BE (Best Effort) queues so that it will increase the efficiency for transporting EF (expedited forwarding) queues. Enter a range between 68~1492 bytes.

Enable 802.1p P bits scheduling. VLAN's VID. Select this option to enable 802.1p P bits classification scheduling in the appropriate VLAN based on IEEE 802.1Q VLAN identification. Enter the VLAN VID (VLAN Identifier) number in the field.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

The Administration Tab

Management

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

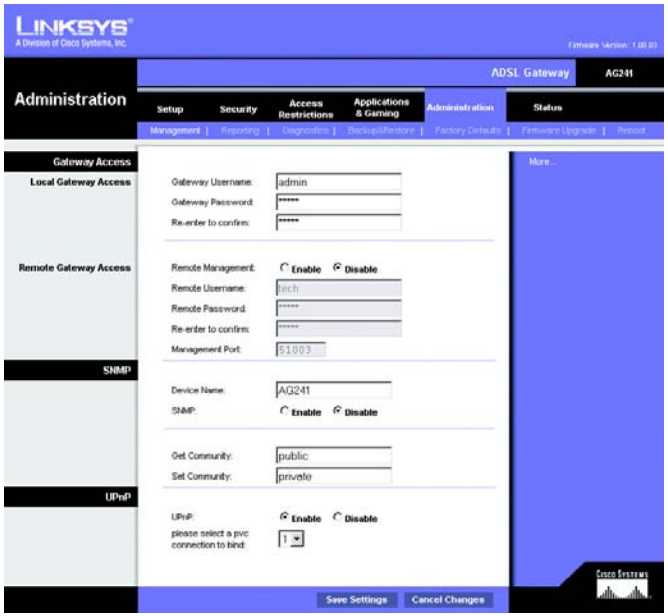


Figure 5-29: Management

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

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

- Remote Administration. This feature allows you to manage the Gateway from a remote location via the Internet. To enable Remote Administration, click **Enabled**.
- Administration Port. Enter the port number you will use to remotely access the Gateway.

SNMP

SNMP is a popular network monitoring and management protocol.

Identification. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**.

UPnP

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

UPnp. To enable UPnP, click **Enabled**.

Please select a pvc connection to bind. Select a number from the drop-down menu._____

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

Reporting

The Reporting tab provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection. It also provides logs for VPN and firewall events.

- Log. To enable log reporting, click **Enabled**.
- Logviewer IP Address. Enter the IP Address that will receive logs into the field.

Figure 5-30: Reporting

Email Alerts

E-Mail Alerts. To enable E-Mail Alerts, click **Enabled**.

- Denial of Service Thresholds. Enter the thresholds of events you want to receive.
- SMTP Mail Server. Enter the IP Address of the SMTP server in the field.
- E-Mail Address for Alert Logs. Enter the e-mail address for alert logs in the field.
- Return E-Mail address. Enter the address for the return e-mail.

To view the logs, click the **View Logs** button.

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

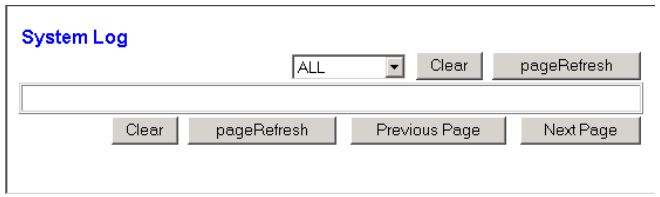


Figure 5-31: System Log

Diagnostics

Ping Test

Ping Test Parameters

- Ping Target IP. Enter the IP Address that you want to ping in the field. This can be either a local (LAN) IP or an Internet (WAN) IP address.
- Ping Size. Enter the size of the ping packets.
- Number of Pings. Enter the number of times that you want to ping.
- Ping Interval. Enter the ping interval in milliseconds.
- Ping Timeout. Enter the time in milliseconds.
- Ping Result. The results of the ping test will be shown here.

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

Figure 5-32: Ping Test

Backup&Restore

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

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

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

Figure 5-33: Backup&Restore

Factory Defaults

Restore Factory Defaults. If you wish to restore the Gateway to its factory default settings and lose all your settings, click **Yes**.

To begin the restore process, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Figure 5-34: Factory Defaults

Firmware Upgrade

The ADSL Gateway allows you to upgrade firmware for the LAN (network) side of the Gateway.

Upgrade from LAN

To upgrade the Gateway's firmware from the LAN:

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

Figure 5-35: Firmware Upgrade

Reboot

This tab allows you to do a soft or hard reboot of your Gateway.

Reboot Mode. To reboot your Gateway, select **Hard** or **Soft**. Choose hard to power cycle the Gateway or soft to restart it without a power cycle.

To begin the reboot process, click the **Save Settings** button. When a screen appears asking you if you really want to reboot the device. Click **OK**.

Click the **Cancel Changes** button if you want to undo your changes.

Figure 5-36: Reboot

The Status Tab

Gateway

This screen displays information about your Gateway and its WAN (Internet) Connections.

Gateway Information

Gateway Information displays the Software Version, MAC Address, and Current Time.

Internet Connections

The Internet Connections will be displayed after selecting the Internet connection number from the drop-down menu. They are the Login Type, interface, IP Address, Subnet Mask, Default Gateway, and DNS 1, 2, and 3 servers.

DHCP Renew. Click the **DHCP Renew** button to replace your Gateway's current IP address with a new IP address.

DHCP Release. Click the **DHCP Release** button to delete your Gateway's current IP address.

Click the **Refresh** button if you want to Refresh your screen.

Local Network

The Local Network information that is displayed is the local Mac Address, IP Address, Subnet Mask, and DHCP Server, Start IP Address, and End IP Address. To view the DHCP Clients Table, click the **DHCP Clients Table** button.

DHCP Clients Table. Click the **DHCP Clients Table** button to show the current DHCP Client data. You will see the MAC address, computer name, and IP address of the network clients using the DHCP server. (This data is stored in temporary memory and changes periodically.) To delete a client from the DHCP server, select the client, then click the **Delete** button.

Click the **Refresh** button if you want to Refresh your screen. Click the **Close** button to close the screen.

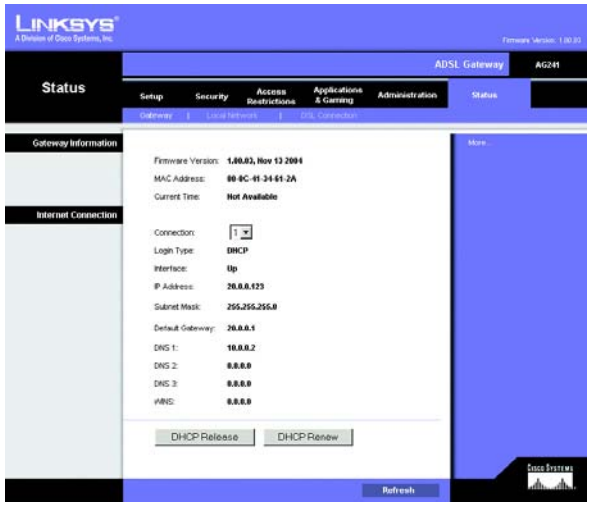


Figure 5-37: Status

Figure 5-38: Local Network

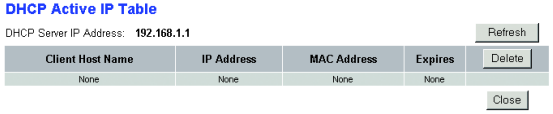


Figure 5-39: DHCP Clients Table

DSL Connection

The DSL Connection information that is displayed is the Status, Downstream Rate, and Upstream Rate.

The PVC Connection information that is displayed is Encapsulation, Multiplexing, QoS, Pcr Rate, Scr Rate, Autodetect, VPI, VCI, and PVC Status.

Click the **Refresh** button if you want to Refresh your screen.

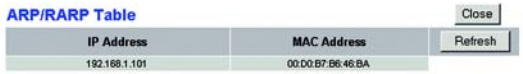


Figure 5-40: DSL Connection

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, or RFC 2364 PPPoA. Please refer to the Setup section of "Chapter 5: Configuring the Gateway" 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 D: 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 need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

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 D: 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 D: 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 4.7 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 5: Configuring the Gateway."

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 20 (seconds).
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**.

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 D: 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.

What is the maximum number of VPN sessions allowed by the Gateway?
The maximum number depends on many factors. At least one IPSec session will work through the Gateway; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

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.

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 many channels/frequencies are available with the Gateway?
There are eleven available channels, ranging from 1 to 11 (in North America).

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

Appendix B: Configuring IPSec between a Windows 2000 or XP Computer and the Gateway

Introduction

This document demonstrates how to establish a secure IPSec tunnel using preshared keys to join a private network inside the Gateway and a Windows 2000 or XP computer. You can find detailed information on configuring the Windows 2000 server at the Microsoft website:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

NOTE: Keep a record of any changes you make. Those changes will be identical in the Windows "secpol" application and the Router's Web-Based Utility.

Environment

The IP addresses and other specifics mentioned in this appendix are for illustration purposes only.

NOTE: This section's instructions and figures refer to the Router. Substitute "Gateway" for "Router". Also, the text on your screen may differ from the text in your instructions for "OK or Close"; click the appropriate button on your screen.

Windows 2000 or Windows XP
IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

WAG54G

WAN IP Address: 140.111.1.1 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0
LAN IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

How to Establish a Secure IPSec Tunnel

Step 1: Create an IPSec Policy

1. Click the **Start** button, select **Run**, and type **secpol.msc** in the **Open** field. The *Local Security Setting* screen will appear as shown in Figure C-1.
2. Right-click **IP Security Policies on Local Computer** (Win XP) or **IP Security Policies on Local Machine** (Win 2000), and click **Create IP Security Policy**.
3. Click the **Next** button, and then enter a name for your policy (for example, to_Router). Then, click **Next**.
4. Deselect the **Activate the default response rule** check box, and then click the **Next** button.
5. Click the **Finish** button, making sure the **Edit** check box is checked.

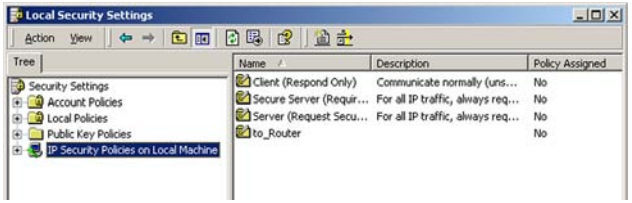


Figure B-1: Local Security Screen

NOTE: The references in this section to "win" are references to Windows 2000 and XP. Substitute the references to "Router" with "Gateway". Also, the text on your screen may differ from the text in your instructions for "OK or Close"; click the appropriate button on your screen.

Step 2: Build Filter Lists

Filter List 1: win->Router

1. In the new policy's properties screen, verify that the **Rules** tab is selected, as shown in Figure C-2. Deselect the **Use Add Wizard** check box, and click the **Add** button to create a new rule.
2. Make sure the **IP Filter List** tab is selected, and click the **Add** button. (See Figure C-3.)The *IP Filter List* screen should appear, as shown in Figure C-4. Enter an appropriate name, such as win->Router, for the filter list, and de-select the **Use Add Wizard** check box. Then, click the **Add** button.

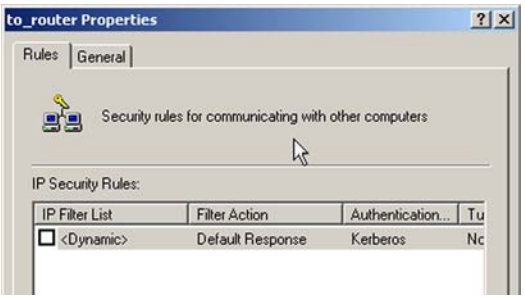


Figure B-2: Rules Tab

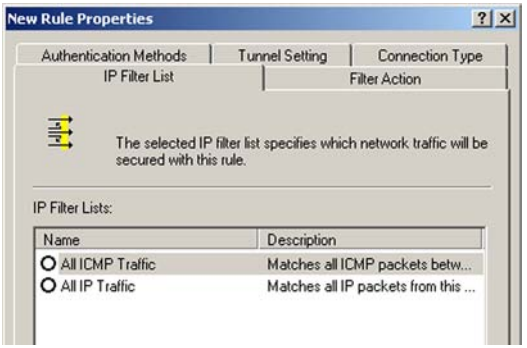


Figure B-3: IP Filter List Tab

3. The *Filters Properties* screen will appear, as shown in Figure C-5. Select the **Addressing** tab. In the *Source address* field, select **My IP Address**. In the *Destination address* field, select **A specific IP Subnet**, and fill in the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (These are the Router's default settings. If you have changed these settings, enter your new values.)

4. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

5. Click the **OK** button. Then, click the **OK** or **Close** button on the *IP Filter List* window.

Filter List 2: Router ->win

6. The *New Rule Properties* screen will appear, as shown in Figure C-6. Select the **IP Filter List** tab, and make sure that **win -> Router** is highlighted. Then, click the **Add** button.

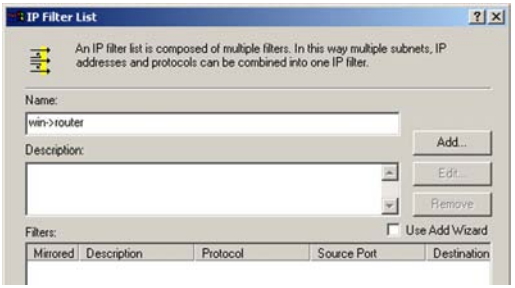


Figure B-4: IP Filter LIst

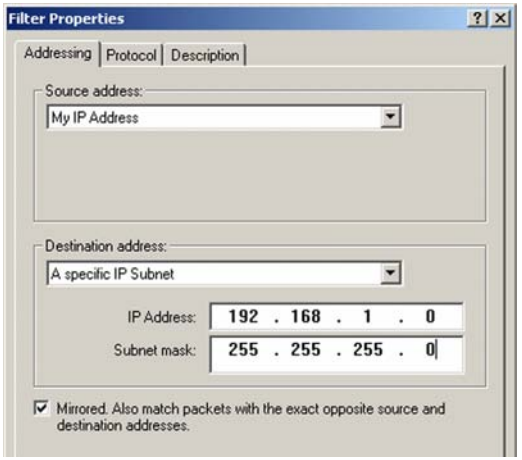


Figure B-5: Filters Properties

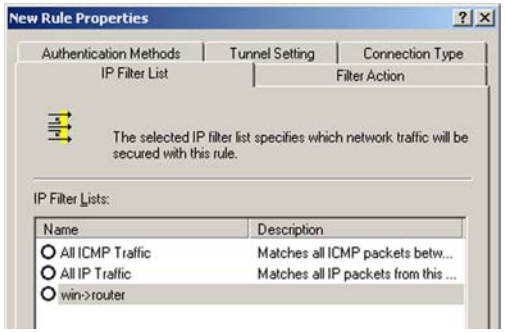


Figure B-6: New Rule Properties

7. The *IP Filter List* screen should appear, as shown in Figure C-7. Enter an appropriate name, such as Router->win for the filter list, and de-select the **Use Add Wizard** check box. Click the **Add** button.

8. The *Filters Properties* screen will appear, as shown in Figure C-8. Select the Addressing tab. In the *Source address* field, select **A specific IP Subnet**, and enter the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (Enter your new values if you have changed the default settings.) In the Destination address field, select **My IP Address**.

9. If you want to enter a description for your filter, click the *Description* tab and enter the description there.

10. Click the **OK** or **Close** button and the *New Rule Properties* screen should appear with the IP Filer List tab selected, as shown in Figure C-9. There should now be a listing for "Router -> win" and "win -> Router". Click the **OK** (for WinXP) or **Close** (for Win2000) button on the *IP Filter List* window.

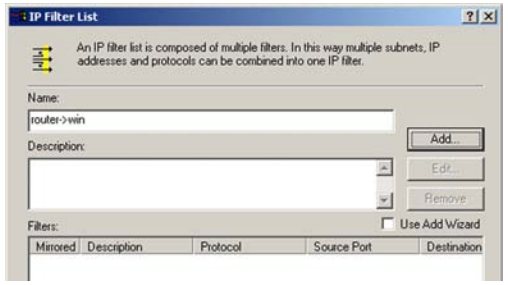


Figure B-7: IP Filter List

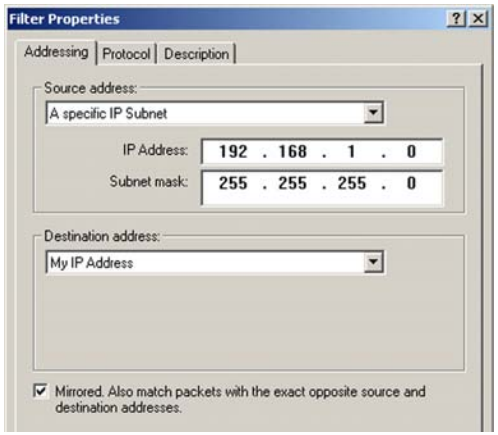


Figure B-8: Filters Properties

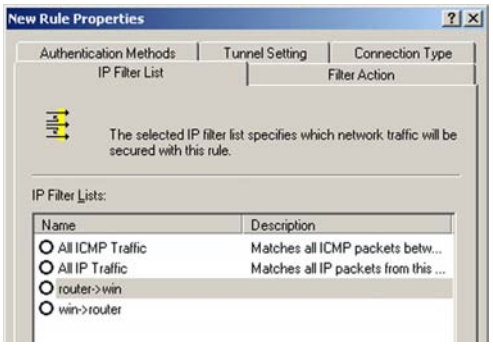


Figure B-9: New Rule Properties

Step 3: Configure Individual Tunnel Rules

Tunnel 1: win->Router

1. From the *IP Filter List* tab, shown in Figure C-10, click the filter list win->Router.

2. Click the **Filter Action** tab (as in Figure C-11), and click the filter action **Require Security** radio button. Then, click the **Edit** button.

3. From the *Security Methods* tab, shown in Figure C-12, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

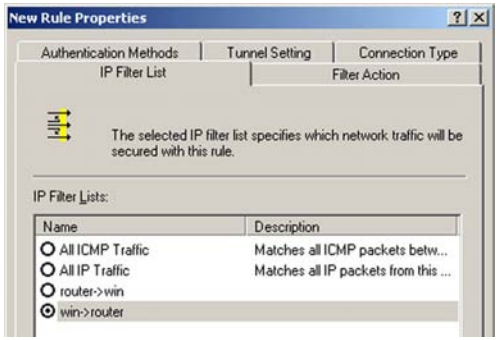


Figure B-10: IP Filter List Tab

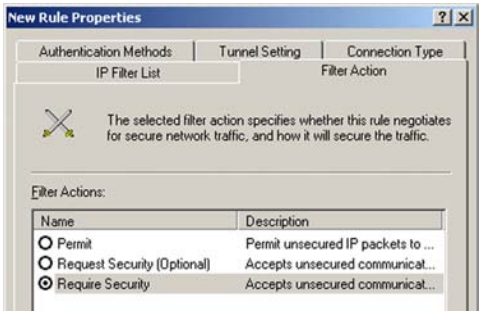


Figure B-11: Filter Acton Tab

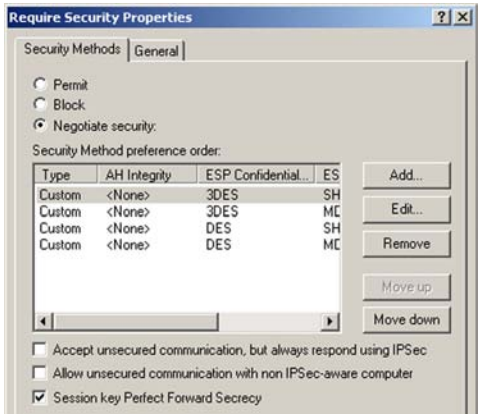


Figure B-12: Security Methods Tab

4. Select the **Authentication Methods** tab, shown in Figure C-13, and click the **Edit** button.

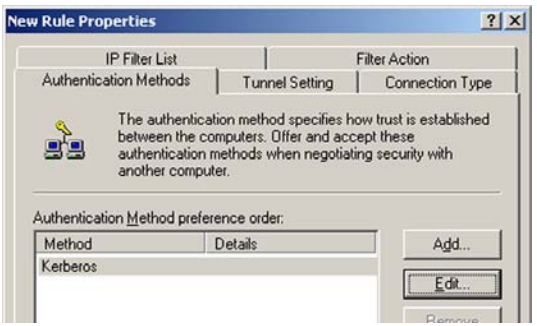


Figure B-13: Authentication Methods

5. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, as shown in Figure C-14, and enter the preshared key string, such as XYZ12345. Click the **OK** button.

6. This new Preshared key will be displayed in Figure C-15. Click the **Apply** button to continue, if it appears on your screen, otherwise proceed to the next step.

Figure B-14: Preshared Key

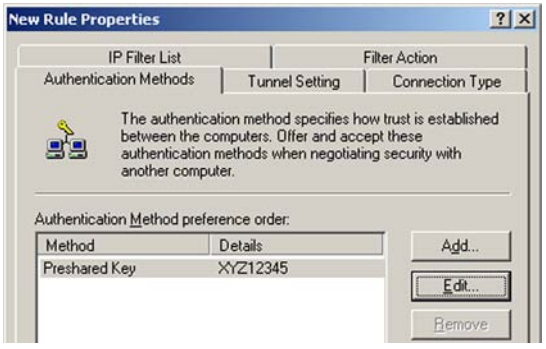


Figure B-15: New Preshared Key

7. Select the **Tunnel Setting** tab, shown in Figure C-16, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the Router's WAN IP Address.

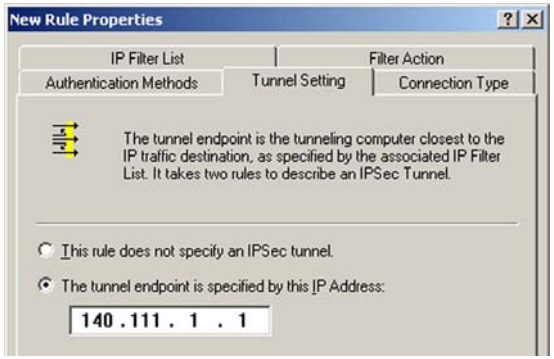


Figure B-16: Tunnel Setting Tab

8. Select the **Connection Type** tab, as shown in Figure C-17, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

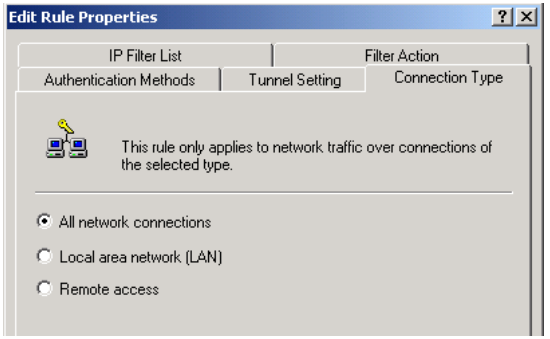


Figure B-17: Connection Type Tab

Tunnel 2: Router->win

9. In the new policy's properties screen, shown in Figure C-18, make sure that "win -> Router" is selected and deselect the **Use Add Wizard** check box. Then, click the **Add** button to create the second IP filter.

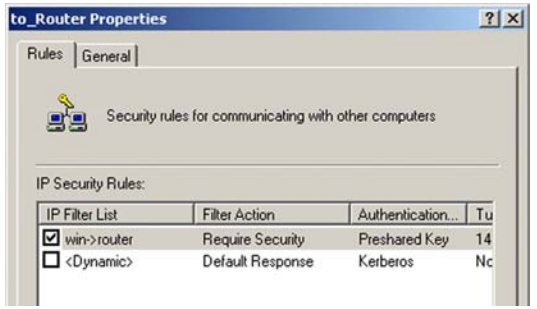


Figure B-18: Properties Screen

10. Go to the **IP Filter List** tab, and click the filter list **Router->win**, as shown in Figure C-19.

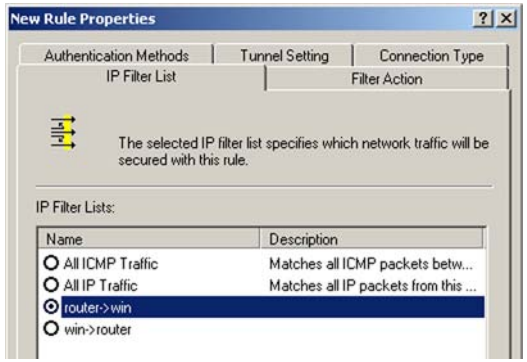


Figure B-19: IP Filter List Tab

11. Click the **Filter Action** tab, and select the filter action **Require Security**, as shown in Figure C-20. Then, click the **Edit** button. From the *Security Methods* tab, shown previously in Figure C-12, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

12. Click the **Authentication Methods** tab, and verify that the authentication method **Kerberos** is selected, as shown in Figure C-21. Then, click the **Edit** button.

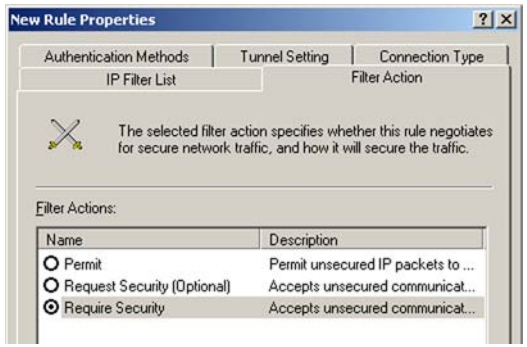


Figure B-20: Filter Action Tab

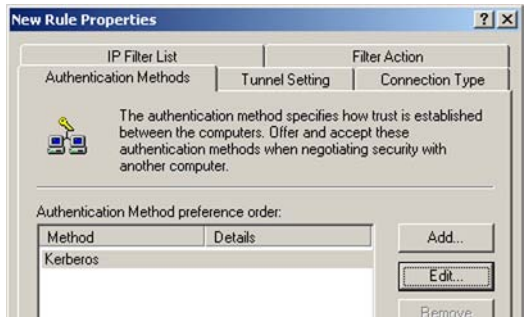


Figure B-21: Authentication Methods Tab

13. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345, as shown in Figure C-22. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click the **OK** button.

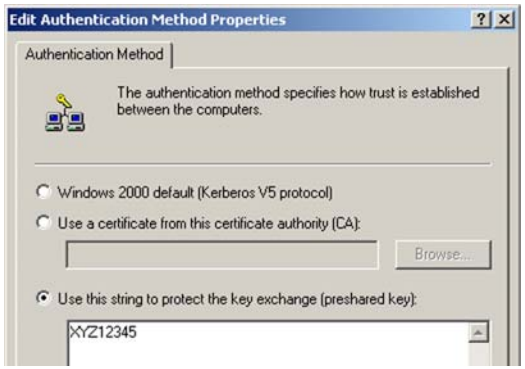


Figure B-22: Preshared Key

14. This new Preshared key will be displayed in Figure C-23. Click the **Apply** button to continue, if it appears on your screen, otherwise proceed to the next step.

15. Click the **Tunnel Setting** tab, shown in Figure C-24, click the radio button for **The tunnel endpoint is specified by this IP Address,** and enter the Windows 2000/XP computer's IP Address.

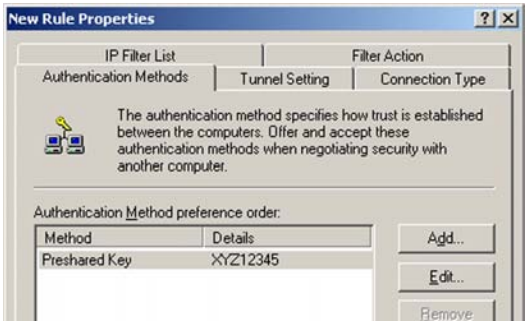


Figure B-23: New Preshared Key

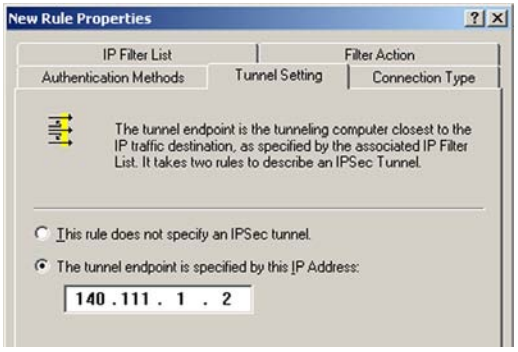


Figure B-24: Tunnel Setting Tab

16. Click the **Connection Type** tab, shown in Figure C-25, and select **All network connections**. Then click the **OK** or **Close** button to finish.

17. From the *Rules* tab, shown in Figure C-26, click the **OK** or **Close** button to return to the secpol screen.

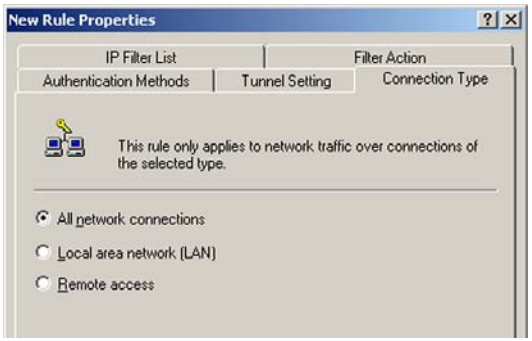


Figure B-25: Connection Type

Step 4: Assign New IPSec Policy

In the IP Security Policies on *Local Computer* window, shown in Figure C-27, right-click the policy named *to_Router*, and click **Assign**. A green arrow appears in the folder icon.

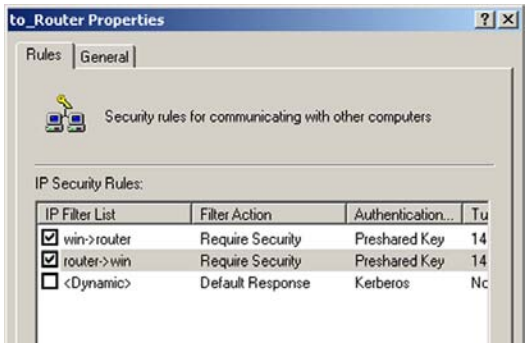


Figure B-26: Rules

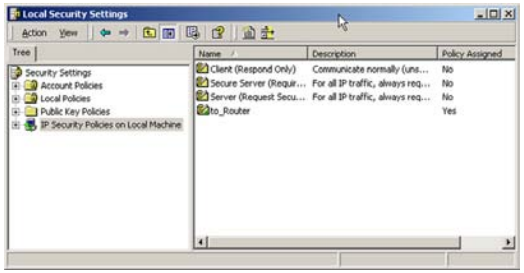


Figure B-27: Local Computer

Step 5: Create a Tunnel Through the Web-Based Utility

1. Open your web browser, and enter **192.168.1.1** in the Address field. Press the **Enter** key.
2. When the User name and Password field appears, enter the default user name and password **admin**. Press the **Enter** key.
3. From the *Setup* tab, click the **VPN** tab.
4. From the *VPN* tab, shown in Figure C-28, select the tunnel you wish to create in the *Select Tunnel Entry* drop-down box. Then click **Enabled**. Enter the name of the tunnel in the *Tunnel Name* field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
5. Enter the IP Address and Subnet Mask of the local VPN Router in the *Local Secure Group* fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).
6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Router or device with which you wish to communicate) in the *Remote Security Router* fields.
7. Select fromtwo different types of encryption: **DES** or **3DES** (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable.
8. Select from two types of authentication: **MD5** and **SHA** (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication.
9. Select the Key Management. Select **Auto (IKE)** and enter a series of numbers or letters in the *Pre-shared Key* field. Check the box next to **PFS** (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the *Key Lifetime* field, you may 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 useful, or leave it blank for the key to last indefinitely.
10. Click the **Save Settings** button to save these changes.

Your tunnel should now be established.

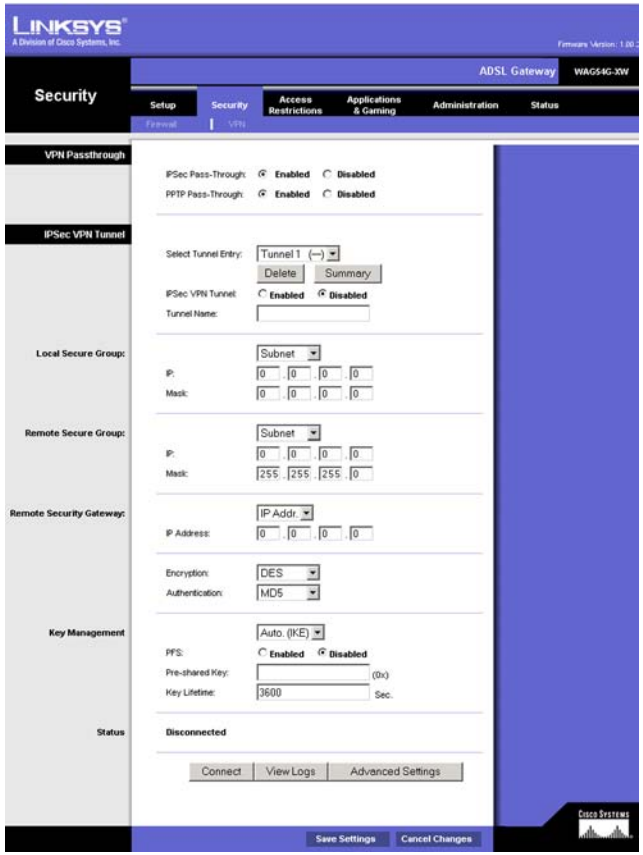


Figure B-28: VPN Tab

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 D-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure D-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 D-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 D-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 D-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 E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

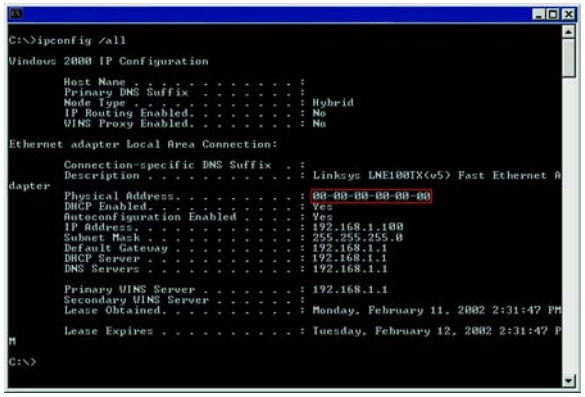


Figure C-3: MAC Address/Physical Address

Appendix D: Upgrading Firmware

The ADSL Gateway allows you to upgrade firmware for the LAN (network) side of the Gateway through the Web-Utility's Firmware Upgrade tab from the Administration tab. Follow these instructions:.

Upgrade from LAN

To upgrade the Gateway's firmware from the LAN:

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

Figure D-1: Upgrade Firmware

Appendix E: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

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.

Access Point - 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 - This is a device that adds network functionality to your computer.

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

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 - The frequency interval of the beacon, which is a packet broadcast by a Gateway to synchronize a wireless network.

Bit - A binary digit.

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

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

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

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

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

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate 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 (Dynamic Domain Name System) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

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

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

DMZ (Demilitarized Zone) - Removes the Gateway's firewall protection from one computer, allowing it to be "seen" from the Internet.

DNS (Domain Name Server) - 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 (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

DSSS (Direct-Sequence Spread-Spectrum) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

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

Encryption - Encoding data to prevent it from being read by unauthorized people.

Ethernet - An IEEE standard network 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 - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

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

FTP (File Transfer Protocol) - A standard protocol for sending files between computers over a TCP/IP network and the Internet.

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

Gateway - A system that interconnects networks.

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 (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

IP (Internet Protocol) - 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 (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio band used in wireless networking transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

Mbps (Megabits Per Second) - One million bits per second; a unit of measurement for data transmission.

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

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.

NNTP (Network News Transfer Protocol) - 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 (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

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.

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 3) - A standard protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - 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.

RJ-45 (Registered Jack-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, such as a local network and the Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

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

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - 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".

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

SSID (Service Set IDentifier) - 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. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

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

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that uses UDP and has no directory or password capability.

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - 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 (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network) - The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting data transmitted on a wireless network for greater security.

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

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

Appendix F: Specifications

Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, G.992.1 (G.dmt), G.992.2 (G.lite), ITU G.992.3, ITU G.992.5, ANSI T1.413i2, WAG54G-E1: Annex-B, WAG54G-DE: UR-2
Ports	Power, LINE (ADSL), Ethernet (1-4)
Buttons	One Reset Button, One On/Off Switch
Cabling Type	UTP CAT 5 or better, Phone Cable (POTS)
LEDs	Power, Ethernet (1-4), DSL, Internet
Security Features	WEP, WPA, RADIUS
WEP Key Bits	64, 128
Dimensions	186 mm x 48 mm x 188 mm
Unit Weight	0.48 kg
Power	External, 12V DC, 1A
Certifications	FCC Part 15B Class B, FCC Part 15C Class B, FCC Part 68, UL 1950, CSA, CE
Operating Temp.	0ºC to 40ºC
Storage Temp.	-20ºC to 70ºC
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix G: 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

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

EC DECLARATION OF CONFORMITY (EUROPE)

In compliance with the EMC Directive 89/336/EEC, Low Voltage Directive 73/23/EEC, and Amendment Directive 93/68/EEC, this product meets the requirements of the following standards:

- EN55022 Emission
- EN55024 Immunity

Appendix H: 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 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
Latin America	support.la@linksys.com
U.S. and Canada	support@linksys.com

LINKSYS®
A Division of Cisco Systems, Inc.

Modem routeur ADSL2

avec commutateur 4 ports

CABLE

Guide de l'utilisateur

Modèle **AG241**

Cisco Systems®

Copyright et marques commerciales

Comment utiliser ce Guide de l'utilisateur ?

Ce guide présentant le modem routeur ADSL2 avec commutateur 4 ports 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 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, les 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 d'une 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

Chapitre 1 : Introduction 1
Bienvenue 1
Contenu de ce guide 2
Chapitre 2 : Planification de la configuration de votre réseau 4
Les fonctions du modem routeur 4
Adresses IP 4
Qu'est ce qu'un VPN ? 5
Pourquoi ai-je besoin d'un VPN ? 6
Chapitre 3 : Présentation du modem routeur ADSL2 avec commutateur 4 ports 8
Panneau arrière 8
Panneau avant 9
Chapitre 4 : Connexion du modem routeur ADSL2 avec commutateur 4 ports 10
Présentation 10
Connexion à un ordinateur 10
Chapitre 5 : Configuration du modem routeur 12
Présentation 12
Comment accéder à l'utilitaire Web ? 14
Onglet Setup (Configuration) 14
Onglet Security (Sécurité) 21
Onglet Access Restrictions (Restrictions d'accès) 26
Onglet Applications and Gaming (Applications et jeux) 28
Onglet Administration 31
Onglet Status (Etat) 36
Annexe A : Dépannage 38
Problèmes courants et solutions 38
Questions fréquemment posées 47
Annexe B : Configuration de IPSec entre un ordinateur Windows 2000 ou Windows XP et le modem routeur 51
Introduction 51
Environnement 51
Comment établir un tunnel IPSec sécurisé ? 52

Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet 62
Instructions pour Windows 98 ou Me 62
Instructions pour Windows 2000 ou Windows XP 63
Annexe D : Glossaire 64
Annexe E : Mise à niveau du micrologiciel 70
Annexe F : Spécifications 71
Annexe G : Réglementation 72
Annexe H : Informations de garantie 73
Annexe I : Contacts 74

Liste des figures

Figure 2-1 : Réseau 4
Figure 2-2 : Modem routeur connectant l'ordinateur et le réseau VPN 6
Figure 2-3 : Modem routeur VPN vers modem routeur VPN 7
Figure 3-1 : Panneau arrière 8
Figure 3-2 : Panneau avant 9
Figure 4-1 : Connexion Ethernet 10
Figure 4-2 : Connexion de l'ADSL 11
Figure 4-3 : Connexion de l'alimentation 11
Figure 5-1 : Ecran de saisie du mot de passe 14
Figure 5-2 : Onglet Basic Setup (Configuration de base) 14
Figure 5-3 : Adresse IP dynamique 15
Figure 5-4 : Adresse IP statique 15
Figure 5-5 : IPoA 16
Figure 5-6 : RFC 2516 PPPoE 16
Figure 5-7 : RFC 2364 PPPoA 17
Figure 5-8 : Bridged Mode Only (Bridged Mode uniquement) 17
Figure 5-9 : Optional Settings (Paramètres facultatifs) 18
Figure 5-10 : DynDNS.org 19
Figure 5-11 : TZO.com 19
Figure 5-12 : Advanced Routing (Routage avancé) 20
Figure 5-13 : Advanced Wireless Settings (Paramètres sans fil avancés) 21
Figure 5-14 : Firewall (Pare-feu) 22
Figure 5-15 : VPN 23
Figure 5-16 : VPN Settings Summary (Récapitulatif des paramètres VPN) 23
Figure 5-17 : Manual Key Management (Gestion de clé manuelle) 24
Figure 5-18 : Fichier journal système 24
Figure 5-19 : Advanced VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec) 25

Figure 5-20 : Internet Access (Accès Internet) 26
Figure 5-21 : Internet Policy Summary (Récapitulatif de la stratégie Internet) 26
Figure 5-22 : List of PCs (Liste des ordinateurs) 27
Figure 5-23 : Services des ports 27
Figure 5-24 : Single Port Forwarding (Transfert de connexion unique) 28
Figure 5-25 : Port Range Forwarding (Transfert de connexion) 28
Figure 5-26 : Port Triggering (Déclenchement de connexion) 29
Figure 5-27 : DMZ 29
Figure 5-28 : QoS (QS) 30
Figure 5-29 : Management (Gestion) 31
Figure 5-30 : Reporting (Rapports) 32
Figure 5-31 : System Log (Fichier journal système) 32
Figure 5-32 : Ping Test (Test Ping) 33
Figure 5-33 : Backup&Restore (Sauvegarde et restauration) 33
Figure 5-34 : Factory Defaults (Paramètres d'usine) 34
Figure 5-35 : Firmware Upgrade (Mise à niveau du micrologiciel) 34
Figure 5-36 : Reboot (Redémarrage) 35
Figure 5-37 : Status (Etat) 36
Figure 5-38 : Local Network (Réseau local) 36
Figure 5-39 : DHCP Clients Table (Tableau des clients DHCP) 36
Figure 5-40 : DSL Connection (Connexion DSL) 37
Figure B-1 : Ecran de sécurité locale 52
Figure B-2 : Onglet Règles 52
Figure B-3 : Onglet Liste de filtres IP 52
Figure B-4 : Liste de filtres IP 53
Figure B-5 : Propriétés de Filtrer 53
Figure B-6 : Propriétés de Nouvelle règle 53
Figure B-7 : Liste de filtres IP 54
Figure B-8 : Propriétés de Filtrer 54
Figure B-9 : Propriétés de Nouvelle règle 54

Figure B-10 : Onglet Liste de filtres IP 55
Figure B-11 : Onglet Action de filtrage 55
Figure B-12 : Onglet Méthodes de sécurité 55
Figure B-13 : Méthodes d'authentification 56
Figure B-14 : Clé pré-partagée 56
Figure B-15 : Nouvelle clé pré-partagée 56
Figure B-16 : Onglet Paramètres du tunnel 57
Figure B-17 : Onglet Type de connexion 57
Figure B-18 : Ecran Propriétés 57
Figure B-19 : Onglet Liste de filtres IP 58
Figure B-20 : Onglet Action de filtrage 58
Figure B-21 : Onglet Méthode d'authentification 58
Figure B-22 : Clé pré-partagée 59
Figure B-23 : Nouvelle clé pré-partagée 59
Figure B-24 : Onglet Paramètres du tunnel 59
Figure B-25 : Type de connexion 60
Figure B-26 : Règles 60
Figure B-27 : Ordinateur local 60
Figure B-28 : Onglet VPN 61
Figure C-1 : Ecran Configuration IP 62
Figure C-2 : Adresse MAC/Adresse de l'adaptateur 62
Figure C-3 : Adresse MAC/Adresse Physique 63
Figure E-1 : Firmware Upgrade (Mise à niveau du micrologiciel) 70

Chapitre 1 : Introduction

Bienvenue

Le modem routeur Linksys ADSL2 avec commutateur 4 ports est la solution tout-en-un pour une connectivité Internet à la maison. La fonction modem ADSL vous offre une connexion Internet ultra-rapide, bien plus rapide que par ligne commutée et sans monopoliser votre ligne téléphonique.

Connectez vos ordinateurs au modem routeur via le commutateur Ethernet 4 ports 10/100 intégré pour démarrer rapidement votre réseau. Vous pouvez partager des fichiers, des imprimantes, de l'espace disque ainsi que d'autres ressources ou encore jouer à des jeux en « tête-à-tête ». Branchez jusqu'à 4 ordinateurs directement ou reliez plusieurs concentrateurs et commutateurs pour créer un réseau dont l'extension correspond à vos besoins. Le modem routeur sert de lien entre ces fonctionnalités et permet à votre réseau de partager cette connexion Internet haut débit

En outre, afin de protéger vos données et votre vie privée, le modem routeur ADSL avec commutateur 4 ports dispose d'un pare-feu avancé empêchant les intrusions et les attaques par le biais d'Internet. Les transmissions sans fil peuvent être protégées par un cryptage de données puissant. Protégez votre famille grâce aux fonctions de contrôle parental telles que la limitation du temps d'accès et le blocage par mot clé. La configuration est instantanée avec n'importe quel navigateur.

Avec le modem routeur Linksys ADSL2 avec commutateur 4 ports au cœur de votre réseau domestique, vous êtes en ligne avec l'avenir.

Contenu de ce guide

Ce guide de l'utilisateur présente les étapes inhérentes à l'installation et à l'utilisation du modem routeur ADSL2 avec commutateur 4 ports.

- Chapitre 1 : Introduction
  Ce chapitre décrit le modem routeur ADSL2avec commutateur 4 ports, ses applications et 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 ADSL2 avec commutateur 4 ports
  Ce chapitre décrit les caractéristiques physiques du routeur.

- Chapitre 4 : Connexion du u modem routeur ADSL2 avec commutateur 4 ports
  Ce chapitre vous explique pas à pas comment connecter le modem routeur à votre réseau.

- Chapitre 5 : Configuration du modem routeur
  Ce chapitre explique comment manipuler l'utilitaire Web pour configurer les paramètres du modem routeur.

- 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 ADSL2 avec commutateur 4 ports.

- Annexe B : Configuration de IPSec entre un ordinateur Windows 2000 ou Windows XP et le modem routeur
  Cette annexe vous explique comment établir un tunnel IPSec sécurisé à l'aide de clés pré-partagées pour connecter un réseau privé au sein du modem routeur VPN et un ordinateur Windows 2000 or XP.

- Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet.
  Cette annexe explique comment rechercher l'adresse MAC de l'adaptateur 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 : Glossaire
  Cette annexe propose un glossaire des termes fréquemment utilisés dans le cadre des réseaux.

- Annexe E : 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 F : Spécifications
  Cette annexe décrit les spécifications techniques du modem routeur.

- Annexe G : Réglementation
  Cette annexe fournit des informations relatives à la réglementation relative à l'utilisation du modem routeur.

- Annexe H : Informations de garantie
  Cette annexe fournit des informations relatives à la garantie 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 la 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

***LAN** : ordinateurs ou produits mis en réseau qui constituent votre réseau local.*

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 généralement utilisées avec des périphériques réseau tels que les serveurs d'ordinateurs ou les serveurs d'impression.

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. Veuillez vous reporter à la présentation du blocage des requêtes WAN à la section Sécurité du « Chapitre 5 : Configuration du modem routeur ».

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 à été attribuée à votre compte. Si c'est le cas, vous aurez besoin de cette adresse IP statique lors de la configuration de votre 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 changées. 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, tel 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 relative au DHCP dans le « Chapitre 5 : Configuration du modem routeur ».

Qu'est ce qu'un VPN ?

Un VPN (Virtual Private Network - réseau privé virtuel) est une connexion entre deux points terminaux (une modem routeur VPN, par exemple) de différents réseaux, qui permet la transmission de données privées sur un réseau partagé ou public, tel qu'Internet. Cette structure permet la transmission sécurisée de données d'un réseau privé entre ces deux emplacements ou réseaux.

Cette opération nécessite la création d'un « tunnel ». Un tunnel VPN connecte deux ordinateurs ou réseaux et permet aux données d'être transmises via Internet comme si elles étaient toujours sur ces réseaux. Il ne s'agit évidemment pas d'un tunnel mais d'une connexion sécurisée grâce au cryptage des données transmises entre les deux réseaux.

Le VPN (réseau privé virtuel) est une solution offrant un excellent rapport coût/efficacité, qui se substitue à la ligne louée, privée et dédiée d'un réseau privé. Grâce à l'utilisation des techniques standard de l'industrie en matière de cryptage et d'authentification, appelées IPSec (abréviation de IP Security), le VPN crée une connexion sécurisée qui fonctionne effectivement comme si vous étiez directement connecté à votre réseau local. Le VPN

peut être utilisé pour créer des liaisons réseau sécurisées entre le siège d'une entreprise et ses filiales. Il est également destiné au télé-travail et/ou aux professionnels souvent en déplacement. Ces derniers peuvent se connecter à un modem routeur VPN à partir de n'importe quel ordinateur sur lequel un logiciel client VPN prenant en charge IPSec est installé (SSH Sentinel, par exemple.)

Il existe deux façons très simples de créer une connexion VPN :

- Modem routeur VPN vers modem routeur VPN
- Ordinateur (utilisant le logiciel client VPN prenant en charge IPSec) vers modem routeur VPN

Le modem routeur VPN crée un tunnel, ou canal, entre les deux points terminaux, assurant la sécurité des données transitant entre ces deux points terminaux. Un ordinateur équipé d'un logiciel client VPN prenant en charge IPSec peut être l'un des deux points terminaux. Tout ordinateur équipé du IPSec Security Manager (Microsoft 2000 et XP) intégré permet au modem routeur VPN de créer un tunnel VPN à l'aide de IPSec. Reportez-vous à l'« Annexe C : Configuration de IPSec entre un ordinateur Windows 2000 ou XP et le modem routeur VPN ». D'autres versions de systèmes d'exploitation Microsoft requièrent l'installation de logiciels client VPN tiers supplémentaires qui prennent en charge IPSec.

Ordinateur (utilisant le logiciel client VPN prenant en charge IPSec) vers modem routeur VPN

Voici un exemple d'installation VPN entre un ordinateur et un modem routeur VPN. (figure 2-2) Dans sa chambre d'hôtel, une femme en déplacement pour son travail se connecte à son fournisseur d'accès Internet. Sur son ordinateur portable, le logiciel client VPN est configuré avec les paramètres VPN de son bureau. Elle accède au logiciel client VPN qui prend en charge IPSec et se connecte au modem routeur VPN au siège de sa société. Puisque les VPN utilisent Internet, la distance ne pose aucun problème. Grâce au VPN, cette personne dispose maintenant d'une connexion sécurisée au réseau du siège de sa société, comme si elle y était physiquement connectée.

Modem routeur VPN vers modem routeur VPN

Voici un exemple d'installation VPN entre deux modems routeurs VPN (Voir figure 2-3). A son domicile, une personne en télé-travail utilise son modem routeur VPN pour sa connexion Internet continue. Son modem routeur est configuré avec les paramètres VPN de son bureau. Lorsqu'il se connecte au modem routeur de son bureau, les deux modems routeurs créent un tunnel VPN, permettant le cryptage et le décryptage des données. Puisque les VPN utilisent Internet, la distance ne pose aucun problème. A l'aide du VPN, le télé-travailleur dispose ainsi d'une connexion sécurisée au réseau du siège de sa société, comme s'il y était physiquement connecté.

Pour obtenir de plus amples informations et des instructions sur la création de votre propre VPN, consultez le site Web international de Linksys à www.linksys.com/international ou reportez-vous à l'« Annexe B : Configuration de IPSec entre un ordinateur Windows 2000 ou XP et le modem routeur VPN ».

Pourquoi ai-je besoin d'un VPN ?

La mise en réseau d'ordinateurs offre une flexibilité que l'on ne trouve pas sur un système classique d'échange de données (documents papiers). Cette flexibilité s'accompagne néanmoins d'un risque plus important en

Figure 2-2 : Modem routeur connectant l'ordinateur et le réseau VPN

IMPORTANT : Vous devez installer au moins un modem routeur VPN à une extrémité du tunnel VPN. A l'autre extrémité du tunnel VPN, vous devez installer un second modem routeur VPN ou un ordinateur équipé du logiciel client VPN prenant en charge IPSec.

matière de sécurité. C'est pour cette raison que les pare-feu ont été mis en place. Les pare-feu aident à protéger les données d'un réseau local. Cependant, que faites-vous une fois que les informations sont envoyées hors de votre réseau local, lorsque des messages électroniques sont envoyés à leur destinataire ou lorsque vous êtes en déplacement et que vous devez vous connecter au réseau de votre société ? Comment vos données sont-elles protégées ?

Le VPN est la solution à vos problèmes. Les VPN sécurisent les données transmises à l'extérieur de votre réseau comme si elles étaient toujours sur votre réseau.

Lorsque des données sont envoyées à l'extérieur via Internet à partir de votre ordinateur, elles sont toujours vulnérables. Il se peut que vous ayez déjà un pare-feu, qui vous aidera à protéger les données transmises sur votre réseau ou contenues sur ce dernier contre des corruptions ou interceptions par des entités extérieures. Néanmoins, dès que ces données quittent votre réseau, lorsque vous envoyez des données par message électronique ou que vous communiquez avec une personne via Internet, le pare-feu ne les protège plus.

A ce stade, vos données deviennent alors accessibles aux pirates qui utilisent diverses méthodes pour voler non seulement les données que vous transmettez mais aussi vos informations de connexion réseau et de sécurité. Les méthodes les plus couramment utilisées sont décrites ci-après :

1) Usurpation d'adresses MAC (MAC Address Spoofing)

Les paquets transmis sur un réseau, soit votre réseau local, soit Internet, sont précédés d'un en-tête de paquet. Ces en-têtes de paquet contiennent les informations de source et de destination permettant au paquet d'être transmis efficacement. Un pirate peut utiliser ces informations pour usurper l'adresse MAC autorisée sur un réseau. Avec cette adresse MAC usurpée, le pirate peut également intercepter des informations destinées à un autre utilisateur.

2) Analyse des données (Data Sniffing)

L'analyse des données est une méthode utilisée par les pirates pour obtenir des données réseau transmises sur des réseaux non-sécurisés tels que Internet. Les outils permettant ce type d'activité, tels que les analyseurs de protocole et les outils de diagnostic réseau, sont souvent intégrés aux systèmes d'exploitation et les données peuvent être visualisées normalement.

3) Attaques centralisées (Man in the Middle Attacks)

Une fois que le pirate à analysé ou usurpé suffisamment d'informations, il peut entreprendre une attaque centralisée. Ces attaques peuvent se produire lorsque les données sont transmises d'un ordinateur à un autre, en déroutant les données vers une autre destination. Même si les données ne sont pas reçues par le destinataire d'origine, l'expéditeur ne le sait pas.

Il s'agit seulement d'une petite partie des méthodes utilisées par les pirates qui ne cessent de perfectionner leurs techniques. Sans la sécurité d'un VPN, vos données sont constamment à la merci de telles attaques lorsqu'elles sont transmises via Internet. Les données transmises via Internet transitent souvent par de nombreux serveurs dans le monde avant d'arriver à destination. Ce parcours est très long lorsqu'il s'agit de données non-sécurisées, ce qui montre bien tout l'intérêt du VPN.

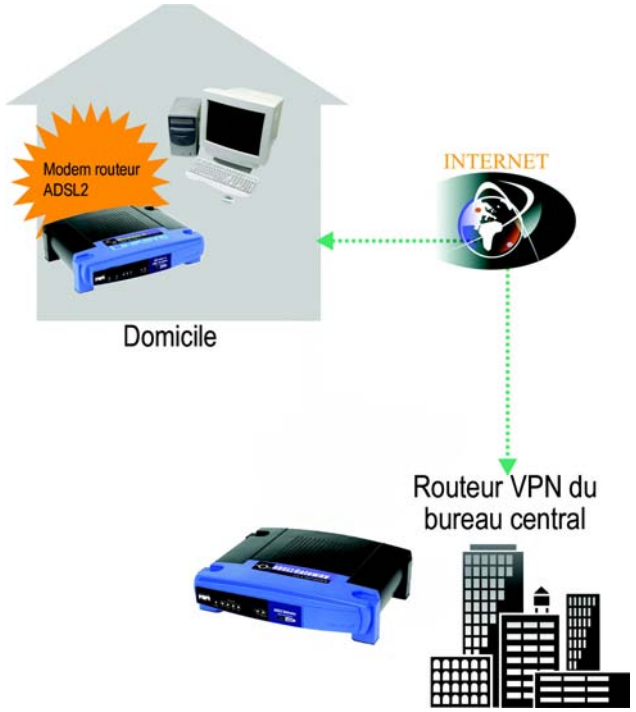


Figure 2-3 : Modem routeur VPN vers modem routeur VPN

Chapitre 3 : Présentation du modem routeur ADSL2 avec commutateur 4 ports

Panneau arrière

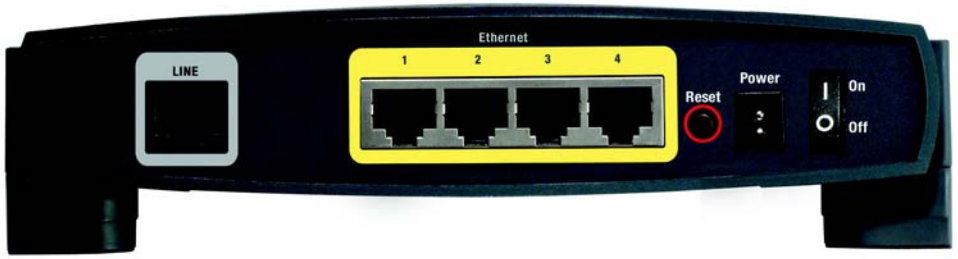


Figure 3-1 : Panneau arrière

Les ports du modem routeur permettant notamment de connecter le câble réseau, sont situés sur le panneau arrière de l'appareil. Les boutons du modem routeur sont également situés sur le panneau arrière de l'appareil.

LINE Le port **LINE** (LIGNE) permet de connecter la câble ADSL.

Ethernet (1-4) Les ports **Ethernet** (Ethernet) permettent de connecter l'appareil à votre ordinateur et à d'autres périphériques réseau.

Bouton Reset (Réinitialisation) Il existe deux façons de réinitialiser les paramètres d'usine de votre modem routeur : soit en appuyant sur le **bouton Reset** (Réinitialisation) pendant une dizaine de secondes, soit en accédant à l'écran Factory Defaults (Paramètres d'usine) dans l'onglet Administration de l'utilitaire Web du modem routeur.

Power (Alimentation) Le port **Power** (Alimentation) est l'emplacement auquel vous devez connecter l'adaptateur électrique.

On/Off (Marche/Arrêt) Ce commutateur permet d'allumer ou d'éteindre le modem routeur.

Fortes de tous ces éléments et des nombreux autres produits Linksys, vos possibilités en matière de développement réseau sont illimitées. Pour obtenir de plus amples informations sur les produits compatibles avec le modem routeur, consultez le site Web international de Linksys à www.linksys.com/international.

Important : La réinitialisation des paramètres d'usine du modem routeur supprime tous les paramètres personnalisés (Cryptage WEP, paramètres de connexion sans fil et LAN, etc.). Ne réinitialisez pas les paramètres du modem routeur si vous souhaitez les conserver.

Panneau avant

Les voyants du modem routeur, qui vous informent de l'activité du réseau, se trouvent sur le panneau avant.

Figure 3-2 : Panneau avant

Power (Alimentation) Vert. Le voyant **Power** s'allume lorsque l'adaptateur est sous tension.

Ethernet (1-4) Vert. Le voyant **LAN** a deux fonctions. S'il est allumé en permanence, cela signifie que le modem routeur est connectée correctement à un périphérique via le port LAN (réseau local). 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 au moment de l'établissement de la connexion.

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 ADSL2 avec commutateur 4 ports

Présentation

La configuration du modem routeur ne consiste pas seulement à connecter les appareils entre eux. Vous devez configurer vos ordinateurs du réseau pour qu'ils acceptent les adresses IP que leur attribue le modem routeur (le cas échéant). Vous devez également configurer le modem routeur à l'aide des paramètres fournis par votre fournisseur d'accès Internet (FAI).

Le technicien de votre fournisseur d'accès Internet doit vous avoir communiqué les données concernant votre modem après avoir installé votre connexion haut débit. 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.

Connexion à un ordinateur

1. Avant de commencer, vérifiez que tous les appareils du réseau sont hors tension, y compris le modem routeur et tous les ordinateurs.
2. Reliez une extrémité d'un câble réseau Ethernet à l'un des ports Ethernet (numérotés de 1 à 4) situés sur le panneau arrière de le modem routeur (figure 4-1) et l'autre extrémité au port Ethernet d'un ordinateur.
3. Procédez de même pour relier d'autres ordinateurs, un commutateur ou des périphériques réseau au modem routeur.

Figure 4-1 : Connexion Ethernet

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 uniquement entre le téléphone et la prise murale et **non** entre le modem et la prise murale sinon votre connexion ADSL ne sera pas établie.

Dans les pays où les prises téléphoniques sont utilisées **sans** connecteurs RJ-11 (par exemple, en France, en Suède, en Suisse, au Royaume-Uni, etc.), sauf pour les utilisateurs RNIS, le microfiltre doit être utilisé entre le modem et la prise murale, car il est équipé d'un connecteur RJ-11.

Les utilisateurs Annex B (versions E1 et DE du modem routeur) doivent utiliser le câble spécial founri pour raccorder le modem routeur à la prise murale (RJ-45 à RJ-12). Si vous avez besoin de séparateurs ou de prises spéciales, prenez contact avec votre fournisseur d'accès.

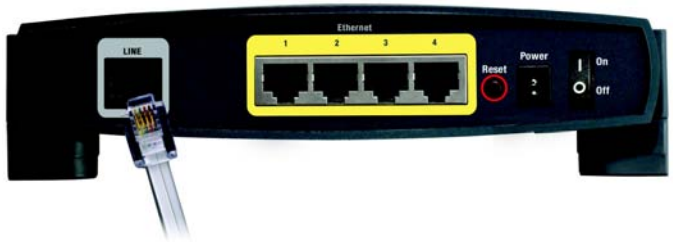


Figure 4-2 : Connexion de l'ADSL

REMARQUE : Branchez toujours l'adaptateur électrique du modem routeur sur une barrette de connexion protégée contre les surtensions.

4. Branchez un câble téléphonique entre le port Line (Ligne) du panneau arrière du modem routeur (voir figure 4-2) et la prise murale de la ligne ADSL. Il peut être nécessaire de placer un microfiltre entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.

5. Branchez l'adaptateur électrique au port Power (Alimentation) du modem routeur (voir figure 4-3) puis raccordez l'autre extrémité à une prise d'alimentation électrique. Appuyez sur le bouton On/Off (Marche/Arrêt).

   - Le voyant d'alimentation situé sur le panneau avant est vert dès que l'adaptateur électrique est correctement connecté et que le commutateur est en position Marche. 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 ».

6. Allumez un des ordinateurs connectés au modem routeur.

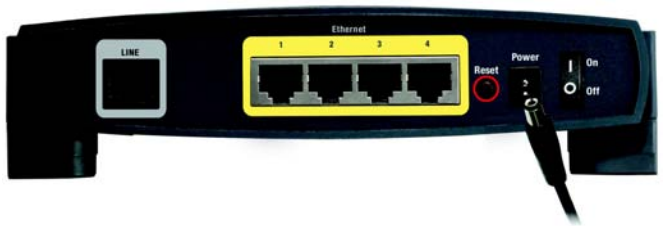


Figure 4-3 : Connexion de l'alimentation

REMARQUE : Veillez à toujours modifier les paramètres par défaut SSID Linksys et activer le cryptage WEP.

L'installation matérielle du modem routeur est maintenant terminée.

Passez au « Chapitre 5 : Configuration du modem routeur ».

Chapitre 5 : Configuration du modem routeur

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), entrez les paramètres fournis par votre FAI.
- 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, choisissez un mot de passe autre que le mot de passe par défaut.

Six onglets principaux sont disponibles : Setup (Configuration), 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.

Setup (Configuration)

- Basic Setup (Configuration de base). Entrez 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 Dynamic Routing (Routage dynamique) et Static Routing (Routage statique).

Sécurité

- Firewall (Pare feu). Cet écran permet de définir les options Filters (Filtres) et Block WAN Requests (Blocage des requêtes WAN). Les filtres permettent d'empêcher des utilisateurs internes d'accéder à Internet mais aussi de bloquer les requêtes Internet anonymes.
- VPN. Cet écran permet d'activer ou de désactiver IPSec et/ou l'intercommunication PPTP mais aussi de configurer des tunnels VPN.

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 votre mot de passe à partir de l'onglet Administration.

Restrictions d'accès

- Internet Access (Accès Internet). Cet écran permet d'autoriser ou non l'accès au réseau aux utilisateurs souhaités.

Applications et jeux

- Single Port Forwarding (Transfert de connexion unique). Cet écran vous permet de configurer des services ou des applications standard sur votre réseau.
- Port Range Forwarding (Transfert de connexion). Cet onglet vous permet de configurer des services publics ou d'autres applications Internet spécialisées sur votre réseau.
- 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 utilisateur local, pour l'accès à des services spécifiques.
- 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.

Administration

- Management (Gestion). Dans cet écran, vous pouvez modifier les privilèges d'accès au modem routeur, les paramètres SNMP, UPnP et WT-82.
- 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 onglet permet de sauvegarder et de restaurer le fichier de 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.
- Reboot (Redémarrage). Cet onglet permet d'effectuer un redémarrage logiciel ou matériel du modem routeur.

Status (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.
- 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 entrez l'adresse IP par défaut du modem routeur, 192.168.1.1, dans le champ Address (Adresse). Appuyez ensuite sur la touche Entrée.

Une page demandant la saisie d'un mot de passe apparaît (figure 5-1). (Les utilisateurs non-Windows XP obtiendront un écran similaire.) Saisissez **admin** (nom d'utilisateur par défaut) dans le champ User Name (Nom d'utilisateur) et **admin** (mot de passe par défaut) dans le champ Password (Mot de passe). Cliquez sur le bouton **OK**.

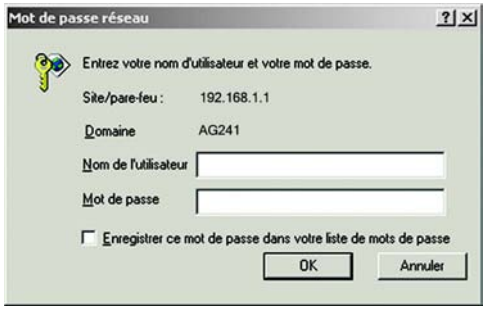


Figure 5-1 : Ecran de saisie du mot de passe

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 ci-contre, puis 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.

Internet Setup (Configuration Internet)

- PVC Connection (Connexion PVC). Sélectionnez un numéro de connexion PVC dans le menu déroulant. Puis, sélectionnez **Enable Now** (Activer maintenant) pour activer la connexion.
- VC Settings (Paramètres VC). Virtual Circuit (Circuit Virtuel) : Ces champs contiennent deux options : VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier). Votre FAI vous indiquera le paramétrage approprié de chacun de ces deux champs.
  - Multiplexing (Multiplexage) : Sélectionnez **LLC** ou **VC** en fonction de votre FAI.
  - QOS Type (Type QS) : Sélectionnez une option 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) : Peak Cell Rate, divisez le débit de la ligne DSL par 424 pour trouver le PCR et obtenir le taux maximal auquel l'expéditeur peut envoyer des cellules. Entrez 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. Normalement, SCR est inférieur à PCR. Entrez le taux dans ce champ (s'il est requis par votre FAI).
  - Autodetect (Détection automatique) : Sélectionnez **Enable** (Activer) pour que les paramètres soient entrés automatiquement ou **Disable** (Désactiver) pour entrer les valeurs manuellement.
  - Virtual Circuit (Circuit virtuel) : Entrez les plages VPI et VCI dans les champs.

Figure 5-2 : Onglet Basic Setup (Configuration de base)

- Internet Connection Type (Type de connexion Internet). Le modem routeur prend en charge cinq encapsulations : RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA et Bridged Mode Only (Bridged Mode uniquement). Les écrans Basic Setup (Configuration de base) et les options disponibles varient selon le type d'encapsulation sélectionné.

RFC 1483 Bridged

Adresse IP dynamique

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.

Static IP (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.
- Gateway (Modem routeur). 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 principal) (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).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

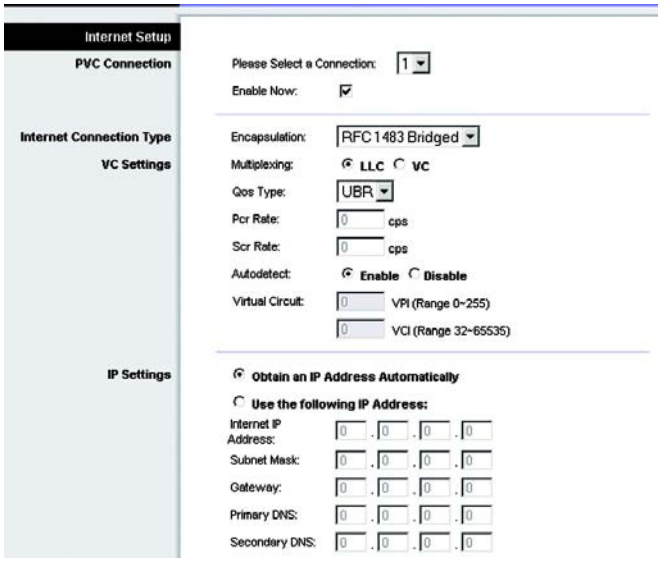


Figure 5-3 : Adresse IP dynamique

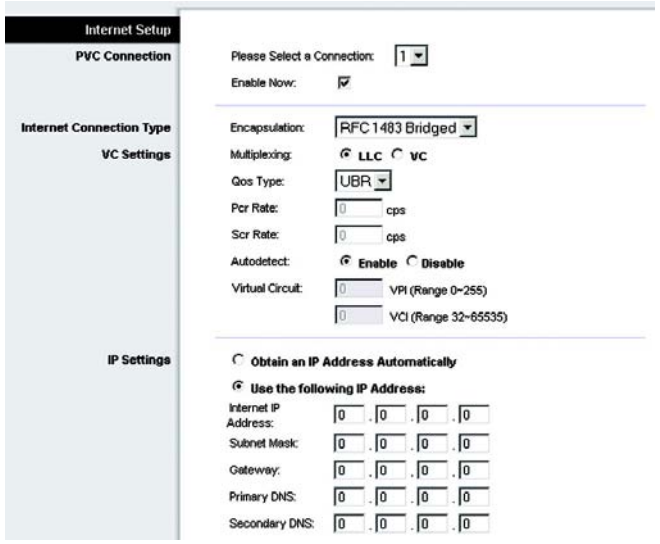


Figure 5-4 : Adresse IP statique

IPoA

Si vous devez utiliser RFC 1577 IPoA (Classical IP over ATM), puis sélectionnez **IPoA**.

- IP Address (Adresse IP). 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 (Modem routeur 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 principal) (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).

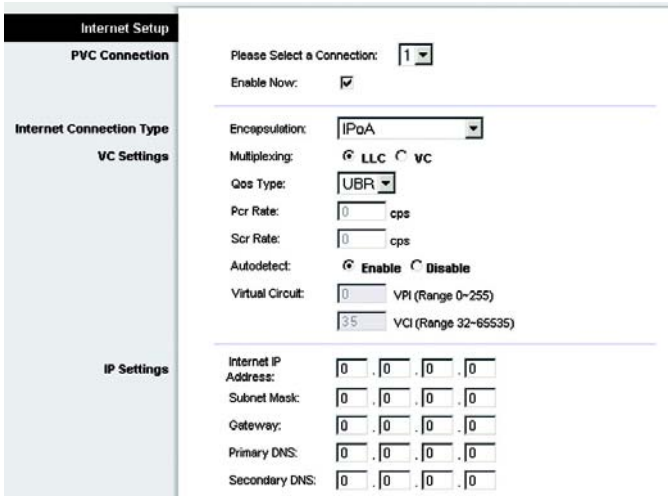


Figure 5-5 : IPoA

RFC 2516 PPPoE

Certains fournisseurs d'accès 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.

- Service Name (Nom du service). Entrez le nom du service PPPoE dans le champ.
- User Name and Password (Nom d'utilisateur et mot de passe). Entrez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand (Connexion à la demande). Max Idle Time (Délai d'inactivité maximal). Vous pouvez configurer le modem routeur afin qu'il 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 radio **Connect on Demand** (Connexion à la demande). Dans le champ Max Idle Time (Délai d'inactivité maximal), entrez 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 la case 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. Durée par défaut devant s'écouler avant rappel est de 30 secondes.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

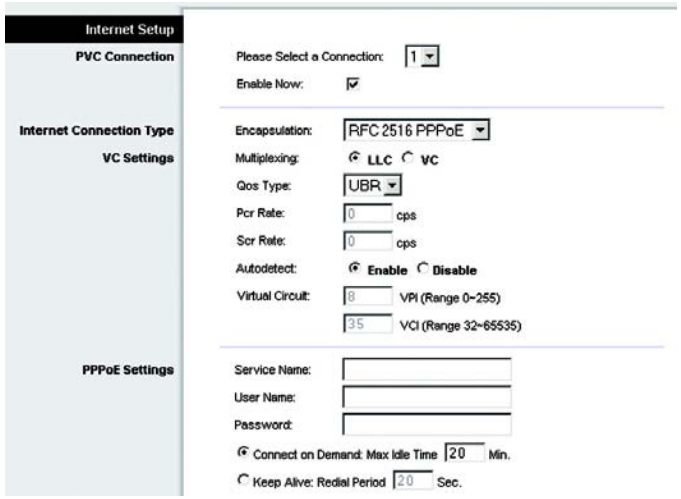


Figure 5-6 : RFC 2516 PPPoE

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). Entrez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand (Connexion à la demande). Max Idle Time (Délai d'inactivité maximal). Vous pouvez configurer le modem routeur afin qu'il 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 radio **Connect on Demand** (Connexion à la demande). Dans le champ Max Idle Time (Délai d'inactivité maximal), entrez le nombre de minutes que vous souhaitez voir s'écouler avant la désactivation de votre connexion Internet.
- Option 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 la case 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. Durée par défaut devant s'écouler avant rappel est de 30 secondes.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

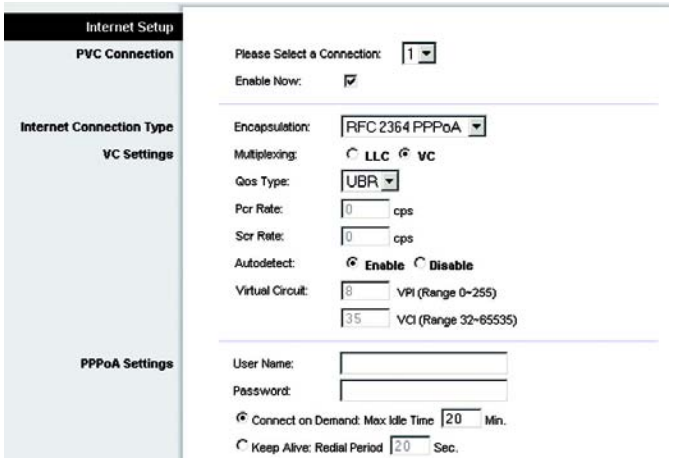


Figure 5-7 : RFC 2364 PPPoA

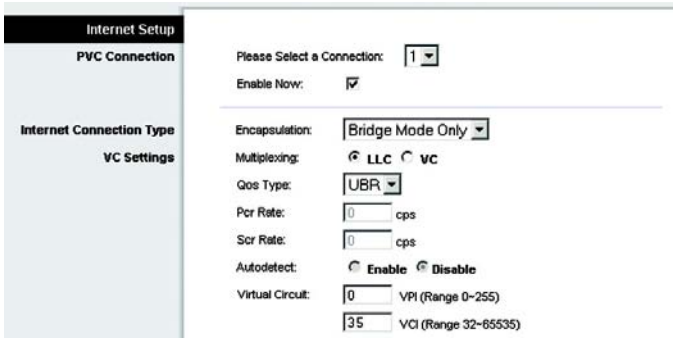


Figure 5-8 : Bridged Mode Only (Bridged Mode uniquement)

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). La technologie NAT et le routage sont désactivés dans ce mode.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Optional Settings (Paramètres facultatifs) (Requis par certains FAI)

- Host Name (Nom d'hôte) et Domain Name (Nom de domaine). Entrez 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. Le paramètre MTU (Maximum Transmission Unit) spécifie la taille de paquet maximale autorisée pour la transmission réseau. Sélectionnez **Manual** (Manuel) et entrez 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.

Network Setup (Configuration 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)). 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.
  - Serveur du relais DHCP Si vous activez l'option Serveur DHCP local ou Relais DHCP pour le serveur DHCP local, entrez l'adresse IP du serveur DHCP dans les champs.
  - AutoDetect LAN DHCP Server (Détection automatique du serveur DHCP LAN).
  - Starting IP Address (Adresse IP de départ). Entrez une valeur de départ 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). Entrez 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 bail du client). Cette option détermine la période pendant laquelle un utilisateur du réseau est autorisé à se connecter au modem routeur à l'aide de son adresse IP dynamique actuelle. Entrez la durée (en minutes) pendant laquelle l'adresse IP dynamique est allouée à l'utilisateur.
  - Static DNS (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

Figure 5-9 : Optional Settings (Paramètres facultatifs)

vous fournir au moins une adresse IP de serveur DNS. Vous pouvez taper jusqu'à trois adresses IP de serveur DNS. Le 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, entrez son adresse IP dans ce champ. Autrement, laissez-le vide.
- Time Setting (Réglage de l'heure). Ce paramètre vous permet de spécifier le fuseau horaire de votre modem routeur. Sélectionnez le fuseau horaire dans le menu déroulant. 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 Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Onglet DDNS

Le modem routeur inclut une fonction DDNS (Dynamic Domain Name System). 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 à l'adresse DynDNS.org.

DDNS

DDNS Service (Service DDNS). Si votre service DDNS est fourni par DynDNS.org, sélectionnez **DynDNS.org** dans le menu déroulant (figure 5-10). Pour désactiver le service DDNS, sélectionnez **Disabled** (Désactivé).

DynDNS.org

- User Name (Nom d'utilisateur), Password (Mot de passe) et Host Name (Nom d'hôte). Entrez le nom d'utilisateur, le mot de passe et le nom d'hôte du compte configuré avec DynDNS.org.
- Internet IP Address (Adresse IP Internet). L'adresse IP Internet actuelle du modem routeur est spécifiée dans ce champ. Puisqu'elle est dynamique, cette adresse change.
- Status (Etat). L'état de la connexion du service DDNS est spécifié dans ce champ.

TZO.com

- Email Address (Adresse e-mail), Password (Mot de passe) et Domain Name (Nom de domaine). Entrez l'adresse e-mail, le mot de passe TZO et le nom de domaine du service que vous configurez avec TZO.
- Internet IP Address (Adresse IP Internet). L'adresse IP Internet actuelle du routeur est spécifiée dans ce champ. Puisqu'elle est dynamique, cette adresse change.

Figure 5-10 : DynDNS.org

Figure 5-11 : TZO.com

- Status (Etat). L'état de la connexion du service DDNS est spécifié dans ce champ.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Onglet Advanced Routing (Routage avancé)

L'écran Advanced Routing (Routage avancé) vous permet de configurer les paramètres de routage dynamique et de routage statique.

Advanced Routing (Routage avancé)

- Operating Mode (Mode opérationnel). 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'il 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. Pour activer le RIP, cliquez sur **Enabled** (Activé). Pour désactiver le RIP, cliquez sur **Disabled** (Désactivé).
  - Transmit RIP Version (Transmettre la version RIP). Pour transmettre des messages RIP, sélectionnez le protocole souhaité : **RIP1, RIP1-Compatible ou RIP2.**
  - Receive RIP Version (Version de réception RIP). Pour recevoir des messages RIP, sélectionnez le protocole souhaité : **RIP1** ou **RIP2**.
- Static Routing (Routage statique). Si le modem routeur est connecté 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. Entrez 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.

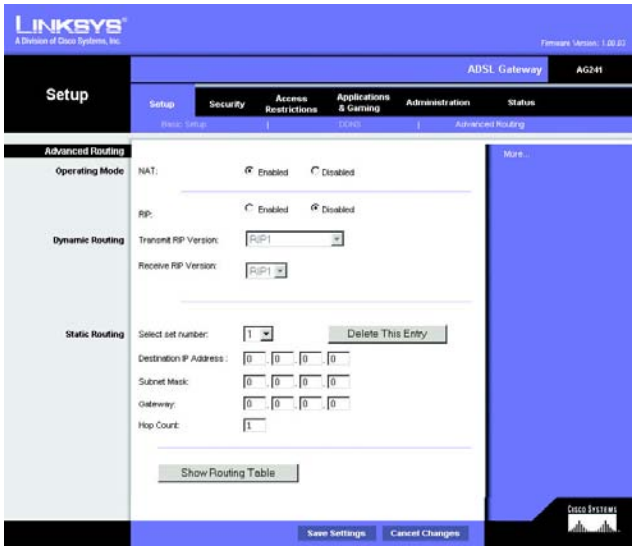


Figure 5-12 : Advanced Routing (Routage avancé)

- Subnet Mask (Masque de sous-réseau). Cette option, que l'on appelle également Masque de réseau, détermine la portion de l'adresse IP qui correspond au réseau et la portion de l'adresse IP qui correspond à l'hôte.
- Gateway (Modem routeur). Il s'agit de l'adresse IP du modem routeur permettant 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). Entrez 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 (LAN). Pour chaque itinéraire, l'adresse IP 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 Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

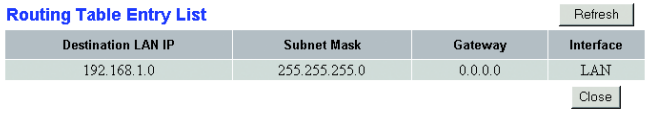


Figure 5-13 : Advanced Wireless Settings (Paramètres sans fil avancés)

Onglet Security (Sécurité)

Firewall (Pare-feu)

Lorsque vous cliquez sur l'onglet Security (Sécurité), l'écran Firewall (Pare-feu) apparaît. Cet écran permet de définir les options Filters (Filtres) et Block WAN Requests (Blocage des requêtes WAN). Les filtres bloquent certains types de données Internet ainsi que les requêtes Internet anonymes. Pour ajouter la protection par pare-feu, cliquez sur **Enable** (Activée). Si vous ne souhaitez pas sélectionner cette option, 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, cliquez sur **Enabled** (Activé).
- 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, cliquez sur **Enabled** (Activé).
- 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 Applet Java, cliquez sur **Enabled** (Activé).

- 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, cliquez sur **Enabled** (Activé).

  Block WAN requests (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. Sélectionnez l'option **Bloquer les requêtes Internet anonymes**. Pour autoriser ces requêtes, désélectionnez cette option**, désélectionnez cette option**.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Figure 5-14 : Firewall (Pare-feu)

VPN

VPN (Virtual Private Networking) est une mesure de sécurité qui crée une connexion sécurisée entre deux emplacements distants. L'écran VPN vous permet de configurer vos paramètres VPN afin d'améliorer la sécurité de votre réseau.

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** (Activée). Pour désactiver l'option Intercommunication IPSec, cliquez sur le bouton **Disable** (Désactivée).
- 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).

IPSec VPN Tunnel (Tunnel VPN IPSec)

Le modem routeur VPN crée un tunnel, ou canal, entre deux points terminaux, ainsi les données ou informations transitant entre ces deux points terminaux sont sécurisées.

- Pour établir ce tunnel, sélectionnez le tunnel que vous voulez créer dans la liste déroulante Select Tunnel Entry (Sélectionner une entrée de tunnel). Vous pouvez créer jusqu'à 5 tunnels simultanés. Cliquez ensuite sur **Enabled** (Activé) pour activer le tunnel VPN IPSec. Une fois le tunnel activé, donnez-lui un nom dans le champ Tunnel Name (Nom du tunnel). Ceci vous permet d'identifier les divers tunnels et il n'est donc pas nécessaire que ce nom corresponde au nom utilisé à l'autre bout du tunnel. Pour supprimer une entrée de tunnel, sélectionnez-le, puis cliquez sur **Delete** (Supprimer). Pour afficher un récapitulatif des paramètres, cliquez sur **Summary** (Récapitulatif).
- Groupe sécurisé local et Groupe sécurisé distant. Groupe sécurisé local correspond à l'ordinateur ou aux ordinateurs de votre réseau local (LAN) pouvant accéder au tunnel. Groupe sécurisé distant correspond à l'ordinateur ou aux ordinateurs du côté distant du tunnel pouvant accéder au tunnel. Ces ordinateurs peuvent être spécifiés par un sous-réseau, une adresse IP spécifique ou une étendue.
- Local Security Gateway (Modem routeur de sécurité locale).
- Remote Security Gateway (Modem routeur de sécurité distante). Le modem routeur de sécurité distante correspond au périphérique VPN, tel qu'un deuxième modem routeur, du côté distant du tunnel VPN. Renseignez les champs IP Address (Adresse IP) et Domain (Domaine) pour le périphérique VPN se trouvant de l'autre côté du tunnel. Le périphérique VPN distant peut être un autre modem routeur VPN, un serveur VPN?ou un ordinateur exécutant un logiciel client VPN prenant en charge IPSec. L'adresse IP peut être statique (permanente) ou dynamique (changeante) selon les paramètres du périphérique VPN distant. Vérifiez que vous avez saisi correctement l'adresse IP. Sinon la connexion ne peut pas être établie. Gardez à l'esprit qu'il ne s'agit PAS de l'adresse IP?du modem routeur locale, mais de l'adresse IP du modem routeur ou du périphérique VPN?distant avec lequel vous voulez communiquer. Si vous entrez une adresse IP, seule l'adresse IP spécifique pourra accéder au tunnel. Si vous sélectionnez **Any** (Toutes), toutes les adresses IP peuvent accéder au tunnel.
- Encryption (Cryptage). Le paramètre Encryption (Cryptage) permet de sécuriser davantage votre connexion. Il existe deux types de cryptage : DES ou 3DES (3DES est le paramètre recommandé car il garantit un niveau de protection plus élevé). Vous pouvez sélectionner l'un de ces deux paramètres, mais le même type de cryptage doit être utilisé par le périphérique VPN à l'autre bout du tunnel. Vous pouvez également ne pas souhaiter utiliser de cryptage. Dans ce cas, sélectionnez l'option Disable (Désactiver). A la figure 5-19, DES (paramètre par défaut) a été sélectionné.
- Authentication (Authentification). L'authentification constitue un niveau de sécurité supplémentaire. Il existe deux types d'authentification : MD5 et SHA. SHA est le paramètre recommandé car il garantit un niveau de protection plus élevé. Comme pour le cryptage, vous pouvez sélectionner l'un de ces deux paramètres, mais le même type d'authentification doit être utilisé par le périphérique VPN à l'autre bout du tunnel. L'authentification peut également être désactivée des deux côtés du tunnel, à l'aide de l'option Disable (Désactiver). Dans l'écran Manual Key Management (Gestion de clé manuelle), la valeur par défaut, MD5, a été sélectionnée.
- Key Management (Gestion de clé). Sélectionnez **Auto (IKE)** ou **Manual** (Manuelle) dans le menu déroulant. Les deux méthodes sont décrites ci-dessous.
  Auto (IKE)

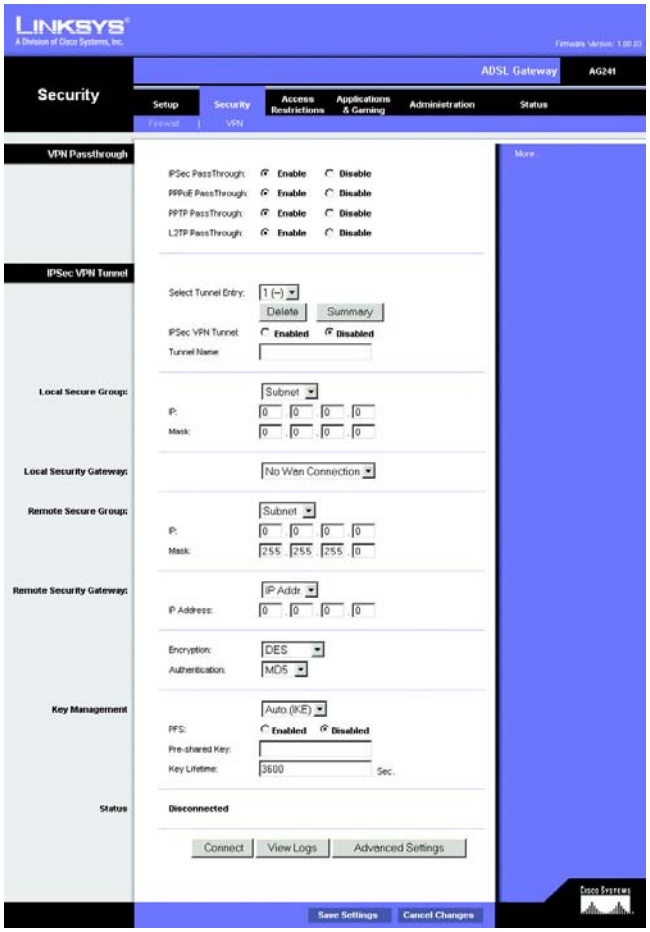


Figure 5-15 : VPN

Figure 5-16 : VPN Settings Summary (Récapitulatif des paramètres VPN)

Sélectionnez **Auto (IKE)** (Auto (IKE)) et saisissez une suite de chiffres ou de lettres dans le champ Pre-shared Key (Clé partagée). Une clé est générée sur la base de ce mot, qui DOIT être saisi des deux côtés du tunnel si cette méthode de cryptage est utilisée. 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. Dans le champ Key Lifetime (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. Cochez la case correspondant à l'option PFS (Perfect Forward Secrecy, Secret de transmission total) pour vous assurer que l'échange de clé et les propositions IKE sont sécurisées.

Manual (Manuelle)
Sélectionnez **Manual** (Manuelle), puis l'algorithme de cryptage souhaité dans le menu déroulant. Entrez la clé de cryptage dans le champ Encryption Key (Clé de cryptage). Si vous avez sélectionné DES pour votre algorithme de cryptage, entrez 16 caractères hexadécimaux. Si vous avez sélectionné 3DES, entrez 48 caractères hexadécimaux. Sélectionnez l'algorithme souhaité dans le menu déroulant Authentication Algorithm (Algorithme d'authentification). Entrez la clé d'authentification dans le champ Clé d'authentification. Si vous avez sélectionné MD5 pour votre algorithme d'authentification, entrez 32 caractères hexadécimaux. Si vous avez sélectionné SHA1, entrez 40 caractères hexadécimaux. Entrez les données souhaitées dans les champs Inbound SPI (SPI entrant) et Outbound SPI (SPI sortants).

- Status (Etat). Ce paramètre indique l'état de la connexion.

Cliquez sur le bouton **Connect** (Connecter) pour connecter votre tunnel VPN. Cliquez sur **View Logs** (Afficher les fichiers journaux) pour afficher les journaux relatifs au système, au pare-feu, aux accès ou l'ensemble des journaux. Cliquez sur le bouton **Advanced Settings** (Paramètres avancés). L'écran Advanced IPSec VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec) s'affiche.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Advanced VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec)

L'écran Advanced IPSec VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec) vous permet de définir les paramètres de tunnels VPN spécifiques.

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.

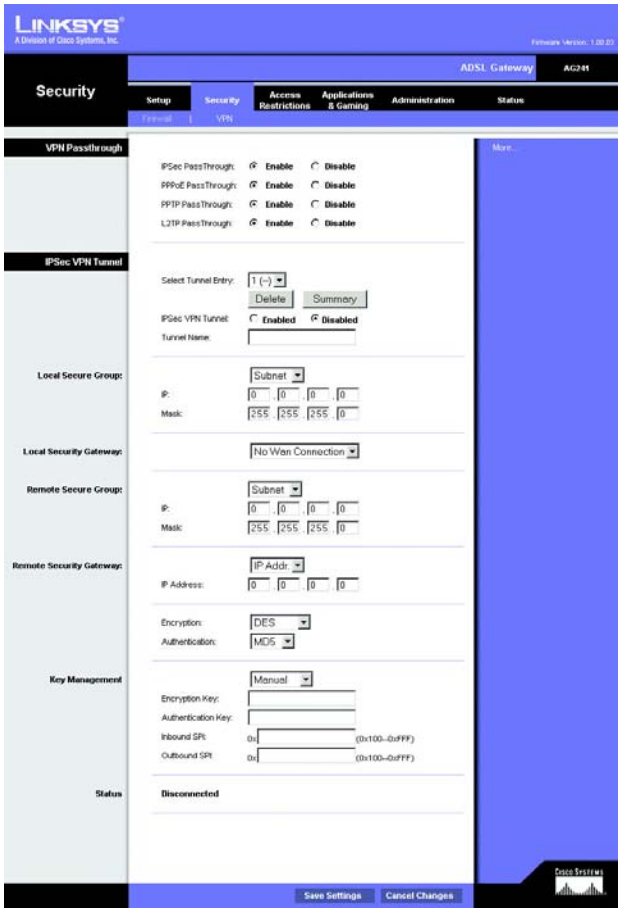


Figure 5-17 : Manual Key Management (Gestion de clé manuelle)

Figure 5-18 : Fichier journal système

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.

- Encryption (Cryptage). Sélectionnez la longueur de la clé utilisée pour crypter/décrypter les paquets ESP. Vous avez deux choix : DES et 3DES. (3DES étant recommandé car plus sûr).
- Authentication (Authentification). Sélectionnez la méthode utilisée pour authentifier les paquets ESP. Vous avez deux choix : MD5 et SHA. (SHA étant recommandé car plus sûr).
- Group (Groupe). Vous pouvez choisir entre deux groupes Diffie-Hellman : 768-bit (768 bits) et 1024-bit (1024 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). Entrez la durée de validité de la clé en secondes avant la prochaine renégociation de clé entre chaque point terminal.

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 deux groupes Diffie-Hellman : 768-bit (768 bits) et 1024-bit (1024 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. Entrez la durée de validité de la clé en secondes avant la prochaine renégociation de clé entre chaque point terminal.

Other Setting (Autres paramètres)

- NetBIOS broadcast (Diffusion NetBIOS). Cochez cette case pour permettre au trafic NetBIOS de passer par le tunnel VPN.
- Anti-replay (Anti-reprise). Cochez cette case pour activer la protection Anti-reprise. Cette fonctionnalité effectue un suivi des séquences à l'arrivée des paquets, assurant ainsi la sécurité au niveau des paquets IP.
- Keep-Alive (Activée). 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.
- Cochez cette case pour bloquer les adresses IP non autorisées. Dans le champ prévu à cet effet, spécifiez combien de fois IKE peut échouer avant le blocage de toutes les adresses IP non autorisées. Entrez cette durée en secondes.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations sur cet onglet, cliquez sur le bouton **Help** (Aide).

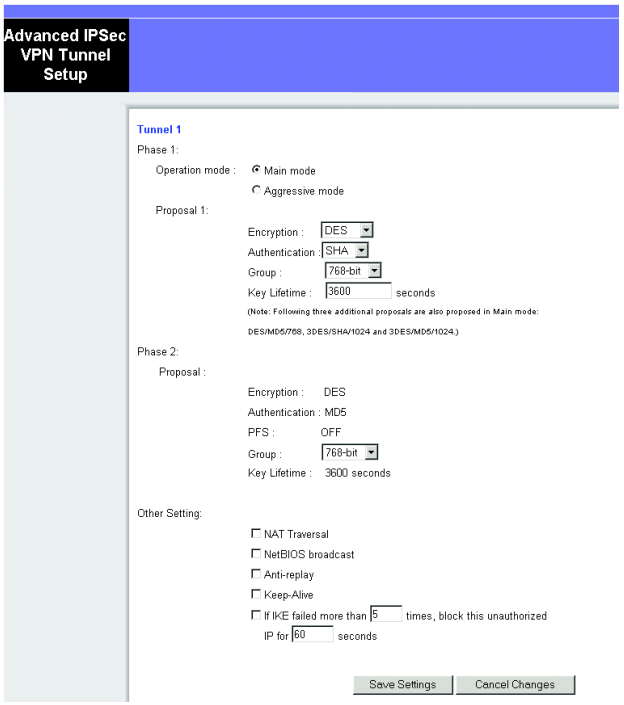


Figure 5-19 : Advanced VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec)

Onglet Access Restrictions (Restrictions d'accès)

Internet Access (Accès Internet)

L'écran Access Restrictions (Restrictions d'accès) 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 définir des filtres en utilisant les numéros de ports du réseau.

- Internet Access Policy (Stratégie d'accès à Internet). L'option Multiple Filters (Filtres multiples) peut être enregistrée sous les paramètres Internet Access Policies (Stratégies d'accès à Internet). Pour modifier une stratégie, sélectionnez son numéro dans le menu déroulant. L'onglet qui apparaît contient les paramètres de cette stratégie. Si vous souhaitez supprimer cette stratégie, cliquez sur le bouton **Delete** (Supprimer). Pour afficher un récapitulatif de toutes les stratégies, cliquez sur le bouton **Summary** (Récapitulatif).

  Les récapitulatifs sont répertoriés dans cet écran. Il contient le nom et les paramètres de chaque stratégie. Pour revenir à l'onglet Filters (Filtres), cliquez sur le bouton **Close** (Fermer).

- Entrer le nom de la stratégie. Les stratégies sont créées à partir des champs présentés ici.

  Pour créer une stratégie d'accès à Internet :

1. Entrez le nom de la stratégie dans le champ Policy Name (Nom de la stratégie) prévu à cet effet. Sélectionnez **Internet Access** (Accès à Internet) comme type de stratégie dans le champ Policy Type (Type de stratégie).

2. Cliquez sur le bouton **Edit List of PCs** (Liste des ordinateurs). L'écran List of PCs (Liste des ordinateurs) s'affiche à l'écran. Dans cet écran, vous pouvez entrer l'adresse IP ou l'adresse MAC de tous les ordinateurs auxquels la stratégie s'applique. Vous pouvez même entrer une étendue d'ordinateurs par adresse IP. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer vos paramètres. Cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour annuler les modifications et revenir dans l'onglet Filters (Filtres).

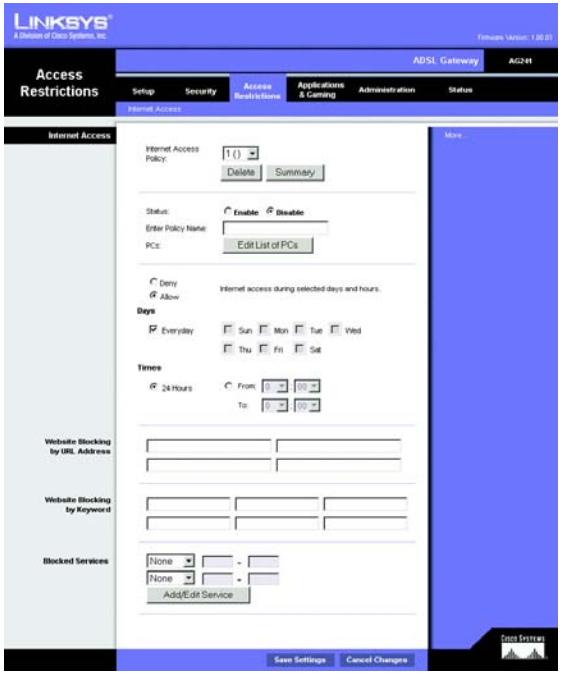


Figure 5-20 : Internet Access (Accès Internet)

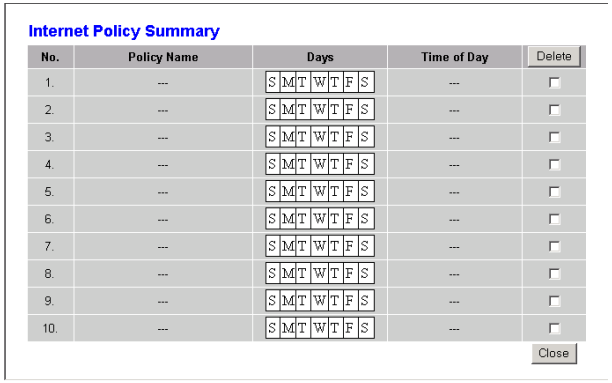


Figure 5-21 : Internet Policy Summary (Récapitulatif de la stratégie Internet)

3. Dans la liste de l'écran List of PCs (Liste des ordinateurs), cliquez sur Allow (Autoriser) pour autoriser l'accès Internet à des ordinateurs ou sur Deny (Refuser) pour le refuser.

4. Vous pouvez filtrer l'accès à divers services accessibles par Internet, notamment le service FTP ou Telnet, en choisissant un service dans les menus déroulants en regard de l'option Blocked Services (Services bloqués). Si un service n'est pas répertorié, vous pouvez cliquer sur le bouton **Add/Edit Service** (Ajouter/Modifier un service) pour ouvrir l'écran Port Services (Services des ports) et ajouter un service à la liste. Vous devrez alors renseigner les champs Service name (Nom du service), Protocol (Protocole) et Port Range (Connexion).

5. En choisissant les paramètres de jour et d'heure appropriés, spécifiez la date et l'heure du filtrage d'accès à Internet.

6. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour activer la stratégie.

Il est également possible de filtrer l'accès à Internet par URL, c'est-à-dire l'adresse Internet permettant d'accéder à un site Web. Pour cela, entrez l'adresse URL souhaitée dans l'un des champs Website Blocking by URL Address (Blocage du site Web par adresse URL). Si vous ne connaissez pas l'adresse URL, vous pouvez effectuer un filtrage par mot-clé en entrant un mot-clé dans l'un des champs Website Blocking by Keyword (Blocage du site Web par mot-clé).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

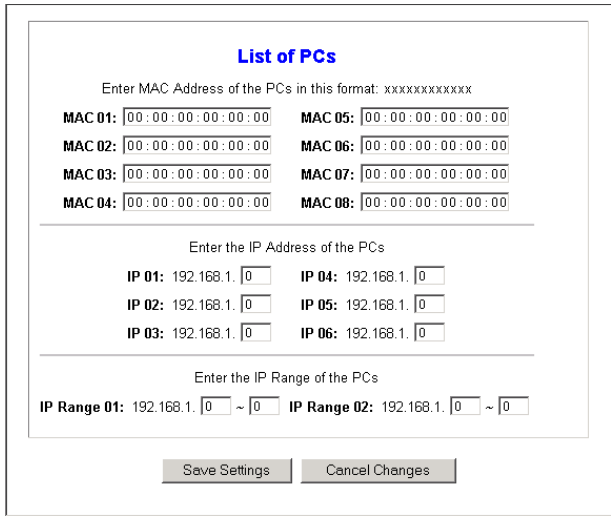


Figure 5-22 : List of PCs (Liste des ordinateurs)

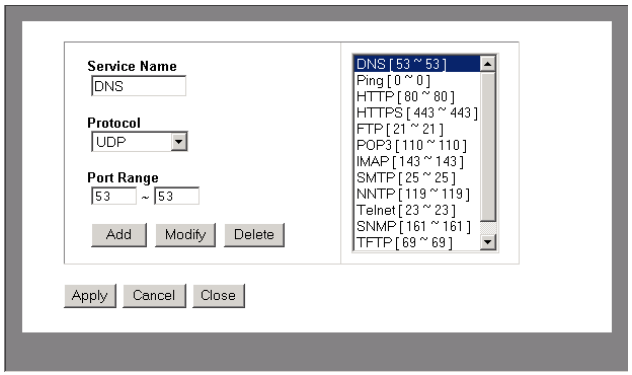


Figure 5-23 : Services des ports

Onglet Applications and Gaming (Applications et jeux)

Single Port Forwarding (Transfert de connexion unique)

Cet écran contient des options de personnalisation de vos services de ports pour les applications fréquemment utilisées.

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.

Sélectionnez ou entrez un nom d'application dans les champs prévus à cet effet. Entrez ensuite les numéros de ports internes et externes dans les champs External Port (Port externe) et Internal Port (Port interne). Sélectionnez le type de protocole que vous souhaitez utiliser pour chaque application : **TCP** ou **UDP**. Entrez l'adresse IP dans le champ Adresse IP. 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 Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

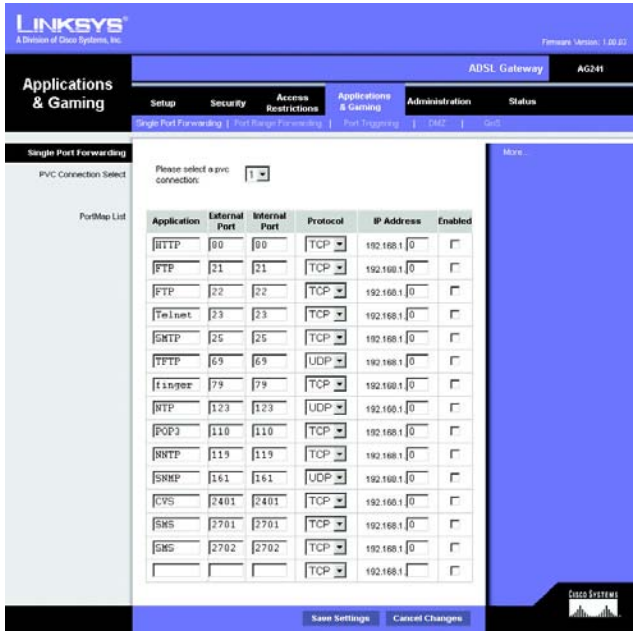


Figure 5-24 : Single Port Forwarding (Transfert de connexion unique)

Port Range Forwarding (Transfert de connexion)

Ce écran permet de configurer les services publics sur votre réseau, tels que les serveurs Web, les serveurs FTP, les serveurs de messagerie électronique ou toutes les autres applications Internet spécialisées. Par applications spécialisées, on entend toutes les applications qui utilisent un accès 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.

- Application. Entrez le nom que vous souhaitez donner à chaque application.
- Start (Début) et End (Fin). Dans les champs Start (Début) et End (Fin), entrez les numéros de début et de fin du port que vous souhaitez transférer.
- TCP UDP. Sélectionnez le type de protocole que vous souhaitez utiliser pour chaque application : **TCP**, **UDP** ou **Both** (Les deux).
- IP Address (Adresse IP). Entrez l'adresse IP et cliquez sur **Enabled** (Activé).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

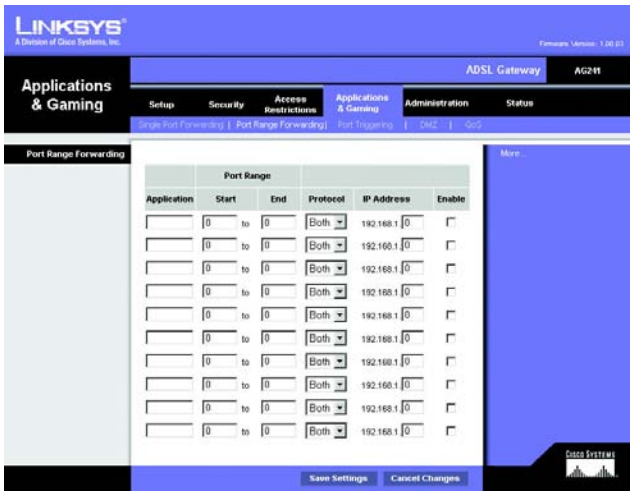


Figure 5-25 : Port Range Forwarding (Transfert de connexion)

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, les données sont dirigées vers l'ordinateur approprié au moyen de l'adresse IP et des règles de mappage de ports.

- Application. Entrez le nom que vous souhaitez donner à chaque application.
- Start Port (Port de début) et End Port (Port de fin). Aux sections Triggered Range (Connexion sortante déclenchée) et Forwarded Range (Connexion entrante transférée), entrez vos informations dans les champs Start Port (Port de début) et End Port (Port de fin) pour le port que vous souhaitez transférer.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

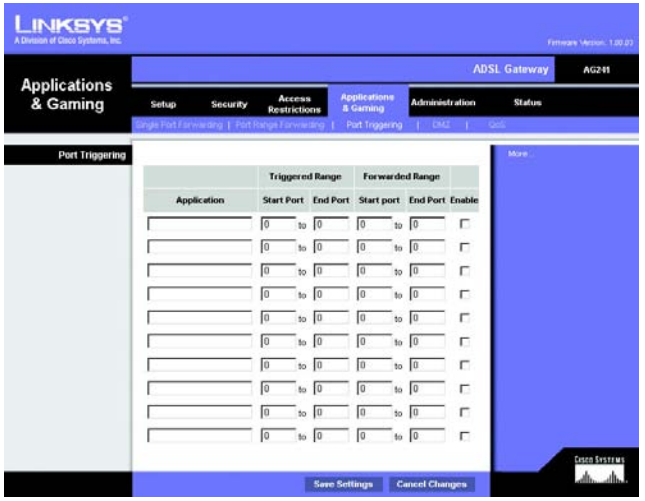


Figure 5-26 : Port Triggering (Déclenchement de connexion)

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.

- 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 **Enabled** (Activé). Pour la désactiver, sélectionnez **Disabled** (Désactivé).
- DMZ Host IP Address (Adresse IP de l'hôte DMZ). Pour exposer un ordinateur, entrez 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 adaptateur Ethernet ».

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Figure 5-27 : DMZ

QoS (QS)

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.

QS basée sur une application

La qualité de service basée sur une application gère les informations telles qu'elles sont transmises et reçues. Selon le paramètre de l'écran *QoS* (QS), cette fonction affecte une priorité faible ou élevée aux cinq applications prédéfinies et aux trois applications supplémentaires que vous spécifiez.

Enable/Disable (Activer/Désactiver). Pour utiliser QS basé sur une application, sélectionnez **Enable** (Activer). Sinon, conservez la valeur par défaut, **Disable** (Désactiver).

High priority (Priorité élevée)/**Medium priority** (Priorité moyenne)/**Low priority** (Faible priorité). Pour chaque application, sélectionnez **High priority** (Priorité élevée) (le trafic de cette file d'attente partage 60 % de la bande passante totale), **Medium priority** (Priorité moyenne) (le trafic de cette file d'attente partage 18 % de la bande passante totale) ou **Low priority** (Priorité faible) (le trafic de cette file d'attente partage 1 % de la bande passante totale).

FTP (File Transfer Protocol). Protocole utilisé pour la transmission de fichiers sur un réseau TCP/IP (Internet, UNIX, etc.). Par exemple, lorsque des pages HTML sont développées pour un site Web sur une machine locale, elles sont généralement téléchargées sur le serveur Web via FTP.

HTTP (HyperText Transport Protocol). Protocole de communication utilisé pour la connexion à des serveurs sur le World Wide Web. Sa principale fonction est d'établir une connexion à un serveur Web et de transmettre les pages HTML au navigateur Web du client.

Telnet. Protocole d'émulation de terminal couramment utilisé sur les réseaux Internet et TCP/IP. Il permet à un utilisateur d'un terminal ou d'un ordinateur de se connecter à un périphérique distant et d'exécuter un programme.

SMTP (Simple Mail Transfer Protocol). Protocole de messagerie standard utilisé sur Internet. Il s'agit d'un protocole TCP/IP qui définit le message et l'agent de transfert de messages (MTA), qui enregistre et transmet les messages.

POP3 (Post Office Protocol 3). Serveur de messagerie standard couramment utilisé sur Internet. Il fournit un emplacement de stockage des messages qui contient les messages entrants jusqu'à ce que les utilisateurs se connectent et les téléchargent. POP3 est un système simple requérant peu de sélections. Tous les messages et pièces jointes en attente sont téléchargés en même temps. POP3 utilise le protocole de messagerie SMTP.

Specific Port# (Numéro de port spécifique). Vous pouvez ajouter trois applications supplémentaires en entrant leur numéro de port correspondant dans les champs *Specific Port#* (Numéro de port spécifique).

Advanced QoS (QS avancé)

Ce paramètre permet de spécifier une priorité de file d'attente du trafic.

Fragment packet's size of AF and BE traffic to be equal to the size of EF traffic (Fragmenter la taille des paquets du trafic AF et BE pour qu'elle soit égale à celle du trafic EF). Sélectionnez cette option pour fragmenter les tailles de paquet des files d'attente AF (Assured Forwarding) et BE (Best Effort) afin d'augmenter l'efficacité des files d'attente EF (Expedited Forwarding) de transport. Entrez une plage comprise en 68 et 1492 octets.

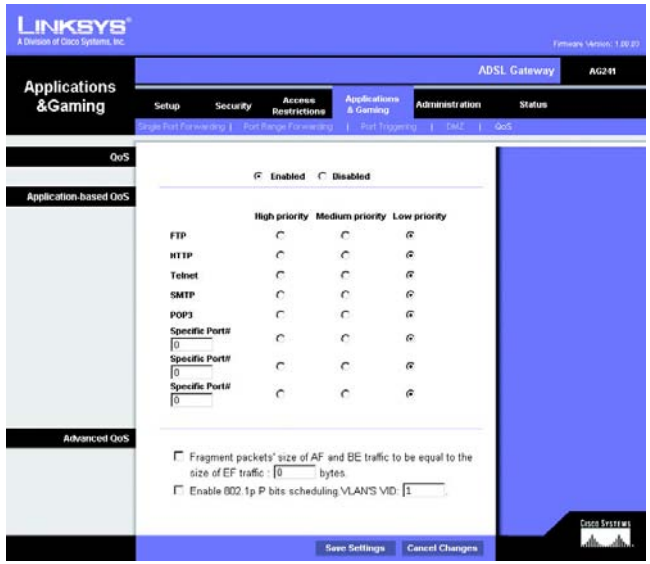


Figure 5-28 : QoS (QS)

Enable 802.1p P bits scheduling, VLAN's VID (Activer la planification de bits 802.1p P. VID VLAN). Sélectionnez cette option pour activer la planification de la classification de bits 802.1p P dans le VLAN approprié en fonction de l'identification IEEE 802.1Q VLAN. Entrez le numéro VID VLAN (Identificateur VLAN) dans ce champ.

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.

Onglet Administration

Management (Gestion)

L'écran Management (Gestion) vous permet de modifier les paramètres d'accès au modem routeur et de configurer le protocole SNMP (Simple Network Management Protocol) ainsi que la fonctionnalité UPnP (Universal Plug and Play).

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 Username (Nom d'utilisateur du modem routeur). Entrez 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 ce mot de passe par défaut par un mot de passe de votre choix.
- Re-enter to confirm (Confirmation du mot de passe). Entrez 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.

  IMPORTANT : L'activation de l'administration à distance permet à chaque personne disposant de votre mot de passe de configurer à distance le modem routeur via Internet.
- Remote Administration (Administration à distance). Cette fonction vous permet d'administrer le modem routeur à partir d'un emplacement distant, via Internet. Pour activer l'administration à distance, cliquez sur **Enabled** (Activé).
- Administration Port (Port d'administration). Entrez le numéro de port que vous souhaitez utiliser pour accéder à distance au modem routeur.

SNMP

SNMP est un protocole très répandu de contrôle et de gestion réseau.

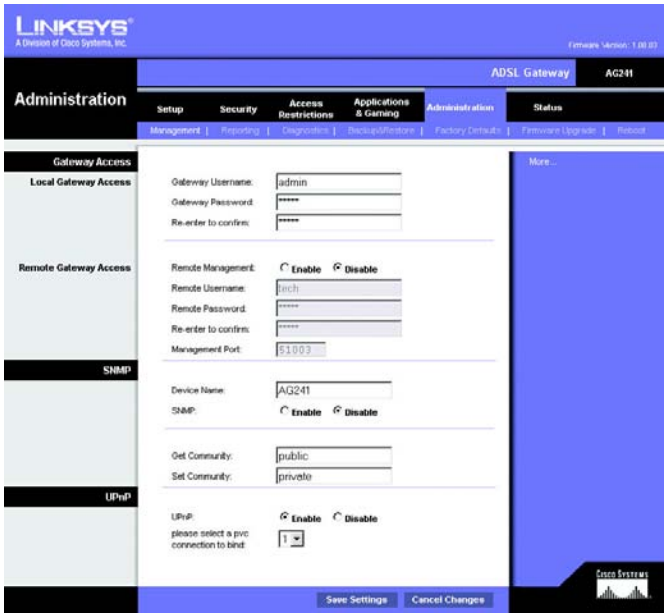


Figure 5-29 : Management (Gestion)

Identification. Pour activer le SNMP, cliquez sur **Enabled** (Activé). Pour désactiver le SNMP, cliquez sur **Disabled** (Désactivé).

UPnP

UPnP permet à Windows 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 **Enabled** (Activé).

Sélectionnez une connexion pvc à lier Sélectionnez un numéro dans le menu déroulant.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Reporting (Rapports)

L'onglet Reporting (Rapports) vous 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.

- Log (Fichier journal). Pour activer la génération de fichiers journaux, cliquez sur **Enabled** (Activé).
- Logviewer IP Address (Adresse IP de réception des fichiers journaux). Entrez l'adresse IP de réception des fichiers journaux.

Email Alerts (Alertes de messagerie électronique)

E-Mail Alerts (Alertes de messagerie électronique). Pour activer les alertes de messagerie électronique, cliquez sur **Enabled** (Activées).

- Denial of Service Thresholds (Seuils de refus de service). Entrez les seuils des événements que vous souhaitez recevoir.
- SMTP Mail Server (Serveur de messagerie électronique SMTP). Entrez l'adresse IP du serveur SMTP.
- E-Mail Address for Alert Logs (Adresse de messagerie électronique pour fichiers journaux d'alertes). Entrez l'adresse de messagerie électronique pour les fichiers journaux d'alertes.
- Return E-Mail address (Adresse de messagerie électronique de retour). Entrez l'adresse de retour des messages électroniques.

Pour afficher les fichiers journaux, cliquez sur le bouton **View Logs** (Afficher les fichiers journaux).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Setting**s (Enregistrer les paramètres) pour les enregistrer ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Figure 5-30 : Reporting (Rapports)

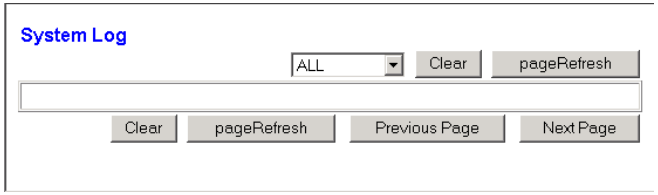


Figure 5-31 : System Log (Fichier journal système)

Diagnostics

Ping Test (Test Ping)

Ping Test Parameters (Paramètres de test Ping)

- Ping Target IP (IP de cible Ping). Entrez 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). Entrez une taille de paquets Ping.
- Number of Pings (Nombre de Pings). Entrez le nombre de fois que vous souhaitez effectuer le Ping.
- Ping Interval (Intervalle de Ping). Entrez l'intervalle de Ping en millisecondes.
- Ping Timeout (Délai de Ping). Entrez le délai en millisecondes.
- Ping Result (Résultat de Ping). Les résultats du test Ping sont affichés ici.

Cliquez sur le bouton **Start Test** (Démarrer le test) pour démarrer le test de Ping.

Figure 5-32 : Ping Test (Test Ping)

BAckup&Restore (Sauvegarde et restauration)

Cet onglet permet de sauvegarder et de restaurer le fichier de configuration du modem routeur.

Pour sauvegarder le fichier de configuration du routeur, cliquez sur le bouton **Backup** (Sauvegarder). Suivez les instructions affichées.

Pour restaurer le fichier de configuration du routeur, cliquez sur le bouton **Browse** (Parcourir) pour localiser le fichier et suivez les instructions affichées. Après avoir sélectionné le fichier, cliquez sur le bouton **Restore** (Restaurer).

Figure 5-33 : Backup&Restore (Sauvegarde et restauration)

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 **Yes** (Oui).

Pour débuter le processus de restauration, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer ces modifications ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour annuler les modifications effectuées.

Figure 5-34 : Factory Defaults (Paramètres d'usine)

Firmware Upgrade (Mise à niveau du micrologiciel)

Le modem routeur ADSL permet de mettre à niveau le micrologiciel côté LAN (réseau) du modem routeur.

Upgrade from LAN (Mise à niveau à partir du réseau LAN)

Pour mettre à niveau le micrologiciel du modem routeur à partir du réseau LAN :

1. Cliquez sur le bouton **Browse** (Parcourir) pour rechercher le fichier de mise à niveau du micrologiciel que vous avez téléchargé à partir du site Web de Linksys puis décompressé.

2. Cliquez deux fois sur le fichier du micrologiciel que vous venez de télécharger et de décompresser. Cliquez sur le bouton **Upgrade** (Mettre à niveau) et suivez les instructions à l'écran.

Figure 5-35 : Firmware Upgrade (Mise à niveau du micrologiciel)

Reboot (Redémarrage)

Cet onglet permet d'effectuer un redémarrage logiciel ou matériel du modem routeur.

Mode de redémarrage. Pour redémarrer le modem routeur sélectionnez **Hard** (Matériel) ou **Soft** (Logiciel). Sélectionnez Hard (Matériel) pour lancer le cycle d'alimentation du modem routeur ou sur Soft (Logiciel) pour le redémarrer sans recourir au cycle d'alimentation.

Pour lancer la procédure de redémarrage, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres). Quand un écran vous demande si vous souhaitez vraiment redémarrer le périphérique. Cliquez sur **OK**.

Cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour annuler vos modifications.

Figure 5-36 : Reboot (Redémarrage)

Onglet Status (Etat)

Modem routeur

Cet écran contient des informations sur votre modem routeur et ses connexions WAN (Internet).

Gateway Information (Informations sur le modem routeur)

Cette section contient les éléments suivants : Software Version (Version du logiciel), MAC Address (Adresse Mac) et Current Time (Heure actuelle).

Internet Connections (Connexions Internet)

Internet Connections (Connexions Internet) s'affiche après sélection du numéro de connexion Internet dans le menu déroulant. Il s'agit des options suivantes : Login Type (Type de connexion), Interface, IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau), Default Gateway (Modem routeur par défaut) et DNS Server (Serveurs DNS) 1, 2 et 3.

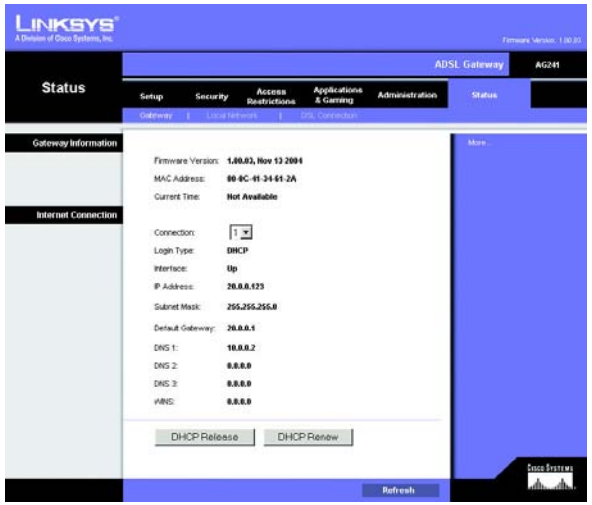


Figure 5-37 : Status (Etat)

DHCP Renew (Renouvellement DHCP). 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). 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 l'écran.

Local Network (Réseau local)

Cette section contient les éléments suivants : 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 tableau des clients DHCP, cliquez sur le bouton **DHCP Clients Table** (Tableau des clients DHCP).

Figure 5-38 : Local Network (Réseau local)

DHCP Clients Table (Tableau des clients DHCP). Cliquez sur le bouton **DHCP Clients Table** (Tableau des clients DHCP) pour afficher les données actuelles des clients DHCP. Ce tableau contient l'adresse Mac, le nom de l'ordinateur et l'adresse IP des clients réseau qui utilisent le serveur DHCP. Les données sont stockées dans la mémoire temporaire et sont régulièrement modifiées. Pour supprimer un client d'un serveur DHCP, sélectionnez le client, puis cliquez sur le bouton **Delete** (Supprimer).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser l'écran. Cliquez sur le bouton **Close** (Fermer) pour fermer l'écran.

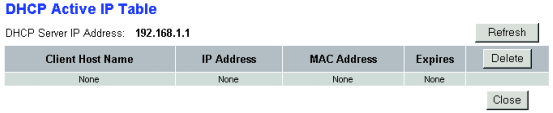


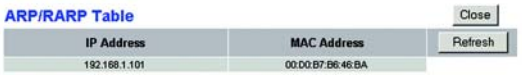
Figure 5-39 : DHCP Clients Table (Tableau des clients DHCP)

DSL Connection (Connexion DSL)

La section DSL Connection (Connexion DSL) contient les éléments suivants : Status (Etat), Downstream Rate (Débit de réception), Upstream Rate (Débit d'émission).

La section PVC Connection (Connexion PVC) contient les éléments suivants Encapsulation, Multiplexing (Multiplexage), QoS (QS), Pcr Rate (Taux Pcr), Scr Rate (Taux Scr), Autodetect (Détection automatique), VPI, VCI et PVC Status (Etat PVC).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser l'écran.



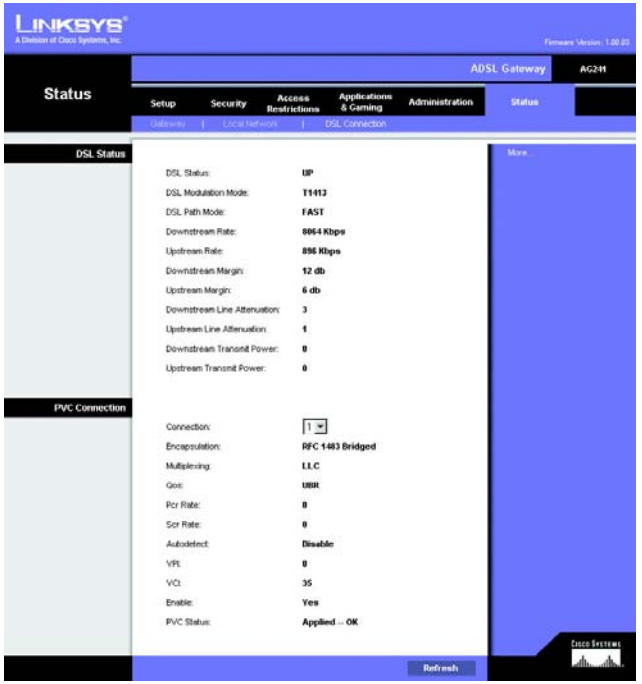


Figure 5-40 : DSL Connection (Connexion DSL)

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**. Cliquez deux fois sur **Réseau**.
     2. Dans la zone Les composants réseau suivants sont installés, sélectionnez le composant TCP/IP associé à votre carte Ethernet. Si une seule carte Ethernet est installée, une seule ligne TCP/IP apparaît sans association à une carte 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. Entrez une adresse IP unique 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 **Passerelle**, puis tapez 192.168.1.1 dans le champ Nouvelle passerelle, c'est-à-dire l'adresse IP par défaut du modem routeur. Cliquez sur le bouton Ajouter pour valider cette entrée.
     5. Cliquez sur l'onglet **Configuration DNS** et assurez-vous que l'option Désactiver DNS est sélectionnée. Entrez les noms de l'hôte et du domaine (par exemple, Jean pour l'hôte et « domicile » pour le domaine). Entrez le DNS fourni par votre fournisseur d'accès Internet (FAI). Si votre FAI ne vous a fourni aucune adresse IP DNS, contactez-le pour obtenir cette information ou recherchez l'information 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 dès que le système vous le demande.
   - Sous Windows 2000 :
     1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois 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. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté au modem routeur.
5. Entrez le masque de sous-réseau 255.255.255.0.
6. Entrez 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 entrez 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 le système vous le demande.

- 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. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté au modem routeur.
  6. Entrez le masque de sous-réseau 255.255.255.0.
  7. Entrez 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 entrez 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 le système vous le demande.

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 carte 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 entrer 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 s'il s'agit de l'ordinateur d'origine qui est la cause 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 s'il s'agit de l'ordinateur d'origine qui est la cause 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 s'il s'agit de l'ordinateur d'origine qui est la cause 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 corrects. Contactez votre FAI pour savoir si votre connexion Internet est de type RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE ou RFC 2364 PPPoA. Reportez-vous à la rubrique Configuration du « Chapitre 5 : Configuration du modem routeur » 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 que vous disposez bien d'une adresse IP dans l'onglet Status (Etat) de l'utilitaire Web du modem routeure.

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 que 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, un modem routeur 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 tel qu'un serveur de messagerie, un 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. Entrez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
  3. Entrez l'étendue des ports externes du service que vous utilisez. Par exemple, si vous utilisez un serveur Web, entrez l'étendue 80 à 80.
  4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.
  5. Entrez 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, entrez 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 un hébergement pour jeux en ligne ou utiliser d'autres applications Internet.

Si vous souhaitez jouer en ligne ou utiliser des applications Internet, la plupart des opérations fonctionnent sans aucun transfert de connexion ou hébergement DMZ. Il se peut, dans certains cas, que vous souhaitiez héberger un jeu en ligne ou une application Internet. Vous devez dans ce cas configurer le modem routeur pour qu'il envoie les paquets entrants ou les données entrantes vers un ordinateur spécifique. Ceci s'applique également aux applications Internet que vous utilisez. Pour connaître les ports à utiliser, le mieux est de consulter directement le site Web des jeux en ligne ou des applications. 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. Entrez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
3. Entrez l'étendue des ports externes du service que vous utilisez. Par exemple, si vous souhaitez héberger Unreal Tournament (UT), entrez l'étendue 7777 à 27900.
4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.
5. Entrez 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, entrez 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 » pour plus d'informations sur l'obtention d'une adresse IP.
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. Le jeu Internet, le serveur ou l'application ne fonctionne pas.

Si vous rencontrez des difficultés à faire fonctionner correctement un jeu Internet, un serveur ou une application, exposez un ordinateur à Internet à l'aide de l'hébergement DMZ (DeMilitarized Zone). Cette option peut être utilisée lorsqu'une application requiert trop de ports ou lorsque vous ne connaissez pas les services de ports à 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 d'accès des 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 entrez l'adresse IP de l'ordinateur.
  2. Contrôlez les pages Port Forwarding (Transfert de connexion) et désactivez les entrées que vous avez spécifiées pour le transfert. Conservez ces informations au cas où vous souhaiteriez les utiliser ultérieurement.
- 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 vers 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. Entrez 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. Entrez un nouveau mot de passe dans le champ Gateway Password (Mot de passe du modem routeur) et entrez le même mot de passe 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 destiné à la connexion Internet, l'ordinateur n'a pas besoin des paramètres de proxy pour l'accès à Internet. Pour vérifier que vos paramètres de proxy sont supprimés et que le navigateur que vous utilisez est défini pour se connecter directement au réseau local (LAN), procédez comme suit :

- Pour Microsoft Internet Explorer 5.0 ou version ultérieure :
  1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois 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 4.7 ou version ultérieure :
  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.

Appuyez pendant 10 secondes sur le bouton **Reset** (Réinitialisation), 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 www.linksys.com/international et télécharger le dernier micrologiciel .

- Procédez comme suit :
  1. Accédez au site Web international de Linksys à www.linksys.com/international et sélectionnez votre région ou pays.
  2. Cliquez sur l'onglet **Produit** et sélectionnez le modem routeur.
  3. Sur la page Web du modem routeur, cliquez sur **Micrologiciel** puis téléchargez la dernière version disponible.
  4. Pour mettre à niveau le modem routeur, suivez les étapes décrites à la rubrique Administration du « Chapitre 5 : Configuration du modem routeur ».

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 votre ordinateur. Reportez-vous au problème 1 (Je dois 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
  Modem routeur : 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.

PPPoE n'est pas réellement 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 la connexion « activée ». Il se peut que cela ne fonctionne pas. Dans ce cas, vous devrez rétablir la connexion de temps à autre.
  1. Pour connecter le modem routeur, ouvrez le navigateur Web et entrez http://192.168.1.1 ou l'adresse IP du modem routeur.
  2. Si le système vous y invite, entrez le nom d'utilisateur et le mot de passe. (Par défaut, admin).
  3. Dans l'écran Setup (Configuration), sélectionnez l'option **Keep Alive** (Activé) et définissez le délai de rappel à 20 (secondes).
  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 corrompues 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 entrez http://192.168.1.1 ou l'adresse IP du modem routeur.
  2. Si le système vous y invite, entrez 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 Taille, entrez 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 la liste de valeurs suivantes (une à la fois et dans cet ordre) 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 spécifie une URL ou une adresse IP, j'obtiens une erreur liée à l'expiration du délai et le système m'invite 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 (Modem routeur par défaut) et DNS). Redémarrez l'ordinateur défaillant.
- Si l'ordinateur est configuré correctement, mais ne fonctionne toujours pas, vérifiez le modem routeur. Vérifiez qu'il est connecté et sous tension. Connectez-y vous et vérifiez ses paramètres. Si vous ne parvenez pas à vous connecter à le modem routeur, vérifiez le réseau local (LAN) et les connexions d'alimentation.

- Si le modem routeur est configuré 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.
- et 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.

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-il installé sur le réseau ?
Dans un environnement standard, le modem routeur est installé entre la prise murale ADSL et le réseau local (LAN).

Le modem routeur prend-il 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 et 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-il 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-il 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 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. Un problème : la version 1.0.1.6 n'autorise pas plusieurs ordinateurs dotés de la même clé CD à 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 carte Ethernet à 10 Mbit/s ou en mode semi-duplex, puis désactivez temporairement la fonctionnalité d'évaluation automatique de la configuration (Auto-negotiate) de votre carte 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-il dans un environnement Macintosh ?
Oui mais les pages de configuration du modem routeur ne sont accessibles que par l'intermédiaire d'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 ?
L'hébergement DMZ (DeMilitarized Zone) permet à une adresse IP (ordinateur) d'être exposée à 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 une adresse IP 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-il 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 peuvent être transférés 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.

Quel est le nombre maximal de sessions VPN que le modem routeur peut prendre en charge ?
Ce nombre dépend de plusieurs facteurs. 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.

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-il être utilisé en tant que serveur DHCP ?
Oui. Le logiciel serveur DHCP est intégré au modem routeur.

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'une carte 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.

Combien de canaux/fréquences sont disponibles avec le modem routeur ?
Onze canaux sont disponibles, classés de1 à 11 (en Amérique du Nord).

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 : Configuration de IPSec entre un ordinateur Windows 2000 ou Windows XP et le modem routeur

Introduction

Cette annexe vous explique comment établir un tunnel IPSec sécurisé à l'aide de clés partagées pour connecter un réseau privé via le modem routeure VPN et une machine Windows 2000 ou XP. Les informations relatives à la configuration d'un serveur Windows 2000 sont disponibles sur le site Web de Microsoft, dans la Base de connaissance technique :

Q252735 - How to Configure IPSec Tunneling in Windows 2000 (Comment configurer un tunnel IPSec sous Windows 2000)
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Q257225 - Basic IPSec Troubleshooting in Windows 2000 (Bases du dépannage IPSec sous Windows 2000)
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

REMARQUE : Notez toutes les modifications que vous effectuez. Ces modifications sont identiques dans l'application Windows « secpol » et l'utilitaire Web du routeur.

Environnement

Les adresses IP et les autres éléments spécifiques aux composants/produits mentionnés dans cette annexe sont des exemples.

REMARQUE : Les instructions et les chiffres de cette section font référence au routeur. Remplacez « Modem routeur » par « Routeur ». De même, le texte de l'écran peut être différent de celui de vos instructions pour « OK » ou « Fermer » ; cliquez sur le bouton approprié de votre écran.

Windows 2000 ou Windows XP
Adresse IP : 140.111.1.2 <= Le FAI de l'utilisateur fournit l'adresse IP (exemple uniquement).

Masque de sous-réseau : 255.255.255.0

WAG54G

Adresse IP WAN : 140.111.1.1 <= Le FAI de l'utilisateur fournit l'adresse IP (exemple uniquement).

Masque de sous-réseau : 255.255.255.0
Adresse IP LAN : 192.168.1.1
Masque de sous-réseau : 255.255.255.0

Comment établir un tunnel IPSec sécurisé ?

Etape 1 : Etablissement d'une stratégie IPSec

1. Cliquez sur le bouton **Démarrer**, sélectionnez **Exécuter** et entrez **secpol.msc** dans le champ **Ouvrir**. L'écran *Paramètres de sécurité locaux* s'affiche (figure B-1).

2. A l'aide du bouton droit de la souris, cliquez sur **Stratégies de sécurité IP sur Ordinateur local** (Win XP) ou **Stratégies de sécurité IP sur Ordinateur local** (Win 2000), puis cliquez sur **Créer une stratégie de sécurité IP**.

3. Cliquez sur le bouton **Suivant**, puis entrez un nom pour la stratégie (par exemple, to_Router). Cliquez ensuite sur Suivant.

4. Décochez la case **Activer la règle de réponse par défaut**, puis cliquez sur le bouton **Suivant**.

5. Cliquez sur le bouton **Terminer** en vérifiant que la case **Modifier** est cochée.

Etape 2 : Création des listes de filtres

Liste de filtres 1 : win->Router

1. Dans ce nouvel écran des propriétés de règles, vérifiez que l'onglet **Règles** est sélectionné (figure B-2). Décochez la case **Utiliser l'Assistant Ajou**t puis cliquez sur le bouton **Ajouter** pour créer une nouvelle règle.

2. Assurez-vous que l'onglet **Liste de filtres IP** est sélectionné, puis cliquez sur le bouton **Ajouter**. (Voir la figure B-3.) L'écran *Liste de filtres IP* apparaît (figure C-4). Entrez le nom souhaité pour la liste de filtres (win->Router, par exemple) et décochez la case **Utiliser l'Assistant Ajout**. Cliquez ensuite sur le bouton **Ajouter**.

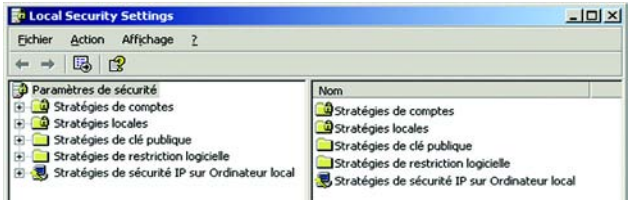


Figure B-1 : Ecran de sécurité locale

REMARQUE : Les références Windows contenues dans cette section sont des références Windows 2000 et Windows XP. Remplacez les références de « Routeur » par « Modem routeur ». De même, le texte de l'écran peut être différent de celui de vos instructions pour « OK » ou « Fermer » ; cliquez sur le bouton approprié de votre écran.

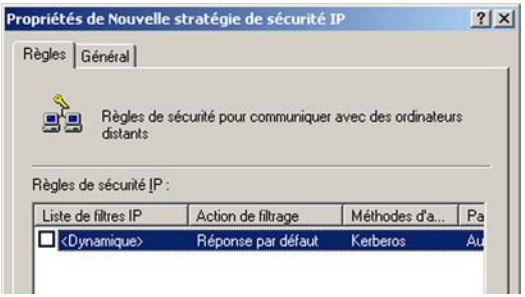


Figure B-2 : Onglet Règles

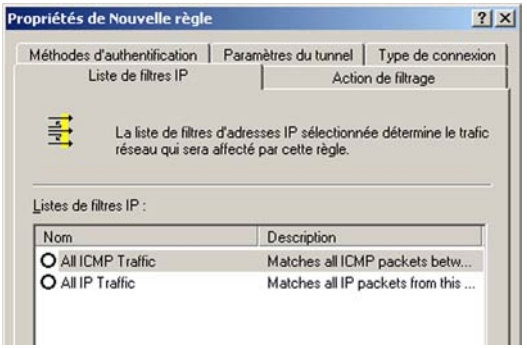


Figure B-3 : Onglet Liste de filtres IP

3. L'écran *Propriétés de filtre* apparaît (figure C-5). Sélectionnez l'onglet **Adressage**. Dans le champ *Adresse source*, sélectionnez **Mon adresse IP**. Dans le champ *Adresse de destination*, sélectionnez **Un sous-réseau IP spécifique**, et entrez l'adresse IP : 192.168.1.0 et le masque de sous-réseau : 255.255.255.0. Ce sont les paramètres par défaut du routeur. Si vous avez modifié ces paramètres, entrez les nouvelles valeurs dans ces champs.)

4. Si vous souhaitez entrer une description de votre filtre, cliquez sur l'onglet **Description** et saisissez votre description.

5. Cliquez sur le bouton **OK**. Puis cliquez sur le bouton **OK** ou **Fermer** de la fenêtre *Liste de filtres IP*.

Liste de filtres 2 : Router ->win

6. L'écran *Propriétés de Nouvelle règle* apparaît (figure C-6). Sélectionnez l'onglet **Liste de filtres IP** et assurez-vous que **win -> Router** apparaît en surbrillance. Cliquez ensuite sur le bouton **Ajouter**.

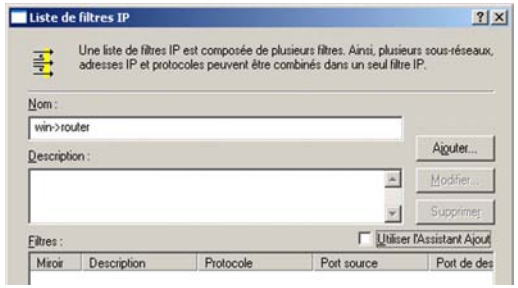


Figure B-4 : Liste de filtres IP

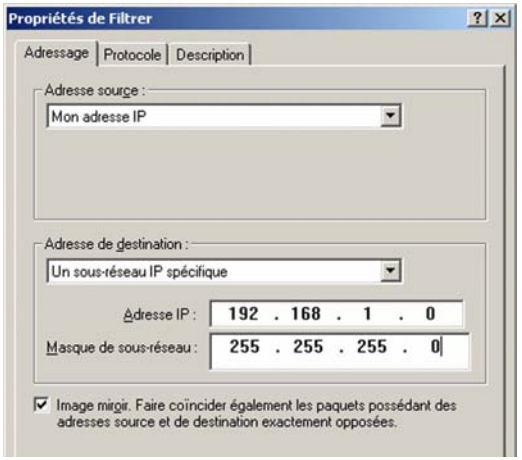


Figure B-5 : Propriétés de Filtrer

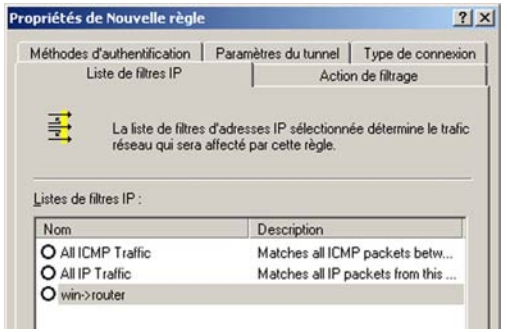


Figure B-6 : Propriétés de Nouvelle règle

7. L'écran *Liste de filtres IP* apparaît (figure B-7). Entrez le nom souhaité pour la liste de filtres (Router->win, par exemple) et désactivez la case à cocher **Utiliser l'Assistant Ajout**. Cliquez ensuite sur le bouton **Ajouter**.

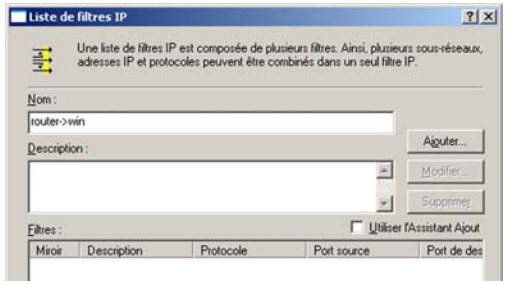


Figure B-7 : Liste de filtres IP

8. L'écran *Propriétés de filtre* apparaît (figure B-8). Sélectionnez l'onglet Adressage. Dans le champ *Adresse source*, sélectionnez **Un sous-réseau IP spécifique**, et entrez l'adresse IP : 192.168.1.0 et le masque de sous-réseau : 255.255.255.0. Si vous avez modifié les paramètres par défaut, entrez vos nouvelles valeurs. Dans le champ Adresse de destination, sélectionnez **Mon adresse IP**.

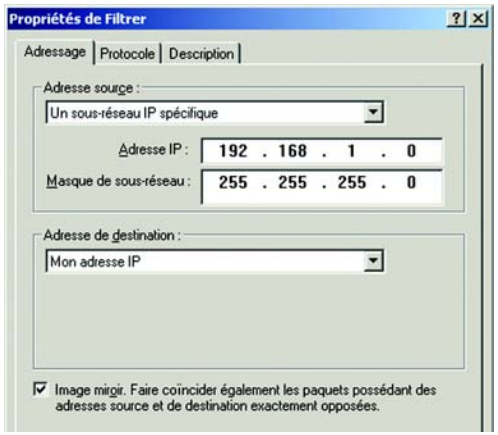


Figure B-8 : Propriétés de Filtrer

9. Si vous souhaitez entrer une description de votre filtre, cliquez sur l'onglet *Description* et saisissez votre description.

10. Cliquez sur le bouton **OK** ou **Fermer**. L'écran *Propriétés de Nouvelle règle* apparaît. L'onglet Liste de filtres IP est sélectionné (figure B-9). « Router -> win » et « win -> Router » doivent maintenant être répertoriés. Cliquez sur le bouton **OK** (Win XP) ou **Fermer** (Win 2000) de la fenêtre *Liste des filtres IP*.

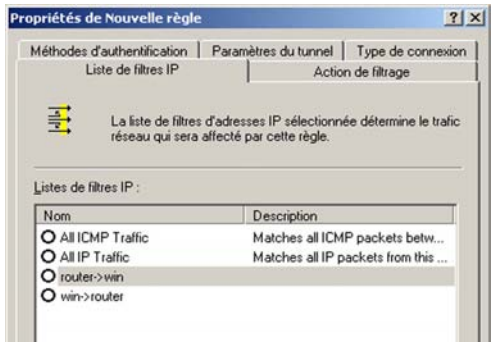


Figure B-9 : Propriétés de Nouvelle règle

Etape 3 : Configuration des règles de tunnel individuelles

Tunnel 1 : win->Router

1. Dans l'onglet *Liste de filtres IP* (figure B-10), cliquez la liste de filtres win->Router.

2. Cliquez sur l'onglet **Action de filtrage** (figure B-11) et cliquez sur le bouton radio **Sécurité requise**. Cliquez ensuite sur le bouton **Modifier**.

3. Dans l'onglet *Méthodes de sécurité* (figure B-12), assurez-vous que l'option **Négocier la sécurité** est activée. Décochez la case **Accepter les communications non sécurisées, mais toujours répondre en utilisant IPSec**. Sélectionnez **Session de clé principale PFS** puis cliquez sur le bouton **OK**.

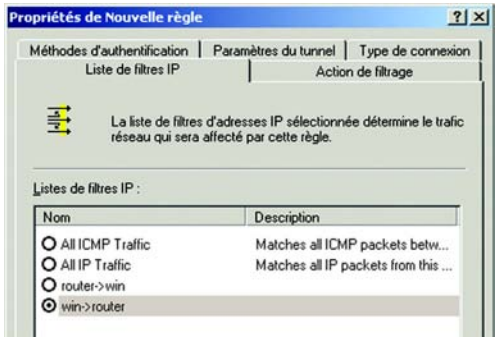


Figure B-10 : Onglet Liste de filtres IP

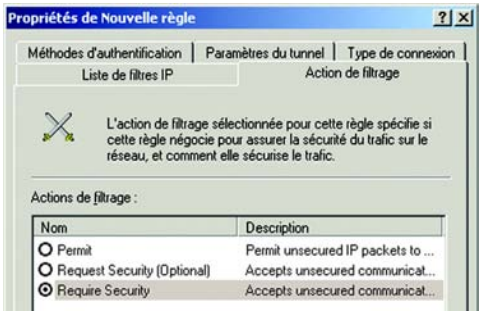


Figure B-11 : Onglet Action de filtrage

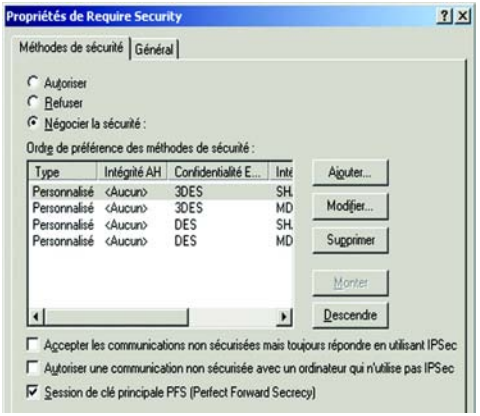


Figure B-12 : Onglet Méthodes de sécurité

4. Sélectionnez l'onglet **Méthodes d'authentification** (figure B-13) puis cliquez sur le bouton **Modifier**.

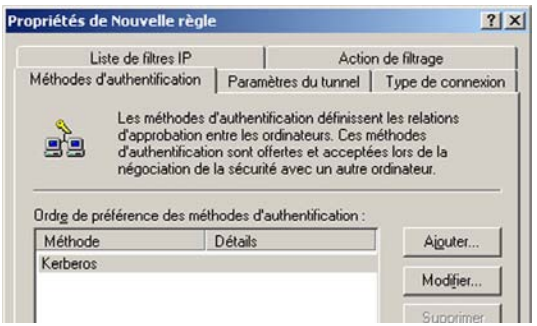


Figure B-13 : Méthodes d'authentification

5. Sélectionnez la méthode d'authentification **Utiliser cette chaîne (clé partagée au préalable)** (figure B-14) et entrez une chaîne de clé partagée, telle que XYZ12345. Cliquez sur le bouton **OK**.

Figure B-14 : Clé pré-partagée

6. Cette nouvelle clé partagée est présentée à la figure B-15. Cliquez sur le bouton **Appliquer** pour continuer si elle s'affiche sur votre écran ; sinon passez à l'étape suivante.

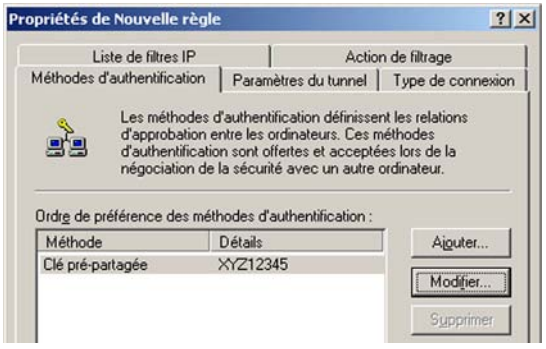


Figure B-15 : Nouvelle clé pré-partagée

7. Sélectionnez l'onglet **Paramètres du tunnel** (figure B-16) et cliquez sur le bouton radio **Le point d'arrêt du tunnel est spécifié par cette adresse IP**. Entrez ensuite l'adresse IP WAN du routeur.

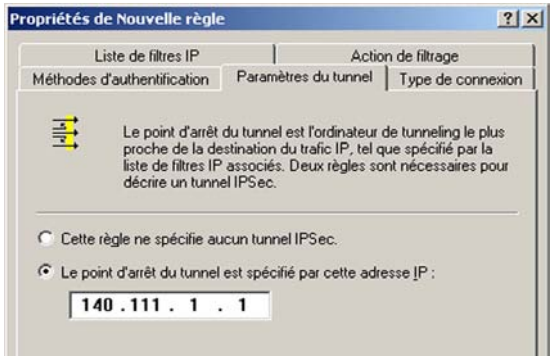


Figure B-16 : Onglet Paramètres du tunnel

8. Sélectionnez l'onglet **Type de connexion** (figure B-17) et cliquez sur **Toutes les connexions réseau**. Cliquez ensuite sur **OK** (Windows XP) ou **Fermer** (Windows 2000) pour terminer cette règle.

Tunnel 2 : Router->win

9. Dans l'écran Propriétés de Nouvelle stratégie de sécurité IP (figure B-18), assurez-vous que « win -> Router » est sélectionné et décochez la case **Utiliser l'Assistant Ajout**. Cliquez ensuite sur **Ajouter** pour créer le second filtre IP.

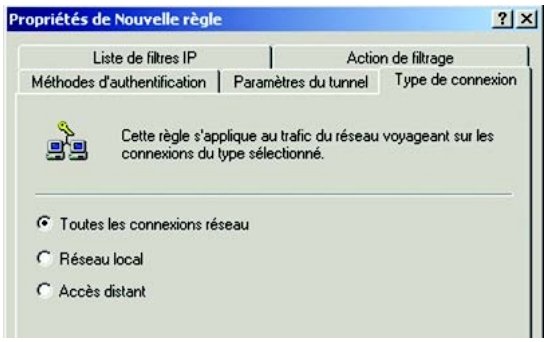


Figure B-17 : Onglet Type de connexion

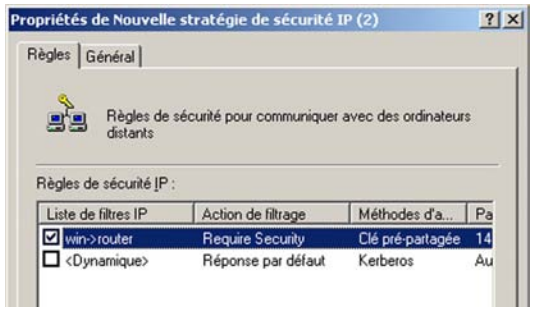


Figure B-18 : Ecran Propriétés

10. Sélectionnez l'onglet **Liste de filtres IP** et cliquez sur la liste de filtres **Router ->win** (figure B-19).

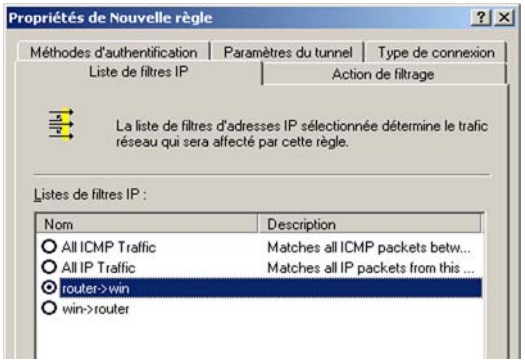


Figure B-19 : Onglet Liste de filtres IP

11. Cliquez sur l'onglet **Action de filtrage** et sélectionnez l'action de filtrage **Sécurité requise** (figure B-20). Cliquez ensuite sur le bouton **Modifier**. Dans l'onglet *Méthodes de sécurité* (figure B-12), assurez-vous que l'option **Négocier la sécurité** est activée. Décochez la case **Accepter les communications non sécurisées, mais toujours répondre en utilisant IPSec**. Sélectionnez **Session de clé principale PFS** puis cliquez sur le bouton **OK**.

Figure B-20 : Onglet Action de filtrage

12. Cliquez sur l'onglet **Méthode d'authentification** et vérifiez que la méthode **Kerberos** est sélectionnée (figure B-21). Cliquez ensuite sur le bouton **Modifier**.

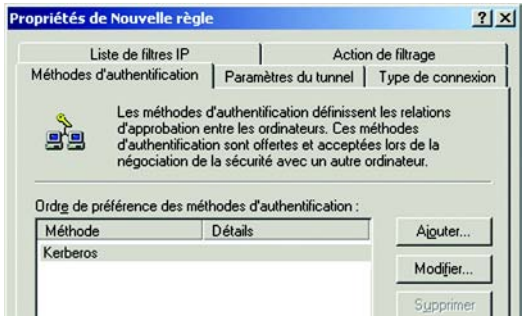


Figure B-21 : Onglet Méthode d'authentification

13. Sélectionnez la méthode d'authentification **Utiliser cette chaîne (clé partagée au préalable)** (figure B-22) et entrez une chaîne de clé partagée, telle que XYZ12345. Il s'agit d'un exemple de chaîne de clé. Votre clé doit être unique et facile à mémoriser. Cliquez sur le bouton **OK**.

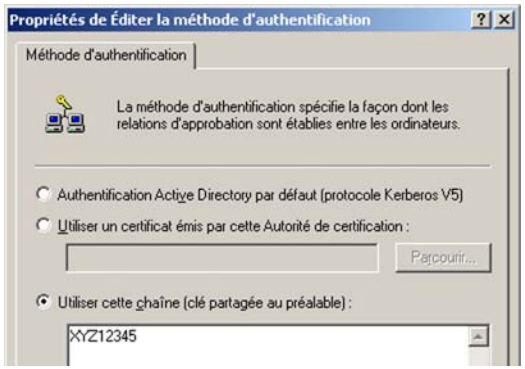


Figure B-22 : Clé pré-partagée

14. Cette nouvelle clé partagée est présentée à la figure B-23. Cliquez sur le bouton **Appliquer** pour continuer si elle s'affiche sur votre écran ; sinon passez à l'étape suivante.

15. Cliquez sur l'onglet **Paramètres du tunnel** (figure B-24), cliquez sur le bouton radio **Le point d'arrêt du tunnel est spécifié par cette adresse IP**. Entrez ensuite l'adresse IP de l'ordinateur Windows 2000/XP.

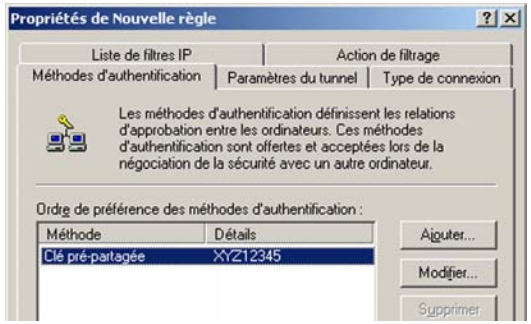


Figure B-23 : Nouvelle clé pré-partagée

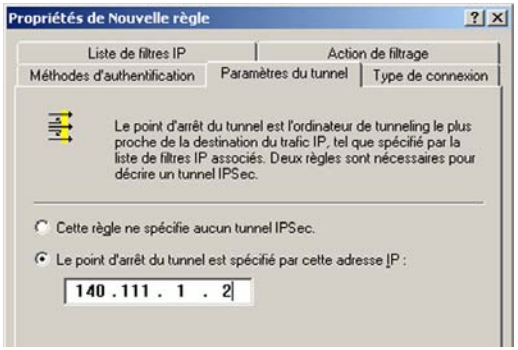


Figure B-24 : Onglet Paramètres du tunnel

16. Sélectionnez l'onglet **Type de connexion** (figure B-25) et cliquez sur **Toutes les connexions réseau**. Cliquez ensuite sur **OK** ou **Fermer** pour terminer.

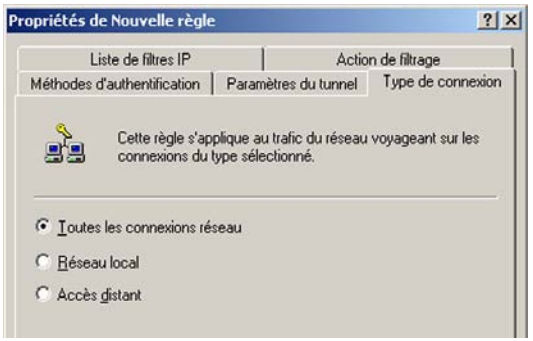


Figure B-25 : Type de connexion

17. Dans l'onglet *Règles* (figure B-26), cliquez sur le bouton **OK** ou **Fermer** pour revenir à l'écran secpol.

Etape 4 : Attribution d'une nouvelle stratégie IPSec

Dans la fenêtre *Stratégies de sécurité IP sur l'ordinateur local* (figure B-27), cliquez à l'aide du bouton droit sur la stratégie *to_Router*, puis cliquez sur **Attribuer**. Une flèche verte apparaît sur l'icône du dossier.

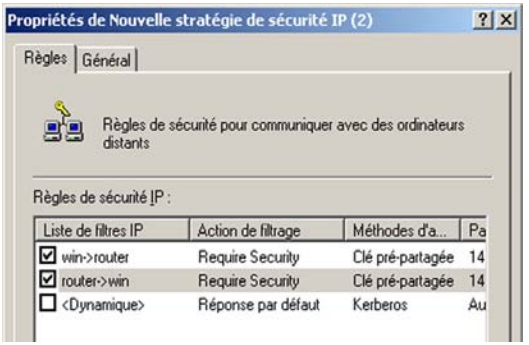


Figure B-26 : Règles

Figure B-27 : Ordinateur local

Etape 5 : Création d'un tunnel à l'aide de l'utilitaire Web

1. Ouvrez votre navigateur Web et entrez **192.168.1.1** dans le champ Address (Adresse). Appuyez sur la touche **Entrée**.
2. Entrez **admin** dans les champs User name (Nom de l'utilisateur) et Password (Mot de passe). Appuyez sur la touche **Entrée**.
3. Dans l'onglet *Setup* (Configuration), cliquez sur l'onglet **VPN**.
4. Dans l'onglet *VPN* (figure B-28), sélectionnez le tunnel que vous souhaitez créer dans la liste déroulante *Select Tunnel Entry* (Sélectionner une entrée de tunnel). Cliquez sur **Enabled** (Activé). Entrez le nom du tunnel dans le champ *Tunnel Name* (Nom du tunnel). Ceci vous permet d'identifier les divers tunnels et il n'est donc pas nécessaire que ce nom corresponde au nom utilisé à l'autre bout du tunnel.
5. Entrez l'adresse IP et le masque de sous-réseau du routeur VPN local dans les champs de la section *Local Secure Group* (Groupe sécurisé local). Pour autoriser l'accès à l'intégralité du sous-réseau IP, entrez 0 pour le dernier ensemble des adresses IP (par exemple, 192.168.1.0).
6. Entrez l'adresse IP et le masque de sous-réseau du périphérique VPN à l'autre extrémité du tunnel (le routeur VPN distant ou le périphérique VPN distant avec laquelle/lequel vous voulez communiquer) dans les champs Remote Security Gateway (Modem routeur de sécurité distante).
7. Sélectionnez l'un des deux types de cryptage : **DES** ou **3DES** (3DES recommandé car garantissant un niveau de protection plus élevé). Vous pouvez sélectionner l'un de ces deux paramètres, mais le même type de cryptage doit être utilisé par le périphérique VPN à l'autre bout du tunnel. Vous pouvez également ne pas souhaiter utiliser de cryptage. Dans ce cas, sélectionnez l'option Disable (Désactiver).
8. Sélectionnez l'un des deux types d'authentification : **MD5** ou **SHA** (SHA étant recommandé car garantissant un niveau de protection plus élevé). Comme pour le cryptage, vous pouvez sélectionner l'un de ces deux paramètres, mais le même type d'authentification doit être utilisé par le périphérique VPN à l'autre bout du tunnel. L'authentification peut également être désactivée des deux côtés du tunnel, à l'aide du paramètre **Disable** (Désactiver).
9. Sélectionnez les paramètres de la section Key Management (Gestion de clé) appropriés. Sélectionnez **Auto (IKE)** et saisissez une suite de chiffres ou de lettres dans le champ *Pre-shared Key* (Clé pré-partagée). Cochez la case correspondant à l'option **PFS** (Perfect Forward Secrecy, Secret de transmission total) pour vous assurer que l'échange de clé et les propositions IKE sont sécurisées. 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. 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 ou laissez ce champ vierge pour que la clé reste valide indéfiniment.
10. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les modifications apportées aux paramètres.

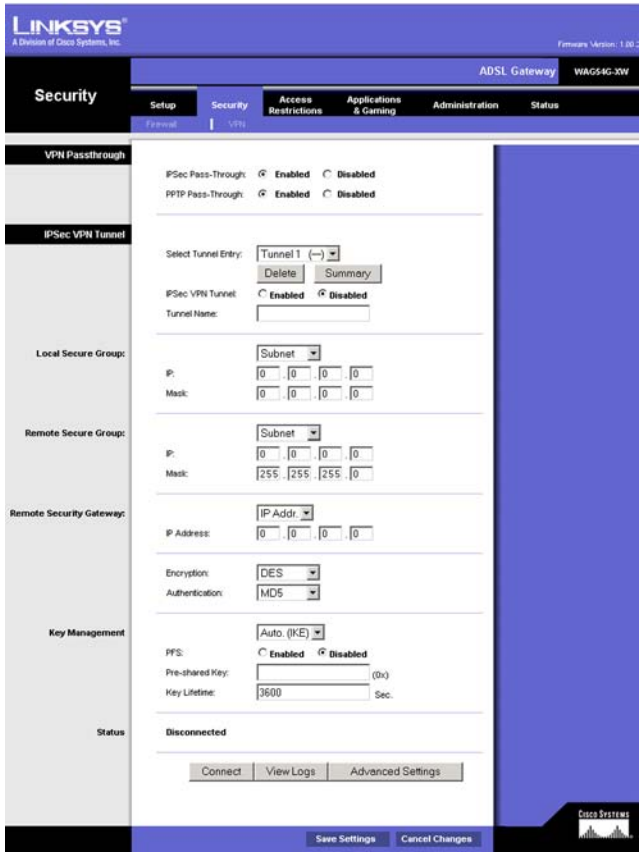


Figure B-28 : Onglet VPN

Votre tunnel est maintenant défini.

Annexe C : Recherche des adresses MAC et IP de votre adaptateur Ethernet

Cette section explique comment rechercher l'adresse MAC de l'adaptateur 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 l'adaptateur 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 l'adaptateur 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*, entrez **winipcfg**. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**.

2. Lorsque l'écran *Configuration IP* apparaît, sélectionnez l'adaptateur Ethernet que vous avez connecté au modem routeur à l'aide d'un câble réseau Ethernet CAT 5. (figure C-1).

3. Notez l'adresse de l'adaptateur qui s'inscrit à l'écran (figure C-2). Il s'agit de l'adresse MAC de votre adaptateur Ethernet. Elle apparaît sous une forme hexadécimale (série de nombres et de lettres).

   L'adresse MAC/adresse de l'adaptateur vous servira pour le filtrage MAC. L'exemple de la figure D-2 indique l'adresse MAC 00-00-00-00-00-00 de l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

   L'exemple de la figure D-2 affiche une adresse IP 192.168.1.100 pour l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

Remarque : L'adresse MAC est également appelée Adresse de l'adaptateur.

Figure C-1 : Ecran Configuration IP

Figure C-2 : Adresse MAC/Adresse de l'adaptateur

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, entrez **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 adaptateur 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. L'exemple de la figure D-3 indique l'adresse MAC 00-00-00-00-00-00. de l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

   L'exemple de la figure C-3 affiche une adresse IP 192.168.1.100 pour l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

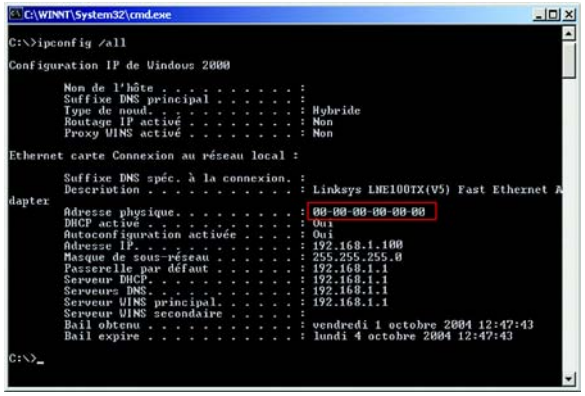


Figure C-3 : Adresse MAC/Adresse Physique

Annexe D : Glossaire

802.11a : norme réseau sans fil IEEE spécifiant un débit de transfert de données maximum de 54 Mbit/s et une fréquence de 5 GHz.

802.11b : norme de mise en réseau sans fil IEEE qui spécifie un débit de transfert de données maximum 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.

Adaptateur : périphérique ajoutant de nouvelles fonctionnalités réseau à votre ordinateur.

Adresse IP dynamique : adresse IP attribuée provisoirement par un serveur DHCP.

Adresse IP statique : adresse fixe attribuée à un ordinateur ou un périphérique connecté à un réseau.

Adresse IP : adresse utilisée pour l'identification d'un ordinateur ou d'un périphérique sur un réseau.

Adresse MAC (Media Access Control) : adresse unique qu'un fabricant attribue à chaque périphérique d'un réseau.

Bande ISM : bande radio utilisée lors de transmissions réseau 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.

Commande Finger : programme indiquant le nom associé à une adresse de messagerie.

Commutateur : 1. Périphérique servant de « noyau » de connexion à des ordinateurs ou d'autres périphériques d'un réseau et permettant le partage de données à haut débit. 2. Périphérique permettant de produire, interrompre ou modifier les connexions au sein d'un circuit électrique.

Cryptage : codage de données pour empêcher qu'elles ne soient lues par des personnes non autorisées.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) : méthode de transfert des données adoptée pour éviter la perte de données sur un réseau.

CTS (Clear To Send) : signal émis par un périphérique pour indiquer qu'il est prêt à recevoir des données.

DDNS (Dynamic Domain Name System) : système permettant de disposer d'un site Web, d'un site FTP ou d'un serveur de messagerie avec une adresse IP dynamique et un nom de domaine fixe.

Débit : quantité de données déplacées avec succès d'un nœud à un autre dans un délai donné.

DHCP (Dynamic Host Configuration Protocol) : protocole permettant à un périphérique sur un réseau local (on parle alors de serveur DHCP) d'attribuer des adresses IP temporaires aux périphériques d'un autre réseau, généralement des ordinateurs.

DNS (Domain Name Server) : 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 (Digital Subscriber Line) : connexion haut débit toujours active par le biais des lignes téléphoniques standard.

DSSS (Direct-Sequence Spread-Spectrum) : type de technologie de transmission radio qui introduit un modèle de bit redondant pour diminuer les risques de perte de données lors d'une transmission. Elle est utilisée dans le cadre de réseaux 802.11b.

DTIM (Delivery Traffic Indication Message) : message intégré aux paquets de données et capable d'accroître l'efficacité des structures sans fil.

Etalement de spectre : technique de fréquence radio à large bande utilisée pour une transmission plus fiable et sécurisée des données.

Ethernet : protocole réseau IEEE standard qui spécifie le mode de placement et d'extraction des données via un support de transmission courant.

Fragmentation : acte de scinder un paquet en unités plus petites lors d'une transmission sur un support réseau inapte à prendre en charge la taille d'origine du paquet.

FTP (File Transfer Protocol) : protocole standard utilisé pour la transmission de fichiers entre des ordinateurs sur un réseau TCP/IP et sur Internet.

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 toujours active.

HTTP (HyperText Transport Protocol) : protocole de communication utilisé pour la connexion à des serveurs sur le World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) : institut indépendant chargé du développement des normes réseau standard.

Infrastructure : équipement informatique et réseau actuellement installé.

Initialiser : démarrer un périphérique et lui demander d'exécuter des instructions.

Intervalle de transmission de balise : intervalle de fréquence de la balise, c'est-à-dire un paquet diffusé par un modem routeur en vue de synchroniser un réseau sans fil.

IP (Internet Protocol) : 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 (Internet Protocol Security) : 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 (réseau local) : ordinateurs et produits composant le réseau que vous installez chez vous ou dans vos locaux professionnels.

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 d'autres périphériques liés aux technologies de l'information.

Mbit/s (mégabits par seconde) : soit un million de bits par seconde ; unité de mesure de transmission des données.

Micrologiciel : 1. Programme destiné à exécuter un périphérique réseau. 2. Il est chargé dans la mémoire morte (ROM) ou la mémoire morte programmable (PROM) et ne peut être modifié par aucun utilisateur final.

Mise à niveau : acte de remplacer un logiciel ou micrologiciel existant par une nouvelle version.

Mode d'infrastructure : configuration dans laquelle un réseau sans fil est relié à un réseau câblé par l'intermédiaire d'un point d'accès.

Modem câble : périphérique qui relie un ordinateur au réseau de télévision câblé, ce réseau permettant à son tour de se connecter à Internet.

Modem routeur par défaut : périphérique utilisé pour transférer un trafic de données Internet depuis votre réseau local.

Modem routeur : système permettant de relier entre eux des réseaux.

Multidiffusion : envoi simultané de données à un groupe de destinataires.

NAT (Network Address Translation) : la technologie NAT permet de convertir les adresses IP d'un réseau local en une adresse IP distincte sur Internet.

Navigateur : application offrant un mode d'affichage et de manipulation des informations sur le World Wide Web.

NNTP (Network News Transfer Protocol) : protocole utilisé pour connecter des groupes Usenet sur Internet.

Nœud : liaison ou point de connexion réseau (généralement, un ordinateur ou une station de travail).

OFDM (Orthogonal Frequency Division Multiplexing) : type de technologie de modulation qui permet de séparer le flux de données en un nombre donné de flux de données à moindre débit, transmis ensuite en parallèle. Cette technologie est utilisée dans le cadre de réseaux 802.11a, 802.11g et PowerLine.

Paquet : unité de données transmises sur un réseau.

Pare-feu : mesures de sécurité protégeant les ressources d'un réseau local contre toute intrusion.

Phrase mot de passe : utilisée comme un mot de passe, une phrase mot de passe simplifie le processus de cryptage WEP en générant automatiquement les clés de cryptage WEP des produits Linksys.

Ping (Packet INternet Groper) : utilitaire Internet utilisé pour déterminer si une adresse IP particulière est en ligne.

Point à point : groupe de périphériques sans fil communiquant directement entre eux (point à point) sans l'intervention d'un point d'accès.

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 entre eux deux différents types de réseau local (par exemple, un réseau sans fil à un réseau câblé Ethernet).

POP3 (Post Office Protocol 3) : protocole standard utilisé pour extraire des messages électroniques stockés sur un serveur de messagerie.

Port - 1. Port de connexion d'un ordinateur ou d'un périphérique réseau utilisé pour raccorder un câble ou une carte. 2. Point de connexion virtuelle via lequel un ordinateur exploite une application spécifique sur un serveur.

PPPoE (Point to Point Protocol over Ethernet, protocole de point à point sur Ethernet) : type de connexion haut débit qui permet l'authentification (nom d'utilisateur et mot de passe) et l'acheminement des données.

PPTP (Point-to-Point Tunneling Protocol, protocole tunnel point à point) : 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.

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.

Réseau : plusieurs ordinateurs ou 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.

RJ-45 (Registered Jack-45) : connecteur Ethernet pouvant accueillir jusqu'à huit broches.

Routage statique : transfert de données sur un réseau par une voie fixe.

Routeur : périphérique de mise en réseau qui relie entre eux plusieurs ordinateurs (réseau local, Internet).

RTS (Request To Send) : paquet transmis lorsqu'un ordinateur dispose de données qu'il doit transmettre. L'ordinateur attend l'arrivée d'un message CTS (Clear To Send) avant de transmettre les données.

Semi-duplex : transmission de données pouvant survenir dans deux directions sur une ligne unique, mais une direction 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 (Simple Mail Transfer Protocol) : protocole de messagerie standard utilisé sur Internet.

SNMP (Simple Network Management Protocol) : protocole très répandu de contrôle et d'administration de réseau.

SSID (Service Set IDentifier) : nom de votre réseau sans fil.

Tampon : bloc de mémoire qui stocke provisoirement des données à manipuler ultérieurement lorsqu'un périphérique trop encombré ne peut accueillir ces données.

TCP/IP (Transmission Control Protocol/Internet Protocol) : protocole réseau de transmission de données exigeant la validation de la personne à qui elles sont destinées.

Téléchargement (réception) : réception d'un fichier transmis par l'intermédiaire d'un réseau.

Téléchargement (réception) : réception d'un fichier transmis par l'intermédiaire d'un réseau.

Telnet : commande utilisateur et protocole TCP/IP utilisés pour l'accès à des ordinateurs distants.

TFTP (Trivial File Transfer Protocol) : version du protocole FTP TCP/IP qui utilise le protocole UDP et n'offre aucune fonction de répertoire ou de mot de passe.

Topologie : configuration physique d'un réseau.

UDP (User Datagram Protocol) : protocole réseau de transmission de données n'exigeant aucune validation de la personne à qui elles sont destinées.

URL (Uniform Resource Locator) : adresse d'un fichier situé sur Internet.

Vitesse de transmission : taux de transmission.

VPN (Virtual Private Network) : mesure de sécurité visant à protéger des données lorsqu'elles quittent un réseau et s'acheminent vers un réseau différent via Internet.

WAN (Wide Area Network) : Internet.

WEP (Wired Equivalent Privacy) : méthode permettant de crypter des données transmises sur un réseau sans fil pour une sécurité accrue.

WINIPCFG : utilitaire Windows 98 et Windows Millennium qui affiche l'adresse IP d'un périphérique réseau spécifique.

WLAN (Wireless Local Area Network) : groupe d'ordinateurs et de périphériques associés qui communiquent entre eux sans fil.

Zone DMZ (zone démilitarisée) : élément qui supprime la protection pare-feu du modem routeur sur un ordinateur et permet ainsi à ce dernier d'être visible sur Internet.

Annexe E : Mise à niveau du micrologiciel

Vous pouvez mettre à niveau le micrologiciel côté LAN (réseau) du modem routeur depuis la section Firmware Upgrade (Mise à niveau du micrologiciel) de l'onglet Administration de l'utilitaire Web. Pour cela, procédez comme suit.

Upgrade from LAN (Mise à niveau à partir du réseau LAN)

Pour mettre à niveau le micrologiciel du modem routeur à partir du réseau LAN :

1. Cliquez sur le bouton **Browse** (Parcourir) pour rechercher le fichier de mise à niveau du micrologiciel que vous avez téléchargé à partir du site Web de Linksys puis décompressé.

2. Cliquez deux fois sur le fichier du micrologiciel que vous venez de télécharger et de décompresser. Cliquez sur le bouton **Upgrade** (Mettre à niveau) et suivez les instructions à l'écran.

Figure E-1 : Firmware Upgrade (Mise à niveau du micrologiciel)

Annexe F : Spécifications

Normes	IEEE 802,3u, IEEE 802.3, G.992,1 (G.dmt), G.992,2 (G.lite), ITU G.992.3, ITU G.992.5, ANSI T1.413i2, AG241-E1: Annex-B, AG241-DE: UR-2
Ports	Alimentation, LINE (LIGNE) (ADSL), Ethernet (1-4)
Boutons	Un bouton Reset (Réinitialisation), un commutateur On/Off (Marche/Arrêt)
Type de câble	UTP CAT 5 ou supérieur, Câble téléphonique (POTS)
Voyants	Alimentation, Ethernet (1-4), DSL, Internet
Dimensions	186 mm x 48 mm x 154 mm
Poids	0,36 kg
Alimentation	Externe, 12 VCC, 1 A
Certifications	FCC Part 15B Class B, FCC Part 68, UL 1950, CE
Température de fonctionnement	0 à 40º C
Température de stockage	-20 à 70º C
Humidité en fonctionnement	10 à 85 %, non condensée
Humidité de stockage	5 à 90 %, non condensée

Annexe G : Réglementation

DECLARATION 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 hautes fréquences nuisible 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 lors de la réception radio ou télévision, détectables en mettant l'équipement hors tension puis sous tension, l'utilisateur peut tenter de remédier à ces interférences en effectuant les opérations 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 un technicien radio/télévision expérimenté

INDUSTRIE CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

DECLARATION DE CONFORMITE UE (EUROPE)

Conformément aux directives 89/336/EEC sur la compatibilité électromagnétique, 73/23/EEC sur les basses tensions et 93/68/EEC sur les modifications, ce produit satisfait aux exigences des normes suivantes :

- Norme EN55022 sur les émissions
- Norme EN55024 sur l'immunité

Annexe H : Informations de garantie

Linksys garantit que vos produits Linksys seront, pour l'essentiel, exempts de vices matériels et de fabrication, sous réserve d'une utilisation normale, pendant une période de deux années consécutives (« Période de garantie »). Votre unique recours et l'entière responsabilité de Linksys seront 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. TOUTE 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 DEMENTIES. Certaines juridictions n'autorisent pas les restrictions relatives à la durée d'une garantie implicite. Par conséquent, la restriction susmentionnée peut ne pas s'appliquer dans votre cas. 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 DE LA THEORIE SUR LES RESPONSABILITES, LINKSYS NE POURRA EN AUCUN CAS ETRE TENU RESPONSABLE DES PERTES DE DONNEES, DE REVENUS OU DE BENEFICES OU DES DOMMAGES SPECIAUX, INDIRECTS, CONSECUTIFS, ACCIDENTELS OU DISSUASIFS (Y COMPRIS LES ACTES DE NEGLIGENCE) 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'appliqueront 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 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-nous un courrier électronique et envoyez-le au service Support technique du pays où vous résidez :

Europe	Adresse électronique
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 électronique
Amérique Latine	support.la@linksys.com
Etats-Unis et Canada	support@linksys.com

LINKSYS®

A Division of Cisco Systems, Inc.

ADSL-Gateway

mit 4-Port-Switch

Benutzerhandbuch

VERDRAHTET

Modell-Nr. **AG241**

CISCO SYSTEMS

Copyright und Marken

Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum ADSL-Gateway mit 4-Port-Switch ist es, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. "Beachten Sie folgende Symbole:"

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".

Table of Contents

Kapitel 1: Einführung 1
Willkommen 1
Der Inhalt dieses Handbuchs 2
Kapitel 2: Planen Ihres Netzwerks 4
Die Funktionen des Gateways 4
IP-Adressen 4
Was ist ein VPN? 5
Wozu benötige ich ein VPN? 7
Kapitel 3: Beschreibung des ADSL-Gateways mit 4-Port-Switch 9
Rückseite 9
Vorderseite 10
Kapitel 4: Anschließen des ADSL-Gateways mit 4-Port-Switch 11
Übersicht 11
Verbindung mit einem Computer 11
Kapitel 5: Konfigurieren des Gateways 13
Übersicht 13
Hinweis für den Zugriff auf das webbasierte Dienstprogramm 15
Registerkarte Einrichtung 15
Registerkarte Sicherheit 24
Registerkarte Zugriffsbeschränkungen 30
Registerkarte Anwendungen und Spiele 32
Registerkarte Verwaltung 36
Registerkarte 40
Anhang A: Fehlerbehebung 42
Behebung häufig auftretender Probleme 42
Häufig gestellte Fragen 52
Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem Gateway 56
Einführung 56
Umgebung 56
Hinweise zum Einrichten eines sicheren IPSec-Tunnels 57
Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters 67
Anweisungen für Windows 98/ME 67

Anweisungen für Windows 2000/XP 68
Anhang D: Glossar 69
Anhang E: Aktualisieren der Firmware 76
Anhang F: Spezifikationen 77
Anhang G: Zulassungsinformationen 78
Anhang H: Garantieinformationen 79
Anhang I: Kontaktinformationen 80

List of Figures

Figure 2-1: Netzwerk 4
Figure 2-2: Computer - VPN-Gateway 6
Figure 2-3: VPN-Gateway - VPN-Gateway 7
Figure 3-1: Rückseite 9
Figure 3-2: Vorderseite 10
Figure 4-1: Ethernet-Verbindung 11
Figure 4-2: ADSL-Verbindung 11
Figure 4-3: Netzstromverbindung 12
Figure 5-1: Fenster für die Passworteingabe 15
Figure 5-2: Registerkarte Grundlegende Einrichtung 15
Figure 5-3: Dynamische IP-Adresse 16
Figure 5-4: Statische IP-Adresse 16
Figure 5-5: IPoA 17
Figure 5-6: RFC 2516 PPPoE 17
Figure 5-7: RFC 2364 PPPoA 18
Figure 5-8: Nur Überbrückungsmodus 18
Figure 5-9: Optionale Einstellungen 19
Figure 5-10: DynDNS.org 21
Figure 5-11: TZO.com 21
Figure 5-12: Erweitertes Routing 22
Figure 5-13: Erweiterte Wireless-Einstellungen 23
Figure 5-14: Firewall 24
Figure 5-15: VPN 25
Figure 5-16: Zusammenfassung der VPN-Einstellungen 25
Figure 5-17: Manuelle Schlüsselverwaltung 27
Figure 5-18: Systemprotokoll 27
Figure 5-19: Erweiterte IPSec VPN-Tunnel-Einrichtung 28
Figure 5-20: Internetzugriff 30

Figure 5-21: Internet-Richtlinien - Zusammenfassung 30
Figure 5-22: PC-Liste 31
Figure 5-23: Anschlussdienste 31
Figure 5-24: Einfaches Port-Forwarding 32
Figure 5-25: Weiterleitung an einen Anschlussbereich 32
Figure 5-26: Port-Triggering 33
Figure 5-27: DMZ 33
Figure 5-28: QOS 34
Figure 5-29: Verwaltungsfunktionen 36
Figure 5-30: Berichtaufzeichnung 37
Figure 5-31: Systemprotokoll 37
Figure 5-32: Ping-Test 38
Figure 5-33: Sichern & Wiederherstellen 38
Figure 5-34: Werkseinstellungen 39
Figure 5-35: Firmware aktualisieren 39
Figure 5-36: Neustart 39
Figure 5-37: Status 40
Figure 5-38: Lokales Netzwerk 40
Figure 5-39: DHCP-Client-Tabelle 41
Figure 5-40: DSL-Verbindung 41
Figure B-1: Fenster "Lokale Sicherheitseinstellungen" 57
Figure B-2: Registerkarte "Regeln" 57
Figure B-3: Registerkarte "IP-Filterliste" 57
Figure B-4: Dialogfeld "IP-Filterliste" 58
Figure B-5: Dialogfeld "Eigenschaften von Filter" 58
Figure B-6: Dialogfeld "Eigenschaften von Neue Regel" 58
Figure B-7: Dialogfeld "IP-Filterliste" 59
Figure B-8: Dialogfeld "Eigenschaften von Filter" 59
Figure B-9: Dialogfeld "Eigenschaften von Neue Regel" 59
Figure B-10: Registerkarte "IP-Filterliste" 60

Figure B-11: Registerkarte "Filteraktion" 60
Figure B-12: Registerkarte "Sicherheitsmethoden" 60
Figure B-13: Registerkarte "Authentifizierungsmethoden" 61
Figure B-14: Vorinstallierter Schlüssel 61
Figure B-15: Neuer vorinstallierter Schlüssel 61
Figure B-16: Registerkarte "Tunneleinstellungen" 62
Figure B-17: Registerkarte "Verbindungstyp" 62
Figure B-18: Fenster für die Eigenschaften der neuen Richtlinie 62
Figure B-19: Registerkarte "IP-Filterliste" 63
Figure B-20: Registerkarte "Filteraktion" 63
Figure B-21: Registerkarte "Authentifizierungsmethode" 63
Figure B-22: Vorinstallierter Schlüssel 64
Figure B-23: Neuer vorinstallierter Schlüssel 64
Figure B-24: Registerkarte "Tunneleinstellungen" 64
Figure B-25: Registerkarte "Verbindungstyp" 65
Figure B-26: Registerkarte "Regeln" 65
Figure B-27: Dialogfeld "Lokale Sicherheitseinstellungen" 65
Figure B-28: Registerkarte "VPN" 66
Figure C-1: Fenster IP-Konfiguration 67
Figure C-2: MAC-Adresse/Adapteradresse 67
Figure C-3: MAC-Adresse/physikalische Adresse 68
Figure E-1: Firmware aktualisieren 76

Kapitel 1: Einführung

Willkommen

Das Linksys ADSL-Gateway mit 4-Port-Switch ist die kompakte Internetverbindungslösung für zu Hause. Die ADSL-Modemfunktion ermöglicht eine extrem schnelle Internetverbindung, die um einiges schneller ist als Einwählverbindungen - ganz ohne Beanspruchen der Telefonleitung.

Schließen Sie Ihre Computer über den integrierten 10/100 Ethernet-Switch mit 4 Ports zum schnellen Hochfahren Ihres Netzwerks an das Gateway an. Sie können Dateien, Drucker, Festplattenspeicher und andere Ressourcen gemeinsam verwenden oder per Computerspiele gegen Spielegegner antreten. Verbinden Sie vier Computer direkt miteinander, oder hängen Sie weitere Hubs und Switches an, um die Größe des Netzwerks Ihren Bedürfnissen gemäß zu gestalten. In diesem Gateway werden all diese Vorteile vereinigt, sodass das gesamte Netzwerk von der High Speed-Internetverbindung profitieren kann.

Zum Schutz Ihrer Daten und Privatsphäre verfügt das ADSL-Gateway mit 4-Port-Switch über eine erweiterte Firewall, mit der Eindringlinge und Angriffe über das Internet abgewehrt werden. Wireless-Datenübertragungen können durch leistungsstarke Datenverschlüsselung geschützt werden. Schützen Sie Ihre Familie mit Kinderschutzfunktionen wie die Beschränkung von Internetzugriffszeiten und dem Blockieren von Schlüsselwörtern. Die Konfiguration ist mit jedem beliebigen Web-Browser kinderleicht.

Mit dem Linksys ADSL-Gateway mit 4-Port-Switch im Zentrum Ihres Netzwerks sind Sie auf dem besten Weg in die Zukunft.

Der Inhalt dieses Handbuchs

In diesem Benutzerhandbuch sind die zur Einrichtung und Verwendung des ADSL-Gateways mit 4-Port-Switch erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden das ADSL-Gateway mit 4-Port Switch, die Anwendungen und das vorliegende Benutzerhandbuch beschrieben.

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

- Kapitel 3: Beschreibung des ADSL-Gateways mit 4-Port-Switch
  In diesem Kapitel werden die physischen Funktionen des Gateways beschrieben.

- Kapitel 4: Anschließen des ADSL-Gateways mit 4-Port-Switch
  In diesem Kapitel finden Sie Anweisungen zum Verbinden des Gateways mit dem Netzwerk.

- Kapitel 5: Konfigurieren des Gateways
  In diesem Kapitel wird erläutert, wie Sie die Einstellungen des Gateways mithilfe des webbasierten Dienstprogramms konfigurieren.

- Anhang A: Fehlerbehebung
  In diesem Anhang werden Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des ADSL-Gateways mit 4-Port-Switch erörtert.

- Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem Gateway
  In diesem Anhang finden Sie Anleitungen dazu, wie Sie über vorläufige gemeinsame Schlüssel einen sicheren IPSec-Tunnel einrichten, um ein privates Netzwerk innerhalb des VPN-Gateways mit einem Windows 2000- oder Windows XP-Computer zu verbinden.

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

- Anhang D: 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 Ihres Computers ermitteln, um die MAC-Filterung bzw. die Gateway-Funktion zum Kopieren von MAC-Adressen verwenden zu können.

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

- Anhang F: Zulassungsinformationen
  In diesem Anhang sind die für das Gateway geltenden Zulassungsinformationen aufgeführt.

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

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

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

Kapitel 2: Planen Ihres Netzwerks

Die Funktionen des Gateways

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

In diesem Fall verbindet das Gateway Ihr lokales 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 Ihr Computernetzwerk geschützt, sodass Ihre Computer für andere Benutzer im Internet nicht "sichtbar" sind. Somit wird der private Charakter Ihres Netzwerks bewahrt. Das Gateway schützt Ihr 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 Internetanschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, sofern zulässig, das jeweilige Paket an den entsprechenden Computer im LAN weiter.

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

Abbildung 2-1: Netzwerk

***LAN**: Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr lokales Netzwerk zusammensetzt.*

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, Ihren Netzwerkgeräten eine IP-Adresse zuzuweisen. Sie können statische IP-Adressen oder mithilfe des Gateways dynamische IP-Adressen zuweisen.

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, wie z. B. Server-Computern oder Druckservern, verwendet.

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 Benutzerhandbuch 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, sodass Gateway und Netzwerk unsichtbar für das Internet sind; weitere Informationen hierzu finden Sie in "Kapitel 5: Konfigurieren des Gateways" unter "Sicherheit" in der Beschreibung zum Blockieren von WAN-Anfragen.

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, wie 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, wie z. B. das Gateway, fungieren. Die DHCP-Serverfunktion des Gateways ist standardmäßig aktiviert.

Wenn in Ihrem Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der beiden DHCP-Server deaktivieren. Wenn mehr als ein DHCP-Server in Ihrem Netzwerk ausgeführt werden, treten Netzwerkfehler, wie z. B. IP-Adresskonflikte, auf. Informationen zum Deaktivieren der DHCP-Funktion beim Gateway erhalten Sie in "Kapitel 5: Konfigurieren des Gateways".

Was ist ein VPN?

Ein VPN (*Virtual Private Network*) ist eine Verbindung zwischen zwei Endpunkten (z. B. ein VPN-Gateway) in verschiedenen Netzwerken, mit deren Hilfe private Daten sicher über ein gemeinsam genutztes oder öffentliches Netzwerk, wie z. B. das Internet, gesendet werden können. Dadurch wird ein privates Netzwerk aufgebaut, über das Daten sicher zwischen diesen beiden Standorten bzw. Netzwerken gesendet werden können.

Dies geschieht mithilfe eines "Tunnels". Die beiden Computer oder Netzwerke werden über einen VPN-Tunnel verbunden, durch den Daten über das Internet so übertragen werden können, als ob die Übertragung innerhalb dieser beiden Netzwerke ausgeführt würde. Dabei handelt es sich nicht um einen tatsächlichen Tunnel, sondern um eine Verbindung, die durch die Verschlüsselung der zwischen den Netzwerken gesendeten Daten gesichert wird.

VPN wurde als kostengünstige Alternative zu einer privaten, speziellen, gemieteten Leitung für ein privates Netzwerk entwickelt. Mit Verschlüsselungs- und Authentifizierungstechnologie, die den Industriestandards

entspricht (IPSec, Kurzform für *IP Security*, IP-Sicherheit), stellt das VPN eine sichere Verbindung her, die praktisch genauso funktioniert, als ob Sie direkt mit Ihrem lokalen Netzwerk verbunden wären. VPNs können zum Aufbau sicherer Netzwerke verwendet werden, durch die ein Zentralbüro mit Zweigniederlassungen, Telearbeitern und/oder Mitarbeitern im Außendienst verbunden werden kann (Reisende können eine Verbindung zu einem VPN-Gateway von jedem beliebigen Computer mit VPN-Client-Software, die IPSec, wie z. B. SSH Sentinel, unterstützt, herstellen).

Es gibt zwei grundlegende Möglichkeiten, eine VPN-Verbindung herzustellen:

- VPN-Gateway - VPN-Gateway
- Computer (mit VPN-Client-Software, die IPSec unterstützt) - VPN-Gateway

Das VPN-Gateway erstellt einen "Tunnel" bzw. Kanal zwischen zwei Endpunkten, sodass die Datenübertragungen dazwischen sicher sind. Ein Computer mit VPN-Client-Software, die IPSec unterstützt, kann als einer der beiden Endpunkte verwendet werden. Das VPN-Gateway kann von jedem beliebigen Computer mit integriertem IPSec Security Manager (Microsoft 2000 und XP) einen VPN-Tunnel mithilfe von IPSec herstellen (weitere Informationen finden Sie in "Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem VPN-Gateway". Für andere Betriebssystemversionen von Microsoft müssen zusätzliche VPN-Client-Softwareanwendungen von Drittanbietern installiert werden, die IPSec unterstützen.

Computer (mit VPN-Client-Software, die IPSec unterstützt) - VPN-Gateway

Im folgenden Beispiel wird ein VPN zwischen einem Computer und einem VPN-Gateway beschrieben (siehe Abb. 2-2). Eine Geschäftsfrau auf Dienstreise stellt in ihrem Hotelzimmer eine Verbindung mit ihrem ISP her. Auf ihrem Notebook-Computer ist VPN-Client-Software installiert, die mit den VPN-Einstellungen ihres Büros konfiguriert ist. Sie ruft die VPN-Client-Software auf, die IPSec unterstützt, und stellt eine Verbindung zum VPN-Gateway im Zentralbüro her. Da VPNs das Internet verwenden, spielt die Entfernung keine Rolle. Über das VPN verfügt die Geschäftsfrau nun über eine ebenso sichere Verbindung zum Netzwerk des Zentralbüros, als ob sie physisch damit verbunden wäre.

VPN-Gateway - VPN-Gateway

Ein Beispiel für ein VPN zwischen zwei VPN-Gateways kann folgendermaßen beschrieben werden (siehe Abb. 2-3). Ein Telearbeiter verwendet sein VPN-Gateway zu Hause für seine stets aktive Internetverbindung. Sein Gateway ist mit den VPN-Einstellungen seines Büros konfiguriert. Wenn er eine Verbindung zum Gateway seines Büros herstellt, erstellen die zwei Gateways einen Tunnel, indem Sie die Daten ver- und entschlüsseln. Da VPNs das Internet verwenden, spielt die Entfernung keine Rolle. Über das VPN verfügt der Telearbeiter nun über eine ebenso sichere Verbindung zum Netzwerk des Zentralbüros, als ob er physisch damit verbunden wäre.

Zusätzliche Informationen und Anweisungen zum Erstellen Ihres eigenen VPNs finden Sie auf der internationalen Website von Linksys unter www.linksys.com/international oder in "Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem VPN-Gateway".

Abbildung 2-2: Computer - VPN-Gateway

WICHTIG: Sie müssen mindestens ein VPN Gateway an ein Ende des VPN-Tunnels schalten. Am anderen Ende des VPN-Tunnels muss sich ein anderes VPN-Gateway oder ein Computer mit sd VPN-Client-Software befinden, die IPSec unterstützt.

Wozu benötige ich ein VPN?

Ein Computernetzwerk bietet hochgradige Flexibilität, die bei einem auf Papier basierenden Schriftverkehr nicht gegeben ist. Mit dieser Flexibilität geht jedoch auch ein erhöhtes Sicherheitsrisiko einher. Aus diesem Grund wurden Firewalls entwickelt. Mit Firewalls werden Daten innerhalb eines lokalen Netzwerks geschützt. Aber wie wird dieser Schutz gewährleistet, sobald Informationen an ein Ziel außerhalb Ihres lokalen Netzwerks gesendet werden, wenn E-Mails gesendet werden, oder wenn Sie eine Verbindung zum Netzwerk Ihres Unternehmens herstellen müssen, während Sie unterwegs sind? Wie werden Ihre Daten geschützt?

Hier kann sich ein VPN als nützlich erweisen. VPNs sichern die Daten, die an ein Ziel außerhalb Ihres Netzwerks gesendet werden, so als ob sie sich immer noch innerhalb des Netzwerks befänden.

Wenn von Ihrem Computer Daten über das Internet gesendet werden, sind sie stets Angriffen ausgesetzt. Möglicherweise verfügen Sie bereits über eine Firewall, mit der die Daten, die verschoben oder an Ziele innerhalb Ihres Netzwerks gesendet werden, vor Angriffen und Beschädigungen von Einheiten außerhalb Ihres Netzwerks geschützt werden. Sobald jedoch Daten an Ziele außerhalb Ihres Netzwerks gesendet werden, d. h. wenn Sie Daten per E-Mail versenden oder mit jemandem über das Internet kommunizieren, werden die Daten nicht mehr durch die Firewall geschützt.

Ihre Daten sind nun Hackern ausgesetzt, die mit einer Reihe von Methoden nicht nur die übertragenen Daten, sondern auch Ihre Netzwerkanmelde- und Sicherheitsdaten stehlen können. Dies sind einige der gängigsten Methoden:

1) MAC-Adressen-Spoofing

Paketen, die über ein Netzwerk, entweder Ihr lokales Netzwerk oder das Internet, übertragen werden, wird eine Paket-Kopfzeile vorangestellt. Diese Paket-Kopfzeilen enthalten sowohl Quell- als auch Zielinformationen, damit das Paket zügig übertragen wird. Ein Hacker kann diese Informationen zum Spoofing (Fälschen) einer auf dem Netzwerk zugelassenen MAC-Adresse verwenden. Mit dieser gefälschten MAC-Adresse kann der Hacker außerdem Informationen für einen anderen Benutzer abfangen.

2) Daten-Sniffing

"Daten-Sniffing" bezeichnet eine Methode, die von Hackern zum Abrufen von Netzwerkdaten verwendet wird, wenn die Daten sich in unsicheren Netzwerken, wie z. B. dem Internet, befinden. Werkzeuge für diese Aktivitäten, wie z. B. Programme zur Protokollanalyse und Netzwerkdiagnose, sind in vielen Fällen im Betriebssystem integriert und ermöglichen die Anzeige der Daten im Textformat.

3) Man-in-the-Middle-Angriffe

Sobald der Hacker entweder durch Spoofing oder Sniffing genug Informationen gesammelt hat, kann er einen "Man-in-the-Middle-Angriff" starten. Dieser Angriff wirkt sich so aus, dass Daten, die von einem Netzwerk an ein anderes Netzwerk übertragen werden, an ein neues Ziel umgeleitet werden. Obwohl die Daten von dem vorgesehenen Empfänger nicht empfangen werden, wird dem Absender genau dies angezeigt.

Dies sind nur einige der von Hackern verwendeten Methoden, und es werden stets neue Methoden entwickelt. Ohne die Sicherheit Ihres VPNs sind Ihre Daten ständig solchen Angriffen ausgesetzt, wenn sie über das Internet

Abbildung 2-3: VPN-Gateway - VPN-Gateway

übertragen werden. Daten, die über das Internet übertragen werden, durchlaufen oftmals viele verschiedene Server in aller Welt, bevor Sie ihr Ziel erreichen. Für nicht geschützte Daten ist dies ein langer Weg; hier erfüllt jedoch ein VPN seinen Zweck.

Kapitel 3: Beschreibung des ADSL-Gateways mit 4-Port-Switch

Rückseite

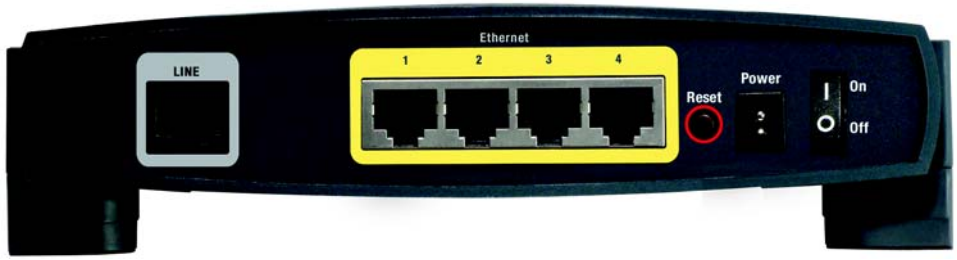


Abbildung 3-1: Rückseite

Die Ports des Gateways für den Anschluss eines Netzwerkkabels befinden sich auf der Rückseite des Geräts. Die Tasten des Gateways befinden sich ebenfalls auf der Rückseite.

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

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

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

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

On/Off (Ein/Aus) Mit diesem Schalter wird das Gateway ein- und ausgeschaltet.

Mit diesen Produkten, wie mit vielen weiteren Linksys Produkten auch, stehen Ihnen grenzenlose Netzwerkbetriebsoptionen offen. Weitere Informationen dazu, welche Produkte mit dem Gateway verwendet werden können, finden Sie auf der internationalen Website von Linksys unter www.linksys.com/international.

Wichtig: Durch das Zurücksetzen des Gateways auf die Werkseinstellungen werden alle Einstellungen (WEP-Verschlüsselung, Wireless- und LAN-Einstellungen usw.) gelöscht und durch die Werkseinstellungen ersetzt. Wenn Sie diese Einstellungen beibehalten möchten, sollten Sie das Gateway nicht zurücksetzen.

Vorderseite

Die LEDs des Gateways, mit denen Informationen zur Netzwerkaktivität angezeigt werden, befinden sich auf der Vorderseite.

Abbildung 3-2: Vorderseite

Power (Netzstrom) Grün. Die Netzstrom-LED leuchtet auf, wenn das Gateway eingeschaltet wird.

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

DSL Grün. Die **DSL-**LED leuchtet bei jeder erfolgreichen DSL-Verbindung auf. Die LED blinkt, während die ADSL-Verbindung hergestellt wird.

Internet Grün. Die **Internet**-LED leuchtet grün auf, wenn eine Internetverbindung zur Sitzung des Internetdienstanbieters (ISP) hergestellt wurde. Die **Internet**-LED leuchtet rot auf, wenn die Verbindung zum ISP fehlgeschlagen ist.

Kapitel 4: Anschließen des ADSL-Gateways mit 4-Port-Switch

Übersicht

Die Einrichtung des Gateways umfasst mehr als das bloße Anschließen der Hardware. Sie müssen Ihre vernetzten Computer so konfigurieren, dass sie die vom Gateway zugewiesenen IP-Adressen annehmen (falls zutreffend); darüber hinaus müssen Sie das Gateway mithilfe von Einstellungen konfigurieren, die Sie von Ihrem ISP (*Internet Service Provider*) erhalten.

Sie haben möglicherweise nach der Installation Ihrer Breitbandverbindung die Informationen zur Einrichtung Ihres Modems vom Installationstechniker Ihres ISP erhalten. 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 der Einrichtung des Gateways beginnen.

Verbindung mit einem Computer

1. Bevor Sie beginnen, stellen Sie sicher, dass all Ihre Hardwaregeräte, einschließlich des Gateways und der Computer, ausgeschaltet sind.
2. Schließen Sie ein Ende des Ethernet-Netzwerkkabels an einen der Ethernet-Ports (mit 1 bis 4 beschriftet) auf der Rückseite des Gateways (siehe Abb. 4-1) und das andere Ende am Ethernet-Port des Computers an.
3. Wiederholen Sie diesen Schritt, um weitere Computer, einen Switch oder andere Netzwerkgeräte an das Gateway anzuschließen.

Abbildung 4-1: Ethernet-Verbindung

4. Schließen Sie ein Ende des zweites Netzwerkkabels an den LINE-Port auf der Rückseite des Gateways (siehe Abb. 4-2) und das andere Ende an den NTBA an.

Abbildung 4-2: ADSL-Verbindung

5. Schließen Sie den Netzstromadapter an den Netzstrom-Port des Gateways an (siehe Abb. 4-3), und stecken Sie den Netzstromadapter anschließend in eine Netzsteckdose. Stellen Sie den On-/Off-Schalter auf **On** (Ein).

   - Sobald das Netzgerät richtig angeschlossen und der Schalter auf **On** (Ein) gestellt ist, sollte die Netzstrom-LED auf der Vorderseite grün leuchten. Die Netzstrom-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen ist. Wenn die LED eine Minute oder länger blinkt, finden Sie Informationen zur Fehlerbehebung in "Anhang A: Fehlerbehebung".

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

Die Installation der Gateway-Hardware ist jetzt abgeschlossen.

Wechseln Sie zu "Kapitel 5: Konfigurieren des Gateways".

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

Abbildung 4-3: Netzstromverbindung

HINWEIS: Sie sollten stets die Standardeinstellung der SSID, **linksys**, ändern und die WEP-Verschlüsselung aktivieren.

Kapitel 5: Konfigurieren des Gateways

Übersicht

Folgen Sie zum Konfigurieren des Gateways den in diesem Kapitel aufgeführten Schritten, und verwenden Sie das webbasierte Dienstprogramm des Gateways. In diesem Kapitel werden alle Webseiten des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können das Dienstprogramm mit einem an das Gateway angeschlossenen Computer über Ihren Web-Browser aufrufen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer nur die folgenden Fenster des Dienstprogramms:

- **Grundlegende Einrichtung**: Geben Sie im Fenster *Grundlegende Einrichtung* die von Ihrem ISP bereitgestellten Einstellungen ein.
- **Verwaltungsfunktionen**: Klicken Sie auf die Registerkarte *Verwaltung* und anschließend auf die Registerkarte **Verwaltungsfunktionen**. Der Standardbenutzername und das Standardpasswort des Gateways lauten **admin**. Ändern Sie das Standardpasswort, um das Gateway zu schützen.

Es gibt sechs Hauptregisterkarten: **Einrichtung**, **Sicherheit**, **Zugriffsbeschränkungen**, **Anwendungen & Spiele**, **Verwaltung** und **Status**. Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar.

Haben Sie: TCP/IP auf Ihren Computern aktiviert? Computer tauschen über das Netzwerk mit diesem Protokoll Daten aus. Weitere Informationen zu TCP/IP erhalten Sie in der Windows-Hilfe.

Hinweis: Für zusätzliche Sicherheit sollten Sie das Passwort über die Registerkarte **Verwaltung** ändern.

Einrichtung

- **Grundlegende Einrichtung**: Geben Sie in dieses 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.
- **Erweitertes Routing**: Sie können in diesem Fenster die Konfigurationseinstellungen für dynamisches und statisches Routing ändern.

Sicherheit

- **Firewall**: Dieses Fenster enthält Filter und geblockte WAN-Anfragen. Durch die Verwendung von Filtern kann der Internetzugriff bestimmter interner Benutzer und anonyme Internet-Anfragen geblockt werden.
- **VPN**: Verwenden Sie dieses Fenster, um die Option **IPSec Passthrough** und/oder **PPTP Passthrough** zu aktivieren oder deaktivieren, und richten Sie VPN-Tunnel ein.

Zugriffsbeschränkungen

- **Internetzugriff**: Mithilfe dieses Fensters können Sie bestimmten Benutzern den Zugriff auf Ihr Netzwerk erlauben bzw. deren Zugriff verhindern.

Anwendungen & Spiele

- **Einfaches Port-Forwarding**: Verwenden Sie dieses Fenster, um die gängigsten Dienste und Anwendungen auf Ihrem Netzwerk einzurichten.
- **Weiterleitung an einen Anschlussbereich**: Klicken Sie auf diese Registerkarte, um öffentliche Dienste oder weitere spezielle Internetanwendungen auf Ihrem Netzwerk einzurichten.
- **Port Triggering**: Klicken Sie auf diese Registerkarte, um die Bereiche für Port-Triggering und Port-Forwarding für Internetanwendungen festzulegen.
- **DMZ**: Verwenden Sie dieses Fenster, um für einen Benutzer die Internetverbindung zur Verwendung von speziellen Diensten einzurichten.
- **QoS:** QoS (*Quality of Service*) sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

Verwaltung

- **Verwaltungsfunktionen**: In diesem Fenster können Sie Zugriffsrechte für das Gateway sowie SNMP-, UPnP- und WT-82-Einstellungen ändern.
- **Berichtaufzeichnung**: Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnose**: Verwenden Sie dieses Fenster, um einen Ping-Test durchzuführen.
- **Sichern & Wiederherstellen**: Mit der Registerkarte **Sichern & Wiederherstellen** können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.
- **Werkseinstellungen**: Verwenden Sie dieses Fenster, wenn Sie das Gateway of die Werkseinstellungen zurücksetzen möchten.
- **Firmware aktualisieren**: Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.
- **Neustart**: Über diese Registerkarte können Sie für Ihr Gateway einen Warm- oder Kaltstart ausführen.

Status

- **Gateway**: In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Lokales Netzwerk**: In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **DSL-Verbindung**: In diesem Fenster sind die Statusinformationen der DSL-Verbindung aufgeführt.

Hinweis für den Zugriff auf das webbasierte Dienstprogramm

Um auf das webbasierte Dienstprogramm zuzugreifen, starten Sie Internet Explorer oder Netscape Navigator, und geben Sie im Adressenfeld die Standard-IP-Adresse des Gateways (192.168.1.1) ein. Drücken Sie anschließend die Eingabetaste.

Das in Abbildung 5-1 angezeigte Fenster zur Eingabe des Passworts wird angezeigt. (Unter anderen Betriebssystemen als Windows XP wird ein ähnliches Fenster angezeigt.) Geben Sie **admin** (als Standardbenutzername) in das Feld **Benutzername** sowie **admin** (als Standardkennwort) in das Feld **Kennwort** ein. Klicken Sie anschließend auf die Schaltfläche **OK**.

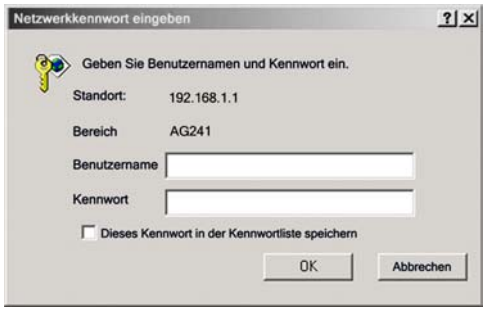


Abbildung 5-1: Fenster für die Passworteingabe

Registerkarte Einrichtung

Registerkarte Grundlegende Einrichtung

Im ersten dargestellten Fenster wird die Registerkarte **Grundlegende Einrichtung** angezeigt. Auf dieser Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie die Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Einstellungen speichern**, um Ihre Änderungen zu übernehmen, oder auf die Schaltfläche **Änderungen verwerfen**, um Ihre Änderungen zu verwerfen.

Interneteinrichtung

- **PVC-Verbindung**: Wählen Sie im Dropdown-Menü **PVC-Verbindung** eine Nummer aus. Aktivieren Sie anschließend **Jetzt aktivieren**, um die Verbindung zu aktivieren.
- **VC-Einstellungen**: **Virtuelle Verbindung, VPI und VCI**: Für diese Felder gibt es zwei Optionen: **VPI** (*Virtual Path Identifier*; Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier*; Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP.
  - **Multiplexing**: Wählen Sie entsprechend dem verwendeten ISP für diese Option **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.
  - **QoS-Typ**: Wählen Sie im Dropdown-Menü aus den 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 Bite Rate*; Variable Bitrate) für diskontinuierlichen Verkehr und Bandbreiten, die mit anderen Anwendungen gemeinsam genutzt werden.

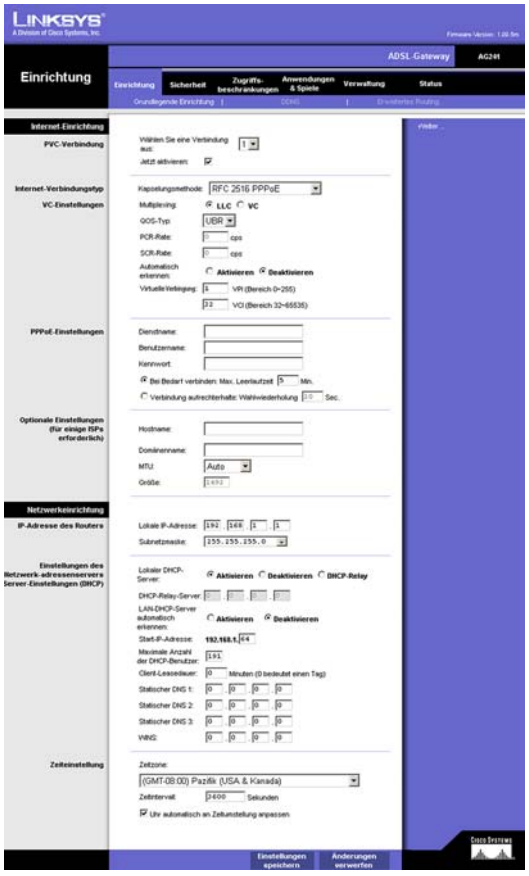


Abbildung 5-2: Registerkarte Grundlegende Einrichtung

- **PCR-Rate**: (*Peak Cell Rate*; Spitzenzellrate): Wenn Sie die Rate der DSL-Leitung durch 424 dividieren, erhalten Sie die PCR-Rate, anhand der Sie die maximale Rate, mit der der Absender Zellen senden kann, feststellen können. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **SCR-Rate**: (*Sustain Cell Rate*; Dauerzellrate): Bestimmt den Mittelwert der Zellrate, die übertragen werden kann. Die Dauerzellrate ist gewöhnlich niedriger als die Spitzenzellrate. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **Automatisch erkennen**: Wählen Sie **Aktivieren** aus, um die Einstellungen automatisch anzuzeigen, bzw. **Deaktivieren**, um die Werte manuell einzugeben.

- **Virtueller Verbindung**: Geben Sie die Bereiche für VPI und VCi in das jeweilige Feld ein.

- **Internet-Verbindungstyp**: Das Gateway unterstützt fünf Kapselungstypen: **RFC 1483-Überbrückung**, **RFC 1483-Weiterleitung**, **RFC 2516 PPPoE**, **RFC 2364 PPPoA** und **Nur Überbrückungsmodus**. Das jeweilige Fenster *Grundlegende Einrichtung* und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.

RFC 1483-Überbrückung

Dynamische IP-Adresse

IP-Einstellungen: Wählen Sie **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, wählen Sie **Folgende IP-Adresse verwenden** aus.

- **Internet-IP-Adresse**: Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.

- **Subnetzmaske**: Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.

- **Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.

- **Primärer DNS** (erforderliche Einstellung) und **Sekundärer DNS** (optionale Einstellung): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

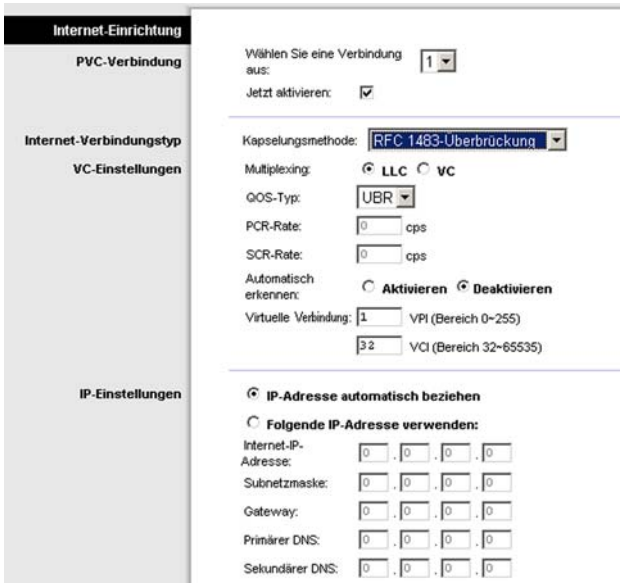


Abbildung 5-3: Dynamische IP-Adresse

Abbildung 5-4: Statische IP-Adresse

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

IPoA

Wenn Sie Classical IP über ATM verwenden müssen, wählen Sie **IPoA**.

- **IP-Adresse**: Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnetzmaske**: Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Standard-Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primärer DNS** (erforderliche Einstellung) und **Sekundärer DNS** (optionale Einstellung): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

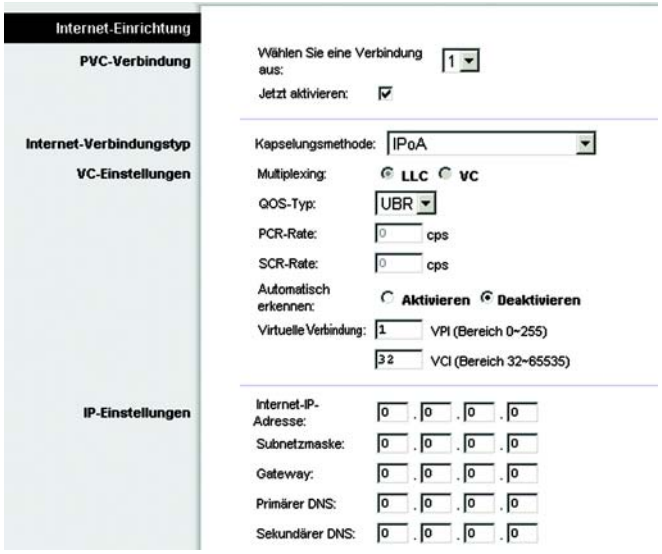


Abbildung 5-5: IPoA

RFC 2516 PPPoE

Einige ISPs auf DSL-Basis verwenden PPPoE (*Point-to-Point Protocol over Ethernet*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Verbindung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoE verwendet wird. Falls ja, aktivieren Sie die Option **PPPoE**.

- **Dienstname**: Geben Sie den Namen Ihres PPPoE-Diensts in das Feld ein.
- **Benutzername/Passwort**: Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **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 **Bei Bedarf verbinden** Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Bei Bedarf verbinden** zu aktivieren. Geben Sie im Feld **Max. Leerlaufzeit** die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Verbindung aufrechterhalten: Wahlwiederholung**: Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche neben **Verbindung aufrechterhalten**. Im Feld **Wahlwiederholung** legen Sie fest, wie oft das Gateway Ihre Internetverbindung überprüfen soll. Die standardmäßige Wahlwiederholung erfolgt nach 30 Sekunden.

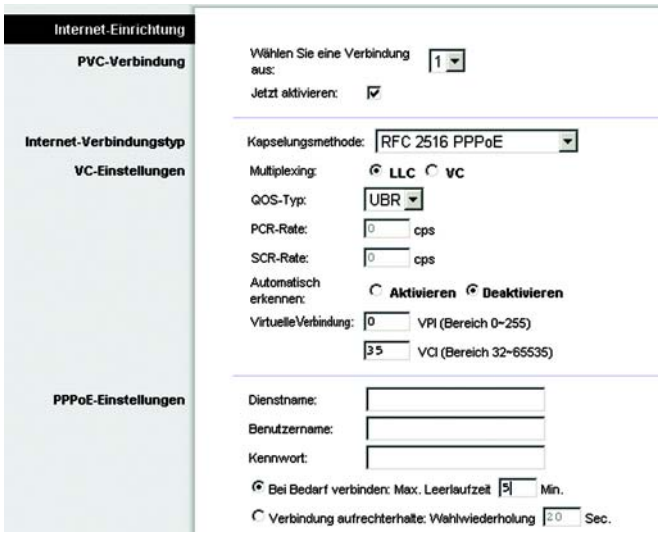


Abbildung 5-6: RFC 2516 PPPoE

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

RFC 2364 PPPoA

Einige ISPs auf DSL-Basis verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Leitung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoA verwendet wird. Falls ja, aktivieren Sie die Option **PPPoA**.

- **Benutzername/Passwort**: Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **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 **Bei Bedarf verbinden** Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Bei Bedarf verbinden** zu aktivieren. Geben Sie im Feld **Max. Leerlaufzeit** die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Verbindung aufrechterhalten: Wahlwiederholung**: Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche neben **Verbindung aufrechterhalten**. Im Feld **Wahlwiederholung** legen Sie fest, wie oft das Gateway Ihre Internetverbindung überprüfen soll. Die standardmäßige Wahlwiederholung erfolgt nach 30 Sekunden.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

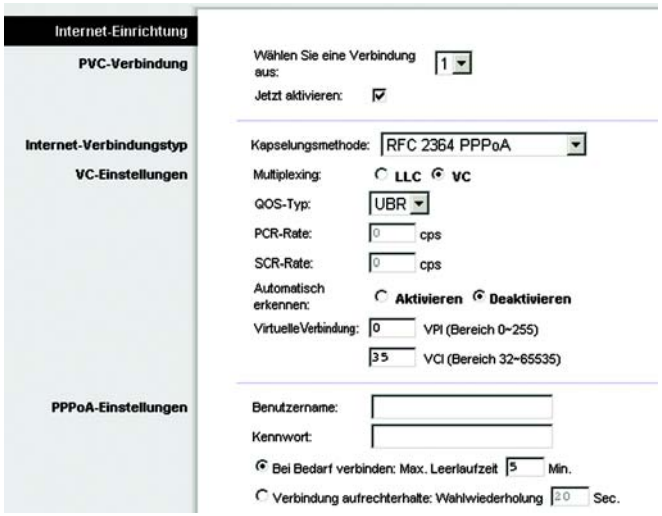


Abbildung 5-7: RFC 2364 PPPoA

Nur Überbrückungsmodus

Wenn Sie Ihr Gateway als Bridge verwenden (dadurch agiert das Gateway als Standalone-Modem), wählen Sie die Option **Nur Überbrückungsmodus** aus. In diesem Modus sind alle Einstellungen für NAT und Routing deaktiviert.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen.**

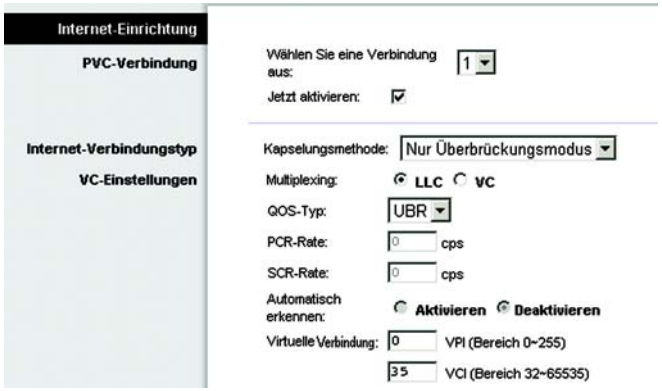


Abbildung 5-8: Nur Überbrückungsmodus

Optionale Einstellungen (für einige ISPs erforderlich)

- **Hostname/Domänenname**: In diese Felder können Sie einen Hostnamen bzw. 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:** Mit der MTU-Einstellung (*Maximum Transmission Unit*; Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie **Manuell** aus, und geben Sie den gewünschten Wert in das Feld *Size* (Größe) ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit (MTU) wird standardmäßig automatisch festgelegt.

Netzwerkeinrichtung

- **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.
  - **Lokale IP-Adresse**: Der Standardwert ist 192.168.1.1.
  - **Subnetzmaske**: Der Standardwert ist 255.255.255.0.
- **Einstellungen des Netzwerkadressenservers (DHCP)**: 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.
  - **DHCP-Relay-Server**: Wenn Sie den lokalen DHCP-Server oder das DHCP-Relay für den lokalen DHCP-Server aktivieren, geben Sie die IP-Adresse für den DHCP-Server in die Felder ein.
  - **LAN-DHCP-Server automatisch erkennen**.
  - **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.
  - **Maximale Anzahl der DHCP-Benutzer**: Geben Sie die maximale Anzahl von Benutzern bzw. Clients ein, denen eine IP-Adresse zugewiesen werden kann. Diese Zahl hängt von der eingegebenen Start-IP-Adresse ab.
  - **Client-Leasedauer**: Bei der Client-Leasedauer handelt es sich um den Zeitraum, über den ein Netzwerkbenutzer mithilfe seiner aktuellen dynamischen IP-Adresse eine Verbindung mit dem Gateway herstellen darf. Geben Sie den Zeitraum in Minuten ein, über den dem Benutzer diese dynamische IP-Adresse gewährt wird.
  - **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

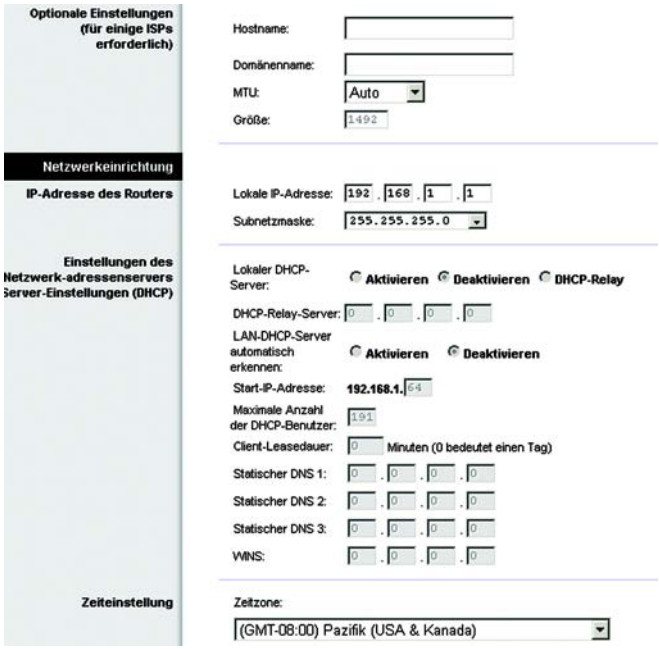


Abbildung 5-9: Optionale Einstellungen

für den DNS-Server. Hier können Sie bis zu drei IP-Adressen für den DNS-Server eingeben. Der Router 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.
- **Zeiteinstellung**: Mit dieser Option legen Sie die Zeitzone für Ihr Gateway fest. Wählen Sie Ihre Zeitzone aus dem Dropdown-Menü aus. Aktivieren Sie gegebenenfalls die Option **Uhr automatisch an Zeitumstellung anpassen**.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

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 bei den DDNS-Dienstanbietern unter www.dyndns.org anmelden.

DDNS

DDNS-Dienst: Wenn der von Ihnen verwendete DDNS-Dienst von DynDNS.org zur Verfügung gestellt wird, wählen Sie im Dropdown-Menü die Option **DynDNS.org** aus (siehe Abbildung 5-10). Um den DDNS-Dienst zu deaktivieren, wählen Sie die Option **Deaktiviert** aus.

Abbildung 5-10: DynDNS.org

DynDNS.org

- **Benutzername**, **Passwort** und **Hostname**: Geben Sie den Benutzernamen, das Passwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Internet-IP-Adresse**: Hier ist die aktuelle IP-Adresse des Gateways aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.

TZO.com

- **E-Mail-Adresse**, **Passwort** und **Domänenname**: Geben Sie die E-Mail-Adresse, das TZO-Passwort und den Domänenname des Dienstes ein, den Sie mit TZO eingerichtet haben.
- **Internet-IP-Adresse**: Hier ist die aktuelle IP-Adresse des Routers aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.

Abbildung 5-11: TZO.com

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Registerkarte Erweitertes Routing

Über das Fenster *Erweitertes Routing* können Sie die Einstellungen für dynamisches und statisches Routing konfigurieren

Erweitertes Routing

- **Betriebsmodus**: Bei NAT handelt es sich um eine Sicherheitsfunktion, die standardmäßig aktiviert ist. Das Gateway kann dank dieser Funktion IP-Adressen Ihres lokalen Netzwerks in eine andere IP-Adresse für die Internetnutzung umwandeln. Um NAT zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktiviert**.
- **Dynamisches Routing**: Mit der Option **Dynamisches Routing** kann das Gateway automatisch an physische Änderungen in der Netzwerkanordnung angepasst werden. Das Gateway legt unter Verwendung des RIP-Protokolls die Route der Netzwerkpakete auf der Grundlage der geringsten Anzahl an Sprüngen zwischen Quelle und Ziel fest. Das RIP-Protokoll sendet in regelmäßigen Abständen Routing-Informationen an andere Gateways im Netzwerk. Klicken Sie zum Aktivieren des RIP-Protokolls auf **Aktiviert**. Klicken Sie zum Deaktivieren des RIP-Protokolls auf **Deaktiviert**.
  - **RIP-Version übertragen**: Wählen Sie für die Übertragung von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1**, **RIP1-kompatibel** oder **RIP2**.
  - **RIP-Version empfangen**: Wählen Sie für den Empfang von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1** oder **RIP2**.
- **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:
  - **Set-Nummer auswählen**: Wählen Sie die Anzahl der statischen Routen aus dem Dropdown-Menü aus. Das Gateway unterstützt bis zu 20 Einträge für statische Routeneinträge. Wenn Sie nach Auswahl eines Eintrags eine Route löschen möchten, klicken Sie auf die Schaltfläche **Diesen Eintrag löschen**.
  - **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.
  - **Subnetzmaske**: Mithilfe der Subnetzmaske (auch Netzwerkmaske genannt) wird festgelegt, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.
  - **Gateway**: Bei dieser IP-Adresse handelt es sich um die IP-Adresse des Gateway-Geräts, das eine Verbindung zwischen dem Gateway und dem entfernten Netzwerk bzw. Host ermöglicht.
  - **Anzahl der Gateways**: Gibt die Anzahl der Gateways bis zu den einzelnen Knoten an, bevor das Ziel erreicht wird (max. 16 Gateways). Geben Sie diese Zahl in das Feld ein.

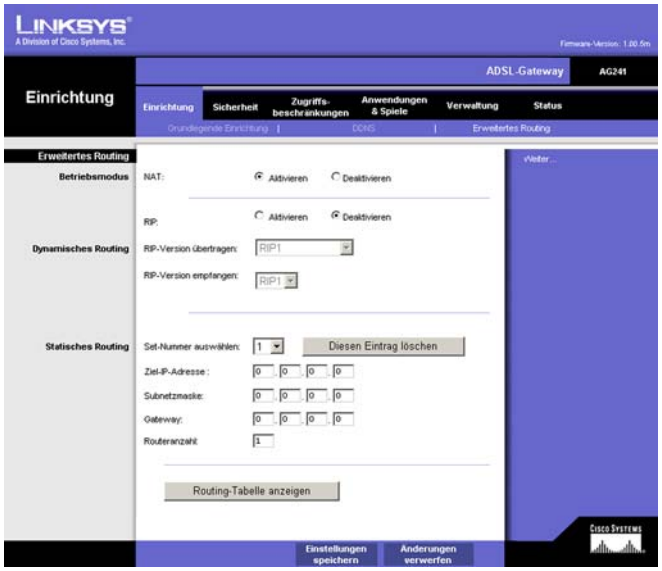


Abbildung 5-12: Erweitertes Routing

- **Routing-Tabelle anzeigen**: Klicken Sie auf die Schaltfläche **Routing-Tabelle anzeigen**, um ein Fenster mit den durch das LAN übertragenen Daten zu öffnen. Für jede Route wird die Ziel-IP-Adresse, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Daten zu aktualisieren. Klicken Sie auf die Schaltfläche **Schließen**, um zum vorherigen Fenster zurückzukehren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-13: Erweiterte Wireless-Einstellungen

Registerkarte Sicherheit

Firewall

Wenn Sie auf die Registerkarte **Sicherheit** klicken, wird das Fenster *Firewall* angezeigt. Dieses Fenster enthält Filter und die Option zum Blockieren von WAN-Anfragen. Durch die Verwendung von Filtern können spezielle Internetdatentypen und anonyme Internet-Anfragen geblockt werden. Klicken Sie zum Hinzufügen des Firewall-Schutzes auf **Aktivieren**. Klicken Sie zum Deaktivieren des Firewall-Schutzes auf **Deaktivieren**.

Abbildung 5-14: Firewall

Zusätzliche Filter

- **Filterproxy**: Die Verwendung von WAN-Proxyservern kann die Sicherheit des Gateways beeinträchtigen. Wenn Sie den Filterproxy ablehnen, wird der Zugriff auf alle WAN-Proxyserver deaktiviert. Um die Proxy-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **Cookies filtern**: Bei einem Cookie handelt es sich um Daten, die auf Ihrem Computer gespeichert sind und von Websites beim Zugriff auf diese Sites verwendet werden. Um die Cookie-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **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. Um die Java Applet-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **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. Um die ActiveX-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.

Blockieren von WAN-Anfragen

- **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 Ihres Netzwerks erhöhen, indem Ihre Netzwerk-Ports nicht angezeigt werden und Ihr Netzwerk vor Angreifern aus dem Internet besser geschützt ist. Aktivieren Sie die Option **Anonyme Internet-Anfragen blockieren**, um anonyme Internet-Anfragen zu blockieren bzw. deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

VPN

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Über dieses Fenster können Sie Ihre VPN-Einstellungen konfigurieren und damit die Sicherheit Ihres Netzwerks erhöhen.

VPN-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 die Optionsschaltfläche **Aktivieren**. Um IPSec-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktivieren**.
- **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 die Optionsschaltfläche **Aktivieren**. Um PPTP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktivieren**.
- **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 **Aktivieren**. Um P2TP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktivieren**.

IPSec VPN-Tunnel

Das VPN-Gateway erstellt einen Tunnel bzw. Kanal zwischen zwei Endpunkten, sodass die Datenübertragungen zwischen diesen beiden Endpunkten sicher sind.

- Um den Tunnel festzulegen, wählen Sie den Tunnel, den Sie erstellen möchten, aus dem Dropdown-Menü **Tunneleintrag auswählen** aus. Es können bis zu 5 gleichzeitig aktive Tunnel erstellt werden. Klicken Sie anschließend auf **Enabled** (Aktiviert), um den IPSec VPN-Tunnel zu aktivieren. Wenn der Tunnel aktiviert ist, geben Sie den Namen des Tunnels in das Feld **Tunnelname** ein. Auf diese Weise können Sie die verschiedenen Tunnel erkennen. Der eingegebene Name muss nicht dem Namen entsprechen, der am anderen Ende des Tunnels verwendet wird. Um einen Tunneleintrag zu löschen, wählen Sie den entsprechenden Tunnel aus, und klicken Sie auf **Löschen**. Klicken Sie auf **Zusammenfassung**, um eine Zusammenfassung der Einstellungen anzuzeigen.
- **Lokale sichere Gruppe** und **Entfernte sichere Gruppe**: **Lokale sichere Gruppe** umfasst die Computer in Ihrem LAN, die auf den Tunnel zugreifen können. **Entfernte sichere Gruppe** umfasst die Computer am entfernten Ende des Tunnels, die auf den Tunnel zugreifen können. Diese Computer können durch ein Subnetz, eine spezielle IP-Adresse oder einen Bereich festgelegt werden.
- **Lokales Sicherheits-Gateway**.

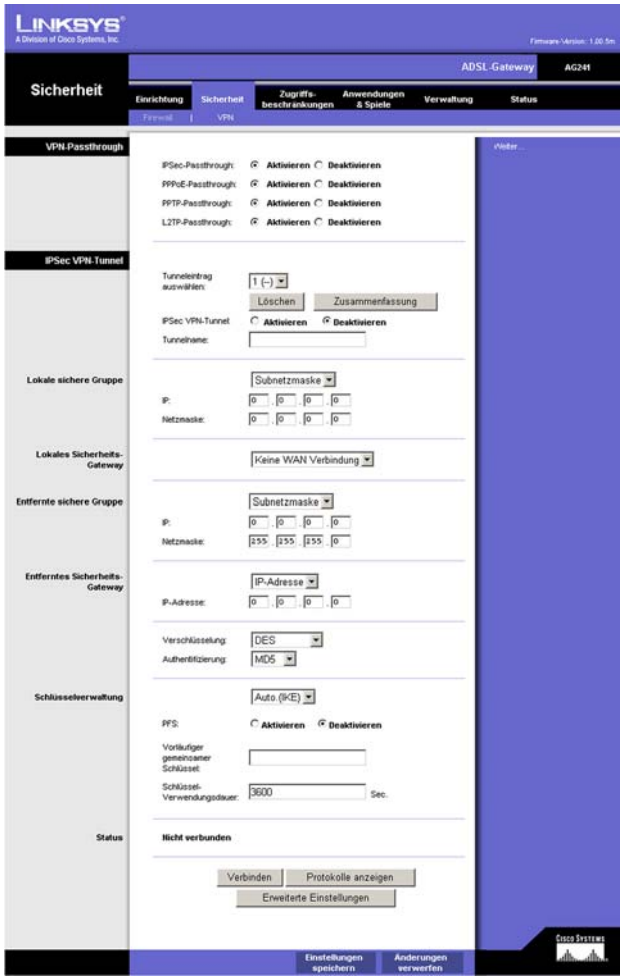


Abbildung 5-15: VPN

Abbildung 5-16: Zusammenfassung der VPN-Einstellungen

- **Entferntes Sicherheits-Gateway**: Bei dem **Entferntes Sicherheits-Gateway** handelt es sich um das VPN-Gerät (beispielsweise ein zweites VPN-Gateway) am entfernten Ende des VPN-Tunnels. Geben Sie die IP-Adresse oder Domäne des VPN-Geräts am anderen Ende des Tunnels ein. Bei dem entfernten VPN-Gerät kann es sich um ein anderes VPN-Gateway, einen VPN-Server oder einen Computer mit VPN-Client-Software handeln, der IPSec unterstützt. Bei der IP-Adresse kann es sich je nach den Einstellungen des entfernten VPN-Geräts um eine statische (permanente) Adresse oder um eine dynamische (sich ändernde) Adresse handeln. Vergewissern Sie sich, dass Sie die korrekte IP-Adresse eingegeben haben; anderenfalls kann keine Verbindung hergestellt werden. Denken Sie daran, dass dies NICHT die IP-Adresse des lokalen VPN-Gateways ist, sondern die IP-Adresse des entfernten VPN-Gateways bzw. -Geräts, mit dem kommuniziert werden soll. Wenn Sie eine IP-Adresse eingeben, kann nur mit der angegebenen IP-Adresse auf den Tunnel zugegriffen werden. Wenn Sie **Alle** auswählen, kann mit jeder IP-Adresse auf den Tunnel zugegriffen werden.
- **Verschlüsselung**: Mit **Verschlüsselung** machen Sie die Verbindung noch sicherer. Es stehen zwei Verschlüsselungstypen zur Verfügung: **DES** und **3DES** (empfohlen wird **3DES**, da dieser Typ sicherer ist). Sie können einen der beiden Typen wählen; die Einstellung muss jedoch mit dem Verschlüsselungstyp übereinstimmen, der vom VPN-Gerät am anderen Ende des Tunnels verwendet wird. Sie können aber auch ohne Verschlüsselung arbeiten, indem Sie **Deaktivieren** auswählen. In Abbildung 5-22 wurde DES ausgewählt (Standardeinstellung).
- **Authentifizierung**: Die Authentifizierung stellt eine weitere Sicherheitsstufe dar. Es stehen zwei Authentifizierungstypen zur Verfügung: **MD5** und **SHA** (empfohlen wird **SHA**, da dieser Typ sicherer ist). Wie bei der Verschlüsselung kann einer der beiden Typen gewählt werden, vorausgesetzt, das VPN-Gerät am anderen Ende des Tunnels verwendet denselben Authentifizierungstyp. Die Authentifizierung kann aber auch mit **Deaktivieren** an beiden Enden des Tunnels deaktiviert werden. Im Fenster *Manual Key Management* (Manuelle Schlüsselverwaltung) wurde der Standardwert **MD5** ausgewählt.
- **Schlüsselverwaltung**: Wählen Sie aus dem Dropdown-Menü **Auto (IKE)** oder **Manuell** aus. Die beiden Methoden werden im Folgenden beschrieben.

  Auto (IKE)
  Wählen Sie **Auto (IKE)**, und geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld **Pre-shared Key** (Vorläufiger gemeinsamer Schlüssel) ein. Wenn dieses Verfahren verwendet wird, MUSS das Wort an beiden Enden des Tunnels eingegeben werden. Auf der Grundlage dieses Worts 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. Im Feld **Schlüssel-Verwendungsdauer** 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. Markieren Sie das Kontrollkästchen neben PFS (Perfect Forward Secrecy) [Vollständige Geheimhaltung bei Weiterleitung], um sicherzustellen, dass der erste Schlüsselaustausch und die IKE-Vorschläge sicher sind.

Manuell
Wählen Sie **Manuell** und anschließend den Verschlüsselungsalgorithmus aus dem Dropdown-Menü aus. Geben Sie den Codierschlüssel in das dafür vorgesehene Feld ein (wenn Sie **DES** als Verschlüsselungsalgorithmus ausgewählt haben, geben Sie 16 hexadezimale Zeichen ein, wenn Sie **3DES** ausgewählt haben, geben Sie 48 hexadezimale Zeichen ein). Wählen Sie den Authentifizierungsalgorithmus aus dem Dropdown-Menü aus. Geben Sie den Authentifizierungsschlüssel in das dafür vorgesehene Feld ein (wenn Sie **MD5** als Verschlüsselungsalgorithmus ausgewählt haben, geben Sie 32 hexadezimale Zeichen ein, wenn Sie **SHA1** ausgewählt haben, geben Sie 40 hexadezimale Zeichen ein). Geben Sie in die entsprechenden Felder **Inbound SPI** (Eingangs-SPI) und **Outbound SPI** (Ausgangs-SPI) ein.

- **Status**: In dieser Zeile wird der Status der Verbindung angezeigt.

Klicken Sie auf die Schaltfläche **Verbinden**, um Ihren VPN-Tunnel zu verbinden. Klicken Sie auf **Protokolle anzeigen**, um die System-, UPnP-, VPN-, Firewall-, Zugriffs- oder alle Protokolle anzuzeigen. Klicken Sie auf die Schaltfläche **Weitere Einstellungen**, um das Fenster *Advanced IPSec VPN Tunnel Setup* (Erweiterte IPSec VPN-Tunnel-Einrichtung) anzuzeigen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

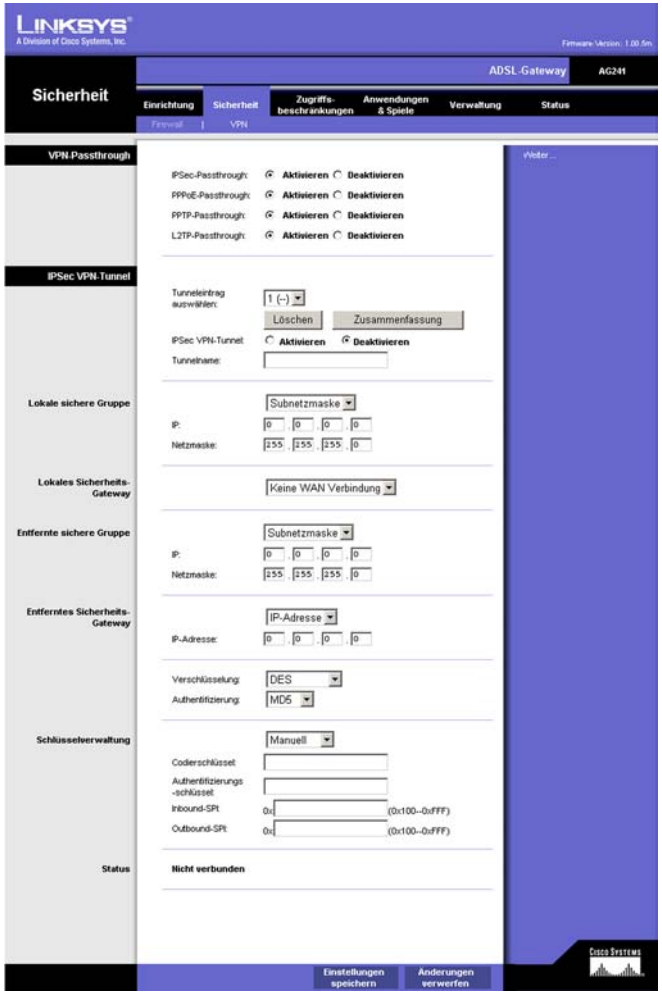


Abbildung 5-17: Manuelle Schlüsselverwaltung

Abbildung 5-18: Systemprotokoll

Erweiterte IPSec VPN-Tunnel-Einrichtung

Sie können über das Fenster *Erweiterte IPSec VPN-Tunnel-Einrichtung* die Einstellungen für bestimmte VPN-Tunnel anpassen.

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.
- **Betriebsmodus**: Es gibt zwei Modi: **Hauptmodus** und **Aggressiver Modus**, die die gleichen IKE-Nutzlasten auf unterschiedlichen Sequenzen austauschen. 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-Gateway Anfragen sowohl im Haupt- als auch im aggressiven Modus vom standortfernen VPN-Gerät akzeptiert.
- **Verschlüsselung**: Wählen Sie die Länge des Schlüssels aus, der zum Verschlüsseln/Entschlüsseln von ESP-Paketen verwendet wird. Sie können zwischen zwei Methoden wählen: **DES** und **3DES**. Die Verwendung von **3DES** wird empfohlen, da diese Verschlüsselungsart sicherer ist.
- **Authentifizierung**: Wählen Sie die Methode aus, die zur Authentifizierung von ESP-Paketen verwendet wird. Sie können zwischen zwei Methoden wählen: **MD5** und **SHA**. Die Verwendung von **SHA** wird empfohlen, da diese sicherer ist.
- **Gruppe**: Es stehen zwei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit und 1024 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.
- **Schlüssel-Verwendungsdauer**: Im Feld **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

- **Verschlüsselung**: Die in Phase 1 ausgewählte Verschlüsselungsmethode wird angezeigt.
- **Authentifizierung**: Die in Phase 1 ausgewählte Authentifizierungsmethode wird angezeigt.
- **PFS** (PFS, *Perfect Forward Secrecy*): In dieser Zeile wird der PFS-Status angezeigt.
- **Gruppe**: Es stehen zwei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit und 1024 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.

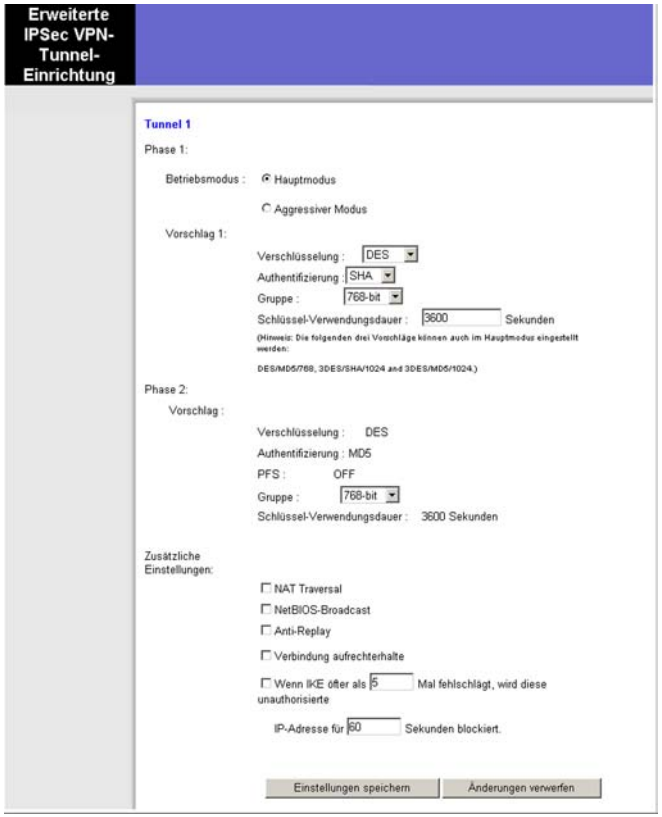


Abbildung 5-19: Erweiterte IPSec VPN-Tunnel-Einrichtung

- **Schlüssel-Verwendungsdauer**: Im Feld **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.

Zusätzliche Einstellung

- **NetBIOS-Broadcast**: Aktivieren Sie das Kontrollkästchen neben **NetBIOS-Broadcast**, um den NetBIOS-Datenverkehr durch den VPN-Tunnel zu leiten.
- **Anti-Replay**: Aktivieren Sie das Kontrollkästchen neben **Anti-Replay**, um den Anti-Replay-Schutz zu aktivieren. Mithilfe dieser Funktion werden die Sequenznummern der eingehenden Datenpakete aufgezeichnet, wodurch die Sicherheit auf IP-Paketebene gewährleistet wird.
- **Verbindung aufrechterhalten**: Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her.
- Aktivieren Sie dieses Kontrollkästchen, um unberechtigte IP-Adressen zu blockieren. Füllen Sie dieses Feld aus, um die Anzahl der fehlgeschlagenen IKE festzulegen, bevor die unberechtigte IP-Adresse blockiert wird. Geben Sie den Zeitraum in Sekunden in dieses Feld ein.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**. Klicken Sie auf die Schaltfläche **Nehr Information**, um weitere Informationen zu dieser Registerkarte zu erhalten.

Registerkarte Zugriffsbeschränkungen

Internetzugriff

Mit der Registerkarte **Zugriffsbeschränkungen** können Sie bestimmte Arten der Internetverwendung blockieren bzw. zulassen. Sie können für bestimmte Computer Sicherheitsrichtlinien für den Internetzugriff und Filter mithilfe von Netzwerk-Anschlussnummern einrichten.

- **Richtlinien für Internetzugriff**: Mehrfache Filter können als Sicherheitsrichtlinien für den Internetzugriff gespeichert werden. Wählen zur Bearbeitung einer Richtlinie die entsprechende Nummer aus dem Dropdown-Menü aus. Die Anzeige der Registerkarte ändert sich, um die Änderungen an den Einstellungen an dieser Richtlinie anzuzeigen. Klicken Sie zum Löschen dieser Richtlinie auf die Schaltfläche **Löschen**. Klicken Sie zur Anzeige einer Zusammenfassung aller Richtiglinien auf die Schaltfläche **Zusammenfassung**.

  Die Zusammenfassung wird in einem Fenster mit dem entsprechenden Namen und den entsprechenden Einstellungen angezeigt. Um zur Registerkarte **Filter** zurückzukehren, klicken Sie auf die Schaltfläche **Schließen**.
- **Richtliniennamen eingeben**: Richtlinien werden auf Grundlage der hier aufgeführten Felder erstellt.

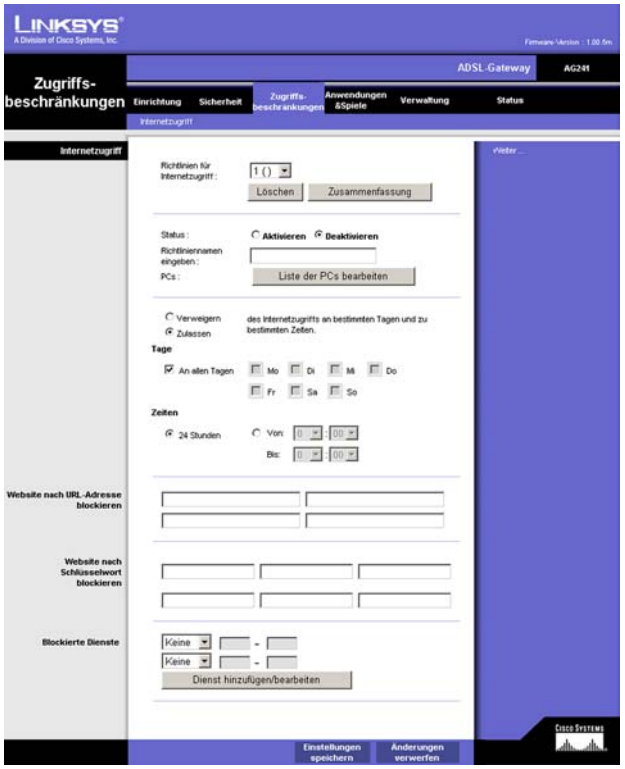


Abbildung 5-20: Internetzugriff

Abbildung 5-21: Internet-Richtlinien - Zusammenfassung

So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Geben Sie im Feld **Richtlinienname** einen Namen für die Richtlinie ein. Wählen Sie **Internetzugriff** als Richtlinientyp aus.
2. Klicken Sie auf die Schaltfläche **PC-Liste bearbeiten**. Das Fenster *PC-Liste* wird geöffnet. In diesem Fenster können Sie die IP-Adresse bzw. MAC-Adresse der Computer angeben, auf die die Richtlinie angewendet werden soll. Sie können auch über die IP-Adresse Computerbereiche eingeben. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um Ihre Einstellungen zu speichern, oder klicken Sie auf die Schaltfläche **Änderungen verwerfen**, um Ihre Änderungen zu verwerfen und zur Registerkarte **Filter** zurückzukehren.
3. Klicken Sie auf die entsprechende Option (**Verweigern** oder **Zulassen**), um den Internetzugriff für die PCs, die im Fenster *PC-Liste* aufgeführt sind, zu blockieren oder zuzulassen.
4. Sie können den Zugang zu verschiedenen Diensten filtern, auf die über das Internet zugegriffen werden kann, wie z. B. FTP oder Telnet, indem Sie diese Dienste in den Dropdown-Menüs neben **Blockierte Dienste** auswählen. Wenn ein Dienst nicht in der Liste aufgeführt ist, klicken Sie auf die Schaltfläche **Dienst hinzufügen/bearbeiten**, um das Fenster *Anschlussdienste* zu öffnen und der Liste einen Dienst hinzuzufügen. Sie müssen einen Dienstnamen und das von diesem Dienst verwendete Protokoll sowie den Anschlussbereich eingeben.
5. Durch Auswahl der entsprechenden Zeit- und Datumseinstellung legen Sie den Zeitpunkt fest, zu dem der Internetzugriff gefiltert wird.
6. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um die Richtlinie zu aktivieren.

   Der Internetzugriff kann auch über die URL-Adresse gefiltert werden, die Sie für den Zugriff auf Internetadressen eingeben. Geben Sie hierfür die Adresse in eines der Felder für 'Website nach URL-Adresse blockieren' ein. Wenn Ihnen die URL-Adresse nicht bekannt ist, können Sie das Filtern mithilfe bestimmter Stichwörter vornehmen. Geben Sie hierfür ein Stichwort in eines der Felder für das Blockieren von Websites nach Schlüsselwort ein.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

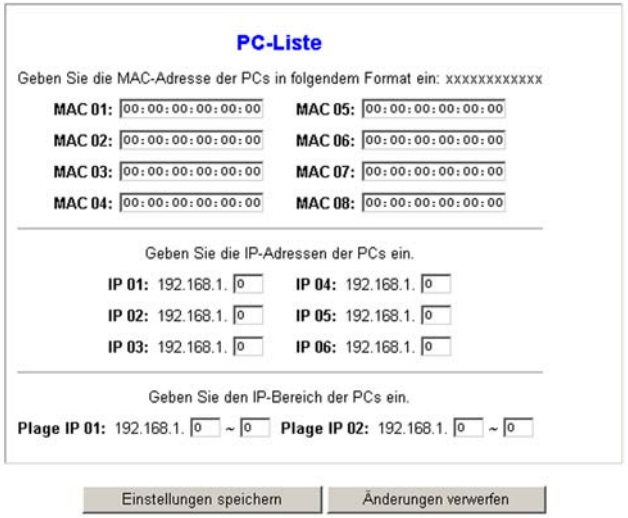


Abbildung 5-22: PC-Liste

Abbildung 5-23: Anschlussdienste

Registerkarte Anwendungen und Spiele

Einfaches Port-Forwarding

Das Fenster *Einfaches Port-Forwarding* bietet Optionen zur Anpassung der Anschlussdienste der gängigsten Anwendungen.

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC 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.

Wählen Sie in diesem Feld eine Anwendung aus, oder geben Sie eine Anwendung ein. Geben Sie in diese Felder anschließend die Anschlussnummern der externen und internen Anschlüsse an. Wählen Sie den Protokolltyp aus, den Sie für jede Anwendung verwenden möchten: **TCP** oder **UDP**. Geben Sie in das Feld die IP-Adresse ein. Klicken Sie auf **Aktivieren**, um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-24: Einfaches Port-Forwarding

Weiterleitung an einen Anschlussbereich

Im Fenster *Port-Forwarding* können Sie öffentliche Dienste auf Ihrem Netzwerk, wie z. B. Web-, FTP-, E-Mail-Server oder spezielle Internetanwendungen, festlegen. (Unter speziellen Internetanwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internetspiele 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 PC 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.

- **Anwendung**: Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Von** und **Bis**: Geben Sie die Anfangs- und Endnummern der Ports ein, die weitergeleitet werden sollen.
- **TCP** und **UDP**: Wählen Sie den Protokolltyp aus, den Sie für jede Anwendung verwenden möchten: **TCP**, **UDP** oder **Beide**.
- **IP-Adresse**: Geben Sie die IP-Adresse ein, und klicken Sie auf **Aktivieren**.

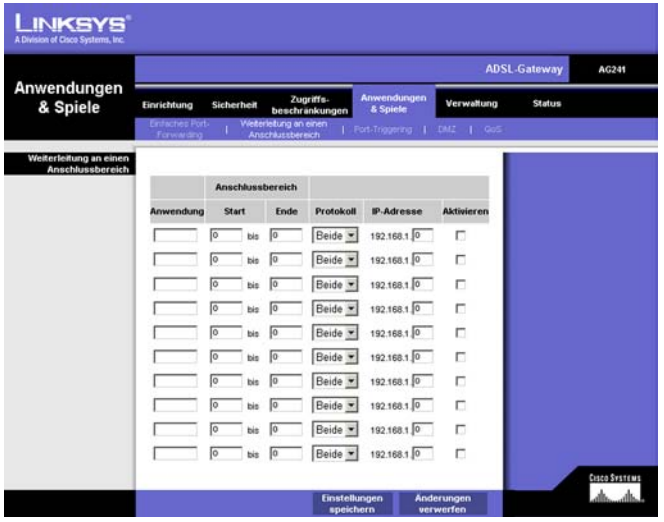


Abbildung 5-25: Weiterleitung an einen Anschlussbereich

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Port-Triggering

Port-Triggering wird bei speziellen Anwendungen verwendet, über die ein Anschluss auf Anfrage geöffnet werden kann. Bei dieser Funktion überprüft das Gateway ausgehende Daten auf spezielle Anschlussnummern. 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 zum richtigen Computer weitergeleitet.

- **Anwendung**: Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Start-Port** und **End-Port**: Geben Sie Anfang und Ende der Bereichsnummern für Port-Triggering sowie die Bereichsnummern für Port-Forwarding der Anschlüsse ein, die Sie weiterleiten möchten.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

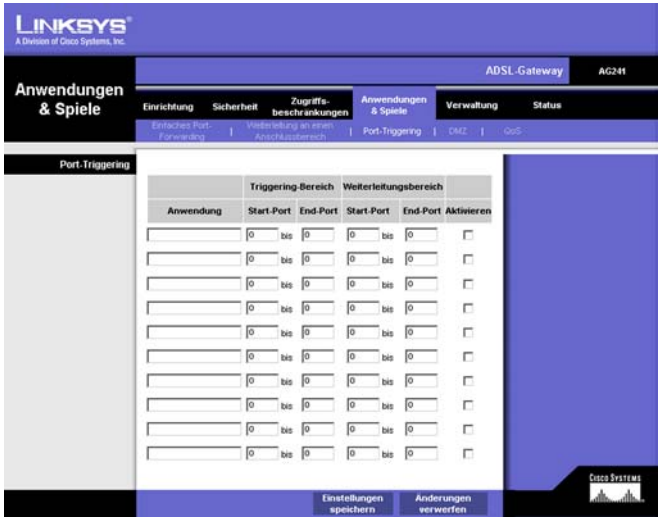


Abbildung 5-26: Port-Triggering

DMZ

Über das Fenster *DMZ* kann mithilfe von DMZ-Hosting für einen Netzwerkbenutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste, wie Internetspiele oder Videokonferenzen, nutzen kann. Mit DMZ-Hosting werden alle Anschlüsse gleichzeitig an einen PC weitergeleitet, im Unterschied zu **Weiterleitung an einen Anschlussbereich**, bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

- **DMZ-Hosting**: Mit der DMZ-Funktion (*Demilitarized Zone*; Entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internetspiele oder Videokonferenzen, nutzen kann. Klicken Sie auf **Aktivieren**, um diese Funktion zu verwenden. Klicken Sie auf **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 einer IP-Adresse 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 **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-27: DMZ

QOS

QoS (*Quality of Service*) sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

Anwendungsbasierte QoS

Über **Anwendungsbasierte QoS** werden Informationen beim Übertragen und Empfangen verwaltet. Je nachdem, welche Einstellungen im Fenster *QoS* festgelegt sind, weist diese Funktion Informationen eine hohe oder niedrige Priorität für die fünf voreingestellten Anwendungen und drei zusätzliche Anwendungen zu, die Sie bestimmen.

Aktivieren/Deaktivieren: Wählen Sie zur Verwendung der anwendungsbasierten QoS die Option **Aktivieren**. Behalten Sie andernfalls die Standardeinstellung **Deaktivieren** bei.

Hohe/mittlere/niedrige Priorität: Wählen Sie für jede der Anwendungen **Hohe Priorität** (Datenverkehr in dieser Warteschlange belegt 60 % der gesamten Bandbreite), **Mittlere Priorität** (Datenverkehr in dieser Warteschlange belegt 18 % der gesamten Bandbreite) oder **Niedrige Priorität** (Datenverkehr in dieser Warteschlange belegt 1 % der gesamten Bandbreite).

FTP (*File Transfer Protocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk (Internet, UNIX usw.). Nachdem HTML-Seiten für eine Website auf einem lokalen System gestaltet wurden, werden sie üblicherweise über FTP auf den Webserver geladen.

HTTP (*HyperText Transport Protocol*): Kommunikationsprotokoll, das zum Anschließen von Servern an das World Wide Web verwendet wird. Seine Hauptfunktion besteht darin, eine Verbindung mit einem Webserver herzustellen und HTML-Seiten an den Webbrowser des Clients zu übertragen.

Telnet: Ein Protokoll zur Terminal-Emulation, das häufig in Internet- und TCP/IP-basierten Netzwerken verwendet wird. Dadurch wird einem Benutzer an einem Terminal oder Computer ermöglicht, sich bei einem entfernten Gerät anzumelden und ein Programm auszuführen.

SMTP (*Simple Mail Transfer Protocol*): **Das standardmäßige E-Mail-Protokoll im Internet.** Ein TCP/IP-Protokoll, mit dem das Meldungsformat sowie der MTA (*Message Transfer Agent*; Meldungsübertragungsagent) festgelegt werden, der die Mail speichert und weiterleitet.

POP3 (*Post Office Protocol 3*): Ein im Internet verbreitet eingesetzter Standard-Mailserver. Er bietet einen Meldungsspeicher, in dem eingehende Mails gespeichert werden, bis sich der entsprechende Empfänger anmeldet und die Mails herunterlädt. POP3 ist ein einfaches System mit wenig Auswahlmöglichkeiten. Alle ausstehenden Meldungen und Anhänge werden zur selben Zeit heruntergeladen. POP3 verwendet das SMTP-Meldungsprotokoll.

Spezielle Anschlussnummer: Sie können drei zusätzliche Anwendungen hinzufügen, indem Sie deren jeweilige Anschlussnummern in die Felder *Spezielle Anschlussnummer* eingeben.

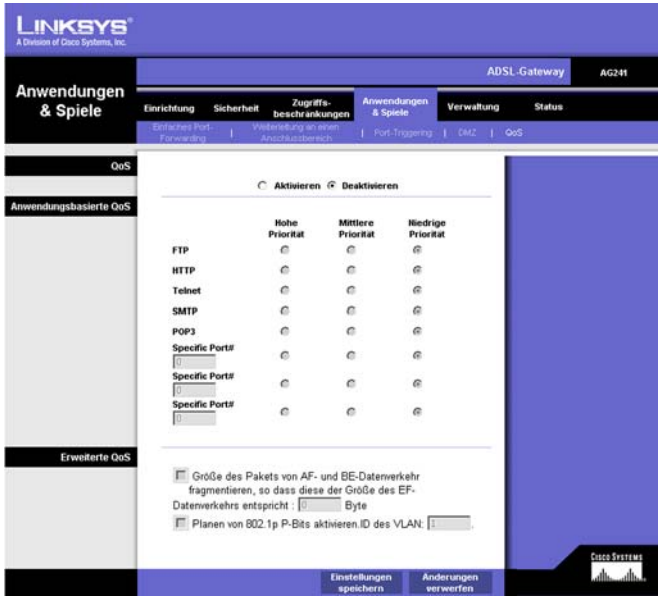


Abbildung 5-28: QOS

Erweiterte QoS

Mit dieser Einstellung können Sie Prioritäten für die Datenverkehrswarteschlange festlegen.

Fragment packet's size of AF and BE traffic to be equal to the size of EF traffic (Größe des Pakets von AF- und BE-Datenverkehr fragmentieren, sodass diese der Größe des EF-Datenverkehrs entspricht): Wählen Sie diese Option aus, um die Paketgrößen von Warteschlangen der Art AF (*Assured Forwarding*; Garantierte Weiterleitung) und BE (*Best Effort*; Beste Bemühung) zu fragmentieren, sodass die Effizienz zum Übertragen von Warteschlangen der Art EF (*Expedited Forwarding*; Express-Weiterleitung) erhöht wird. Geben Sie einen Bereich zwischen 68 und 1492 Byte ein.

Enable 802.1p P bits scheduling. VLAN's VID. (Planen von 802.1p P-Bits aktivieren. ID des VLAN): Wählen Sie diese Option aus, um das Planen von 802.1p P-Bits-Klassifikationen für das entsprechende VLAN basierend auf der IEEE 802.1Q VLAN-Identifikation zu aktivieren. Geben Sie die VLAN-ID in das Feld ein.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Einstellungen speichern**, oder klicken Sie auf die Schaltfläche **Änderungen verwerfen**, um die Änderungen rückgängig zu machen.

Registerkarte Verwaltung

Verwaltungsfunktionen

Über das Fenster *Verwaltungsfunktionen* können Sie die Einstellungen für den Gateway-Zugriff sowie die Einstellungen für **SNMP** (*Simple Network Management Protocol*) und **UPnP** (*Universal Plug and Play*) ändern.

Gateway-Zugriff

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 sind **admin**.

- **Gateway-Benutzername**: Geben Sie den Standardbenutzernamen **admin** ein. Es wird empfohlen, dass Sie Ihren Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway-Passwort**: Es wird empfohlen, dass Sie Ihr Standardpasswort in ein persönliches Passwort ändern.
- **Zur Bestätigung erneut eingeben**: Geben Sie das neue Gateway-Passwort erneut ein, um es zu bestätigen.
- **Entfernter Gateway-Zugriff**: Mit dieser Funktion können Sie auf das Gateway von einem entfernten Standort aus über das Internet zugreifen.

WICHTIG: Durch Aktivieren der Funktion **Entfernte Verwaltung** ist es jedem Benutzer, der auf Ihr Passwort zugreifen kann, möglich, das Gateway von jedem beliebigen Standort im Internet aus zu konfigurieren.

- **Entfernte Verwaltung**: Mit dieser Funktion können Sie das Gateway von einem entfernten Standort aus über das Internet verwalten. Um **Entfernte Verwaltung** zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **Verwaltungsanschluss**: Geben Sie die Anschlussnummer ein, die Sie für den entfernten Zugriff auf das Gateway verwenden möchten.

SNMP

SNMP ist ein häufig verwendetes Protokoll zur Netzwerküberwachung und -verwaltung.

Identifikation: Um **SNMP** zu verwenden, klicken Sie auf **Aktiviert**. Um **SNMP** zu deaktivieren, klicken Sie auf **Deaktiviert**.

Abbildung 5-29: Verwaltungsfunktionen

UPnP

Mit UPnP kann unter Windows XP das Gateway automatisch für verschiedene Internetanwendungen, wie z. B. Internetspiele oder Videokonferenzen, konfiguriert werden.

UPnP: Um **UPnP** zu verwenden, klicken Sie auf **Aktivieren**.

Wählen Sie eine PVC-Verbindung aus. Wählen Sie im Dropdown-Menü eine Nummer aus.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Berichtaufzeichnung

Über die Registerkarte **Berichtaufzeichnung** steht ein Protokoll zur Verfügung, in dem alle eingehenden und ausgehenden URLs bzw. IP-Adressen für Ihre Internetverbindung aufgeführt sind. Über diese Registerkarte stehen auch Protokolle für VPN- und Firewall-Ereignisse zur Verfügung.

- **Protokoll**: Um die Berichtaufzeichnung zu verwenden, klicken Sie auf **Aktivieren**.
- **Logviewer-IP-Adresse**: Geben Sie in dieses Feld die IP-Adresse ein, über die die Protokolle empfangen werden sollen.

E-Mail-Warnungen

E-Mail-Warnungen: Um E-Mail-Warnungen zu verwenden, klicken Sie auf die Option **Aktivieren**.

- **DoS-Schwellwerte**: Geben Sie die Schwellwerte der Ereignisse an, die Sie empfangen möchten.
- **SMTP Mail-Server**: Geben Sie in dieses Feld die IP-Adresse des SMTP-Servers ein.
- **E-Mail-Adresse für Warnungsprotokolle**: Geben Sie in dieses Feld die E-Mail-Adresse für die Warnungsprotokolle ein.
- **E-Mail-Antwortadresse**: Geben Sie die E-Mail-Adresse für Antwort-E-Mails ein.

Um Protokolle anzuzeigen, klicken Sie auf die Schaltfläche **Protokolle anzeigen**.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-30: Berichtaufzeichnung

Abbildung 5-31: Systemprotokoll

Diagnose

Ping-Test

Ping-Test-Parameter

- **Ping-Ziel-IP-Adresse**: Geben Sie in dieses Feld die IP-Adresse ein, die Sie für den Ping-Befehl verwenden möchten. Dies kann eine lokale IP-Adresse (LAN) oder eine Internet-IP-Adresse (WAN) sein.
- **Ping-Größe**: Geben Sie die Größe des Ping-Pakets an.
- **Anzahl der Pings**: Geben Sie die Anzahl der Pings an, die durchgeführt werden soll.
- **Ping-Intervall**: Geben Sie das Ping-Intervall in Millisekunden an.
- **Ping-Wartezeit**: Geben Sie die Wartezeit in Millisekunden an.
- **Ping-Ergebnisse**: In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

Klicken Sie auf die Schaltfläche **Test starten**, um den Ping-Test zu starten.

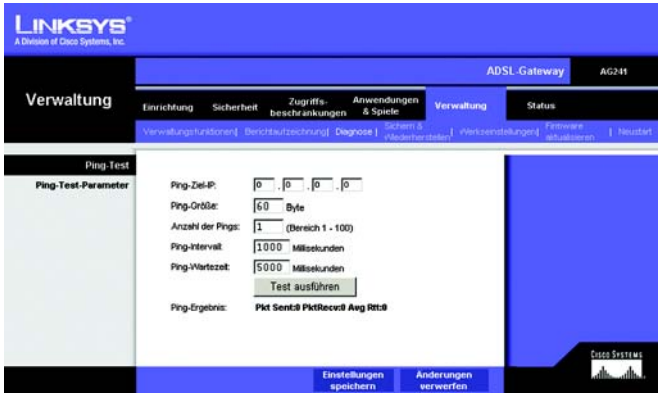


Abbildung 5-32: Ping-Test

Sichern & Wiederherstellen

Mit der Registerkarte **Sichern & Wiederherstellen** können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.

Klicken Sie zum Erstellen einer Sicherungskopie der Konfigurationsdatei des Routers auf die Schaltfläche **Sichern**. Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Klicken Sie zum Wiederherstellen der Konfigurationsdatei des Routers auf die Schaltfläche **Browse** (Durchsuchen), um nach der Datei zu suchen, und befolgen Sie dann die Anweisungen auf dem Bildschirm. Wenn Sie die Datei gefunden haben, klicken Sie auf die Schaltfläche **Wiederherstellen**.

Abbildung 5-33: Sichern & Wiederherstellen

Werkseinstellungen

Werkseinstellungen wiederherstellen: Wenn Sie das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen werden dabei nicht beibehalten), klicken Sie auf **Ja**.

Um den Wiederherstellungsvorgang zu starten und die Einstellungen zu speichern, kicken Sie auf die Schaltfläche **Einstellungen speichern** bzw. klicken Sie auf **Änderungen verwerfe**), um Ihre Änderungen zu verwerfen.

Abbildung 5-34: Werkseinstellungen

Aktualisieren der Firmware

Mit dem ADSL Gateway können Sie Firmware für die LAN-Seite (Netzwerkseite) des Gateways aktualisieren.

Aktualisieren aus dem LAN

So aktualisieren Sie die Gateway-Firmware aus dem LAN:

1. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der Firmware-Aktualisierungsdatei zu suchen, die Sie von der Linksys Website heruntergeladen und extrahiert haben.
2. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben. Klicken Sie auf die Schaltfläche **Aktualisieren**, und folgen Sie den daraufhin angezeigten Anweisungen.

Abbildung 5-35: Firmware aktualisieren

Neustart

Über diese Registerkarte können Sie für Ihr Gateway einen Warm- oder Kaltstart ausführen.

Neustart-Modus: Um Ihr Gateway neu zu starten, wählen Sie **Kaltstart** oder **Warmstart** aus. Um das Gateway aus- und wieder einzuschalten, wählen Sie die Option **Kaltstart**. Um das Gateway neu zu starten, ohne es auszuschalten, wählen Sie die Option **Warmstart**.

Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um den Neustart zu starten. Ein Fenster wird angezeigt, in dem Sie gefragt werden, ob das Gerät neu gestartet werden soll. Klicken Sie auf **OK**.

Klicken Sie auf die Schaltfläche **Änderungen verwerfen**, wenn Sie Ihre Änderungen rückgängig machen möchten.

Abbildung 5-36: Neustart

Registerkarte

Gateway

In diesem Fenster werden Informationen zu Ihrem Gateway und den WAN-Internetverbindungen angezeigt.

Gateway-Informationen

Im Bereich der Gateway-Informationen sind Angaben zur Software-Version, MAC-Adresse und zur derzeitigen Zeit enthalten.

Internetverbindungen

Nachdem Sie die Nummer der Internetverbindung aus dem Dropdown-Menü ausgewählt haben, werden die Optionen der Internetverbindungen angezeigt. Dabei handelt es sich um **Anmeldetyp**, **Schnittstelle**, **IP-Adresse**, **Subnetzmaske**, **Standard-Gateway** und die Server **DNS 1**, **2** und **3**.

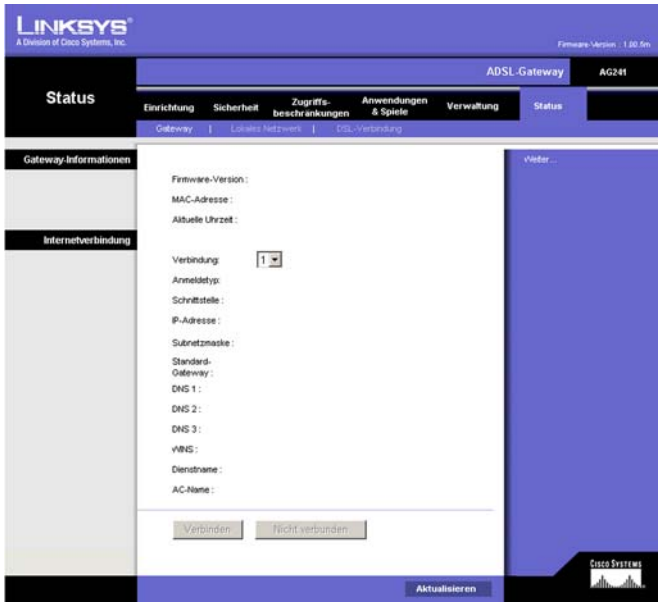


Abbildung 5-37: Status

DHCP erneuern: Klicken Sie auf die Schaltfläche **DHCP erneuern**, um die aktuelle IP-Adresse Ihres Gateways durch eine neue IP-Adresse zu ersetzen.

DHCP löschen: Klicken Sie auf die Schaltfläche **DHCP löschen**, um die aktuelle IP-Adresse Ihres Gateways zu löschen.

Klicken Sie auf die Schaltfläche Aktualisieren, um die Anzeige zu aktualisieren.

Lokales Netzwerk

Im Bereich der Angaben zum lokalen Netzwerk sind Informationen zur lokalen Mac-Adresse, IP-Adresse, Subnetzmaske, DHCP-Server und zur End-IP-Adresse aufgeführt. Um die DHCP-Client-Tabelle anzuzeigen, klicken Sie auf die Schaltfläche **DHCP-Client-Tabelle**.

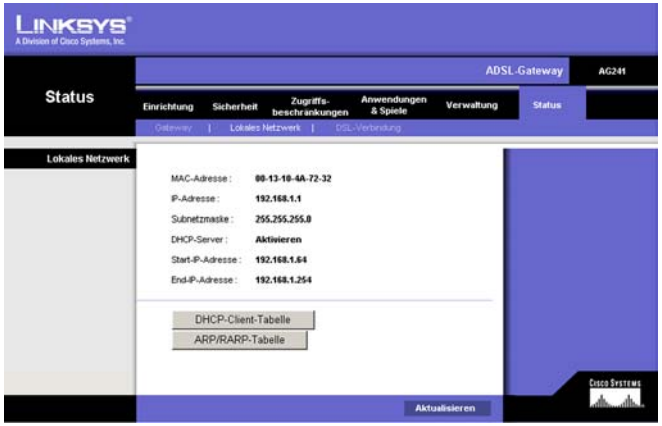


Abbildung 5-38: Lokales Netzwerk

DHCP-Client-Tabelle: Klicken Sie auf die Schaltfläche **DHCP-Client-Tabelle**, um die aktuellen DHCP-Client-Daten aufzurufen. In diesem Bereich sind MAC-Adresse, Computername sowie IP-Adresse der Netzwerk-Clients, die den DHCP-Server verwenden, aufgeführt. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Um einen Client vom DHCP-Server zu löschen, wählen Sie den entsprechenden Client aus, und klicken Sie anschließend auf die Schaltfläche **Löschen**.

Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Anzeige zu aktualisieren. Klicken Sie auf die Schaltfläche **Schließen**, um das Fenster zu schließen.

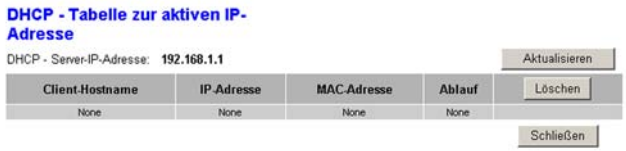


Abbildung 5-39: DHCP-Client-Tabelle

DSL-Verbindung

Die angezeigten DSL-Verbindungsinformationen beziehen sich auf den Status, die Downstream- und die Upstream-Rate.

Im Bereich der PVC-Verbindung sind folgende Informationen aufgeführt: Kapselungsmethode, Multiplexing, QoS (*Quality of Service*; Dienstqualität), PCR-Rate, SCR-Rate, automatische Erkennungsfunktion, VPI (*Virtual Path Identifier*; Virtueller Pfadidentifizierer), VCI (*Virtual Channel Identifier*; Virtueller Kanalidentifizierer) sowie PVC-Status.

Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Anzeige zu aktualisieren.

Abbildung 5-40: 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 in 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 die Option **DNS** aktiviert ist. Geben Sie den Host- und den Domänennamen 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 Ihren 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 Ihren 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)**. 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 Ihren Computer neu.

B. Öffnen Sie eine Eingabeaufforderung.

Für Benutzer von Windows 98 und ME:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie in das Feld **Öffnen** den Eintrag **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 in die Eingabeaufforderung den Eintrag **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 in die Eingabeaufforderung den Eintrag **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 den Eintrag **ping 1.2.3.4** eingeben und anschließend die Eingabetaste drücken.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Gateway verbunden.
- Wenn Sie KEINE Antwort erhalten, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

D. Geben Sie in die Eingabeaufforderung den Eintrag **ping www.yahoo.com** ein, und drücken Sie die Eingabetaste.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Internet verbunden. Wenn Sie KEINE Website öffnen können, geben Sie den Ping-Befehl über einen 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 über einen 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-Übertragung), RFC 2516 PPPoE oder RFC 2364 PPPoA. Weitere Einzelheiten zu den Einstellungen für die Internetverbindung finden Sie in "Kapitel 5: Konfigurieren des Gateways" im Abschnitt zur Einrichtung.
  2. Stellen Sie sicher, dass Sie das richtige Kabel verwenden. Überprüfen Sie, ob in der Spalte für das Gateway die ADSL-LED konstant leuchtet.
  3. Stellen Sie sicher, dass das an den ADSL-Port Ihres Gateways angeschlossene Kabel in die Wandbuchse der ADSL-Verbindung eingesteckt ist. Überprüfen Sie, ob in der Statusseite des webbasierten Dienstprogramms des Gateways eine gültige IP-Adresse Ihres 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 auf die Einrichtungsseite des webbasierten Dienstprogramms des Gateways nicht zugreifen.

- Informationen zur Überprüfung einer ordnungsgemäßen Verbindung des Computers mit dem Gateway finden Sie unter "2. Ich möchte meine Internetverbindung prüfen".
  1. Weitere Informationen dazu, ob Ihr Computer eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS besitzt, finden Sie in "Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters".
  2. Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter "1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?".
  3. Folgen Sie den 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 in 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 **Einrichtung**.
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie seine 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 Port 500/UDP-Pakete 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 Port-Weiterleitung über das webbasierte Dienstprogramm des Gateways einzurichten. Im Folgenden finden Sie Anweisungen zum Einrichten von Web-, FTP- und Mail-Servern.
  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 **Anwendungen und Spiele** die Registerkarte **Weiterleitung an einen Anschlussbereich** auf.
  2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
  3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Wenn Sie beispielsweise einen Webserver verwenden, legen Sie den Bereich zwischen 80 und 80 fest.
  4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
  5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-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 **Aktivieren**. Beachten Sie folgendes 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 **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. kein Port-Forwarding bzw. kein DMZ-Hosting notwendig. In einigen Fällen müssen Sie u. U. das Hosting für Online-Spiele oder Internetanwendungen anwenden. Dafür 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 **Anwendungen und Spiele** die Registerkarte **Weiterleitung an einen Anschlussbereich** auf.
2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Um beispielsweise Unreal Tournament (UT) auszuführen, müssen Sie den Bereich von 7777 bis 27900 eingeben.
4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-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 **Aktivieren**. Beachten Sie folgendes Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
UT	7777 bis 27900	X	X	192.168.1.100	X
Halflife	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 **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-Hosting (*DeMilitarized Zone*) 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 Forwarding-Einträge deaktiviert sind, um das DMZ-Hosting erfolgreich zu verwenden, da das Forwarding Vorrang vor dem DMZ-Hosting hat. (Mit anderen Worten: In dem Gateway eingehende Daten werden zuerst hinsichtlich ihrer Forwarding-Einstellungen überprüft. Falls die Daten von einer Port-Nummer eingehen, für die kein Port-Forwarding 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 **Anwendungen und Spiele** die Registerkarte **DMZ** auf. Wählen Sie **Aktiviert** aus, und geben Sie die IP-Adresse des Computers ein.
  2. Überprüfen Sie die Seiten zum Port-Forwarding, und deaktivieren bzw. entfernen Sie die Einträge zum Forwarding. Speichern Sie diese Informationen, falls Sie sie zu einem späteren Zeitpunkt verwenden möchten.
- Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **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 **Verwaltung** die Registerkarte **Verwaltungsfunktionen** auf.
  2. Geben Sie in das Feld für das Gateway-Passwort ein anderes Passwort ein. Geben Sie anschließend das gleiche Passwort in das zweite Feld ein, um es dadurch zu bestätigen.
  3. Klicken Sie auf die Schaltfläche **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 Benutzer von Netscape 4.7 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 Forwarding-Funktion sowie weitere Einstellungen des Gateways auf die Werkseinstellungen zurückgesetzt. Anders ausgedrückt: Das Gateway greift auf die werkseitigen Konfigurationseinstellungen zurück.

12. Ich möchte die Firmware aktualisieren.

Um die aktuellsten Funktionen für Ihre Firmware zu erhalten, gehen Sie auf die internationale Website von Linksys und laden Sie die neueste Firmware unter www.linksys.com/international 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 **Produkte**, 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. Um die Firmware zu aktualisieren, führen Sie die in "Kapitel 5: Konfigurieren des Gateways" im Abschnitt **Verwaltung** aufgeführten Schritte durch.

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 eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie 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 der Registerkarte **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 Einrichtungsoption 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 Setup-Fenster die Option **Verbindung aufrechterhalten** aus, und legen Sie für die Option **Wahlwiederholung** 20 Sekunden fest.
  4. Klicken Sie auf die Schaltfläche **Einstellungen speichern**. Klicken Sie auf die Registerkarte **Status**, und klicken Sie auf Schaltfläche **Verbinden**.
  5. Möglicherweise wird **Verbindung wird hergestellt** als Anmeldestatus angezeigt. Drücken Sie die F5-Taste, um den Bildschirm zu aktualisieren, bis **Verbunden** als Anmeldestatus angezeigt wird.
  6. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um fortzufahren.
- Falls die Verbindung erneut unterbrochen wird, führen Sie die Schritte 1 bis 6 aus, um die Verbindung wiederherzustellen.

15. Ich kann weder auf meine E-Mail noch auf das Internet oder auf das VPN zugreifen, oder ich bekomme 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 **Manuell** aus. Geben Sie in das Feld Size (Größe) den Wert **1492** ein.
  4. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um fortzufahren.
- Wenn das Problem weiterhin besteht, ändern Sie den MTU-Wert in einen anderen Wert. Verwenden Sie aus der folgenden Liste jeweils einen Wert in der angegebenen Reihenfolge, bis Ihr Problem gelöst ist:
  1462
  1400
  1362
  1300

16. Die Netzstrom-LED leuchtet durchgehend.

Die Netzstrom-LED leuchtet auf, wenn das Gerät erstmals eingeschaltet wird. Zwischenzeitlich fährt der Computer hoch und wird auf einen ordnungsgemäßen Betrieb hin geprüft. Nach dem Überprüfungsvorgang leuchtet die LED konstant, wodurch der ordnungsgemäße Betrieb angezeigt wird. Wenn die LED immer noch blinkt, funktioniert das Gerät nicht ordnungsgemäß. Führen Sie einen Firmware-Flash durch, indem Sie dem Computer eine statische IP-Adresse zuweisen, und aktualisieren Sie anschließend die Firmware. 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, bei dem das Problem aufgetreten ist, erneut.
- 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 Gateway 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.

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 der ADSL-Wandbuchse und dem LAN installiert.

Unterstützt das Gateway IPX oder AppleTalk?
Nein. TCP/IP ist der einzige Internet-Protokollstandard 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 mit einem 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 Sicherheitsstufe 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 Adressen hinter einer einzigen vom ISP zur Verfügung gestellten 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 folgende Schritte dazu aus: Klicken Sie auf das Menü **ICQ**, dann auf **Einstellungen** und auf die Registerkarte **Verbindungen**. Aktivieren Sie dann die Option **Ich bin hinter einer Firewall oder einem Proxy**. Legen Sie nun in den Einstellungen für die Firewall 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 sich jedoch nicht mit dem Server verbinden. 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 einen weiteren Port weiterleiten. (Das kann Port 8080 sein, der jedoch für die Remote-Verwaltung verwendet wird. Sie müssen u. U. diese Funktion 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 den gleichen CD-Schlüssel 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 Ausführen 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 Website reagiert nicht, heruntergeladene Dateien sind beschädigt, oder es werden nur unleserliche Zeichen auf dem Bildschirm angezeigt. Was muss ich tun?
Legen Sie für Ihren Ethernet-Adapter 10 Mbit/s bzw. den Halbduplex-Modus fest, und deaktivieren Sie als vorübergehende Maßnahme für den Ethernet-Adapter die Funktion zur automatischen Aushandlung. (Rufen Sie über die Netzwerksystemsteuerung die Registerkarte für die erweiterten Eigenschaften 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 Reset-Taste drücken, bis die Netzstrom-LED aufleuchtet und wieder erlischt. Setzen Sie das DSL-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 Linksys-Firmware 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 **Administration** (Verwaltung) 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 Einrichtungsseiten 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 Benutzer als auch Gateway die öffentliche IP-Adresse?
Nein.

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-Weiterleitung, Routing und DDNS.

Wie viele VPN-Sitzungen unterstützt das Gateway maximal?
Die maximale Anzahl hängt von vielen Faktoren ab. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen. Je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
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 in der Registerkarte **Port Forwarding** (Port-Forwarding) 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.

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 Reset-Taste auf der Rückseite des Gateways ca. 10 Sekunden lang gedrückt. Dadurch wird das Gateway auf die Werkseinstellungen zurückgesetzt.

Wenn Ihre Fragen hier nicht beantwortet wurden, finden Sie weitere Informationen auf der internationalen Linksys-Website unter www.linksys.com/international.

Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem Gateway

Einführung

In diesem Dokument finden Sie Anweisungen dazu, wie Sie über vorläufige gemeinsame Schlüssel einen sicheren IPSec-Tunnel einrichten, um ein privates Netzwerk innerhalb des VPN-Gateways mit einem Windows 2000- oder Windows XP-Computer zu verbinden. Detaillierte Informationen zur Konfiguration von Windows 2000-Servern finden Sie auf der Website von Microsoft:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

HINWEIS: Zeichnen und bewahren Sie sämtliche von Ihnen vorgenommenen Änderungen auf. Diese Änderungen sind für die Windows-Anwendung "secpol" und dem webbasierten Dienstprogramm des Routers identisch.

Umgebung

Die hier erwähnten IP-Adressen und weiteren Einstellungen sind lediglich zu Darstellungszwecken aufgeführt.

HINWEIS: Die Anweisungen und Abbildungen in diesem Abschnitt der Anleitung beziehen sich auf den Router. Ersetzen Sie "Router" durch "Gateway". Die Optionen "OK" bzw. "Schließen" können in den auf Ihrem Computer angezeigten Fenstern vom Text in der Anleitung abweichen; klicken Sie auf die Ihrem Fenster entsprechende Schaltfläche.

Windows 2000 oder Windows XP
IP-Adresse: 140.111.1.2 <= Die IP-Adresse wird vom ISP des Benutzers zur Verfügung gestellt; die hier aufgeführte IP-Adresse dient lediglich als Beispiel.

Subnetzmaske: 255.255.255.0

AG241

WAN-IP-Adresse: 140.111.1.1 <= Die IP-Adresse wird vom ISP des Benutzers zur Verfügung gestellt; die hier aufgeführte WAN-IP-Adresse dient lediglich als Beispiel.

Subnetzmaske: 255.255.255.0
LAN-IP-Adresse: 192.168.1.1
Subnetzmaske: 255.255.255.0

Hinweise zum Einrichten eines sicheren IPSec-Tunnels

Schritt 1: Erstellen einer IPSec-Richtlinie

1. Klicken Sie auf die Schaltfläche **Start**, wählen Sie **Ausführen** aus, und geben Sie in das Feld **Öffnen** den Eintrag **secpol.msc** ein. Das in Abbildung B-1 dargestellte Fenster *Lokale Sicherheitseinstellungen* wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf Lokaler Computer** (Win XP) bzw. auf **IP-Sicherheitsrichtlinien auf lokalem Computer** (Win 2000), und wählen Sie anschließend **IP-Sicherheitsrichtlinie erstellen** aus.

3. Klicken Sie auf die Schaltfläche **Weiter**, und geben Sie für Ihre Richtlinie einen Namen ein (zum Beispiel "an_Router"). Klicken Sie anschließend auf **Weiter**.

4. Deaktivieren Sie das Kontrollkästchen **Die Standardantwortregel aktivieren**, und klicken Sie anschließend auf die Schaltfläche **Weiter**.

5. Klicken Sie auf die Schaltfläche **Fertig stellen**, und vergewissern Sie sich, dass das Kontrollkästchen **Eigenschaften bearbeiten** aktiviert ist.

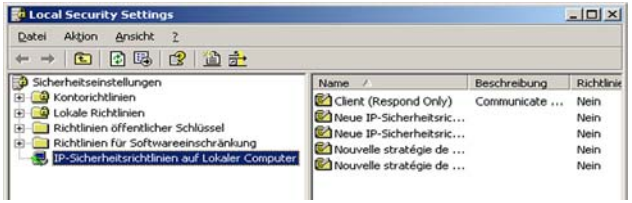


Abbildung B-1: Fenster "Lokale Sicherheitseinstellungen"

HINWEIS: Jeder Bezug in diesem Kapitel auf "win" verweist auf Windows 2000 und Windows XP. Ersetzen Sie die Hinweise auf "Router" durch "Gateway". Die Optionen "OK" bzw. "Schließen" können in den auf Ihrem Computer angezeigten Fenstern vom Text in der Anleitung abweichen; klicken Sie auf die Ihrem Fenster entsprechende Schaltfläche.

Schritt 2: Erstellen von Filterlisten

Filterliste 1: win->Router

1. Vergewissern Sie sich, dass im Fenster für die Eigenschaften der neuen Richtlinie die Registerkarte **Regeln** ausgewählt ist (siehe Abbildung B-2). Deaktivieren Sie das Kontrollkästchen **Assistent verwenden**, und klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel zu erstellen.

2. Stellen Sie sicher, dass die Registerkarte **IP-Filterliste** ausgewählt ist, und klicken Sie auf die Schaltfläche **Hinzufügen** (siehe Abbildung B-3). Das Fenster *IP-Filterliste* wird angezeigt (siehe Abbildung B-4). Geben Sie für die Filterliste einen geeigneten Namen, wie z. B. win -> Router, ein, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

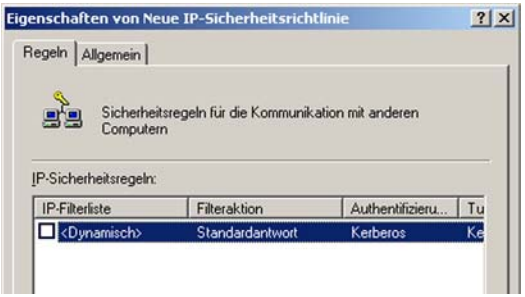


Abbildung B-2: Registerkarte "Regeln"

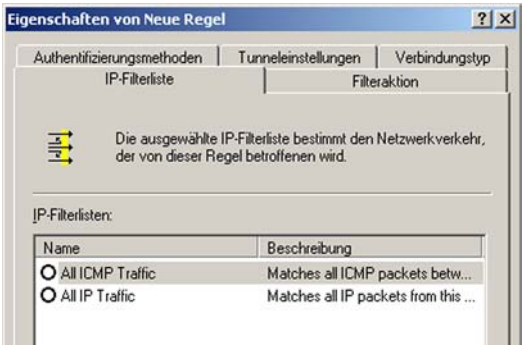


Abbildung B-3: Registerkarte "IP-Filterliste"

3. Das Fenster für die Filtereigenschaften wird angezeigt (siehe Abbildung B-5).Wählen Sie die Registerkarte **Adressierung**. Wählen Sie im Feld **Quelladresse** die Option **Eigene IP-Adresse** aus. Wählen Sie im Feld **Zieladresse** die Option **Spezielles IP-Subnetz** aus, und geben Sie die IP-Adresse. 192.168.1.0 und Subnetzmaske 255.255.255.0 ein. (Dabei handelt es sich um die Standardeinstellungen des Routers. Falls Sie an diesen Einstellungen Änderungen vorgenommen haben, geben Sie die geänderten Werte ein.)

4. Wenn Sie eine Beschreibung für Ihren Filter eingeben möchten, klicken Sie auf die Registerkarte **Beschreibung** und geben die Beschreibung ein.

5. Klicken Sie auf **OK**. Klicken Sie anschließend im Fenster *Filterliste* auf die Schaltfläche **OK** bzw. **Schließen**.

Filterliste 2: Router ->win

6. Das Fenster *Eigenschaften von Neue Regel* wird angezeigt (siehe Abbildung B-6). Wählen Sie die Registerkarte **IP-Filterliste** aus, und stellen Sie sicher, dass **win -> Router** markiert ist. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

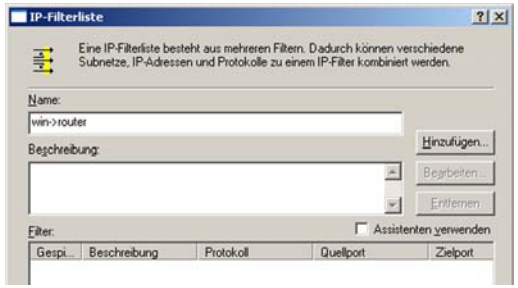


Abbildung B-4: Dialogfeld "IP-Filterliste"

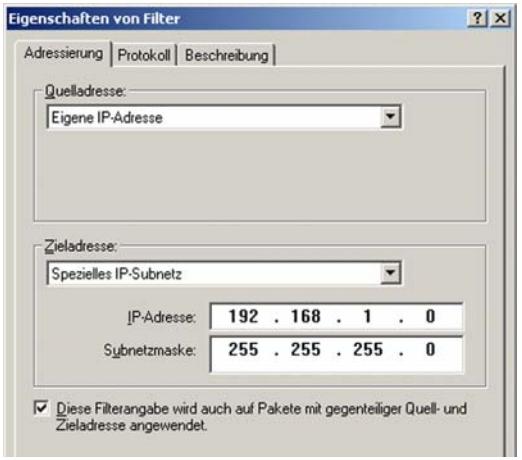


Abbildung B-5: Dialogfeld "Eigenschaften von Filter"

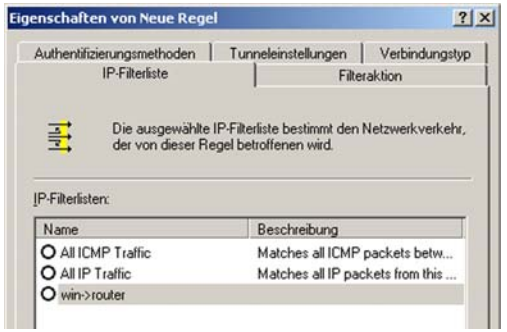


Abbildung B-6: Dialogfeld "Eigenschaften von Neue Regel"

7. Das Fenster *IP-Filterliste* wird angezeigt (siehe Abbildung B-7). Geben Sie für die Filterliste einen geeigneten Namen, z. B. Router->win, ein, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

8. Das Fenster für die Filtereigenschaften wird angezeigt (siehe Abbildung B-8). Wählen Sie die Registerkarte **Adressierung**. Wählen Sie im Feld **Quelladresse** die Option **Spezielles IP-Subnetz** aus, und geben Sie die IP-Adresse 192.168.1.0 und Subnetzmaske 255.255.255.0 ein. (Falls Sie an diesen Standardeinstellungen Änderungen vorgenommen haben, geben Sie hier die neuen Werte ein.) Wählen Sie im Feld **Zieladresse** die Option **Eigene IP-Adresse** aus.

9. Wenn Sie eine Beschreibung für Ihren Filter eingeben möchten, klicken Sie auf die Registerkarte **Beschreibung** und geben die Beschreibung ein.

10. Klicken Sie auf die Schaltfläche **OK** bzw. **Schließen**, woraufhin das Fenster *Eigenschaften von Neue Regel* angezeigt wird und die Registerkarte **IP-Filterliste** ausgewählt ist (siehe Abbildung B-9). Hier sollte der Listeneintrag "Router -> win" und "win -> Router" aufgeführt sein. Klicken Sie im Fenster *IP-Filterliste* auf die Schaltfläche **OK** (unter Windows XP) bzw. die Schaltfläche **Schließen** (unter Windows 2000).

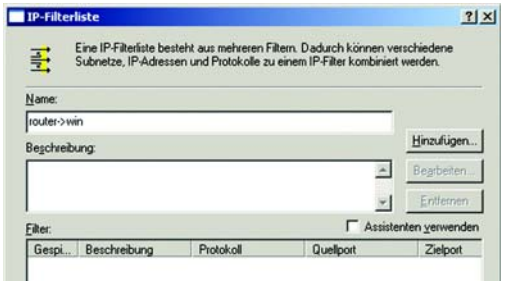


Abbildung B-7: Dialogfeld "IP-Filterliste"

Abbildung B-8: Dialogfeld "Eigenschaften von Filter"

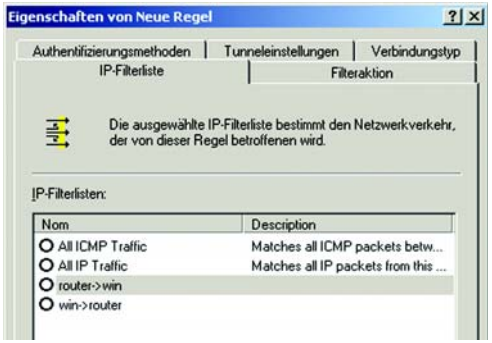


Abbildung B-9: Dialogfeld "Eigenschaften von Neue Regel"

Schritt 3: Konfigurieren von individuellen Tunnelregeln

Tunnel 1: win->Router

1. Klicken Sie, wie in Abbildung B-10 dargestellt, auf die Registerkarte **IP-Filterliste** und anschließend auf die Filterliste "win -> Router".

2. Klicken Sie auf die Registerkarte **Filteraktion** (siehe Abbildung B-11), und klicken Sie auf die für die Filteraktion erforderliche Optionsschaltfläche **Sicherheit erforderlich**. Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**.

3. Stellen Sie in der Registerkarte **Sicherheitsmethoden** (siehe Abbildung B-12) sicher, dass die Option **Sicherheit aushandeln** aktiviert ist, und deaktivieren Sie das Kontrollkästchen **Unsichere Kommunikat. annehmen, aber immer mit IPSec antworten**. Wählen Sie die Option **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)** aus, und klicken Sie auf die Schaltfläche **OK**.

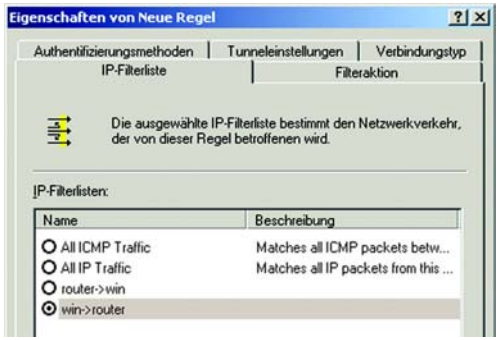


Abbildung B-10: Registerkarte "IP-Filterliste"

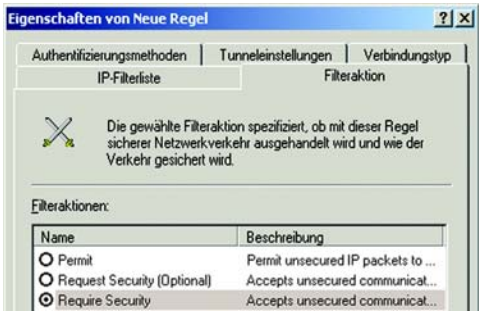


Abbildung B-11: Registerkarte "Filteraktion"

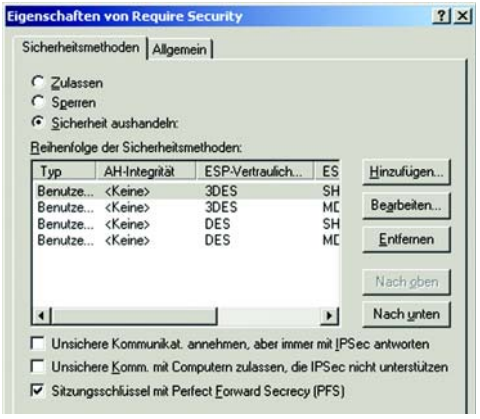


Abbildung B-12: Registerkarte "Sicherheitsmethoden"

4. Klicken Sie auf die Registerkarte **Authentifizierungsmethoden** (siehe Abbildung B-13), und klicken Sie auf die Schaltfläche **Bearbeiten**.

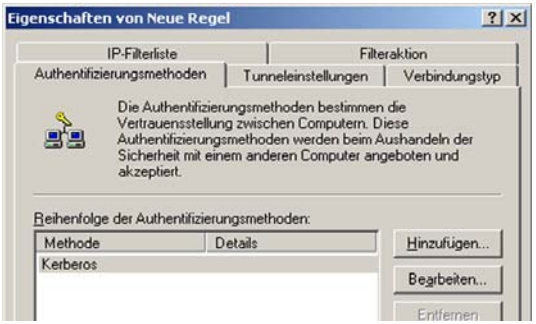


Abbildung B-13: Registerkarte "Authentifizierungsmethoden"

5. Ändern Sie die Authentifizierungsmethode auf **Diese Zeichenkette (vorinstallierter Schlüssel) verwenden** (siehe Abbildung B-14), und geben Sie die Zeichenkette für den vorinstallierten Schlüssel, z. B. XYZ12345, ein. Klicken Sie auf **OK**.

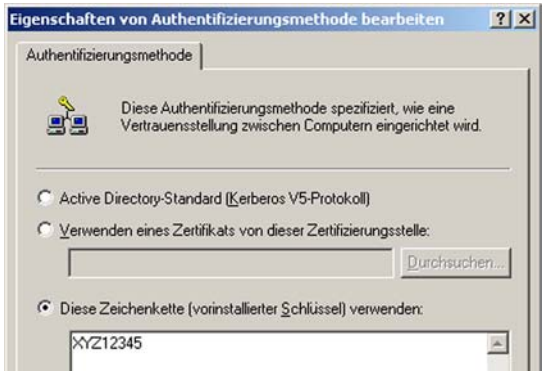


Abbildung B-14: Vorinstallierter Schlüssel

6. Dieser neue vorinstallierte Schlüssel ist in Abbildung B-15 aufgeführt. Klicken Sie gegebenenfalls auf die Schaltfläche **Übernehmen**, um fortzufahren; andernfalls fahren Sie mit dem nächsten Schritt fort.

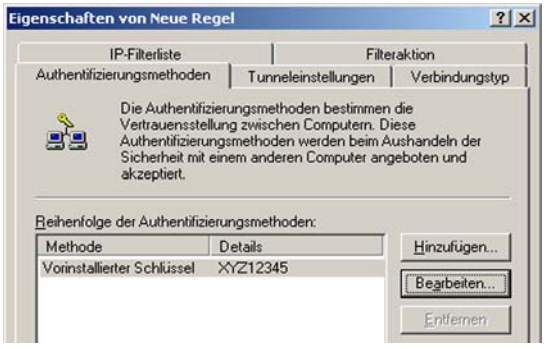


Abbildung B-15: Neuer vorinstallierter Schlüssel

7. Wählen Sie die Registerkarte **Tunneleinstellungen** (siehe Abbildung B-16), und aktivieren Sie die Optionsschaltfläche **Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert**. Geben Sie anschließend die WAN-IP-Adresse des Routers ein.

Abbildung B-16: Registerkarte "Tunneleinstellungen"

8. Wählen Sie die Registerkarte **Verbindungstyp** (siehe Abbildung B-17), und klicken Sie auf **Alle Netzwerkverbindungen**. Klicken Sie anschließend auf die Schaltfläche **OK** bzw. auf **Schließen**, um diese Regel abzuschließen.

Abbildung B-17: Registerkarte "Verbindungstyp"

Tunnel 2: Router->win

9. Vergewissern Sie sich, dass im Dialogfeld für die Eigenschaften der neuen Richtlinie (siehe Abbildung B-18) der Eintrag "win -> Router" ausgewählt ist, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um einen zweiten IP-Filter zu erstellen.

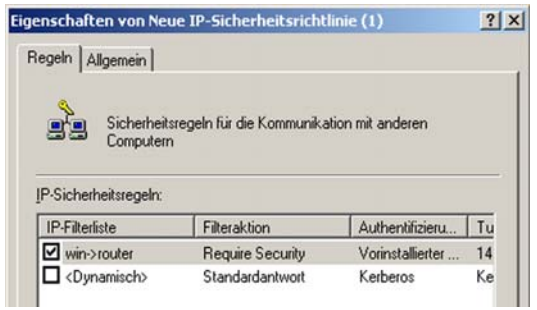


Abbildung B-18: Fenster für die Eigenschaften der neuen Richtlinie

10. Aktivieren Sie in der Registerkarte **IP-Filterliste** die Optionsschaltfläche für die Filterliste **Router -> win** (siehe Abbildung B-19).

11. Klicken Sie auf die Registerkarte **Filteraktion**, und wählen Sie die Filteraktion **Sicherheit erforderlich** aus (siehe Abbildung B-20). Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**. Stellen Sie in der Registerkarte **Sicherheitsmethoden** (siehe Abbildung B-12) sicher, dass die Option **Sicherheit aushandeln** aktiviert ist, und deaktivieren Sie das Kontrollkästchen **Unsichere Kommunikat. annehmen, aber immer mit IPSec antworten**. Wählen Sie die Option **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)** aus, und klicken Sie auf die Schaltfläche **OK**.

12. Klicken Sie auf die Registerkarte **Authentifizierungsmethoden**, und stellen Sie sicher, dass die Kerberos-Authentifizierungsmethode aktiviert ist (siehe Abbildung B-21). Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**.

Abbildung B-19: Registerkarte "IP-Filterliste"

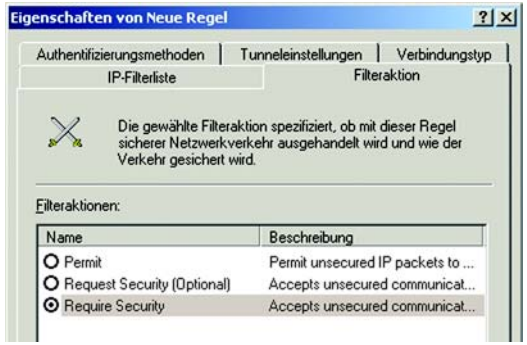


Abbildung B-20: Registerkarte "Filteraktion"

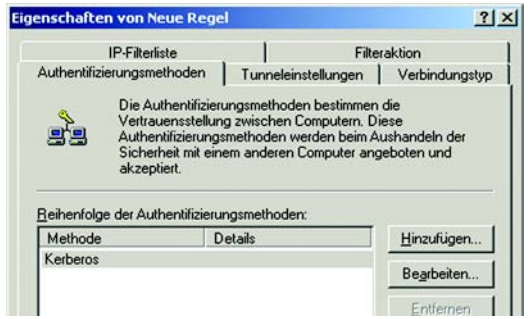


Abbildung B-21: Registerkarte "Authentifizierungsmethode"

13. Ändern Sie die Authentifizierungsmethode auf **Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden** (siehe Abbildung B-22), und geben Sie die Zeichenkette für den vorinstallierten Schlüssel, z. B. XYZ12345, ein. (Die hier aufgeführte Schlüsselzeichenkette dient als Beispiel. Ihre Schlüsselzeichenkette sollte eindeutig und leicht zu merken sein.) Klicken Sie anschließend auf die Schaltfläche **OK**.

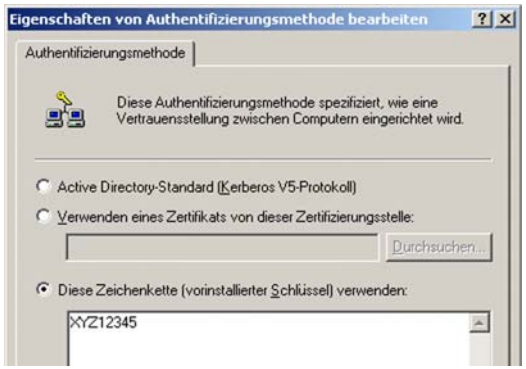


Abbildung B-22: Vorinstallierter Schlüssel

14. Dieser neue vorinstallierte Schlüssel ist in Abbildung B-23 aufgeführt. Klicken Sie gegebenenfalls auf die Schaltfläche **Übernehmen**, um fortzufahren; andernfalls fahren Sie mit dem nächsten Schritt fort.

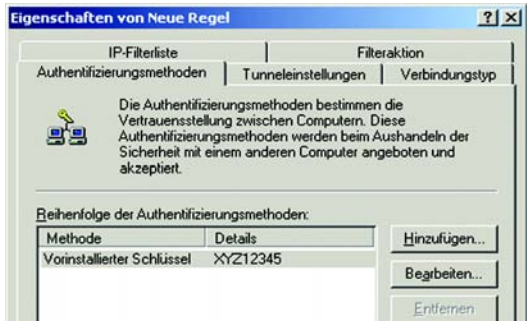


Abbildung B-23: Neuer vorinstallierter Schlüssel

15. Aktivieren Sie in der Registerkarte **Tunneleinstellungen** (siehe Abbildung B-24) die Optionsschaltfläche **Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert**, und geben Sie die IP-Adresse des Computers ein, auf dem Windows 2000 bzw. Windows XP verwendet wird.

Abbildung B-24: Registerkarte "Tunneleinstellungen"

16. Klicken Sie auf die Registerkarte **Verbindungstyp** (siehe Abbildung B-25), und klicken Sie auf **Alle Netzwerkverbindungen**. Klicken Sie anschließend auf die Schaltfläche **OK** bzw. auf **Schließen**, um den Vorgang zu beenden.

17. Klicken Sie in der Registerkarte **Regeln** (siehe Abbildung B-26) auf die Schaltfläche **OK** bzw. auf **Schließen**, um zum secpol-Bildschirm zurückzukehren.

Abbildung B-25: Registerkarte "Verbindungstyp"

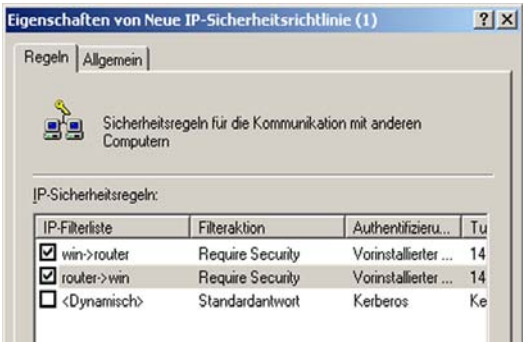


Abbildung B-26: Registerkarte "Regeln"

Schritt 4: Zuweisen einer neuen IPSec-Richtlinie

Klicken Sie im Bereich **Struktur** auf den Eintrag **IP-Sicherheitsrichtlinien auf lokalem Computer** (Abbildung B-27) und anschließend mit der rechten Maustaste auf die Richtlinie "an_Router". Klicken Sie nun auf die Option **Zuweisen**. Im Ordnersymbol wird ein grüner Pfeil angezeigt.

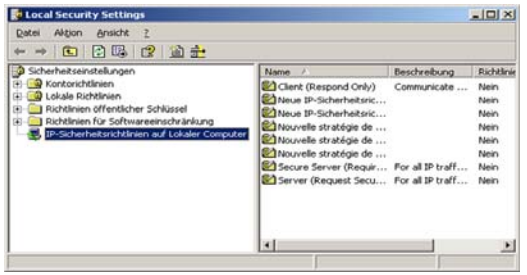


Abbildung B-27: Dialogfeld "Lokale Sicherheitseinstellungen"

Schritt 5: Erstellen eines Tunnels mithilfe des webbasierten Dienstprogramms

1. Geben Sie im Adressfeld des Web-Browsers **192.168.1.1** ein. Drücken Sie die Eingabetaste.
2. Wenn die Felder für den Benutzernamen und das Passwort angezeigt werden, geben Sie den Standardbenutzernamen und das Standardpasswort **admin** ein. Drücken Sie die Eingabetaste.
3. Klicken Sie in der Registerkarte **Setup** (Einrichtung) auf die Registerkarte **VPN**.
4. Wählen Sie in der Registerkarte **VPN**, wie in Abbildung B-28 dargestellt, den zu erstellenden Tunnel aus der Dropdown-Liste **Tunneleintrag auswählen** aus. Klicken Sie dann auf **Aktivieren**. Geben Sie im Feld **Tunnelname** den Namen des Tunnels ein. Auf diese Weise können Sie die verschiedenen Tunnel erkennen. Der eingegebene Name muss nicht dem Namen entsprechen, der am anderen Ende des Tunnels verwendet wird.
5. Geben Sie im Feld **Lokale sichere Gruppe** die IP-Adresse und Subnetzmaske des lokalen VPN-Routers ein. Geben für den letzten IP-Adressensatz **0** ein, um das gesamte IP-Subnetz freizugeben (z. B. 192.168.1.0).
6. Geben Sie im Feld **Entfernter Sicherheits-Router** die IP-Adresse und die Subnetzmaske des VPN-Geräts am anderen Ende des Tunnels ein (der entfernte VPN-Router oder das Gerät, mit dem Sie kommunizieren möchten).
7. Wählen Sie aus zwei unterschiedlichen Verschlüsselungstypen aus: **DES** und **3DES** (empfohlen wird **3DES**, da dieser Typ sicherer ist). Sie können einen der beiden Typen wählen; die Einstellung muss jedoch mit dem Verschlüsselungstyp übereinstimmen, der vom VPN-Gerät am anderen Ende des Tunnels verwendet wird. Sie können aber auch ohne Verschlüsselung arbeiten, indem Sie **Deaktivieren** auswählen.
8. Wählen Sie aus zwei Authentifizierungstypen aus: **MD5** und **SHA** (empfohlen wird **SHA**, da dieser Typ sicherer ist). Wie bei der Verschlüsselung kann einer der beiden Typen gewählt werden, vorausgesetzt, das VPN-Gerät am anderen Ende des Tunnels verwendet denselben Authentifizierungstyp. Die Authentifizierung kann aber auch mit **Disable** (Deaktivieren) an beiden Enden des Tunnels deaktiviert werden.
9. Wählen Sie die Schlüsselverwaltung aus. Wählen Sie **Auto (IKE)**, und geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld **Vorläufiger gemeinsamer Schlüssel** ein. Markieren Sie das Kontrollkästchen neben **PFS** (Perfect Forward Secrecy) [Vollständige Geheimhaltung bei Weiterleitung], um sicherzustellen, dass der erste Schlüsselaustausch und die IKE-Vorschläge sicher sind. Sie können in diesem Feld eine Kombination aus bis zu 24 Zahlen und Buchstaben eingeben. Es dürfen keine Sonderzeichen oder Leerzeichen verwendet werden. Im Feld **Schlüssel-Verwendungsdauer** 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.
10. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um die Änderungen zu speichern.

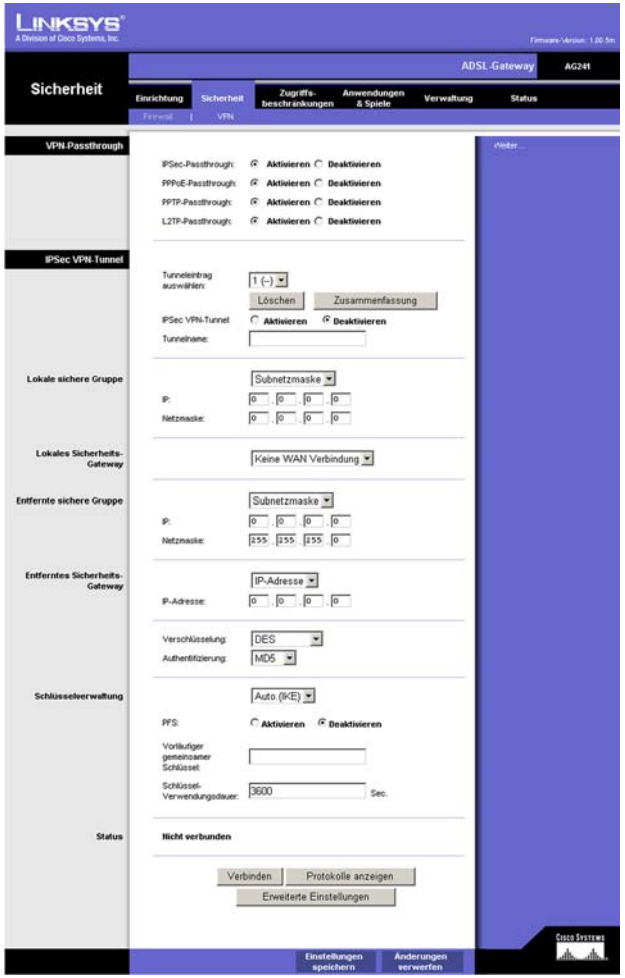


Abbildung B-28: Registerkarte "VPN"

Der Tunnel ist nun hergestellt.

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-, Forwarding- 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 Configuration* (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 auf dem Bildschirm Ihres Computers angezeigt wird (siehe Abbildung C-2). Sie bildet die MAC-Adresse Ihres Ethernet-Adapters und wird im hexadezimalen Format als Folge von Zahlen 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 dem 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 dem Computer angezeigte Adresse kann davon abweichen.

Hinweis: Die MAC-Adresse wird auch als Adapteradresse bezeichnet.

Abbildung C-1: Fenster 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 physikalische Adresse bezeichnet.

2. Geben Sie in die Eingabeaufforderung **ipconfig /all** ein. Drücken Sie die Eingabetaste.

3. Notieren Sie die physikalische Adresse so, wie sie am Computer anzeigt wird (Abbildung C-3). Diese Adresse stellt die MAC-Adresse Ihres Ethernet-Adapters dar. Sie wird als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/physikalische 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 dem 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 dem Computer angezeigte Adresse kann davon abweichen.

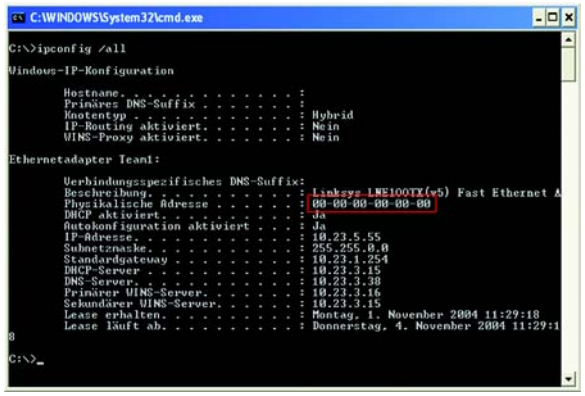


Abbildung C-3: MAC-Adresse/physikalische Adresse

Anhang D: Glossar

802.11a: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 Mbit/s sowie eine Betriebsfrequenz von 5 GHz festlegt.

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.

Access Point: Gerät, über das Computer und andere Geräte mit Wireless-Funktionalität mit einem Kabelnetzwerk kommunizieren können. Wird auch verwendet, um die Reichweite von Wireless-Netzwerken zu erweitern.

Adapter: Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhält.

Ad-Hoc: Eine Gruppe von Wireless-Geräten, die statt über einen Access Point direkt miteinander kommunizieren (Peer-to-Peer).

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: Das Sendeintervall des Beacons, einer Paketübertragung eines Gateways zur Synchronisierung eines Wireless-Netzwerks.

Bit: Eine binäre Einheit.

Breitband: Eine stets aktive, schnelle Internetverbindung.

Bridge: Ein Gerät, das zwei verschiedene lokale Netzwerke verbindet, wie beispielsweise ein Wireless-Netzwerk mit einem verdrahteten Netzwerk.

Browser: Ein Browser ist eine Anwendung, mit der auf alle im World Wide Web enthaltenen Informationen zugegriffen werden kann.

CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*): Eine Datenübertragungsmethode, die verwendet wird, um Datenverluste im Netzwerk zu verhindern.

CTS (*Clear To Send*): Ein von einem 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 (*Dynamic Domain Name System*): System, in dem eine Website, ein FTP- oder E-Mail-Server mit einer dynamischen IP-Adresse einen festen Domänennamen verwenden kann.

DHCP (*Dynamic Host Configuration Protocol*): Ein Protokoll, das es einem Gerät in einem LAN (auch als DHCP-Server bezeichnet) ermöglicht, anderen Geräten im Netzwerk, in der Regel Computern, temporäre IP-Adressen zuzuweisen.

DMZ (*Demilitarized Zone*): Hebt den Firewall-Schutz des Gateways für einen Computer auf, sodass dieser im Internet "sichtbar" wird.

DNS (*Domain Name Server*): 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 (*Digital Subscriber Line*): Eine stets aktive Breitbandverbindung über herkömmliche Telefonleitungen.

DSSS (*Direct-Sequence Spread-Spectrum*): Eine bestimmte Art der Funkübertragungstechnologie, die ein redundantes Bit-Muster enthält, um die Wahrscheinlichkeit von Datenverlusten bei der Übertragung zu senken. Wird für 802.11b-Netzwerke verwendet.

DTIM (*Delivery Traffic Indication Message*): 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.

Ethernet: IEEE-Standardnetzwerkprotokoll, 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: Sicherheitsmaßnahmen, durch die die Ressourcen in einem lokalen Netzwerk vor dem Zugriff durch nicht autorisierte Dritte geschützt werden.

Firmware: 1. Die Programmierung in Netzwerkgeräten, mit der das Gerät gesteuert wird. 2. In den Lesespeicher (ROM) bzw. programmierbaren Lesespeicher (PROM) geladene Programmierung, die von Endbenutzern nicht geändert werden kann.

Fragmentierung: Das Aufteilen von Paketen in kleinere Einheiten bei der Übertragung über ein Netzwerkmedium, das die ursprüngliche Größe des Pakets nicht unterstützt.

FTP (*File Transfer Protocol*): Standardprotokoll für das Senden von Dateien zwischen Computern über ein TCP/IP-Netzwerk und das Internet.

Gateway: System zur Verbindung von Netzwerken untereinander.

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 (*HyperText Transport Protocol*): Kommunikationsprotokoll, das zum Anschließen von Servern an das World Wide Web verwendet wird.

IEEE (*The Institute of Electrical and Electronics Engineers*): Unabhängiges Institut, das Standards für den Netzwerkbetrieb entwickelt.

Infrastruktur: Die aktuell installierten Computer und Geräte im Netzwerk.

Infrastrukturmodus: Konfiguration, bei der ein Wireless-Netzwerk über einen Access Point mit einem verdrahteten Netzwerk verbunden ist.

IP (*Internet Protocol*): Zum Senden von Daten über das Netzwerk verwendetes Protokoll.

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 von bestimmten Geräten im Netzwerk anzeigt.

IPSec (*Internet Protocol Security*): VPN-Protokoll, das für den sicheren Austausch von Paketen auf der IP-Ebene verwendet wird.

ISM-Band: Bei Übertragungen im Wireless-Netzwerkbetrieb verwendetes Funkband.

ISP (*Internet Service Provider;* Internetdienstanbieter): 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 (*Local Area Network*): Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr Heim- oder Büronetzwerk zusammensetzt.

MAC-Adresse (*Media Access Control*): Die eindeutige Adresse, die ein Hersteller den einzelnen Netzwerkbetriebsgeräten zuweist.

Mbit/s (Megabit pro Sekunde): Eine Million Bit pro Sekunde. Messeinheit für die Datenübertragung.

Multicasting: Das gleichzeitige Senden von Daten an mehrere Ziele.

NAT (*Network Address Translation*): 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 (*Network News Transfer Protocol*): Das Protokoll, mit dem eine Verbindung zu Usenet-Gruppen im Internet hergestellt wird.

OFDM (*Orthogonal Frequency Division Multiplexing*): Eine bestimmte Art der Modulationstechnologie, bei der der Datenstrom in eine Reihe von Datenströmen mit geringerer Geschwindigkeit geteilt wird, die dann parallel

übertragen werden. Wird in 802.11a- und 802.11g-Netzwerken sowie beim Netzwerkbetrieb über Stromkabel verwendet.

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-Codierschlüssel erstellt werden.

Ping (*Packet INternet Groper*): Internetdienstprogramm, mit dem bestimmt werden kann, ob eine bestimmte IP-Adresse online ist.

POP3 (*Post Office Protocol 3*): Standardprotokoll, das zum Abrufen von E-Mails verwendet wird, die auf einem Mail-Server gespeichert sind.

Port: 1. Der Anschlusspunkt an einem Computer oder Netzwerkbetriebsgerät, an dem ein Kabel oder ein Adapter angeschlossen wird. 2. Der virtuelle Anschlusspunkt, über den ein Computer auf eine bestimmte Anwendung auf dem Server zugreift.

PPPoE (*Point to Point Protocol over Ethernet*): Eine Art Breitbandverbindung, die neben der Datenübertragung eine Authentifizierungsmöglichkeit (Benutzername und Passwort) bietet.

PPTP (*Point-to-Point Tunneling Protocol*): 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: Ein Speicherblock, der vorübergehend Daten zur späteren Bearbeitung zurückhält, wenn ein Gerät zum betreffenden Zeitpunkt zu beschäftigt ist, um die Daten zu empfangen.

RJ-45 (*Registered Jack-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 die Verbindung zu unterbrechen.

Router: Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden, wie beispielsweise das lokale Netzwerk und das Internet.

RTS (Request To Send): Ein Paket, das gesendet wird, wenn ein Computer über Daten zur Übertragung verfügt. Der Computer wartet den Eingang einer CTS-Mitteilung (*Clear To Send*) ab, bevor die Daten gesendet werden.

Server: Ein beliebiger Computer, der innerhalb eines Netzwerks dafür sorgt, dass Benutzer auf Dateien zugreifen, kommunizieren sowie Druckvorgänge und andere Aktionen ausführen können.

SMTP (*Simple Mail Transfer Protocol*): Das standardmäßige E-Mail-Protokoll im Internet.

SNMP (*Simple Network Management Protocol*): Ein weit verbreitetes und häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

Software: Befehle für den Computer. Eine Folge von Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, wird als "Programm" bezeichnet.

SSID (*Service Set IDentifier*): 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. Gerät, das den zentralen Verbindungspunkt für Computer und andere Geräte in einem Netzwerk darstellt, sodass Daten bei voller Übertragungsgeschwindigkeit gemeinsam genutzt werden können. 2. Ein Gerät zum Herstellen, Trennen und Ändern der Verbindungen innerhalb von elektrischen Schaltkreisen.

TCP/IP (*Transmission Control Protocol/Internet Protocol*): Ein Netzwerkprotokoll zum Übertragen von Daten, bei dem eine Bestätigung des Empfängers der gesendeten Daten erforderlich ist.

Telnet: Benutzerbefehl und TCP/IP-Protokoll zum Zugriff auf entfernte Computer.

TFTP (*Trivial File Transfer Protocol*): Eine Version des TCP/IP-FTP-Protokolls, das UDB verwendet und über keinerlei Verzeichnis- oder Passwortfunktionalitäten verfügt.

Topologie: Die physische Anordnung eines Netzwerks.

TX-Rate: Übertragungsrate.

UDP (*User Datagram Protocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem keine Bestätigung vom Empfänger der gesendeten Daten erforderlich ist.

URL (*Uniform Resource Locator*): Die Adresse einer sich im Internet befindlichen Datei.

Verschlüsselung: Die Kodierung von Daten, um diese vor einem Zugriff durch nicht autorisierte Dritte zu schützen.

Vollduplex: Die Fähigkeit von Netzwerkgeräten, Daten gleichzeitig empfangen und übertragen zu können.

VPN (*Virtual Private Network*): Sicherheitsmaßnahme zum Schutz von Daten im Internet zwischen dem Verlassen eines Netzwerks und dem Eingehen bei einem anderen.

WAN (*Wide Area Network*): Das Internet.

WEP (*Wired Equivalent Privacy*): Eine hochgradig sichere Methode zum Verschlüsseln von Daten, die in einem Wireless-Netzwerk übertragen werden.

WINIPCFG: Dienstprogramm für Windows 98 und Windows ME, das die IP-Adresse für ein bestimmtes Netzwerkbetriebsgerät anzeigt.

WLAN (*Wireless Local Area Network*): Eine Reihe von Computern und Geräten, die über Wireless-Verbindungen miteinander kommunizieren.

Anhang E: Aktualisieren der Firmware

Mit dem ADSL-Gateway können Sie die Firmware des Gateways für LAN (Netzwerk) über die Registerkarte **Verwaltung** des webbasierten Dienstprogramms aktualisieren. Führen Sie die folgenden Schritte aus:

Aktualisieren aus dem LAN

So aktualisieren Sie die Gateway-Firmware aus dem LAN:

1. Klicken Sie auf die Schaltfläche **Durchsuchen**, um nach der Firmware-Aktualisierungsdatei zu suchen, die Sie von der Linksys Website heruntergeladen und extrahiert haben.

2. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben. Klicken Sie auf die Schaltfläche **Aktualisieren**, und folgen Sie den daraufhin angezeigten Anweisungen.

Abbildung E-1: Firmware aktualisieren

Anhang F: Spezifikationen

Standards	IEEE 802.3u, IEEE 802.3, G.992.1 (G.dmt), G.992.2 (G.lite), ITU G.992.3, ITU G.992.5, ANSI T1.413i2, AG241-E1: Annex-B, AG241-DE: UR-2
Ports	Netzstrom, LINE (ADSL), Ethernet (1-4)
Tasten	Reset-Taste, Ein-/Aus-Taste
Kabeltyp	UTP CAT 5 oder höher, Telefonkabel (analog)
LEDs	Netzstrom, Ethernet (1 bis 4), DSL, Internet
Abmessungen	186 mm x 48 mm x 154 mm
Gewicht	0,36 kg
Stromversorgung	Extern, 12 V GS, 1 A
Zertifizierungen	FCC Teil 15B Klasse B, FCC Teil 68, UL 1950, CE
Betriebstemperatur	0 ºC bis 40 ºC
Lagertemperatur	-20 ºC bis 70 ºC
Luftfeuchtigkeit bei Betrieb	10 % bis 85 %, nicht kondensierend
Luftfeuchtigkeit bei Lagerung	5 % bis 90 %, nicht kondensierend

Anhang G: 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.
- Erhöhen Sie den Abstand zwischen der Ausrüstung oder den Geräten.
- 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.

KANADISCHE INDUSTRIEBESTIMMUNGEN

Dieses digitale Gerät der Klasse B erfüllt die kanadischen Bestimmungen der Richtlinie ICES-003.
This Class B digital apparatus complies with Canadian ICES-003
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

EU-KONFORMITÄTSERKLÄRUNG (EUROPA)

In Einklang mit der EWG-Richtlinie 89/336/EWG, der Niederspannungsrichtlinie 73/23/EWG sowie dem Merkblatt zur EU-Richtlinie 93/68/EWG entspricht dieses Produkt den folgenden Standards:

- EN55022 Emission
- EN55024 Immunität

Anhang H: Garantieinformationen

Linksys sichert Ihnen für einen Zeitraum von zwei 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 eigenem Ermessen 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 HAFTUNGSTHEORIE (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 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
Lateinamerika	support.la@linksys.com
USA und Kanada	support@linksys.com