

BELKIN®

ADSL2+ Modem with Wireless G Router

EN

FR

DE

NL

ES

IT



User Manual

F5D7632ea4A

Table of Contents

1. Introduction	1
Product Features	1
Benefits of a Home Network	3
Advantages of a Belkin Wireless Network	3
2. Make Sure You Have the Following	4
Package Contents	4
System Requirements	4
Setup Assistant Software System Requirements	4
Internet Connection Settings	4
3. Knowing your Router	5
4. Connecting and Configuring your Router	8
Step 1A: Hardware Connections – Follow the Quick Installation Guide (QIG)	8
Step 1B: Replacing an Existing Modem or Modem Route	9
Step 2: Set Up the Router – Run the Setup Assistant Software	10
5. Manually Configuring your Router	13
Understanding the Web-Based User Interface	13
Changing LAN Settings	15
DHCP Client List	16
Internet WAN	17
Connection Type	17
Wireless	23
Encryption/Security	25
Wireless Range Extension and Bridging	35
Firewall	37
Utilities	43
6. Manually Configuring Network Adapters	51
7. Recommended Web Browser Settings	55
8. Troubleshooting	57
9. Technical-Support Information	68
10. Appendixes	69
Appendix A: Glossary	69
Appendix B: Important Factors for Placement and Setup	74
11. Information	77

Introduction

1
2
3
4
5
6
7
8
9
10
11

section

Thank you for purchasing the Belkin ADSL2+ Modem with Wireless G Router (the Router). In minutes you will be able to share your Internet connection and network your computers with your new Router. The following is a list of features that make your Router an ideal solution for your home or small office network. Please be sure to read through this User Manual completely, and pay special attention to Appendix B entitled “Important Factors for Placement and Setup”.

Product Features

Compatibility with both PCs and Mac® Computers

The Router supports a variety of networking environments including Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP, Vista, and others. You need an Internet browser and a network adapter that supports TCP/IP (the standard language of the Internet).

Front-Panel LED Display

Lighted LEDs on the front of the Router indicate which functions are in operation. You'll know at-a-glance whether your Router is connected to the Internet. This feature eliminates the need for advanced software and status-monitoring procedures.

Web-Based Advanced User Interface

You can set up the Router's advanced functions easily through your web browser, without having to install additional software onto the computer. There are no disks to install or keep track of and, best of all, you can make changes and perform setup functions from any computer on the network quickly and easily.

Integrated 10/100 4-Port Switch

The Router has a built-in, 4-port network switch to allow your wired computers to share printers, data and MP3 files, digital photos, and much more. The switch features automatic detection so it will adjust to the speed of connected devices. The switch will transfer data between computers and the Internet simultaneously without interrupting or consuming resources.

Integrated 802.11g Wireless Access Point

802.11g is an exciting new wireless technology that achieves data rates up to 54Mbps, nearly five times faster than 802.11b.

Built-In Dynamic Host Configuration Protocol (DHCP)

Built-In Dynamic Host Configuration Protocol (DHCP) on-board makes for the easiest possible connection of a network. The DHCP server will assign IP addresses to each computer automatically so there is no need for a complicated networking setup.

NAT IP Address Sharing

Your Router employs Network Address Translation (NAT) to share the single IP address assigned to you by your Internet Service Provider while saving the cost of adding additional IP addresses to your Internet service account.

SPI Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP with zero length, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect, and fragment flooding.

MAC Address Filtering

For added security, you can set up a list of MAC addresses (unique client identifiers) that are allowed access to your network. Every computer has its own MAC address. Simply enter these MAC addresses into a list using the web-based user interface and you can control access to your network.

Universal Plug-and-Play (UPnP) Compatibility

UPnP (Universal Plug-and-Play) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant.

Support for VPN Pass-Through

If you connect to your office network from home using a VPN connection, your Router will allow your VPN-equipped computer to pass through the Router and to your office network.

Benefits of a Home Network

By following our simple setup instructions, you will be able to use your Belkin home network to:

- Share one high-speed Internet connection with all the computers in your home
- Share resources, such as files, and hard drives among all the connected computers in your home
- Share a single printer with the entire family
- Share documents, music, video, and digital pictures
- Store, retrieve, and copy files from one computer to another
- Simultaneously play games online, check Internet email, and chat

Advantages of a Belkin Wireless Network

Mobility — you'll no longer need a dedicated "computer room"—now you can work on a networked laptop or desktop computer anywhere within your wireless range

Easy installation — Belkin's Setup Wizard makes setup simple

Flexibility — set up and access printers, computers, and other networking devices from anywhere in your home

Easy Expansion — the wide range of Belkin networking products let you expand your network to include devices such as printers and gaming consoles

No cabling required — you can spare the expense and hassle of retrofitting Ethernet cabling throughout the home or office

Widespread industry acceptance — choose from a wide range of interoperable networking products

Make Sure You Have the Following

Package Contents

- ADSL2+ Modem with Wireless G Router
- RJ11 Telephone Cord - Gray
- RJ45 Ethernet Networking Cable – Yellow
- ADSL Microfilter*
- Power Adapter
- User Manual and Belkin Setup Assistant Software on CD-ROM

*ADSL microfilter varies by country. If it's not included, you will need to purchase one.

System Requirements

- An active ADSL service with a telephone wall jack for connecting the Router
- At least one computer with a Network Interface Card (NIC) and Internet browser installed and correctly configured
- TCP/IP networking protocol installed on each computer connected to the Router
- No other DHCP server on your local network assigning IP addresses to computers and devices

Setup Assistant Software System Requirements

- A PC running Windows® 2000, XP, or Vista™
- Minimum 500MHz processor and 128MB RAM
- Internet browser

Internet Connection Settings

The Setup Assistant contains a database of Internet Service Providers (ISPs) in each country to help you set up your Router quickly. If your ISP is not on the list, please collect the following information from your ISP before setting up the Router:

- Internet connection protocol: (PPPoE, PPPoA, Dynamic IP, Static IP)
- Multiplexing method or Encapsulation: (LLC or VC MUX)
- Virtual circuit: VPI (Virtual Path Identifier) _____
(a number between 0 and 255)
- VCI (Virtual Channel Identifier) _____
(a number between 1 and 65535)
- For PPPoE and PPPoA users: ADSL account user name and password _____
- For static IP users: IP Address ____ . ____ . ____ . ____
Subnet Mask ____ . ____ . ____ . ____
Default Gateway Server ____ . ____ . ____ . ____
- IP address for Domain Name Server ____ . ____ . ____ . ____ (If given by your ISP)

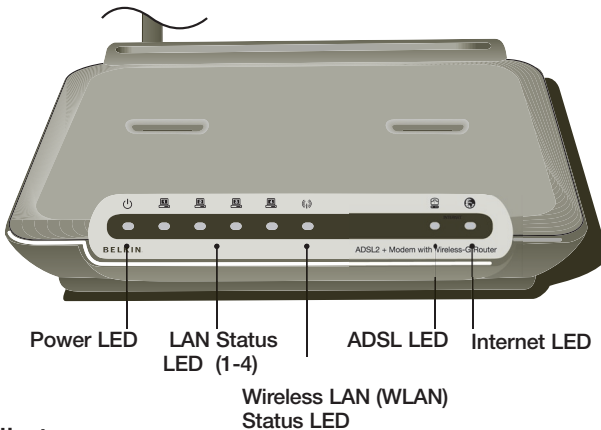
Knowing your Router

1	
2	Section
3	
4	
5	
6	
7	
8	
9	
10	
11	

The Router has been designed to be placed on a desktop. All of the cables exit from the rear of the Router for better organization and utility. The LED indicators are easily visible on the front of the Router to provide you with information about network activity and status.

Front Panel




The following illustration shows the front panel of the Router:



LED Indicators

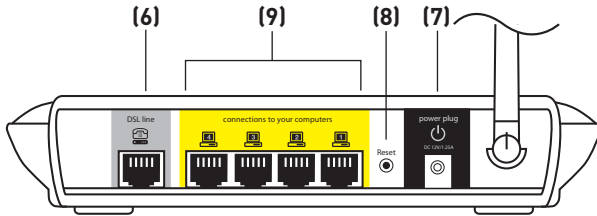
The Router is equipped with nine LEDs on the front panel as described in the table on the next page (from left to right):

Knowing your Router

LED	Color	Status	Description
ADSL			
	Green	OFF	Power off or ADSL line connection is physically disconnected
		Blinking	Handshaking or training is in progress
		Solid	ADSL line connection is OK
Wireless			
	Green	OFF	Power off or no radio signal (WLAN card is not present or fails to function)
		Blinking	Traffic is going through wireless LAN interface
		Solid	Wireless LAN interface ready to work
Internet			
	Green	OFF	No Internet connection
		Blinking	Transmitting or receiving data
		Solid	Connected to the Internet
LAN 1 to LAN 4			
LAN 1 - 4	Green	OFF	Power off or no Ethernet carrier is present
		Blinking	Ethernet carrier is present and user data is going through Ethernet port
		Solid	Ethernet carrier is present
Power			
	Green	OFF	Power off
		Solid	Power on

Rear Panel

The following figure illustrates the rear panel of your Router.



Power Plug — Connect the included power supply to this inlet. Using the wrong type of power adapter may cause damage to your Router.

Ethernet Ports —The Ethernet ports are RJ45, 10/100 auto-negotiation. The ports are labeled 1 through 4. These ports correspond to the numbered LEDs on the front of the Router. Connect your network-enabled computers or any networking devices to one of these ports.

ADSL Line —This port is for connection to your ADSL line. Connect your ADSL line to this port.

Reset Button —The “Reset” button is used in rare cases when the Router may function improperly. Resetting the Router will restore the Router’s normal operation while maintaining the programmed settings. You can also restore the factory default settings by using the “Reset” button. Use the restore option in instances where you may have forgotten your custom password.

a. Resetting the Router

Push and hold the “Reset” button for one second then release it. When the “Power/Ready” light becomes solid again, the reset is complete.

b. Restoring the Factory Defaults

Press and hold the “Reset” button for 20 seconds then release it. When the “Power/Ready” light becomes solid again, the restore is complete.

Connecting and Configuring your Router

Setup Assistant

Belkin has provided Setup Assistant software to make installing your Router a simple and easy task. You can use it to get your Router up and running in minutes. The Setup Assistant requires that your Windows 2000, XP, or Vista™ computer be connected directly to your ADSL and that the Internet connection is active and working at the time of installation. If it is not, you must use the “Alternate Setup Method” section of this User Manual to configure your Router. Additionally, if you are using an operating system other than Windows 2000, XP, or Vista, or Mac OS X, you must use the “Alternate Setup Method” section of this User Manual.

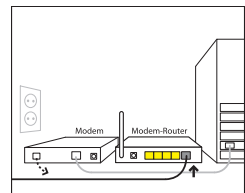
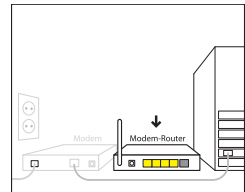
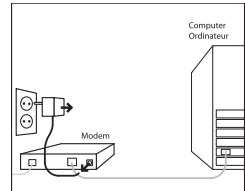
Step 1A: Hardware Connections – Follow the Quick Installation Guide (QIG)

New Router Setup

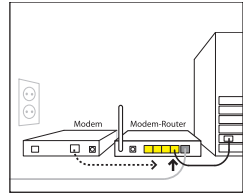
Follow these steps if you are NOT replacing an existing modem. If you are replacing an existing modem, skip to the next section, “Replacing an Existing Modem or Modem Router”, starting on page 9.

- 1A.1** Unpack your new Router from the box and place it next to your computer. Raise the Router’s antenna.
- 1A.2** Retrieve the yellow RJ45 cable that was included with your Router. First, connect one end to any yellow port labeled “Wired Computers” on the back of your Router. Then, connect the other end to the networking port on the back of your computer. [Insert Ethernet logo]
- 1A.3** Retrieve the included gray RJ11 phone cord. Connect one end to the gray port labeled “DSL” on the back of your Router. Then, connect the other end to your ADSL connection (either a wall jack or an ADSL splitter).

Note: Some ADSL connections require a microfilter. Your ADSL provider can tell you if you need one. Belkin includes a microfilter in regions known to use them. To determine if you need a microfilter, please refer to your ADSL provider’s user manual.



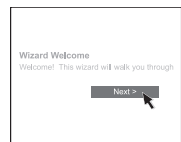
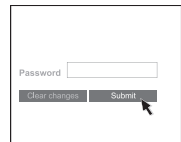
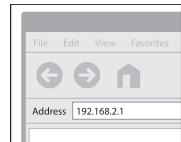
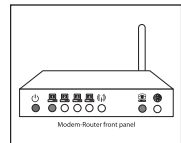
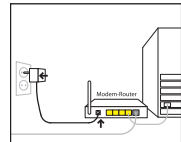
- 1A.4** Plug your Router's power supply into the black port labeled "Power" on the back of your Router. Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the "Wired" and "Modem-Router" icons are lit in green. If they are not, recheck your connections.



Step 1B: Replacing an Existing Modem or Modem Router

Follow these steps if you currently have a modem or a modem router that you will be replacing with your new Router.

- 1B.1** **Unpack** your new Router from the box and place it next to your old modem. Raise the Router's antenna. Unplug your old modem's power cord.
- 1B.2** Locate the cable that connects your old modem to your computer. Unplug that cable from your old modem, and plug it into any yellow port labeled "Wired Computers" on the back of your new Router.
- 1B.3** Locate the cable that connects your old modem to the ADSL wall jack. Unplug it from your old modem and then connect it to the gray port labeled "DSL" on the back of your Router.
- 1B.4** Plug your Router's power supply into the black port labeled "Power" on the back of your Router.
- 1B.5** **Wait** 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the "ADSL" and "LAN" LEDs are lit in green. If they are not, recheck your connections.



Step 2: Set Up the Router – Run the Setup Assistant Software

2.1 Shut down any programs that are running on your computer at this time. Turn off any firewall or Internet-connection-sharing software on your computer.

2.2 Insert the CD into your computer. The Setup Assistant will automatically appear on your computer's screen within 15 seconds. Click on "Go" to run the Setup Assistant. Follow the instructions there.

IMPORTANT: Run the Setup Assistant from the computer that is directly connected to the Router from Step 1A.2.

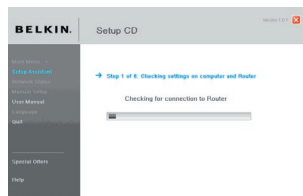
Note for Windows Users: If the Setup Assistant does not start up automatically, select your CD-ROM drive from "My Computer" and double-click on the file named "SetupAssistant" to start the Setup Assistant.

2.3 Select Country. Select your country from the drop-down box. Click "Begin" to continue.

2.4 Confirmation Screen. Verify that you have completed all QIG steps by checking the box to the right of the arrow. Click "Next" to continue.

2.5 Progress Screen Setup Assistant will show you a progress screen each time a step in the setup has been completed.

2.6 Checking Settings. The Setup Assistant will now examine your computer's network settings and gather information needed to complete the Router's connection to the Internet.



Connecting and Configuring your Router

1
2
3
4
5
6
7
8
9
10
11
section

2.7 Verifying Hardware Connections

The Setup Assistant will now verify your hardware connection.

2.8 Naming your Wireless Network

The Setup Assistant will display the default wireless network name or Service Set Identifier (SSID). This is the name of your wireless network to which your computers or devices with wireless network adapters will connect. You can either use the default or change it to something unique. Write down this name for future reference. Click “Next” to continue.

2.9 Requesting Internet Account Info (if needed)

If your Internet account requires a login and password, you will be prompted with a screen similar to the illustration below. Select your country or ISP from the drop-down boxes.

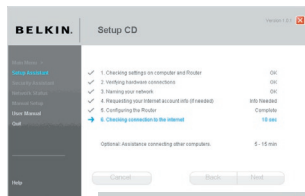
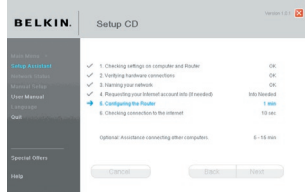
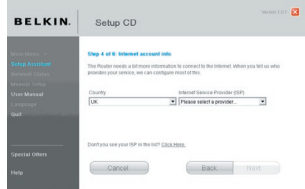
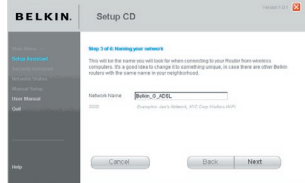
2.10 Configuring the Router

The Setup Assistant will now configure your Router by sending data to the Router and restarting it. Wait for the on-screen instructions.

Note: Do not disconnect any cable or power off the Router while the Router is rebooting. Doing so will render your Router inoperable.

2.11 Checking Internet Connection

We are almost done. The Setup Assistant will now check your connection to the Internet.



Connecting and Configuring your Router

Congratulations

You have finished installing your new Belkin Router. You will see the Congratulations screen when your Router can connect to the Internet. You can begin surfing by opening your browser and going to any website.

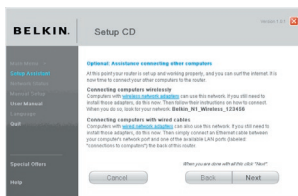
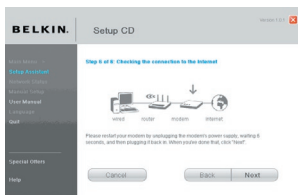
You can use the Setup Assistant to set up your other wired and wireless computers to connect to the Internet by clicking “Next”. If you decide to add computers to your Router later, select “Exit the Assistant” and then click “Next”.

Troubleshooting

If the Setup Assistant is not able to connect to the Internet, you will see the following screen. Follow the on-screen instructions to go through the troubleshooting steps.

2.12 Optional: Assistance Connecting Other Computers. This optional step will help you to connect additional wired and wireless computers to your network. Follow the on-screen instructions.

Once you have verified that your other wired and wireless computers are properly connected, your network is set up and working. You can now surf the Internet. Click “Next” to take you back to the main menu.



Manually Configuring your Router

1
2
3
4
5
6
7
8
9
10
11

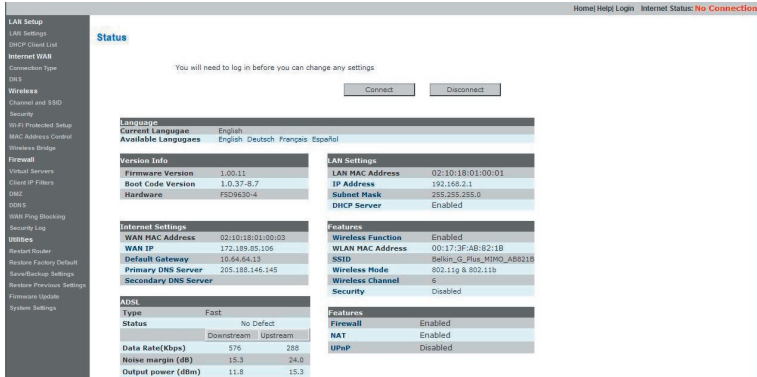
section

Understanding the Web-Based User Interface

The home page shows you a quick view of the Router's status and settings. All advanced setup pages can be reached from this page.

Using Web-Based Manager

Once your host PC is properly configured, start your web browser and type the private IP address of the Router into the URL field: "192.168.2.1" and then click "Enter".



1. Quick-Navigation Links

You can go directly to any of the Router's UI pages by clicking directly on these links. The links are divided into logical categories and grouped by tabs to make finding a particular setting easier to find. Clicking on the header of each tab will show you a short description of the tab's function.

2. Home Button

The "Home" button is available in every page of the UI. Pressing this button will take you back to the home page.

3. Help Button

The "Help" button gives you access to the Router's help pages. Help is also available on many pages by clicking "more info" next to certain sections of each page.

4. Login/Logout Button

This button enables you to log in and out of the Router with the press of one button. When you are logged into the Router, this button will change to read "Logout". Logging into the Router will take you to a separate login page where you will need to enter a password. When you are logged into the Router, you can make changes to the settings. When you are finished making changes, you can log out of the Router by clicking the "Logout" button. For more information about logging into the Router, see the section called "Logging into the Router".

5. Internet Status Indicator

This indicator is visible in all pages of the Router, showing the connection status of the Router. When the indicator says “connection OK” in GREEN, the Router is connected to the Internet. When the Router is not connected to the Internet, the indicator will read “no connection” in RED. The indicator is automatically updated when you make changes to the settings of the Router.

6. LAN Settings

Shows you the settings of the Local Area Network (LAN) side of the Router. Changes can be made to the settings by clicking the “LAN” “Quick Navigation” link on the left side of the screen.

7. Features

Shows the status of the Router’s NAT, firewall, and wireless features. Changes can be made to the settings by clicking on any one of the links or by clicking the “Quick Navigation” links on the left side of the screen.

8. Internet Settings

Shows the settings of the Internet/WAN side of the Router that connects to the Internet. Changes to any of these settings can be made by clicking on the “Internet/WAN” “Quick Navigation” link on the left side of the screen.

9. Version Info

Shows the firmware version, boot-code version, hardware version, and serial number of the Router.

10. Page Name

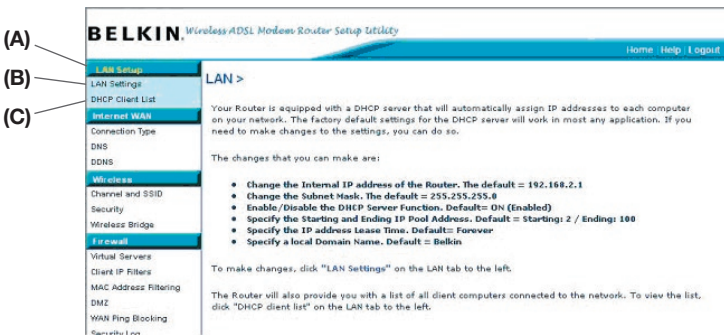
The page you are on can be identified by this name. This manual will sometimes refer to pages by name. For instance, “LAN > LAN Settings” refers to the “LAN Settings” page.

Changing LAN Settings

All settings for the internal LAN setup of the Router can be viewed and changed here.

LAN Settings

Clicking on the header of the LAN tab (A) will take you to the LAN tab's header page. A quick description of the functions can be found here. To view the settings or make changes to any of the LAN settings, click on "LAN Settings" (B) or to view the list of connected computers, click on "DHCP Client List" (C).



IP Address

The "IP address" is the internal IP address of the Router. The default IP address is "192.168.2.1". To access the advanced setup interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type in the new IP address and click "Apply Changes". The IP address you choose should be a non-routable IP. Examples of a non-routable IP are:

192.168.x.x (where x is anything between 0 and 255)

10.x.x.x (where x is anything between 0 and 255)

Subnet Mask

There is no need to change the subnet mask. This is a unique, advanced feature of your Belkin Router.

DHCP Server

The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network automatically. The default setting is “On”. The DHCP server can be turned OFF if necessary; however, in order to do so, you must manually set a static IP address for each computer on your network. To turn off the DHCP server, select “Off” and click “Apply Changes”.

IP Pool

The range of IP addresses set aside for dynamic assignment to the computers on your network. If you want to change this number, you can do so by entering a new starting and ending IP address and clicking on “Apply Changes”. The starting IP address must be lower in number than the ending IP address.

Lease Time

The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to “Forever”. The default setting is “Forever”, meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular computer. Setting lease times for shorter intervals such as one day or one hour frees IP addresses after the specified period of time. This also means that a particular computer's IP address may change over time. If you have set any of the other advanced features of the Router such as DMZ or client IP filters, these are dependent on the IP address. For this reason, you will not want the IP address to change.

Local Domain Name

You can set a local domain name (network name) for your network. There is no need to change this setting unless you have a specific advanced need to do so. You can name the network anything you want such as “MY NETWORK”.

DHCP Client List

You can view a list of the computers, which are connected to your network. You are able to view the IP address of the computer, the host name (name of the computer in your network), and the MAC address of the computer's network interface card (NIC). Pressing the “Refresh” button will update the list. If there have been any changes, the list will be updated.

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing “Refresh” will update the list.

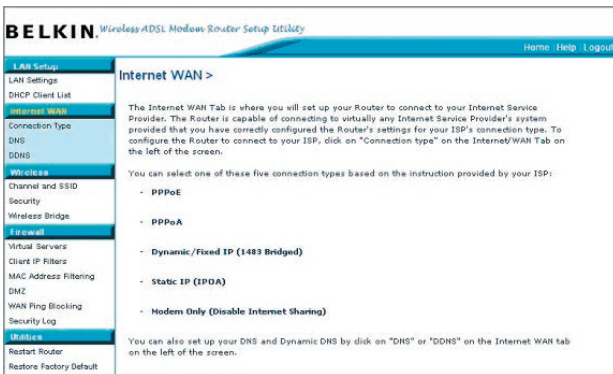
IP Address	Host Name	MAC Address
192.168.2.11	Ericd-XP	00-30-BD-3D-AB-09

[Refresh](#)

Internet WAN

The “Internet WAN” tab is where you will set up your Router to connect to your Internet Service Provider (ISP). The Router is capable of connecting to virtually any ADSL Service Provider’s system provided you have correctly configured the Router’s settings for your ISP’s connection type. Your connection settings are provided to you by your ISP.

To configure the Router with the settings that your ISP gave you, click “Connection Type” (1) on the left side of the screen. Select the connection type you use. If your ISP gave you DNS settings, clicking “DNS” (2) allows you to enter DNS address entries for ISPs that require specific settings. When you have finished making settings, the “Internet Status” indicator will read “Connected” if your Router is set up properly.



Connection Type

From the “Connection Type” page, you can select one of these five connection types based on the instruction provided by your ISP:

- PPPoE**
- PPPoA**
- Dynamic IP (1483 Bridged)**
- Static IP (IPoA)**
- Modem Only (Disable Internet Sharing)**

Note: If you are not sure which connection type to select, please contact your ISP.

Select the type of connection you use by clicking the radio button next to your connection type and then clicking “Next”.

Manually Configuring your Router

WAN > Connection type

The following information is usually provided by your ISP.
Please select the Internet sharing protocol.

- PPPoE
- PPPoA
- Dynamic/Fixed IP (1483 Bridged)
- Static IP (IPoA)
- Modem Only (Disable Internet Sharing)

Next

Setting your ISP Connection Type to PPPoE or PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) is the standard method of connecting networked devices. It requires a user name and password to access the network of your ISP for connecting to the Internet. PPPoA (PPP over ATM) is similar to PPPoE, but is mostly implemented in the UK. Select PPPoE or PPPoA and click “Next”. Then, enter the information provided by your ISP, and click “Apply Changes” to activate your settings.

WAN > Connection Type > PPPoE Interface

More Info
ATM Interface

(1) Username

(2) Password

(3) Retype Password

(4) IP assigned by ISP > Yes No

IP Address

Subnet Mask

Default Gateway

(5) VPI/VCI /

(6) Encapsulation

(7) Dial on Demand >

(8) Idle Time (Minute) >

(9) MTU >

1. User Name — Enter the user name. (Assigned by your ISP).

2. Password — Enter your password. (Assigned by your ISP).

3. Retype Password — Confirm the password.

(Assigned by your ISP).

4. IP Assigned by ISP — Leave “Yes” if your ISP automatically assigns an IP address. If your ISP assigned a fixed IP address, select “No” and enter assigned values.

Manually Configuring your Router

1

2

3

4

5

6

7

8

9

10

11

section

- 5. **VPI/VCI** — Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).
- 6. **Encapsulation** — Select your encapsulation type (supplied by your ISP) to specify how to handle multiple protocols at the ATM transport layer. VC-MUX: PPPoA Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with fewer overheads. LLC: PPPoA Logical Link Control allows multiple protocols running over one virtual circuit (more overhead).
- 7. **Dial on Demand** — By selecting “Dial on Demand”, your Router will automatically connect to the Internet when a user opens up a web browser.
- 8. **Idle Time (Minutes)** — Enter the maximum idle time for the Internet connection. After this time has been exceeded, the connection will be terminated.
- 9. **MTU** — The MTU setting should never be changed unless your ISP requires a specific MTU setting. Making changes to the MTU can cause problems with your Internet connection, including disconnection from the Internet, slow Internet access, and problems with Internet applications working properly.

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

IP assigned by ISP >

IP Address

Subnet Mask

Default Gateway

VPI/VCI

Encapsulation

Yes				
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	/	35		
LLC				

Clear Changes

Apply Changes

Setting your Connection Type to Dynamic IP (1483 Bridged)

This connection method bridges your network and ISP's network together. The Router will obtain an IP address automatically from your ISP's DHCP server.

Manually Configuring your Router

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

(1) IP assigned by ISP > Yes

(2) IP Address > 0 0 0 0

Subnet Mask > 0 0 0 0

(2) Default Gateway > 0 0 0 0

VPI/VCI > 0 / 35

(3) Encapsulation > LLC

Clear Changes Apply Changes

1. IP Assigned by ISP — Leave “Yes” if your ISP automatically assigns an IP address. If your ISP assigned a fixed IP address, select “No” and enter assigned values.

2. VPI/VCI — Enter your VPI and VCI parameter here. These identifiers are assigned by your ISP.

3. Encapsulation — Select LLC or VC MUX your ISP uses.

Setting your ISP Connection Type to Static IP (IPoA)

This connection type is also called “Classical IP over ATM” or “CLIP”, which your ISP provides a fixed IP for your Router to connect to the Internet.

WAN > Connection Type > Static IP(IPoA)

More Info
ATM Interface

(1) IP Address > 0 0 0 0

(2) Subnet Mask > 0 0 0 0

(3) Default Gateway > 0 0 0 0

(4) VPI/VCI > 0 / 35

(5) Encapsulation > LLC

Clear Changes Apply Changes

1. IP Address — Enter an IP address assigned by your ISP for the Router WAN interface.

2. Subnet Mask — Enter a subnet mask assigned by your ISP.

3. Default Gateway — Enter a default gateway IP address. If the Router cannot find the destination address within its local network, it will forward the packets to the default gateway assigned by your ISP.

4. VPI/VCI — Enter your VPI and VCI parameter here. These identifiers are assigned by your ISP.

5. Encapsulation — Select LLC or VC MUX your ISP uses.

Setting your Connection Type to Modem Only (Disable Internet Sharing)

In this mode, the Router simply acts as a bridge passing packets across the DSL port. It requires additional software to be installed on your computers in order to access the Internet.



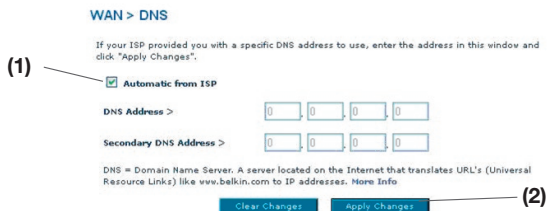
1. **VPI/VCI** — Enter your VPI and VCI parameter here. (Assigned by your ISP).

2. **Encapsulation** — Select LLC or VC MUX. (Assigned by your ISP).

DNS (Domain Name Server) Settings

A “Domain Name Server” is a server located on the Internet that translates Universal Resource Links (URLs) like “www.belkin.com” to IP addresses. Many ISPs do not require you to enter this information into the Router. The “Automatic from ISP” box (1) [Designer: call this out in screenshot below] should be checked if your ISP did not give you a specific DNS address. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is dynamic or PPPoE, it is likely that you do not have to enter a DNS address.

Leave the “Automatic from ISP” box checked. To enter the DNS address settings, uncheck the “Automatic from ISP” box and enter your DNS entries in the spaces provided. Click “Apply Changes” (2) [Designer: call this out in screenshot below] to save the settings.



Manually Configuring your Router

Using DDNS (Dynamic DNS)

The DDNS service allows you to alias a dynamic IP address to a static host name in any of the many domains DynDNS.org offers, allowing your network computers to be more easily accessed from various locations on the Internet. DynDNS.org provides this service, for up to five host names, free to the Internet community. TZO.com is another alternative to DynDNS.org. DDNS service is ideal for a home website, file server, or to make it easy to access your home PC and stored files while you're at work. Using the service can ensure that your host name always points to your IP address, no matter how often your ISP changes it. When your IP address changes, your friends and associates can always locate you by visiting yourname.dyndns.org instead! To register free for your Dynamic DNS host name, please visit <http://www.dyndns.org>.

Setting up the Router's Dynamic DNS Update Client

You must register with DynDNS.org's free update service before using this feature. Once you have your registration, follow the directions below.

1. Enter your DynDNS.org user name in the "Account / E-mail" field (1).
2. Enter your DynDNS.org password in the "Password / Key" field (2).
3. Enter the DynDNS.org domain name you set up with DynDNS.org in the "Domain Name" field (3).
4. Click "Apply Changes" to update your IP address.

Whenever your IP address assigned by your ISP changes, the Router will automatically update DynDNS.org's servers with your new IP address. You can also do this manually by clicking the "Apply Changes" button (4).

From the "Connection Type" page, you can select the type of connection you want to use by selecting the "Connection Type" from the pull-down list.

WAN > DDNS

DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP address is dynamic. You must Register for DDNS service at one of the listed DDNS Services.

DDNS Service >

DDNS Status >

(1)

(2)

(3)

(4)

Wireless

The “Wireless” tab lets you make changes to the wireless network settings. From this tab, you can make changes to the wireless network name (SSID), operating channel, and encryption security settings.

Channel and SSID

Wireless > Channel and SSID

This page allows you to enter the Wireless Network Name (SSID in Wi-Fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as an wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. [More Info](#)

SSID >	<input type="text" value="Belkin54g"/>
ESSID Broadcast >	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode >	<input type="text" value="Mixed (11b+11g)"/>
Wireless Channel >	<input type="text" value="Auto"/>
<input type="button" value="Clear Changes"/> <input type="button" value="Apply Changes"/>	

1. Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. You can change this to anything you want to or you can leave it unchanged. If there are other wireless networks operating in your area, you will want to make sure that your SSID is unique (does not match that of another wireless network in the area). To change the SSID, type in the SSID that you want to use in the SSID field and click “Apply Changes”. The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.

2. Using the ESSID Broadcast Feature

For security purposes, you can choose not to broadcast your network’s SSID. Doing so will keep your network name hidden from computers that are scanning for the presence of wireless networks. To turn off the broadcast of the SSID, select “DISABLE” and then click “Apply Changes”. The change is immediate. Each computer now needs to be set to connect to your specific SSID; an SSID of “ANY” will no longer be accepted. Refer to the documentation of your wireless network adapter for information on making this change.

Note: This advanced feature should be employed by advanced users only.

3. Using the Wireless Mode Switch

Your Router can operate in three different wireless modes: “Mixed (11b+11g)”, “11g Only”, and “11b Only”. The different modes are explained below.

Mixed (11b+11g) Mode

In this mode, the Router is compatible with 802.11b and 802.11g wireless clients simultaneously. This is the factory default mode and ensures successful operation with all devices compatible with Wi-Fi®. If you have a mix of 802.11b and 802.11g clients in your network, we recommend that you keep the default setting. This setting should only be changed if you have a specific reason to do so.

11g-Only Mode

802.11g-Only mode works with 802.11g clients only. This mode is recommended only if you want to prevent 802.11b clients from accessing your network. To switch modes, select the desired mode from the “Wireless Mode” drop-down box. Then, click “Apply Changes”.

11b-Only Mode

We recommend you DO NOT use this mode unless you have a very specific reason to do so. This mode exists only to solve unique problems that may occur with some 802.11b client adapters and is NOT necessary for interoperability of 802.11g and 802.11b standards.

4. Changing the Wireless Channel

There are a number of operating channels from which to choose. In the United States, there are 11 channels. In the United Kingdom and most of Europe, there are 13 channels. In a small number of other countries, there are other channel requirements. Your Router is configured to operate on the proper channels in which the country you reside. The default is “Auto”. The channel can be changed if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks. For best performance, use a channel that is at least five channels away from the other wireless network. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. To change the channel, select the channel from the drop-down list. Click “Apply Changes”. The change is immediate.

Encryption/Security

Securing your Wi-Fi Network

Here are a few different ways you can maximize the security of your wireless network and protect your data from prying eyes and ears. This section is intended for the home, home-office, and small-office user. At the time of this User Manual's publication, there are four encryption methods available.

Name	64-Bit Wired Equivalent Privacy	128-Bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronym	64-bit WEP	128-bit WEP	WPA-TKIP/AES (or just WPA)	WPA2-AES (or just WPA2)
Security	Good	Better	Best	Best
Features	Static keys	Static keys	Dynamic key encryption and mutual authentication	Dynamic key encryption and mutual authentication
	Encryption keys based on RC4 algorithm (typically 40-bit keys)	More secure than 64-bit WEP using a key length of 104 bits plus 24 additional bits of system-generated data	TKIP (Temporal Key Integrity Protocol) added so that keys are rotated and encryption is strengthened	AES (Advanced Encryption Standard) does not cause any throughput loss

Wired Equivalent Privacy (WEP)

WEP is a common protocol that adds security to all wireless products that are compliant with Wi-Fi. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.

64-Bit WEP

64-bit WEP was first introduced with 64-bit encryption, which includes a key length of 40 bits plus 24 additional bits of system-generated data (64 bits total). Some hardware manufacturers refer to 64-bit as 40-bit encryption. Shortly after the technology was introduced, researchers found that 64-bit encryption was too easy to decode.

128-Bit WEP

As a result of 64-bit WEP's potential security weaknesses, a more secure method of 128-bit encryption was developed. 128-bit encryption includes a key length of 104 bits plus 24 additional bits of system-generated data (128 bits total). Some hardware manufacturers refer to 128-bit as 104-bit encryption. Most of the new wireless equipment in the market today supports both 64-bit and 128-bit WEP encryption, but you might have older equipment that only supports 64-bit WEP. All Belkin wireless products will support both 64-bit and 128-bit WEP.

Encryption Keys

After selecting either the “64-bit” or “128-bit WEP” encryption mode, it is critical that you generate an encryption key. If the encryption key is not consistent throughout the entire wireless network, your wireless networking devices will be unable to communicate with one another on your network and you will not be able to successfully communicate within your network. You can enter your key by typing in the hex key manually, or you can type in a passphrase in the “Passphrase” field and click “Generate” to create a key. A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit WEP key

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key

The WEP passphrase is NOT the same as a WEP key. Your wireless card uses this passphrase to generate your WEP keys, but different hardware manufacturers might have different methods for generating the keys. If you have equipment from multiple vendors in your network, you can use the hex WEP key from your Router or access point and enter it manually into the hex WEP key table in your wireless card's configuration screen.

Wi-Fi Protected Access (WPA)

WPA is a new Wi-Fi standard that was designed to improve upon the security features of WEP. To use WPA security, the drivers and software of your wireless equipment must be upgraded to support WPA. These updates will be found on the wireless vendors' websites. There are two types of WPA security: WPA-PSK (no server) and WPA (with 802.1x radius server).

WPA-PSK (no server)

This method uses what is known as a “pre-shared key” as the network key. A network key is basically a password that is between eight and 63 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same network key to access the network. Typically, this is the mode that will be used in a home environment.

WPA (with 802.1x radius server)

With this system, a radius server distributes the network key to the clients automatically. This is typically found in a business environment.

WPA2

The Router features WPA2, which is the second generation of the WPA-based 802.11i standard. It offers a higher level of wireless security by combining advanced network authentication and stronger AES encryption methods.

WPA2 Requirements

IMPORTANT: In order to use WPA2 security, all your computers and wireless client adapters must be upgraded with patches, drivers, and client utility software that support WPA2. At the time of this User Manual's publication, a couple security patches are available, for free download, from Microsoft®. These patches work only with the Windows XP operating system. Other operating systems are not supported at this time.

For a Windows XP computer that does not have Service Pack 2 (SP2), a file from Microsoft called "Windows XP Support Patch for Wireless Protected Access (KB 826942)" is available for free download at <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91>.

For Windows XP computers with SP2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB893357). The update can be download from: <http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en>.

IMPORTANT: You also need to ensure that all your wireless client cards and adapters support WPA2, and that you have downloaded and installed the latest driver. Most of the Belkin wireless cards have updated drivers available for download from the Belkin support site: www.belkin.com/networking. For a list of Belkin wireless products that support WPA/WPA2, please visit our website at www.belkin.com/networking.

Sharing the Same Network Keys

Most Wi-Fi products ship with security turned off. So, once you have your network working, you need to activate WEP or WPA and make sure your wireless networking devices are sharing the same network key.

Manually Configuring your Router

Using a Hexadecimal Key

A hexadecimal key is a mixture of numbers and letters from A–F and 0–9. 64-bit keys are five 2-digit numbers. 128-bit keys are 13 2-digit numbers.

For instance:

AF 0F 4B C3 D4 = 64-bit key

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit key

In the boxes below, make up your key by writing in two characters between A–F and 0–9 in each box. You will use this key to program the encryption settings on your Router and your wireless computers.

Note to Mac users: Original Apple® AirPort® products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

WEP Setup

1. Select “WEP” from the drop-down menu.
2. Select “WEP Mode” of 64-bit or 128-bit.
3. After selecting your WEP mode, you can enter your key by typing in the hex key manually.

A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit key

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit key

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	WEP
WEP Mode >	<input checked="" type="radio"/> 64 bit <input type="radio"/> 128 bit
Key Entry Method >	<input type="radio"/> HEX <input checked="" type="radio"/> ASCII
Key Provisioning >	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Key 1 >	<input type="text"/>
Key 2 >	<input type="text"/>
Key 3 >	<input type="text"/>
Key 4 >	<input type="text"/>
Default Key ID >	1
Passphrase >	<input type="checkbox"/> <input type="text"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Clear Changes"/>	

3. Click “Apply Changes” to finish. Encryption in the Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router from a computer with a wireless client, you will need to ensure that security is turned ON for this wireless client. If this is not done, you will lose your wireless connection.

Changing the Wireless Security Settings

Your Router is equipped with WPA/WPA2, the latest wireless security standard. It also supports the legacy security standard, WEP. By default, wireless security is disabled. To enable security, you must first determine which standard you want to use. To access the security settings, click “Security” on the “Wireless” tab.

WPA Setup

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this User Manual’s publication, a security patch download is available free from Microsoft. This patch works only with the Windows XP operating system. You also need to download the latest driver for your Belkin Wireless G Desktop or Notebook Card from the Belkin support site. Other operating systems are not supported at this time. Microsoft’s patch only supports devices with WPA-enabled drivers such as Belkin 802.11g products.

There are two types of WPA security: WPA-PSK (no server) and WPA (with radius server). WPA-PSK (no server) uses a so-called pre-shared key (PSK) as the security key. A pre-shared key is a password that is between eight and 63 characters long. It can be a combination of letters, numbers, and other characters. Each client uses the same key to access the network. Typically, this mode will be used in a home environment. WPA (with radius server) is a configuration wherein a radius server distributes the keys to the clients automatically. This is typically used in a business environment. WPA2 is the second generation of WPA, offering a more advanced encryption technique over WPA.

Setting WPA/WPA2-PSK (no server)

1. From the “Allowed Client Type” drop-down menu, select “WPA/WPA2”.
2. For “Authentication”, select “Pre-shared Key” for typical home/SOHO use. This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up. For example, your pre-shared key might be something like: “Smith family network key”.

Manually Configuring your Router

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >

WPA/WPA2 ▾

Authentication >

802.1X Pre-shared Key

Pre-shared Key >

Apply Changes

Clear Changes

4. Click “Apply Changes” to finish. You must now set all clients to match these settings.

Setting WPA/WPA2 (with radius server) Settings

If your network uses a radius server to distribute keys to the clients, use this setting.

1. From the “Allowed Client Type” drop-down menu, select “WPA/WPA2”.
2. For “Encryption Technique”, select “802.1x” for environments with RADIUS servers. This setting will have to be identical on the clients that you set up.
3. Enter the session idle time-out of the radius server into the “Session Idle Timeout” field.
4. Enter the key interval—how often the keys are distributed (in packets)—in the “Re-Authentication Period” field.
5. Enter the waiting time after authentication failed in the “Quiet Period” field.
6. Enter the IP address and port number of the radius server into the “Server-IP” and “Server-Port” fields.
7. Enter the radius key into the “Secret Key” field.
8. Click “Apply Changes” to finish. You must now set all clients to match these settings.

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	WPA/WPA2
Authentication >	<input checked="" type="radio"/> 802.1X <input type="radio"/> Pre-shared Key
Session Idle Timeout >	300 Seconds (0 for no timeout checking)
Re-Authentication Period >	3600 Seconds (0 for no re-authentication)
Quiet Period >	60 Seconds after authentication failed
Server-IP >	192 . 168 . 2 . 1
Server-Port >	1812
Secret Key >	<input type="text"/>
NAS-ID >	<input type="text"/>

Note: Make sure your wireless computers are updated to work with WPA2 and have the correct settings to get proper connection to the Router.

Configuring your Belkin Wireless G Network Cards to Use Security

Note: This section provides information on how to configure your Belkin Wireless G Network Cards to use security. At this point, you should already have your Wireless Router or access point set to use WPA or WEP. In order for you to gain a wireless connection, you will need to set your wireless notebook card and wireless desktop card to use the same security settings.

Connecting your Computer to a Wireless Network that Requires a 64-Bit or 128-Bit WEP Key

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen. The “Advanced” button will allow you to view and configure more options of your wireless card.
2. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click “Configure”.
3. Under “Data Encryption”, select “WEP”.
4. Ensure the check box, “Network key is provided for me automatically”, at the bottom is unchecked. If you are using this computer to connect to a corporate network, consult your network administrator if this box needs to be checked.
5. Type your WEP key in the “Network key” box.

1

2

3

4

5

6

7

8

9

10

11

Manually Configuring your Router

Wireless > Security

Security Mode

Key 1

Key 2

Key 3

Key 4

(hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, input it here

PassPhrase

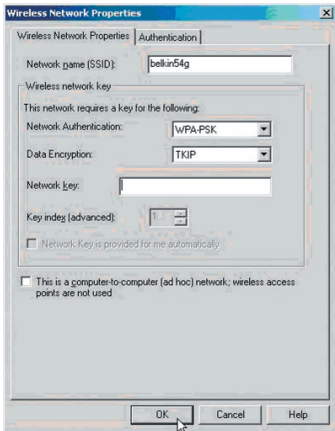
Important: A WEP key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 keys. For 64-bit WEP, you need to enter 10 keys. This network key needs to match the key you assign to your Router.

6. Click “OK” to save the settings.

Connecting your Computer to a Wireless Network that Requires WPA-PSK (no server)

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen. The “Advanced” button will allow you to view and configure more options of your wireless card.
2. Under the “Wireless Networks” tab, select a network name from the “Available networks” list and click “Configure”.
3. Under “Network Authentication”, select “WPA-PSK (No Server)”.
4. Type your WPA key in the “Network key” box.

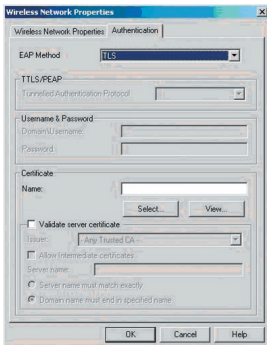
Important: WPA-PSK is a mixture of numbers and letters from A–Z and 0–9. For WPA-PSK, you can enter eight to 63 keys. This network key needs to match the key you assign to your Router.



5. Click “OK” to save the settings.

Connecting your Computer to a Wireless Network that Requires WPA (with radius server)

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen. The “Advanced” button will allow you to view and configure more options of your wireless card.
2. Under the “Wireless Networks” tab, select a network name from the “Available networks” list and click “Configure”.
3. Under “Network Authentication”, select WPA.
4. Under the “Authentication” tab, select the settings that are indicated by your network administrator.



5. Click “OK” to save the settings.

Setting up WPA for Wireless Desktop and Wireless Notebook Cards that are NOT Manufactured by Belkin

For WPA wireless desktop and wireless notebook cards that are NOT manufactured by Belkin and that are not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available as a free download.

Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time.

Important: You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.

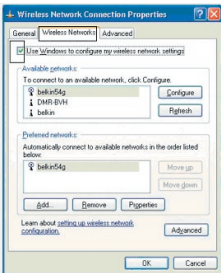
Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

Setting up Windows XP Wireless Network Utility to Use WPA-PSK

In order to use WPA-PSK, ensure you are using Windows Wireless Network Utility by doing the following:

1. Under Windows XP, click “Start > Control Panel > Network Connections”.
2. Right-click on “Wireless Network Connection”, and select “Properties”.
3. Clicking on the “Wireless Networks” tab will display the following screen. Ensure the “Use Windows to configure my wireless network settings” box is checked
4. Under the “Wireless Networks” tab, click the “Configure” button, and you will see the following screen.

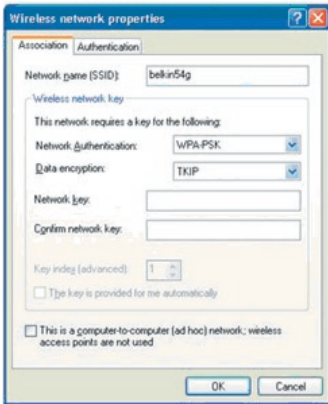


5. For a home or small-business user, select “WPA-PSK” under “Network Authentication”.

Manually Configuring your Router

1
2
3
4
5 section
6
7
8
9
10
11

Note: Select “WPA” if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server. Consult your network administrator for further information.



6. Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the Router.

7. Type in your encryption key in the “Network Key” box.

Important: Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.

8. Click “OK” to apply settings.

Wireless Range Extension and Bridging

What is a Wireless Bridge?

A wireless bridge is actually an operation “mode” you can use to extend the range of your wireless network, or add an extension of your network in another area of your office or home without running cables.

Note: We can make no guarantees that this feature will interoperate with hardware from other wireless manufacturers.

Note: Please make sure to download the latest firmware version for the Router for optimal performance at: <http://web.belkin.com/support>.

Adding Another Network Segment Wirelessly

Connecting a network switch or hub to the Router’s RJ45 jack will allow a number of computers connected to the switch access to the rest of the network.

Manually Configuring your Router

Setting up a Bridge Between your Router and a Secondary Access Point

Bridging your Belkin Router to a secondary access point requires that you access the Router's Advanced Setup Utility and enter the MAC address of the access point in the appropriate area. There are also a few other requirements.

PLEASE BE SURE TO FOLLOW THE STEPS BELOW CAREFULLY.

1. Set your access point to the same channel as the Router. For more information on changing channels, see the "Wireless - Channel and SSID" section of this User Manual.
2. Find the access point's MAC address on the bottom of the access point. There are two MAC addresses on the bottom label. You will need the MAC address named "WLAN MAC Address". The MAC address starts with "0030BD" and is followed by six other numbers or letters (i.e., 0030BD-XXXXXX). Write the MAC address below. Go to the next step.
3. Place your secondary access point within range of your Router and near the area where you want to extend the range or add the network segment. Typically, indoor range should be between 100 and 200 feet.
4. Connect power to your access point. Make sure the access point is on and proceed to the next step.
5. From a computer already connected to your Router, access the Advanced Setup Utility by opening your browser. In the address bar, type in "192.168.2.1". Do not type in "www" or "http://" before the number. Note: If you have changed your Router's IP address, use that IP address.
6. You will see the Router's user interface in the browser window. Click "Wireless Bridge" (2) on the left-hand side of the screen. You will see the following screen.
7. Check the box that says, "Enable ONLY specific Access Points to connect" (1)].

Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

1) Wireless Channel must match between Router and AP.
2) Security Settings (WEP) must match between Router and AP.
3) If MAC Filtering is enabled, user must be sure to add the WLAN MAC address(es) of the Router/AP in order to allow communication with each other.

Enable Wireless Bridging. (enabling this feature allows other Access Points to connect to this Access point.)

Enable ONLY specific Access Points to connect. (enter Wireless MAC Address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Hint: the MAC address can be found using a site survey on a wireless client card.)

AP1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Disable ability for Wireless CLIENT to connect. (This feature should only be used when the AP is used exclusively to other APs.)

Manually Configuring your Router

1

2

3

4

5

6

7

8

9

10

11

section

8. In the field named “AP1” (3), type in the MAC address of your secondary access point. When you have typed in the address, click “Apply Changes”.

9. Bridging is now set up.

Note: It may take up to a minute for the bridged connection to properly establish itself. In some cases, it may be necessary to restart the access point and the Router to initiate the bridge.

Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:

- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be “Stealth”, meaning that essentially they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.

Firewall >

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable / Disable > Enable Disable

Clear Changes

Apply Changes

Manually Configuring your Router

Virtual Servers

Virtual servers allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications, through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be “seen”. If you need to configure the virtual server function for a specific application, you will need to contact the application vendor to find out which port settings you need. You can manually input this port information into the Router.

Firewall > Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. [More Info](#)

No.	LAN IP Address	Description	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.1.1		TCP			<input checked="" type="checkbox"/>	Clear Clean
2	192.168.1.1		TCP			<input checked="" type="checkbox"/>	Clear Clean
3	192.168.1.1		TCP			<input checked="" type="checkbox"/>	Clear Clean

Choosing an Application

Select your application from the drop-down list. Click “Add”. The settings will be transferred to the next available space in the screen. Click “Apply Changes” to save the setting for that application. To remove an application, select the number of the row that you want to remove, then click “Clear”.

Manually Entering Settings into the Virtual Server

To manually enter settings, enter the IP address in the space provided for the internal (server) machine, the port(s) required to pass, the port type (TCP or UDP), and click “Apply Changes”. Each inbound port entry has two fields with five characters maximum per field that allows a start and end port range (e.g., [xxxxx]-[xxxxx]). For each entry, you can enter a single port value by filling in the two fields with the same value (e.g., [7500]-[7500]) or a wide range of ports (e.g., [7500]-[9000]). If you need multiple single-port values or a mixture of ranges and a single value, you must use multiple entries up to the maximum of 20 entries (e.g., 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Client IP Filters

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

Manually Configuring your Router

1

2

3

4

5

6

7

8

9

10

11

section

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function > Enable Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

> Add PC

Apply Changes

Access Control

Access control allows users to define the outgoing traffic permitted or denied access through the WAN interface. The default is to permit all outgoing traffic. To configure restrictive access to your computers, do the following:

1. Click “Add PC” on the “Access Control” screen.
2. Define the appropriate settings for client PC services (as shown on the following screen).

Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the “URL Blocking URL” page. For the scheduling function, you also need to configure the schedule rule first on the “Schedule Rule” page.

Client PC Description >

Client PC IP Address > -

> Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 8080, 8081, 8082	<input type="checkbox"/>
WWW with URL Blocking	HTTP (with URL Blocking Tab Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 115	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MIM Messenger	ICQ, TCP Port 1363	<input type="checkbox"/>
Remote Service	TCP Port 23	<input type="checkbox"/>

3. Click “OK” and then click “Apply Changes” to save your settings.

URL Blocking

To configure the URL-blocking feature, specify the websites (www.somesite.com) and or keywords you want to filter on your network. Click “Apply Changes” to activate the change. To complete this configuration, you will need to create or modify an access rule in the “Client IP filters” section. To modify an existing rule, click the “Edit” option next to the rule you want to modify. To create a new rule, click on the “Add PC” option. From the “Access Control > Add PC” section, check the option for “WWW with URL Blocking” in the “Client PC Service” table to filter out the websites and keywords specified.

Manually Configuring your Router

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [Home Info](#)

To configure the URL Blocking feature, use the table below to specify the websites ([www.somewhere.com](#)) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section. To modify an existing rule, click the "Edit" option next to the rule you want to modify. To create a new rule, click on the "Add PC" option.

From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below...

Rule Number	URL / Keyword
SW_1	
SW_2	
SW_3	
SW_4	
SW_5	

Schedule Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the "Schedule Rule", and apply the rule on the "Access Control" page.

Follow these steps to add a schedule:

1. Click "Add Schedule Rule".
2. You will see the following screen.
3. To configure the schedule rule, specify the name, comment, start time, and end time that you want to filter on your network.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [Home Info](#)

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Rule Name	Rule Comment	Configure
+ Add Schedule Rule	No Valid Schedule Rule Yet	

[Clear Changes](#) [Apply Changes](#)

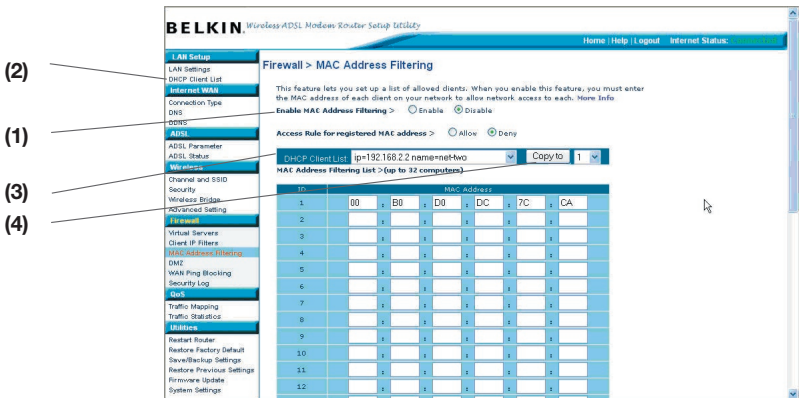
4. Click "OK" and then "Apply Changes" to save your settings.
5. To complete this configuration, you will need to create or modify an access rule in the "Client IP filters" section. This activates the schedule for use in the "Access Control" page.

Setting MAC-Address Filtering

The MAC-address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client (computer) on your network to allow network access to each. The “Block” feature lets you turn on and off access to the network easily for any computer without having to add and remove the computer’s MAC address from the list. To enable this feature, select “Enable MAC Address Filtering” (1). Next, select the access rule as “Allow” or “Deny”.

Then, enter the MAC address of each computer on your network by selecting from the “DHCP Client List” drop-down box (2) and the ID to copy to (3) before clicking “Copy to”. As an alternative method, click in the space provided (4) [Designer: pls callout (4) in the screenshot] and enter the MAC address of the computer you want to add to the list. Click “Apply Changes” (5) to save the settings. Click “Apply Changes” to save the settings.

Note: You will not be able to delete the MAC address of the computer you are using to access the Router’s administrative functions (the computer you are using now).



DMZ (Demilitarized Zone)

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted 2-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video-conferencing application. Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

Manually Configuring your Router

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted fire-wall Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks. [More Info](#)

DMZ > ENABLE DISABLE

> IP Address of Virtual DMZ Host

Index	Index IP	Static IP
1	0 0 0 0	192.168.2 0
2	0 0 0 0	192.168.2 0
3	0 0 0 0	192.168.2 0
4	0 0 0 0	192.168.2 0
5	0 0 0 0	192.168.2 0
6	0 0 0 0	192.168.2 0
7	0 0 0 0	192.168.2 0
8	0 0 0 0	192.168.2 0

To put a computer in the DMZ, enter the last digits of its IP address in the IP field and select “Enable”. Click “Apply Changes” for the change to take effect. If you are using multiple static WAN IP addresses, it is possible to select to which WAN IP address the DMZ host will be directed. Type in the WAN IP address to which you wish the DMZ host to direct, enter the last two digits of the IP address of the DMZ host computer, select “Enable”, and click “Apply Changes”.

Blocking an ICMP Ping

Computer hackers use what is known as “pinging” to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an ICMP ping from the outside. This heightens the level of security of your Router.

Firewall > WAN Ping Blocking

ADVANCE FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to WAN port). This offers a heightened level of security. [More Info](#)

Block ICMP Ping

(1) —————

To turn off the ping response, select “Block ICMP Ping” (1) and click “Apply Changes”. The Router will not respond to an ICMP ping.

Utilities

The “Utilities” screen lets you manage different parameters of the Router and perform certain administrative functions.

Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Restart Router**
Sometimes it may be necessary to Restart or Reboot the Router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Defaults**
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Current Settings**
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Saved Settings**
This option will allow you to restore a previously saved configuration.
- **Firmware Update**
From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
- **System Settings**
The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the NAT function of the Router.

Restart Router

At times it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.

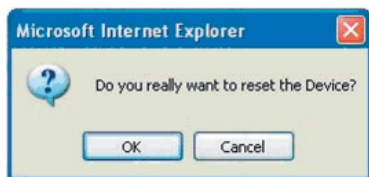
Utilities > Restart Router

Sometimes it may be necessary to Restart or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the “Restart Router” button below to Restart the Router.

Restart Router

Restarting the Router to Restore Normal Operation

1. Click the “Restart Router” button.
2. The following message will appear.
Click “OK” to restart your Router.



Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.

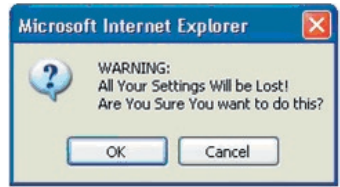
Utilities > Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the “Restore Defaults” button below.

Restore Defaults

Manually Configuring your Router

1. Click the “Restore Defaults” button.
2. The following message will appear. Click “OK” to restore factory defaults.



Saving/Backing up Current Settings

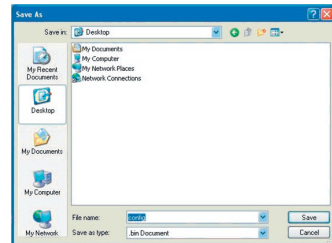
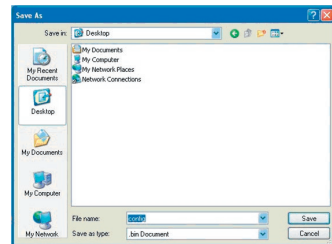
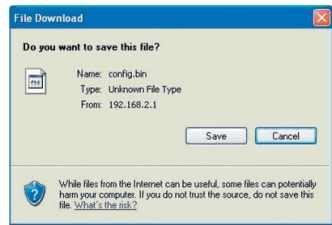
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.

1. Click “Save”. A window called “File Download” will open. Click “Save”.
2. A window will open that allows you to select the location in which to save the configuration file. Select a location. There are no restrictions on the file name; however, be sure to name the file so you can locate it yourself later. When you have selected the location and entered the file name, click “Save”.
3. When the save is complete, you will see the window below. Click “Close”. The configuration is now saved.

UTILITIES > Save/Backup current settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

Save



Restore Previous Settings

This option will allow you to restore a previously saved configuration.

Utilities > Restore Previous Settings

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the "Restore" button below.



1. Click "Browse". A window will open that allows you to select the location of the configuration file. Locate the configuration file, "config.bin", and double-click on it.
2. Then, click "Open".

Updating Firmware

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed. When Belkin releases new firmware, you can download the firmware from the Belkin website and update your Router's firmware to the latest version.

Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click here](#) to go to the Backup/Restore current settings page.



Checking for a New Version of Firmware

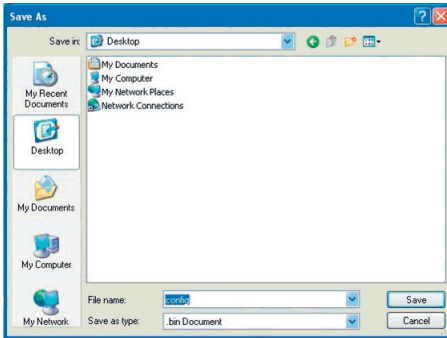
The "Check Firmware" (1) [Designer: pls callout (1) in the screenshot] button allows you to instantly check for a new version of firmware. When you click the button, a new browser window will appear informing you that either no new firmware is available or that there is a new version available. If a new version is available, you will have the option to download it.

Downloading a New Version of Firmware

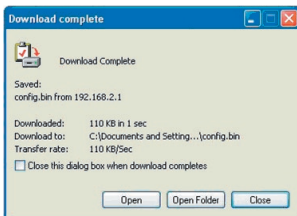
If you click the "Check Firmware" button and a new version of firmware is available, you will see a screen similar to the one below.

1. To download the new version of firmware, click "Download".
2. A window will open that allows you to select the location where you want to save the firmware file. Select a location. You can name the file anything you want, or use the default name. Be sure to locate the file in a place where you can locate it yourself later. When you have selected the location, click "Save".

Manually Configuring your Router

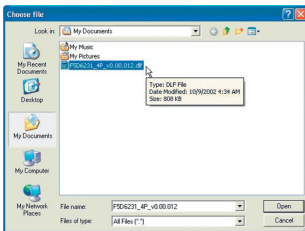


3. When the save is complete, you will see the following window. Click “Close”. The download of the firmware is complete. To update the firmware, follow the next steps in “Updating the Router’s Firmware”.



Updating the Router’s Firmware

1. In the “Firmware Update” page, click “Browse” (2) [Designer: pls callout (2) in the screenshot]. A window will open that allows you to select the location of the firmware update file.



2. Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.
3. The “Update Firmware” box will now display the location and name of the firmware file you just selected. Click “Update”.

Manually Configuring your Router

1
2
3
4
5 section
6
7
8
9
10
11

Utilities > Firmware Update

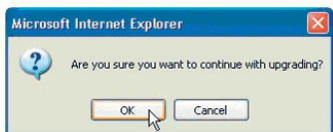
From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click Here](#) to go to the Save/Backup current settings page.

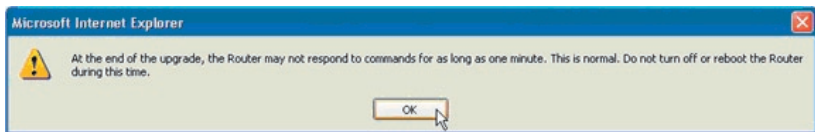
Firmware Version > 3.01.05
Check for new firmware version >

Update Firmware >

4. You will be asked if you are sure you want to continue. Click "OK".



5. You will see one more message. This message tells you that the Router may not respond for as long as one minute as the firmware is loaded into the Router and the Router is rebooted. Click "OK".



A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router firmware update will be complete. The Router home page should appear automatically. If not, type in the Router's address (default = 192.168.2.1) into the navigation bar of your browser.

System Settings

The "System Settings" page is where you can enter a new administrator password, set the time zone, enable remote management, and turn on and off the UPnP function of the Router.

Manually Configuring your Router

Setting or Changing the Administrator Password

The Router ships with NO password entered. If you wish to add a password for greater security, you can set a password here. Write down your password and keep it in a safe place, as you will need it if you need to log in to the Router in the future. It is also recommended that you set a password if you plan to use the remote-management feature of your Router.

Utilities > System Settings

Administrator Password:

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

Changing the Login Time-Out Setting

The login time-out option allows you to set the period of time that you can be logged into the Router's advanced setup interface. The timer starts when there has been no activity. For example, you have made some changes in the advanced setup interface, then left your computer alone without clicking "Logout". Assuming the time-out is set to 10 minutes, then 10 minutes after you leave, the login session will expire. You will have to log in to the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes. Note: Only one computer can be logged in to the Router's advanced setup interface at one time.

Setting the Time and Time Zone

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone in which you reside. If you reside in an area that observes daylight saving time, then place a check mark in the box next to "Daylight Savings". The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself. You now have the option to select a primary and a backup NTP server to keep your Router's clock synchronized with different NTP time servers on the Internet. Select your desired NTP server from the drop-down boxes, or simply keep it as is.

Time and Time Zone: August 1, 2003 4:26:00 AM

Please set your time zone. If you are in an area that observes daylight saving check this box. [More Info](#)

Daylight Savings

Set Time Zone > (GMT-08:00)Pacific Time (US & Canada), Tijuana

Configure Time Server (NTP) > Enable Automatic Time Server Maintenance

Primary Server > 132.163.4.102 - North America

Secondary server > 192.5.41.41 - North America

[Apply Changes](#)

Enabling Remote Management

Before you enable this advanced feature of your Belkin Router, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD**. Remote management allows you to make changes to your Router's settings from anywhere on the Internet.

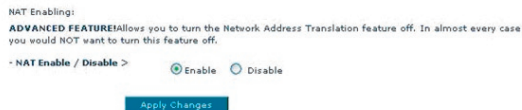
There are two methods of remotely managing the Router. The first is to allow access to the Router from anywhere on the Internet by selecting, "Any IP address can remotely manage the Router". By typing in your WAN IP address from any computer on the Internet, you will be presented with a login screen where you need to type in the password of your Router. The second method is to allow a specific IP address only to remotely manage the Router. This is more secure, but less convenient. To use this method, enter the IP address from which you know you will be accessing the Router in the space provided and select, "Only this IP address can remotely manage the Router".

Before you enable this function, it is **STRONGLY RECOMMENDED** that you set your administrator password. Leaving the password empty will potentially open your Router to intrusion. The remote-access port defaults to port 8080. You can choose a different port by entering a new port number in the "remote port" field. Click on the "Apply Changes" button to save your settings.



Enabling/Disabling Network Address Translation (NAT)

Note: This advanced feature should be employed by advanced users only. Before enabling this function, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD**. NAT is the method by which the Router shares the single IP address assigned by your ISP with the other computers on your network. This function should only be used if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn off NAT, the computers on your network will not be able to access the Internet. Other problems may also occur. Turning off NAT will disable your firewall functions.



Manually Configuring your Router

Enabling/Disabling Universal Plug-and-Play (UPnP)

UPnP is yet another advanced feature offered by your Belkin Router. It is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant.

Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports, and in some instances, setting trigger ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish to take advantage of the UPnP features, you can enable the UPnP feature. Simply select "Enable" in the "UPnP Enabling" section of the "Utilities" page. Click "Apply Changes" to save the change.

UPnP Enabling:

ADVANCED FEATURE! Allows you to turn the UPnP feature of the Router on or off. If you use applications that support UPnP, enabling UPnP will allow these applications to automatically configure the router. [Here Info](#)

UPnP Enable / Disable >

Enable Disable

[Apply Changes](#)

Enabling/Disabling Auto Firmware Update

This innovation provides the Router with the built-in capability to automatically check for a new version of firmware and alert you that the new firmware is available. When you log into the Router's Web-Based Advanced User Interface, the Router will perform a check to see if new firmware is available. If so, you will be notified. You can choose to download the new version or ignore it. The Router ships with this feature disabled. If you want to disable it, select "Enable" and click "Apply Changes".

Auto Update Firmware Enabling:

ADVANCED FEATURE! Allows you to automatically check the availability of firmware updates for your router. [Here Info](#)

Auto Update Firmware

Enable / Disable >

Enable Disable

[Apply Changes](#)

Setting up your Computers

In order for your computer to properly communicate with your Router, you will need to change your computer's "TCP/IP/Ethernet" settings to "Obtain an IP address automatically/Using DHCP". This is normally the default setting in most home computers.

You can set up the computer that is connected to the ADSL modem FIRST using these steps. You can also use these steps to add computers to your Router after the Router has been set up to connect to the Internet.

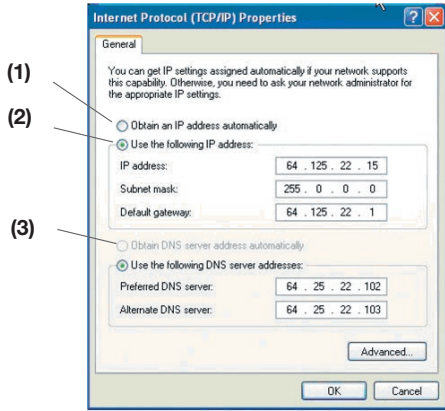
Manually Configuring Network Adapters

1
2
3
4
5
6
7
8
9
10
11

section

Windows XP, 2000, or NT

1. Click “Start”, “Settings”, then “Control Panel”.
2. Double-click on the “Network and dial-up connections” icon (Windows 2000) or the “Network” icon (Windows XP).
3. Right-click on the “Local Area Connection” associated with your network adapter and select “Properties” from the drop-down menu.
4. In the “Local Area Connection Properties” window, click “Internet Protocol (TCP/IP)” and click the “Properties” button. The following screen will appear:



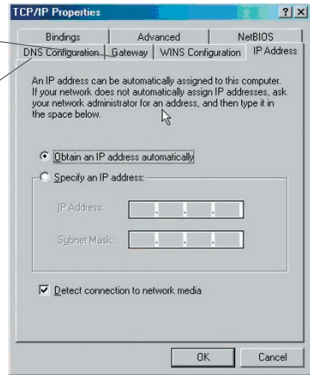
5. If “Use the following IP address” (2) [Designer: pls callout (2) in the screenshot above] is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

Manually Configuring Network Adapters

6. If not already selected, select “Obtain an IP address automatically” (1) and “Obtain DNS server address automatically” (3). Click “OK”. Your network adapter(s) are now configured for use with the Router.

Windows 98SE or Me

1. Right-click on “My Network Neighborhood” and select “Properties” from the drop-down menu.
2. Select “TCP/IP -> settings” for your installed network adapter. You will see the following window.
3. If “Specify an IP address” is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.
4. Write down the IP address and subnet mask from the “IP Address” tab (3).
5. Click the “Gateway” tab (2). Write down the gateway address in the chart.
6. Click the “DNS Configuration” tab (1). Write down the DNS address(es) in the chart.



(2)

(1)

(3)

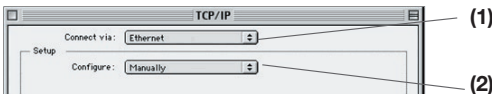
IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

7. If not already selected, select “Obtain an IP address automatically” on the “IP Address” tab. Click “OK”. Restart the computer. When the computer restarts, your network adapter(s) are now configured for use with the Router. Set up the computer that is connected to the cable or DSL modem by FIRST using these steps. You can also use these steps to add computers to your Router after the Router has been set up to connect to the Internet.

Mac OS up to 9.x

In order for your computer to properly communicate with your Router, you will need to change your Mac computer’s TCP/IP settings to DHCP.

1. Pull down the Apple menu. Select “Control Panels” and select “TCP/IP”.
2. You will see the TCP/IP control panel. Select “Ethernet Built-In” or “Ethernet” in the “Connect via:” drop-down menu (1).



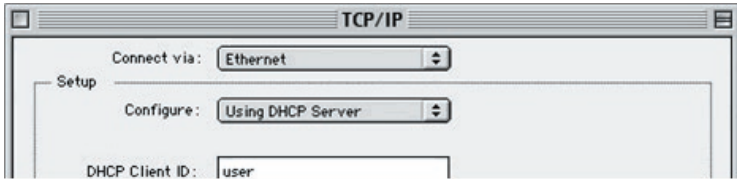
Manually Configuring Network Adapters

1
2
3
4
5
6 section
7
8
9
10
11

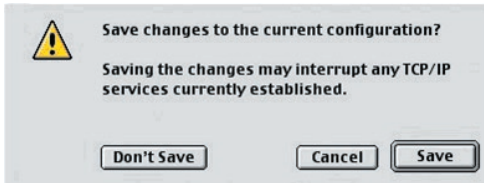
- Next to “Configure” (2) [Designer: pls callout (2) in the screenshot above], if “Manually” is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

- If not already set, at “Configure:”, choose “Using DHCP Server”. This will tell the computer to obtain an IP address from the Router.



- Close the window. If you made any changes, the following window will appear. Click “Save”.



Restart the computer. When the computer restarts, your network settings are now configured for use with the Router.

Mac OS X

- Click on the “System Preferences” icon.

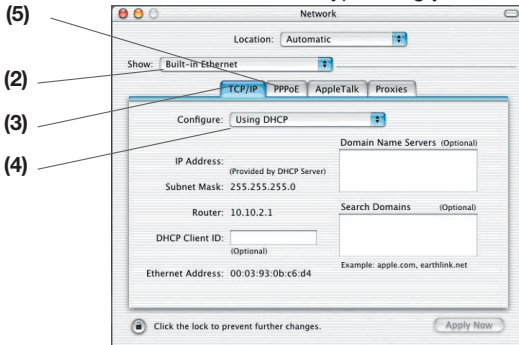


Manually Configuring Network Adapters

2. Select “Network” (1) from the “System Preferences” menu.
3. Select “Built-in Ethernet” (2) next to “Show” in the “Network” menu.



4. Select the “TCP/IP” tab (3). Next to “Configure” (4), you should see “Manually” or “Using DHCP”. If you do not, check the PPPoE tab (5) to make sure that “Connect using PPPoE” is NOT selected. If it is, you will need to configure your Router for a PPPoE connection type using your user name and password.



5. If “Manually” is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.
6. If not already selected, select “Using DHCP” next to “Configure” (4), then click “Apply Now”.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

Your network adapter(s) are now configured for use with the Router.

Recommended Web Browser Settings

1

2

3

4

5

6

7

8

9

10

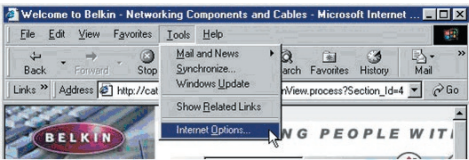
11

section

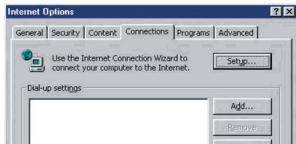
In most cases, you will not need to make any changes to your web browser's settings. If you are having trouble accessing the Internet or the Web-Based Advanced User Interface, then change your browser's settings to the recommended settings in this section.

Microsoft Internet Explorer 4.0 or Higher

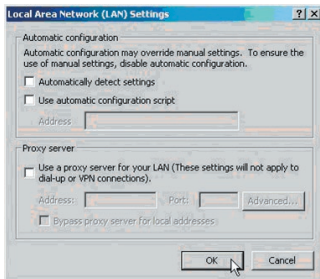
1. Start your web browser. Select "Tools" then "Internet Options".



2. In the "Internet Options" screen, there are three selections: "Never dial a connection", "Dial whenever a network connection is not present", and "Always dial my default connection". If you can make a selection, select, "Never dial a connection". If you cannot make a selection, go to the next step.
3. Under the "Internet Options" screen, click on "Connections" and select "LAN Settings...".



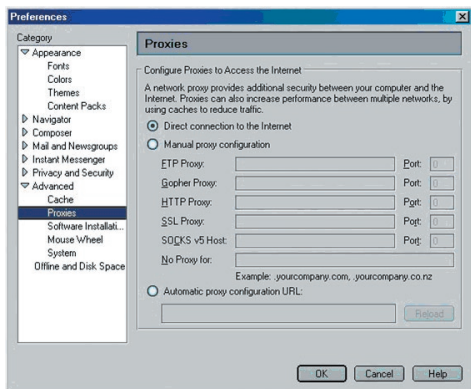
4. Make sure there are no check marks next to any of the displayed options: "Automatically detect settings", "Use automatic configuration script", and "Use a proxy server". Click "OK". Then, click "OK" again in the "Internet Options" page.



Recommended Web Browser Settings

Netscape® Navigator® 4.0 or Higher

1. Start Netscape. Click on “Edit”, then “Preferences”.
2. In the “Preferences” window, click on “Advanced”, then select “Proxies”. In the “Proxies” window, select “Direct connection to the Internet”.



Troubleshooting

Problem:

The ADSL LED is not on.

Solution:

1. Check the connection between the Router and ADSL line. Make sure the cable from the ADSL line is connected to the port on the Router labeled “DSL Line”.
2. Make sure the Router has power. The [Insert: Power Icon] Power LED on the front panel should be illuminated.

Problem:

The Internet LED is not on.

Solution:

1. Make sure the cable from the ADSL line is connected to the port on the Router labeled “DSL Line” and the [Insert: ADSL icon] ADSL LED is on.
2. Make sure you have the correct VPI/VCI, user name, and password from your ISP provider.

Problem:

My connection type is static IP address. I cannot connect to the Internet.

Solution:

Since your connection type is static IP address, your ISP must assign you the IP address, subnet mask, and gateway address. Instead of using the Wizard, go to “Connection Type”, and then select your connection type. Click “Next”, select “Static IP”, and enter your IP address, subnet mask, and default gateway information.

Problem:

I’ve forgotten or lost my password.

Solution:

Press and hold the “Reset” button on the rear panel for at least six seconds to restore the factory defaults.

1

2

3

4

5

6

7

8

9

10

11

section

Problem:

My wireless PC cannot connect to the Router.

Solution:

1. Make sure the wireless PC has the same SSID settings as the Router, and you have the same security settings on the clients such as WPA or WEP encryption.
2. Make sure the distance between the Router and wireless PC are not too far away.

Problem:

The wireless network is often interrupted.

Solution:

1. Move your wireless PC closer to the Router to find a better signal.
2. There may also be interference, possibly caused by a microwave oven or 2.4GHz cordless phones. Change the location of the Router or use a different wireless channel.

Problem:

I can't connect to the Internet wirelessly.

Solution:

If you are unable to connect to the Internet from a wireless computer, please check the following items:

1. Look at the lights on your Router. If you're using a Belkin Router, the lights should be as follows:
 - The "Power" light should be on.
 - The "Connected" light should be on, and not blinking.
 - The "WAN" light should be either on or blinking.
2. Open your wireless utility software by clicking on the icon in the system tray at the bottom right-hand corner of the screen. If you're using a Belkin Wireless Card, the tray icon should look like this [INSERT ICON] (the icon may be red or green):
3. The exact window that opens will vary depending on the model of wireless card you have; however, any of the utilities should have a list of "Available Networks"—those wireless networks it can connect to.

Does the name of your wireless network appear in the results?

Yes, my network name is listed—go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, but my network name is listed".

No, my network name is not listed—go to the troubleshooting solution titled “I can’t connect to the Internet wirelessly, and my network name is not listed”.

Problem:

I can’t connect to the Internet wirelessly, but my network name is listed.

Solution:

If the name of your network is listed in the “Available Networks” list, please follow the steps below to connect wirelessly:

1. Click on the correct network name in the “Available Networks” list. If the network has security (encryption) enabled, you will need to enter the network key. For more information regarding security, see the page entitled “Changing the Wireless Security Settings”.
2. Within a few seconds, the tray icon in the lower left-hand corner of your screen should turn green, indicating a successful connection to the network.

Problem:

I can’t connect to the Internet wirelessly, and my network name is not listed.

Solution:

If the correct network name is not listed under “Available Networks” in the wireless utility, please attempt the following troubleshooting steps:

1. Temporarily move computer, if possible, five to 10 feet from the Router. Close the wireless utility, and re-open it. If the correct network name now appears under “Available Networks”, you may have a range or interference problem. Please see the suggestions discussed in Appendix B entitled “Important Factors for Placement and Setup”.
2. Using a computer that is connected to the Router via a network cable (as opposed to wirelessly), ensure that “Broadcast SSID” is enabled. This setting is found on the Router’s wireless “Channel and SSID” configuration page.

If you are still unable to access the Internet after completing these steps, please contact Belkin Technical Support.

Problem:

My wireless network performance is inconsistent.
Data transfer is sometimes slow.
Signal strength is poor.
Difficulty establishing and/or maintaining a Virtual Private Network (VPN) connection.

Solution:

Wireless technology is radio-based, which means connectivity and the throughput performance between devices decreases when the distance between devices increases. Other factors that will cause signal degradation (metal is generally the worst culprit) are obstructions such as walls and metal appliances. As a result, the typical indoor range of your wireless devices will be between 100 to 200 feet. Note also that connection speed may decrease as you move farther from the Router or Access Point.

In order to determine if wireless issues are related to range, we suggest temporarily moving the computer, if possible, five to 10 feet from the Router.

Changing the wireless channel - Depending on local wireless traffic and interference, switching the wireless channel of your network can improve performance and reliability. The default channel the Router is shipped with is channel 11, you may choose from several other channels depending on your region; see the section entitled "Changing the Wireless Channel" on page XX for instructions on how to choose other channels.

Limiting the wireless transmit rate - Limiting the wireless transmit rate can help improve the maximum wireless range, and connection stability. Most wireless cards have the ability to limit the transmission rate. To change this property, go to the Windows Control Panel, open "Network Connections" and double-click on your wireless card's connection. In the "Properties" dialog, select the "Configure" button on the "General" tab (Windows 98 users will have to select the wireless card in the list box and then click "Properties"), then choose the "Advanced" tab and select the rate property. Wireless client cards are usually set to automatically adjust the wireless transmit rate for you, but doing so can cause periodic disconnects when the wireless signal is too weak; as a rule, slower transmission rates are more stable. Experiment with different connection rates until you find the best one for your environment; note that all available transmission rates should be acceptable for browsing the Internet. For more assistance, see your wireless card's user manual.

Problem:

How do I extend the range of my wireless network?

Solution:

Belkin recommends using one of the following products to extend wireless network coverage throughout large homes or offices:

- Wireless Access Point: A wireless access point can effectively double the

coverage area of your wireless network. An access point is typically placed in the area not currently covered by your wireless router, and connected to the router using either an Ethernet cable, or through your home's power lines using two powerline Ethernet adapters.

- For 802.11g (54g) wireless networks, Belkin offers a Wireless Range Extender/ Access Point that can be connected wirelessly to a Belkin 802.11g Wireless Router, without requiring an Ethernet cable or powerline Ethernet adapters.

These Belkin products are available at your local retailer, or can be ordered from Belkin directly.

For network/range extension information, please visit: www.belkin.com/networking to find out more about:

Wireless G Range Extender/Access Point (F5D7132)

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Belkin Router or Belkin Access Point.

Solution:

1. Log into your Wireless Router or Access Point.
2. Open your web browser and type in the IP address of the Wireless Router or Access Point. (The Router default is 192.168.2.1, the 802.11g Access Point is 192.168.2.254.) Log into your Router by clicking on the "Login" button in the top right-hand corner of the screen. You will be asked to enter your password. If you never set a password, leave the password field blank and click "Submit".
3. Click the "Wireless" tab on the left of your screen. Select the "Encryption" or "Security" tab to get to the security settings page.
4. Select "128-bit WEP" from the drop-down menu.
5. After selecting your WEP encryption mode, you can type in your hex WEP key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a WEP key from the passphrase. Click "Apply Changes" to finish. You must now set all of your clients to match these settings. A hex (hexadecimal) key is a mixture of numbers and letters from A-F and 0-9. For 128-bit WEP, you need to enter 26 hex keys.

For example:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key

6. Click "Apply Changes" to finish. Encryption in the Wireless Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router or Access Point from a computer with a wireless client, you will need to ensure that security is turned on for this wireless client. If this is not done, you will lose your wireless connection.

1

2

3

4

5

6

7

8

9

10

11

Note to Mac users: Original Apple AirPort products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your Apple AirPort product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Belkin Wireless Card.

Solution:

The Wireless Card must use the same key as the Wireless Router or Access Point. For instance, if your Wireless Router or Access Point uses the key 00112233445566778899AABBCC, then the Wireless Card must be set to the exact same key.

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Data Encryption” select “WEP”.
6. Ensure the check box “The key is provided for me automatically” at the bottom is unchecked. If you are using this computer to connect to a corporate network, please consult your network administrator if this box needs to be checked.
7. Type your WEP key in the “Network key” box.

Important: A WEP key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 keys. This network key needs to match the key you assign to your Wireless Router or Access Point.

For example: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key

8. Click “OK”, and then “Apply” to save the settings.

If you are NOT using a Belkin Wireless Card, please consult the manufacturer for that card’s user manual.

Problem:

Do Belkin products support WPA?

Solution:

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this FAQ publication, a security patch download is available, for free, from Microsoft. This patch works only with the Windows XP operating system.

Download the patch here:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

You also need to download the latest driver for your Belkin 802.11g Wireless Desktop Network Card or Notebook Network Card from the Belkin support site. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as Belkin 802.11g products.

Download the latest driver at <http://www.belkin.com/uk/support/tech/index.asp>

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Router or Belkin Access Point for a home network.

Solution:

1. From the "Security Mode" drop-down menu, select "WPA-PSK (no server)".
2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key (PSK). This can be from eight to 63 characters and can be letters, numbers, or symbols or spaces. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".
4. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Router or Belkin Access Point for a business.

Solution:

If your network uses a radius server to distribute keys to the clients, use this

setting. This is typically used in a business environment.

1. From the “Security Mode” drop-down menu, select “WPA (with server)”.
2. For “Encryption Technique”, select “TKIP” or “AES”. This setting will have to be identical on the clients that you set up.
3. Enter the IP address of the radius server into the “Radius Server” fields.
4. Enter the radius key into the “Radius Key” field.
5. Enter the key interval. Key interval is how often the keys are distributed (in packets).
6. Click “Apply Changes” to finish. You must now set all clients to match these settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Card for a home network.

Solution:

Clients must use the same key that the wireless router or access point uses. For instance if the key is “Smith Family Network Key” in the wireless router or access point, the clients must also use that same key.

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the Card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Network Authentication” select “WPA-PSK (no server).”
6. Type your WPA key in the “Network key” box.

Important: WPA-PSK is a mixture of numbers and letters from A–Z and 0–9. For WPA-PSK you can enter eight to 63 characters. This network key needs to match the key you assign to your wireless router or access point.

7. Click “OK, then “Apply” to save the settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Belkin Wireless Card for a business.

Solution:

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the Card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Network Authentication” select “WPA”.
6. In the “Authentication” tab, select the settings that are indicated by your network administrator.
7. Click “OK, then “Apply” to save the settings.

Problem:

I am having difficulty setting up Wi-Fi Protected Access (WPA) security and I am NOT using a Belkin Wireless Card for a home network.

Solution:

If you are not using a Belkin Wireless Desktop or Wireless Notebook Network Card that is not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available for free download. Download the patch from Microsoft by searching the knowledge base for Windows XP WPA.

Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time. You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.

Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

Enabling WPA-PSK (no server)

1. Under Windows XP, click “Start > Control Panel > Network Connections”.

2. Right-clicking on the “Wireless Networks” tab will display the following screen. Ensure the “Use Windows to configure my wireless network settings” box is checked.
3. Under the “Wireless Networks” tab, click the “Configure” button.
4. For a home or small business user, select “WPA-PSK” under “Network Administration”.

Note: Select WPA (with radius server) if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server. Please consult your network administrator for further information.

5. Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the wireless router or access point that you set up.
6. Type in your encryption key in the “Network Key” box.

Important: Enter your PSK. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.

7. Click “OK” to apply settings.

What is the difference between 802.11b, 802.11g, 802.11a, and Pre-N? Currently there are four levels of wireless networking standards, which transmit data at very different maximum speeds. Each is based on the designation 802.11(x), so named by the IEEE, the board that is responsible for certifying networking standards. The most common wireless networking standard, 802.11b, transmits information at 11Mbps; 802.11a and 802.11g work at 54Mbps; and Pre-N works at 108Mbps. Pre-N, the precursor to the upcoming 802.11n release, promises speeds that exceed 802.11g, and up to twice the wireless coverage area. See the following chart for more detailed information.

Belkin Wireless Comparison Chart

Wireless Technology	G (802.11g)	G Plus MIMO (802.11g with MIMO MFC)	N MIMO (draft 802.11n with MIMO)	N1 MIMO (draft 802.11n with MIMO)
Speed/Data Rate*	Up to 54Mbps*	Up to 54Mbps*	Up to 300Mbps*	Up to 300Mbps*
Frequency	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz
Compatibility	Compatible with 802.11b/g	Compatible with 802.11b/g	Compatible with draft 802.11n** and 802.11b/g	Compatible with draft 802.11n** and 802.11b/g
Coverage*	Up to 400 ft.*	Up to 1,000 ft.*	Up to 1,200 ft.*	Up to 1,400 ft.*
Advantage	Common—widespread use for Internet sharing	Better coverage and consistent speed and range	Enhanced speed and coverage	Leading edge— best coverage and throughput

*Distance and connection speeds will vary depending on your networking environment.

**This Router is compatible with products based on the same version of the draft 802.11n specifications, and may require a software upgrade for best results

Technical-Support Information

Free Tech Support* *National call rates may apply

www.belkin.com

You can find additional support information on our website www.belkin.com through the tech-support area. If you want to contact technical support by phone, please call the number you need from the list below*.

COUNTRY	NUMBER	INTERNET ADDRESS
AUSTRIA	0820 200766	www.belkin.com/uk/networking/
BELGIUM	07 07 00 073	www.belkin.com/nl/networking/
CZECH REPUBLIC	239 000 406	www.belkin.com/uk/networking/
DENMARK	701 22 403	www.belkin.com/uk/networking/
FINLAND	097 25 19 123	www.belkin.com/uk/networking/
FRANCE	08 - 25 54 00 26	www.belkin.com/fr/networking/
GERMANY	0180 - 500 57 09	www.belkin.com/de/networking/
GREECE	00800 - 44 14 23 90	www.belkin.com/uk/networking/
HUNGARY	06 - 17 77 49 06	www.belkin.com/uk/networking/
ICELAND	800 8534	www.belkin.com/uk/networking/
IRELAND	0818 55 50 06	www.belkin.com/uk/networking/
ITALY	02 - 69 43 02 51	www.belkin.com/it/support/tech/issues_more.asp
LUXEMBOURG	34 20 80 85 60	www.belkin.com/uk/networking/
NETHERLANDS	0900 - 040 07 90 <small>€0.10 per minute</small>	www.belkin.com/nl/networking/
NORWAY	81 50 0287	www.belkin.com/uk/networking/
POLAND	00800 - 441 17 37	www.belkin.com/uk/networking/
PORTUGAL	707 200 676	www.belkin.com/uk/networking/
RUSSIA	495 580 9541	www.belkin.com/networking/
SOUTH AFRICA	0800 - 99 15 21	www.belkin.com/uk/networking/
SPAIN	902 - 02 43 66	www.belkin.com/es/support/tech/networkingsupport.asp
SWEDEN	07 - 71 40 04 53	www.belkin.com/se/support/tech/networkingsupport.asp
SWITZERLAND	08 - 48 00 02 19	www.belkin.com/uk/networking/
UNITED KINGDOM	0845 - 607 77 87	www.belkin.com/uk/networking/
OTHER COUNTRIES	+44 - 1933 35 20 00	

Appendix A: Glossary

IP Address

The “IP address” is the internal IP address of the Router. To access the advanced setup interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type in the new IP address and click “Apply Changes”. The IP address you choose should be a non-routable IP. Examples of a non-routable IP are:

192.168.x.x (where x is anything between 0 and 255)

10.x.x.x (where x is anything between 0 and 255)

Subnet Mask

Some networks are far too large to allow all traffic to flood all its parts. These networks must be broken down into smaller, more manageable sections, called subnets. The subnet mask is the network address plus the information reserved for identifying the “subnetwork”.

DNS

DNS is an acronym for Domain Name Server. A Domain Name Server is a server located on the Internet that translates URLs (Universal Resource Links) like www.belkin.com to IP addresses. Many ISPs do not require you to enter this information into the Router. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is Dynamic or PPPoE, it is likely that you do not have to enter a DNS address.

PPPoE

Most ADSL providers use PPPoE as the connection type. If you use an ADSL modem to connect to the Internet, your ISP may use PPPoE to log you into the service.

Your connection type is PPPoE if:

1. Your ISP gave you a user name and password which is required to connect to the Internet.
2. Your ISP gave you software such as WinPoET or Enternet300 that you use to connect to the Internet.
3. You have to double-click on a desktop icon other than your browser to get on the Internet.

To set the Router to use PPPoE, type in your user name and password in the spaces provided. After you have typed in your information, click “Apply Changes”.

1

2

3

4

5

6

7

8

9

10

11

section

Appendix A: Glossary

After you apply the changes, the “Internet Status” indicator will read “connection OK” if your Router is set up properly.

PPPoA

Enter the PPPoA information in the provided spaces, and click “Next”. Click “Apply” to activate your settings.

1. User name - Enter the user name. (Assigned by your ISP).
2. Password - Enter your password. (Assigned by your ISP).
3. Retype Password - Confirm the password. (Assigned by your ISP).
4. VPI/VCI - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier(VCI) parameter here. (Assigned by your ISP).

Disconnect after X...

This feature is used to automatically disconnect the Router from your ISP when there is no activity for a specified period of time. For instance, placing a check mark next to this option and entering “5” into the minute field will cause the Router to disconnect from the Internet after five minutes of no Internet activity. This option should be used if you pay for your Internet service by the minute.

Channel and SSID

To change the channel of operation of the Router, select the desired channel from the drop-down menu and select your channel. Click “Apply Changes” to save the setting. You can also change the SSID. The SSID is the equivalent to the wireless network’s name. You can make the SSID anything you want to. If there are other wireless networks in your area, you should give your wireless network a unique name. Click inside of the SSID box and type in a new name. Click “Apply Changes” to make the change.

ESSID Broadcast

Many wireless network adapters currently on the market possess a feature known as site survey. It scans the air for any available network and allows each computer to automatically select a network from the survey. This occurs if the computer’s SSID is set to “ANY”. Your Belkin Router can block this random search for a network. If you disable the “ESSID Broadcast” feature, the only way a computer can join your network is by its SSID being set to the specific name of the network (like WLAN). Be sure that you know your SSID (network name) before enabling this feature. It is possible to make your wireless network nearly invisible. By turning off the broadcast of the SSID, your network will not appear in a site survey. Obviously, turning off the broadcast feature of the SSID helps increase security.

Encryption

Setting encryption can help keep your network secure. The Router uses Wired Equivalent Privacy (WEP) encryption to protect your data and features two rates of encryption: 64-bit and 128-bit. Encryption works on a system of keys. The key on the computer must match the key on the Router, and there are two ways to make a key. The easiest is to let the Router's software convert a passphrase you've created into a key. The advanced method is to enter the keys manually.

Application Gateways

Application gateways let you specify specific ports to be open for specific applications to work properly with the Network Address Translation (NAT) feature of the Router. A list of popular applications has been included. You can select an application from the popular choices included in the drop-down list. Your selections will be programmed into the Router. From the drop-down list, select the row that you want to copy the settings from, and the row you want to copy to, and then click "Copy To". The settings will be transferred to the row you specified. Click "Apply Changes" to save the setting for that application. If your application is not here, you will need to check with the application vendor to determine which ports need to be configured. You can manually input this port information into the Router.

Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be "seen". If you need to configure the virtual server function for a specific application, you will need to contact the application vendor to find out which port settings you need.

To manually enter settings, enter the IP address in the space provided for the internal machine, the port type (TCP or UDP), and the LAN and public port(s) required to pass. Then select "Enable" and click "Set". You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Client IP Filters

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

URL Blocking

To configure the URL-blocking feature, specify the websites (www.somesite.com) and/or keywords you want to filter on your network. Click “Apply Changes” to activate the change. To complete this configuration, you will need to create or modify an access rule in the client IP filters section. To modify an existing rule, click the “Edit” option next to the rule you want to modify. To create a new rule, click on the “Add PC” option. From the “Access Control Add PC” section, check the option for “WWW with URL Blocking” in the “Client PC Service” table to filter out the websites and keywords specified.

Schedule Rule

To configure the schedule rule, specify the name, comment, start time, and end time that you want to filter on your network. This page defines schedule rule names and activates the schedule for use in the “Access Control” page.

MAC-Address Filtering

The MAC-address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access

the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client on your network to allow network access to each or copy the MAC address by selecting the name of the computer from the “DHCP Client List”. To enable this feature, select “Enable”. Next, click “Apply Changes” to save the settings.

DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks. To put a computer in the DMZ, enter the last digits of its LAN IP address in the “Static IP” field and click “Apply Changes” for the change to take effect. If you have only one public (WAN) IP address, then you can leave the public IP to “0.0.0.0”. If you are using multiple public (WAN) IP addresses, it is possible to select which public (WAN) IP address the DMZ host will be directed to. Type in the public (WAN) IP address you wish the DMZ host to direct to, enter the last two digits of the IP address of the DMZ host computer, and click “Apply Changes”.

Administrator Password

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password from your Router's web-based user interface. Keep your password in a safe place as you will need this password if you need to log into the Router in the future. It is **STRONGLY RECOMMENDED** that you set a password if you plan to use the remote management feature. The login time-out option allows you to set the period of time that you can be logged into the Router's advanced setup interface. The timer starts when there has been no activity. For example, you have made some changes in the advanced setup interface, then left your computer alone without clicking "Logout".

Assuming the time-out is set to 10 minutes, then 10 minutes after you leave, the login session will expire. You will have to log into the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes. Note, only one computer can be logged into the Router's advanced setup interface at a time.

Time and Time Zone

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in. If you reside in an area that observes daylight saving time, then place a check mark in the box next to "Enable Daylight Saving". The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

Remote Management

Before you enable this function, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD**. Remote management allows you to make changes to your Router's settings from anywhere on the Internet.

UPnP

UPnP (Universal Plug-and-Play) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports and in some instances setting trigger ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish to take advantage of the UPnP features, you can enable the UPnP feature. Simply select "Enable" in the "UPnP Enabling" section of the "Utilities" page. Click "Apply Changes" to save the change.

Appendix B: Important Factors for Placement and Setup

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

1. Wireless Router (or Access Point) Placement

Place your wireless router (or access point), the central connection point of your network, as close as possible to the center of your wireless network devices. To achieve the best wireless network coverage for your “wireless clients” (i.e., computers enabled by Belkin Wireless Notebook Network Cards, Wireless Desktop Network Cards, and Wireless USB Adapters):

- Ensure that your wireless router’s (or access point’s) networking antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your wireless router (or access point) itself is positioned vertically, point the antennas as much as possible in an upward direction.
- In multistory homes, place the wireless router (or access point) on a floor that is as close to the center of the home as possible. This may mean placing the wireless router (or access point) on an upper floor.
- Try not to place the wireless router (or access point) near a cordless 2.4GHz phone.

2. Avoid Obstacles and Interference

Avoid placing your wireless router (or access point) near devices that may emit radio “noise,” such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based UV tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal’s path (between your computers and wireless router or access point).

3. Cordless Phones

If the performance of your wireless network is impaired after attending to the above issues, and you have a cordless phone:

- Try moving cordless phones away from wireless routers (or access points) and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer’s information). If this fixes the problem, your phone may be interfering.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the

Appendix B: Important Factors for Placement and Setup

phone to channel 1 and move your wireless router (or access point) to channel 11. See your phone's user manual for detailed instructions.

- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

4. Choose the “Quietest” Channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with yours.

Use the Site Survey capabilities found in the Wireless LAN Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's manual), and move your wireless router (or access point) and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices.

For Belkin wireless networking products, use the detailed Site Survey and wireless channel information included in your User Manual.

These guidelines should allow you to cover the maximum possible area with your wireless router (or access point). Should you need to cover an even wider area, we suggest the Belkin Wireless Range Extender/Access Point.

5. Secure Connections, VPNs, and AOL

Secure connections typically require a user name and password, and are used where security is important. Secure connections include:

- Virtual Private Network (VPN) connections, often used to connect remotely to an office network
- The “Bring Your Own Access” program from America Online (AOL), which lets you use AOL through broadband provided by another cable or DSL service
- Most online banking websites
- Many commercial websites that require a user name and password to access your account

Secure connections can be interrupted by a computer's power management setting, which causes it to “go to sleep.” The simplest solution to avoid this is to simply reconnect by rerunning the VPN or AOL software, or by re-logging into the secure website.

1
2
3
4
5
6
7
8
9
10
11

section

Appendix B: Important Factors for Placement and Setup

A second alternative is to change your computer's power management settings so it does not go to sleep; however, this may not be appropriate for portable computers. To change your power management setting under Windows, see the "Power Options" item in the Control Panel.

If you continue to have difficulty with Secure Connections, VPNs, and AOL, please review the steps above to be sure you have addressed these issues.

FCC Statement

DECLARATION OF CONFORMITY WITH FCC RULES FOR ELECTROMAGNETIC COMPATIBILITY

We, Belkin International, Inc., of 501 West Walnut Street, Compton, CA 90220, declare under our sole responsibility that the product,

F5D7632uk4A

to which this declaration relates, complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: Exposure to Radio Frequency Radiation.

The radiated output power of this device is far below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When connecting an external antenna to the device, the antenna shall be placed in such a manner to minimize the potential for human contact during normal operation. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Federal Communications Commission Notice

This equipment has been tested and found to comply with the limits 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. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

1

2

3

4

5

6

7

8

9

10

11

Modifications

The FCC requires the user to be notified that any changes or modifications to this device that are not expressly approved by Belkin International, Inc., may void the user's authority to operate the equipment.

Canada-Industry Canada (IC)

The wireless radio of this device complies with RSS 139 & RSS 210 Industry Canada. This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Europe-European Union Notice

Radio products with the CE 0682 or CE alert marking comply with the R&TTE Directive (1995/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following European Norms (in brackets

are the equivalent international standards).

- EN 60950 (IEC60950) – Product Safety
- EN 300 328 Technical requirement for radio equipment
- ETS 300 826 General EMC requirements for radio equipment.

To determine the type of transmitter, check the identification label on your Belkin product.

Products with the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage

Directive (72/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards).

- EN 55022 (CISPR 22) – Electromagnetic Interference
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Electromagnetic Immunity
- EN 61000-3-2 (IEC610000-3-2) – Power Line Harmonics
- EN 61000-3-3 (IEC610000) – Power Line Flicker
- EN 60950 (IEC60950) – Product Safety

Products that contain the radio transmitter are labeled with CE 0682 or CE alert marking and may also carry the CE logo.



BELKIN.

EC Declaration of Conformity to R&TTE Directive 1999/5/EC

Manufacturer : BELKIN LTD,
EXPRESS BUSINESS PARK,
SHIPTON WAY
,RUSHDEN
NN10 6GL ENGLAND

Representative : Belkin Ltd
(residing in the EC
holding the TCF)

Product / Apparatus : **ADSL Modem/Wireless G Router**

Type Number : **F5D7632-4**

Variants include : **All Country Variants**

Declaration

I declare that above product conforms to all the applicable requirements of EU Directive 1999/5/EC and is CE-marked accordingly:

Article 3.1a: (Standard(s)) used to show compliance with LVD, 73/23/EEC:
IEC 60950-1 2001 Compliant Test Report No: LD931001H03 03 NOV 04

Article 3.1b: (Standard(s)) used to show compliance with EMC Directive, 89/336/EEC:
EN301 489-1 V1.4.1 (2002-08);EN 301 489-17 V1.2.1 (2002-08) Compliant Test Report
No:RM931001H03

Article 3.2: Standard(s) used to show compliance:
...EN300 328 V1.4.1 (2003-04)..... Compliant Test Report No:RC93100H03

Signature : 

Name : K Simpson

Title : European Regulatory Compliance Manager

Date : 20 MAR 2006

Belkin International, Inc., Limited Lifetime Product Warranty

What this warranty covers.

Belkin International, Inc., warrants to the original purchaser of this Belkin product that the product shall be free of defects in design, assembly, material, or workmanship.

What the period of coverage is.

Belkin International, Inc., warrants the Belkin product for the lifetime of the product.

What will we do to correct problems?

Product Warranty.

Belkin will repair or replace, at its option, any defective product free of charge (except for shipping charges for the product).

What is not covered by this warranty?

All above warranties are null and void if the Belkin product is not provided to Belkin International, Inc., for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin International, Inc., determines that the Belkin product has been improperly installed, altered in any way, or tampered with. The Belkin Product Warranty does not protect against acts of God such as flood, lightning, earthquake, war, vandalism, theft, normal-use wear and tear, erosion, depletion, obsolescence, abuse, damage due to low voltage disturbances (i.e. brownouts or sags), non-authorized program, or system equipment modification or alteration.

How to get service.

To get service for your Belkin product you must take the following steps:

1. Contact Belkin International, Inc., at 501 W. Walnut St., Compton CA 90220, Attn: Customer Service, or call (800)-223-5546, within 15 days of the Occurrence. Be prepared to provide the following information:
 - a. The part number of the Belkin product.
 - b. Where you purchased the product.
 - c. When you purchased the product.
 - d. Copy of original receipt.
2. Your Belkin Customer Service Representative will then instruct you on how to forward your receipt and Belkin product and how to proceed with your claim. Belkin International, Inc., reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin International, Inc., for inspection shall be borne solely by the purchaser. If Belkin determines, in its sole discretion, that it is impractical to ship the damaged equipment to Belkin

International, Inc., Belkin may designate, in its sole discretion, an equipment repair facility to inspect and estimate the cost to repair such equipment. The cost, if any, of shipping the equipment to and from such repair facility and of such estimate shall be borne solely by the purchaser. Damaged equipment must remain available for inspection until the claim is finalized. Whenever claims are settled, Belkin International, Inc., reserves the right to be subrogated under any existing insurance policies the purchaser may have.

How state law relates to the warranty.

THIS WARRANTY CONTAINS THE SOLE WARRANTY OF BELKIN INTERNATIONAL, INC., THERE ARE NO OTHER WARRANTIES, EXPRESSED OR, EXCEPT AS REQUIRED BY LAW, IMPLIED, INCLUDING THE IMPLIED WARRANTY OR CONDITION OF QUALITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND SUCH IMPLIED WARRANTIES, IF ANY, ARE LIMITED IN DURATION TO THE TERM OF THIS WARRANTY.

Some states do not allow limitations on how long an implied warranty lasts, so the above limitations may not apply to you.

IN NO EVENT SHALL BELKIN INTERNATIONAL, INC., BE LIABLE FOR INCIDENTAL, SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL OR MULTIPLE DAMAGES SUCH AS, BUT NOT LIMITED TO, LOST BUSINESS OR PROFITS ARISING OUT OF THE SALE OR USE OF ANY BELKIN PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This warranty gives you specific legal rights, and you may also have other rights, which may vary from state to state. Some states do not allow the exclusion or limitation of incidental, consequential, or other damages, so the above limitations may not apply to you.

For information on product disposal please refer to <http://environmental.belkin.com>



FOR USE IN	AT	BE	CY	CZ	DK	EE	FI	FR	DE	GR	HU	IE		
IT	LV	LT	LU	MT	NL	PL	PT	SK	SI	ES	SE	GB	IS	LI
NO	CH	BG	RO	TR	OPERATES ON CHANNELS 1-13									

Restricted Use in Certain Countries.....Class 2 Equipment

BELKIN®

ADSL2+ Modem with Wireless G Router

BELKIN®

www.belkin.com

Belkin Tech Support

UK: 0845 607 77 87

Europe: www.belkin.com/support

Belkin Ltd.

Express Business Park
Shipton Way, Rushden
NN10 6GL, United Kingdom
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin SAS

130 rue de Sully
92100 Boulogne-Billancourt,
France
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH

Hanebergstrasse 2
80637 Munich
Germany
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

Belkin Iberia

C/ Anabel Segura, 10 planta baja, Of. 2
28108, Alcobendas, Madrid
Spain
+34 91 791 23 00
+34 91 490 23 35 fax

Belkin Italy & Greece

Via Carducci, 7
Milano 20123
Italy
+39 02 862 719
+39 02 862 719 fax

Belkin B.V.

Boeing Avenue 333
1119 PH Schiphol-Rijk,
Netherlands
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

© 2007 Belkin International, Inc. All rights reserved. All trade names are registered trademarks of respective manufacturers listed. Mac, Mac OS, Apple, and AirPort are trademarks of Apple Inc., registered in the U.S. and other countries. Windows, NT, Microsoft, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

P74725ea-A

BELKIN®

Modem ADSL2+ avec Routeur Sans Fil G

EN

FR

DE

NL

ES

IT



Manuel de l'utilisateur

F5D7632ea4A

Table des matières

1. Introduction	1
Caractéristiques du produit	1
Avantages d'un réseau domestique.....	3
Les avantages d'un réseau sans fil à domicile de Belkin	3
2. Assurez-vous de posséder le matériel suivant	4
Contenu de l'emballage.....	4
Configuration requise.....	4
Configuration requise pour l'Assistant d'installation	4
Paramètres Internet	4
3. Présentation de votre routeur	5
4. Branchement et configuration de votre routeur	8
Étape 1A : Branchement du matériel – Consultez le Guide d'installation rapide (GIR)	8
Étape 1B : Remplacement d'un modem ou d'un modem-routeur existant	9
Étape 2 : Configuration du routeur – Exécutez l'Assistant d'installation	10
5. Configuration manuelle du routeur	13
Faites connaissance avec l'interface-utilisateur basée sur navigateur Web	13
Modification des paramètres système	15
Liste de Clients DHCP	16
Internet WAN	17
Type de connexion	17
Sans fil	23
Chiffrement/sécurité	25
Amplification du signal et passerelle	35
Pare-feu	37
Utilitaires	43
6. Configuration manuelle des adaptateurs réseau	51
7. Configuration des paramètres du navigateur	55
8. Dépannage	57
9. Informations à propos de l'assistance technique	68
10. Appendices	69
Appendice A : Glossaire	69
Appendice B : Facteurs à considérer pour l'installation et la mise en route	74
11 Information.....	77

Introduction

Merci d'avoir choisi le Modem ADSL2+ avec Routeur Sans Fil G de Belkin (le routeur). En peu de temps, vous pourrez partager votre connexion Internet et mettre vos ordinateurs en réseau grâce à votre nouveau routeur. Voici la liste des fonctions qui font de votre routeur la solution idéale pour vos réseaux domestiques et de petites entreprises. Assurez-vous de lire attentivement ce manuel, particulièrement l'Appendice B intitulée « Facteurs à considérer pour l'installation et la mise en route ».

Caractéristiques du produit

Compatible avec les ordinateurs PC et Mac®

Le routeur prend en charge divers environnements réseau, notamment Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP et Vista, et plusieurs autres. Tout ce dont vous avez besoin est un navigateur Internet et un adaptateur réseau prenant en charge le TCP/IP (le langage standard de l'Internet).

Voyants DEL du panneau avant

Les voyants DEL du panneau avant du routeur indiquent quelles fonctions sont en opération. D'un seul coup d'œil vous saurez si votre routeur est connecté à l'Internet. Cette fonction élimine la nécessité de logiciels ou de procédures de surveillance d'état avancés.

Interface utilisateur avancée basée sur le Web

Vous pouvez configurer les fonctions avancées du routeur facilement par le biais de votre navigateur Web, sans devoir installer de logiciels supplémentaires. Il n'a pas de disques à installer ou dont se rappeler et, mieux encore, vous pouvez apporter des modifications et exécuter des fonctions de réglage à partir de n'importe lequel ordinateur du réseau, rapidement et facilement.

Switch 10/100 à 4 Ports intégré

Le routeur dispose d'un switch réseau 4 ports intégré afin que vos ordinateurs filaires puissent partager imprimantes, données, fichiers MP3, photos numériques et bien d'autres. Le switch dispose d'une détection automatique pour régler la vitesse des unités qui lui sont connectées. Il transfère simultanément les données entre les ordinateurs et Internet sans interruption ni consommation de ressources.

Point d'accès sans fil 802.11g intégré

La nouvelle technologie sans fil 802.11g vous procure une vitesse réseau tout près de cinq fois supérieure à la norme actuelle Wi-Fi (802.11b), soit 54 Mbps.

DHCP (Dynamic Host Configuration Protocol) intégré

Le protocole DHCP (Dynamic Host Configuration Protocol) intégré rend la connexion au réseau aussi simple que possible. Le serveur DHCP attribuera des adresses IP automatiquement à chaque ordinateur, de façon à ce qu'il n'y aura pas besoin d'un réglage complexe du réseau.

Partage d'adresse IP par NAT

La Traduction d'Adresse Réseau (Network Address Translation - NAT) représente le procédé employé par le routeur pour partager avec les ordinateurs de votre réseau l'adresse IP unique fournie par votre FAI.

Pare-feu SPI

Votre routeur possède un pare-feu afin de protéger votre réseau contre une multitude d'attaques provenant de pirates informatiques, incluant l'usurpation d'adresse IP, le Land Attack, le Ping de la Mort (Ping of Death - PoD), le Smurf Attack, l'attaque par Déni de Service (Denial of Service - DoS), l'IP with zero length, le TCP Null Scan, le SYN flood, le UDP flooding, le Tear Drop Attack, l'ICMP defect, le RIP defect, et le fragment flooding .

Filtrage des adresses MAC

Pour augmenter la sécurité, vous pouvez définir une liste d'adresses MAC (identificateurs de client unique) à qui est permis l'accès au réseau. Chaque ordinateur dispose de sa propre adresse MAC. Il vous suffit d'entrer ces adresses dans une liste grâce à l'interface utilisateurs basée sur le Web afin de contrôler l'accès à votre réseau.

Compatibilité Universal Plug & Play (UPnP)

L'UPnP (Universal Plug-and-Play) est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux, et d'autres applications compatibles avec l'UPnP.

Prise en charge VPN Pass-Through

Si vous vous connectez à votre réseau d'entreprise à partir de la maison par une connexion VPN, votre routeur permettra à vos ordinateurs VPN de passer à travers le routeur et de rejoindre le réseau de votre entreprise.

Avantages d'un réseau domestique

Grâce à nos instructions pas à pas, votre réseau domestique Belkin vous permettra de :

- Partager une connexion Internet à haut débit avec tous les ordinateurs de votre domicile
- Partager des ressources, telles que des fichiers et des disques durs, avec tous les ordinateurs de votre domicile
- Partager une imprimante avec toute la famille
- Partager des documents, des fichiers de musique et vidéo, ainsi que des photos numériques
- Stocker, récupérer et copier des fichiers d'un ordinateur à un autre
- Simultanément jouer à des jeux en ligne, consulter une messagerie électronique et discuter

Les avantages d'un réseau sans fil à domicile de Belkin

La Mobilité – nul besoin de confiner votre ordinateur à une seule pièce. Vous pourrez maintenant travailler sur un ordinateur de bureau ou portable, partout dans la zone couverte par votre réseau sans fil

Installation simple – l'assistant d'Installation de Belkin vous facilite la vie

Polyvalence – accédez à des imprimantes, des ordinateurs ou d'autres périphériques réseau de partout à votre domicile

Possibilité d'expansion – l'étendue de la gamme de produits de mise en réseau offerte par Belkin vous permet d'étendre votre réseau afin d'y inclure des périphériques tels que des imprimantes ou des consoles de jeu

Aucun câblage nécessaire – plus besoin d'effectuer de câblage Ethernet fastidieux et dispendieux

Reconnaissance de l'industrie – choisissez parmi une gamme étendue de produits de mise en réseau interopérables

Assurez-vous de posséder le matériel suivant

Contenu de l'emballage

- Modem ADSL2+ avec Routeur Sans Fil G
- Cordon téléphonique RJ11 - Gris
- Câble réseau Ethernet RJ45 – Jaune
- Micro-filtre ADSL*
- Bloc d'alimentation
- Manuel de l'utilisateur et logiciel assistant d'installation Belkin sur CD-ROM

*Le filtre ADSL varie d'un pays à l'autre. S'il n'est pas inclus, vous devrez en acheter un.

Configuration requise

- Une connexion ADSL active avec une prise téléphonique pour y brancher le routeur
- Au moins un ordinateur doté d'une carte d'interface réseau (CIR) et un navigateur Internet installé et configuré
- Protocole réseau TCP/IP installé sur chaque ordinateur relié au routeur
- Aucun autre serveur DHCP sur votre réseau local assignant des adresses IP aux ordinateurs et aux dispositifs

Configuration requise pour l'assistant d'installation

- Un PC sous Windows® 2000, XP ou Vista™
- Processeur 500 MHz et 128 Mo RAM minimum
- Navigateur Internet

Paramètres Internet

L'assistant d'installation contient une base de données de fournisseurs d'accès à Internet (FAI) pour chaque pays, afin de faciliter la configuration de votre routeur. Si votre FAI ne se trouve pas dans la liste, veuillez obtenir les informations suivantes auprès de votre FAI avant de mettre en route la configuration du routeur.

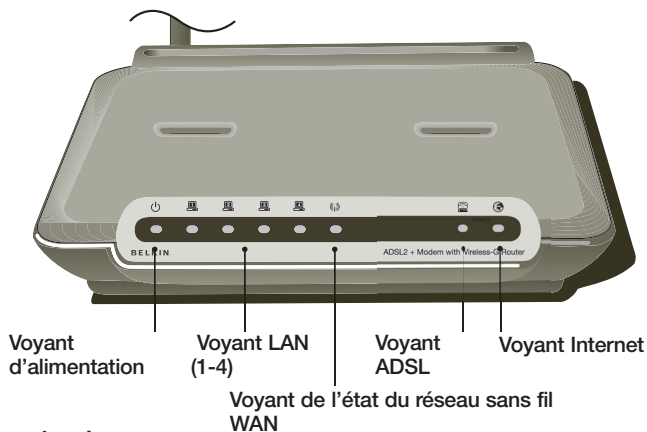
- Protocole Internet : (PPPoE, PPPoA, IP dynamique, IP fixe)
- Méthode de multiplexage ou encapsulation : (LLC ou VC MUX)
- Circuit virtuel : VPI (Virtual Path Identifier) _____
(un chiffre compris entre 0 et 255)
- VCI (Virtual Channel Identifier) _____
(un chiffre compris entre 1 et 65535)
- Pour les utilisateurs PPPoE et PPPoA : Nom d'utilisateur du compte ADSL _____ et mot de passe _____
- Pour les utilisateurs avec adresse IP fixe : Adresse IP ____ . ____ . ____ . ____
Masque de sous-réseau ____ . ____ . ____ . ____
Serveur de passerelle par défaut ____ . ____ . ____ . ____
- Adresse IP du serveur de nom de domaine ____ . ____ . ____ . ____
____ . ____ (si votre FAI vous en a fourni un)

Faites connaissance avec votre routeur

Le routeur a été conçu pour être placé sur une surface de travail. Tous les câbles sortent de la partie arrière du routeur, pour une gestion aisée de ceux-ci. Les voyants DEL visibles à l'avant du routeur vous fournissent des informations sur l'activité et l'état du réseau.

Panneau avant

L'illustration montre la face avant du routeur :






Voyants lumineux

Le routeur possède un panneau de voyants DEL, tel que décrit dans le tableau en page suivante (de gauche à droite) :

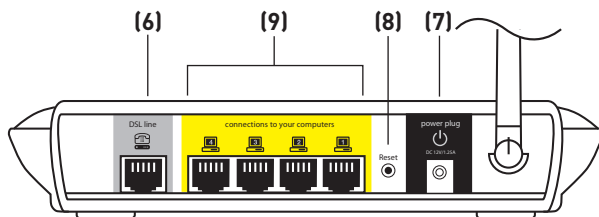
1
2 section
3
4
5
6
7
8
9
10
11

Faites connaissance avec votre routeur

Voyant DEL	Couleur	État	Description
ADSL			
	Vert	Éteint	Hors tension ou connexion ADSL connectée physiquement
		Clignotant	Protocole de contrôle du flux ou phase de synchronisation et d'établissement en cours
		Solide	Connexion de la ligne ADSL OK
Sans fil			
	Vert	Éteint	Hors tension ou aucun signal radio (carte WLAN absente ou mauvais fonctionnement de celle-ci)
		Clignotant	Trafic en cours au niveau de l'interface LAN sans fil
		Solide	Interface LAN sans fil prête à l'emploi
Internet			
	Vert	Éteint	Aucune connexion Internet
		Clignotant	Transmission ou réception de données
		Solide	Connecté à l'Internet
LAN 1 – LAN 4			
LAN 1 - 4	Vert	Éteint	Hors tension ou aucun opérateur Ethernet présent
		Clignotant	Opérateur Ethernet présent et données transmises par le port Ethernet
		Solide	Opérateur Ethernet présent
Alimentation			
	Vert	Éteint	Mise hors tension
		Solide	Mise sous tension

Face arrière

L'illustration suivante montre la face arrière de votre routeur.



Prise d'alimentation – Branchez le bloc d'alimentation fourni sur cette prise. L'utilisation de tout autre bloc d'alimentation peut endommager votre routeur.

Ports Ethernet – Les ports réseau sont de type RJ45, avec auto-négociation 10/100. Les ports sont numérotés de 1 à 4. Ces ports correspondent aux voyants situés à l'avant du routeur. Branchez vos ordinateurs ou tout autre périphérique réseau à l'un de ces ports.

ADSL – Ce port sert au branchement de votre ligne ADSL. Branchez votre ligne ADSL à ce port.

Bouton de réinitialisation – Le bouton de réinitialisation s'utilise dans les rares cas où votre routeur fonctionne de façon incongrue. La réinitialisation du routeur rétablit son fonctionnement normal, tout en conservant les paramètres enregistrés. Vous pouvez également rétablir les paramètres par défaut du fabricant à l'aide du bouton de réinitialisation. Vous pouvez utiliser le rétablissement des paramètres par défaut lorsque vous avez oublié votre mot de passe.

a. Réinitialisation du routeur

Appuyez sur le bouton « Reset [Réinitialisation] » et maintenez-le enfoncé pendant 1 seconde, puis relâchez-le. Lorsque le voyant « Alimentation/Prêt » est allumé en continu, la réinitialisation est terminée.

b. Rétablissement des paramètres par défaut d'usine

Appuyez sur le bouton « Reset [Réinitialisation] » et maintenez-le enfoncé pendant 20 secondes, puis relâchez-le. Lorsque le voyant « Alimentation/Prêt » est allumé en continu, la réinitialisation est terminée.

Branchement et configuration du routeur

Assistant d'installation

Belkin fournit son assistant d'installation pour faciliter l'installation du routeur. Utilisez-le pour installer votre routeur en un tournemain. L'assistant d'installation exige que votre ordinateur Windows 2000, XP ou Vista™ soit connecté directement à la ligne ADSL et que la connexion Internet soit active et fonctionnelle au moment de l'installation. Si elle ne l'est pas, vous devez utiliser la méthode décrite à la section « Autre méthode de configuration » de ce manuel pour configurer le routeur. En outre, si vous utilisez un système d'exploitation autre que Windows 2000, XP ou Vista, ou Mac OS X v10.x., vous devez aussi utiliser la méthode « Autre méthode de configuration » décrite dans ce même Manuel pour pouvoir configurer le routeur.

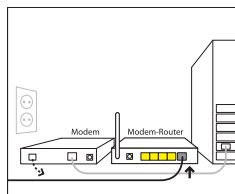
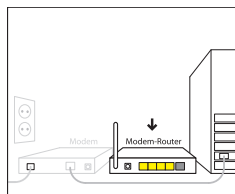
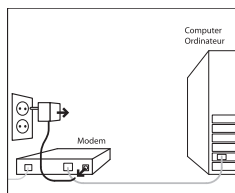
Etape 1A : Branchement du matériel – Consultez le Guide d'installation rapide (GIR)

Nouvelle installation du routeur

Suivez la procédure suivante si vous ne remplacez pas un modem existant. Si vous remplacez un modem existant, passez à la section suivante, « Remplacement d'un modem ou d'un modem-routeur existant » en page 9.

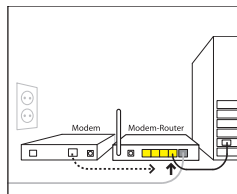
- 1A.1** Sortez le routeur de son emballage et placez-le à côté de votre ordinateur. Redressez l'antenne du routeur.
- 1A.2** Repérez le câble RJ45 jaune fourni avec votre routeur. Branchez-le à l'un des ports jaunes « Wired Computers [ordinateurs filaires] » à l'arrière de votre routeur. Branchez l'autre extrémité au port réseau à l'arrière de votre ordinateur. [Insert Ethernet logo]
- 1A.3** Repérez le cordon téléphonique gris RJ11. Branchez-le au port gris « ADSL » à l'arrière de votre routeur. Branchez ensuite l'autre extrémité à votre connexion ADSL (prise murale ou filtre ADSL).

Remarque : Certaines connexions ADSL nécessitent l'utilisation d'un filtre. Votre FAI peut vous renseigner à ce sujet. Belkin fournit un filtre pour les régions où l'utilisation d'un filtre est généralement requis. Pour déterminer sur vous avez besoin d'un filtre, consultez le manuel de l'utilisateur de votre fournisseur de services ADSL.



- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11

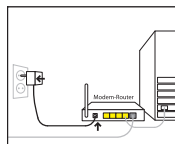
1A.4 Branchez le bloc d'alimentation fourni avec votre routeur au port noir « Power [alimentation] » à l'arrière de votre routeur. Patientez 20 secondes pendant le démarrage du routeur. Jetez un œil aux voyants à l'avant du routeur. Assurez-vous que les icônes « Wired » et « Modem-Router » sont allumées en vert. Si ce n'est pas le cas, vérifiez à nouveau les branchements.



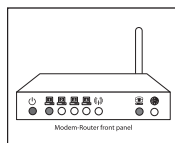
Etape 1B : Remplacement d'un modem ou d'un modem-routeur existant

Suivez la procédure suivante si vous remplacez un modem ou un modem-routeur avec votre nouveau routeur Belkin.

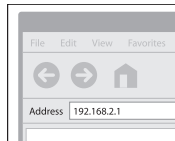
1B.1 **Sortez** le routeur de son emballage et placez-le à côté de votre ordinateur. Redressez l'antenne du routeur. Débranchez le câble d'alimentation de votre modem.



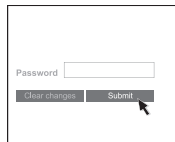
1B.2 Repérez le câble qui relie votre ordinateur au modem. Débranchez ce câble de votre ancien modem et branchez-le dans l'un des ports jaunes (« Wired Computers [ordinateurs filaires] ») à l'arrière du routeur.



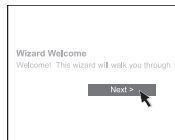
1B.3 Repérez le câble qui relie votre ancien modem à la prise murale ADSL. Débranchez-le de votre ancien modem et branchez-le au port gris « ADSL » à l'arrière de votre routeur.



1B.4 Branchez le bloc d'alimentation fourni avec votre routeur au port noir « Power [alimentation] » à l'arrière de votre routeur.



1B.5 **Patientez** 20 secondes pendant le démarrage du routeur. Jetez un œil aux voyants à l'avant du routeur. Assurez-vous que les voyants « ADSL » et « LAN » soient allumés. Si ce n'est pas le cas, vérifiez à nouveau les branchements.



Étape 2 : Configuration du routeur – Exécutez l'Assistant d'installation

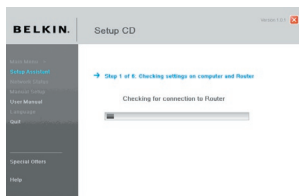
- 2.1 Arrêtez tout programme en cours d'exécution sur l'ordinateur en ce moment. Éteignez tout pare-feu ou logiciel de partage d'accès à Internet sur l'ordinateur.
- 2.2 Insérez le CD dans l'ordinateur. L'assistant d'installation apparaît automatiquement à l'écran dans les 15 secondes. Cliquez sur « Go [Aller] » pour exécuter l'Assistant d'installation. Suivez les instructions qui s'affichent.

IMPORTANT : Exécutez l'assistant d'installation à partir de l'ordinateur connecté directement au routeur à l'Étape 1A.2.

Remarque aux utilisateurs de Windows :

Si l'assistant d'installation ne s'exécute pas automatiquement, choisissez votre lecteur de CD-ROM à partir de « My Computer [Poste de Travail] », et cliquez deux fois sur le fichier appelé « SetupAssistant » sur le CD-ROM.

- 2.3 Choisissez le pays. Choisissez votre pays à partir de la liste déroulante. Cliquez sur « Begin [Commencer] » pour continuer.
- 2.4 Écran de confirmation. Assurez-vous d'avoir complété toutes les étapes du GIR et cochez la case située à droite de la flèche. Cliquez sur « Next [Suivant] » pour continuer.
- 2.5 Écran de progression . L'Assistant d'installation vous montre un écran de progression chaque fois qu'une étape est complétée.
- 2.6 Vérification des paramètres. L'assistant examine maintenant les paramètres de l'ordinateur et recueille les informations nécessaires pour terminer la connexion du routeur à Internet.



2.7 Vérification des connexions physiques

L'Assistant vérifie les branchements et les connexions physiques.

2.8 Attribution d'un nom à votre réseau sans fil.

L'assistant d'installation affiche le nom réseau sans fil par défaut ou le Service Set Identifier (SSID). Il s'agit du nom de votre réseau sans fil, auquel vos ordinateurs ou dispositifs avec adaptateurs réseau sans fil se connecteront. Vous pouvez utiliser le nom par défaut ou choisir un nom unique. Notez ce nom pour y référer plus tard. Cliquez sur « Next [Suivant] » pour continuer.

2.9 Recherche des informations relatives à votre compte Internet (si besoin).

Si la connexion à votre compte Internet requiert l'utilisation d'un nom d'utilisateur et d'un mot de passe, vous verrez un écran semblable à celui ci-dessous. Choisissez votre pays ou votre FAI dans les boîtes de sélection.

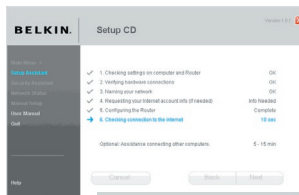
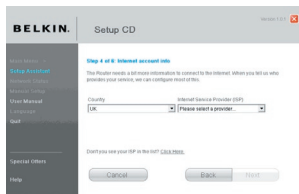
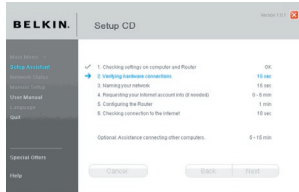
2.10 Configuration du routeur.

L'assistant d'installation configure maintenant votre routeur en envoyant des données à celui-ci et en le redémarrant. Attendez les instructions qui apparaissent à l'écran.

Remarque : Il est important de ne débrancher aucun câble ou de ne pas mettre le routeur hors tension pendant le redémarrage. Sinon, le routeur pourrait subir des dommages irréversibles.

2.11 Vérification de la connexion à Internet.

La configuration est presque terminée. L'Assistant d'installation vérifie maintenant votre connexion à l'Internet.



Félicitations

Vous avez terminé l'installation de votre nouveau routeur Belkin. Vous verrez l'écran de Félicitations lorsque votre routeur peut se connecter à l'Internet. Vous pouvez commencer à naviguer en lançant votre navigateur et en visitant un site Web.

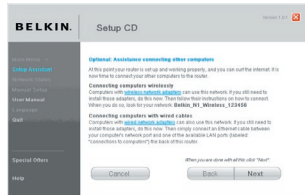
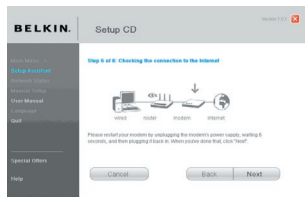
Vous pouvez vous servir de l'assistant d'installation pour configurer vos ordinateurs filaires ou sans fil pour la connexion à l'Internet en cliquant sur « Next [Suivant] ». Si vous décidez d'ajouter des ordinateurs à votre routeur plus tard, choisissez « Exit the Assistant [Quitter l'assistant] » puis sur « Next [Suivant] ».

Dépannage

Si l'assistant n'a pas été en mesure d'établir une connexion à l'Internet, vous verrez cet écran. Suivez les instructions à l'écran pour effectuer les étapes de la résolution de problèmes.

2.12 Facultatif : Aide pour la connexion d'autres ordinateurs. Cette étape facultative vous aidera à connecter d'autres ordinateurs filaires ou sans fil à votre réseau. Suivez les instructions qui apparaissent à l'écran.

Après avoir vérifié la connexion de vos ordinateurs filaires et sans fil, votre réseau est prêt. Vous pouvez maintenant naviguer sur Internet. Cliquez « Next [Suivant] » pour retourner au menu principal.

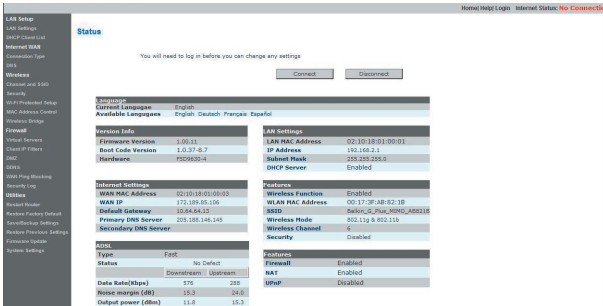


Faites connaissance avec l'interface-utilisateur basée sur navigateur Web

La page d'accueil vous montre un aperçu de l'état du routeur et de ses paramètres. À partir de cette page, vous pouvez rejoindre toutes les pages ayant trait à la configuration.

Utilisation de la gestion basée sur navigateur

Après avoir configuré adéquatement le PC hôte, lancez votre navigateur Web et entrez l'adresse IP privée du routeur dans le champ d'adresse URL : « 192.168.2.1 » et cliquez ensuite sur « Enter ».



1. Raccourcis de navigation

Vous pouvez passer à n'importe quelle autre page de l'IU en cliquant directement sur ces raccourcis. Les raccourcis sont classés par catégories et groupés à l'aide d'onglets pour faciliter l'accès à un paramètre particulier. En cliquant sur le titre de chaque onglet, vous verrez une courte description des fonctions classées sous cet onglet.

2. Bouton Accueil

Le bouton « Accueil » est disponible à chaque page de l'IU. En cliquant sur ce bouton, vous retournez à la page d'accueil.

3. Bouton Aide

Le bouton « Aide » vous permet d'accéder aux pages d'aide du routeur. Vous pouvez également obtenir de l'aide sur de nombreuses pages. Pour cela, cliquez sur « More info [Plus d'infos] » en regard de certaines sections de chaque page.

4. Bouton Connexion/Déconnexion

Ce bouton vous permet d'ouvrir ou de fermer une session sur le routeur en appuyant sur un bouton. Lorsque vous êtes connecté au routeur, ce bouton indique « Logout [Déconnexion] ». La connexion au routeur vous transportera vers une page de connexion séparée, où vous devrez entrer un mot de passe. Lorsque vous êtes connecté au routeur, vous pouvez apporter des modifications aux paramètres. Une fois les modifications apportées, vous pouvez vous déconnecter du routeur. Pour cela, cliquez sur le bouton « Logout [Déconnexion] ». Pour plus d'informations sur la connexion au routeur, reportez-vous à la section « Connexion au routeur ».

5. Indicateur de l'état de l'Internet

Cet indicateur est visible sur toutes les pages du routeur, et montre l'état de la connexion du routeur. Lorsqu'il indique « connexion OK [Connexion OK] » en VERT, le routeur est connecté à Internet. Lorsque le routeur n'est pas connecté à Internet, l'indicateur affiche « No connection [Pas de connexion] » en ROUGE. Lorsque vous apportez des modifications aux paramètres du routeur, l'indicateur est mis à jour automatiquement.

6. Paramètres LAN

Montre les paramètres du réseau local, du côté du routeur. Des modifications aux paramètres peuvent être effectuées en cliquant sur le raccourci « LAN » à la gauche de l'écran.

7. Fonctions

Montre l'état de la NAT, du pare-feu et des caractéristiques sans fil du routeur. Pour modifier ces paramètres, cliquez sur l'un des liens ou sur le lien de navigation rapide sur la partie gauche de l'écran.

8. Paramètres Internet

Indique les paramètres Internet/WAN du routeur connecté à l'Internet. Vous pouvez modifier les paramètres en cliquant sur le raccourci de navigation « Internet/WAN » à la gauche de l'écran.

9. Informations sur la version

Montre les versions du micrologiciel, du code de démarrage, du matériel, ainsi que le numéro de série du routeur.

10. Nom de la page

La page sur laquelle vous vous trouvez peut être identifiée par ce nom. Ce manuel réfère parfois au nom de ces pages. Par exemple, « LAN > LAN Settings [LAN > Paramètre LAN] » réfère à la page « LAN Settings [Paramètres LAN] ».

Modification des paramètres de réseau local (LAN)

Tous les paramètres de réseau local (LAN) du routeur peuvent être visualisés et modifiés ici.

Paramètres de réseau local

Pour accéder à page d'accueil de l'onglet LAN (réseau local) (A), cliquez sur le titre de celui-ci. Vous y trouverez une courte description des fonctions. Pour afficher les paramètres ou modifier n'importe quel de ces paramètres de réseau local, cliquez sur « LAN Settings [Paramètres de réseau local] » (B) ou pour afficher la liste des ordinateurs connectés, cliquez sur « DHCP Client List [Liste des clients DHCP] » (C).

(A) LAN Setup

(B) LAN Settings

(C) DHCP Client List

Internet WAN

Connection Type

DNS

DDNS

Miscelan

Channel and SSID

Security

Wireless Bridge

Firewall

Virtual Servers

Client IP Filters

MAC Address Filtering

DMZ

WAN Ping Blocking

Restore Factory

LAN >

Your Router is equipped with a DHCP server that will automatically assign IP addresses to each computer on your network. The factory default settings for the DHCP server will work in most any application. If you need to make changes to the settings, you can do so.

The changes that you can make are:

- Change the Internal IP address of the Router. The default = 192.168.2.1
- Change the Subnet Mask. The default = 255.255.255.0
- Enable/Disable the DHCP Server Function. Default: ON (Enabled)
- Specify the Starting and Ending IP Pool Address. Default = Starting: 2 / Ending: 100
- Specify the IP address Lease Time. Default: Forever
- Specify a local Domain Name. Default = Belkin.

To make changes, click "LAN Settings" on the LAN tab to the left.

The Router will also provide you with a list of all client computers connected to the network. To view the list, click "DHCP client list" on the LAN tab to the left.

Adresse IP

L'« Adresse IP » représente l'Adresse IP interne du routeur. L'adresse IP par défaut est 192.168.2.1. Pour accéder à l'Interface de configuration avancée, entrez cette adresse IP dans la barre d'adresse de votre navigateur. Cette adresse peut être modifiée au besoin. Pour modifier l'adresse IP, entrez la nouvelle adresse IP et cliquez sur « Apply Changes [Enregistrer les Modifications] ». L'adresse IP choisie doit être une adresse IP non-acheminable. Exemples d'adresses IP non-acheminables :

192.168.x.x (où x est un nombre compris entre 0 et 255)

10.x.x.x (où x est un nombre compris entre 0 et 255)

Masque de sous-réseau

Il n'est pas nécessaire de modifier le masque de sous-réseau. Il consiste en une fonction avancée unique à votre routeur.

Serveur DHCP

Le serveur DHCP rend la mise en œuvre d'un réseau très simple, en attribuant automatiquement des adresses IP à tous les ordinateurs du réseau. La valeur par défaut est « ON [Activé] ». La fonction de serveur DHCP peut être désactivée si nécessaire. Toutefois, si vous désactivez le Serveur DHCP, vous devrez entrer manuellement une adresse IP statique pour chacun des ordinateurs de votre réseau. Pour désactiver le serveur DHCP, sélectionnez l'option « Off [Désactivé] », puis cliquez sur « Apply Changes [Enregistrer les modifications] ».

Groupe IP

Il s'agit de l'ensemble d'adresses IP réservé pour l'attribution dynamique aux ordinateurs du réseau. Pour changer ce nombre, entrez de nouvelles adresses IP de début et de fin, puis cliquez sur « Apply Changes [Enregistrer les modifications] ». L'adresse IP de départ doit être inférieure en nombre à l'adresse IP d'arrivée.

Durée d'autorisation

La durée pendant laquelle le serveur DHCP réservera l'adresse IP pour chaque ordinateur. Nous vous conseillons de laisser la durée d'autorisation à « Forever [Toujours] ». La valeur par défaut est « Forever [Toujours] », ce qui signifie que chaque fois que le serveur DHCP attribue une adresse IP à un ordinateur, cette adresse ne changera pas pour l'ordinateur. La prédéfinition d'une durée d'autorisation plus courte, tel que un jour ou une heure, libérera les adresses IP en question après l'écoulement du temps spécifié. Ceci veut en outre dire que l'adresse IP d'un ordinateur peut changer au fil du temps. Si vous avez défini d'autres fonctions avancées du routeur, comme la DMZ ou le filtrage des clients IP, celles-ci dépendront de l'adresse IP. Ainsi, il serait préférable que l'adresse IP demeure la même.

Nom de domaine local

Vous pouvez donner un nom de domaine local (nom de réseau) à votre réseau. Il n'est pas nécessaire de modifier ce paramètre, à moins qu'un besoin avancé spécifique ne vous oblige à le faire. Vous êtes libre de donner le nom de votre choix à votre réseau, comme par exemple Mon Réseau .

Liste de Clients DHCP

Vous pouvez visualiser une liste d'ordinateurs (appelés « clients ») connectés à votre réseau. Vous êtes en mesure de visualiser l'adresse IP (1) de l'ordinateur, le nom d'hôte (2) (nom de l'ordinateur sur votre réseau), et l'adresse MAC (3) de la carte d'interface réseau de cet ordinateur. Cliquez sur le bouton « Refresh [Actualiser] » pour mettre la liste à jour. La liste est mise à jour s'il y a eu un quelconque changement.

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing "Refresh" will update the list.

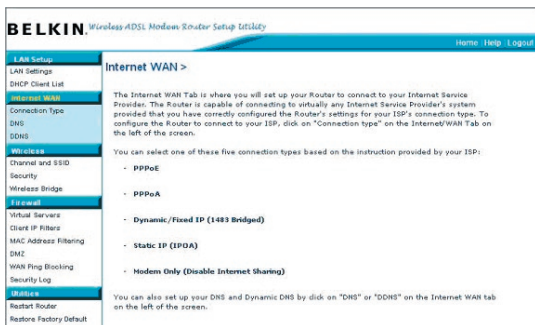
IP Address	Host Name	MAC Address
192.168.2.11	Eriod-XP	00-30-8D-3D-AB-09

Refresh

Internet WAN

L'onglet « Internet/WAN » est l'endroit où vous allez configurer le routeur pour qu'il se connecte à votre Fournisseur d'Accès à Internet (FAI). Le routeur peut se connecter pratiquement à n'importe quel système ADSL offerts par un FAI, si bien sûr vous avez configuré votre routeur avec les paramètres appropriés au type de connexion de votre FAI. Vos paramètres de connexion vous sont fournis par votre FAI.

Pour configurer le routeur avec les paramètres fournis par le FAI, cliquez sur « Connection Type [Type de connexion] » (1) sur le côté gauche de l'écran. Sélectionnez votre type de connexion. Si votre FAI vous a fourni des paramètres DNS, cliquez sur « DNS » (2) pour entrer l'adresse DNS de votre FAI qui nécessite des paramètres particuliers. Lorsque vous avez terminé d'apporter ces modifications, l'indicateur « Internet Status [État de l'Internet] » affiche « Connected [Connecté] » si le routeur a été correctement configuré.



Type de Connexion

À partir de la page Type de connexion, vous pouvez choisir l'un des cinq types de connexions, selon les informations fournies par votre FAI :

PPPoE

PPPoA

Dynamic IP (1483 Bridged)

IP fixe (IPoA)

Modem uniquement (désactiver le partage d'Internet)

Remarque : En cas de doute, contactez votre FAI.

Pour ce faire, cliquez sur le bouton radio en regard du type de connexion, puis cliquez sur Next [Suivant].

Configuration manuelle du routeur

WAN > Connection type

The following information is usually provided by your ISP.
Please select the Internet sharing protocol.

- PPPoE
- PPPoA
- Dynamic/Fixed IP (483 Bridged)
- Static IP (PPoA)
- Modem Only (Disable Internet Sharing)

Next

Configuration de votre connexion de type PPPoE ou PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) est la méthode de connexion standard pour les dispositifs réseau. Elle requiert un nom d'utilisateur et un mot de passe pour accéder au réseau de votre FAI, pour vous connecter à l'Internet. Le PPPoA (PPP over ATM) est similaire au PPPoE, mais se retrouve plutôt au Royaume-Uni. Sélectionnez PPPoE ou PPPoA et cliquez sur « Next [Suivant] ». Entrez ensuite les informations fournies par votre FAI, puis cliquez « Apply Changes

WAN > Connection Type > PPPoE Interface

More Info
ATM Interface

(1)	Username	<input type="text"/>
(2)	Password	<input type="password"/>
(3)	Retype Password	<input type="password"/>
(4)	IP assigned by ISP >	Yes <input type="button" value="v"/>
	IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
	Subnet Mask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
	Default Gateway	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
(5)	VPI/VCI	<input type="text" value="0"/> / <input type="text" value="35"/>
(6)	Encapsulation	LLC <input type="button" value="v"/>
(7)	Dial on Demand >	<input checked="" type="checkbox"/>
(8)	Idle Time (Minute) >	<input type="text" value="0"/>
(9)	MTU >	<input type="text" value="1456"/>

[Enregistrer les modifications] » pour activer les paramètres.

1. Nom d'utilisateur - Entrez le nom d'utilisateur. (Attribuée par votre FAI.)
2. Mot de passe - Entrez votre mot de passe. (Attribuée par votre FAI.)
3. Entrez à nouveau le mot de passe - Confirmez le mot de passe. (Attribuée par votre FAI.)
4. P attribuée par le FA – Laissez « Yes [Oui] » si votre FAI attribue automatiquement l'adresse. Si votre FAI attribue une adresse IP fixe, sélectionnez « No [Non] » et entrez les valeurs correspondantes.

5. VPI/VCI — Entrez ici vos paramètres de d'identificateur de trajet virtuel (VPI) et d'identificateur de voie virtuelle (VCI). (Attribuée par votre FAI.)
6. Encapsulation — Sélectionnez votre type d'encapsulation (fourni par votre FAI) afin de spécifier comment traiter les protocoles multiples sur la couche de transport ATM. VC-MUX : Le PPPoA Virtual Circuit Multiplexer (null encapsulation) ne permet qu'un seul protocole par circuit virtuel, avec moins de surdébits. LLC : Le PPPoA Logical Link Control permet plusieurs protocoles sur un circuit virtuel (plus de surdébit).
7. Dial on Demand — Si vous sélectionnez « Dial on Demand », votre routeur se connecte à l'Internet lorsqu'un utilisateur lance un navigateur Web.
8. Temps d'inactivité (minutes) — Entrez le temps d'inactivité maximum de la connexion à Internet. Lorsque cet intervalle de temps est dépassé, la connexion à Internet prend fin.
9. MTU — Le paramètre MTU ne devrait jamais être modifié, à moins que votre FAI ne vous ait fourni un paramètre spécifique. Apporter des modifications aux valeurs MTU peut causer des problèmes pour la connexion à l'Internet, y compris déconnexion de l'Internet, accès lent à l'Internet et difficultés avec des applications Internet qui fonctionnaient correctement auparavant.

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

IP assigned by ISP >

IP Address

Subnet Mask

Default Gateway

VPI/VCI

Encapsulation

Yes				
0	0	0	0	
0	0	0	0	
0	0	0	0	
0	/	35		
LLC				

Clear Changes

Apply Changes

Configuration de votre type de connexion avec IP Dynamique (1483 Bridged)

Cette méthode de connexion relie votre réseau et le réseau de votre FAI. Le routeur obtient une adresse IP automatiquement du serveur DHCP de votre FAI.

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

(1) IP assigned by ISP > Yes

(2) IP Address > 0 0 0 0

(2) Subnet Mask > 0 0 0 0

(2) Default Gateway > 0 0 0 0

(3) VPI/VCI > 0 / 35

(3) Encapsulation > LLC

Clear Changes Apply Changes

1. IP attribuée par le FAI – Laissez Yes [Oui] si votre FAI attribue automatiquement l'adresse IP. Si votre FAI attribue une adresse IP fixe, sélectionnez « No [Non] » et entrez les valeurs correspondantes.

2. VPI/VCI — Entrez ici vos paramètres de VPI et VCI. Ces identifiants vous sont fournis par votre FAI.

3. Encapsulation — Sélectionnez LLC ou VC MUX, selon le paramètre de votre FAI.

Réglage du type de connexion FAI comme « IP fixe » (IPoA)

Ce type de connexion est également appelé « Classical IP over ATM [IP Classique sur ATM] » ou « CLIP », où votre FAI vous attribue une adresse IP fixe pour la connexion du routeur à l'Internet.

WAN > Connection Type > Static IP(IPoA)

More Info
ATM Interface

(1) IP Address > 0 0 0 0

(2) Subnet Mask > 0 0 0 0

(3) Default Gateway > 0 0 0 0

(4) VPI/VCI > 0 / 35

(5) Encapsulation > LLC

Clear Changes Apply Changes

1. Adresse IP – Entrez une adresse IP fournir par votre FAI pour l'interface WAN du routeur.

2. Masque de sous-réseau — Entrez un masque de sous-réseau fourni par votre FAI.

3. Passerelle par défaut — Entrez une adresse IP de passerelle par défaut. Si le routeur ne peut trouver l'adresse de destination au sein de son réseau local, il reliaera les paquets de données vers la passerelle par défaut fournie par votre FAI.

4. VPI/VCI — Entrez ici vos paramètres de VPI et VCI. Ces identifiants vous sont fournis par votre FAI.

5. Encapsulation — Sélectionnez LLC ou VC MUX, selon le paramètre de votre FAI.

Configuration de votre connexion pour désactiver le partage de l'Internet

Dans ce mode, le routeur agit en tant que simple passerelle pour les paquets de données transitant sur le port DSL. Vous devez également installer des logiciels supplémentaires sur votre ordinateur pour accéder à l'Internet.

WAN > Connection Type > Modem Only(Disable Internet Sharing)

More Info
ATM Interface

(1) — VPI/VCI

(2) — Encapsulation

0 / 35

LLC

Clear Changes Apply Changes

1. VPI/VCI – Entrez ici vos paramètres de VPI et VCI. (Attribuée par votre FAI.)

2. Encapsulation — Sélectionnez LLC ou VC MUX. (Attribuée par votre FAI.)

Paramètres DNS (Domain Name Server - serveur de nom de domaine)

Un Serveur de Noms de Domaine est un serveur que l'on retrouve sur l'Internet et qui traduit les URL (Universal Resource Links), telles que www.belkin.com, en adresses IP. Cette information n'est pas requise de la plupart des FAI lors de la configuration du routeur. La case « Automatic from ISP [Obtenir automatiquement du FAI] » (1) doit être cochée si votre FAI ne vous a pas fourni d'adresse DNS particulière. Si vous êtes utiliser une connexion de type IP statique, vous pouvez avoir besoin de saisir une adresse DNS spécifique ainsi qu'une adresse DNS secondaire pour que votre connexion puisse fonctionner correctement. Si vous utilisez une connexion de type dynamique ou PPPoE, il est fort probable que vous n'ayez pas à entrer une adresse de DNS.

Laissez la case « Automatic from ISP [Obtenir automatiquement du FAI] » cochée. Pour entrer les paramètres d'adresse DNS, désélectionnez la case « Automatic from ISP [Obtenir automatiquement du FAI] » et entrez les numéros DNS dans les espaces fournis à cet effet. Cliquez sur « Apply changes [Enregistrer les modifications] »(2) pour enregistrer les paramètres.

WAN > DNS

If your ISP provided you with a specific DNS address to use, enter the address in this window and click "Apply Changes".

(1) Automatic from ISP

DNS Address > 0 0 0 0

Secondary DNS Address > 0 0 0 0

DNS = Domain Name Server. A server located on the Internet that translates URL's (Universal Resource Links) like www.belkin.com to IP addresses. More Info

Clear changes Apply Changes (2)

Utilisation du DDNS (Dynamic DNS)

Le service DNS Dynamique vous permet d'attribuer une adresse IP dynamique à un nom d'hôte statique parmi ceux offerts par DynDNS.org, ce qui vous permet d'accéder à vos ordinateurs à partir de maints endroits sur Internet. DynDNS.org offre ce service à la communauté des Internaute, gratuitement, pour jusqu'à cinq noms d'hôte. TZO est une alternative à DynDNS.org. Le service DNS Dynamique est idéal pour les sites web maison, les serveurs de fichiers, ou pour vous faciliter l'accès à votre PC ou aux fichiers stockés sur votre PC lorsque vous êtes au boulot. Le service garantit que votre nom d'hôte pointe toujours vers votre adresse IP, peu importe si votre FAI modifie celle-ci. Lorsque votre adresse IP change, vos amis et associés peuvent toujours vous retrouver en visitant votrenom.dyndns.org ! Inscrivez-vous gratuitement et obtenez votre nom d'hôte DNS Dynamique à <http://www.dyndns.org>.

Configuration du client DNS Dynamique du routeur

Vous devez vous inscrire au service gratuit de mise à jour de DynDNS.org avant d'utiliser cette fonction. Après vous être inscrit, veuillez suivre les étapes ci-dessous.

1. Entrez votre nom d'utilisateur DynDNS dans le champ « Account / E-mail » (1).
2. Entrez votre mot de passe DynDNS.org dans le champ « Password » (2).
3. Entrez votre nom d'utilisateur DynDNS.org dans le champ « User Name [Nom d'utilisateur] » (3).
4. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour mettre à jour l'adresse IP.

Lorsque votre FAI modifie l'adresse IP qui vous est attribuée, le routeur s'occupe de la mise à jour des serveurs DynDNS.org, avec votre nouvelle adresse IP. Vous pouvez également le faire manuellement, en cliquant sur le bouton « Update Dynamic DNS [Mise à jour DNS Dynamique] » (4).

partir de la page Type de connexion, choisissez le type de connexion dont vous disposez à partir du menu déroulant.

WAN > DDNS

DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP address is dynamic. You must Register for DDNS service at one of the listed DDNS Services.

DDNS Service >

DDNS Status >

(1) Account / E-mail >

(2) Password / Key >

(3) Domain Name >

(4)

Technologie

L'onglet Sans Fil vous permet d'apporter des modifications aux paramètres de votre réseau sans fil. Vous pouvez apporter des modifications au nom du réseau sans fil (SSID), au canal d'opération et aux paramètres de chiffrement.

Canal et SSID

Wireless > Channel and SSID

This page allows you to enter the Wireless Network Name (SSID in Wi-Fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as an wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. More Info

SSID >	<input type="text" value="Belkin54g"/>
ESSID Broadcast >	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode >	<input type="text" value="Mixed (11b+11g)"/>
Wireless Channel >	<input type="text" value="Auto"/>
<input type="button" value="Clear Changes"/> <input type="button" value="Apply Changes"/>	

1. Modification du nom du réseau sans fil (SSID)

Le SSID (Service Set Identifier) correspond au nom de votre réseau sans fil. Vous pouvez le modifier selon vos goûts, ou le laisser tel quel. S'il y a d'autres réseaux sans fil en fonction dans votre zone, assurez-vous que votre SSID est unique (n'est pas identique au SSID d'un autre réseau sans fil dans votre zone). Pour modifier le SSID, entrez le SSID désiré dans le champ SSID et cliquez sur « Apply Changes [Enregistrer les modifications] » pour valider le changement. Le changement est immédiat. Si vous modifiez le SSID, vos ordinateurs sans fil doivent aussi être configurés à l'aide de ce même SSID afin qu'ils puissent se connecter à votre réseau sans fil. Reportez-vous à la documentation de votre adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

2. Utilisation de la fonction de diffusion ESSID

Pour des raisons de sécurité, vous pouvez choisir de ne pas diffuser le SSID de votre réseau. Ainsi, le nom de votre réseau restera caché lorsque d'autres ordinateurs recherchent la présence de réseaux sans fil. Pour désactiver la diffusion du SSID, sélectionnez « Désactiver » et cliquez sur « Apply Changes [Enregistrer les modifications] ». Le changement est immédiat. Chaque ordinateur doit maintenant être défini pour se connecter à votre SSID. Le paramètre « ANY » (TOUS) pour le SSID ne sera plus accepté. Reportez-vous à la documentation de votre adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

Remarque : Cette fonction avancée ne devrait être utilisée que par les utilisateurs avancés.

3. Utilisation de la fonction de commutation entre les modes sans fil

Votre routeur est en mesure de fonctionner sous trois modes sans fil différents : « Mixed », « 11g Only », et « 11b Only ». Ces modes vous sont décrits ci-dessous.

Mixte (11b+11g)

Dans ce mode, le routeur est compatible avec des clients sans fil 802.11b et 802.11g, de façon simultanée. Ce mode est le mode par défaut, et vous assure une entière compatibilité avec tous les dispositifs Wi-Fi®. Si votre réseau se compose de clients 802.11b et 802.11g, nous vous recommandons le paramètres par défaut. Ce paramètre ne devrait pas être modifié que si vous avez une raison spécifique de le faire,

Mode 11g-Only

Ce mode ne fonctionne qu'en présence de clients 802.11g. Ce mode n'est recommandé que si vous désirez empêcher l'accès à votre réseau aux clients 802.11b. Pour basculer vers un autre mode, sélectionnez le mode désiré à partir du menu déroulant à côté de « Mode sans fil ». Ensuite, cliquez sur « Apply Changes [Enregistrer les Modifications] ».

Mode 802.11b-Only

Il n'est PAS recommandé d'utiliser ce mode à moins que vous ne le deviez absolument. Ce mode existe dans l'unique but de résoudre les problèmes pouvant survenir avec certains adaptateurs 801.11b et n'est PAS nécessaire pour assurer l'interopérabilité entre les normes 802.11b et 802.11g.

4. Modification du canal

Vous pouvez choisir parmi plusieurs canaux de fonctionnement. Aux États-Unis, il existe 11 canaux. Au Royaume-Uni et dans la plupart des pays d'Europe, il existe 13 canaux. Dans un petit nombre de pays, il existe d'autres exigences par rapport aux canaux. Votre routeur est configuré de façon à fonctionner sur les canaux appropriés à votre pays de résidence. Le nom par défaut est « Auto ». Vous pouvez modifier le canal au besoin. S'il y a d'autres réseaux sans fil en fonction dans votre zone, votre réseau devrait fonctionner sur un canal différent de ceux utilisés par ces autres réseaux sans fil. Pour de meilleures performances, nous vous suggérons d'utiliser un canal éloigné des autres réseaux sans fil d'au moins cinq canaux. Par exemple, si un autre réseau fonctionne sur le canal 11, configurez votre réseau afin qu'il fonctionne sur le canal 6 ou moins. Pour modifier le canal, sélectionnez le canal à partir du menu déroulant. Cliquez sur « Apply Changes [Enregistrer les Modifications] ». Le changement est immédiat.

chiffrement/sécurité

Protection de votre réseau sans fil Wi-Fi

Il existe plusieurs façons de garantir la sécurité de votre réseau sans fil et protéger vos données des intrus. Cette section est destinée aux utilisateurs de réseaux sans fil à domicile, ou en entreprise (y compris les bureaux à domicile). Au moment de mettre ce manuel sous presse, quatre méthodes de chiffrement sont disponibles.

Nom	Wired Equivalent Privacy 64 bits	Wired Equivalent Privacy 128 bits	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronyme	WEP sur 64 bits	WEP sur 128 bits	WPA-TKIP/AES (ou WPA)	WPA2-AES (ou WPA2)
Sécurité	Bon	Mieux	Meilleur	Excellent
Caractéristiques	Clés statiques	Clés fixes	Chiffrement dynamique de la clé et authentification mutuelle	Chiffrement dynamique de la clé et authentification mutuelle
	Clés de chiffrement basées sur l'algorithme RC4 (clés de 40 bits)	Sécurité renforcée par rapport au WEP sur 64 bits, utilisant une clé de 104 bits, plus 24 bits additionnels pour des données générées par le système.	Le TKIP (temporal key integrity protocol) s'ajoute afin d'assurer la rotation des clés et de renforcer le chiffrement	L'AES (Advanced Encryption Standard) n'entraîne pas de perte de performances

Wired Equivalent Privacy (WEP)

Le WEP (Wired Equivalent Privacy) est un protocole courant qui renforce la sécurité de tous les dispositifs sans fil Wi-Fi. Le WEP est conçu dans le but d'offrir aux réseaux sans fil un niveau de protection comparable à celui des réseaux filaires.

WEP sur 64 bits

Le WEP 64 bits a été introduit la première fois avec un chiffrement de 64 bits, ce qui comprend une clé de 40 bits plus 24 bits supplémentaires composés de données générées par le système (64 bits au total). Certains fabricants réfèrent au chiffrement sur 64 bits lorsqu'ils parlent du chiffrement sur 40 bits. Peu après le lancement de la technologie, les chercheurs ont découvert que le chiffrement sur 64 bits était trop simple à décoder.

WEP sur 128 bits

Pour contrer la faille de sécurité du WEP 64 bits, une méthode de chiffrement plus sécurisée, le WEP 128 bits, a été créée. Le WEP sur 128 bits comprend une clé de 104 bits plus 24 bits supplémentaires composés de données générées par le système (128 bits au total). Certains fabricants réfèrent au chiffrement sur 128 bits lorsqu'ils parlent du chiffrement sur 104 bits. La plupart des dispositifs sans fil disponibles sur le marché aujourd'hui prennent en charge le chiffrement WEP sur 64 et 128 bits, mais il se peut que vous possédiez un dispositif plus ancien ne prenant en charge que le WEP sur 64 bits. Tous les produits sans fil de Belkin prennent en charge le WEP 64 et 128 bits.

Clés de chiffrement

Après avoir choisi le mode de chiffrement (64 ou 128 bits), il est primordial de générer une clé de chiffrement. Si la clé de chiffrement n'est pas la même à travers tout le réseau sans fil, vos dispositifs sans fil ne seront pas en mesure de communiquer entre eux sur votre réseau. Vous pouvez entrer votre clé en entrant la clé hexadécimale manuellement ou vous pouvez entrer une expression mot de passe dans le champ « Passphrase [Expression mot de passe] » et cliquer sur « Generate [Générer] » pour créer la clé. Une clé hexadécimale est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP 64 bits, vous devez entrer 10 clés hexadécimales. Pour le WEP 128 bits, vous devez entrer 26 clés hexadécimales.

Par exemple :

AF 0F 4B C3 D4 = clé WEP sur 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé WEP sur 128 bits

L'expression mot de passe WEP n'est PAS la même chose que la clé WEP. Votre carte se sert de cette expression mot de passe pour générer vos clés WEP, mais les différents fabricants peuvent avoir des méthodes différentes de générer ces clés. Si vous possédez des appareils venant de différents fabricants sur votre réseau, la solution la plus simple consiste à utiliser la clé hex WEP de votre routeur ou de votre point d'accès et l'entrer manuellement dans la table de clés hex WEP, dans l'écran de configuration de votre adaptateur.

Accès protégé par WiFi (WiFi protected Access - WPA)

Le WPA (Wi-Fi Protected Access) est une nouvelle norme Wi-Fi, surpassant les caractéristiques de sécurité du WEP. Pour utiliser la sécurité WPA, vos dispositifs sans fil doivent être mis à jour avec les logiciels et les pilotes prenant en charge le WPA. Ces mises à jour peuvent être téléchargées à partir du site Web de leurs fabricants respectifs. Il existe deux types de sécurité par WPA : le WPA-PSK (sans serveur) et le WPA (avec serveur radius).

WPA-PSK (sans serveur)

Le WPA-PSK utilise ce qu'on appelle une clé pré-partagée comme clé de sécurité. Une clé réseau est en quelque sorte un mot de passe composé de 8 à 63 caractères. Il peut être composé de lettres, de chiffres ou de symboles. Chaque client utilise la même clé pour accéder au réseau. De façon générale, ce mode est utilisé pour les réseaux domestiques.

Configuration du WPA (avec serveur radius)

Avec ce système, un serveur radius distribue les clés réseau aux clients de façon automatique. Ce système se retrouve surtout en entreprise.

WPA2

Le routeur comprend une fonction WPA2, la deuxième génération de chiffrement WPA, basé sur la norme 802.11i. Elle offre un niveau de protection sans fil plus élevé en combinant une authentification réseau avancée et une méthode de chiffrement AES renforcée.

Configuration requise pour le WPA2

IMPORTANT : Pour utiliser la sécurité WPA2, tous vos ordinateurs et vos adaptateurs clients sans fil doivent être mis à niveau avec des rustines, des clients et des logiciels utilitaires clients prenant en charge le WPA2. Au moment de mettre ce manuel sous presse, plusieurs rustines de sécurité sont disponibles pour téléchargement gratuit, auprès de Microsoft®. Ces patches ne fonctionnent qu'avec Windows XP. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment.

Pour les ordinateurs sous Windows XP sans Service Pack 2 (SP2), un fichier Microsoft appelé « Windows XP Support Patch for Wireless Protected Access (KB 826942) » est disponible pour téléchargement gratuit à <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91>.

Pour Windows XP avec Service Pack 2, Microsoft a lancé un fichier pour téléchargement gratuit afin de mettre à niveau les composants du client sans fil pour prise en charge du WPA2 (KB893357). Vous pouvez télécharger la mise à jour ici : <http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en>.

IMPORTANT : Vous devez également vous assurer que toutes vos cartes/adaptateurs clients sans fil prennent en charge le WPA2, et que vous avez téléchargé et installé le pilote le plus récent. Un pilote mis à jour pour la plupart des cartes sans fil Belkin est disponible pour téléchargement à partir du site de l'assistance technique Belkin : www.belkin.com/networking. Pour la liste des produits Belkin prenant en charge le WPA/WPA2, visitez notre site Web au www.belkin.com/networking.

Partage des clés réseau

La plupart des dispositifs Wi-Fi désactivent la fonction de sécurité par défaut. Après avoir mis en route votre réseau, vous devez activer le WEP ou le WPA et vous assurer que tous les dispositifs sans fil de votre réseau partagent la même clé réseau.

Utilisation d'une clé hexadécimale

Une clé hexadécimale est un mélange de chiffres et de lettres de A à F et de 0 à 9. Les clés sur 64 bits sont formées de 5 nombres à 2 chiffres. Les clés sur 128 bits sont formées de 13 nombres à 2 chiffres.

Par exemple :

AF 0F 4B C3 D4 = clé sur 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé sur 128 bits

Dans les cases ci-dessous, créez vos clés en écrivant deux caractères de A à F et de 0 à 9. Vous utiliserez cette clé pour programmer les paramètres de chiffrement du routeur et les ordinateurs sans fil.

Remarque aux utilisateurs de Mac : Les produits AirPort® d'Apple® ne prennent en charge que le chiffrement sur 64 bits. Les produits Apple AirPort 2 prennent en charge le chiffrement sur 64 bits ou 128 bits. Veuillez vérifier la version de votre produit. Si vous ne parvenez pas à configurer le réseau avec le chiffrement sur 128 bits, essayez sur 64 bits.

Configuration du WEP

1. Sélectionnez « WEP » dans le menu déroulant.
2. Choisissez 64 bits ou 128 bits pour le « WEP Mode [Mode WEP] ».
3. Après avoir sélectionné votre mode de chiffrement WEP, entrez votre clé hexadécimale manuellement.

Une clé hexadécimale est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP 64 bits, vous devez entrer 10 clés hexadécimales. Pour le WEP 128 bits, vous devez entrer 26 clés hexadécimales.

Par exemple :

AF 0F 4B C3 D4 = clé sur 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé sur 128 bits

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [View Help](#)

Allowed Client Type >	WEP
WEP Mode >	<input checked="" type="radio"/> 64 bit <input type="radio"/> 128 bit
Key Entry Method >	<input type="radio"/> HEX <input checked="" type="radio"/> ASCII
Key Provisioning >	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Key 1 >	<input type="text"/>
Key 2 >	<input type="text"/>
Key 3 >	<input type="text"/>
Key 4 >	<input type="text"/>
Default Key ID >	1
Passphrase >	<input type="checkbox"/> <input type="text"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Clear Changes"/>	

3. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Le chiffrement de votre routeur est maintenant configuré. Chaque ordinateur de votre réseau sans fil devra maintenant être configuré avec les mêmes paramètres de sécurité.

AVERTISSEMENT : Si vous configurez le routeur sans fil à partir d'un ordinateur doté d'un client sans fil, vous devez vous assurer que la sécurité est ACTIVÉE pour ce client sans fil. Sinon, vous perdez votre connexion sans fil.

Modification des paramètres de sécurité sans fil

Votre routeur comprend la toute dernière norme de sécurité, appelée WPA/WPA2. Il prend également en charge la norme de sécurité WEP. Par défaut, la sécurité sans fil est désactivée. Pour activer la sécurité, vous devez d'abord déterminer la méthode de chiffrement de votre choix. Pour accéder aux paramètres de sécurité, cliquez sur « Security [Sécurité] », sous l'onglet « Wireless [Sans Fil] ».

Configuration du WPA

Remarque : Pour utiliser la sécurité par WPA, votre client doit être mis à jour avec les logiciels et les pilotes qui le prennent en charge. Au moment de mettre ce manuel sous presse, une rustine de sécurité est disponible pour téléchargement gratuit, auprès de Microsoft. Ce patch ne fonctionne qu'avec Windows XP. Vous devrez en outre télécharger le plus récent pilote pour votre Carte Sans Fil G pour ordinateur de bureau ou portable de Belkin, que vous trouverez sur le site de l'assistance technique de Belkin. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment. Le patch de Microsoft ne prend en charge que les dispositifs avec pilotes compatibles WPA, tels que les produits 802.11g de Belkin.

Il existe deux types de sécurité par WPA : le WPA-PSK (sans serveur) et le WPA (avec serveur radius). Le WPA-PSK (sans serveur) utilise ce qu'on appelle une « clé pré-partagée » (PSK) en tant que clé de sécurité. Une clé pré-partagée est en quelque sorte un mot de passe composé de 8 à 63 caractères. Il peut être composé de lettres, de chiffres ou de symboles. Chaque client utilise la même clé pour accéder au réseau. De façon générale, ce mode est utilisé pour les réseaux domestiques. Le WPA (avec serveur radius) consiste en un système où le serveur radius distribue automatiquement les clés aux clients. Ce système se retrouve surtout en entreprise. Le WPA2, c'est le WPA de seconde génération. Il offre une technique de chiffrement plus avancée que le WPA.

Configuration du WPA/WPA2-PSK (sans serveur)

1. À partir du menu déroulant « Allowed Client Type [Type de client autorisé] », sélectionnez « WPA/WPA2 ».
2. Pour l'authentification, sélectionnez « Pre-shared Key [Clé pré-partagée] » pour particuliers ou petites entreprises. Ce paramètre devra être identique à celui des clients que vous configurerez.
3. Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres, ou symboles). Cette clé doit être utilisée pour tous les clients branchés au réseau. Par exemple, votre clé pré-partagée peut ressembler à : « Clé réseau de la famille Dupont ».

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >

WPA/WPA2

Authentication >

802.1X Pre-shared Key

Pre-shared Key >

Apply Changes

Clear Changes

4. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Configuration du WPA/WPA2 (avec serveur radius)

Si votre réseau utilise un serveur Radius pour distribuer les clés aux clients, veuillez utiliser ce paramètre.

1. À partir du menu déroulant « Allowed Client Type [Type de client autorisé] », sélectionnez « WPA/WPA2 ».
2. Pour la technique de chiffrement, sélectionnez « 802.1x » pour un environnement avec serveur RADIUS. Ce paramètre devra être identique à celui des clients que vous configurerez.
3. Entrez le paramètre de temporisation de la session du serveur radius dans le champ « Session Idle Timeout [Temporisation du temps mort de la session] ».
4. Entrez l'intervalle de clé, le nombre de fois où les clés sont distribuées (en paquets), dans le champ « Re-Authentication Period [Période de ré-authentification] ».
5. Entrez le temps d'attente après l'échec de l'authentification dans le champ « Quiet Period [Période calme] ».
6. Entrez l'adresse IP et le numéro du port de votre serveur Radius dans les champs « Server IP [IP du serveur] » et « Server Port [Port du serveur] ».
7. Entrez la clé radius dans le champ « Secret Key [Clé secrète] ».
8. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Remarque : Assurez-vous que vos ordinateurs sans fil sont mis à jour afin de prendre en charge le WPA2 et possèdent les réglages appropriés permettant une connexion au routeur.

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	WPA/WPA2
Authentication >	<input checked="" type="radio"/> 802.1X <input type="radio"/> Pre-shared Key
Session Idle Timeout >	300 Seconds (0 for no timeout checking)
Re-Authentication Period >	3600 Seconds (0 for no re-authentication)
Quiet Period >	60 Seconds after authentication failed
Server-IP >	192 . 168 . 2 . 1
Server-Port >	1812
Secret Key >	<input type="text"/>
NAS-ID >	<input type="text"/>

Configuration des paramètres de sécurité de votre Carte Sans Fil G Belkin

Remarque : Cette section vous informe sur la configuration de votre Carte Réseau Sans Fil G Belkin pour utilisation de la fonction de sécurité. Jusqu'à maintenant, vous avez configuré votre routeur ou point d'accès sans fil afin qu'il(s) utilise(nt) le WPA ou le WEP. Pour obtenir une connexion sans fil, tous les cartes/adaptateurs réseau sans fil doivent maintenant être configurés avec ces mêmes paramètres de sécurité.

Connexion de votre ordinateur à un réseau sans fil utilisant une clé WEP 64 ou 128 bits :

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte sans fil.
2. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Configure [Configurer] ».
3. Sous « Data Encryption [Chiffrement de données] », sélectionnez « WEP ».
4. Assurez-vous que la case « The key is provided for me automatically [J'obtiens une clé automatiquement] » n'est pas cochée. Si vous utilisez cet ordinateur pour vous connecter à un réseau d'entreprise, prenez conseil auprès de votre administrateur réseau afin de savoir si cette case doit être cochée.
5. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

1

2

3

4

5

6

7

8

9

10

11

Wireless > Security

Security Mode

Key 1

Key 2

Key 3

Key 4

(hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, input it here

PassPhrase

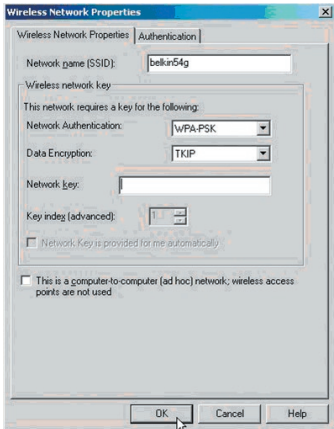
Important : Une clé WEP est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP sur 128 bits, vous devez entrer 26 clés hexadécimales. Pour le WEP sur 64 bits, vous devez entrer 10 clés hexadécimales. Cette clé réseau doit être identique à la clé que vous avez attribuée à votre routeur

6. Cliquez « OK » pour enregistrer les paramètres.

Connexion de votre ordinateur à un réseau sans fil utilisant le WPA-PSK (sans serveur)

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte sans fil.
2. Sous l'onglet « Wireless Network [Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Configure [Configurer] ».
3. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA-PSK (No server) [WPA-PSK (Sans serveur)] ».
4. Entrez votre clé WPA dans la boîte « Network Key [Clé Réseau] ».

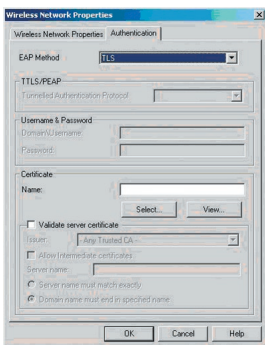
Important : Une clé WPA-PSK est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WPA-PSK, vous devez entrer de 8 à 63 caractères. Cette clé réseau doit être identique à la clé que vous avez attribuée à votre routeur



5. Cliquez « OK » pour enregistrer les paramètres.

Connexion de votre ordinateur à un réseau sans fil utilisant le WPA (avec serveur radius)

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ». Le bouton « Advanced [Avancé] » vous permet d'afficher et de configurer un plus grand nombre d'options de la carte sans fil.
2. Sous l'onglet « Wireless Network [Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Configure [Configurer] ».
3. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA ».
4. Sous l'onglet « Authentication [Authentification] », choisissez les paramètres spécifiés par l'administrateur de votre réseau.



5. Cliquez « OK » pour enregistrer les paramètres.

Configuration du WPA pour les cartes réseau sans fil AUTRES que Belkin

Pour les cartes réseau sans fil pour ordinateurs de bureau ou portable autres que Belkin qui ne prenant pas en charge le WPA, une rustine de Microsoft, nommée « Windows XP Support Patch for Wireless Protected Access » est disponible pour téléchargement gratuit.

Remarque : Cette rustine ne fonctionne qu'avec Windows XP. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment.

Important : Vous devrez en outre vous assurer que le fabricant de votre carte sans fil prend en charge le WPA et que vous avez téléchargé et installé le pilote le plus récent, que vous trouverez sur leur site web.

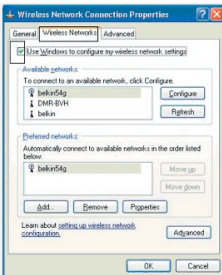
Systèmes d'exploitation pris en charge :

- Windows XP Professionnel
- Windows XP Édition Familiale

Configuration de l'Utilitaire Réseau Sans Fil de Windows XP pour utilisation du WPA-PSK

Afin d'utiliser le WPA-PSK, assurez-vous d'utiliser l'Utilitaire Réseau Sans Fil de Windows. Procédez comme suit :

1. Sous Windows XP, cliquez Démarrer > Panneau de Configuration > Connexions Réseaux et Internet .
2. Cliquez avec le bouton droit de la souris sur « Wireless Network Connection [Connexion Réseau Sans Fil] » et sélectionnez « Propriétés [Propriétés] ».
3. En cliquant avec le bouton droit de votre souris sur « Wireless Networks [Réseaux Sans Fil] », vous verrez une fenêtre s'afficher comme suit : Assurez-vous que la case « Utiliser Windows pour configurer mes paramètres réseau sans fil » est cochée
4. Sous l'onglet « Wireless Networks [Réseaux Sans Fil] », cliquez sur le bouton « Configurer [Configurer] » et vous verrez une fenêtre s'afficher comme suit :



5. Pour l'utilisateur de réseau domestique ou de petite entreprise, sélectionnez « WPA-PSK » sous « Network Authentication [Authentification Réseau] ».

Remarque : Sélectionnez le WPA si vous utilisez cet ordinateur pour vous brancher à un réseau d'entreprise, qui à son tour prend en charge un serveur d'authentification tel que le serveur RADIUS. Renseignez-vous auprès de l'administrateur de votre réseau pour de plus amples informations.



6. Sélectionnez « TKIP » ou « AES » sous « Data Encryption [Chiffrement de données] ». Ce paramètre doit être identique à celui du routeur.

7. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

Important : Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres, ou symboles). Cette clé doit être utilisée pour tous les clients branchés au réseau.

8. Cliquez « OK » pour enregistrer les paramètres.

Extension de portée et Passerelle

Qu'est-ce qu'une Passerelle Sans Fil ?

Il s'agit d'un « mode » de fonctionnement qui peut être utilisé pour étendre la portée de votre réseau sans fil, ou pour ajouter une extension supplémentaire à votre réseau, ailleurs dans votre bureau ou à votre domicile, et ce sans utiliser de câblage.

Remarque : Nous ne pouvons garantir le fonctionnement de ce mode avec du matériel vendu par d'autres fabricants de produits sans fil.

Remarque : Assurez-vous de télécharger la dernière version du micrologiciel du routeur ou du point d'accès pour une performance optimale : <http://web.belkin.com/support>.

Ajouter un autre segment de réseau sans fil

En branchant un switch réseau ou un hub au port RJ45 du routeur, vous permettez aux ordinateurs reliés au switch d'accéder au reste du réseau.

Établir une passerelle entre votre routeur et un point d'accès secondaire

La création d'une passerelle entre votre routeur et un point d'accès secondaire nécessite que vous accédiez à l'Utilitaire de configuration avancée du routeur, et que vous entriez l'adresse MAC du point d'accès dans la case appropriée. Il existe aussi quelques autres pré-requis.

ASSUREZ-VOUS DE PROCÉDER COMME SUIT.

1. Configurez votre point d'accès de façon à ce que le canal de celui-ci soit identique à celui du routeur. Pour savoir comment modifier le canal, voyez la section « Sans Fil - Canal et SSID » de ce manuel.
2. Repérez l'Adresse MAC du point d'accès, que vous trouverez sous celui-ci. Cette étiquette en comporte deux. Vous aurez besoin de l'adresse MAC appelée « WLAN MAC Address ». Cette adresse MAC commence par 0030BD et se poursuit avec six autres chiffres ou lettres (par ex. 0030BD-XXXXXX). Écrivez l'adresse MAC ci-dessous. Passez à l'étape suivante.
3. Placez le point d'accès secondaire à l'intérieur de la portée de fonctionnement du routeur, et près de la zone à laquelle vous désirez étendre la portée ou ajouter un segment de réseau. La portée à l'intérieur peut aller de 15 à 45 mètres.
4. Branchez le bloc d'alimentation sur votre point d'accès. Veillez à ce que votre point d'accès soit allumé, et passez à l'étape suivante.
5. À partir d'un ordinateur déjà relié au routeur, accédez à l'interface de configuration avancée en ouvrant votre navigateur. Dans la barre d'adresse de votre navigateur, tapez « 192.168.2.1 ». N'entrez pas « www » ni « http:// » devant les chiffres. Remarque : Si vous avez modifié l'adresse IP de votre routeur, veuillez utiliser cette adresse IP.
6. Dans la fenêtre de votre navigateur apparaîtra l'interface utilisateur du routeur. Cliquez sur « Wireless Bridge [Pont Sans Fil] » (2) à la gauche de l'écran. Vous verrez l'écran suivant.
7. Cochez la case « Enable ONLY specific Access Points to connect [N'autoriser la connexion qu'à des Points d'Accès spécifiques SEULEMENT] » (1).

Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

(1) **Enable Wireless Bridging.** (enabling this feature allows other Access Points to connect to this Access Point.)

(3) **Enable ONLY specific Access Points to connect.** (enter Wireless MAC Address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Note: the MAC address can be found using a site survey on a wireless client card.)

AP1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Disable ability for Wireless CLIENT to connect. (This feature should only be used when the AP is used exclusively to other APs.)

[Clear Changes](#) [Apply Changes](#)

8. Dans le champ appelé « AP1 », (3) entrez l'adresse MAC de votre point d'accès secondaire. Après avoir entré l'adresse, cliquez sur « Apply Changes [Enregistrer les modifications] ».

9. La passerelle est maintenant établie.

Remarque : Il peut s'écouler environ une minute pour que la passerelle soit établie. Il peut parfois être nécessaire de redémarrer le routeur et le point d'accès pour établir la passerelle.

Pare-feu

Votre routeur est équipé d'un pare-feu qui sert à protéger le réseau d'une variété d'attaques de pirates informatiques, y compris :

- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

Le pare-feu masque en outre les ports réseau qui font fréquemment l'objet d'attaques. Ces ports sont invisibles, ce qui veut dire qu'ils n'existent pas pour un potentiel hacker. Vous pouvez désactiver la fonction de pare-feu au besoin. Toutefois, il est recommandé de que le pare-feu soit activé en tout temps. Désactiver le pare-feu ne rendra pas votre réseau totalement vulnérable aux attaques provenant des pirates informatiques, mais il est recommandé d'activer le pare-feu en tout temps.

Firewall >

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable / Disable > Enable Disable

Clear Changes

Apply Changes

Serveurs Virtuels

Les serveurs virtuels vous permettent d'acheminer, via le routeur et vers votre réseau interne, les appels externes (Internet) de services tels qu'un serveur web (port 80), un serveur FTP (port 21) ou d'autres applications. Parce que vos ordinateurs internes sont protégés par le pare-feu, les machines provenant de l'Internet ne peuvent accéder à ceux-ci puisqu'ils sont invisibles. Si vous devez configurer la fonction de Serveur Virtuel pour une application particulière, vous devez contacter le fabricant de votre application et déterminer quels paramètres de ports sont nécessaires. Vous pouvez entrer ces informations manuellement dans les paramètres du routeur.

Firewall > Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (port 21), or other applications through your Router to your internal network. More info.

No.	List of Address	Description	Protocol Type	Port	Public Port	Enable	Action
1	270.140.0		TCP			<input type="checkbox"/>	Add [Clear]
2	140.140.0		TCP			<input type="checkbox"/>	Add [Clear]
3	270.140.0		TCP			<input type="checkbox"/>	Add [Clear]

Choix d'une application

Choisissez votre application à partir de la liste déroulante. Cliquez sur « Add [Ajouter] ». Les paramètres seront alors transférés vers la place suivante disponible à l'écran. Cliquez sur « Apply Changes [Enregistrer les Modifications] » pour sauvegarder les paramètres de cette application. Pour supprimer l'application, sélectionnez le numéro de la ligne à supprimer, puis cliquez sur « Clear [Effacer] ».

Saisie manuelle des paramètres du serveur virtuel

Pour saisir manuellement les paramètres, entrez l'adresse IP dans le champ fourni pour la machine (serveur) interne, les ports requis pour la transmission, choisissez le type de port (TCP ou UDP), puis cliquez sur Apply Changes [Enregistrer les Modifications]. Chaque entrée de port d'entrée possède deux champs, pouvant contenir 5 caractères maximum. Ces champs délimitent le début et la fin de la plage, soit [xxxxx]-[xxxxx]. Pour chaque entrée, vous pouvez entrer une seule valeur de port en remplissant les deux champs avec la même valeur (par ex. [75000]-[75000]) ou une plage étendue (par ex. [75000]-[9000]). Si vous avez besoin de valeurs multiples pour un seul port, ou plusieurs plages et une seule valeur, vous devez utiliser plusieurs entrées (maximum de 20). Par ex": 1. [7500]-[7500] 2. [8023]-[8023] 3. [9000]-[9000]). Vous pouvez seulement faire passer un seul port par adresse IP interne. L'ouverture des ports de votre pare-feu peut compromettre la sécurité de votre réseau. Vous pouvez facilement activer ou désactiver cette fonction. Il est recommandé de désactiver cette fonction lorsque vous n'utilisez pas une application spécifique.

Filtres d'IP des clients

Le routeur peut être configuré de sorte à limiter l'accès de certains ordinateurs à Internet, au courrier électronique et autres fonctions réseaux, à des jours et des heures donnés. La restriction peut s'appliquer à un seul ordinateur, à un groupe d'ordinateurs ou à plusieurs ordinateurs.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. More Info

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function > Enable Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

> Add PC

Apply Changes

Contrôle de l'Accès

Le contrôle d'accès permet aux utilisateurs de définir le type de trafic permis ou non permis, au port du réseau sans fil local. Le paramètre part défaut permet le trafic sortant. Pour configurer la restriction d'accès à votre ordinateur, veuillez procéder comme suit :

1. Cliquez « Add PC [Ajouter un PC] » à l'écran du contrôle de l'accès.
2. Définissez les paramètres appropriés pour le service client (tel que démontré à l'écran suivant).

Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. More Info

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL Blocking function, you need to configure the URL address first on the "URL Blocking SW" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address > -

> Client PC Services:

Service Name	Default Description	Blocking
WWW	HTTP, TCP Port 80, 8080, 8081, 8082	<input checked="" type="checkbox"/>
WWW with URL Blocking	HTTP (with URL Blocking SW Page)	<input checked="" type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input checked="" type="checkbox"/>
News Feeds	NNTP, TCP Port 119	<input checked="" type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input checked="" type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input checked="" type="checkbox"/>
MSN Messenger	TCP Port 1863	<input checked="" type="checkbox"/>
Default Service	TCP Port 25	<input checked="" type="checkbox"/>

3. Cliquez sur « OK » et sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres.

Blocage d'URL

Pour configurer la fonction de Blocage d'URL, spécifiez les sites web (www.unsite.com) et/ou les mots-clés que vous désirez voir filtrés sur votre réseau. Cliquez sur « Apply Changes [Enregistrer les Modifications] » pour que celles-ci soient prises en compte. Pour terminer cette configuration, vous devrez créer ou modifier une règle d'accès à la section Filtrage d'IP des clients. Pour modifier une règle existante, cliquez sur l'option Modifier située à côté de la règle à modifier. Pour créer une nouvelle règle, cliquez sur l'option « Ajouter un PC ». À partir de la section « Contrôle d'Accès > Ajouter un PC », cochez l'option « WWW avec Blocage d'URL » dans le tableau de « Service de PC client », pour filtrer les sites web et les mots-clés spécifiés.

Configuration manuelle du routeur

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

To configure the URL Blocking feature, use the table below to specify the websites ([www.somewhere.com](#)) and or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section. To modify an existing rule, click the "Edit" option next to the rule you want to modify. To create a new rule, click on the "Add PC" option.

From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below.

Rule Number	URL / Keyword
SNL_1	
SNL_2	
SNL_3	
SNL_4	
SNL_5	

Règle d'horaire

Vous pouvez filtrer l'accès à Internet des clients locaux à l'aide de règles. Chaque règle d'accès peut être activée à un moment déterminé. Définissez l'horaire sous « Règle d'horaire » et appliquez la règle à la page « Contrôle d'accès ».

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Rule Name	Rule Comment	Configure
	No Valid Schedule Rule ID	

> Add Schedule Rule

[Clear Changes](#) [Apply Changes](#)

Procédez comme suit pour ajouter un horaire.

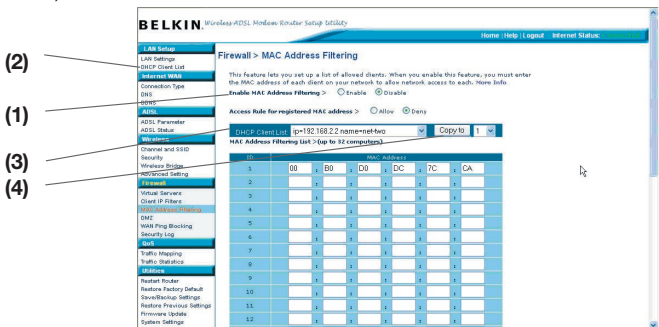
1. Cliquez sur « Add Schedule Rule [Ajouter une règle d'horaire] ».
2. Vous verrez l'écran suivant.
3. Pour configurer la Règle d'horaire, spécifiez le Nom, le Commentaire, l'Heure du début et l'Heure de fin que vous désirez filtrer sur votre réseau.
4. Cliquez sur « OK » et sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres.
5. Pour terminer cette configuration, vous devrez créer ou modifier une règle d'accès à la section Filtrage d'IP des clients. Ceci active l'horaire qui sera utilisé à la page « Contrôle d'accès ».

Configuration du filtrage d'adresses MAC

Le filtrage d'adresses MAC est une fonction de sécurité puissante qui vous permet de spécifier les ordinateurs autorisés à se connecter au réseau. Tout ordinateur non spécifié dans les paramètres du filtre et qui tente d'accéder au réseau se verra refuser l'accès. Lorsque vous activez cette fonction, vous devez entrer l'adresse MAC de chaque client (ordinateur) de votre réseau, pour permettre à chacun d'accéder au réseau. La fonction « Block [Bloquer] » vous permet d'activer et de désactiver facilement l'accès au réseau pour tout ordinateur, sans devoir ajouter l'adresse MAC de l'ordinateur à la liste ni la supprimer. Pour activer cette fonctionnalité, sélectionnez « Enable MAC Address Filtering [Activer le filtrage d'adresses MAC] » (1). Ensuite, définissez la règle d'accès à « Allow [Autoriser] » ou « Deny [Refuser] ».

Ensuite, entrez l'adresse MAC de chaque ordinateur de votre réseau à partir de la boîte déroulante « DHCP Client List [Liste de clients DHCP] » (2) et l'identifiant à copier (3) avant de cliquer sur « Copy to [Copier vers] ». Ou en cliquant dans l'espace donné (4) et en entrant l'adresse MAC de l'ordinateur à ajouter à la liste. Cliquez sur « Apply changes [Enregistrer les modifications] » (5) pour enregistrer les paramètres. Ensuite, cliquez sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres.

Remarque : Vous ne pourrez pas supprimer l'adresse MAC de l'ordinateur que vous utilisez pour accéder aux fonctions d'administration du routeur (celui que vous utilisez en ce moment).



DMZ (zone démilitarisée)

Si un de vos PC clients ne peut exécuter une application Internet convenablement parce qu'il se trouve derrière un pare-feu, vous pouvez modifier les restrictions en permettant à l'accès à internet bidirectionnel. Cette opération peut s'avérer nécessaire si la traduction d'adresse réseau (NAT) empêche le bon fonctionnement d'applications telles que les jeux ou les vidéoconférences. Servez-vous de cette fonction au besoin. L'ordinateur placé dans la zone DMZ ne sera pas protégé contre les attaques provenant de hackers.

Configuration manuelle du routeur

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** [More Info](#)

DMZ > ENABLE DISABLE

> IP Address of Virtual DMZ Host

Index	IP	Host IP
1	0 0 0 0	192.168.2.0
2	0 0 0 0	192.168.2.0
3	0 0 0 0	192.168.2.0
4	0 0 0 0	192.168.2.0
5	0 0 0 0	192.168.2.0
6	0 0 0 0	192.168.2.0
7	0 0 0 0	192.168.2.0
8	0 0 0 0	192.168.2.0

Pour placer un ordinateur dans la DMZ, entrez les derniers chiffres de son adresse IP dans le champ « IP », puis cliquez sur « Enable [Activer] ». Cliquez sur « Apply Changes [Enregistrer les modifications] » pour que le changement soit pris en compte. Si vous utilisez plusieurs adresses IP WAN fixes, il est possible de sélectionner vers quelle adresse IP WAN l'hôte DMZ sera dirigé. Entrez l'adresse IP WAN vers laquelle doit se diriger l'hôte DMZ, entrez les deux derniers chiffres de l'adresse IP de l'ordinateur hôte DMZ, sélectionnez « Enable [Activer] », puis cliquez sur « Apply Changes [Enregistrer les modifications] ».

Blocage du ping ICMP

Les pirates informatiques utilisent une technique appelée Pinging pour dénicher sur Internet leurs victimes potentielles. En faisant un ping vers une adresse IP particulière et en recevant une réponse de la part de celle-ci, un pirate informatique peut décider de s'intéresser à ce qui se trouve derrière cette adresse. Le routeur peut être défini de façon à ne pas répondre à un ping ICMP provenant de l'extérieur. Ceci rehausse le niveau de sécurité de votre routeur.

Firewall > WAN Ping Blocking

ADVANCE FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to WAN port).

This offers a heightened level of security. [More Info](#)

Block ICMP Ping

(1)

Pour désactiver la réponse au ping, sélectionnez « Block ICMP Ping [Bloquer le ping ICMP] » (1), puis cliquez sur « Apply Changes [Enregistrer les modifications] ». Le routeur ne répondra pas aux pings ICMP.

Utilitaires

L'écran Utilitaires vous permet de gérer plusieurs paramètres du routeur et accomplir certaines tâches administratives.

Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Restart Router**
Sometimes it may be necessary to Reset or Reboot the Router if it begins working improperly. Resetting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Defaults**
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Current Settings**
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Saved Settings**
This option will allow you to restore a previously saved configuration.
- **Firmware Update**
From time to time, Linksys may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
- **System Settings**
The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the NAT function of the Router.

Redémarrer le routeur

Il peut parfois être utile de redémarrer le routeur lorsque celui-ci fonctionne de façon incongrue. Le redémarrage ou le réamorçage du routeur ne supprimera AUCUN de vos paramètres de configuration.

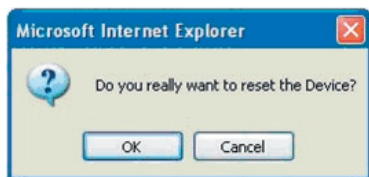
Utilities > Restart Router

Sometimes it may be necessary to Restart or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.

Restart Router

Redémarrer le routeur pour rétablir le fonctionnement normal

1. Cliquez sur le bouton « Restart Router [Redémarrer le routeur] ».
2. Le message suivant apparaît. Cliquez sur « OK » pour redémarrer le routeur.



Rétablir les paramètres par défaut du fabricant

Cette option rétablira les paramètres du routeur vers les paramètres par défaut du fabricant. Nous vous recommandons de faire une copie de sauvegarde de vos paramètres avant de rétablir la configuration par défaut.

Utilities > Restore Factory Defaults

This option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.

Restore Defaults

Configuration manuelle du routeur

1. Cliquez sur le bouton « Restore Defaults [Rétablir les Paramètres] ».
2. Le message suivant apparaît. Cliquez sur « OK » pour rétablir les paramètres par défaut du fabricant.



Enregistrer/Sauvegarder les paramètres actuels

Vous pouvez sauvegarder votre configuration actuelle grâce à cette fonction. Cela vous permettra de la rétablir plus tard si vous perdez les paramètres ou s'ils sont modifiés. Nous vous recommandons de faire une copie de vos paramètres avant de mettre à jour le micrologiciel.

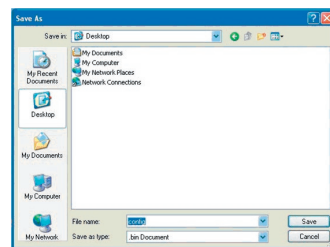
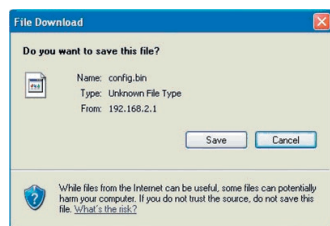
1. Cliquez « Save [Enregistrer] ». La fenêtre « File Download [Téléchargement de fichier] » apparaît. Cliquez sur « Save [Enregistrer] ».

UTILITIES > Save/Backup current settings

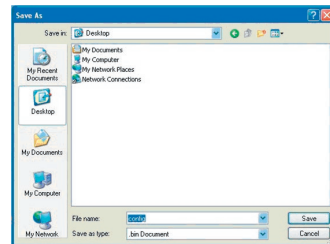
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

OK

2. Une nouvelle fenêtre s'ouvrira pour vous permettre de choisir l'endroit où se trouve le fichier de configuration. Sélectionnez un emplacement. Vous pouvez donner n'importe quel nom à votre fichier, mais assurez-vous de pouvoir le retrouver plus tard. Lorsque vous avez choisi l'emplacement et le nom du fichier, cliquez sur « Save [Enregistrer] ».



3. Lorsque la sauvegarde est terminée, vous verrez la fenêtre ci-dessous. Cliquez sur « Close » (Fermer). Votre configuration est maintenant sauvegardée.



Rétablir les Paramètres Précédents

Cette option vous permet de rétablir une configuration sauvegardée préalablement.

Utilities > Restore Previous Settings

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the "Restore" button below.

1. Cliquez « Browse [Parcourir] ». Une nouvelle fenêtre s'ouvrira pour vous permettre de choisir l'endroit où se trouve le fichier de configuration. Localisez le fichier de configuration « config.bin » désiré et double-cliquez sur celui-ci.
2. Cliquez sur « Open [Ouvrir] ».

Mise à jour du micrologiciel

De temps à autre, Belkin peut lancer une nouvelle version du micrologiciel du routeur. Ces mises à jour peuvent contenir des améliorations et des solutions aux problèmes existants. Lorsque Belkin lance un nouveau micrologiciel, vous pouvez le télécharger à partir du site de mises à jours de Belkin, et mettre à jour votre micrologiciel avec la toute dernière version.

Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click here to go to the Search/Backup current settings page.](#)

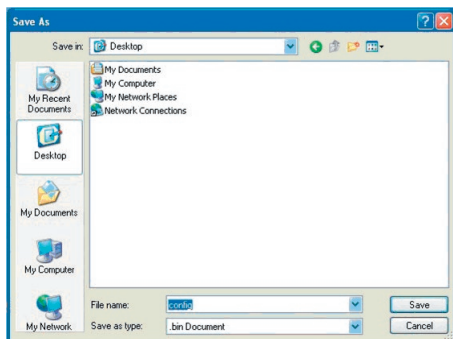
Recherche d'une nouvelle version du micrologiciel

Le bouton « Check Firmware [Vérifier le micrologiciel] » (1) vous permet de vérifier instantanément s'il existe une nouvelle version du micrologiciel. Lorsque vous cliquez sur le bouton, une fenêtre de navigateur apparaît. Elle vous informe qu'aucune nouvelle version n'est disponible ou, au contraire, qu'il existe une nouvelle version. Vous aurez alors la possibilité de la télécharger.

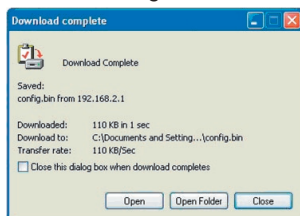
Téléchargement de la nouvelle version du micrologiciel

Si vous cliquez sur le bouton « Check Firmware [Vérifier le micrologiciel] » et qu'une nouvelle version est disponible, un écran similaire à celui-ci apparaît.

1. Pour télécharger la nouvelle version du micrologiciel, cliquez sur « Download [Télécharger] ».
2. Une fenêtre apparaît. Elle vous permet de sélectionner l'emplacement où vous souhaitez enregistrer le micrologiciel. Sélectionnez un emplacement. Vous pouvez donner à votre fichier le nom que vous voulez. Vous pouvez également utiliser le nom par défaut. Veillez à placer le fichier à un endroit où vous pourrez le retrouver ultérieurement. Une fois l'emplacement choisi, cliquez sur « Save [Enregistrer] ».

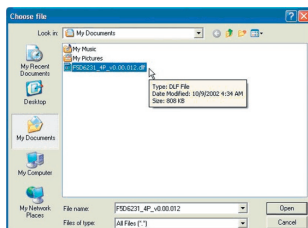


3. Lorsque la sauvegarde est terminée, vous verrez la fenêtre ci-dessous. Cliquez sur « Close [Fermer] ». Le téléchargement du micrologiciel est terminé. Pour mettre le logiciel à jour, procédez comme indiqué dans la section « Mise à jour du micrologiciel du routeur ».



Mise à jour du micrologiciel du routeur

1. Sur la page « Firmware Update [Mise à jour du micrologiciel] », cliquez sur « Browse [Parcourir] » (2). Une nouvelle fenêtre s'ouvrira pour vous permettre de choisir l'endroit où se trouve le fichier de mise à jour du micrologiciel.



2. Parcourez afin de localiser le fichier que vous venez de télécharger. Sélectionnez le fichier en double-cliquant sur le nom du fichier.
3. La boîte de dialogue « Update Firmware [Mise à jour du micrologiciel] » affiche maintenant l'emplacement et le nom du fichier que vous venez de sélectionner. Cliquez sur « Update [Mettre à jour] ».

Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click Here](#) to go to the Save/Backup current settings page.

Firmware Version > 3.01.05
Check for new firmware version >

Update Firmware >

4. Un message vous demande si vous êtes certain de vouloir continuer. Cliquez sur « OK ».



5. Un autre message apparaît. Il vous informe que le routeur peut ne pas répondre pendant une minute, car le micrologiciel est en cours de chargement et que le routeur est en cours de redémarrage. Cliquez sur « OK ».



Le compte à rebours de 60 secondes apparaît à l'écran. Lorsqu'il parvient à zéro, la mise à jour du micrologiciel du routeur est terminée. La page d'accueil du routeur doit apparaître automatiquement. Si tel n'est pas le cas, saisissez l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation de votre navigateur.

Paramètres du Système

À la page des Paramètres du Système, vous pouvez entrer un nouveau mot de passe administrateur, régler le fuseau horaire, activer la gestion à distance, et activer/désactiver la fonction de NAT du routeur.

Entrer ou modifier le mot de passe administrateur

Le routeur est livré SANS mot de passe défini. Si par souci de sécurité vous désirez ajouter un mot de passe, vous pouvez le configurer ici. Écrivez votre mot de passe et conservez-le dans un endroit sûr, puisque vous en aurez besoin plus tard pour vous connecter au routeur. Nous recommandons aussi l'ajout d'un mot de passe si vous prévoyez utiliser la fonction de gestion à distance du routeur.

Utilities > System Settings

Administrator Password:

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

Modification du délai de temporisation de la connexion

L'option de temporisation de la connexion vous permet de déterminer une plage horaire pendant laquelle vous pouvez être connecté à l'interface de configuration avancée du routeur. La temporisation débute lorsqu'il n'y a plus d'activité. Par exemple, vous avez apporté des modifications au niveau de l'interface de configuration évoluée, puis vous avez quitté l'ordinateur sans cliquer sur « Logout [Déconnexion] ». En prenant pour exemple un temporisateur paramétré à 10 minutes, votre connexion prendra fin 10 minutes après votre départ. Vous devrez donc vous connecter à nouveau au routeur pour apporter d'autres modifications. L'option de temporisation de la connexion sert à des fins de sécurité, et le paramètre par défaut est 10 minutes. Remarque : Un seul ordinateur à la fois peut être connecté à l'interface de configuration avancée du routeur.

Définition d'un fuseau horaire

Le routeur harmonise le temps en se connectant à un serveur SNTP (Simple Network Time Protocol). Ceci permet au routeur de synchroniser l'horloge du système avec l'Internet planétaire. L'horloge ainsi synchronisée est utilisée par le routeur pour garder un journal de connexions et pour contrôler le filtrage des clients. Sélectionnez votre fuseau horaire. Si vous demeurez dans une région ayant recours à l'heure d'été, cochez la boîte située à côté de « Enable Daylight Saving [Activer l'heure d'été] ». L'horloge du système peut ne pas être mise à jour immédiatement. Laissez au minimum 15 minutes au routeur pour contacter les serveurs horaires sur Internet et obtenir une réponse. Vous ne pouvez pas modifier l'horloge vous-même. Vous avez maintenant l'option de sélectionner un serveur NTP principal et secondaire afin que l'horloge de votre routeur soit synchronisée avec les serveurs temps NTP de l'Internet. Sélectionnez le serveur NPT à partir du menu déroulant ou conservez le serveur par défaut.

Time and Time Zone: **August 1, 2003 4:26:00 AM**

Please set your time zone. If you are in an area that observes daylight saving check this box. [More Info](#)

Daylight Savings

Set Time Zone > (GMT-08:00/Pacific Time (US & Canada)) **Tijuana**

Configure Time Server (NTP) > Enable Automatic Time Server Maintenance

Primary Server > 132.163.4.102 - North America

Secondary Server > 192.5.41.41 - North America

[Apply Changes](#)

Activer de la gestion à distance

Avant d'activer cette fonctionnalité évoluée de votre routeur Belkin, ASSUREZ-VOUS D'AVOIR DÉFINI VOTRE MOT DE PASSE ADMINISTRATEUR. La gestion à distance vous permet d'apporter des changements aux paramètres de votre routeur, où que vous soyez grâce à l'Internet.

Il existe deux méthodes de gestion à distance du routeur. La première consiste à accéder au routeur depuis un endroit quelconque d'Internet en sélectionnant « Any IP address can remotely manage the Router [Toute adresse IP peut gérer le routeur à distance] ». Lorsque vous aurez entré votre adresse IP WAN depuis un ordinateur sur Internet, un écran de connexion apparaîtra. Vous devrez y entrer le mot de passe du routeur. La seconde méthode consiste à autoriser une seule adresse IP spécifique à gérer le routeur à distance. Cette méthode est la plus sécuritaire, mais la moins pratique. Pour y avoir recours, entrez l'adresse IP autorisée à accéder au routeur dans le champ fourni à cet effet, puis sélectionnez « Only this IP address can remotely manage the Router [Seule cette adresse IP est autorisée à gérer le routeur à distance] ».

Avant d'activer cette fonction, il est FORTEMENT RECOMMANDÉ d'entrer un mot de passe administrateur. Si vous laissez le mot de passe vide, vous autorisez potentiellement des intrusions sur le routeur. Le port d'accès distant est 8080 par défaut. Vous pouvez choisir un port différent en entrant un nouveau numéro de port dans le champ « Remote port [Port distant] ». Cliquez sur le bouton « Apply Changes [Enregistrer les modifications] » pour enregistrer les paramètres.



Activation/Désactivation du NAT (Network Address Translation)

Remarque : Cette fonction avancée ne devrait être utilisée que par les utilisateurs avancés. Avant d'activer cette fonction, ASSUREZ-VOUS D'AVOIR DÉFINI LE MOT DE PASSE DE L'ADMINISTRATEUR. La traduction d'adresses réseau (Network Address Translation, NAT) est la méthode qui permet au routeur de partager une seule adresse IP attribuée par le FAI avec les autres ordinateurs du réseau. Cette fonction ne devrait être utilisée que si votre FAI vous attribue de multiples adresses IP, ou vous devrez désactiver la NAT pour accéder aux configurations avancées du système. Si vous ne possédez qu'une adresse IP et désactivez la NAT, les ordinateurs de votre réseau ne pourront accéder à l'Internet. D'autres problèmes peuvent aussi survenir. La désactivation NAT désactive les fonctions de votre pare-feu.



Activer/désactiver l'UPnP (Universal Plug-and-Play)

L'UPnP (Universal Plug-and-Play) est une fonction avancée unique à votre routeur. C'est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux, et d'autres applications compatibles avec l'UPnP.

Certaines applications nécessitent que le pare-feu du routeur soit configuré selon certains paramètres pour fonctionner adéquatement. Pour ce faire, vous devez habituellement ouvrir des ports TCP et UDP, et parfois même configurer des ports de déclenchement. Une application qui est compatible avec l'UPnP possède la capacité de communiquer avec le routeur, lui indiquant la façon dont le pare-feu doit être configuré. Le routeur est livré avec la fonction UPnP désactivée. Si vous utilisez une application qui est compatible avec l'UPnP, et si vous désirez bénéficier des avantages de l'UPnP, vous pouvez activer la fonction UPnP. Choisissez simplement « Enable [Activer] » dans la partie « UPnP Enabling [Activation UPnP] » de la page « Utilities [Utilitaires] ». Cliquez sur « Apply Changes [Enregistrer les modifications] » pour enregistrer les modifications.

UPnP Enabling:

ADVANCED FEATURE! Allows you to turn the UPnP feature of the Router on or off. If you use applications that support UPnP, enabling UPnP will allow these applications to automatically configure the router. More Info

UPnP Enable / Disable >

Enable Disable

Apply Changes

Activation/Désactivation de la mise à jour automatique du micrologiciel

Cette innovation permet au routeur, grâce à une fonction intégrée, de vérifier automatiquement l'existence d'une nouvelle version du micrologiciel et de vous avertir lorsqu'elle est disponible. Lorsque vous vous connectez à l'interface évoluée du routeur, ce dernier effectue une vérification pour savoir s'il existe une nouvelle version du micrologiciel. Si tel est le cas, vous en êtes informé. Vous pouvez choisir de télécharger cette nouvelle version ou de l'ignorer. Le routeur est livré avec cette fonction désactivée. Pour la désactiver, sélectionnez « Disable [Désactiver] », puis cliquez sur « Apply Changes [Enregistrer les modifications] ».

Configuration de vos ordinateurs

Afin que votre ordinateur soit en mesure de communiquer avec votre routeur, vous devez vous assurer que les paramètres TCP/IP Ethernet soient à « Obtain an IP address automatically/Using DHCP [Obtenir une adresse IP automatiquement/ Utiliser serveur DHCP] ». C'est le paramètre par défaut de la plupart des ordinateurs domestiques.

Procédez comme suit pour configurer D'ABORD l'ordinateur connecté au modem ADSL. Vous pouvez également suivre les étapes suivantes pour ajouter des ordinateurs à votre routeur après que celui-ci soit configuré pour accéder à l'Internet.

Auto Update Firmware Enabling:

ADVANCED FEATURE! Allows you to automatically check the availability of firmware updates for your router. More Info

Auto Update Firmware
Enable / Disable >

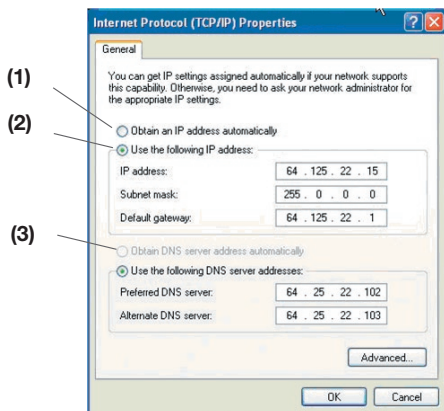
Enable Disable

Apply Changes

Configuration manuelle des adaptateurs réseau

Windows XP, 2000 ou NT

1. Cliquez sur « Démarrer », « Paramètres » puis « Panneau de Configuration ».
2. Cliquez deux fois sur l'icône « Network and dial-up connections [Connexions réseau et accès à distance] » (Windows 2000) ou sur l'icône « Network [Réseau] » (Windows XP).
3. Cliquez avec le bouton droit de la souris sur la connexion au réseau local associée à votre carte réseau, puis sélectionnez « Propriétés [Propriétés] » dans le menu déroulant.
4. Dans la fenêtre « Local Area Connection Properties [Propriétés de la connexion au réseau local] », sélectionnez « Internet Protocol (TCP/IP) [Protocole Internet (TCP/IP)] », puis cliquez sur le bouton « Propriétés [Propriétés] ». L'écran suivant apparaît :



5. Si l'option « Use the following IP address [Utiliser l'adresse IP suivante] » est sélectionnée, votre routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le routeur.

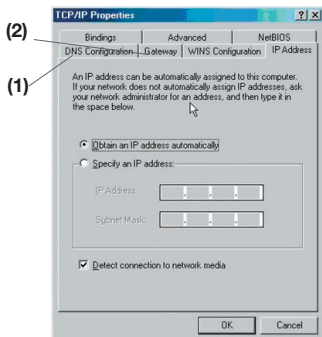
1
2
3
4
5
6 section
7
8
9
10
11

Configuration manuelle des adaptateurs réseau

- Si elles ne sont pas déjà sélectionnées, choisissez les options « Obtain an IP address automatically [Obtenir automatiquement une adresse IP] » (1) et « Obtain DNS server address automatically [Obtenir les adresses des serveurs DNS automatiquement] » (3). Cliquez sur « OK ». Votre(vos) adaptateur(s) réseau est(ont) maintenant configuré(s) de manière à fonctionner avec le routeur.

Windows 98 SE ou Me

- Cliquez avec le bouton droit de la souris sur « Network Neighborhood [Voisinage réseau] » et sélectionnez « Propriétés [Propriétés] » dans le menu déroulant.
- Sélectionnez « TCP/IP -> settings [TCP/IP -> paramètres] » pour la carte réseau installée. Vous verrez l'écran suivant.
- Si l'option « Specify an IP address [Spécifier une adresse IP] » est sélectionnée, votre routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le routeur.
- Écrivez l'adresse IP et le masque de sous-réseau de l'onglet « IP Address [Adresse IP] » (3).
- Cliquez sur l'onglet « Gateway [Passerelle] » (2). Notez l'adresse de la passerelle dans le tableau.
- Cliquez sur l'onglet « DNS Configuration [Configuration DNS] » (1). Inscrivez les adresses DNS dans le tableau.
- Si elle n'est pas déjà sélectionnée, choisissez l'option « Obtain IP address automatically [Obtenir automatiquement une adresse IP] » sur l'onglet des adresses IP. Cliquez sur « OK ». Redémarrez l'ordinateur. Lorsque l'ordinateur redémarre, votre(vos) adaptateur(s) réseau est(ont) maintenant configuré(s) de manière à fonctionner avec le routeur. Procédez comme suit pour configurer D'ABORD l'ordinateur connecté au modem câble ou ADSL. Vous pouvez aussi suivre les étapes suivantes pour ajouter des ordinateurs à votre routeur après que celui-ci est configuré pour accéder à l'Internet.

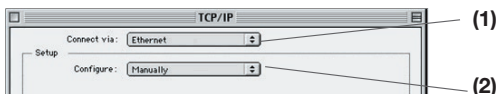


(3)

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

Mac OS jusqu'à 9.x

Afin que votre ordinateur puisse communiquer efficacement avec votre routeur, vous devrez modifier les paramètres TCP/IP de votre Mac à DHCP.



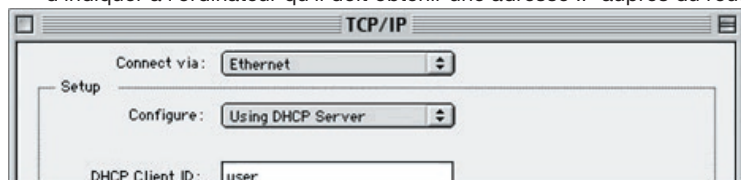
- Déroulez le menu Pomme. Sélectionnez « Control Panels [Tableaux de bord] », puis « TCP/IP ».
- Vous verrez le tableau de bord TCP/IP. Sélectionnez « Ethernet Built-In [Ethernet intégré] » ou « Ethernet » dans le menu déroulant « Connect via: [Connecter via :] » (1).

Configuration manuelle des adaptateurs réseau

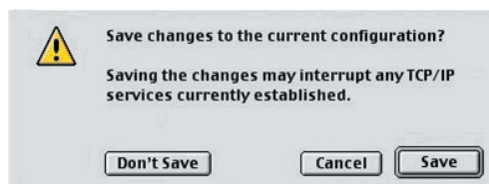
3. À côté de « Configure [Configurer] » (2), si l'option « Manually [Manuellement] » est sélectionnée, votre routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le routeur.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

4. Si cela n'est pas déjà fait, au niveau de « Configure [Configurer] », choisissez « Using DHCP Server [Utiliser le serveur DHCP] ». Ceci permet d'indiquer à l'ordinateur qu'il doit obtenir une adresse IP auprès du routeur.



5. Fermez la fenêtre. Si vous avez apporté des modifications, la fenêtre suivante apparaît. Cliquez sur « Save [Enregistrer] ».



Redémarrez l'ordinateur. Lorsque l'ordinateur redémarre, vos paramètres réseau sont maintenant configurés de manière à fonctionner avec le routeur.

Mac OS X

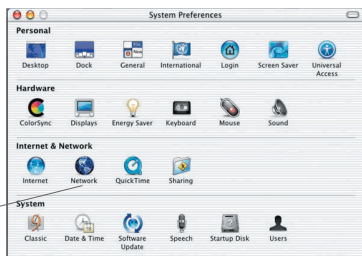
1. Cliquez sur l'icône « System Preferences [Préférences système] ».



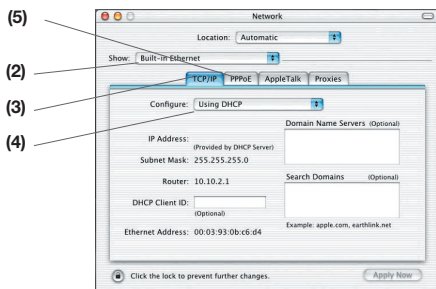
1
2
3
4
5
6 section
7
8
9
10
11

Configuration manuelle des adaptateurs réseau

2. Sélectionnez « Network [Réseau] » (1) à partir du menu « System Preferences [Préférences du système] ».
3. Sélectionnez « Built-in Ethernet [Ethernet intégré] » (2) à côté de « Show [Montrer] », dans le menu « Network [Réseau] ».



4. Sélectionnez l'onglet « TCP/IP » (3). À côté de « Configure [Configurer] » (4), vous devriez voir « Manually [Manuellement] » ou « Using DHCP [Utiliser DHCP] ». Si tel n'est pas le cas, vérifiez dans l'onglet « PPPoE » (5) que l'option « Connect using PPPoE [Se connecter via PPPoE] » n'est PAS sélectionnée. Si c'est le cas, vous devrez configurer votre routeur pour une connexion de type PPPoE, utilisant votre nom d'utilisateur et mot de passe.



5. Si l'option « Manually [Manuellement] » est sélectionnée, votre routeur devra être configuré pour un type de connexion IP fixe. Entrez l'information sur l'adresse dans le tableau ci-dessous. Vous devrez entrer ces informations dans le routeur.
6. Si cela n'est pas déjà fait, sélectionnez « Using DHCP [Via DHCP] » à côté de « Configure [Configurer] » (4), puis cliquez sur « Apply Now [Appliquer maintenant] ».

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

Votre(vos) adaptateur(s) réseau est(sont) maintenant configuré(s) de manière à fonctionner avec le routeur.

Paramètres de navigateur recommandés

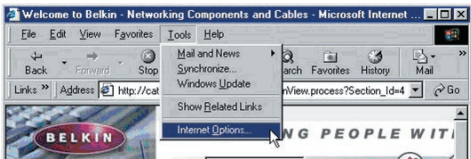
1
2
3
4
5
6
7
8
9
10
11

section

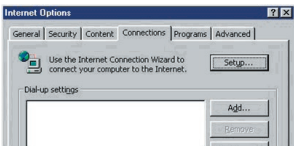
La plupart du temps, vous n'aurez pas besoin de modifier les paramètres de votre navigateur Web. Si vous éprouvez des difficultés à accéder à l'Internet ou à l'interface utilisateur basée sur navigateur Web, modifiez alors les paramètres de votre navigateur avec les paramètres recommandés dans cette section.

Internet Explorer 4.0 ou version ultérieure

1. Lancez votre navigateur Web. Dans le menu « Tools [Outils] », sélectionnez la commande « Internet Options [Options Internet] ».

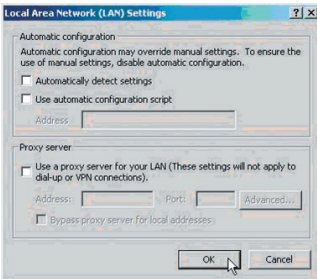


2. À l'écran « Internet Options [Options Internet] », trois choix sont possibles : « Never dial a connection [Ne jamais établir de connexion] », « Dial whenever a network connection is not present [Établir une connexion s'il n'existe pas de connexion réseau] » et « Always dial my default connection [Toujours établir la connexion par défaut] ». Si vous le pouvez, sélectionnez l'option « Never dial a connection [Ne jamais établir de connexion] ». Si vous ne pouvez pas, passez à l'étape suivante.



3. À l'écran « Internet Options [Options Internet] », cliquez sur « Connections [Connexions] », puis sélectionnez « LAN Settings... [Paramètres du réseau local] ».

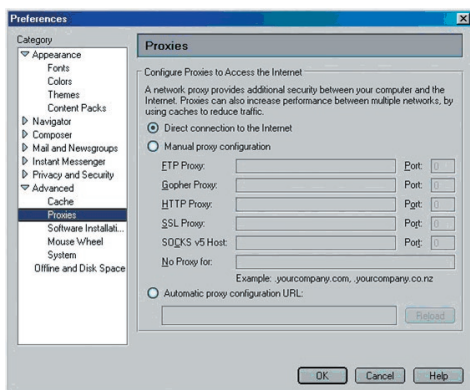
4. Assurez-vous qu'aucune de ces options n'est cochée : « Automatically detect settings [Détecter automatiquement les paramètres de connexion] »,



« Use automatic configuration script [Utiliser un script de configuration automatique] » et « Use a proxy server [Utiliser un serveur proxy] ». Cliquez sur « OK ». Ensuite, cliquez de nouveau sur « OK » à la page « Internet Options [Options Internet] ».

Netscape® Navigator® 4.0 ou version ultérieure

1. Lancez Netscape. Dans le menu « Edit [Edition] », cliquez sur « Preferences [Préférences] ».
2. Dans la fenêtre « Preferences [Préférences] », cliquez sur « Advanced [Avancé] », puis sélectionnez « Proxies [Serveurs proxy] ». Dans la fenêtre « Proxies [Serveurs proxy] », sélectionnez « Direct connection to the Internet [Connexion directe à Internet] ».



Dépannage

Problème :

Le voyant ADSL est éteint.

Solution :

1. Vérifiez la connexion entre le routeur et la ligne ADSL. Assurez-vous que le câble réseau provenant de la ligne ADSL est branché au port « ADSL » du routeur.
2. Assurez-vous que le courant arrive au routeur. Le voyant d'alimentation à l'avant du routeur doit être allumé.

Problème :

Le voyant Internet est éteint.

Solution :

1. Assurez-vous que le câble réseau provenant de la ligne ADSL est branché au port « ADSL » du routeur et que le voyant ADSL est allumé.
2. Assurez-vous que vous avez entré les paramètres de VPI/VCI, de nom d'utilisateur et de mot de passe fournis par votre FAI.

Problème :

Ma connexion est de type « Adresse IP fixe ». Je n'arrive pas à me connecter à Internet.

Solution :

Puisque vous utilisez une adresse IP fixe, votre FAI doit vous attribuer l'adresse IP, l'adresse de masque de sous-réseau ainsi que l'adresse de la passerelle. Au lieu d'utiliser l'Assistant, allez à « Connexion Type [Type de connexion] » et sélectionnez votre type de connexion. Cliquez « Next [Suivant] », sélectionnez « Static IP [IP fixe] », et entrez votre adresse IP, votre masque de sous-réseau et votre passerelle par défaut.

Problème :

J'ai oublié / j'ai perdu mon mot de passe.

Solution :

Appuyez sur le bouton de réinitialisation (à l'arrière du routeur) et maintenez-le enfoncé pendant 6 secondes afin de rétablir les paramètres par défaut du fabricant.

1

2

3

4

5

6

7

8

9

10

11

section

Problème :

Mon PC sans fil n'arrive pas à se connecter au routeur.

Solution :

1. Assurez-vous que le PC sans fil possède le même SSID que le routeur, et que les paramètres de sécurité (WPA et WEP) sont identiques sur chaque client et sur le routeur.
2. Assurez-vous que la distance entre le routeur et le PC sans fil n'est pas trop grande.

Problème :

Ma connexion au réseau sans fil est souvent interrompue.

Solution :

1. Déplacez votre PC sans fil plus près de votre routeur, afin d'obtenir un meilleur signal.
2. Il y a peut-être beaucoup d'interférences, causées peut-être par un four à micro-ondes ou un téléphone sans fil 2,4 GHz. Déplacez le routeur ou utilisez un canal différent.

Problème :

Je n'arrive pas à me connecter sans fil à Internet.

Solution :

Si vous n'arrivez pas à vous connecter à l'Internet à partir d'un ordinateur sans fil, veuillez vérifier les points suivants :

1. Observez les voyants sur votre routeur. Si vous utilisez un routeur Belkin, les voyants devraient être comme suit :
 - Le voyant d'alimentation doit être allumé.
 - Le voyant « Connected [Connecté] » doit être allumé et ne pas clignoter.
 - Le voyant WAN doit être allumé ou clignoter.
2. Lancez le logiciel de l'utilitaire sans fil en cliquant sur l'icône dans la barre de tâches, à l'angle inférieur droit de l'écran. Si vous utilisez une carte sans fil Belkin, l'icône de la barre de tâches devrait ressembler à celle-ci (elle peut être rouge ou verte) :
3. L'allure générale de la fenêtre qui s'ouvre dépend du modèle de la carte réseau que vous possédez. Toutefois, n'importe quel utilitaire doit posséder une liste de « Available Networks [Réseaux Disponibles] », soit les réseaux auxquels vous pouvez vous connecter.

Est-ce que le nom de votre réseau apparaît dans la liste des réseaux disponibles ?

Oui, le nom de mon réseau apparaît - allez à la section intitulée « Je ne peux me connecter sans fil à l'Internet mais mon réseau apparaît dans la liste ».

Non, le nom de mon réseau n'apparaît pas – allez à la section intitulée « Je ne peux me connecter sans fil à l'Internet et mon réseau n'apparaît pas dans la liste ».

Problème :

Je ne peux me connecter sans fil à l'Internet mais mon réseau apparaît dans la liste.

Solution :

Si le nom de réseau apparaît dans la liste des réseaux disponibles, veuillez suivre les étapes suivantes afin de vous connecter sans fil :

1. Cliquez sur le nom de réseau valide dans la liste des réseaux disponibles.

Si le réseau est sécurisé (chiffrement), vous devrez entrer la clé réseau. Pour plus d'informations sur la sécurité, rendez vous à la page intitulée « Configuration des paramètres de sécurité sans fil ».

2. Dans les secondes qui suivent, l'icône de la barre de tâches, à l'angle inférieur droit de l'écran, tournera au vert, indiquant une connexion au réseau.

Problème :

Je ne peux me connecter sans fil à l'Internet et mon réseau n'apparaît pas dans la liste.

Solution :

Si le nom de votre réseau n'apparaît pas dans la liste des réseaux disponibles dans l'utilitaire, veuillez vérifier les points suivants :

1. Déplacez l'ordinateur, autant que possible, afin qu'il soit situé de 1,5 à 3 mètres du routeur. Fermez l'utilitaire de réseau sans fil, et rouvrez-le. Si le nom de votre réseau sans fil apparaît maintenant dans la liste des réseaux disponibles, il se peut que votre problème soit dû à la portée ou à une interférence. Veuillez consulter l'Appendice B à propos des « Facteurs à considérer pour le choix de l'emplacement et l'installation ».

2. À l'aide d'un ordinateur connecté au routeur sans fil ou au point d'accès via un câble réseau (et non pas sans fil), assurez-vous que la « Broadcast SSID [Diffusion du SSID] » est activée. Ce paramètre se trouve à la page de configuration du Canal et SSID du manuel du routeur.

Si vous ne pouvez toujours pas accéder à l'Internet après avoir vérifié les points précédents, veuillez contacter l'assistance technique de Belkin.

Problème :

Mon réseau sans fil ne fonctionne pas toujours.

Le transfert de données est parfois très lent.

La force du signal est faible.

1

2

3

4

5

6

7

8

9

10

11

J'éprouve des difficultés à établir/maintenir une connexion de type VPN (Virtual Private Network).

Solution :

La technologie sans fil est basée sur des ondes radio. Ceci implique que les performances et le débit de transfert entre les appareils diminuent lorsque ceux-ci sont éloignés les uns des autres. D'autres facteurs peuvent engendrer une dégradation du signal : le métal en est généralement responsable. Des obstacles tels des murs et des appareils métalliques peuvent aussi affecter la qualité du signal. Ainsi, la portée à l'intérieur de vos appareils sans fil va de 30 à 60 mètres. Prenez note que la vitesse de connexion diminue également si vous vous éloignez du routeur sans fil ou du point d'accès.

Afin de déterminer si vos problèmes de connexion sans fil sont dus à la portée, déplacez temporairement votre ordinateur dans un rayon d'environ 1,5 à 3 mètres de votre routeur.

Modification du canal sans fil - Selon le trafic de données et les interférences au niveau local, passer à un autre canal peut améliorer la performance de votre réseau. Le canal par défaut de votre routeur est 11. Vous pouvez choisir à partir de plusieurs autres canaux, dépendamment de votre région. Consultez la page XX - « Modification du canal sans fil » pour de plus amples informations concernant le choix du canal.

Limiter le débit de données sans fil - Limiter le débit de données sans fil peut améliorer la portée sans fil maximale et la stabilité de la connexion. La plupart des cartes sans fil sont en mesure de limiter le débit de transmission. Pour modifier cette propriété, allez au « Panneau de Configuration » de Windows, ouvrez les « Connexions Réseau » et double-cliquez sur la connexion sans fil de votre carte sans fil. Dans la boîte de dialogue Propriétés, sélectionnez le bouton « Configure [Configurer] » à partir de l'onglet « Général ». (Les utilisateurs de Windows 98SE devront sélectionner la carte sans fil à partir de la liste, et cliquer ensuite sur Propriétés.) Choisissez ensuite l'onglet « Advanced [Avancé] » et sélectionnez la propriété « Rate [Débit] ». Les cartes clients sans fil sont habituellement configurées de façon à ajuster automatiquement le débit de transmission. Toutefois, ceci peut mener à des déconnexions périodiques lorsque le signal sans fil est trop faible. De façon générale, les débits de transmission plus lents sont plus stables. Faites des expériences avec différents débits de transmission jusqu'à ce que vous trouviez celui qui convient à votre environnement. Veuillez noter que chaque débit de transmission est acceptable pour naviguer sur Internet. Pour de plus amples informations, consultez le manuel de l'utilisateur de votre carte sans fil.

Problème :

Comment puis-je étendre la portée de mon réseau sans fil ?

Solution :

Belkin vous recommande l'utilisation d'un des produits suivants afin d'étendre la portée de votre réseau sans fil, chez vous ou au bureau :

- Point d'accès sans fil : Un point d'accès sans fil peut en effet doubler la portée de votre réseau sans fil. Un point d'accès se positionne généralement dans une zone non couverte par votre routeur sans fil et est relié au routeur grâce à un câble Ethernet.
- Pour les réseaux sans fil 802.11g (54g), Belkin vous offre un Amplificateur de signal/point d'accès sans fil qui peut se connecter sans fil à un Routeur Sans Fil 802.11g de Belkin, sans câble Ethernet.

Ces produits Belkin sont disponibles chez votre détaillant Belkin, ou directement de Belkin.

Pour obtenir de plus amples informations sur comment étendre la portée de votre réseau, visitez : www.belkin.com/networking et découvrez le produit suivant : Amplificateur de signal/Point d'accès sans fil (F5D7130)

Problème :

J'éprouve des difficultés dans la configuration du Wired Equivalent Privacy (WEP) sur mon routeur ou mon point d'accès Belkin.

Solution :

1. Connectez-vous à votre routeur ou votre point d'accès sans fil .
2. Ouvrez votre navigateur Web et entrez l'adresse IP du routeur ou du point d'accès sans fil. (L'adresse par défaut du routeur est 192.168.2.1 et celle du point d'accès est 192.168.2.254.) Appuyez sur le bouton « Login [Connexion] », situé au coin supérieur droit du clavier, pour vous connecter au routeur. Un message vous demande d'entrer votre mot de passe. Si vous n'avez pas encore créé un mot de passe personnalisé, laissez ce champ vide et cliquez sur « Submit [Envoyer] ».
3. Cliquez sur l'onglet « Wireless [Sans Fil] » à la gauche de votre écran. Cliquez sur l'onglet « Encryption [Chiffrement] » ou « Security [Sécurité] » pour accéder à la page des paramètres de sécurité.
4. Sélectionnez « WEP 128 bits » dans le menu déroulant.
5. Après avoir sélectionné le mode de chiffrement WEP, vous pouvez entrer votre clé hexadécimale WEP manuellement ou vous pouvez entrer une expression mot de passe dans le champ « Passphrase [Expression mot de passe] » et cliquer sur « Generate [Générer] » pour créer la clé WEP à partir de l'expression mot de passe. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être

configurés avec ces paramètres. Une clé hexadécimale est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP 128 bits, vous devez entrer 26 clés hexadécimales.

Par exemple :

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = clé 128 bits

6. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Le chiffrement de votre routeur sans fil est maintenant configuré. Chaque ordinateur de votre réseau sans fil devra maintenant être configuré avec les mêmes paramètres de sécurité.

AVERTISSEMENT : Si vous configurez le routeur sans fil ou le point d'accès à partir d'un ordinateur doté d'un client sans fil, vous devez vous assurer que la sécurité est ACTIVÉE pour ce client sans fil. Sinon, vous perdez votre connexion sans fil.

Remarque aux utilisateurs de Mac : Les produits AirPort d'Apple ne prennent en charge que le chiffrement sur 64 bits. Les produits Apple AirPort 2 prennent en charge le chiffrement sur 64 bits ou 128 bits. Veuillez vérifier la version de votre produit Apple AirPort. Si vous ne parvenez pas à configurer le réseau avec le chiffrement sur 128 bits, essayez sur 64 bits.

Problème :

J'éprouve des difficultés dans la configuration du Wired Equivalent Privacy (WEP) sur ma carte réseau.

Solution :

Votre carte réseau doit utiliser la même clé que votre routeur ou point d'accès sans fil. Par exemple, si votre routeur sans fil ou point d'accès utilise la clé 0011 2233445566778899AABBCC, votre carte réseau doit être paramétrée de façon à utiliser cette même clé.

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ».
2. Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
3. Ensuite, l'utilitaire LAN Sans Fil de Belkin apparaît. Cet Utilitaire vous permet d'accéder à toutes les fonctions avancées de votre carte réseau sans fil Belkin.
4. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Properties [Propriétés] ».
5. Sous « Data Encryption [Chiffrement de données] », sélectionnez « WEP ».
6. Assurez-vous que la case « The key is provided for me automatically [J'obtiens une clé automatiquement] » n'est pas cochée. Si vous utilisez cet ordinateur

pour vous connecter à un réseau d'entreprise, prenez conseil auprès de votre administrateur réseau afin de savoir si cette case doit être cochée.

7. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

Important : Une clé WEP est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WEP sur 128 bits, vous devez entrer 26 clés hexadécimales. Cette clé réseau doit être identique à la clé que vous avez assignée à votre routeur ou point d'accès sans fil.

Par exemple : C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = clé 128 bits

8. Cliquez sur « OK » et sur « Apply Changes [Enregistrer les Modifications] »

pour enregistrer les paramètres.

Si vous utilisez une carte réseau sans fil AUTRE qu'une carte Belkin, consultez le manuel de l'utilisateur de votre carte sans fil.

Problème :

Est-ce que les produits Belkin prennent en charge le WPA ?

Solution :

Remarque : Pour utiliser la sécurité par WPA, votre client doit être mis à jour avec les logiciels et les pilotes qui le prennent en charge. Au moment de mettre ce manuel sous presse, une rustine de sécurité est disponible pour téléchargement gratuit, auprès de Microsoft. Ce patch ne fonctionne qu'avec Windows XP.

Vous pouvez télécharger la rustine ici :

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

Vous devrez en outre télécharger le plus récent pilote pour votre Carte sans fil 802.11g pour ordinateur de bureau ou portable de Belkin, que vous trouverez sur le site de l'assistance technique de Belkin. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment. La rustine de Microsoft ne prend en charge que les dispositifs avec pilotes compatibles WPA, tels que les produits 802.11g de Belkin.

Téléchargez le pilote le plus réseau à <http://www.belkin.com/uk/support/tech/index.asp>

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur mon routeur ou mon point d'accès sans fil Belkin, pour mon réseau domestique.

1

2

3

4

5

6

7

8

9

10

11

Solution :

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA-PSK (no server) [sans serveur] ».
2. À « Encryption Technique [Technique de chiffrement] », choisissez « TKIP » ou « AES ». Ce paramètre devra être identique à celui des clients que vous configurerez.
3. Entrez votre clé pré-partagée. Elle peut être composée de 8 à 63 caractères (lettres, chiffres, symboles ou espaces). Cette clé doit être utilisée pour tous les clients branchés au réseau. Par exemple, votre clé pré-partagée peut ressembler à : « Clé réseau de la famille Dupont ».
4. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur mon routeur ou mon point d'accès sans fil Belkin, pour mon réseau d'entreprise.

Solution :

Si votre réseau utilise un serveur Radius pour distribuer les clés aux clients, veuillez utiliser ce paramètre. Ce système se retrouve surtout en entreprise.

1. À partir du menu déroulant « Security Mode [Mode de Sécurité] », sélectionnez « WPA (with server) [avec serveur] ».
2. À « Encryption Technique [Technique de chiffrement] », choisissez « TKIP » ou « AES ». Ce paramètre devra être identique à celui des clients que vous configurerez.
3. Entrez l'adresse IP de votre serveur Radius dans le champ « Radius server [Serveur Radius] ».
4. Entrez la clé Radius dans le champ « Clé Radius ».
5. Entrez l'intervalle de clé. L'intervalle de clé correspond au nombre de fois où les clés sont distribuées (en paquets).
6. Cliquez sur « Apply Changes [Enregistrer les modifications] » pour terminer. Tous les clients doivent maintenant être configurés avec ces paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur ma Carte Sans Fil Belkin, pour mon réseau domestique.

Solution :

Les clients doivent utiliser la même clé que le routeur ou le point d'accès sans fil. Par exemple, si le routeur ou le point d'accès sans fil est configuré avec la clé

« Clé réseau de la famille Dupont », tous les clients doivent utiliser cette même clé.

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ».
2. Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
3. Ensuite, l'utilitaire LAN Sans Fil de Belkin apparaît. Cet Utilitaire vous permet d'accéder à toutes les fonctions avancées de votre carte réseau sans fil Belkin.
4. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Properties [Propriétés] ».
5. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA-PSK (No server) [WPA-PSK (Sans serveur)] ».
6. Entrez votre clé WPA dans la boîte « Network Key [Clé Réseau] ».

Important : Une clé WPA-PSK est une combinaison de chiffres et de lettres, compris entre A et F et entre 0 et 9. Pour le WPA-PSK, vous devez entrer de 8 à 63 caractères. Cette clé réseau doit être identique à la clé que vous avez assignée à votre routeur ou point d'accès sans fil.

7. Cliquez sur « OK » et sur « Apply [Enregistrer] » pour enregistrer les paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur ma Carte Sans Fil Belkin, pour mon réseau d'entreprise.

Solution :

1. Cliquez deux fois sur cette icône pour afficher l'écran « Wireless Network [Réseau Sans Fil] ».
2. Le bouton « Advanced [Avancé] » vous permet d'afficher et de configuration un plus grand nombre d'options de la carte.
3. Ensuite, l'utilitaire LAN Sans Fil de Belkin apparaît. Cet Utilitaire vous permet d'accéder à toutes les fonctions avancées de votre carte réseau sans fil Belkin.
4. Sous l'onglet « Wireless Network Properties [Propriétés Réseau sans fil] », sélectionnez un réseau dans la liste « Available networks [Réseaux disponibles] », puis cliquez sur « Properties [Propriétés] ».
5. Sous « Network Authentication [Authentification Réseau] », choisissez « WPA ».
6. Sous l'onglet « Authentication [Authentification] », choisissez les paramètres spécifiés par l'administrateur de votre réseau.
7. Cliquez sur « OK » et sur « Apply [Enregistrer] » pour enregistrer les paramètres.

Problème :

J'éprouve des difficultés dans la configuration du Wi-Fi Protected Access (WPA) sur ma Carte Sans Fil AUTRE que Belkin, pour mon réseau domestique.

Solution :

Pour les Cartes réseau sans fil pour ordinateurs de bureau ou portables autres que Belkin et qui ne prenant pas en charge le WPA, une rustine de Microsoft, nommée « Windows XP Support Patch for Wireless Protected Access » est disponible pour téléchargement gratuit. Téléchargez la rustine de Microsoft en cherchant la base de connaissances avec « Windows XP WPA ».

Remarque : Cette rustine ne fonctionne qu'avec Windows XP. Les autres systèmes d'exploitation ne sont pas pris en charge pour le moment. Vous devez en outre vous assurer que le fabricant de votre carte sans fil prend en charge le WPA et que vous avez téléchargé et installé le pilote le plus récent, que vous trouverez sur leur site web.

Systèmes d'exploitation pris en charge :

- Windows XP Professionnel
- Windows XP Édition Familiale

Pour activer le WPA-PSK (sans serveur)

1. Sous Windows XP, cliquez Démarrer > Panneau de Configuration > Connexions Réseaux et Internet .
2. En cliquant avec le bouton droit de votre souris sur « Wireless Networks [Réseaux Sans Fil] », vous verrez une fenêtre s'afficher comme suit : Assurez-vous que la case « Utiliser Windows pour configurer mes paramètres réseau sans fil » est cochée.
3. Sous l'onglet « Wireless Networks [Réseaux Sans Fil] », cliquez sur le bouton « Configurer [Configurer] ».
4. Pour l'utilisateur de réseau domestique ou de petite entreprise, sélectionnez « WPA-PSK » sous « Network Administration [Administration Réseau] ».

Remarque : Sélectionnez le WPA si vous utilisez cet ordinateur pour vous brancher à un réseau d'entreprise, qui à son tour prend en charge un serveur d'authentification tel que le serveur RADIUS. Renseignez-vous auprès de l'administrateur de votre réseau pour de plus amples informations.

5. Sélectionnez « TKIP » sous « Data Encryption [Chiffrement de données] ». Ce paramètre devra être identique à ce lui que vous configurerez sur le routeur ou le point d'accès sans fil.
6. Entrez votre clé WEP dans la boîte « Network Key [Clé Réseau] ».

Important : Entrez votre PSK. Elle peut être composée de 8 à 63 caractères (lettres, chiffres ou symboles). Cette clé doit être utilisée pour tous les clients branchés au réseau.

7. Cliquez « OK » pour enregistrer les paramètres.

Quelle est la différence entre 802.11b, 802.11g, 802.11a et Pre-N ?

À l'heure actuelle, il existe quatre normes de réseaux sans fil qui transmettent des données à des débits maximaux différents. Chaque norme est basée sur le radical 802.11(x), utilisé par la IEEE, l'organisme responsable de la certification des normes réseaux. La norme réseau la plus courante, le 802.11b, transmet les données à 11 Mbps. Les normes 802.11a et 802.11g transmettent à 54 Mbps. Le Pre-N, quand à lui, transmet à 108 Mbps. Le Pre-N, précurseur de la norme 802.11n qui sera lancée prochainement, promet un débit supérieur au 802.11g et une couverture deux fois plus étendue. Consultez le tableau suivant pour de plus amples informations.

Tableau comparatif des réseaux sans fil

Technologie sans fil	G (802.11g)	G+ MIMO (802.11g avec MIMO MRC)	N MIMO (projet 802.11n avec MIMO)	N1 MIMO (projet 802.11n avec MIMO)
Débit de données*	Jusqu'à 54 Mbps*	Jusqu'à 54 Mbps*	Jusqu'à 300 Mbps*	Jusqu'à 300 Mbps*
Fréquence	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz	Les appareils domestiques courants tels que téléphones sans fil et fours à micro-ondes peuvent interférer avec la bande sans autorisation 2,4 GHz
Compatibilité	Compatible avec le 802.11b/g	Compatible avec le 802.11b/g	Compatible avec le projet 802.11n** et le 802.11b/g	Compatible avec le projet 802.11n** et le 802.11b/g
Couverture*	Jusqu'à 120 mètres*	Jusqu'à 305 mètres*	Jusqu'à 365 mètres*	Jusqu'à 425 mètres*
Avantage	Populaire : grande popularité pour le partage d'une connexion Internet	Meilleure couverture avec débit plus stable	Meilleure couverture et débit plus rapide	Technologie de pointe : le meilleur débit et la meilleure couverture

*La portée et le débit de la connexion dépendent de l'environnement de votre réseau.

**Ce routeur est compatible avec les produits basés sur la même version des spécifications du projet 802.11n. Une mise à jour logicielle peut être nécessaire pour de meilleurs résultats.

Informations à propos de l'assistance technique

Assistance technique gratuite* *Hors coût de communication

nationale

www.belkin.com

Vous trouverez des informations techniques sur le site www.belkin.fr dans la zone d'assistance technique. Pour contacter le service d'assistance technique par téléphone, veuillez composer le numéro correspondant dans la liste ci-dessous*.

PAYS	NUMÉRO	ADRESSE INTERNET
AUTRICHE	0820 200766	www.belkin.com/uk/networking/
BELGIQUE	07 07 00 073	www.belkin.com/nl/networking/
RÉPUBLIQUE TCHÈQUE	239 000 406	www.belkin.com/uk/networking/
DANEMARK	701 22 403	www.belkin.com/uk/networking/
FINLANDE	097 25 19 123	www.belkin.com/uk/networking/
FRANCE	08 - 25 54 00 26	www.belkin.com/fr/networking/
ALLEMAGNE	0180 - 500 57 09	www.belkin.com/de/networking/
GRÈCE	00800 - 44 14 23 90	www.belkin.com/uk/networking/
HONGRIE	06 - 17 77 49 06	www.belkin.com/uk/networking/
ISLANDE	800 8534	www.belkin.com/uk/networking/
IRLANDE	0818 55 50 06	www.belkin.com/uk/networking/
ITALIE	02 - 69 43 02 51	www.belkin.com/it/support/tech/issues_more.asp
LUXEMBOURG	34 20 80 85 60	www.belkin.com/uk/networking/
PAYS-BAS	0900 - 040 07 90 0,10 € par minute	www.belkin.com/nl/networking/
NORVÈGE	81 50 0287	www.belkin.com/uk/networking/
POLOGNE	00800 - 441 17 37	www.belkin.com/uk/networking/
PORTUGAL	707 200 676	www.belkin.com/uk/networking/
RUSSIE	495 580 9541	www.belkin.com/networking/
AFRIQUE DU SUD	0800 - 99 15 21	www.belkin.com/uk/networking/
ESPAGNE	902 - 02 43 66	www.belkin.com/es/support/tech/networkingsupport.asp
SUÈDE	07 - 71 40 04 53	www.belkin.com/se/support/tech/networkingsupport.asp
SUISSE	08 - 48 00 02 19	www.belkin.com/uk/networking/
ROYAUME-UNI	0845 - 607 77 87	www.belkin.com/uk/networking/
AUTRES PAYS	+44 - 1933 35 20 00	

Appendice A : Glossaire

Adresse IP

L' « Adresse IP » représente l'Adresse IP interne du routeur. Pour accéder à l'interface de configuration avancée, entrez cette adresse IP dans la barre d'adresse de votre navigateur. Cette adresse peut être modifiée au besoin. Pour modifier l'adresse IP, entrez la nouvelle adresse IP et cliquez sur « Apply Changes [Enregistrer les Modifications] ». L'adresse IP choisie doit être une adresse IP non-acheminable. Exemples d'adresses IP non-acheminables :

192.168.x.x (où x est un nombre compris entre 0 et 255)

10.x.x.x (où x est un nombre compris entre 0 et 255)

Masque de sous-réseau

Certains réseaux sont beaucoup trop élargis pour permettre à tout le trafic de submerger toutes ses parties. Ces réseaux doivent être divisés en sections plus restreintes et facilement administrables : les sous-réseaux. Le masque de sous-réseau consiste en l'adresse du réseau, en plus de l'information réservée à l'identification du sous-réseau.

DNS

DNS est l'acronyme de Domain Name Server, qui se traduit par Serveur de noms de domaine. Un Serveur de Noms de Domaine est un serveur que l'on retrouve sur l'Internet et qui traduit les URL (Universal Resource Links), telles que www.belkin.com, en adresses IP. Cette information n'est pas requise de la plupart des FAI lors de la configuration du routeur. Si vous êtes utiliser une connexion de type IP statique, vous pouvez avoir besoin de saisir une adresse DNS spécifique ainsi qu'une adresse DNS secondaire pour que votre connexion puisse fonctionner correctement. Si vous utilisez une connexion de type Dynamique ou PPPoE, il est fort probable que vous n'ayez pas à entrer une adresse de DNS.

PPPoE

La plupart des fournisseurs de services ADSL utilisent la connexion de type PPPoE. Si vous utilisez un modem ADSL pour vous brancher à Internet, votre FAI utilise probablement le protocole PPPoE pour vous relier au service.

Vous possédez une connexion PPPoE si :

1. Votre FAI vous a attribué un nom d'utilisateur et un mot de passe, qui sont requis pour vous brancher à Internet.
2. Votre FAI vous a fourni des logiciels tels que WinPOET et Enternet300, et vous utilisez ceux-ci pour vous brancher à Internet,
3. Vous devez double-cliquer une icône sur votre bureau, autre que celle de votre navigateur, pour vous brancher à Internet.

Pour configurer le routeur selon le protocole PPPoE, entrez votre nom d'utilisateur et votre mot de passe dans les champs prévus. Après avoir entré les informations, cliquez sur « Apply Changes [Enregistrer les Modifications] ».

L'indicateur d'état de l'Internet affichera « Connexion OK » si votre routeur est configuré de façon appropriée.

1

2

3

4

5

6

7

8

9

10

11

section

PPPoA

Entrez les informations relative au PPPoA dans les champs prévus, et cliquez sur « Next [Suivant] ». Cliquez sur « Apply [Appliquer] » pour que les paramètres soient pris en compte.

1. Nom d'utilisateur – Entrez le nom d'utilisateur. (Attribuée par votre FAI.)
2. Mot de passe – Entrez votre mot de passe. (Attribuée par votre FAI.)
3. Entrez à nouveau le mot de passe – Confirmez le mot de passe. (Attribuée par votre FAI.)
- 4 VPI/VCI - Entrez ici vos paramètres de d'identificateur de trajet virtuel (VPI) et d'identificateur de voie virtuelle (VCI). (Attribuée par votre FAI.)

Déconnecter après X...

Cette fonction permet de déconnecter automatiquement le routeur de votre FAI, lorsque celui-ci est inactif pour une période de temps déterminée. Par exemple, si vous cochez cette option et que vous mettez « 5 » dans le champ des minutes, le routeur se déconnectera de l'Internet après 5 minutes d'inactivité Internet.

Cette option devrait être utilisée si votre FAI vous facture à la minute.

Canal et SSID

Pour modifier le canal d'opération du routeur, sélectionnez le canal désiré à partir de la liste déroulante et sélectionnez votre canal. Ensuite, cliquez sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres. Vous pouvez aussi modifier le SSID. Le SSID est l'équivalent du nom du réseau sans fil. Vous pouvez donner n'importe quel nom au SSID. S'il y a d'autres réseaux sans fil dans votre environnement immédiat, vous devriez donner un nom unique au vôtre. Pour modifier le SSID, cliquez sur la boîte SSID , et entrez le nouveau nom. Cliquez sur « Apply Changes [Enregistrer les Modifications] » pour qu'elles soient prises en compte.

Diffusion de l'ESSID

Plusieurs adaptateurs réseau sans fil disponibles sur le marché à l'heure actuelle comprennent une fonction appelée ' analyse du site '. Cette fonction permet de balayer l'air ambiant à la recherche de n'importe quel réseau disponible, et permet à chaque ordinateur de sélectionner automatiquement un réseau parmi ceux-ci. C'est possible lorsque le SSID de l'ordinateur est paramétré avec « TOUS ». Votre routeur Belkin permet le blocage de cette recherche de réseaux. Si vous désactivez la fonction « ESSID Broadcast [Diffusion d'ESSID] », le seul moyen dont dispose votre ordinateur pour se brancher au réseau est de paramétrer le SSID de celui-ci en lui donnant le nom spécifique du réseau (par exemple WLAN). Assurez-vous de connaître le SSID (nom du réseau) avant d'activer cette fonction. Il est possible de rendre presque invisible votre réseau sans fil. En désactivant la diffusion du SSID, votre réseau n'apparaîtra pas lors de l'analyse du site. Il va de soi que désactiver la fonction de diffusion du SSID augmente le niveau de sécurité.

Chiffrement

Le chiffrement contribue à préserver la sécurité de votre réseau. Pour protéger vos données, le routeur utilise le Wired Equivalent Privacy (WEP). Votre routeur présente deux niveaux de chiffrement : 64 bits et 128 bits. Le chiffrement fonctionne avec un système de clés. La clé de l'ordinateur doit correspondre à la clé du routeur. On peut créer une clé de deux façons.

La façon la plus simple consiste à laisser le logiciel du routeur convertir en clé une expression mot de passe que vous avez entrée. Une méthode plus avancée consiste à entrer la clé manuellement.

Passerelles d'applications

Les Passerelles d'Applications vous permettent d'ouvrir des ports spécifiques pour permettre à certaines applications de fonctionner adéquatement avec la fonction de Traduction d'Adresse Réseau (NAT) du routeur. Vous pouvez choisir vos applications à partir d'une liste d'applications courantes. Veuillez sélectionner une application courante à partir de la liste déroulante. Vos sélections seront programmées dans le routeur. Sélectionnez la ligne dont vous désirez copier les paramètres à partir de la liste déroulante, sélectionnez la ligne vers laquelle vous voulez les copier, et cliquez ensuite sur « Copier vers ». Les paramètres seront transférés vers la ligne spécifiée. Cliquez sur « Apply Changes [Enregistrer les Modifications] » pour sauvegarder les paramètres de cette application. Si vous ne trouvez pas votre application, vous devez contacter le fabricant de l'application afin de déterminer les ports qui doivent être configurés. Vous pouvez entrer ces informations manuellement dans les paramètres de votre routeur.

Serveurs Virtuels

Cette fonction vous permet d'acheminer, via le routeur et vers votre réseau interne, les appels externes (Internet) de services tels qu'un serveur web (port 80), un serveur FTP (port 21) ou d'autres applications. Parce que vos ordinateurs internes sont protégés par le pare-feu, les machines provenant de l'Internet ne peuvent accéder à ceux-ci puisqu'ils sont invisibles. Si vous devez configurer la fonction de Serveur Virtuel pour une application particulière, vous devez contacter le fabricant de votre application et déterminer quels paramètres de ports sont nécessaires.

Pour entrer les paramètres manuellement, entrez l'adresse IP dans l'espace prévu pour la machine (serveur) interne, les ports public et LAN requis pour la passerelle. Sélectionnez ensuite « Enable [Activer] » et cliquez sur « Set [Établir] ». Vous pouvez seulement faire passer un seul port par adresse IP interne. L'ouverture des ports de votre pare-feu peut compromettre la sécurité de votre réseau. Vous pouvez facilement activer ou désactiver cette fonction. Il est recommandé de désactiver cette fonction lorsque vous n'utilisez pas une application spécifique.

Filtres d'IP des clients

Le routeur peut être configuré de sorte à limiter l'accès de certains ordinateurs à Internet, au courrier électronique et autres fonctions réseaux, à des jours et des heures donnés. La restriction peut s'appliquer à un ordinateur unique, un groupe d'ordinateurs ou de multiples ordinateurs.

Blocage d'URL

Pour configurer la fonction de Blocage d'URL, spécifiez les sites web (www.onsite.com) et/ou les mots-clés que vous désirez voir filtrés sur votre réseau. Cliquez sur « Apply Changes [Enregistrer les Modifications] » pour que celles-ci soient prises en compte. Pour terminer cette configuration, vous devez créer ou modifier une règle

1

2

3

4

5

6

7

8

9

10

11

d'accès à la section Filtres d'IP des clients . Pour modifier une règle existante, cliquez sur l'option Modifier située à côté de la règle à modifier. Pour créer une nouvelle règle, cliquez sur l'option « Ajouter un PC ». À partir de la section « Contrôle d'Accès > Ajouter un PC », cochez l'option « WWW avec Blocage d'URL » dans le tableau de « Service de PC client », pour filtrer les sites web et les mots-clé spécifiés.

Règle d'horaire

Pour configurer la Règle d'horaire, spécifiez le Nom, le Commentaire, l'Heure du début et l'Heure de fin que vous désirez filtrer sur votre réseau. Cette page définit les noms des règles de l'horaire et active l'horaire en question, pour utilisation sur la page de « Contrôle d'Accès ».

Filtrage des adresses MAC

Le filtrage d'adresses MAC est une fonction de sécurité puissante qui vous permet de spécifier les ordinateurs autorisés à se connecter au réseau. Tout ordinateur non spécifié dans les paramètres du filtre et qui tente d'accéder au réseau se verra refuser l'accès. Lorsque vous activez cette fonction, vous devez entrer l'adresse MAC de chaque client de votre réseau, pour permettre à chacun d'accéder au réseau, ou copier l'adresse MAC en sélectionnant le nom de l'ordinateur à partir de la Liste de clients DHCP . Si vous souhaitez activer cette fonction, sélectionnez l'option Activer . Ensuite, cliquez sur « Apply Changes [Enregistrer les Modifications] » pour enregistrer les paramètres.

Zone DMZ

Si un de vos PC clients ne peut exécuter une application Internet convenablement parce qu'il se trouve derrière un pare-feu, vous pouvez modifier les restrictions en permettant l'accès à internet bidirectionnel. Cette opération peut s'avérer nécessaire si la traduction d'adresse réseau (NAT) empêche le bon fonctionnement d'applications telles que les jeux ou les vidéoconférences. Servez-vous de cette fonction au besoin. L'ordinateur placé dans la zone DMZ ne sera pas protégé contre les attaques provenant de hackers. Pour placer un ordinateur dans la zone DMZ, entrez les derniers chiffres de son adresse IP de réseau local dans le champ de saisie d'IP Statique, et cliquez sur « Apply Changes [Enregistrer les Modifications] » pour que celles-ci soient prises en compte.

Si vous n'avez qu'une adresse IP publique (WAN), vous pouvez laisser l'IP publique à « 0.0.0.0 ». Si vous utilisez plusieurs adresses IP (WAN) publiques, il est possible de sélectionner vers quelle adresse IP (WAN) publique l'hôte DMZ sera dirigé. Entrez l'adresse IP (WAN) publique vers laquelle vous désirez diriger l'hôte DMZ, entrez les deux derniers chiffres de l'adresse IP de l'ordinateur hôte de la zone DMZ, choisissez Activer et cliquez sur « Apply Changes [Enregistrer les Modifications] ».

Mot de passe Administrateur

Le routeur est livré SANS mot de passe défini. Si par souci de sécurité vous désirez ajouter un mot de passe, vous pouvez le configurer à partir de l'interface basée sur navigateur Web de votre routeur. Conservez votre mot de passe dans un endroit sûr, puisque vous aurez

besoin de ce mot de passe lorsque vous voudrez vous connecter au routeur par la suite. Il est **FORTEMENT RECOMMANDÉ** d'ajouter un mot de passe si vous prévoyez utiliser la fonction de gestion à distance du routeur. L'option de temporisation de la connexion vous permet de déterminer une plage horaire pendant laquelle vous pouvez être connecté à l'interface de configuration avancée du routeur. La temporisation débute lorsqu'il n'y a plus d'activité. Par exemple, vous avez apporté des modifications au niveau de l'interface de configuration évoluée, puis vous avez quitté l'ordinateur sans cliquer sur « Logout [Déconnexion] ».

En prenant pour exemple un temporisateur paramétré à 10 minutes, votre connexion prendra fin 10 minutes après votre départ. Vous devrez donc vous connecter à nouveau au routeur pour apporter d'autres modifications. L'option de temporisation de la connexion sert à des fins de sécurité, et le paramètre par défaut est 10 minutes. À titre de remarque, un seul ordinateur à la fois peut être connecté à l'interface de configuration avancée du routeur.

Définition d'un fuseau horaire

Le routeur harmonise le temps en se connectant à un serveur SNTP (Simple Network Time Protocol). Ceci permet au routeur de synchroniser l'horloge du système avec l'internet planétaire. L'horloge ainsi synchronisée est utilisée par le routeur pour garder un journal de connexions et pour contrôler le filtrage des clients. Sélectionnez le fuseau horaire du pays dans lequel vous résidez. Si vous résidez dans une région qui applique l'horaire d'été, cochez la case près de l'option « Enable Daylight Saving [Appliquer les horaires d'été] ». L'horloge du système peut ne pas être mise à jour immédiatement. Laissez au minimum 15 minutes au routeur pour contacter les serveurs horaires sur Internet et obtenir une réponse. Vous ne pouvez pas modifier l'horloge vous-même.

Gestion à distance

Avant d'activer cette fonction, **ASSUREZ-VOUS D'AVOIR AJOUTÉ UN MOT DE PASSE ADMINISTRATEUR**. La gestion à distance vous permet d'apporter des changements aux paramètres de votre routeur, où que vous soyez grâce à l'Internet.

UPnP

L'UPnP (Universal Plug-and-Play) est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux, et d'autres applications compatibles avec l'UPnP. Certaines applications nécessitent que le pare-feu du routeur soit configuré selon certains paramètres pour fonctionner adéquatement. Pour ce faire, vous devez habituellement ouvrir des ports TCP et UDP, et parfois même configurer des ports de déclenchement. Une application qui est compatible avec l'UPnP possède la capacité de communiquer avec le routeur, lui indiquant la façon dont le pare-feu doit être configuré. Le routeur est livré avec la fonction UPnP désactivée. Si vous utilisez une application qui est compatible avec l'UPnP, et si vous désirez bénéficier des avantages de l'UPnP, vous pouvez activer la fonction UPnP. Choisissez simplement « Enable [Activer] » dans la partie « UPnP Enabling [Activation UPnP] » de la page « Utilities [Utilitaires] ». Cliquez sur « Apply Changes [Enregistrer les modifications] » pour enregistrer les modifications.

Appendice B : Facteurs à considérer pour l'installation et la mise en route

Remarque : Alors que certains des objets énumérés ci-dessous peuvent affecter la performance de votre réseau, ils n'empêcheront pas son fonctionnement. Si vous croyez que votre réseau sans fil ne fonctionne pas à pleine capacité, ces solutions peuvent vous aider.

1. Choix de l'emplacement de votre routeur ou votre point d'accès sans fil

Placez votre routeur réseau sans fil (ou point d'accès), le centre nerveux de votre réseau sans fil, aussi près que possible du centre de la zone de couverture désirée. Afin d'assurer une zone de couverture optimale pour vos « clients réseau » (soit les ordinateurs dotés d'une carte réseau pour ordinateur de bureau ou portable ou d'un adaptateur USB de Belkin) :

- Assurez-vous que les antennes de votre routeur ou de votre point d'accès sont parallèles et disposées à la verticale (en pointant vers le plafond). Si votre routeur (ou votre point d'accès) est posé à la verticale, essayez autant que possible de disposer les antennes de façon à ce qu'elles pointent vers le haut.
- Dans des habitations à plusieurs étages, placez le routeur (ou le point d'accès) à l'étage le plus central de votre domicile. Ceci peut signifier que devrez placer le routeur sans fil (ou le point d'accès) à un étage supérieur
- Évitez de placer le routeur (ou le point d'accès) près d'un téléphone sans fil 2.4 GHz.

2. Éviter les obstacles et les interférences

Évitez de placer le routeur ou le point d'accès près d'un appareil émettant des ondes radio, comme un four à micro-ondes. Exemples d'objets denses pouvant empêcher la communication sans fil :

- Réfrigérateurs
- Lave-linge et/ou sèche-linge
- Étagère en métal
- Grands aquariums
- Fenêtres teintées (contre les UV) à base de métal

Si le signal de votre réseau semble plus faible à certains endroits, assurez-vous qu'aucun de ces objets ne peut faire obstruction à celui-ci (entre vos ordinateurs et votre routeur ou votre point d'accès.)

3. Téléphones sans fil

Si les performances de votre réseau sans fil sont toujours affectées malgré les solutions mentionnées ci-dessus et si vous possédez un téléphone sans fil :

- Éloignez votre téléphone de votre routeur ou votre point d'accès sans fil ainsi que de vos ordinateurs sans fil.
- Débranchez et retirez la batterie de tout téléphone sans fil fonctionnant sur la bande de 2.4 GHz. (Consultez la documentation accompagnant votre téléphone à cet effet.) Si ces gestes semblent résoudre le problème, c'est que votre téléphone interfère avec les signaux du réseau sans fil.
- Si votre téléphone prend en charge la sélection du canal, modifiez le canal de votre téléphone en choisissant autant que possible le canal le plus éloigné du

Appendice B : Facteurs à considérer pour l'installation et la mise en route

canal de votre réseau sans fil. Par exemple, choisissez le canal 1 pour votre téléphone et modifiez le canal de votre routeur ou de votre point d'accès en choisissant le canal 11. Consultez la documentation accompagnant votre téléphone pour de plus amples informations.

- Si nécessaire, vous pouvez également faire l'acquisition d'un téléphone sans fil de 900 MHz ou de 5 GHz.

4. Choisissez le canal le plus « paisible » pour votre réseau sans fil

Dans des environnements domiciliaires ou d'entreprise rapprochés, tels que les appartements et les immeubles à bureaux, il se peut qu'un autre réseau sans fil interfère et entre en conflit avec votre réseau.

Grâce à la fonction d'analyse du site de l'Utilitaire de réseau sans fil, vous pourrez localiser d'autres réseaux sans fil disponibles (consultez le manuel de votre adaptateur sans fil), et choisir pour votre routeur sans fil (ou point d'accès) un canal aussi loin que possible du canal utilisé par ces réseaux.

Essayez plusieurs canaux parmi ceux disponibles afin de déterminer la connexion la plus claire et éviter les interférences de la part de téléphones sans fil ou d'autres dispositifs sans fil se trouvant dans votre voisinage.

Pour les dispositifs de réseau sans fil d'une marque différente, utilisez la fonction d'analyse de site détaillée et consultez les informations concernant les canaux qui se trouvent dans ce manuel.

Ces solutions devraient vous permettre d'obtenir une zone de couverture maximale avec votre routeur ou votre point d'accès. Si vous devez étendre votre zone de couverture, nous vous suggérons l'Amplificateur de signal/Point d'accès de Belkin

5. Connexions sécurisées, VPN et AOL

Une connexion sécurisée est une connexion qui requiert un nom d'utilisateur et un mot de passe et qui est utilisée là où la sécurité revêt une grande importance. Parmi les connexions sécurisées :

- Les connexions de type Virtual Private Network (VPN - réseau privé virtuel) souvent utilisées pour accéder à distance à un réseau d'entreprise.
- Le programme « Bring your own access » d'America Online (AOL) qui vous permet d'utiliser AOL via une connexion à haut débit (ADSL ou câble) offerte par un autre fournisseur d'accès à Internet.
- La plupart des banques en ligne
- Plusieurs sites commerciaux qui requièrent un nom d'utilisateur et un mot de passe afin d'accéder à un compte.

Les connexions sécurisées peuvent être interrompues par les paramètres de gestion de l'énergie de votre ordinateur (lorsqu'il est en état de veille). La solution la plus simple afin d'éviter cette situation est de vous reconnecter en lançant le logiciel de VPN ou d'AOL ou en vous reconnectant via le site web sécurisé.

1
2
3
4
5
6
7
8
9
10
11

section

Appendice B : Facteurs à considérer pour l'installation et la mise en route

Une solution alternative consiste à changer les paramètres de gestion de l'énergie afin qu'il ne soit plus mis en état de veille. Toutefois, cette solution peut ne pas être appropriée pour les ordinateurs portables. Pour modifier les paramètres de gestion de l'énergie de Windows, rendez-vous à « Power Options [Options d'alimentation] », dans le « Control Panel [Panneau de Configuration] ». Si les difficultés liées aux connexions sécurisées, au VPN et à AOL persistent, veuillez relire les étapes ci-dessus afin de vous assurer d'avoir tenté les solutions proposées.

Déclaration FCC

DÉCLARATION DE CONFORMITÉ À LA RÉGLEMENTATION FCC EN MATIÈRE DE COMPATIBILITÉ ÉLECTROMAGNÉTIQUE

Nous, Belkin International, Inc., sis au 501 West Walnut Street, Compton CA, 90220, États-Unis, déclarons sous notre seule responsabilité que le produit

F5D7632uk4A

auquel se réfère la présente déclaration, est conforme aux normes énoncées à l'alinéa 15 de la réglementation de la FCC. Le fonctionnement est assujéti aux deux conditions suivantes : (1) cet appareil ne peut pas provoquer d'interférence nuisible et (2) cet appareil doit accepter toute interférence reçue, y compris des interférences pouvant entraîner un fonctionnement non désiré.

Attention : Exposition aux radiations dues aux fréquences radio.

La puissance d'émission en sortie de cet appareil reste largement en dessous des limites d'exposition aux fréquences radios de la FCC. Toutefois, il est conseillé d'utiliser l'appareil de manière à minimiser les risques d'exposition dans des conditions de fonctionnement normales.

Lorsqu'une antenne extérieure est raccordée à l'appareil, la placer de manière à minimiser les risques d'exposition dans des conditions de fonctionnement normales. Pour éviter la possibilité d'excéder les limites d'exposition aux fréquences radio de la FCC, il est conseillé d'éviter qu'une personne se trouve à moins de 20 cm de l'antenne dans des conditions de fonctionnement normales.

Avvertissement de la Commission Fédérale des Communications (FCC)

Cet appareil a été testé et satisfait aux limites établies pour les appareils numériques de classe B, conformément à l'alinéa 15 de la réglementation FCC. Ces limites sont conçues de manière à assurer une protection raisonnable contre les interférences nuisibles au sein d'une installation domestique.

L'appareil génère, utilise et peut irradier une énergie radiofréquence. Si cet équipement cause des interférences nuisibles sur le plan de la réception radio ou télévision, pouvant être déterminées en mettant l'appareil sous et hors tension, l'utilisateur est invité à tester et à corriger l'interférence en prenant une des mesures suivantes :

- Réorienter ou changer de place l'antenne de réception.
- Augmenter la distance entre l'appareil et le récepteur.
- Connecter l'appareil à une prise située sur un circuit différent de celui sur lequel le récepteur est connecté.
- Consulter le revendeur ou un technicien en radio/TV pour obtenir de l'aide.

Modifications

La réglementation de la FCC souligne la nécessité d'indiquer à l'utilisateur que toute modification, de quelque nature que ce soit et non agréée par Belkin Internationa, Inc., lui retire le droit d'utiliser l'appareil.

Canada-Industrie Canada (IC)

La radio sans fil de cet appareil est conforme aux normes RSS 139 & RSS 210 Industry 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.

Europe - Prescription Union européenne

Les produits radio portant le label CE 0682 ou CE alert satisfont à la directive R&TTE (1995/5/CE) établie par la Commission de la Communauté européenne. La conformité avec ces normes sous-entend la conformité avec les normes européennes suivantes

(le standard international équivalent est indiqué entre parenthèses).

- EN 60950 (IEC60950) - Sécurité des produits
- EN 300 328 - Conditions techniques exigées pour les appareils radio
- ETS 300 826 - Conditions générales en matière de compatibilité électromagnétique pour les appareils radio.

Prière de consulter la plaque d'identification apposée sur votre produit Belkin pour déterminer le type d'émetteur.

Les produits portant le label CE satisfait à la directive relative à la compatibilité électromagnétique (89/336/EEC) et la directive sur les basses tensions (72/23/EEC) publiées par la Commission de la Communauté européenne.

La conformité avec ces normes sous-entend la conformité avec les normes européennes suivantes (le standard international équivalent est indiqué entre parenthèses).

- EN 55022 (CISPR 22) - Interférences électromagnétiques
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11)- Immunité électromagnétique
- EN 61000-3-2 (IEC610000-3-2) - Émissions de courants harmoniques
- EN 61000-3-3 (IEC610000) - Fluctuations de tension et flicker
- EN 60950 (IEC60950) - Sécurité des produits

Les produits équipés de transmetteurs radio portent la marque CE 0682 ou CE alert et peuvent également afficher le logo CE.



BELKIN.

EC Declaration of Conformity to R&TTE Directive 1999/5/EC

Manufacturer : BELKIN LTD,
EXPRESS BUSINESS PARK,
SHIPTON WAY
,RUSHDEN
NN10 6GL ENGLAND

Representative : Belkin Ltd
(residing in the EC
holding the TCF)

Product / Apparatus : ADSL Modem/Wireless G Router

Type Number : F5D7632-4

Variants include : All Country Variants

Declaration

I declare that above product conforms to all the applicable requirements of EU Directive 1999/5/EC and is CE-marked accordingly:

Article 3.1a: (Standard(s)) used to show compliance with LVD, 73/23/EEC:

IEC 60950-1 2001 Compliant Test Report No: LD931001H03 03 NOV 04

Article 3.1b: (Standard(s)) used to show compliance with EMC Directive, 89/336/EEC:

EN301 489-1 V1.4.1 (2002-08);EN 301 489-17 V1.2.1 (2002-08) Compliant Test Report No:RM931001H03

Article 3.2: Standard(s) used to show compliance:

...EN300 328 V1.4.1 (2003-04)..... Compliant Test Report No:RC93100H03

Signature : 

Name : K Simpson

Title : European Regulatory Compliance Manager

Date : 20 MAR 2006

Garantie à vie du produit limitée à vie de Belkin International, Inc.

Couverture offerte par la garantie

Belkin International, Inc. garantit à l'acheteur initial de ce produit Belkin que le produit est exempt de défauts de conception, de montage, de matériau et de fabrication.

Période de couverture

Belkin International, Inc. garantit le produit Belkin pour toute la durée de vie du produit.

En cas de problème

Garantie du produit

Belkin s'engage à réparer ou à remplacer gratuitement, à sa convenance, tout produit défectueux (sans intervention dans les frais d'expédition du produit).

Limites de la couverture offerte par la garantie

Toutes les garanties précitées sont nulles et non avenues si le produit Belkin n'est pas retourné à Belkin International, Inc. à la demande expresse de celui-ci, l'acheteur étant responsable de l'acquittement des frais d'expédition, ou si Belkin International, Inc. détermine que le produit Belkin a été installé de façon inappropriée ou modifié d'une quelconque manière. La garantie du produit Belkin ne protège pas contre des calamités naturelles comme les inondations, les tremblements de terre, la foudre ou la guerre, le vandalisme, le vol, l'usure normale, l'érosion, l'épuisement, l'obsolescence, l'abus, les dommages provoqués par des perturbations de basse tension (baisses ou affaissements de tension, par exemple), un programme non autorisé ou une modification de l'équipement du système.

Pour une demande d'intervention

Vous devez prendre les mesures suivantes pour faire réparer ou entretenir votre produit Belkin :

1. Contactez Belkin International, Inc. au 501 W. Walnut St., Compton CA 90220, U.S.A. À l'attention de : Customer Service (service client) ou appelez le (800)-223-5546 15 jours maximum après l'événement. Préparez-vous à fournir les informations suivantes :

- a. Référence du produit Belkin.
- b. Lieu d'achat du produit.
- c. Date d'achat du produit.
- d. Copie de la facture d'origine.

2. Le représentant du service client Belkin vous donnera alors toutes les instructions sur la façon d'expédier votre facture et le produit Belkin et la façon de présenter votre réclamation.

Belkin International, Inc. se réserve le droit d'examiner le produit Belkin endommagé. Tous les frais d'expédition du produit Belkin à l'adresse de Belkin International, Inc. en vue de son inspection seront entièrement à la charge de l'acheteur. Si Belkin détermine, à son entière discrétion, qu'il serait impossible d'expédier l'équipement

endommagé à Belkin International, Inc., Belkin peut désigner un atelier de réparation de son choix pour l'inspection du produit et l'établissement d'un devis de réparation. Les coûts, s'il en est, pour l'expédition de l'équipement jusqu'à l'atelier de réparation et le retour, et pour l'estimation, seront entièrement assumés par l'acheteur. L'équipement endommagé doit être disponible pour inspection jusqu'à ce que la demande de réclamation soit réglée. Lors de tout règlement, Belkin International, Inc. se réserve le droit d'un recours en subrogation sous toute autre police d'assurance détenue par l'acheteur.

Relation entre le Droit national et la garantie

BELKIN INTERNATIONAL, INC. REJETTE PAR LE PRÉSENT DOCUMENT TOUTES LES AUTRES GARANTIES, EXPLICITES OU IMPLICITES, SAUF EXCEPTIONS PRÉVUES PAR LA LOI, Y COMPRIS MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES AFFÉRENTES À LA QUALITÉ LOYALE ET MARCHANDE ET À L'ADÉQUATION À UNE FINALITÉ DONNÉE, ET CES GARANTIES IMPLICITES, S'IL Y A LIEU, SONT D'UNE DURÉE LIMITÉE AU CONDITIONS DE LA PRÉSENTE GARANTIE.

Certains pays ne permettent pas d'imposer de limite à la durée de validité des garanties implicites. Il se peut donc que les limites ci-dessus ne s'appliquent pas dans votre cas.

BELKIN INTERNATIONAL, INC. NE PEUT EN AUCUN CAS ÊTRE TENU RESPONSABLE DE DOMMAGES ACCESSOIRES, DIRECTS, INDIRECTS OU MULTIPLES, Y COMPRIS, MAIS SANS S'Y LIMITER, LES PERTES COMMERCIALES OU DE REVENUS DÉCOULANT DE LA VENTE OU DE L'UTILISATION DE TOUT PRODUIT BELKIN, MÊME LORSQU'IL A ÉTÉ AVISÉ DE LA PROBABILITÉ DES DITS DOMMAGES.

La garantie vous confère des droits légaux spécifiques. Vous pouvez également bénéficier d'autres droits qui varient d'un pays à l'autre. Certains pays ne permettent pas d'exclure ou de limiter les dommages accidentels, consécutifs ou autres, de sorte que les limitations d'exclusions précitées peuvent ne pas s'appliquer dans votre cas.

Pour en savoir plus sur la récupération du produit, visitez <http://environmental.belkin.com>



POUR UTILISATION DANS
LES PAYS SUIVANTS

AT BE CY CZ DK EE FI FR DE GR HU IE
IT LV LT LU MT NL PL PT SK SI ES SE GB IS LI
NO CH BG RO TR

CANAUX DE FONCTIONNEMENT 1-13

Utilisation restreinte dans certains pays. . Équipement de Classe 2

BELKIN®

Modem ADSL2+ avec Routeur Sans Fil G

BELKIN®

www.belkin.com

Assistance Technique Belkin

Royaume-Uni : 0845 607 77 87

Europe : www.belkin.com/support

Belkin Ltd.

Express Business Park
Shipton Way, Rushden
NN10 6GL, Royaume-Uni
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 Fax

Belkin SAS

130 rue de Sully
92100 Boulogne-Billancourt,
France
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH

Hanebergstrasse 2
80637 Munich
Allemagne
+49 (0) 89 143405 0
+49 (0) 89 143405 100 Fax

Belkin Iberia

C/ Anabel Segura, 10 planta baja, Of. 2
28108, Alcobendas, Madrid
Espagne
+34 91 791 23 00
+34 91 490 23 35 fax

Belkin Italie & Grèce

Via Carducci, 7
Milan 20123
Italie
+39 02 862 719
+39 02 862 719 Fax

Belkin B.V.

Boeing Avenue 333
1119 PH Schiphol-Rijk,
Pays-Bas
+31 (0) 20 654 7300
+31 (0) 20 654 7349 Fax

© 2007 Belkin International, Inc. Tous droits réservés. Toutes les raisons commerciales sont des marques déposées de leurs fabricants respectifs. Mac, Mac OS, Apple et AirPort sont des marques de commerce d'Apple Inc., enregistrées aux États-Unis et dans d'autres pays. Microsoft, NT, Windows et Windows Vista sont des marques déposées ou des marques de commerce de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

P74725ea-A

BELKIN®

ADSL2+ Modem mit integriertem kabellosen G Router

EN

FR

DE

NL

ES

IT



Benutzerhandbuch

F5D7632ea4A

Inhaltsverzeichnis

1. Einleitung	1
Produktmerkmale	1
Vorzüge eines Netzwerks zu Hause	3
Vorteile eines kabellosen Netzwerks von Belkin	3
2. Sie benötigen Folgendes	4
Verpackungsinhalt	4
Systemvoraussetzungen	4
Systemanforderungen für die Installationssoftware	4
Internet-Verbindungseinstellungen	4
3. Beschreibung des Routers	5
4. Anschließen und Konfigurieren des Routers	8
Schritt 1A: Hardware anschließen – Folgen Sie den Anweisungen in der Installationsanleitung	8
Schritt 1B: Ein vorhandenes Modem oder einen Modem-Router ersetzen	9
Schritt 2: Router einrichten – Installationsprogramm ausführen	10
5. Manuelle Konfiguration des Routers	13
Übersicht über die Webgestützte Erweiterte Benutzeroberfläche	13
Ändern der LAN-Einstellungen	15
DHCP-Client-Liste	16
Internet-WAN	17
Verbindungstyp	17
Funknetz	23
Verschlüsselung/Sicherheit	25
Kabellose Bereichserweiterung und Bridging	35
Firewall	37
Dienstprogramme	43
6. Manuelle Konfiguration der Netzwerkadapter	51
7. Empfohlene Browser-Einstellungen	55
8. Fehlerbehebung	57
9. Technische Support Informationen	68
10. Anhang	69
Anhang A: Glossar	69
Anhang B: Wichtige Faktoren bei Aufstellung und Einrichtung	74
11. Informationen	77

Wir beglückwünschen Sie zum Kauf dieses ADSL2+ Modems mit integriertem kabellosen Router (im Folgenden als „Router“ bezeichnet). In wenigen Minuten können Sie Ihren Internet-Zugang gemeinsam nutzen und Ihre Computer zu einem Netzwerk verbinden. Die folgende Liste beinhaltet die Merkmale, die Ihren Router zur idealen Lösung für Ihr Netzwerk zu Hause oder in einem kleinen Büro machen. Bitte lesen Sie dieses Handbuch sorgfältig durch und beachten Sie besonders den Anhang B mit dem Titel „Wichtige Faktoren bei Aufstellung und Einrichtung“.

Produktmerkmale

Geeignet für PCs und Mac® Computer

Der Router unterstützt eine Reihe von Netzwerkkombinationen, darunter unter anderem Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP, Vista und andere. Sie benötigen einen Internet-Browser und einen Netzwerkadapter, der TCP/IP unterstützt, die Standardsprache im Internet.

LED-Anzeige an der Vorderseite

Leuchtanzeigen an der Routervorderseite zeigen die Funktionen an, die in Betrieb sind. Sie sehen auf den ersten Blick, ob Ihr Router mit dem Internet verbunden ist. Dadurch ersparen Sie sich komplexe Software und Statusüberwachungsverfahren.

Webgestützte Erweiterte Benutzeroberfläche

Sie können die vielseitigen Routerfunktionen bedienerfreundlich mit Ihrem Browser einstellen, ohne zusätzliche Software auf dem Computer zu installieren. Es müssen also keine Installations-CDs eingelegt werden. Alle Änderungen und Konfigurationen können Sie einfach und schnell an einem beliebigen Computer im Netz vornehmen.

Integrierter 10/100 4-Port Switch

Über den integrierten 4-Port Netzwerk-Switch des Routers können die über Kabel vernetzten Computer Drucker, Daten und MP3-Dateien, digitale Fotos und vieles mehr gemeinsam nutzen. Der Switch passt sich automatisch an die Geschwindigkeit der angeschlossenen Geräte an. Er überträgt gleichzeitig Daten zwischen den Computern und dem Internet, ohne dabei Ressourcen zu unterbrechen oder zu verbrauchen.

Integrierter 802.11g Kabelloser Access Point

802.11g ist eine bahnbrechende neue Funktechnologie, die Datenraten von bis zu 54 Mbit/s bietet und damit fast fünfmal so schnell ist wie der übliche Standard 802.11b.

Integriertes DHCP (Dynamic Host Configuration Protocol)

Das integrierte DHCP (Dynamic Host Configuration Protocol, dynamisches Host-Konfigurationsprotokoll) sorgt für eine besonders einfache Netzwerkverbindung. Es weist jedem Computer automatisch eine IP-Adresse zu, so dass dem Benutzer eine komplizierte Netzwerkeinrichtung erspart bleibt.

Gemeinsame Nutzung von IP-Adressen (NAT IP Address Sharing)

Ihr Router nutzt die einzelne IP-Adresse, die Ihnen der Internet-Provider zuweist, mittels des sogenannten NAT-Verfahrens (Network Address Translation) für mehrere Computer, so dass Sie keine zusätzlichen IP-Adressen anmieten müssen.

SPI-Firewall

Ihr Router ist mit einer Firewall ausgestattet, die Ihr Netzwerk vor einer Vielzahl verbreiteter Hackerangriffe schützt, wie z. B. IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP der Länge Null, Smurf Attack, TCP Null Scan, SYN Flood, UDP Flooding, Tear Drop Attack, ICMP Defect, RIP Defect und Fragment Flooding.

MAC-Adressfilter

Sie können die Sicherheit erhöhen, indem Sie eine Liste von MAC-Adressen festlegen (eindeutige Client-Kennungen), die auf Ihr Netzwerk zugreifen dürfen. Jeder Computer verfügt über eine eigene MAC-Adresse. Sie können diese MAC-Adressen in eine Liste auf der browsergestützten Benutzeroberfläche eingeben und dadurch den Zugriff auf das Netzwerk kontrollieren.

Universales Plug&Play (UPnP)

Die UPnP-Technologie (Universales Plug&Play) ermöglicht den nahtlosen Betrieb von Sprach- und Videomeldungen, Spielen und anderen Anwendungen, die dem UPnP-Standard entsprechen.

Unterstützung für VPN Pass-Thru

Wenn Sie von zu Hause aus über VPN eine Verbindung zu Ihrem Büro-Netzwerk herstellen, lässt der Router Ihren VPN-Computer passieren, so dass er Zugriff auf das Netzwerk erhält.

Vorzüge eines Netzwerks zu Hause

Wenn Sie unseren einfachen Installationsanleitungen folgen, können Sie Ihr Belkin-Heimnetzwerk folgendermaßen einsetzen:

- Nutzung einer Hi-Speed Internetverbindung mit allen Computern bei Ihnen zu Hause
- Nutzung von Ressourcen wie Dateien und Festplatten auf allen angeschlossenen Computern bei Ihnen zu Hause
- Nutzung eines einzigen Druckers mit der ganzen Familie
- Gemeinsamer Zugriff auf Dokumente, Musik, Video und digitale Fotos
- Speichern von Dateien auf verschiedenen Computern; Aufrufen und Kopieren dieser auf verschiedenen Computern
- Gleichzeitig Spielen von Spielen im Internet, Verschicken und Empfangen von E-Mails und Chatten

Vorteile eines kabellosen Netzwerks von Belkin

Mobilität — Sie brauchen kein spezielles „Computerzimmer“ mehr - Sie können jetzt überall in der Reichweite des kabellosen Netzwerks an einem vernetzten Notebook oder Desktop-Computer arbeiten

Einfache Installation — der Installationsassistent von Belkin vereinfacht die Konfiguration

Flexibilität — überall bei Ihnen zu Hause können Sie Drucker, Computer und andere Netzwerkgeräte aufstellen und benutzen

Einfache Erweiterung — die große Palette an Netzwerkprodukten von Belkin ermöglicht die Erweiterung Ihres Netzwerks mit Geräten wie Druckern und Spielkonsolen

Keine Verkabelung erforderlich — Sie können sich Kosten und Mühe für die Aufrüstung der Ethernetverkabelung im ganzen Haus oder Büro sparen

Breite Akzeptanz auf dem Markt — wählen Sie aus einem großen Angebot an Netzwerkprodukten aus, die vollständig kompatibel sind

Sie benötigen Folgendes

Verpackungsinhalt

- ADSL2+ Modem mit integriertem kabellosen G Router
- RJ11 Telefonschnur - Grau
- RJ45 Ethernet-Netzwerkkabel - Gelb
- ADSL-Mikrofilter*
- Netzteil
- Benutzerhandbuch und Installationssoftware von Belkin auf CD-ROM

*ADSL-Mikrofilter (Splitter) sind landesspezifisch. Ist dieser nicht vorhanden, müssen Sie einen erwerben.

Systemvoraussetzungen

- Ein aktiver ADSL-Dienst mit einem Telefonanschluss zur Verbindung mit dem Router
- Mindestens ein richtig konfigurierter Computer mit einer Netzwerkkarte (Network Interface Card - NIC) und installiertem Browser.
- TCP/IP-Netzwerkprotokoll auf jedem Computer installiert, der mit dem Router verbunden ist
- Kein anderer DHCP-Server in Ihrem lokalen Netzwerk, der Computern und anderen Geräten IP-Adressen zuteilt

Systemvoraussetzungen für die Installationssoftware

- Ein PC mit dem Betriebssystem Windows® 2000, XP oder Vista™
- Mindestens 500-MHz-Prozessor und 128-MB-Arbeitsspeicher
- Internet-Browser

Internet-Verbindungseinstellungen

Der Installationsassistent verfügt über Daten zu Internet Service Providern (ISP) in jedem Land, die Ihnen die Einrichtung Ihres Routers erleichtern. Wenn Ihr ISP nicht auf der Liste aufgeführt wird, wenden Sie sich vor der Einrichtung des Routers bitte an Ihren ISP:

- Internet-Verbindungsprotokoll: (PPPoE, PPPoA, Dynamische IP, Statische IP)
- Methode: Multiplexing oder Kapselung: (LLC oder VC MUX)
- Virtuelle Pfaderkennung: VPI (Virtual Path Identifier) _____
(eine Zahl zwischen 0 und 255)
- VCI (Virtual Channel Identifier) _____
(eine Zahl zwischen 1 und 65535)
- Für PPPoE- und PPPoA-Nutzer: ADSL-Konto-Benutzername und Kennwort _____
- Nutzer einer statischen IP: IP-Adresse ____ . ____ . ____ . ____
Subnetz-Maske ____ . ____ . ____ . ____
Standard Gateway-Server ____ . ____ . ____ . ____
- IP-Adresse für Domännennamen-Server ____ . ____ . ____ . ____
____ . ____ . ____ (wenn vom ISP zugeteilt)

Beschreibung des Routers

1

2

3

4

5

6

7

8

9

10

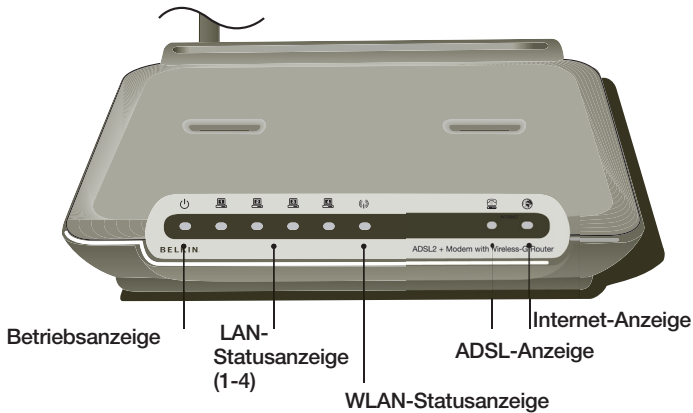
11

Kapitel

Der Router kann auf dem Schreibtisch aufgestellt werden. Alle Kabel sind an der Rückseite des Routers angeschlossen, um eine ordentliche Installation zu erleichtern. Die LED-Anzeigen sind gut sichtbar an der Routervorderseite angebracht, so dass Sie Status und Aktivität des Netzwerks jederzeit ablesen können.

Vorderseite




Auf der Abbildung sehen Sie die Vorderseite des Routers:



LED-Anzeigen

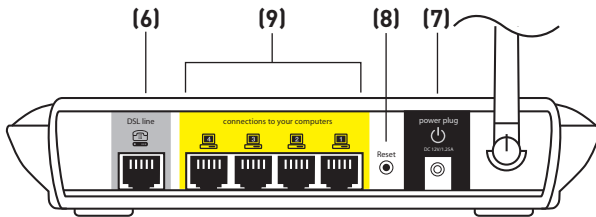
Der Router ist mit neun LED-Anzeigen an der Vorderseite ausgestattet (s. Tabelle auf der nächsten Seite):

Beschreibung des Routers

LED	Farbe	Status	Beschreibung
ADSL			
	Grün	AUS	Keine Stromversorgung oder physische Verbindung mit ADSL-Leitung ist unterbrochen
		Blinkanzeige	Handshaking oder Training wird durchgeführt
		Daueranzeige	Verbindung mit ADSL-Leitung ist OK
Wireless			
	Grün	AUS	Keine Stromversorgung oder kein Funksignal (WLAN-Karte nicht vorhanden oder nicht funktionsfähig)
		Blinkanzeige	Datenverkehr über WLAN-Schnittstelle
		Daueranzeige	WLAN-Schnittstelle ist betriebsbereit
Internet			
	Grün	AUS	Keine Internetverbindung
		Blinkanzeige	Datenübertragung
		Daueranzeige	Verbunden mit dem Internet
LAN 1 bis LAN 4			
LAN 1 - 4			
	Grün	AUS	Keine Stromversorgung oder keine Ethernet-Schnittstelle vorhanden
		Blinkanzeige	Ethernet-Schnittstelle ist vorhanden und Benutzerdaten werden über die Ethernet-Schnittstelle übertragen
		Daueranzeige	Ethernet-Schnittstelle ist vorhanden
Stromversorgung			
	Grün	AUS	Ausgeschaltet
		Daueranzeige	Eingeschaltet

Rückseite

Auf der folgenden Abbildung sehen Sie die Rückseite des Routers.



Netzanschluss — Zum Anschließen des enthaltenen Netzteils. Die Verwendung eines falschen Adaptertyps kann zu Schäden am Router führen.

Ethernet-Anschlüsse — Die Ethernet-Anschlüsse sind RJ45, 10/100 Auto-Negotiation. Die Ports sind mit den Zahlen 1 bis 4 bezeichnet, die mit den nummerierten LED-Lampen an der Vorderseite des Routers übereinstimmen. Schließen Sie Ihre Netzwerk-Computer oder andere Netzwerkgeräte an einen dieser Ports an.

ADSL-Leitung — Dieser Anschluss dient der Verbindung mit der ADSL-Leitung. Verbinden Sie das ADSL-Kabel mit diesem Port.

Rücksetztaste — Die Rücksetztaste wird nur in seltenen Fällen benötigt, wenn der Router nicht mehr korrekt arbeitet. Beim Zurücksetzen wird der Router in den Normalbetrieb versetzt. Die programmierten Einstellungen bleiben erhalten. Mit der Rücksetztaste können Sie auch die Werkseinstellungen wiederherstellen. Dies ist zum Beispiel nützlich, wenn Sie das von Ihnen eingestellte Kennwort vergessen haben.

a. Zurücksetzen des Routers

Halten Sie die Rücksetztaste eine Sekunde lang gedrückt. Wenn die Betriebs-/Bereitschaftsanzeige wieder Dauerlicht anzeigt, ist das Zurücksetzen abgeschlossen.

b. Wiederherstellen der Werkseinstellungen

Halten Sie die Rücksetztaste 20 Sekunden lang gedrückt. Wenn die Betriebs-/Bereitschaftsanzeige wieder Dauerlicht anzeigt, ist die Wiederherstellung abgeschlossen.

Anschließen und Konfigurieren des Routers

Installationsassistent

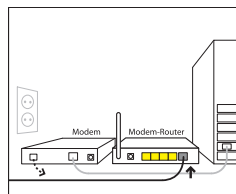
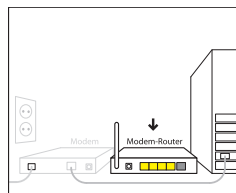
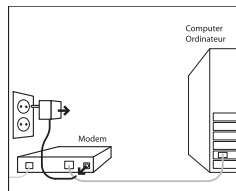
Der Installationsassistent von Belkin macht die Routerinstallation zum Kinderspiel. Dadurch können Sie Ihren Router in wenigen Minuten zum Laufen bringen. Zur Verwendung des Installationsassistenten muss der Computer mit dem Betriebssystem Windows 2000, XP oder Vista™ direkt an den ADSL-Anschluss angeschlossen werden und die Internetverbindung muss während der Installation aktiv sein und funktionieren. Ist dies nicht der Fall, müssen Sie den Router manuell konfigurieren, wie unter „Alternatives Einrichtungsverfahren“ beschrieben. Wenn Sie ein anderes Betriebssystem als Windows 2000, XP oder Vista bzw. Mac OS X verwenden, müssen Sie den Router ebenfalls mit dem alternativen Einrichtungsverfahren konfigurieren.

Schritt 1A: Hardware anschließen – Folgen Sie den Anweisungen in der Installationsanleitung

Erstinstallation des Routers

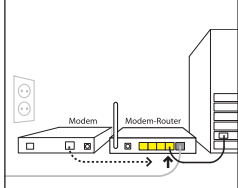
Gehen Sie nach folgenden Schritten vor, wenn Sie KEIN vorhandenes Modem ersetzen. Wenn Sie ein vorhandenes Modem ersetzen, fahren Sie mit dem Abschnitt „Ein vorhandenes Modem oder einen Modem-Router ersetzen“ auf Seite 9 fort.

- 1A.1** Nehmen Sie Ihren neuen Router aus der Verpackung und legen Sie ihn neben den Computer. Richten Sie die Antennen des Routers nach oben aus.
- 1A.2** Nehmen Sie das gelbe RJ45-Kabel, das im Lieferumfang des Routers enthalten ist. Schließen Sie zuerst ein Ende an einen der gelben Anschlüsse mit der Aufschrift „Wired Computers“ (Verkabelte Computer) an der Rückseite Ihres Routers an. Schließen Sie dann das andere Ende an den Netzwerkanschluss an der Rückseite Ihres Computers an. [Insert Ethernet logo]
- 1A.3** Nehmen Sie das enthaltene graue RJ11-Telefonkabel. Schließen Sie ein Ende an den grauen Anschluss mit der Aufschrift „DSL“ an der Rückseite des Routers an. Schließen Sie dann das andere Ende an den ADSL-Anschluss an (entweder an die Wanddose oder an den ADSL-Splitter).



Hinweis: Für manche ADSL-Verbindungen ist ein Mikrofilter (Splitter) erforderlich. Fragen Sie beim ADSL-Provider nach, ob Sie einen benötigen. In Ländern, in denen ein Mikrofilter verwendet wird, ist dieser im Lieferumfang enthalten. Sie erfahren bei Ihrem ADSL-Provider, ob Sie einen Mikrofilter benötigen.

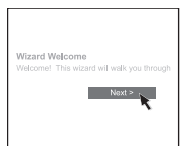
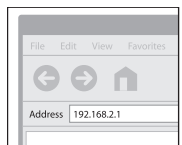
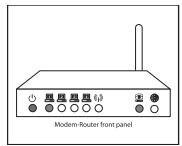
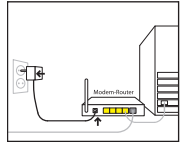
1A.4 Schließen Sie das Netzteil Ihres Routers an den schwarzen Anschluss mit der Aufschrift „Power“ (Strom) an der Rückseite des Routers an. Es kann ca. 20 Sekunden dauern, bis der Router hochgefahren ist. Sehen Sie sich die Anzeigen an der Vorderseite des Routers an. Die Symbole „Wired“ (Verkabelt) und „Modem-Router“ müssen grün leuchten. Ist dies nicht der Fall, überprüfen Sie die Kabelverbindungen.



Schritt 1B: Ein vorhandenes Modem oder einen Modem-Router ersetzen

Gehen Sie nach diesen Schritten vor, wenn Sie bereits über ein Modem oder einen Modem-Router verfügen und dieses/diesen durch den neuen Router ersetzen wollen.

- 1B.1 Nehmen** Sie Ihren neuen Router aus der Verpackung und legen Sie ihn neben das alte Modem. Richten Sie die Antennen des Routers nach oben aus. Ziehen Sie das Netzkabel am alten Modem ab.
- 1B.2** Nehmen Sie das Kabel, über welches Modem und Computer miteinander verbunden sind. Ziehen Sie dieses Kabel am alten Modem ab und schließen Sie es an einen der gelben Anschlüsse mit der Aufschrift „Wired Computers“ an der Rückseite des neuen Routers an.
- 1B.3** Nehmen Sie das Kabel, mit welchem Ihr altes Modem an den ADSL-Anschluss angeschlossen ist. Ziehen Sie es an Ihrem alten Modem ab und schließen Sie es an den grauen Anschluss an der Rückseite des Routers an, der mit der Aufschrift „DSL“ gekennzeichnet ist.
- 1B.4** Schließen Sie das Netzteil Ihres Routers an den schwarzen Anschluss mit der Aufschrift „Power“ (Strom) an der Rückseite des Routers an.
- 1B.5 Wait** Es kann ca. 20 Sekunden dauern, bis der Router hochgefahren ist. Sehen Sie sich die Anzeigen an der Vorderseite des Routers an. Kontrollieren Sie, ob die ADSL- und LAN-Anzeigen grün leuchten. Ist dies nicht der Fall, überprüfen Sie die Kabelverbindungen.



Schritt 2: Router einrichten – Installationsprogramm ausführen

2.1 Schließen Sie alle auf dem Computer ausgeführten Anwendungen. Soweit vorhanden, deaktivieren Sie die Firewall und die Software für die gemeinsame Internetnutzung auf Ihrem Computer.

2.2 Legen Sie die CD in das CD-ROM-Laufwerk des Computers ein. Der Installationsassistent wird automatisch innerhalb von 15 Sekunden auf dem Bildschirm Ihres Computers angezeigt. Klicken Sie auf „Go“ (Weiter), um die Installationssoftware auszuführen. Folgen Sie den Anweisungen auf dem Bildschirm.

WICHTIG: Führen Sie das Installationsprogramm auf dem Computer aus, der ab Schritt 1A.2 direkt mit dem Router verbunden ist.

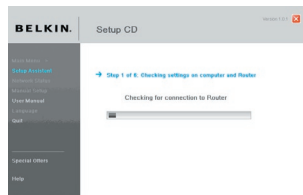
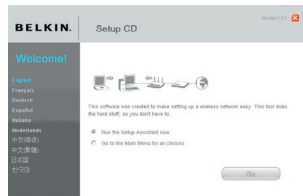
Hinweis für Benutzer von Windows: Wenn der Installationsassistent nicht automatisch startet, wählen Sie Ihr CD-ROM-Laufwerk unter „Arbeitsplatz“ und doppelklicken Sie auf die Datei „SetupAssistant“, um ihn zu starten.

2.3 Standortauswahl. Wählen Sie Ihren Standort in der Dropdown-Liste aus. Klicken Sie auf „Begin“ (Starten), um fortzufahren.

2.4 Bestätigung. Bestätigen Sie, dass Sie alle Schritte in der Installationsanleitung ausgeführt haben, indem Sie das Feld rechts neben dem Pfeil markieren. Klicken Sie auf „Next“ (Weiter), um fortzufahren.

2.5 Fortschritt Jeder abgeschlossene Schritt der Installation wird gesondert angezeigt.

2.6 Einstellungen überprüfen. Der Installationsassistent untersucht jetzt die Einstellungen Ihres Computers und ermittelt Informationen, die er später für die Verbindung des Routers mit dem Internet benötigt.



2.7 Überprüfen der Hardware-Verbindungen
Der Installationsassistent überprüft jetzt die Hardware-Verbindungen.

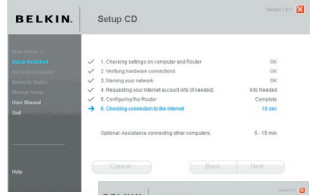
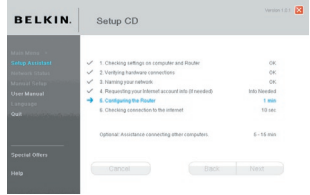
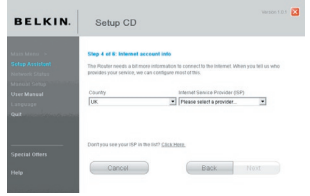
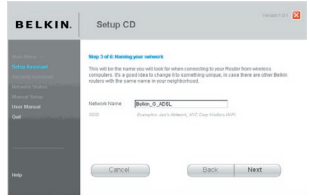
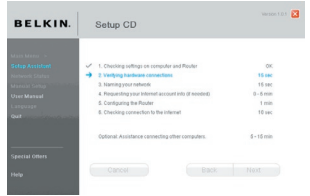
2.8 Benennung Ihres kabellosen Netzwerks
Der Installationsassistent zeigt den vorgegebenen Namen des kabellosen Netzwerks oder SSID (Service Set Identifier) an. Dies ist der Name Ihres kabellosen Netzwerks, in welches Ihre Computer oder andere Geräte mit kabellosen Adaptern eingebunden werden. Sie können entweder die Vorgabe übernehmen oder den Namen ändern. Notieren Sie sich diesen Namen für zukünftige Verwendung. Klicken Sie auf „Next“ (Weiter), um fortzufahren.

2.9 Anfordern der Daten Ihres Internetkontos (falls erforderlich)
Wenn Sie für Ihr Internetkonto einen Anmeldennamen und ein Kennwort benötigen, erscheint ein Fenster, das dem auf der Abbildung unten gleicht. Wählen Sie in der Dropdown-Liste Ihren Standort oder Internet-Provider aus.

2.10 Konfigurieren des Routers
Der Installationsassistent konfiguriert jetzt Ihren Router, indem er ihm Daten zusendet und ihn neu startet. Bitte befolgen Sie die Anweisungen auf dem Bildschirm.

Hinweis: Ziehen Sie während des Neustarts des Routers keine Kabel ab und schalten Sie den Router nicht aus. Ansonsten ist Ihr Router nicht funktionsfähig.

2.11 Prüfen der Internetverbindung.
Sie sind fast fertig. Der Installationsassistent überprüft jetzt Ihre Internetverbindung.

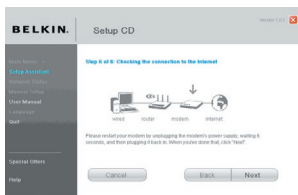


Anschließen und Konfigurieren des Routers

Herzlichen Glückwunsch!

Sie haben die Installation Ihres neuen Belkin Routers abgeschlossen. Das Fenster mit den Glückwünschen (Congratulations) wird angezeigt, wenn der Router eine Verbindung zum Internet herstellen kann. Sie können mit dem Surfen beginnen, indem Sie den Browser öffnen und zu einer beliebigen Website gehen.

Sie können den Installationsassistenten verwenden, um Ihre anderen über Kabel oder kabellos vernetzten Computer so einzurichten, dass Sie eine Verbindung zum Internet herstellen können. Klicken Sie hierzu auf „Next“ (Weiter). Wenn Sie erst später zusätzliche Computer mit dem Router verbinden wollen, wählen Sie „Exit the Assistant“ (Den Assistenten schließen) und klicken Sie dann auf „Next“ (Weiter).

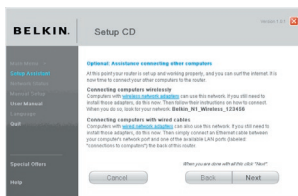


Fehlerbehebung

Sollte der Installationsassistent keine Internetverbindung herstellen können, erscheint dieses Fenster auf dem Bildschirm. Folgen Sie zur Fehlerbehebung den Anweisungen auf dem Bildschirm.

2.12 Optional: Hilfe bei der Einbindung weiterer Computer.. Dieser optionale Schritt unterstützt Sie bei der Einbindung zusätzlicher über Kabel und kabellos vernetzter Computer in Ihr Netzwerk. Folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie überprüft haben, ob Ihre anderen über Kabel und kabellos vernetzten Computer eine einwandfreie Verbindung haben, ist Ihr Netzwerk eingerichtet und betriebsbereit. Sie können nun im Internet surfen. Klicken Sie auf „Next“ (Weiter), um zurück zum Hauptmenü zu gelangen.

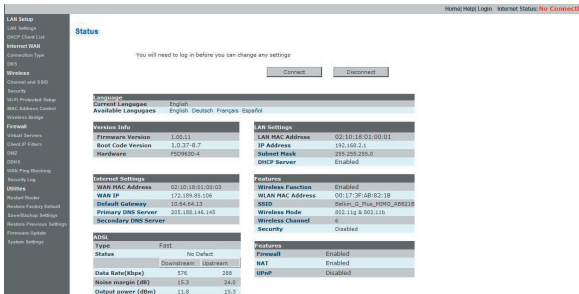


Übersicht über die Webgestützte Erweiterte Benutzeroberfläche

Diese Seite gibt einen Überblick über den Status und die Einstellungen des Routers. Alle weiteren Konfigurationssseiten können von dieser Seite aus abgerufen werden.

Verwendung der Webgestützten Erweiterten Benutzeroberfläche

Wenn Ihr Host-PC korrekt konfiguriert ist, starten Sie Ihren Browser und geben Sie die private IP-Adresse des Routers in das URL-Feld: „192.168.2.1“. Klicken Sie dann auf „Enter“ (Eingabetaste).



1. Navigationslinks

Wenn Sie auf einen dieser Links klicken, gelangen Sie direkt auf eine Einstellungsseite der Benutzeroberfläche. Die Links sind in mehrere Rubriken gegliedert und auf Registerkarten angeordnet, damit Sie die gesuchten Einstellungen leichter finden. Die Funktion der einzelnen Register wird angezeigt, wenn Sie auf den Titel der Registerkarten klicken.

2. Schaltfläche Home

Die Schaltfläche „Home“ finden Sie auf jeder Seite der Erweiterten Benutzeroberfläche. Mit ihr gelangen Sie zurück auf die Startseite.

3. Schaltfläche Hilfe

Mit der Schaltfläche „Help“ (Hilfe) öffnen Sie die Hilfeseiten des Routers. Die Hilfe kann auf vielen Seiten mit der Option „more info“ (Weitere Informationen) aufgerufen werden, die neben vielen Abschnitten angezeigt wird.

4. Schaltfläche Anmelden/Abmelden

Mit dieser Schaltfläche melden Sie sich am Router an oder ab. Wenn Sie am Router angemeldet sind, heißt die Schaltfläche „Logout“ (Abmelden). Beim Anmelden gelangen Sie auf eine eigene Anmeldeseite, auf der Sie ein Kennwort eingeben müssen. Wenn Sie sich am Router angemeldet haben, können Sie Änderungen an den Einstellungen vornehmen. Wenn Sie mit den Änderungen fertig sind, können Sie sich mit der Schaltfläche „Logout“ (Abmelden) wieder vom Router abmelden. Weitere Hinweise zur Anmeldung finden Sie unter „Anmelden an den Router“.

5. Internet-Statusanzeige

Diese Anzeige steht auf allen Routerseiten zur Verfügung. Sie gibt den Verbindungsstatus des Routers an. Erscheint die grüne Anzeige „Connection OK“ (Verbindung OK), ist der Router mit dem Internet verbunden. Besteht keine Verbindung zum Internet, meldet die Anzeige „no connection“ (keine Verbindung) in roten Lettern. Die Anzeige wird automatisch aktualisiert, wenn Sie die Routereinstellungen ändern.

6. LAN-Einstellungen

Ruft die LAN-seitigen Einstellungen des Routers ab. Änderungen an diesen Einstellungen können vorgenommen werden, indem Sie auf den Navigationslink „LAN“ auf der linken Seite des Bildschirms klicken.

7. Merkmale

Zeigt den Status des Router-NAT, der Firewall und der Funkfunktionen an. Sie können die Einstellungen ändern, indem Sie auf einen dieser Links oder auf einen der Navigationslinks links auf dem Bildschirm klicken.

8. Internet-Einstellungen

Zeigt die Internet- und WAN-seitigen Einstellungen des mit dem Internet verbundenen Routers an. Änderungen an diesen Einstellungen können vorgenommen werden, indem Sie auf den Navigationslink „Internet/WAN“ auf der linken Seite des Bildschirms klicken.

9. Versions-Info

Ruft die Firmware-Version, Bootcode-Version, Hardwareversion und die Seriennummer des Routers ab.

10. Seitenname

Die Seite, auf der Sie sich befinden, ist durch diesen Namen gekennzeichnet. Er wird verwendet, wenn im Handbuch auf diese Seite verwiesen wird. Zum Beispiel verweist „LAN > LAN Settings“ auf die Seite „LAN Settings“ (LAN-Einstellungen).

LAN-Einstellungen ändern

Hier können Sie alle Einstellungen für die interne LAN-Konfiguration des Routers überprüfen und ändern.

LAN-Einstellungen

Durch Klicken auf den Reiter der Registerkarte „LAN“ (A) öffnen Sie die Hauptseite der LAN-Einstellungen. Hier finden Sie eine kurze Beschreibung der Funktionen. Zum Anzeigen der Einstellungen oder für Änderungen an den LAN-Einstellungen klicken Sie auf „LAN Settings“ (LAN-Einstellungen) (B). Zum Anzeigen der Liste mit den angeschlossenen Computern klicken Sie auf „DHCP client list“ (DHCP Client Liste) (C).

IP-Adresse

Diese „IP-Adresse“ ist die interne IP-Adresse des Routers. Die Standard-IP-Adresse ist 192.168.2.1. Um die erweiterte Konfigurationsoberfläche zu öffnen, geben Sie diese IP-Adresse in die Adresszeile Ihres Browsers ein. Bei Bedarf können Sie die Adresse ändern. Geben Sie hierzu die neue IP-Adresse ein, und klicken Sie auf „Apply Changes“ (Änderungen übernehmen). Achten Sie darauf, dass Sie eine nicht routbare IP-Adresse wählen. Beispiele für nicht routbare IP-Adressen:

192.168.x.x (x steht für eine Zahl zwischen 0 und 255)

10.x.x.x (x steht für eine Zahl zwischen 0 und 255)

Subnet-Mask

Die Subnetz-Maske muss nicht verändert werden. Dies ist eine eigene, erweiterte Funktion des Routers von Belkin.

DHCP-Server

Die DHCP-Serverfunktion erleichtert die Einrichtung eines Netzwerks, da jedem Computer automatisch eine IP-Adresse zugewiesen wird. Die Standardeinstellung ist „On“ (aktiviert). Der DHCP-Server kann bei Bedarf deaktiviert werden; hierzu müssen Sie allerdings jedem Computer im Netzwerk eine statische IP-Adresse zuweisen. Um den DHCP-Server zu deaktivieren, wählen Sie „Off“ (Aus) und klicken auf „Apply Changes“. (Änderungen übernehmen).

IP-Pool

Die Reihe der IP-Adressen, die für eine dynamische Zuweisung an die Computer im Netzwerk reserviert sind. Wenn Sie diese Zahl ändern möchten, geben Sie eine neue Start- und eine neue Endadresse ein und klicken auf „Apply Changes“ (Änderungen übernehmen). Die Start-IP-Adresszahl muss kleiner sein als die Endzahl.

Frist

Die Zeit, während der der DHCP-Server die IP-Adresse für die einzelnen Computer reserviert. Es wird empfohlen, die Vorgabe „Forever“ (Unbefristet) beizubehalten. Die Vorgabe bedeutet, dass sich die IP-Adresse eines Computers nicht mehr ändert, nachdem sie vom DHCP-Server zugewiesen wurde. Wenn Sie eine andere Frist einstellen, zum Beispiel einen Tag oder eine Stunde, wird die IP-Adresse nach dem Fristablauf freigegeben. Daher kann sich die IP-Adresse eines Computers im Laufe der Zeit ändern. Wenn Sie weiterführende Funktionen des Routers wie DMZ oder Client-IP-Filter eingestellt haben, sind diese an die IP-Adresse gebunden. Daher sollte die IP-Adresse beibehalten werden.

Lokaler Domänenname

Sie können einen lokalen Domännennamen (Netzwerknamen) für Ihr Netzwerk festlegen. Diese Einstellung muss normalerweise nicht geändert werden, soweit Ihrerseits kein bestimmter Grund vorliegt. Sie können den Namen für Ihr Netzwerk frei wählen, z. B. „MY NETWORK“ (MEIN NETZWERK).

DHCP-Client-Liste

Sie können sich die Computer auflisten lassen, die mit dem Netzwerk verbunden sind. Die Liste gibt die IP-Adresse des Computers an, seinen Hostnamen (Name des Computers im Netzwerk) und die MAC-Adresse der Netzwerkkarte des Computers. Mit der Taste „Refresh“ (Aktualisieren) bringen Sie die Liste auf den neuesten Stand. Dadurch werden alle Änderungen sichtbar.

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing "Refresh" will update the list.

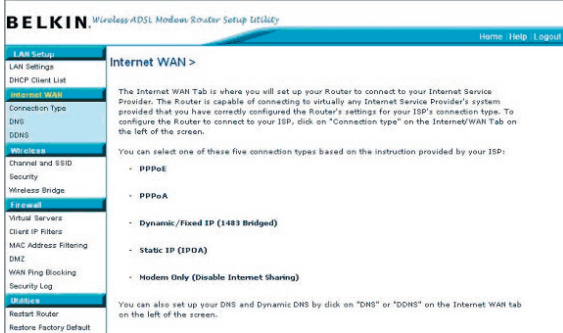
IP Address	Host Name	MAC Address
192.168.2.11	Ericd-XP	00-30-8D-3D-AB-09

[Refresh](#)

Internet-WAN

Auf der Registerkarte „Internet/WAN“, richten Sie den Router für die Verbindung mit Ihrem Provider ein. Der Router kann die Verbindung zu fast jedem ADSL-Anbietersystem herstellen, sofern Sie die Routereinstellungen an den Verbindungstyp anpassen. Die Verbindungseinstellungen werden Ihnen von Ihrem Internetprovider mitgeteilt.

Um die vom Provider vorgeschriebenen Einstellungen am Router vorzunehmen, klicken Sie links auf dem Bildschirm auf „Connection Type“ (Verbindungstyp). Wählen Sie den verwendeten Verbindungstyp aus. Wenn Sie vom Anbieter DNS-Einstellungen erhalten haben, klicken Sie auf „DNS“ (2), um die DNS-Adressangaben für Provider einzugeben, die besondere Einstellungen verlangen. Wenn Sie alle Einstellungen vorgenommen haben, meldet die Statusanzeige „Connection OK“ (Verbindung ok), wenn der Router korrekt konfiguriert wurde.



Verbindungstyp

Auf der Verbindungstypseite können Sie einen von fünf je nach den Angaben Ihres Providers:

PPPoE

PPPoA

Dynamische IP (1483 Bridged)

Statische IP (IPoA)

Nur Modem (Gemeinsame Internetnutzung wird deaktiviert)

Hinweis: Wenn Sie nicht genau wissen, welchen Verbindungstypen Sie wählen sollen, wenden Sie sich bitte an Ihren Provider.

Klicken Sie für die Auswahl des Verbindungstyps auf das entsprechende Optionsfeld und dann auf „Next“ (Weiter).

Manuelle Konfiguration des Routers

WAN > Connection type

The following information is usually provided by your ISP.
Please select the Internet sharing protocol.

- PPPoE
- PPPoA
- Dynamic/Fixed IP (488 Bridged)
- Static IP (1PoA)
- Modem Only (Disable Internet Sharing)

Next

Einstellen des ISP-Verbindungsstyps auf PPPoE oder PPPoA

PPPoE (Point-to-Point Protokoll über Ethernet) ist die Standardmethode, mit der Netzwerkgeräte miteinander verbunden werden. Sie benötigen einen Benutzernamen und ein Kennwort, um über das Netzwerk Ihres Internetanbieters auf das Internet zuzugreifen. PPPoA (PPP über ATM) ist dem PPPoE ähnlich, wird aber meist in Großbritannien verwendet. Wählen Sie „PPPoE“ oder „PPPoA“ aus und klicken Sie anschließend auf „Next“ (Weiter). Geben Sie dann die Informationen von Ihrem Provider an und klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Einstellungen zu aktivieren.

WAN > Connection Type > PPPoE Interface

More Info
ATM Interface

(1) Username

(2) Password

(3) Retype Password

(4) IP assigned by ISP >

IP Address

Subnet Mask

Default Gateway

(5) VPI/VCI

(6) Encapsulation

(7) Dial on Demand >

(8) Idle Time (Minute) >

(9) MTU >

Yes

0 0 0 0

0 0 0 0

0 0 0 0

0 / 35

LLC

0

1456

Clear Changes Apply Changes

1. Benutzername — Geben Sie Ihren Benutzernamen ein. (Vom Internetprovider vergeben).
2. Kennwort — Geben Sie Ihr Kennwort ein. (Vom Internetprovider vergeben).
3. Kennwort erneut eingeben — Bestätigen Sie das Kennwort. (Vom Internetprovider vergeben).
4. Vom ISP zugewiesene IP-Adresse — Lassen Sie „Yes“ (Ja), wenn Ihr Internetprovider automatisch IP-Adressen zuweist. Wenn Ihr Internetprovider eine feste IP-Adresse vergeben hat, wählen Sie „No“ (Nein).

5. VPI/VCI – Geben Sie Ihren Virtual Path Identifier (Virtuelle Pfaderkennung - VPI) und Virtual Circuit Identifier (Virtuelle Circuiterkennung - VCI) hier ein. (Vom Internetprovider vergeben).
6. Kapselung – Wählen Sie Ihre Kapselung aus (vom Internetprovider vergeben), um zu bestimmen, wie mit mehreren Protokollen bei ATM-Transportschicht (ATM transport layer) umgegangen wird. VC-MUX: PPPoA Virtual Circuit Multiplexer (Null-Kapselung) erlaubt es, pro virtuellem Circuit mit weniger Overheads nur ein Protokoll zugleich auszuführen. LLC: PPPoA Logical Link Control ermöglicht es, mehrere Protokolle mit einem virtuellen Circuit (mehr Overheads) zugleich auszuführen.
7. DFÜ-Verbindung automatisch herstellen – Wenn Sie „DFÜ-Verbindung automatisch herstellen“ (Dial on Demand) wählen, wird Ihr Router automatisch mit dem Internet verbunden, wenn ein Benutzer einen Webbrowser öffnet.
8. Zeitlimit (Minuten) – Geben Sie das maximale Zeitlimit für die Internetverbindung an. Nach Ablauf dieser Zeit wird die Verbindung unterbrochen.
9. MTU – Die MTU-Einstellung darf nicht geändert werden, es sei denn, Ihr Provider verlangt ausdrücklich eine bestimmte MTU-Einstellung. Änderungen an der MTU-Einstellung können zu Problemen mit der Internet-Verbindung führen wie Trennung vom Internet, langsamen Verbindungen und Fehlern bei der Arbeit mit Internet-Anwendungen.

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

IP assigned by ISP >	Yes
IP Address	0 0 0 0
Subnet Mask	0 0 0 0
Default Gateway	0 0 0 0
VPI/VCI	0 / 35
Encapsulation	LLC

[Clear Changes](#)[Apply Changes](#)

Einstellen Ihres Verbindungstyps auf Dynamische IP (1483 Bridged)

Diese Verbindungsmethode verbindet Ihr Netzwerk und das Netzwerk des Providers miteinander. Der Router erhält automatisch eine IP-Adresse vom DHCP-Server des Internetproviders (ISP).

Manuelle Konfiguration des Routers

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

(1) IP assigned by ISP >

IP Address

Subnet Mask

(2) Default Gateway

VPI/VCI

(3) Encapsulation

Yes	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	/ 35			
LLC				

Clear Changes Apply Changes

1. Vom ISP zugewiesene IP-Adresse – Lassen Sie „Yes“ (Ja), wenn Ihr Internetprovider automatisch IP-Adressen zuweist. Wenn Ihr Internetprovider eine feste IP-Adresse vergeben hat, wählen Sie „No“ (Nein).

2. VPI/VCI – Geben Sie Ihre VPI- und VCI-Kennziffer hier ein. Diese Erkennung wird vom Internetprovider erteilt.

3. Kapselung – Wählen Sie, ob Ihr Internetprovider LLC oder VC MUX verwendet.

Einstellen der ISP-Verbindung auf Statische IP (IPoA)

Dieser Verbindungstyp wird auch als „Classical IP over ATM“ (Klassische IP über ATM) oder „CLIP“ bezeichnet, wobei der Internetprovider eine feste IP für Ihren Router erstellt.

1. IP-Adresse – Geben Sie eine IP-Adresse ein, die vom Internetprovider für die WAN-Schnittstelle des Routers erteilt wurde.

2. Subnetz-Maske – Geben Sie hier die Subnetz-Maske ein, die vom Internetprovider festgelegt wurde.

WAN > Connection Type > Static IP(IPoA)

More Info
ATM Interface

(1) IP Address >

(2) Subnet Mask >

(3) Default Gateway >

(4) VPI/VCI >

(5) Encapsulation >

0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	/ 35			
LLC				

Clear Changes Apply Changes

3. Standard-Gateway – Geben Sie eine Standard-Gateway IP-Adresse ein. Wenn der Router die Zieladresse innerhalb des lokalen Netzwerks nicht finden kann, wird er die Pakete an die Standard-Gateway senden.

4. VPI/VCI – Geben Sie Ihre VPI- und VCI-Kennziffer hier ein. Diese Kennung wird vom Provider zugewiesen.

5. Kapselung – Wählen Sie, ob Ihr Internetprovider LLC oder VC MUX verwendet.

Einstellen Ihres Verbindungstyps auf „Nur Modem (Gemeinsame Internetnutzung deaktivieren)“

In diesem Modus funktioniert der Router einfach als Bridge zur Versendung von Paketen über den DSL-Anschluss. Dazu muss eine ergänzende Software auf dem Computer installiert werden, über den der Zugang zum Internet erfolgen soll.

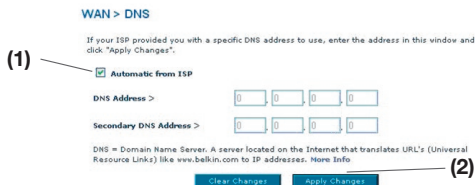


1. VPI/VCI — Geben Sie Ihre VPI- und VCI-Kennziffer hier ein. (Vom Internetprovider vergeben).
2. Kapselung — Wählen Sie LLC oder VC MUX. (Vom Internetprovider vergeben).

DNS (Domain Name Server - Domännennamenserver)-Einstellungen

Als DNS (Domain Name Server) wird ein Server im Internet bezeichnet, der URLs (Universal Resource Links) wie „www.belkin.com“ zu IP-Adressen auflöst. Bei vielen Providern ist eine Eingabe dieser Informationen in den Router unnötig. Markieren Sie das Feld „Automatisch vom ISP“, wenn Ihnen der Provider keine bestimmte DNS-Adresse mitgeteilt hat. Wenn Sie einen statischen Verbindungstyp verwenden, müssen Sie möglicherweise eine bestimmte DNS-Adresse sowie eine sekundäre DNS-Adresse angeben, damit die Verbindung ordnungsgemäß funktioniert. Wenn Sie mit einem dynamischen Verbindungstyp oder PPPoE arbeiten, müssen Sie wahrscheinlich keine DNS-Adresse eingeben.

Lassen Sie dann das Kontrollkästchen „Automatic from ISP“ (Automatisch vom ISP) markiert. Um die DNS-Adresseinstellungen einzugeben, deaktivieren Sie das Kontrollkästchen „Automatic from ISP“ (Automatisch vom ISP) und geben Sie die DNS-Einträge in die entsprechenden Felder ein. Klicken Sie auf „Apply Changes“ (2) (Änderungen übernehmen), um die Einstellungen zu speichern.



Verwenden von DDNS (Dynamische DNS)

Der DDNS-Dienst ermöglicht Ihnen, eine dynamische IP-Adresse in jeder der zahlreichen Domänen, die DynDNS.org anbietet, als statischen Hostnamen auszuweisen. Sie erlauben Ihren Netzwerkcomputern damit, leichter auf verschiedene Bereiche des Internets zuzugreifen. DynDNS.org bietet diesen Dienst für maximal fünf Hostnamen kostenlos im Internet an. Alternativ zu DynDNS.org können Sie auch TZO.com verwenden. Der Dynamische DDNS-Dienst ist ideal für private Internetseiten, Dateiserver oder um den Zugriff zu Ihrem Heim-PC von Ihrem Arbeitsplatz aus zu erleichtern. Verwenden Sie den Dienst, wenn Sie sicher gehen möchten, dass Ihr Hostname immer zu Ihrer IP-Adresse führt, unabhängig davon, wie oft diese von Ihrem Provider geändert wird. Auch wenn sich Ihre IP-Adresse ändert, können Ihre Freunde und Bekannte sie immer im Internet finden, indem Sie ersatzweise die Adresse ihrname.dyndns.org eingeben! Um sich kostenlos für Dynamic DNS anzumelden, öffnen Sie die Seite <http://www.dyndns.org> (englischsprachig).

Einstellen des Update-Clients für Dynamisches DNS

Sie müssen sich beim kostenlosen Aktualisierungsdienst von DynDNS.org anmelden, bevor Sie diese Funktion nutzen können. Nach der Registrierung befolgen Sie bitte diese Anweisungen.

1. Geben Sie in das Feld „Account / E-mail“ (1) (Konto / E-Mail) Ihren DynDNS.org-Benutzernamen ein.
2. Geben Sie in das Feld „Password / Key“ (2) (Kennwort / Schlüssel) Ihr DynDNS.org-Kennwort ein.
3. Geben Sie in das Feld „Domain Name“ (3) (Domänenname) den DynDNS.org-Domännennamen ein, den Sie mit DynDNS.org eingestellt haben.

Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um Ihre IP-Adresse zu aktualisieren.

Immer wenn Ihre IP-Adresse vom Provider verändert wird, wird der Router automatisch die Server von DynDNS.org mit der neuen IP-Adresse aktualisieren. Sie können dies auch manuell tun, indem Sie auf die Schaltfläche „Apply changes“ (4) (Änderungen übernehmen) klicken.

Auf der Seite Verbindungstyp können Sie den Verbindungstyp einstellen, den Sie verwenden wollen, indem Sie ihn in der Liste „Connection Type“ (Verbindungstyp) auswählen.

The screenshot shows the 'WAN > DDNS' configuration page. At the top, there is a descriptive paragraph: 'DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP address is dynamic. You must Register for DDNS service at one of the listed DDNS Services.' Below this, there are several controls: a 'DDNS Service >' dropdown menu currently set to 'Disable DDNS' with a 'Web Site' button next to it; a 'DDNS Status >' label; three input fields labeled (1) 'Account / E-mail >', (2) 'Password / Key >', and (3) 'Domain Name >'; and two buttons at the bottom: 'Clear changes' and 'Apply Changes', with the latter being pointed to by a line labeled (4).

Funknetz

Auf der Registerkarte „Wireless“ (Funknetz) können Sie die Einstellungen des kabellosen Netzwerks ändern. Sie können Änderungen am Namen des Funknetzwerks (SSID), am Betriebskanal und an der Sicherheitsverschlüsselung vornehmen.

Kanal und SSID

1. Ändern des Netzwerknamens (SSID)

Wireless > Channel and SSID

This page allows you to enter the Wireless Network Name (SSID in Wi-Fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as a wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. [More Info](#)

SSID >	<input type="text" value="Belkin54g"/>
ESSID Broadcast >	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode >	<input type="text" value="Mixed (11b+11g)"/>
Wireless Channel >	<input type="text" value="Auto"/>
<input type="button" value="Clear Changes"/> <input type="button" value="Apply Changes"/>	

Zur Kennzeichnung Ihres kabellosen Netzwerks dient die sogenannte SSID, der Netzwerkname. Sie können sie beliebig verändern oder die Vorgabe beibehalten. Werden weitere kabellose Netzwerke im Funkbereich betrieben, sollten Sie eine eindeutige SSID festlegen, also eine SSID, die von keinem anderen Netzwerk in der Nähe genutzt wird. Sie können die SSID ändern, indem Sie im Feld SSID die gewünschte SSID eingeben und auf „Apply Changes“ (Änderungen übernehmen) klicken. Die Änderung wird unmittelbar wirksam. Wenn Sie die SSID ändern, müssen Ihre kabellos vernetzten Computer ggf. an den neuen Netzwerknamen angepasst werden. Informationen zur Vornahme dieser Änderung finden Sie in der Dokumentation Ihres Netzwerkadapters.

2. Verwenden der Funktion Broadcast ESSID (ESSID senden)

Aus Sicherheitsgründen können Sie festlegen, dass die SSID Ihres Netzwerks nicht gesendet wird. Danach wird Ihr Netzwerk so verborgen, dass es über die Standortübersicht von anderen Computern nicht erkannt wird. Wenn Sie die Versendung der SSID deaktivieren möchten, klicken Sie auf „DISABLE“ (Deaktivieren) und dann auf „Apply Changes“ (Änderungen übernehmen). Die Änderung wird unmittelbar wirksam. Jeder Computer muss jetzt genau auf die SSID Ihres Netzwerks eingestellt werden. Die SSID-Einstellung „ANY“ (Beliebig) wird nicht mehr akzeptiert. Informationen zur Vornahme dieser Änderung finden Sie in der Dokumentation Ihres Netzwerkadapters.

Hinweis: Diese weiterführende Funktion sollte nur von erfahrenen Benutzern bedient werden.

3. Einstellen des Funkmodus

Ihr Router kann in drei verschiedenen Funkmodi betrieben werden: „Mixed (11b+11g)“ (Gemischt [11b+11g]), „11g Only“ (Nur 11g) und „11b Only“ (Nur 11b). Die verschiedenen Modi werden unten erläutert.

Modus „Gemischt (11b+11g)“

In diesem Modus ist der Router mit Clients der beiden Typen 802.11b und 802.11g kompatibel. Dieser Modus ist die Werkseinstellung; er sorgt für volle Kompatibilität mit allen WiFi-kompatiblen Geräten. Wenn sich in Ihrem Netzwerk sowohl 802.11b- als auch 802.11g-Clients befinden, empfehlen wir Ihnen, die Werkseinstellung nicht zu ändern. Diese Einstellung sollte nur geändert werden, wenn ein besonderer Grund dafür vorliegt.

Modus „Nur 11g“

Im Modus „Nur 802.11g“ sind nur 802.11g-Clients einsetzbar. Dieser Modus wird nur dann empfohlen, wenn Sie verhindern möchten, dass 802.11b-Clients auf Ihr Netzwerk zugreifen. Um zwischen Modi zu wechseln, wählen Sie den erforderlichen Modus im Drop-Downmenü „Wireless Mode“ (Funkmodus). Klicken Sie dann auf „Apply Changes“ (Änderungen übernehmen).

Modus „Nur 11b“

Wir empfehlen, diesen Modus NICHT zu verwenden, wenn nicht ein besonderer Grund dafür vorliegt. Dieser Modus dient nur der Lösung bestimmter Probleme, die mit einigen 802.11b-Clientadaptern auftreten können und ist für die Zusammenwirkung der 802.11g- und 802.11b-Standards nicht notwendig.

4. Wechseln des Funkkanals

Sie können einen von mehreren Betriebskanälen auswählen. In den USA stehen 11 Kanäle zur Auswahl, in Großbritannien und den meisten anderen europäischen Ländern 13 Kanäle. Bestimmte Länder haben abweichende Funkvorschriften. Der Router ist für den zulässigen Betrieb Ihres Landes konfiguriert. Der Standardname lautet „Auto“. Bei Bedarf können Sie den Kanal wechseln. Sind im Funkgebiet weitere kabellose Netzwerke in Betrieb, sollten Sie für Ihr Netzwerk einen Kanal wählen, der von diesen nicht genutzt wird. Wählen Sie am besten einen Kanal aus, der sich um mindestens fünf Kanalstufen von den anderen Netzwerken unterscheidet. Wenn zum Beispiel ein Netzwerk auf Kanal 11 betrieben wird, stellen Sie Ihr Netzwerk auf Kanal 6 oder einen niedrigeren Kanal ein. Sie wechseln den Kanal, indem Sie den Kanal in der Dropdown-Liste wählen. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen). Die Änderung wird unmittelbar wirksam.

Verschlüsselung/Sicherheit

Sicherung des Wi-Fi Netzwerks

Es folgen ein paar Möglichkeiten, mit denen Sie die Sicherheit Ihres kabellosen Netzwerks optimieren können und Ihre Daten vor unerwünschtem Zugriff schützen können. Dieses Kapitel richtet sich speziell an Benutzer, die Ihr Netzwerk privat oder in einem kleinen Unternehmen nutzen. Zum Zeitpunkt der Veröffentlichung gibt es vier Verschlüsselungsmethoden.

Name	64-Bit Wired Equivalent Privacy Verschlüsselung	128-Bit Wired Equivalent Privacy Verschlüsselung	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Akronym	64-Bit WEP	128-Bit WEP	WPA-TKIP/AES (oder nur WPA)	WPA2-AES (oder nur WPA2)
Sicherheit	Gut	Besser	Ausgezeichnet	Ausgezeichnet
Merkmale	Statische Schlüssel	Statische Schlüssel	Dynamische Verschlüsselung und gegenseitige Authentifizierung	Dynamische Verschlüsselung und gegenseitige Authentifizierung
	Verschlüsselung auf Basis von RC4 Algorithmus (normalerweise 40-Bit-Schlüssel)	Zusätzliche Sicherheit über 64-Bit-WEP unter Benutzung einer Schlüssellänge von 104 Bits, ergänzt durch weitere 24 Bits Daten, die das System erzeugt	Zugefügtes TKIP (Temporal Key Integrity Protocol), damit Schlüssel rotieren und die Verschlüsselung verstärkt wird	AES (Advanced Encryption Standard) verursacht keinen Durchsatzverlust

Wired Equivalent Privacy (WEP)

WEP ist ein verbreitetes Protokoll, das allen Wi-Fi-kompatiblen Geräten für kabellose Netzwerke Sicherheit verleiht. WEP schützt Daten in kabellosen Netzwerken auf einem Niveau, das mit verkabelten Netzwerken vergleichbar ist.

64-Bit-WEP

64-Bit-WEP wurde mit 64-Bit-Verschlüsselung eingeführt, die aus einer Schlüssellänge von 40 Bits und 24 weiteren Bits an Daten, die vom System erzeugt werden, besteht (insgesamt 64 Bits). Manche Hardwarehersteller bezeichnen 64-Bit als 40-Bit-Verschlüsselung. Kurz nachdem die Technologie eingeführt worden war, haben Fachleute festgestellt, dass die 64-Bit-Verschlüsselung zu einfach zu entschlüsseln war.

128-Bit-WEP

Aufgrund der möglichen Sicherheitsschwächen wurde mit 128-Bit-Verschlüsselung eine sicherere Methode entwickelt. 128-Bit-Verschlüsselung basiert auf einer Schlüssellänge von 104 Bits und 24 weiteren Bits, die durch das System erzeugt werden (insgesamt 128 Bits). Manche Hardwarehersteller bezeichnen 128-Bit als 104-Bit-Verschlüsselung. Die meisten neueren Geräte für kabellose Netzwerke, die heutzutage auf dem Markt sind, unterstützen sowohl 64-Bit als auch 128-Bit-WEP-Verschlüsselung. Vielleicht haben Sie aber ältere Geräte, die nur 64-Bit-WEP unterstützen. Alle Produkte für kabellose Netzwerke von Belkin unterstützen sowohl 64-Bit- als auch 128-Bit-WEP.

Verschlüsselungsschlüssel

Nachdem Sie sich entweder für den 64-Bit- oder den 128-Bit-WEP-Verschlüsselungsmodus entschieden haben, müssen Sie einen Schlüssel erzeugen. Wenn der Verschlüsselungsschlüssel nicht überall im kabellosen Netzwerk einheitlich ist, können Ihre Geräte für kabellose Netzwerke nicht miteinander kommunizieren. Auch kann keine Kommunikation mit anderen Netzwerken erfolgen. Sie können Ihren Schlüssel eingeben, indem Sie den Hexadezimalschlüssel manuell eintragen oder Sie können eine Passphrase (Kennfolge) im „Passphrase“ Feld eintragen und „Generate“ (Erzeugen) klicken, um einen Schlüssel zu erstellen. Ein Hex (Hexadezimalschlüssel) ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0–9. Für 64-Bit-WEP müssen Sie 10 Hexzeichen eingeben. Für 128-Bit-WEP müssen Sie 26 Hexzeichen eingeben.

Beispiel:

AF 0F 4B C3 D4 = 64-Bit-WEP-Schlüssel

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-Bit-WEP-Schlüssel

Die WEP-Kennfolge ist NICHT dasselbe wie ein WEP-Schlüssel. Ihre kabellose Netzwerkkarte benutzt diese Passphrase, um Ihre WEP-Schlüssel zu bilden, aber andere Hardwarehersteller verwenden möglicherweise andere Erstellungsmethoden. Wenn Sie für Ihr Netzwerk Geräte von verschiedenen Herstellern benutzen, sollten Sie der Einfachheit halber den Hex-WEP-Schlüssel Ihres kabellosen Routers oder Access Points benutzen und ihn manuell in die Hex-WEP-Schlüssel Tabelle im Konfigurationsbildschirm Ihrer kabellosen Netzwerkkarte eingeben.

Wi-Fi Protected Access (WPA)

WPA ist ein neuer Wi-Fi-Standard, der entwickelt wurde, um die Sicherheitsstandards von WEP zu übertreffen. Wenn Sie WPA-Sicherheit nutzen wollen, müssen die Treiber und die Software Ihrer Geräte für kabellose Netzwerke entsprechend aufgerüstet sein. Die Aktualisierungen können Sie auf der Website Ihres Händlers finden. Es gibt zwei Arten von WPA-Sicherheitseinstellungen: WPA-PSK (kein Server) und WPA (mit 802.1x Radius-Server).

WPA-PSK (kein Server)

WPA-PSK verwendet einen sogenannten „Pre-shared Key (PSK)“ als Sicherheitsschlüssel. Ein Netzwerkschlüssel ist ein Kennwort, das zwischen acht und 63 Zeichen lang ist. Es kann aus einer Kombination aus Buchstaben, Ziffern oder Sonderzeichen bestehen. Jeder Client verwendet denselben Netzwerkschlüssel, um auf das Netzwerk zuzugreifen. Normalerweise ist dies der Modus, der in einem Heimnetzwerk verwendet wird.

WPA (Mit 802.1x Radius-Server)

In diesem System verteilt der Radius-Server die Netzwerkschlüssel automatisch an die Clients. Diese Technik wird häufig in Firmen eingesetzt.

WPA2

Der Router verwendet WPA2. Dies ist die zweite Generation des auf WPA basierenden 802.11i-Standards. Diese Methode bietet höhere Sicherheit im kabellosen Netzwerk, da eine komplexe Netzwerkauthentifizierung und stärkere AES-Verschlüsselungsmethoden verwendet werden.

WPA2-Anforderungen

WICHTIGER HINWEIS: Wenn Sie die WPA2-Sicherheitsfunktion verwenden wollen, müssen alle verwendeten Computer und Adapter kabelloser Clients mit aktualisierten Patches, Treibern und aktualisierter Software des Client-Dienstprogramms ausgestattet sein, die WPA2 unterstützen. Zum Zeitpunkt der Erstellung dieses Benutzerhandbuchs sind kostenlose Sicherheitspatches von Microsoft® als Download erhältlich. Diese Patches gelten nur für das Betriebssystem Windows XP. Andere Betriebssysteme können zur Zeit nicht unterstützt werden.

Für Windows XP Computer, die nicht mit Service Pack 2 (SP2) ausgestattet sind, ist eine Datei von Microsoft mit dem Namen „Windows XP Support Patch for Wireless Protected Access (KB 826942)“ als kostenloser Download erhältlich. Sie finden Sie unter: <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91>.

Für Windows XP mit Service Pack 2 stellt Microsoft einen kostenlosen Download zur Verfügung, mit welchem Sie die Komponenten der kabellosen Clients so aktualisieren können, dass Sie WPA2 (KB893357) unterstützen. Die Aktualisierung steht Ihnen unter folgender Adresse zur Verfügung: <http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en>.

WICHTIGER HINWEIS: All Ihre Netzwerkkarten/Adapter kabelloser Clients müssen WPA2 unterstützen und entsprechend über die neuesten Treiber verfügen. Aktualisierungen von Treibern der meisten kabellosen Netzwerkkarten von Belkin finden Sie auf der Support-Site von Belkin: www.belkin.com/networking. Eine Liste von Belkin-Produkten, die WPA/WPA2 unterstützen, finden Sie auf unserer Website unter www.belkin.com/networking.

Gemeinsame Nutzung von Netzwerkschlüsseln

Die meisten Wi-Fi Produkte werden mit deaktivierter Sicherheitsfunktion geliefert. Sobald Ihr Netzwerk in Betrieb ist, müssen Sie WEP oder WPA aktivieren und sicherstellen, dass die Geräte ihres kabellosen Netzwerks denselben Netzwerkschlüssel verwenden.

Verwenden eines Hexadezimalschlüssels

Ein Hexadezimalschlüssel ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0-9. 64-Bit-Schlüssel bestehen aus fünf zweistelligen Zahlen. 128-Bit-Schlüssel sind 13 zweistellige Zahlen.

Beispiel:

AF 0F 4B C3 D4 = 64-Bit-Schlüssel

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-Bit-Schlüssel

Legen Sie in den Feldern unten Ihren Schlüssel fest, indem Sie jeweils zwei Zeichen zwischen A-F und 0-9 eingeben. Mit diesem Schlüssel programmieren Sie später die Verschlüsselungseinstellungen in Ihrem Router und den kabellos vernetzten Computern.

Hinweis an Mac-Benutzer: AirPort®-Produkte von Apple unterstützen in der Original-Ausführung nur Verschlüsselung mit 64 Bit. Apple AirPort 2-Produkte unterstützen sowohl 64-Bit- als auch 128-Bit-Verschlüsselung. Bitte prüfen Sie, welche Version Ihr Produkt nutzt. Wenn Sie Ihr Netzwerk nicht mit 128 Bit verschlüsseln können, sollten Sie es mit der 64-Bit-Verschlüsselung probieren.

WEP-Einstellung

1. Wählen Sie im Dropdown-Menü die Option „WEP“.

Wählen Sie „WEP Mode“ (WEP-Modus) mit 64- oder 128-Bit

3. Nachdem Sie die WEP-Methode gewählt haben, können Sie den Schlüssel eingeben, indem Sie den Hexadezimalschlüssel manuell eintragen.

Ein Hexadezimalschlüssel ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0–9. Für 64-Bit-WEP müssen Sie 10 Hexadezimalschlüssel eingeben. Für 128-Bit-WEP müssen Sie 26 Hexzeichen eingeben.

Beispiel:

AF 0F 4B C3 D4 = 64-Bit-Schlüssel

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-Bit-Schlüssel

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	WEP
WEP Mode >	<input checked="" type="radio"/> 64 bit <input type="radio"/> 128 bit
Key Entry Method >	<input type="radio"/> HEX <input checked="" type="radio"/> ASCII
Key Provisioning >	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Key 1 >	<input type="text"/>
Key 2 >	<input type="text"/>
Key 3 >	<input type="text"/>
Key 4 >	<input type="text"/>
Default Key ID >	1
Password >	<input type="checkbox"/> <input type="text"/>

3. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um abzuschließen. Jetzt ist die Verschlüsselung im Router eingestellt. Jeder Computer in Ihrem kabellosen Netzwerk muss jetzt mit denselben Sicherheitseinstellungen konfiguriert werden.

ACHTUNG: Wenn Sie für die Einstellung des kabellosen Routers einen Computer mit kabellosem Client verwenden, vergewissern Sie sich, dass die Sicherheitsfunktion für diesen kabellosen Client aktiviert ist. Falls dies nicht der Fall ist, wird die Funkverbindung unterbrochen.

Änderungen der Sicherheitseinstellungen des Funknetzwerks

Ihr Router ist mit WPA/WPA2 ausgestattet. Er unterstützt auch den älteren WEP-Sicherheitsstandard. Werkseitig ist die Sicherheitsfunktion deaktiviert. Um diese zu aktivieren, müssen Sie zuerst festlegen, welchen Standard Sie verwenden möchten. Um die Sicherheitseinstellungen zu bearbeiten, klicken Sie auf der Registerkarte „Wireless“ (Funknetz) auf „Security“ (Sicherheit).

WPA-Einstellung

Hinweis: Um die WPA-Sicherheitsfunktion zu verwenden, müssen alle Ihre Clients über aktuelle Software und Treiber verfügen, die WPA unterstützen. Zum Zeitpunkt der Erstellung dieses Benutzerhandbuchs ist von Microsoft ein kostenloses Sicherheitspatch als Download erhältlich. Dieses Patch gilt nur für das Betriebssystem Windows XP. Sie benötigen auch die aktuellen Treiber von Belkin für Ihre Kabellose G Notebook-Karte. Diese finden Sie auf der Support-Website von Belkin. Andere Betriebssysteme können zur Zeit nicht unterstützt werden. Das Patch von Microsoft unterstützt nur Geräte mit WPA-aktivierten Treibern, wie die 802.11g-Produkte von Belkin.

Es gibt zwei Arten von WPA-Sicherheitseinstellungen: WPA-PSK (kein Server) und WPA (mit Radius-Server). WPA-PSK (kein Server) verwendet sogenannte pre-shared Schlüssel (PSK) zur Sicherheitskodierung. Ein pre-shared Schlüssel ist ein Kennwort, das zwischen acht und 63 Zeichen lang ist. Es kann aus einer Kombination aus Buchstaben, Ziffern und anderen Zeichen bestehen. Jeder Client verwendet denselben Schlüssel, um auf das Netzwerk zuzugreifen. Normalerweise ist dies der Modus, der in einem Netzwerk zu Hause verwendet wird. WPA (mit Radius-Server) ist ein System, in dem ein Radius-Server die Schlüssel an die Clients automatisch verteilt. Diese Technik wird typischerweise in einer Unternehmensumgebung eingesetzt. WPA2 ist die zweite Generation von WPA und bietet eine komplexere Verschlüsselungstechnik als WPA.

Einstellen von WPA-PSK (kein Server)

1. Wählen Sie im Dropdown-Menü „Allowed Client Type“ (Erlaubter Client-Typ) „WPA/WPA2“.
2. Wählen Sie zur Authentifizierung bei Heim-/SOHO-Netzwerken „Pre-shared Key“. Diese Einstellungen müssen mit denen Ihrer Clients übereinstimmen.
3. Geben Sie Ihren Pre-Shared Key (PSK) ein. Er kann aus acht bis 63 Zeichen (Buchstaben, Ziffern, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >

Authentication > 802.1X Pre-shared Key

Pre-shared Key >

für alle Clients verwenden, die Sie einrichten. Ihr PSK kann zum Beispiel heißen: „Familie Simpsons Netzwerkschlüssel“.

4. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients entsprechend einstellen

Einstellen von WPA/WPA2 (mit Radius-Server)

Wenn Sie in Ihrem Netzwerk einen Radius-Server verwenden, um die Schlüssel an die Clients zu verteilen, verwenden Sie diese Einstellung.

1. Wählen Sie im Dropdown-Menü „Allowed Client Type“ (Erlaubter Client-Typ) „WPA/WPA2“.
2. Wählen Sie in Umgebungen mit Radiusserver „802.1x“ als Verschlüsselungsmethode. Diese Einstellungen müssen mit denen Ihrer Clients übereinstimmen.
3. Geben Sie das Passivitätslimit der Sitzung des Radiusservers im Feld „Session Idle Timeout“ (Passivitätslimit der Sitzung) ein.
4. Geben Sie im Feld „Re-Authentication Period“ (Neu-Authentifizierungszeitraum) das Schlüsselintervall ein, in welchem die Schlüssel verteilt werden sollen (in Paketen).
5. Geben Sie im Feld „Quiet Period“ (Ruhephase) die Wartezeit nach einem fehlgeschlagenen Authentifizierungsversuch ein.
6. Geben Sie die IP-Adresse und Schnittstellenummer des Radius-Servers in die Felder „Server-IP“ bzw. „Server-Port“ ein.
7. Geben Sie den Radius-Schlüssel in das Feld „Radius Key“ (Radius-Schlüssel) ein.
8. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients entsprechend einstellen.

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. More Info

Allowed Client Type >	<input type="text" value="WPAWPA2"/>
Authentication >	<input checked="" type="radio"/> 802.1X <input type="radio"/> Pre-shared Key
Session Idle Timeout >	<input type="text" value="300"/> Seconds (0 for no timeout checking)
Re-Authentication Period >	<input type="text" value="3800"/> Seconds (0 for no re-authentication)
Quiet Period >	<input type="text" value="60"/> Seconds after authentication failed
Server-IP >	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="2"/> <input type="text" value="1"/>
Server-Port >	<input type="text" value="1812"/>
Secret Key >	<input type="text"/>
NAS-ID >	<input type="text"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Clear Changes"/>	

Hinweis: Stellen Sie sicher, dass die Computer Ihres kabellosen Netzwerks über die Aktualisierungen verfügen, die für die Verwendung von WPA2 erforderlich sind, und dass die Einstellungen eine korrekte Verbindung mit dem Router zulassen.

Einstellen der Sicherheitsfunktion bei Kabellosen G Netzwerkarten von Belkin

Hinweis: In diesem Abschnitt finden Sie Informationen zum Konfigurieren Ihrer Kabellosen G Netzwerkarten von Belkin. An dieser Stelle sollten Sie Ihren kabellosen Router oder Access Point bereits auf die Verwendung von WPA oder WEP eingestellt haben. Für eine kabellose Verbindung müssen Sie Ihre kabellose Notebook- oder Desktop-Karte auf die gleiche Sicherheitsstufe einstellen.

Einbindung Ihres Computers in ein kabelloses Netzwerk, das einen 64-Bit- oder 128-Bit WEP-Schlüssel erfordert

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network“ (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen. Mit der Schaltfläche „Advanced“ (Weitere Optionen) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
2. Wählen Sie auf der Registerkarte „Wireless Network Properties“ (Netzwerkeigenschaften) einen Netzwerknamen in der Liste „Available networks“ (Verfügbare Netzwerke) aus und klicken Sie auf „Properties“ (Eigenschaften).
3. Wählen Sie bei „Data Encryption“ (Datenverschlüsselung) „WEP“.
4. Das untere Feld „Network key is provided for me automatically“ (Netzwerkschlüssel wird automatisch vergeben) darf nicht aktiviert sein. Wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk herzustellen, fragen Sie sich bitte Ihren Netzwerkadministrator, ob dieses Feld aktiviert werden muss.
5. Geben Sie Ihren WEP-Schlüssel in das Feld „Network Key“ (Netzwerkschlüssel) ein.

Wireless > Security

Security Mode

Key 1

Key 2

Key 3

Key 4

(hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, input it here

PassPhrase

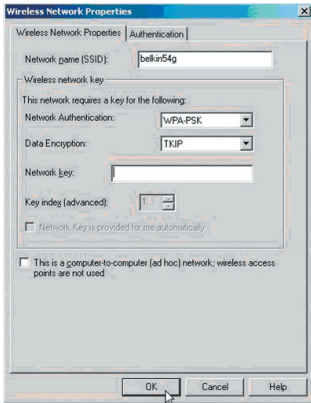
Wichtiger Hinweis: Ein WEP-Schlüssel ist eine Kombination aus Zahlen und Buchstaben von A-F und 0-9. Für 128-Bit WEP müssen Sie 26 Schlüssel eingeben. Für 64-Bit-WEP müssen Sie zehn Schlüssel eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres Routers übereinstimmen.

6. Klicken Sie auf „OK“, um die Einstellungen zu speichern.

Einbindung Ihres Computers in ein kabelloses Netzwerk, das einen WPA-PSK (kein Server) erfordert.

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network“ (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen. Mit der Schaltfläche „Advanced“ (Erweitert) können Sie zusätzliche Optionen für Ihre kabellose Karte überprüfen und einstellen.
2. Wählen Sie auf der Registerkarte „Wireless Network“ (Kabelloses Netzwerk) einen Netzwerknamen in der Liste „Available networks“ (Verfügbare Netzwerke) aus und klicken Sie auf „Configure“ (Konfigurieren).
3. Wählen Sie unter „Network Authentication“ (Netzwerk-Authentifizierung) den Eintrag „WPA-PSK (No Server)“ (WPA-PSK [Kein Server]) aus.
4. Geben Sie Ihren WPA-Schlüssel in das Feld „Network Key“ (Netzwerkschlüssel) ein.

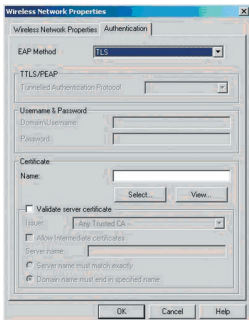
Wichtiger Hinweis: Ein WPA-PSK ist eine Kombination aus Zahlen und Buchstaben von A-Z und 0-9. Für WPA-PSK können Sie acht bis 63 Zeichen eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres Routers übereinstimmen.



5. Klicken Sie auf „OK“, um die Einstellungen zu speichern.

Verbinden Sie Ihren Computer mit einem kabellosen Netzwerk, das WPA (mit Radius-Server) erfordert.

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network“ (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen. Mit der Schaltfläche „Advanced“ (Erweitert) können Sie zusätzliche Optionen für Ihre kabellose Karte überprüfen und einstellen.
2. Wählen Sie auf der Registerkarte „Wireless Network“ (Kabelloses Netzwerk) einen Netzwerknamen in der Liste „Available networks“ (Verfügbare Netzwerke) aus und klicken Sie auf „Configure“ (Konfigurieren).
3. Wählen Sie unter „Network Authentication“ (Netzwerk-Authentifizierung) den Eintrag „WPA“ aus.
4. Wählen Sie auf der Registerkarte „Authentication“ (Authentifizierung) die Einstellungen, die Sie vom Netzwerkadministrator erhalten haben.



5. Klicken Sie auf „OK“, um die Einstellungen zu speichern.

WPA für kabellose Desktop- und Notebook-Karten, die NICHT von Belkin hergestellt wurden, einstellen

Für kabellose Desktop- und Notebook-Karten von Drittanbietern, die nicht mit WPA-Software ausgestattet sind, kann ein Sicherheitspatch von Microsoft mit dem Namen „Windows XP Support Patch for Wireless Protected Access“ kostenlos heruntergeladen werden.

Hinweis: Dieses von Microsoft zur Verfügung gestellte Patch gilt nur für das Betriebssystem Windows XP. Andere Betriebssysteme können zur Zeit nicht unterstützt werden.

Wichtiger Hinweis: Sie müssen auch überprüfen, ob der Hersteller der kabellosen Karte WPA unterstützt und Sie die aktuellsten Treiber heruntergeladen und installiert haben.

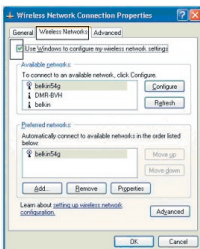
Unterstützte Betriebssysteme:

- Windows XP Professional
- Windows XP Home Edition

Das Netzwerkprogramm „Windows XP Wireless Network Utility“ für WPA-PSK einstellen

Um WPA-PSK einsetzen zu können, müssen Sie das Windows Wireless Network Utility (Kabelloses Netzwerkprogramm) verwenden. Gehen Sie dazu folgendermaßen vor:

1. Unter Windows XP, klicken Sie auf „Start > Systemsteuerung > Netzwerkverbindungen“.
2. Klicken Sie mit der rechten Maustaste auf „Drahtlose Netzwerkverbindung“ (Wireless Network Connection) und wählen Sie „Eigenschaften“.
3. Klicken Sie mit der rechten Maustaste auf „Drahtlose Netzwerke“ (Wireless Networks). Das folgende Fenster wird angezeigt. Vergewissern Sie sich, dass das Kontrollkästchen „Use Windows to configure my wireless network settings“ (Windows zum Konfigurieren der Einstellungen des drahtlosen Netzwerks benutzen) markiert ist.
4. Klicken Sie auf der Registerkarte „Wireless Networks“ (Drahtlose Netzwerke) auf die Schaltfläche „Configure“ (Konfigurieren). Das folgende Fenster wird angezeigt.



5. Nutzer von Heim- oder kleinen Unternehmensnetzwerken wählen „WPA-PSK“ unter „Network Authentication“ (Netzwerkauthentifizierung).

Hinweis: Wählen Sie „WPA“ aus, wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk herzustellen, in welchem ein Authentifizierungsserver, z.B. ein Radius-Server, verwendet wird. Wenden Sie sich für weitere Informationen an Ihren Netzwerkadministrator.



6. Wählen Sie unter „Data Encryption“ (Datenverschlüsselung) „TKIP“ oder „AES“. Diese Einstellung muss genau mit der Einstellung Ihres Routers übereinstimmen.

7. Geben Sie Ihren Verschlüsselungsschlüssel in das Feld „Network Key“ (Netzwerkschlüssel) ein.

Wichtiger Hinweis: Geben Sie Ihren Pre-Shared Key (PSK) ein. Er kann aus acht bis 63 Zeichen (Buchstaben, Ziffern, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten.

8. Klicken Sie auf „OK“, um die Einstellungen zu übernehmen.

Kabellose Bereichserweiterung und Bridging

Was ist eine Kabellose Bridge?

Eine Kabellose Bridge ist ein Betriebsmodus, mit welchem Sie die Reichweite Ihres kabellosen Netzwerks vergrößern können. Ebenso können Sie ein vorhandenes Netzwerk in einen anderen Bereich Ihres Büros oder Hauses ausdehnen, ohne hierzu Kabel zu verlegen.

Hinweis: Wir können nicht garantieren, dass diese Funktion bei der Verwendung von Hardware anderer Hersteller kabelloser Netzwerkprodukte einsetzbar ist.

Hinweis: Damit Sie die optimale Leistung erzielen können, steht Ihnen die neueste Version der Firmware für den Router unter folgender Adresse als Download zur Verfügung: <http://web.belkin.com/support>.

Erweitern des kabellosen Netzwerks

Wenn Sie einen Netzwerk-Switch oder -Hub an die RJ45-Buchse des Routers anschließen, können Sie mehrere Computer mit ihm verbinden und auf diese Weise in das restliche Netzwerk einbinden.

Einrichten einer Bridge zwischen dem kabellosen Router und einem sekundären Access Point

Für das Bridging des Belkin Routers mit dem sekundären Access Point müssen Sie das Erweiterte Konfigurationsprogramm des Routers öffnen und die MAC-Adresse des Access Points eintragen. Zudem müssen Sie einige Gesichtspunkte beachten:

BITTE GEHEN SIE SORGFÄLTIG NACH FOLGENDEN SCHRITTEN VOR.

1. Stellen Sie am Access Point und am Router jeweils denselben Funkkanal ein. Weitere Informationen über die Änderung von Kanälen finden im Abschnitt „Funknetz - Kanal und SSID“ in diesem Benutzerhandbuch.
2. Suchen Sie die MAC-Adresse des Access Points an der Unterseite des Geräts. Beachten Sie, dass dort zwei MAC-Adressen vermerkt sind. Sie benötigen die MAC-Adresse, die mit „WLAN MAC Address“ gekennzeichnet ist. Sie beginnt mit „0030BD“, gefolgt von sechs weiteren Ziffern oder Buchstaben (z. B. 0030BD-XXXXXX). Schreiben Sie die MAC-Adresse in das untenstehende Feld. Fahren Sie mit dem nächsten Schritt fort.
3. Stellen Sie den sekundären Access Point innerhalb der Reichweite des Routers in dem Bereich auf, in den Sie das Netzwerk ausdehnen möchten. Die Reichweite in Innenräumen beträgt meist zwischen 30 und 60 m.
4. Schließen Sie den Access Point an das Stromnetz an. Schalten Sie den Access Point ein, und fahren Sie mit dem nächsten Schritt fort.
5. Öffnen Sie an einem Computer, der bereits mit dem Router verbunden ist, das Erweiterte Konfigurationsprogramm. Öffnen Sie hierzu Ihren Browser. Geben Sie in die Adresszeile 192.168.2.1 ein. Lassen Sie alle weiteren Angaben wie http:// und www weg. Hinweis: Wenn Sie die IP-Adresse Ihres Routers geändert haben, verwenden Sie die aktuelle Adresse.
6. Im Browser wird die Router-Benutzeroberfläche angezeigt. Klicken Sie links im Fenster (2) auf „Wireless Bridge“ (Funkbrücke). Daraufhin erscheint das folgende Fenster.
7. Aktivieren Sie die Option „Enable ONLY specific Access Points to connect“ (Nur mit BESTIMMTEN Access Points kann eine Verbindung hergestellt werden.) (1).

Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

(1) Enable Wireless Bridging. (enabling this feature allows other Access Points to connect to this Access Point.)

(3) Enable ONLY specific Access Points to connect. (enter Wireless MAC Address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Hint: the MAC address can be found using a site survey on a wireless client card.)

AP1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Disable ability for Wireless CLIENT to connect. (This feature should only be used when the AP is used exclusively to other APs.)

8. Geben Sie in das Feld „AP1 (3)“ die MAC-Adresse des sekundären Access Point ein. Klicken Sie nach der Eingabe der Adresse auf „Apply Changes“ (Änderungen übernehmen).

9. Das Bridging ist jetzt eingerichtet.

Hinweis: Die Herstellung der Bridge-Verbindung kann eine Minute in Anspruch nehmen. Möglicherweise müssen Sie den Access Point und den Router neu starten, um die Bridge zu aktivieren.

Firewall

Ihr Router verfügt über eine Firewall, die Ihr Netzwerk vor zahlreichen Hacker-Angriffen schützt:

- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP mit Nulllänge
- Smurf Attack
- TCP Null Scan
- SYN Flood
- UDP Flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment-Flooding

Außerdem verdeckt die Firewall Ports, die oft zu Angriffen auf Netzwerke missbraucht werden. Diese Ports werden so abgeschirmt, dass sie für potentielle Hacker nicht sichtbar sind. Sie können die Firewall-Funktion bei Bedarf deaktivieren. Es wird jedoch empfohlen, die Firewall aktiv zu lassen. Wenn Sie den Firewall-Schutz deaktivieren, ist Ihr Netzwerk Angriffen nicht völlig schutzlos ausgeliefert; die Gefahr unbefugter Eingriffe wächst jedoch.

Firewall >

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable / Disable > Enable Disable

Clear Changes

Apply Changes

Virtuelle Server

Mit der Funktion „Virtual Servers“ (Virtuelle Server) können Sie externe Anrufe (aus dem Internet) von Diensten wie Webserver (Port 80), FTP-Server (Port 21) oder anderen Anwendungen über Ihren Router in Ihr internes Netzwerk umleiten. Da Ihre internen Computer durch eine Firewall geschützt sind, kann auf diese aus dem Internet nicht zugegriffen werden, weil sie dort nicht „sichtbar“ sind. Wenn Sie die virtuelle Serverfunktion für eine bestimmte Anwendung einstellen müssen, sollten Sie Kontakt zum Hersteller des Programms aufnehmen, um dort zu erfahren, welche Port-Einstellungen Sie vornehmen müssen. Sie können die Port-Informationen dann manuell eingeben.

Firewall > Virtual Servers

This function will allow you to make external (Internet) calls for services such as a web server (port 80), FTP server (port 21), or other applications through your Router to your internal network. Note: Info

ID	Use IP Address	Description	Protocol Type	Port Range	Status
1			TCP		Off
2			TCP		Off
3			TCP		Off

Auswählen einer Anwendung

Wählen Sie die Anwendung in der Dropdown-Liste aus. Klicken Sie auf „Add“ (Hinzufügen). Die Einstellungen werden in das nächste freie Feld im Fenster eingetragen. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Einstellungen für diese Anwendung zu sichern. Sie können eine Anwendung entfernen, indem Sie die entsprechende Zeile markieren und auf „Clear“ (Löschen) klicken.

Manuelle Eingabe von Einstellungen in den virtuellen Server

Um Einstellungen manuell einzugeben, tragen Sie die IP-Adresse in das Feld für den internen Server ein, dann die Ports, die freigegeben werden müssen und den Port-Typ (TCP oder UDP); klicken Sie dann auf „Apply Changes“ (Änderungen übernehmen). Jeder eingehende Port verfügt über zwei Felder mit maximal fünf Zeichen pro Feld. So kann ein Start- und Endpunkt des Port-Bereichs festgelegt werden ([xxxxx]-[xxxxx]). Für jeden Eintrag können Sie einen Port-Wert eingeben, indem Sie in die beiden Felder denselben Wert eingeben (z. B. [7500]-[7500]) oder einen weiten Port-Bereich (z. B. [7500]-[9000]). Wenn Sie mehrere Einzelport-Werte oder eine Kombination aus Bereichen und Einzelwerten benötigen, müssen Sie bis zur maximalen Anzahl von 20 Einträgen mehrere vornehmen (z. B. 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). Sie können pro interner IP-Adresse nur einen Port freigeben. Das Öffnen von Ports in Ihrer Firewall kann ein Sicherheitsrisiko darstellen. Das Aktivieren und Deaktivieren von Einstellungen geht schnell von der Hand. Daher sollten Sie die Einstellungen deaktivieren, wenn Sie eine bestimmte Anwendung momentan nicht verwenden.

Client-IP-Filter

Sie können den Router so einstellen, dass der Zugriff auf das Internet, E-Mail oder andere Netzwerke auf bestimmte Tage und Zeiten beschränkt wird. Die Beschränkung kann für einen einzelnen oder mehrere Computer festgelegt werden.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

Access Control allows users to define the traffic type permitted or not-permitted to WAN port services. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function > Enable Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Active Filtering Rule !!!				

> Add PC

Apply Changes

Zugriffskontrolle

Über die Zugriffskontrolle (Access Control) können Anwender festlegen, ob der ausgehende Datenverkehr über die WAN-Schnittstelle zugelassen oder nicht zugelassen wird. Voreingestellt ist das Zulassen des ausgehenden Datenverkehrs. Um Ihre Computer für beschränkten Zugriff zu konfigurieren, gehen Sie wie folgt vor:

1. Klicken Sie unter „Address Control“ (Adressenkontrolle) auf „Add PC“ (PC hinzufügen).
2. Legen Sie die entsprechenden Einstellungen für die Dienste der Client-PCs fest (wie in der folgenden Abbildung dargestellt).
3. Klicken Sie auf „OK“ und anschließend auf „Apply Changes“ (Änderungen übernehmen), um die Einstellungen zu speichern.

Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule settings. After the scheduling function, users can configure the client address list on the "Schedule Rule" page. For the scheduling function, you also need to configure the scheduler rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address >

> Client PC Service

Service Name	Detail Description	Enable
WWW	HTTP, TCP, Protocol, 80, 8080, 8081, 8082	<input checked="" type="checkbox"/>
WWW with URL Blocking	HTTP, TCP, 80, Blocking, 8080, 8081, 8082	<input checked="" type="checkbox"/>
Client Control	SMTP, TCP, 25, 587	<input checked="" type="checkbox"/>
Mail Access	SMTP, TCP, 25, 587	<input checked="" type="checkbox"/>
Client Filtering	SMTP, TCP, 25, 587	<input checked="" type="checkbox"/>
Service FTP	HTTP, TCP, 21, 20	<input checked="" type="checkbox"/>
Mail Transfer	POP, TCP, 110, 143	<input checked="" type="checkbox"/>
Mail Exchange	TCP, 25, 110, 143	<input checked="" type="checkbox"/>
Client Control	TCP, 25, 110, 143	<input checked="" type="checkbox"/>

URL-Blockierung

Verwenden Sie zur Konfiguration der URL-Blockierfunktion die nachstehende Tabelle, um die Websites festzulegen (www.eineseite.de) und/oder die Schlüsselwörter zu bestimmen, die Sie in Ihrem Netzwerk herausfiltern möchten. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Änderung zu aktivieren. Um diese Konfiguration zu beenden, müssen Sie eine Zugriffsregel im Abschnitt „Client-IP-Filter“ erstellen oder bearbeiten. Um eine bestehende Regel zu bearbeiten, klicken Sie neben der Regel auf „Edit“ (Bearbeiten). Um eine neue Regel zu erstellen, klicken Sie auf die Option „Add PC“ (PC hinzufügen). Aktivieren Sie in der Dienstabelle der Client-PCs im Abschnitt „Access Control > Add PC“ (Zugriffskontrolle > PC hinzufügen) die Option für „WWW with URL Blocking“ (WWW mit URL-Blockierung), um die ausgewählten Internetseiten und Schlüsselwörter herauszufiltern.

Manuelle Konfiguration des Routers

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. More Info.

To configure the URL Blocking feature, use the table below to specify the websites (www.somewebsite.com) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section. To modify an existing rule, click the "Edit" option next to the rule you want to modify. To create a new rule, click on the "Add PC" option.

From the "Access Control Add PC" section check the option for "Filter with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below.

Rule Number	URL / Keyword
Rule 1	
Rule 2	
Rule 3	
Rule 4	
Rule 5	

Zeitplanregel

Sie können den Internetzugang für lokale Clients durch Regeln festlegen. Jede Zugriffsregel kann zu einem festgelegten Zeitpunkt aktiviert werden. Definieren Sie die Zeitplanregel im Fenster „Schedule Rule“ (Zeitplanregel erstellen) und fügen Sie die Regel auf der Seite „Access Control“ (Zugriffskontrolle) hinzu.

Folgen Sie diesen Schritten, um eine Zeitplanregel hinzuzufügen:

1. Klicken Sie auf „Add Schedule Rule“ (Zeitplanregel hinzufügen).

2. Daraufhin erscheint das folgende Fenster.

3. Um die Zeitplanregel einzustellen, geben Sie den Namen, eine Beschreibung und die Beginn- und Endzeit an, in der Ihr Netzwerk gefiltert werden soll.

4. Klicken Sie auf „OK“ und anschließend auf „Apply Changes“ (Änderungen übernehmen), um die Einstellungen zu speichern.

5. Um diese Konfiguration zu beenden, müssen Sie eine Zugriffsregel im Abschnitt „Client-IP-Filter“ erstellen oder bearbeiten. Dadurch wird die Zeitplanregel für die Verwendung auf der Seite „Access Control“ (Zugriffskontrolle) aktiviert.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. More Info.

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Rule Name	Rule Comment	Configure
No Valid Schedule Rule !!!		
> Add Schedule Rule		

Clear Changes Apply Changes

Manuelle Konfiguration des Routers

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** [More Info](#)

DMZ > ENABLE DISABLE

> IP Address of Virtual DMZ Host

Static IP	Static IP
1	192.168.2.0
2	192.168.2.0
3	192.168.2.0
4	192.168.2.0
5	192.168.2.0
6	192.168.2.0
7	192.168.2.0
8	192.168.2.0

Um einen Computer in den DMZ-Status zu versetzen, geben Sie die letzten Ziffern seiner IP-Adresse in das IP-Feld ein und wählen „Enable“ (Aktivieren). Klicken Sie auf „Apply changes“ (Änderungen übernehmen), um die Änderung in Kraft zu setzen. Wenn Sie mehrere statische WAN-IP-Adressen verwenden, können Sie die IP-Adresse festlegen, zu der der DMZ-Host umgeleitet wird. Geben Sie die WAN-IP-Adresse ein, zu der der DMZ-Host umgeleitet werden soll, geben Sie die beiden letzten Ziffern der IP-Adresse des DMZ-Host-Computers ein, wählen Sie „Enable“ (Aktivieren) und klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Blockieren von ICMP-Pings

Computerhacker bedienen sich sogenannter Pings, um potenzielle Opfer im Internet zu finden. Über die Ping-Prüfung einer IP-Adresse und die Antwort des adressierten Rechners kann ein Hacker Angriffspunkte feststellen. Der Router kann so eingerichtet werden, dass er auf ICMP-Pings von außen nicht antwortet. Dadurch verbessern Sie den Schutz Ihres Routers.

Firewall > WAN Ping Blocking

ADVANCE FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to WAN port). This offers a heightened level of security. [More Info](#)

Block ICMP Ping

(1)

Um die Ping-Antwort zu deaktivieren, wählen Sie „Block ICMP Ping“ (1) und klicken auf „Apply Changes“ (Änderungen übernehmen). Der Router lässt jetzt ICMP-Pings unbeantwortet.

Dienstprogramme

Auf der Seite „Utilities“ (Dienstprogramme) können Sie verschiedene Parameter des Routers einstellen und bestimmte administrative Aufgaben durchführen.

Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Restart Router**
Sometimes it may be necessary to Reset or Reboot the Router if it begins working improperly. Resetting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Defaults**
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Current Settings**
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Saved Settings**
This option will allow you to restore a previously saved configuration.
- **Firmware Update**
From time to time, Linksys may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
- **System Settings**
The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the NAT function of the Router.

Neustart Router

Bisweilen kann es notwendig sein, den Router zurückzusetzen oder neu zu starten, falls dieser nicht mehr einwandfrei funktioniert. Bei einem Neustart bleiben die Konfigurationseinstellungen erhalten.

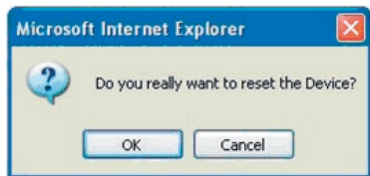
Utilities > Restart Router

Sometimes it may be necessary to Restart or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.



Wiederherstellen des Normalbetriebs durch einen Neustart

1. Klicken Sie auf die Schaltfläche „Restart Router“ (Router neu starten).
2. Das folgende Meldungsfenster wird geöffnet. Klicken Sie auf „OK“, um den Router neu zu starten.

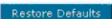


Werkseinstellungen

Mit dieser Option setzen Sie alle Routereinstellungen auf die Werkseinstellungen zurück. Es wird empfohlen, die aktuellen Einstellungen zu sichern, bevor Sie die Werkseinstellungen wiederherstellen.

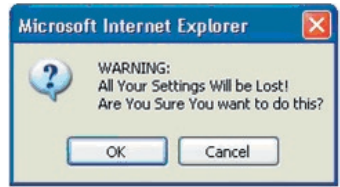
Utilities > Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.



Manuelle Konfiguration des Routers

1. Klicken Sie auf die Schaltfläche „Restore Defaults“ (Werkseinstellungen wiederherstellen).
2. Das folgende Meldungsfenster wird geöffnet. Klicken Sie auf „OK“, um die Werkseinstellungen wiederherzustellen.



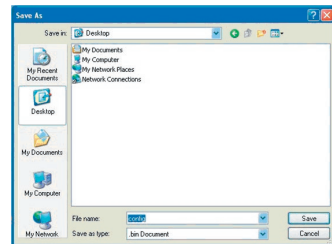
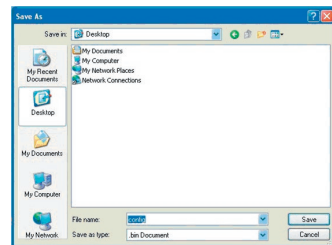
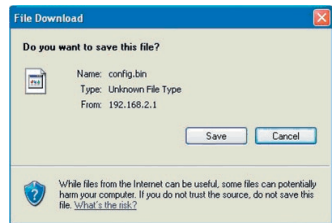
Aktuelle Einstellungen sichern/ Sicherheitskopie erstellen

Mit dieser Funktion können Sie die aktuelle Konfiguration sichern. Dadurch können Sie Ihre Konfigurierung später wiederherstellen, wenn die Einstellungen zwischenzeitlich verloren gehen oder geändert werden. Sie sollten die aktuelle Konfiguration sichern, bevor Sie ein Firmware-Upgrade durchführen.

1. Klicken Sie auf „Save“ (Speichern). Das Fenster „File Download“ (Datei heruntergeladen) wird geöffnet. Klicken Sie auf „Save“ (Sichern).
2. Es wird ein Fenster geöffnet, in dem Sie den Speicherort der Konfigurationsdatei festlegen können. Legen Sie den Pfad fest. Es gibt keine Beschränkungen bezüglich des Dateinamens; dennoch sollten Sie der Datei einen Namen geben, damit Sie sie später wiederfinden. Wenn Sie Speicherort und Namen der Datei festgelegt haben, klicken Sie auf „Save“ (Speichern).
3. Nach dem Speichern erscheint das folgende Fenster. Klicken Sie auf „Close“ (Schließen). Die Konfiguration ist jetzt gesichert.

UTILITIES > Save/Backup current settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.



Vorherige Einstellungen wiederherstellen

Über diese Option stellen Sie die zuvor gespeicherten Einstellungen wieder her.

Utilities > Restore Previous Settings

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the "Restore" button below.



1. Klicken Sie auf „Browse“ (Durchsuchen). Es wird ein Fenster geöffnet, in dem Sie den Speicherort der Konfigurationsdatei festlegen können. Klicken Sie die Konfigurationsdatei, „config.bin“ doppelt an.
2. Klicken Sie dann auf „Open“ (Öffnen).

Firmware aktualisieren

Von Zeit zu Zeit veröffentlicht Belkin neue Versionen der Router-Firmware. Firmware-Updates enthalten verbesserte Funktionen und Lösungen für eventuelle Probleme. Wenn Belkin eine neue Firmware veröffentlicht, können Sie sie von der Belkin Website herunterladen und die Firmware Ihres Routers auf den neuesten Stand bringen.

Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have occurred.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click here](#) to go to the Setup/Backup current settings page.



Abfragen einer neuen Firmware-Version

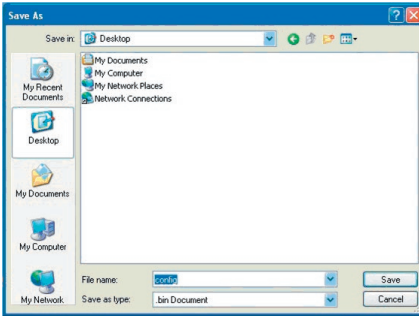
Mit der Schaltfläche „Check Firmware“ (1)(Firmware abfragen) [Designer: pls callout (1) in the screenshot] können Sie ohne große Suche nachsehen, ob eine neue Firmware-Version verfügbar ist. Wenn Sie auf die Schaltfläche klicken, wird Ihnen in einem neuen Browser-Fenster mitgeteilt, ob neue Firmware verfügbar ist. Ist dies der Fall, besteht die Möglichkeit zum Herunterladen.

Herunterladen einer neuen Firmware-Version

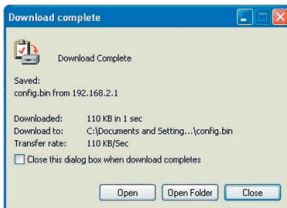
Wenn Sie auf die Schaltfläche „Check Firmware“ (Firmware abfragen) klicken und eine neue Firmware-Version verfügbar ist, wird folgender oder ein ähnlicher Bildschirm angezeigt:

1. Klicken Sie zum Herunterladen der neuen Firmware-Version auf „Download“ (Herunterladen).
2. Es wird ein Fenster geöffnet, in dem Sie den Speicherort für die Konfigurationsdatei festlegen können. Legen Sie den Pfad fest. Sie können einen beliebigen Dateinamen festlegen oder die Vorgabe übernehmen. Speichern Sie die Datei so, dass Sie sie später wieder finden. Wenn Sie den Pfad festgelegt haben, klicken Sie auf „Save“ (Sichern).

Manuelle Konfiguration des Routers

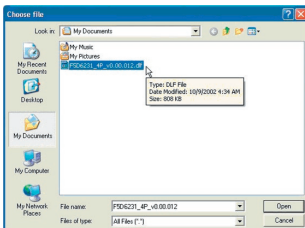


3. Nach dem Speichern wird das folgende Fenster geöffnet. Klicken Sie auf „Close“ (Schließen). Das Laden der Firmware ist abgeschlossen. Zur Aktualisierung der Firmware folgen Sie den nächsten Schritten unter Aktualisieren der Router-Firmware.



Aktualisieren der Router-Firmware

1. Klicken Sie auf der Seite „Firmware Update“ (Firmware-Aktualisierung) auf „Browse“ (Durchsuchen) (2). Designer: pls callout (2) in the screenshot]. Wenn Sie auf „Browse“ (Durchsuchen) klicken, wird ein Fenster geöffnet, in dem Sie den Pfad der Firmware-Aktualisierungsdatei wählen können.



2. Suchen Sie die Firmware-Datei, die Sie heruntergeladen haben. Doppelklicken Sie auf den Dateinamen.
3. Das Feld „Update Firmware“ (Firmware aktualisieren) zeigt jetzt den Dateipfad und -namen der gerade ausgewählten Firmware-Datei an. Klicken Sie auf „Update“ (Aktualisieren).

Utilities > Firmware Update

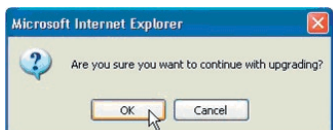
From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click Here](#) to go to the Save/Backup current settings page.

Firmware Version > 3.01.05
Check for new firmware version >

Update Firmware >

4. Sie werden gefragt, ob Sie fortfahren möchten. Klicken Sie auf „OK“.



5. Ein weiteres Meldungsfenster erscheint. Es weist darauf hin, dass der Computer eine Minute lang nicht reagieren wird, während die Firmware geladen und der Router neu gestartet wird. Klicken Sie auf „OK“.



Auf dem Bildschirm erscheint ein Countdown von 60 Sekunden. Wenn der Countdown Null erreicht, ist die Aktualisierung der Router-Firmware abgeschlossen. Jetzt müsste die Router-Homepage automatisch geöffnet werden. Geben Sie andernfalls die Routeradresse (standardmäßig 192.168.2.1) in die Adresszeile des Browsers ein.

Systemeinstellungen

Auf der Seite „System Settings“ (Systemeinstellungen) können Sie ein neues Administratorkennwort festlegen, die Zeitzone einstellen, die Fernverwaltung aktivieren und die UPnP-Funktion des Routers ein- oder ausschalten.

Einstellen oder Ändern des Administratorkennworts

Der Router wird OHNE festgelegtes Kennwort geliefert. Sie können auf dieser Seite ein Kennwort festlegen und dadurch die Sicherheit erhöhen. Notieren Sie sich das Kennwort, und bewahren Sie es sicher auf. Sie benötigen es, wenn Sie sich künftig am Router anmelden möchten. Sie sollten ein Kennwort festlegen, wenn Sie die Fernverwaltung des Routers nutzen möchten.

Utilities > System Settings

Administrator Password:

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

Ändern der Einstellung für das Anmeldezeitlimit

Durch die Option Anmelde-Zeitlimit können Sie einen Zeitraum festlegen, in dem Sie für die Erweiterte Benutzeroberfläche des Routers angemeldet sind. Die Zähluhr startet, wenn keine Aktivität mehr registriert wird. Beispiel: Sie haben Änderungen mit der erweiterten Konfigurationsoberfläche vorgenommen und verlassen Ihren Arbeitsplatz, ohne auf „Logout“ (Abmelden) zu klicken. Angenommen, das Zeitlimit ist auf 10 Minuten eingestellt, dann wird die angemeldete Sitzung nach 10 Minuten abgebrochen. Wenn Sie weitere Änderungen vornehmen möchten, müssen Sie sich erneut am Router anmelden. Das Zeitlimit für die Anmeldung dient der Sicherheit und ist auf 10 Minuten voreingestellt. Hinweis: Es kann jeweils nur ein Computer an der Erweiterten Benutzeroberfläche zur Routerkonfiguration angemeldet sein.

Einstellen von Uhrzeit und Zeitzone

Der Router hält die Uhrzeit auf dem Laufenden, indem er sich mit einem Simple Network Time Protocol (SNTP)-Server verbindet. Dadurch kann der Router die Systemuhr mit dem weltweiten Internet synchronisieren. Die synchronisierte Routeruhr dient zur Aufzeichnung des Sicherheitsprotokolls und zur Steuerung des Client-Filters. Wählen Sie Ihre Zeitzone aus. Wenn Sie sich in einer Region befinden, in der zwischen Sommer- und Winterzeit umgestellt wird, markieren Sie das Feld neben „Enable Daylight Saving“ (Sommerzeit aktivieren). Die Systemuhr wird nicht immer sofort aktualisiert. Sie müssen mindestens 15 Minuten abwarten, bis der Router die Zeitserver im Internet abfragt und eine Antwort erhält. Sie können die Uhr nicht selbst einstellen. Sie haben nun die Option, einen Primär- und einen Backup-NTP-Server zu wählen, damit die Uhr Ihres Routers mit verschiedenen NTP-Zeit-Servern im Internet synchronisiert werden kann. Wählen Sie den gewünschten NPT-Server in der Dropdown-Liste aus oder lassen Sie die aktuelle Einstellung unverändert.

Time and Time Zone: **August 1, 2003 4:26:00 AM**

Please set your time zone. If you are in an area that observes daylight saving check this box. [More Info](#)

Daylight Savings

Set Time Zone

Configure Time Server (NTP) Enable Automatic Time Server Maintenance

Primary Server

Secondary Server

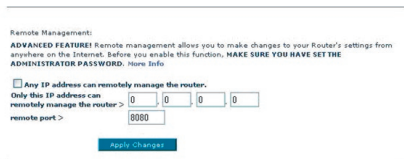
[Back](#)

Aktivieren der Fernverwaltung

Bevor Sie diese Funktion des Belkin Routers aktivieren, **STELLEN SIE SICHER; DASS SIE DAS ADMINISTRATORENKENNWORT EINGESTELLT HABEN.** Die Fernverwaltung ermöglicht das Ändern Ihrer Routereinstellungen von jedem Ort aus, an dem sich ein Internet-Anschluss befindet.

Für die Fernverwaltung des Routers gibt es zwei Methoden. Die erste Möglichkeit ist, den Zugriff auf den Router von überall aus dem Internet zuzulassen. Dazu wählen Sie die Option „Any IP address can remotely manage the Router“ (Jede IP-Adresse ist zum Fernmanagement des Routers berechtigt). Wenn Sie Ihre WAN-IP-Adresse an einem beliebigen Computer im Internet eingeben, erscheint ein Anmeldefenster, in dem Sie Ihr Routerkennwort eingeben müssen. Zum anderen können Sie eine bestimmte IP-Adresse festlegen, an der Sie die Fernverwaltung des Routers durchführen können. Dies ist sicherer, aber auch unpraktischer. Geben Sie für diese Methode die IP-Adresse des Computers, an dem Sie den Router fernverwalten möchten, in das entsprechende Feld ein, und aktivieren Sie die Option „Only this IP address can remotely manage the Router“ (Nur diese IP-Adresse zur Fernverwaltung des Routers zulassen).

Bevor Sie diese Funktion aktivieren, sollten Sie **UNBEDINGT ein Administratorkennwort festlegen!** Wenn Sie auf das Kennwort verzichten, setzen Sie Ihren Router der Gefahr von Manipulationen durch Unbefugte aus. Werkseitig ist Port 8080 für die Fernverwaltung eingestellt. Sie können auch einen anderen Port festlegen, indem eine neue Portnummer im Feld „remote port“ (Fernverwaltungsport) eingeben. Klicken Sie auf „Apply Changes“, um die Einstellungen zu speichern.



Aktivieren/Deaktivieren der NAT-Funktion

Hinweis: Diese weiterführende Funktion sollte nur von erfahrenen Benutzern bedient werden. Bevor Sie diese Funktion aktivieren, **SOLLTEN SIE UNBEDINGT EIN ADMINISTRATORENKENNWORT FESTLEGEN.** NAT (Netzwerkadressübersetzung) ist die Methode, mit der der Router die einzelne IP-Adresse, die Sie von Ihrem Internet-Provider erhalten haben, auf mehrere Computer im Netzwerk aufspaltet. Diese Funktion sollte nur dann neu eingestellt werden, wenn Ihnen Ihr Provider mehrere IP-Adressen zuteilt oder wenn Sie NAT zur weitergehenden Systemkonfiguration abschalten müssen. Wenn Sie nur eine IP-Adresse besitzen und NAT deaktivieren, können die Computer in Ihrem Netzwerk nicht auf das Internet zugreifen. Zudem können weitere Probleme auftreten. Eine Deaktivierung von NAT schaltet die Funktionen der Firewall ab.



Aktivieren und Deaktivieren von UPnP (Universelles Plug&Play)

UPnP (Universelles Plug-and-Play) ist eine weitere neue Funktion Ihres Belkin Routers. Diese Technologie ermöglicht den nahtlosen Betrieb von Sprach- und Videomeldungen, Spielen und anderen Anwendungen, die dem UPnP-Standard entsprechen.

Für bestimmte Anwendungen muss die Router-Firewall auf eine ganz bestimmte Weise konfiguriert werden, damit sie störungsfrei funktionieren. Hierzu müssen meistens TCP- und UDP-Ports geöffnet und in bestimmten Fällen auch Trigger-Ports gesetzt werden. UPnP-kompatible Anwendungen können mit dem Router kommunizieren und ihm mitteilen, wie die Firewall konfiguriert werden muss. Werkseitig ist die UPnP-Funktion des Routers deaktiviert. Wenn Sie UPnP-kompatible Anwendungen einsetzen und die UPnP-Funktionen nutzen möchten, können Sie die UPnP-Option aktivieren. Wählen Sie hierzu auf der Seite „Utilities“ (Dienstprogramme) im Abschnitt „UPnP Enabling“



(UPnP-Aktivierung) die Option „Enable“ (Aktivieren). Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Änderung zu speichern.

Aktivieren/Deaktivieren der Automatischen Firmware-Aktualisierung

Mit dieser neuartigen Funktion kann der Router automatisch anfragen, ob eine neue Firmware-Version vorliegt und Sie ggf. darauf aufmerksam machen. Wenn Sie sich an der Webgestützten Erweiterten Benutzeroberfläche des Routers anmelden, überprüft der Router, ob neue Firmware verfügbar ist. Ist dies der Fall, werden Sie benachrichtigt. Sie können die neue Version herunterladen oder die



Benachrichtigung ignorieren. Werkseitig ist diese Funktion des Routers deaktiviert. Wenn Sie die Funktion aktivieren möchten, wählen Sie „Enable“ (Aktivieren) und „Apply Changes“ (Änderungen übernehmen).

Einrichten der Computer

Damit Ihr Computer korrekt mit dem Router kommunizieren kann, müssen Sie die „TCP/IP / Ethernet“-Einstellungen Ihres Computers auf „Obtain an IP address automatically/ Using DHCP“ (DNS-Serveradresse automatisch beziehen/DHCP verwenden) ändern. Dies ist bei den meisten PCs in der Regel als Standard voreingestellt.

Manuelle Konfiguration der Netzwerkadapter

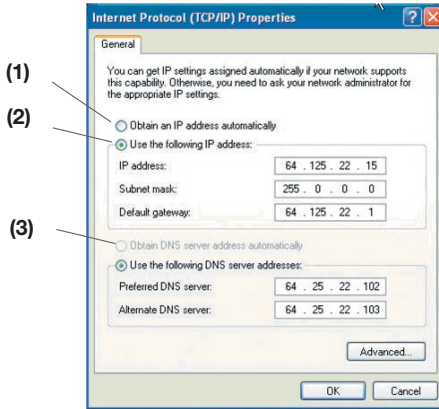
1
2
3
4
5
6
7
8
9
10
11

Kapitel

Richten Sie den Computer, der mit dem ADSL-Modem verbunden ist, ZUERST mit den folgenden Schritten ein. Auf die gleiche Weise können Sie weitere Computer zum Router hinzufügen, nachdem der Router für die Internetverbindung konfiguriert wurde.

Windows XP, 2000 oder NT

1. Klicken Sie auf Start, Einstellungen, Systemsteuerung.
2. Doppelklicken Sie auf das Symbol „Network and dial-up connections“ (Netzwerk- und DFÜ-Verbindungen öffnen) (Windows 2000) bzw. „Network“ (Netzwerk) (Windows XP).



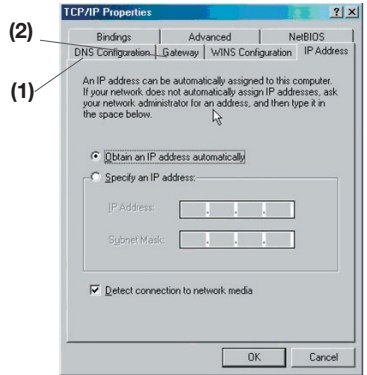
3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung Ihres Netzwerkadapters und wählen Sie „Properties“ (Eigenschaften) aus dem Dropdown-Menü.
4. Markieren Sie im Fenster Eigenschaften von LAN-Verbindung die Option Internetprotokoll (TCP/IP), und klicken Sie auf „Eigenschaften“. Daraufhin wird das folgende Fenster geöffnet:
5. Wenn „Use the following IP address“ (2) (Folgende IP-Adresse verwenden) (2) [Designer: pls callout (2) in the screenshot above] ausgewählt ist, muss Ihr Router für eine statische IP-Verbindung eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.

Manuelle Konfiguration der Netzwerkadapter

- Wählen Sie „Obtain an IP address automatically“ (IP-Adresse automatisch beziehen) (1) und „Obtain DNS server address automatically“ (DNS-Serveradresse automatisch beziehen) (3), wenn diese Punkte noch nicht ausgewählt sind. Klicken Sie auf „OK“. Ihre Netzwerkadapter werden jetzt für den Gebrauch mit dem Router konfiguriert.

Windows 98SE oder Me Benutzer

- Klicken Sie mit der rechten Maustaste auf „Netzwerkumgebung“, und wählen Sie „Eigenschaften“ im Dropdown-Menü.
- Wählen Sie die Option „TCP/IP > Einstellungen“ für den installierten Netzwerkadapter aus. Daraufhin wird das folgende Fenster geöffnet.
- Wenn die Option „Specify an IP address“ (IP-Adresse festlegen) ausgewählt ist, muss der Router für einen statischen IP-Verbindungstyp eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.
- Notieren Sie sich die in der Registerkarte IP-Adresse angegebene IP-Adresse und Subnetz-Maske (3).
- Klicken Sie auf die Registerkarte „Gateway“ (2). Notieren Sie die Gateway-Adresse in der Tabelle.
- Klicken Sie auf die Registerkarte „DNS Configuration“ (DNS-Konfiguration) (1). Notieren Sie die DNS-Adresse(n) in der Tabelle.
- Soweit noch nicht geschehen, aktivieren Sie auf der Registerkarte IP-Adresse die Option „IP-Adresse automatisch beziehen.“ Klicken Sie auf „OK“. Starten Sie den Computer neu. Während des Neustarts werden Ihre Netzwerkadapter für den Gebrauch mit dem Router konfiguriert. Richten Sie den Computer, der mit dem Kabel- oder DSL-Modem verbunden ist, ZUERST ein, indem Sie nach den folgenden Schritten vorgehen. Auf die gleiche Weise können Sie weitere Computer zum Router hinzufügen, nachdem der Router für die Internet-Verbindung konfiguriert wurde.

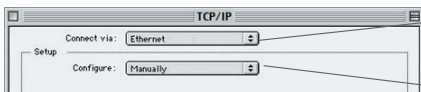


(3)

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

Mac OS bis 9.x

Damit Ihr Computer korrekt mit dem Router kommunizieren kann, müssen Sie die TCP/IP-Einstellungen Ihres Mac-Computers zu DHCP ändern.



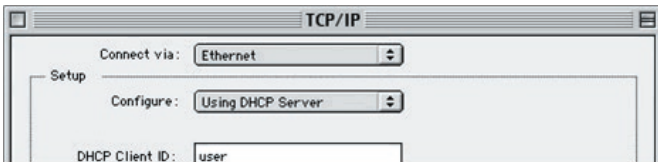
- Öffnen Sie das Applemenü. Wählen Sie „Control Panels“ (Kontrollfelder) und „TCP/IP“.
- Die TCP/IP-Kontrollfelder werden

angezeigt. Wählen Sie unter „Connect Via:“ (Verbindung:) entweder „Ethernet Built In“ (Ethernet integriert) oder „Ethernet“ (1).

3. Wenn neben „Configure“ (Konfigurationsmethode) (2) [Designer: pls callout (2) in the screenshot above] „Manually“ (Manuell) ausgewählt ist, muss der Router für eine statische IP-Verbindung eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.

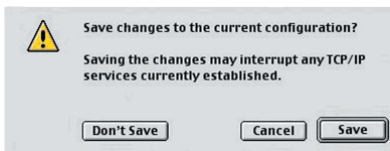
IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

4. Soweit noch nicht unter „Configure“ (Konfigurationsmethode) eingestellt, wählen Sie die Option „Using DHCP Server“ (Über DHCP-Server). Dadurch wird der Computer angewiesen, eine IP-Adresse vom Router anzufordern.



5. Schließen Sie das Fenster. Wenn Sie Änderungen vorgenommen haben, erscheint das folgende Fenster. Klicken Sie auf „Save“ (Speichern).

Starten Sie den Computer neu. Während des Neustarts werden die Netzwerkeinstellungen für den Router konfiguriert.



Mac OS X

1. Klicken Sie auf das Symbol „System Preferences“ (Systemeinstellungen).

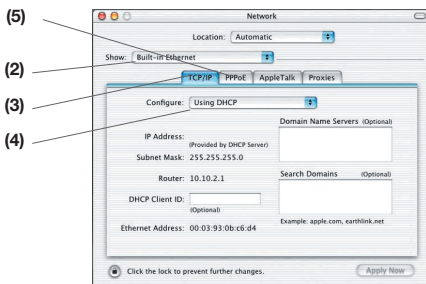


Manuelle Konfiguration der Netzwerkadapter

2. Wählen Sie das Symbol (Netzwerk) „Network“ (1) unter „System Preferences“ (Systemeinstellungen) aus.



3. Wählen Sie unter „Network“ (Netzwerk) „Built-in Ethernet“ (Ethernet integriert) (2) neben „Show“ (Zeigen).
4. Wählen Sie die Registerkarte „TCP/IP“ (3). Neben „Configure“ (4) (Konfiguration) müsste „Manually“ (Manuell) oder „Using DHCP“ (DHCP verwenden) angezeigt werden. Wenn nicht, vergewissern Sie sich, dass auf der Registerkarte „PPPoE“ (5) „PPPoE verwenden“ NICHT ausgewählt ist. Ist dies der Fall, müssen Sie den Router mittels Benutzername und Kennwort für einen PPPoE-Verbindungstyp konfigurieren.



5. Wenn die Option „Manually“ (Manuell) ausgewählt ist, muss der Router für einen statischen IP-Verbindungstyp eingerichtet werden. Notieren Sie die Adressinformationen in der Tabelle unten. Sie müssen sie später in den Router eingeben.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

6. Soweit noch nicht geschehen, wählen Sie neben „Configure“ (4) (Konfiguration) „Using DHCP“ (DHCP verwenden) und klicken Sie auf „Apply Now“ (Jetzt aktivieren).

Ihre Netzwerkadapter werden jetzt für den Gebrauch mit dem Router konfiguriert.

Empfohlene Browser-Einstellungen

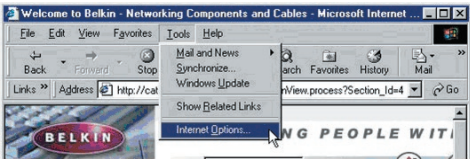
1
2
3
4
5
6
7
8
9
10
11

Kapitel

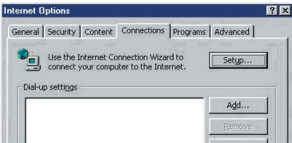
Normalerweise können Sie die Browser-Einstellungen unverändert lassen. Wenn es beim Zugriff auf das Internet oder die Webgestützte Erweiterte Benutzeroberfläche zu Problemen kommt, können Sie jedoch auf die empfohlenen Einstellungen in diesem Abschnitt zurückgreifen.

Microsoft Internet Explorer 4.0 (oder höher)

1. Starten Sie Ihren Webbrowser. Wählen Sie „Extras“ und die Funktion „Internetoptionen“.

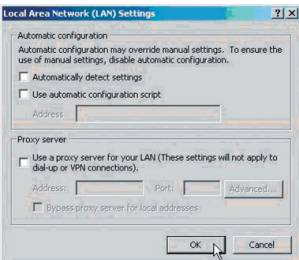


2. Im Fenster Internetoptionen stehen drei Optionen zur Auswahl: „Keine Verbindung wählen“, „Nur wählen, wenn keine Netzwerkverbindung besteht“ und „Immer Standardverbindung wählen“. Wenn die Optionen verfügbar sind, aktivieren Sie „Keine Verbindung wählen“. Wenn die Optionen nicht verfügbar sind, fahren Sie mit dem nächsten Schritt fort.



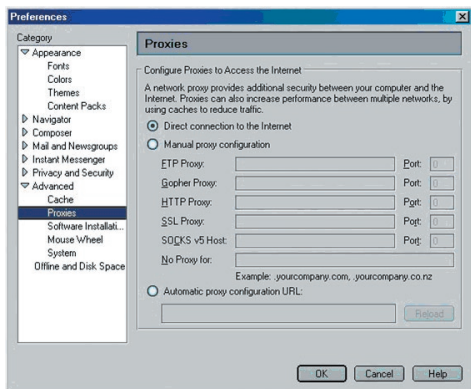
3. Klicken Sie auf die Registerkarte „Verbindungen“, und wählen Sie „LAN-Einstellungen...“.

4. Stellen Sie sicher, dass keine der folgenden Optionen aktiviert ist: „Automatische Suche der Einstellungen“, „Automatisches Konfigurationsskript verwenden“ sowie „Einen Proxyserver verwenden“. Klicken Sie auf „OK“. Klicken Sie im Dialogfeld „Internetoptionen“ abermals auf „OK“.



Netscape® Navigator® 4.0 oder höher

1. Starten Sie Netscape. Klicken Sie auf „Bearbeiten“ > „Einstellungen“.
2. Klicken Sie im Dialogfeld Einstellungen auf „Erweitert“ und dann auf „Proxies“.
Klicken Sie im Dialogfeld „Proxies“ auf „Direkte Verbindung zum Internet“.



Fehlerbehebung

1

Problem:

Die ADSL-Statusanzeige ist nicht an.

2

Lösung:

1. Überprüfen Sie die Verbindung zwischen Router- und ADSL-Leitung. Stellen Sie sicher, dass das ADSL-Kabel an den Port des Routers angeschlossen ist, der mit „DSL Line“ (DSL-Leitung) bezeichnet ist.
2. Überprüfen Sie, ob der Router mit Strom versorgt wird. [Power Icon] Die Betriebsanzeige auf der Vorderseite sollte leuchten.

3

4

Problem:

Die Internet-Statusanzeige ist nicht an.

5

Lösung:

1. Stellen Sie sicher, dass das ADSL-Kabel an den Port des Routers angeschlossen ist, der mit „DSL Line“ (DSL-Leitung) bezeichnet ist. [Insert: ADSL icon] Die ADSL-Statusanzeige ist an.
2. Stellen Sie sicher, dass Sie die richtige VPI/VCI, den richtigen Benutzernamen und das korrekte Kennwort Ihres ISP (Internetproviders) verwenden.

6

7

8

Problem:

Ich arbeite mit einer statischen IP-Adresse. Ich kann keine Verbindung zum Internet herstellen.

9

10

Lösung:

Da Sie mit statischer IP-Adressierung arbeiten, muss Ihnen der Provider die IP-Adresse, die Subnetz Maske und die Gateway-Adresse zuweisen. Verwenden Sie an Stelle des Assistenten den „Connection Type“ (Verbindungstyp) und wählen Sie Ihre Verbindung aus. Klicken Sie auf „Next“ (Weiter), wählen Sie „Static IP“ (Statische IP-Adresse) und geben Sie Ihre IP-Adresse, Subnetz-Maske und die Standard-Gateway-Informationen an.

11

Problem:

Ich habe mein Kennwort vergessen oder verloren.

Lösung:

Halten Sie den Schalter „Reset“ (Zurücksetzen) auf der Rückseite für mindestens 6 Sekunden gedrückt, um die Werkseinstellung wieder herzustellen.

Problem:

Mein kabellos vernetzter PC kann keine Verbindung mit dem Router herstellen.

Lösung:

1. Stellen Sie sicher, dass Ihr kabellos vernetzter PC die gleichen SSID-Einstellungen wie der Router hat, und dass auf den Clients die gleichen Sicherheitseinstellungen wie WPA- und WEP-Verschlüsselung vorhanden sind.
2. Stellen Sie sicher, dass die Entfernung zwischen dem Router und dem kabellos vernetzten PC nicht zu groß ist.

Problem:

Es treten oft Störungen im kabellosen Netzwerk auf.

Lösung:

1. Stellen Sie Ihren kabellos vernetzten PC näher an den Router, um ein besseres Signal zu erhalten.
2. Es könnten auch Interferenzen vorhanden sein, die durch eine Mikrowelle oder schnurlose Telefone mit 2.4GHz verursacht werden. Ändern Sie den Standort des Routers oder benutzen Sie einen anderen Funkkanal.

Problem:

Ich kann keine Funkverbindung zum Internet herstellen.

Lösung:

Wenn Sie mit einem kabellos vernetzten Computer keine Internetverbindung aufbauen können, prüfen Sie Folgendes:

1. Schauen Sie sich die Leuchtanzeigen Ihres Routers an. Wenn Sie einen Router von Belkin benutzen, sehen diese wie folgt aus:
 - Die Betriebsleuchte sollte leuchten..
 - Die Anzeige „Connected“ (Verbunden) sollte an sein aber nicht blinken.
 - Die WAN-Anzeige sollte entweder an sein oder blinken.
2. Klicken Sie in der rechten unteren Ecke des Bildschirms im System-Tray auf das Symbol des WLAN-Programms, um es zu öffnen. Wenn Sie eine kabellose Netzwerkkarte von Belkin benutzen, sollte das Tray-Symbol wie dieses [INSERT ICON] aussehen (das Symbol kann rot oder grün sein):
3. Das Fenster, das sich nun öffnet, wird je nach Modell der kabellosen Netzwerkkarte variieren; jedes Dienstprogramm sollte jedoch über eine Liste „Verfügbare Netzwerke“ verfügen - mit den kabellosen Netzwerken, mit denen eine Verbindung hergestellt werden kann.

Wird der Name Ihres kabellosen Netzwerks in der Liste angezeigt?

Ja, in der Liste ist mein Netzwerkname aufgeführt — beachten Sie den Abschnitt „Ich kann keine kabellose Internetverbindung aufbauen, aber mein Netzwerkname wird angezeigt“ in diesem Kapitel.

Nein, in der Liste ist mein Netzwerkname nicht aufgeführt—beachten Sie den Abschnitt „Ich kann keine kabellose Internetverbindung aufbauen und mein Netzwerkname wird nicht angezeigt“ in diesem Kapitel.

Problem:

Ich kann keine kabellose Internetverbindung aufbauen aber mein Netzwerkname wird angezeigt.

Lösung:

Ist Ihr Netzwerkname auf der Liste der verfügbaren Netzwerke zu sehen, folgen Sie bitte diesen Schritten, um die Verbindung herzustellen:

1. Klicken Sie in der Liste „Available Networks“ (Verfügbare Netzwerke) auf den korrekten Netzwerknamen.

Ist die Sicherheitsfunktion (Verschlüsselung) aktiviert, müssen Sie den Netzwerkschlüssel eingeben. Weitere Informationen zur Sicherheit finden Sie auf der Seite „Änderungen der Sicherheitseinstellungen des Funknetzwerks“.

2. Nach wenigen Sekunden sollte das Symbol in der linken unteren Bildschirmcke der Symbolleiste grün leuchten, ein Zeichen dafür, dass eine Verbindung zum Netzwerk aufgebaut wurde.

Problem:

Ich kann keine kabellose Internetverbindung aufbauen und mein Netzwerkname wird nicht angezeigt.

Lösung:

Wenn der korrekte Netzwerkname nicht auf der Liste für „Available Networks“ (Verfügbare Netzwerke) steht, gehen Sie zur Fehlerbehebung bitte nach folgenden Schritten vor:

1. Stellen Sie den Computer, wenn möglich, zeitweilig im Abstand von etwa ein bis drei Metern vom Router auf. Schließen Sie das Dienstprogramm für kabellose Netzwerke und öffnen Sie es erneut. Wenn der korrekte Netzwerkname jetzt auf der Liste für „Available Networks“ (Verfügbare Netzwerke) erscheint, ist das Problem möglicherweise auf die Reichweite oder eine Störung zurückzuführen. Beachten Sie bitte die Lösungsvorschläge in Anhang B mit dem Titel „Wichtige Faktoren bei Aufstellung und Einrichtung“.
2. Wird ein Computer verwendet, der mit einem Netzkabel an den Router angeschlossen ist (im Gegensatz zur kabellosen Verbindung), prüfen Sie ob „Broadcast SSID“ (SSID rundsenden) aktiviert ist. Diese Einstellung ist auf der Seite für „Kanal und SSID“-Einstellungen des Routers zu finden.

Wenn Sie nach diesen Schritten weiterhin keine Internetverbindung aufbauen können, melden Sie sich bitte beim technischen Support von Belkin.

Problem:

Mein kabelloses Netzwerk arbeitet nicht konsistent.

Die Datenübertragung ist manchmal langsam.

Die Signalstärke ist unzureichend.

Es ist schwierig, eine Virtual Private Network (VPN)-Verbindung aufzubauen und/oder aufrechtzuerhalten.

Lösung:

Funktechnologie basiert auf Radiotechnik. Das bedeutet, dass die Verbindungsqualität und die Funktionalität zwischen den Geräten abnimmt, wenn die Entfernung zwischen den Geräten zunimmt. Andere Faktoren, die zur Verschlechterung des Signals führen können, sind Hindernisse wie Wände und Metallvorrichtungen (gerade Metall ist ein großer Störfaktor). Daraus ergibt sich in geschlossenen Räumen eine durchschnittliche Reichweite für kabellose Netzwerkgeräte von 30 bis 60 Metern. Bitte beachten Sie, dass die Verbindungsgeschwindigkeit abnehmen könnte, wenn Sie weiter vom Router oder Access Point entfernt sind.

Um zu prüfen, ob die Funkprobleme auf die Entfernung zurückzuführen sind, stellen Sie den Computer zeitweilig, wenn möglich, in etwa eineinhalb bis drei Metern vom Router auf.

Wechseln des Funkkanals - Wenn Störungen auftreten, z.B. durch andere kabellose Netzwerke in der Umgebung, können Sie die Leistung und Verlässlichkeit Ihres Netzwerks verbessern, indem Sie den Kanal Ihres kabellosen Netzwerks wechseln. Der Standard-Kanal Ihres Routers ist werksbedingt auf 11 eingestellt. Sie können, je nach Standort, aus diversen anderen Kanälen auswählen. Bitte beachten Sie hierzu auf Seite 30 den Abschnitt „Ändern des Funkkanals“, um andere Kanäle einzustellen.

Verringerung der Übertragungsrate des kabellosen Netzwerks - Verringerung der Übertragungsrate des kabellosen Netzwerks kann die maximale Reichweite des kabellosen Netzwerks und die Stabilität der Verbindung verbessern. Bei vielen kabellosen Netzwerkkarten kann die Übertragungsrate verringert werden. Gehen Sie hierfür zur Systemsteuerung von Windows, öffnen Sie die Netzwerkverbindungen und klicken Sie doppelt auf die Funknetzverbindung Ihrer Karte. Wählen Sie im Dialogfeld „Eigenschaften“ auf der Registerkarte „Allgemein“ den Konfigurationsschalter aus (Anwender von Windows 98 müssen die kabellose Netzwerkkarte im Listenfeld auswählen und dann auf „Eigenschaften“ klicken), wählen Sie den Schalter „Erweitert“ und anschließend die entsprechende Übertragungsrate. Kabellose Client-Karten sind normalerweise so eingestellt, dass sie die Übertragungsrate automatisch anpassen; dies kann allerdings zu periodischen Unterbrechungen führen, wenn

das Funksignal zu schwach ist; langsamere Übertragungsraten sind in der Regel stabiler. Probieren Sie verschiedene Übertragungsraten aus, bis Sie die passende für Ihre Umgebung gefunden haben; bitte beachten Sie, dass die Übertragungsraten für den Internetgebrauch anwendbar sein müssen. Beachten Sie für weitere Informationen das Handbuch Ihrer kabellosen Netzwerkkarte.

Problem:

Wie kann ich mein kabelloses Netzwerk erweitern?

Lösung:

Belkin empfiehlt den Gebrauch der folgenden Produkte, um die Funkabdeckung in großen Räumen oder Büros zu vergrößern:

- **Kabelloser Access Point:** Ein kabelloser Access Point kann den Deckungsbereich Ihres kabellosen Netzwerks effektiv erweitern. Ein Access Point (Zugriffspunkt) wird üblicherweise in einem Bereich platziert, der noch nicht von einem kabellosen Router gedeckt ist und mit diesem entweder mit einem Ethernet-Kabel oder über Ihre Stromleitungen mit zwei Powerline-Ethernet-Adaptern verbunden ist.
- Für Kabellose Netzwerke mit dem Standard 802.11g (54g) bietet Belkin einen Kabellosen Range Extender/Access Point an, der ohne die Verwendung eines Ethernet-Kabels oder Powerline-Ethernet-Adapters mit einem kabellosen 802.11g-Router verbunden werden kann.

Diese Produkte von Belkin erhalten Sie bei Ihrem Fachhändler oder durch direkte Bestellung bei Belkin.

Für Informationen zur Netzwerk -und Bereichserweiterung besuchen Sie bitte: www.belkin.com/networking. Dort finden Sie weitere Informationen zum: Kabellosen Range Extender/Access Point (F5D7132)

Problem:

Ich habe Schwierigkeiten beim Einstellen der Wired Equivalent Privacy (WEP) auf einem Router oder Access Point von Belkin.

Lösung:

1. Melden Sie sich an Ihren kabellosen Router oder Access Point an.
2. Öffnen Sie Ihren Internet-Browser und tragen Sie die IP-Adresse des kabellosen Routers oder Access Points ein. (Beim Router ist dies standardmäßig 192.168.2.1, beim 802.11g Access Point ist dies 192.168.2.254). Melden Sie sich durch Klicken auf den Schalter „Login“ (Anmelden) in der oberen rechten Ecke des Bildschirms an Ihren Router an. Sie werden nach Ihrem Kennwort gefragt. Wenn Sie noch kein Kennwort eingestellt haben, lassen Sie das Feld frei und klicken Sie auf „Submit“ (Abschicken).
3. Klicken Sie links im Bildschirm auf die Registerkarte „Wireless“ (Funknetz). Wählen Sie „Encryption“ (Verschlüsselung) oder „Security“ (Sicherheit), um zur Sicherheitseinstellungsseite zu gelangen.
4. Wählen Sie im Dropdown-Menü die Option „128-bit WEP“.
5. Nachdem Sie den WEP-Verschlüsselungsmodus gewählt haben, können Sie den HEX WEP-Schlüssel manuell eingeben oder ein Kennwort in das Feld

„Passphrase“ (Kennfolge) eingeben und auf „Generate“ (Generieren) klicken, um aus der Passphrase automatisch einen WEP-Schlüssel zu erstellen. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients entsprechend einstellen. Ein Hex (Hexadezimalschlüssel) ist eine Kombination aus Ziffern und Buchstaben von A-F und von 0–9. Für 128-Bit-WEP müssen Sie 26 Hexzeichen eingeben.

Beispiel:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-Bit-Schlüssel

6. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um abzuschließen. Die Verschlüsselung ist nun im kabellosen Router eingestellt. Jeder Computer in Ihrem kabellosen Netzwerk muss jetzt mit denselben Sicherheitseinstellungen konfiguriert werden.

ACHTUNG: Wenn Sie für die Einstellung des kabellosen Routers oder Access Points einen Computer mit kabellosem Client verwenden, müssen Sie die Sicherheitsfunktion für diesen kabellosen Client aktivieren. Falls dies nicht der Fall ist, wird die Funkverbindung unterbrochen.

Hinweis an Mac-Benutzer: AirPort-Produkte von Apple unterstützen in der Original-Ausführung nur Verschlüsselung mit 64 Bit. Apple AirPort 2-Produkte unterstützen sowohl 64-Bit- als auch 128-Bit-Verschlüsselung. Bitte überprüfen Sie, welche Version des Apple Airport-Produkts Sie verwenden. Wenn Sie Ihr Netzwerk nicht mit 128 Bit verschlüsseln können, sollten Sie es mit der 64-Bit-Verschlüsselung probieren.

Problem:

Ich habe Schwierigkeiten beim Einstellen der Wired Equivalent Privacy (WEP) auf einer kabellosen Netzwerkkarte von Belkin.

Lösung:

Die kabellose Netzwerkkarte muss den gleichen Schlüssel wie der kabellose Router oder Access Point verwenden. Benutzt Ihr kabelloser Router oder Access Point z. B. den Schlüssel 00112233445566778899AABBCC, muss die kabellose Netzwerkkarte exakt auf den gleichen Schlüssel eingestellt werden.

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network“ (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen.
2. Mit der Schaltfläche „Advanced“ (Erweitert) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
3. Sobald die Schaltfläche „Advanced“ (Erweitert) angeklickt ist, erscheint das LAN-Dienstprogramm von Belkin. Das Dienstprogramm erlaubt Ihnen die Verwaltung aller erweiterter Funktionen der kabellosen Netzwerkkarte von Belkin.
4. Wählen Sie auf der Registerkarte „Wireless Network Properties“ (Netzwerkeigenschaften) einen Netzwerknamen in der Liste „Available networks“ (Verfügbare Netzwerke) aus und klicken Sie auf „Properties“ (Eigenschaften).
5. Wählen Sie bei „Data Encryption“ (Datenverschlüsselung) „WEP“.
6. Das untere Feld „Network key is provided for me automatically“

(Netzwerkschlüssel wird automatisch vergeben) darf nicht aktiviert sein. Wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk herzustellen, wenden Sie sich bitte an Ihren Netzwerkadministrator, um zu erfahren, ob dieses Feld aktiviert werden muss.

7. Geben Sie Ihren WEP-Schlüssel in das Feld „Network Key“ (Netzwerkschlüssel) ein.

Wichtiger Hinweis: Ein WEP-Schlüssel ist eine Kombination aus Zahlen und Buchstaben von A-F und 0-9. Für 128-Bit WEP müssen Sie 26 Schlüssel eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres kabellosen Routers oder Access Points übereinstimmen.

Beispiel: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-Bit-Schlüssel

8. Klicken Sie auf „OK“, und dann auf „Apply“ (Übernehmen), um die Einstellungen zu speichern.

Wenn Sie KEINE kabellose Netzwerkkarte von Belkin benutzen, sollten Sie sich an den Hersteller Ihrer Netzwerkkarte wenden, um das Benutzerhandbuch für die Karte zu erhalten.

Problem:

Unterstützen die Produkte von Belkin WPA?

Lösung:

Hinweis: Um WPA zu verwenden, müssen alle Ihre Clients die Software und Treiber, die WPA unterstützen, aktualisieren. Zum Zeitpunkt der Erstellung dieser Anleitung ist von Microsoft ein kostenloses Sicherheits-Patch als Download erhältlich. Dieses Patch gilt nur für das Betriebssystem Windows XP.

Laden Sie sich das Patch hier herunter:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

Sie benötigen auch die aktuellen Treiber von Belkin für Ihre kabellose 802.11g Desktop- oder Notebook-Netzwerkkarte. Diese finden Sie auf der Support-Seite von Belkin. Andere Betriebssysteme können zur Zeit nicht unterstützt werden. Das Patch von Microsoft unterstützt nur Geräte mit WPA-aktivierten Treibern, wie die 802.11g-Produkte von Belkin.

Hier laden Sie den aktuellen Treiber herunter: <http://www.belkin.com/uk/support/tech/index.asp>

Problem:

Ich habe in einem Heimnetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einem Router oder Access Point von Belkin.

Lösung:

1. Wählen Sie im Dropdown-Menü „Security Mode“ (Sicherheitsmodus) „WPA-PSK (no server)“ (WPA-PSK (kein Server)) aus.
2. Wählen Sie als Verschlüsselungstechnik „TKIP“ oder „AES“ aus. Diese

1

2

3

4

5

6

7

8

9

10

11

Einstellungen müssen mit denen Ihrer Clients übereinstimmen.

3. Geben Sie Ihren Pre-Shared Key (PSK) ein. Dieser kann aus acht bis 63 Zeichen (Buchstaben, Zahlen, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten. Ihr PSK kann zum Beispiel heißen: „Familie Simpsons Netzwerkschlüssel“.
4. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.

Problem:

Ich habe in einem Firmennetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einem Router oder Access Point von Belkin.

Lösung:

Wenn Sie in Ihrem Netzwerk einen Radius-Server verwenden, um die Schlüssel an die Clients zu verteilen, verwenden Sie diese Einstellung. Diese Technik wird typischerweise in einer Unternehmensumgebung eingesetzt.

1. Wählen Sie im Dropdown-Menü „Security Mode“ (Sicherheitsmodus) „WPA-PSK (mit Server)“ aus.
2. Wählen Sie als Verschlüsselungstechnik „TKIP“ oder „AES“ aus. Diese Einstellungen müssen mit denen Ihrer Clients übereinstimmen.
3. Geben Sie die IP-Adresse des Radius-Servers in die Felder unter „Radius Server“ ein.
4. Geben Sie den Radius-Schlüssel in das Feld „Radius Key“ (Radius-Schlüssel) ein.
5. Geben Sie das Schlüsselintervall ein. Das Schlüsselintervall gibt an, wie oft die Schlüssel verteilt werden (in Paketen).
6. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um abzuschließen. Sie müssen nun alle Clients für diese Einstellungen einrichten.

Problem:

Ich habe in einem Heimnetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einer kabellosen Netzwerkkarte von Belkin..

Lösung:

Die Clients müssen den gleichen Schlüssel wie der kabellose Router oder Access Point verwenden. Heißt der Schlüssel im kabellosen Router oder Access Point z.B. „Familie Simpsons Netzwerkschlüssel“, müssen die Clients den gleichen Schlüssel verwenden.

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network“ (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen.
2. Mit der Schaltfläche „Advanced“ (Erweitert) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
3. Sobald die Schaltfläche „Advanced“ (Erweitert) angeklickt ist, erscheint das LAN-Dienstprogramm von Belkin. Das Dienstprogramm erlaubt Ihnen die Verwaltung aller erweiterter Funktionen der kabellosen Netzwerkkarte von Belkin.
4. Wählen Sie auf der Registerkarte „Wireless Network Properties“ (Netzwerkeigenschaften) einen Netzwerknamen in der Liste „Available networks“ (Verfügbare Netzwerke) aus und klicken Sie auf „Properties“ (Eigenschaften).

5. Wählen Sie unter „Network Authentication“ (Netzwerk-Authentifizierung) den Eintrag „WPA-PSK (No Server)“ (WPA-PSK [Kein Server]) aus.
6. Geben Sie Ihren WPA-Schlüssel in das Feld „Network Key“ (Netzwerkschlüssel) ein.

Wichtiger Hinweis: Ein WPA-PSK ist eine Kombination aus Zahlen und Buchstaben von A-Z und 0-9. Für WPA-PSK können Sie acht bis 63 Zeichen eingeben. Dieser Netzwerkschlüssel muss mit dem Ihres kabellosen Routers oder Access Points übereinstimmen.

7. Klicken Sie auf „OK“, und dann auf „Apply“ (Übernehmen), um die Einstellungen zu speichern.

Problem:

Ich habe in einem Firmennetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) auf einer kabellosen Netzwerkkarte von Belkin.

Lösung:

1. Klicken Sie doppelt auf das Signalsymbol, um das Fenster „Wireless Network“ (Kabelloses Netzwerk) auf dem Bildschirm aufzurufen.
2. Mit der Schaltfläche „Advanced“ (Erweitert) können Sie zusätzliche Kartenoptionen überprüfen und verändern.
3. Sobald die Schaltfläche „Advanced“ (Erweitert) angeklickt ist, erscheint das LAN-Dienstprogramm von Belkin. Das Dienstprogramm erlaubt Ihnen die Verwaltung aller erweiterter Funktionen der kabellosen Netzwerkkarte von Belkin.
4. Wählen Sie auf der Registerkarte „Wireless Network Properties“ (Netzwerkeigenschaften) einen Netzwerknamen in der Liste „Available networks“ (Verfügbare Netzwerke) aus und klicken Sie auf „Properties“ (Eigenschaften).
5. Wählen Sie unter „Network Authentication“ (Netzwerk-Authentifizierung) den Eintrag „WPA“ aus.
6. Wählen Sie auf der Registerkarte „Authentication“ (Authentifizierung) die Einstellungen, die Sie vom Netzwerkadministrator erhalten haben.
7. Klicken Sie auf „OK“, und dann auf „Apply“ (Übernehmen), um die Einstellungen zu speichern.

Problem:

Ich habe in einem Heimnetzwerk Schwierigkeiten beim Einstellen von Wi-Fi Protected Access (WPA) und ich benutze KEINE kabellose Netzwerkkarte von Belkin.

Lösung:

Für kabellose Desktop- und Notebookkarten von Drittanbietern, die nicht mit WPA-Software ausgestattet sind, steht ein Sicherheitspatch von Microsoft mit dem Namen „Windows XP Support Patch for Wireless Protected Access“ kostenlos als Download zur Verfügung. Suchen Sie in der Unterstützungsdatenbank von Microsoft unter dem Suchwort Windows XP WPA und laden Sie das Patch herunter.

Hinweis: Dieses von Microsoft zur Verfügung gestellte Patch gilt nur für das Betriebssystem Windows XP. Andere Betriebssysteme können zur Zeit nicht unterstützt werden. Sie müssen auch überprüfen, ob der Hersteller der kabellosen Karte WPA unterstützt und Sie die aktuellsten Treiber heruntergeladen und installiert haben.

Unterstützte Betriebssysteme:

- Windows XP Professional
- Windows XP Home Edition

WPA-PSK (kein Server) aktivieren

1. Unter Windows XP, klicken Sie auf „Start > Systemsteuerung > Netzwerkverbindungen“.
2. Klicken Sie mit der rechten Maustaste auf „Drahtlose Netzwerke“ (Wireless Networks). Das folgende Fenster wird angezeigt. Vergewissern Sie sich, dass das Kontrollkästchen „Use Windows to configure my wireless network settings“ (Windows zum Konfigurieren der Netzwerkeinstellungen verwenden) markiert ist.
3. Klicken Sie auf der Registerkarte „Wireless Networks“ (Drahtlose Netzwerke) auf die Schaltfläche „Configure“ (Konfigurieren).
4. Nutzer von Heim- oder kleinen Unternehmensnetzwerken wählen „WPA-PSK“ unter „Network Administration“ (Netzwerkverwaltung).

Hinweis: Wählen Sie „WPA (with radius server)“ (WPA [mit Radius-Server]) aus, wenn Sie diesen Computer verwenden, um eine Verbindung mit einem Unternehmensnetzwerk herzustellen, das einen Authentifizierungsserver wie einen Radius-Server unterstützt. Wenden Sie sich für weitere Informationen bitte an Ihren Netzwerkadministrator.

5. Wählen Sie unter „Data Encryption“ (Datenverschlüsselung) „TKIP“ oder „AES“. Diese Einstellungen müssen identisch mit denen Ihres kabellosen Routers oder Access Points sein.
6. Geben Sie Ihren Schlüssel in das Feld „Network Key“ (Netzwerkschlüssel) ein.

Wichtiger Hinweis: Geben Sie Ihren PSK ein. Er kann aus acht bis 63 Zeichen (Buchstaben, Ziffern, Sonderzeichen) bestehen. Sie müssen diesen Schlüssel für alle Clients verwenden, die Sie einrichten.

7. Klicken Sie auf „OK“, um die Einstellungen zu übernehmen.

Was ist der Unterschied zwischen 802.11b, 802.11g, 802.11a und Pre-N?

Es gibt heutzutage vier verschiedene WLAN-Standards, die Daten bei sehr unterschiedlichen Höchstgeschwindigkeiten übertragen. Jede basiert auf der Zuweisung 802.11(x), benannt vom IEEE, dem Gremium, das für zertifizierte Netzwerkstandards verantwortlich ist. Der gebräuchlichste WLAN-Standard, 802.11b, überträgt Daten mit 11 Mbit/s; 802.11a und 802.11g arbeiten mit 54 Mbit/s und Pre-N arbeitet mit 108 Mbit/s. Pre-N, der Vorreiter des 802.11n-Standards, der bald auf den Markt kommen wird, erreicht höhere Geschwindigkeiten als 802.11g und sorgt für eine doppelt so hohe Funkabdeckung. Beachten Sie für weitere Informationen die folgende Tabelle:

Vergleich zwischen verschiedenen WLAN-Standards

Funktechnologie	G (802.11g)	G+ MIMO (802.11g mit MIMO MFC)	N MIMO (Entwurf 802.11n mit MIMO)	N1 MIMO (Entwurf 802.11n mit MIMO)
Geschwindigkeit/ Datenrate*	Bis zu 54 Mbit/s*	Bis zu 54 Mbit/s*	Bis zu 300 Mbit/s*	Bis zu 300 Mbit/s*
Frequenz	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen	Normale Geräte im Haushalt, wie schnurlose Telefone und Mikrowellen, können im lizenzfreien 2,4-GHz-Frequenzband Störungen verursachen
Kompatibilität	Kompatibel mit 802.11b/g	Kompatibel mit 802.11b/g	Kompatibel mit dem Entwurf des Standards 802.11n** und 802.11b/g	Kompatibel mit dem Entwurf des Standards 802.11n** und 802.11b/g
Reichweite*	Bis zu 122 m*	Bis zu 300 m*	Bis zu 366 m*	Bis zu 425 m*
Vorzug	Bekannt – verbreitet bei der gemeinsamen Internetnutzung	Bessere Funkabdeckung und gleichmäßige Übertragungsgeschwindigkeit	Höhere Geschwindigkeit und bessere Funkabdeckung	Brandneu – beste Funkabdeckung und Durchsatzleistung

*Reichweite und Verbindungsgeschwindigkeit sind abhängig von Ihrer Netzwerkumgebung.

**Dieser Router ist kompatibel mit Produkten derselben Version des Entwurfs des 802.11n-Standards; ein Software-Upgrade kann für die beste Leistung erforderlich sein.

Technische Support Informationen

Kostenloser technischer Support* *Zum normalen

Telefontarif

www.belkin.com

Technische Informationen und Unterstützung erhalten Sie auf unserer Website: www.belkin.com im Bereich Tech-Support. Wenn Sie den technischen Support telefonisch erreichen wollen, wählen Sie die entsprechende Nummer auf der unten aufgeführten Liste *.

LAND	NUMMER	INTERNET-ADRESSE
ÖSTERREICH	0820 200766	www.belkin.com/uk/networking/
BELGIEN	07 07 00 073	www.belkin.com/nl/networking/
TSCHECHISCHE	239 000 406	www.belkin.com/uk/networking/
DÄNEMARK	701 22 403	www.belkin.com/uk/networking/
FINNLAND	097 25 19 123	www.belkin.com/uk/networking/
FRANKREICH	08 - 25 54 00 26	www.belkin.com/fr/networking/
DEUTSCHLAND	0180 - 500 57 09	www.belkin.com/de/networking/
GRIECHENLAND	00800 - 44 14 23 90	www.belkin.com/uk/networking/
UNGARN	06 - 17 77 49 06	www.belkin.com/uk/networking/
ISLAND	800 8534	www.belkin.com/uk/networking/
IRLAND	0818 55 50 06	www.belkin.com/uk/networking/
ITALIEN	02 - 69 43 02 51	www.belkin.com/it/support/tech/issues_more.asp
LUXEMBURG	34 20 80 85 60	www.belkin.com/uk/networking/
NIEDERLANDE	0900 - 040 07 90	0,10 € pro www.belkin.com/nl/networking/
NORWEGEN	81 50 0287	www.belkin.com/uk/networking/
POLEN	00800 - 441 17 37	www.belkin.com/uk/networking/
PORTUGAL	707 200 676	www.belkin.com/uk/networking/
RUSSLAND	495 580 9541	www.belkin.com/networking/
SÜDAFRIKA	0800 - 99 15 21	www.belkin.com/uk/networking/
SPANIEN	902 - 02 43 66	www.belkin.com/es/support/tech/networkingsupport.asp
SCHWEDEN	07 - 71 40 04 53	www.belkin.com/se/support/tech/networkingsupport.asp
SCHWEIZ	08 - 48 00 02 19	www.belkin.com/uk/networking/
GROSSBRITANNIEN	0845 - 607 77 87	www.belkin.com/uk/networking/
SONSTIGE LÄNDER	+44 - 1933 35 20 00	

IP-Adresse

Diese „IP-Adresse“ ist die interne IP-Adresse des Routers. Um die erweiterte Konfigurationsoberfläche zu öffnen, geben Sie diese IP-Adresse in die Adresszeile Ihres Browsers ein. Bei Bedarf können Sie die Adresse ändern. Geben Sie hierzu die neue IP-Adresse ein, und klicken Sie auf „Apply Changes“ (Änderungen übernehmen). Achten Sie darauf, dass Sie eine nicht routbare IP-Adresse wählen. Beispiele für nicht routbare IP-Adressen:

192.168.x.x (x steht für eine Zahl zwischen 0 und 255)

10.x.x.x (x steht für eine Zahl zwischen 0 und 255)

Subnetz-Maske

Viele Netzwerke sind zu groß, um den Datenverkehr in alle ihre Bereiche zuzulassen. Diese Netzwerke müssen in kleinere, überschaubarere Abschnitte aufgeteilt werden, sogenannte „Subnets“ (Subnetze). Die Subnetz-Maske ist die Netzwerkadresse plus der Information, die für die Identifizierung des „subnetwork“ (Subnetzwerk) reserviert ist.

DNS

DNS ist die Abkürzung für Domain Name Server (Domännennamen-Server). Als DNS (Domain Name Server) wird ein Server im Internet bezeichnet, der URLs (Universal Resource Links) wie „www.belkin.com“ zu IP-Adressen umwandelt. Bei vielen Providern ist eine Eingabe dieser Informationen in den Router unnötig. Wenn Sie einen statischen Verbindungstyp verwenden, müssen Sie möglicherweise eine bestimmte DNS-Adresse sowie eine sekundäre DNS-Adresse angeben, damit die Verbindung ordnungsgemäß funktioniert. Wenn Sie mit einem dynamischen Verbindungstyp oder PPPoE arbeiten, müssen Sie wahrscheinlich keine DNS-Adresse eingeben.

PPPoE

Die meisten DSL-Anbieter nutzen den Verbindungstyp PPPoE. Wenn Sie per ADSL-Modem mit dem Internet verbunden sind, erfolgt die Anmeldung an den Service des Providers möglicherweise über PPPoE.

Ihr Verbindungstyp ist PPPoE, wenn folgende Voraussetzungen zutreffen:

1. Ihr Provider hat Ihnen einen Benutzernamen und ein Kennwort für die Verbindung zum Internet zugewiesen.
2. Ihr Internetprovider hat Ihnen für die Internetverbindung Software wie WinPOET oder Enternet300 geliefert.
3. Sie müssen auf ein Desktop-Symbol doppelklicken (zusätzlich zum Browser), um ins Internet zu gelangen.

Um den Router auf PPPoE einzurichten, geben Sie in den entsprechenden Feldern Ihren Benutzernamen und Ihr Kennwort ein. Klicken Sie nach der Eingabe Ihrer Informationen auf „Apply Changes“ (Änderungen übernehmen).

Wenn Sie die Einstellungen übernommen haben, meldet die Statusanzeige „connection OK“ (Verbindung OK), wenn der Router korrekt konfiguriert wurde.

PPPoA

Geben Sie die PPPoA Informationen in die vorgegebenen Felder und klicken Sie auf „Next“ (Weiter). Klicken Sie auf „Apply“ (Übernehmen), um Ihre Einstellungen zu aktivieren.

1. Benutzername - Geben Sie den Benutzernamen ein. (Vom Internetprovider vergeben).
2. Kennwort - Geben Sie Ihr Kennwort ein. (Vom Internetprovider vergeben).
3. Kennwort erneut eingeben - Bestätigen Sie das Kennwort. (Vom Internetprovider vergeben).
4. VPI/VCI - Geben Sie Ihren Virtual Path Identifier (Virtuelle Pfaderkennung - VPI) und Virtual Circuit Identifier (Virtuelle Circuiterkennung - VCI) hier ein. (Vom Internetprovider vergeben).

Trennen nach X...

Die Funktion „Disconnect“ dient zur automatischen Trennung des Routers vom Internet, wenn eine bestimmte Zeit lang keine Aktivität mehr festgestellt wird. Wenn Sie diese Option aktivieren und zum Beispiel „5“ in das Feld „Minute“ eingeben, wird der Router nach fünf Minuten Inaktivität vom Internet getrennt.

Diese Option sollte nur verwendet werden, wenn Ihre Internet-Nutzung nach Zeit abgerechnet wird.

Kanal und SSID

Sie können den Betriebskanal des Routers wechseln. Wählen Sie hierzu den gewünschten neuen Kanal aus dem Dropdown-Menü. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Einstellung zu sichern. Sie können auch die SSID ändern. Die SSID entspricht dem Namen des kabellosen Netzwerks. Sie können die SSID frei festlegen. Wenn sich in der näheren Umgebung weitere kabellose Netzwerke befinden, müssen Sie dem Netzwerk einen eindeutigen Namen zuweisen. Klicken Sie in das SSID-Feld und geben Sie einen neuen Namen ein. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Änderung zu speichern.

ESSID Broadcast

Viele kabellose Netzwerkadapter, die zur Zeit auf dem Markt sind, verfügen über eine Funktion namens Standortübersicht. Sie überprüft die Umgebung nach verfügbaren Netzwerken und ermöglicht jedem Computer, automatisch ein Netzwerk in der Umgebung auszuwählen. Dies geschieht, wenn die SSID des Computers auf „ANY“ (ALLE) steht. Ihr Belkin Router kann diese Zufallssuche nach einem Netzwerk blockieren. Wenn Sie die Funktion „ESSID Broadcast“ deaktivieren, kann Ihr Computer nur dann in das Netzwerk, wenn seine SSID auf den Namen des Netzwerkes (wie WLAN) eingestellt wurde. Bevor Sie diese Option nutzen, sollten Sie sich vergewissern, dass Sie Ihre SSID (den Netzwerknamen) kennen. Sie können Ihr kabelloses Netzwerk fast unsichtbar machen. Wenn Sie das Rundsenden der SSID deaktivieren, wird Ihr Netzwerk nicht in Standortübersichten aufgenommen. Wenn Sie die Rundsendung der SSID deaktivieren, verbessern Sie die Netzwerksicherheit.

Verschlüsselung

Mit einer Verschlüsselung können Sie die Sicherheit Ihres Netzwerks verbessern. Der Router benutzt zwei Arten von Wired Equivalent Privacy (WEP)-Verschlüsselung, um Ihre Daten und Funktionen zu schützen: 64- oder 128-Bit. Verschlüsselung basiert auf mehreren Codeschlüsseln. Der Schlüssel des Computers muss mit dem des Routers übereinstimmen und es gibt zwei Arten, einen Schlüssel zu erstellen. Die einfachste, ist die Software des Routers zum Umwandeln eines von Ihnen gewählten Kennwortes in einen Schlüssel zu benutzen. Alternativ hierzu können die Schlüssel auch manuell festgelegt werden.

Anwendungs-Gateways

Anhand von Anwendungs-Gateways können Sie spezielle Ports festlegen, die für bestimmte Anwendungen offen bleiben, damit die Interaktion mit der NAT-Funktion (Netzwerkadressübersetzung) des Routers ordnungsgemäß funktioniert. Eine Liste populärer Anwendungen wurde beigefügt. Sie können eine Anwendung in der Liste der populären Anwendungen auswählen. Ihre Auswahl wird in den Router einprogrammiert. Wählen Sie die Reihe, aus der Sie die Einstellungen kopieren möchten sowie die Reihe, in die Sie kopieren möchten in der Drop-Down-Liste aus und klicken Sie anschließend auf „=„Copy To“ (Kopieren). Die Einstellungen werden in die angegebene Zeile übertragen. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Einstellungen für diese Anwendung zu sichern. Wenn Sie Ihre Anwendung nicht finden, müssen Sie beim Hersteller der Anwendung nachfragen, welche Ports für diese eingestellt werden müssen. Sie können die Port-Informationen manuell in den Router eingeben.

Virtuelle Server

Mit dieser Funktion können Sie externe Aufrufe (aus dem Internet) von Diensten wie Webserver (Port 80), FTP-Server (Port 21) und andere Anwendungen über Ihren Router in das interne Netzwerk umleiten. Da Ihre internen Computer durch eine Firewall geschützt sind, kann auf diese aus dem Internet nicht zugegriffen werden, weil sie dort nicht „sichtbar“ sind. Wenn Sie die virtuelle Serverfunktion für eine bestimmte Anwendung einstellen müssen, sollten Sie Kontakt zum Hersteller des Programms aufnehmen, um dort zu erfahren, welche Port-Einstellungen Sie vornehmen müssen.

Für die manuelle Eingabe, geben Sie die IP-Adresse in das vorgegebene Feld für interne Geräte, den Port Typ (TCP oder UDP) sowie die LAN und öffentlichen Ports, die passiert werden müssen, ein. Wählen Sie dann „Enable“ (Aktivieren) und „Set“ (Eingestellt). Sie können pro interner IP-Adresse nur einen Port freigeben. Das Öffnen von Ports in Ihrer Firewall kann ein Sicherheitsrisiko darstellen. Das Aktivieren und Deaktivieren von Einstellungen geht schnell von der Hand. Daher sollten Sie die Einstellungen deaktivieren, wenn Sie eine bestimmte Anwendung momentan nicht verwenden.

Client-IP-Filter

Sie können den Router so einstellen, dass der Zugriff auf das Internet, E-

Mail oder andere Netzwerke auf bestimmte Tage und Zeiten beschränkt wird. Die Beschränkung kann für einen einzelnen oder mehrere Computer festgelegt werden.

URL-Filter

Verwenden Sie zur Konfigurierung der URL-Blockierfunktion die nachstehende Tabelle, um die Websites festzulegen (www.einewebsite.com) und/oder die Schlüsselwörter zu bestimmen, die Sie in Ihrem Netzwerk herausfiltern möchten. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Änderung zu aktivieren. Um diese Konfiguration zu beenden, müssen Sie eine Zugriffsregel im Abschnitt „Client-IP-Filter“ erstellen oder bearbeiten. Um eine bestehende Regel zu bearbeiten, klicken Sie neben der Regel auf „Edit“ (Bearbeiten). Um eine neue Regel zu erstellen, klicken Sie auf die Option „Add PC“ (PC hinzufügen). Aktivieren Sie in der Dienstabellen der Client-PCs im Abschnitt „Access Control > Add PC“ (Zugriffskontrolle > PC hinzufügen) die Option für „WWW with URL Blocking“ (WWW mit URL-Filter), um die ausgewählten Internetseiten und Schlüsselwörter herauszufiltern.

Zeitplanregel

Um die Zeitplanregel einzustellen, geben Sie den Namen, eine Beschreibung und die Beginn- und Endzeit an, in der Ihr Netzwerk gefiltert werden soll. Diese Seite definiert die Zeitplanregel und aktiviert den Zeitplan für den Gebrauch auf der Seite „Access Control“ (Zugriffskontrolle).

MAC Adress-Filter

Der MAC-Adressfilter ist eine leistungsstarke Sicherheitsfunktion, mit der Sie festlegen können, welche Computer für das Netzwerk zugelassen sind. Computern, die nicht in der Filterliste verzeichnet sind, wird der Zugriff auf das Netzwerk verweigert. Wenn Sie diese Funktion aktivieren, müssen Sie die MAC-Adresse jedes Clients aus Ihrem Netzwerk angeben, um den Netzwerkzugriff für diesen zu ermöglichen oder die MAC-Adresse kopieren, indem Sie den Namen des Computers aus der „DHCP Client-Liste“ auswählen. Um diese Funktion zu aktivieren, wählen Sie „Enable“ (Aktivieren). Klicken Sie dann auf „Apply Changes“ (Änderungen übernehmen), um die Einstellungen zu speichern.

DMZ

Wenn Sie einen Client-PC haben, auf dem hinter der Firewall keine Internetanwendung richtig ausgeführt werden kann, können Sie den Client für ungehinderten Internetzugriff einstellen. Das kann erforderlich sein, wenn die NAT-Funktion bei einer Anwendung Probleme verursacht, zum Beispiel bei einem Spiel oder einer Videokonferenzanwendung. Verwenden Sie diese Funktion nur zeitweise. Der DMZ-Computer ist nicht vor Hacker-Angriffen geschützt. Um einen Computer in die DMZ zu versetzen, geben Sie die letzten Ziffern der LAN-IP-Adresse in das Feld für die statische IP-Adresse ein und klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Änderungen zu aktivieren.

Haben Sie nur eine öffentliche (WAN) IP-Adresse, können Sie diese öffentliche IP auf „0.0.0.0“ stehen lassen. Wenn Sie mehrere öffentliche (WAN)-IP-Adressen verwenden, können Sie wählen, welche öffentliche (WAN)-IP-Adresse dem DMZ-Host zugewiesen werden soll. Geben Sie die öffentliche (WAN)-IP-Adresse ein, zu der der DMZ-Host umgeleitet werden soll, geben Sie die beiden letzten Ziffern der IP-Adresse des DMZ-Host-Computers ein und klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Administratorkennwort

Der Router wird OHNE festgelegtes Kennwort geliefert. Wenn Sie zur Sicherheit ein Kennwort angeben möchten, können Sie dieses auf der webgestützten Benutzeroberfläche des Routers einstellen. Bewahren Sie das Kennwort sicher auf. Sie benötigen es, wenn Sie sich künftig am Router anmelden möchten. Es wird DRINGEND EMPFOHLEN ein Kennwort festzulegen, wenn Sie die Fernverwaltung des Routers benutzen wollen. Das Zeitlimit für die Anmeldung ermöglicht Ihnen, einen Zeitraum zu bestimmen, in dem Sie für die erweiterte Konfigurationsoberfläche des Routers angemeldet sind. Die Zähluhr startet, wenn keine Aktivität mehr registriert wird. Beispiel: Sie haben Änderungen mit der erweiterten Konfigurationsoberfläche vorgenommen und verlassen Ihren Arbeitsplatz, ohne auf „Logout“ (Abmelden) zu klicken.

Angenommen, das Zeitlimit ist auf 10 Minuten eingestellt. Dann läuft die Anmeldesitzung 10 Minuten nach dem Verlassen ab. Sie müssen sich dann erneut anmelden, um weitere Änderungen durchzuführen. Das Zeitlimit für die Anmeldung dient der Sicherheit und ist auf 10 Minuten voreingestellt. Es kann jeweils nur ein Computer an der erweiterten Konfigurationsoberfläche zur Routerkonfiguration angemeldet sein.

Uhrzeit und Zeitzone

Der Router hält die Uhrzeit auf dem Laufenden, indem er sich mit einem Simple Network Time Protocol (SNTP)-Server verbindet. Dadurch kann der Router die Systemuhr mit dem weltweiten Internet synchronisieren. Die synchronisierte Routeruhr dient zur Aufzeichnung des Sicherheitsprotokolls und zur Steuerung des Client-Filters. Wählen Sie die Zeitzone, in der Sie sich befinden. Wenn Sie sich in einer Region befinden, in der zwischen Sommer- und Winterzeit umgestellt wird, markieren Sie das Feld neben „Enable Daylight Saving“ (Sommerzeit aktivieren). Die Systemuhr wird nicht immer sofort aktualisiert.

Sie müssen mindestens 15 Minuten abwarten, bis der Router die Zeitserver im Internet abfragt und eine Antwort erhält. Sie können die Uhr nicht selbst einstellen.

Fernverwaltung

Bevor Sie diese Funktion aktivieren, SOLLTEN SIE UNBEDINGT EIN ADMINISTRATORKENNWORT FESTLEGEN. Die Fernverwaltung ermöglicht das Ändern Ihrer Routereinstellungen von jedem Ort aus, an dem sich ein Internetanschluss befindet.

1

2

3

4

5

6

7

8

9

10

11

Anhang B: Wichtige Faktoren bei Aufstellung und Einrichtung

UPnP

Die UPnP-Technologie (Universales Plug&Play) ermöglicht den nahtlosen Betrieb von Sprach- und Videomeldungen, Spielen und anderen Anwendungen, die dem UPnP-Standard entsprechen. Für bestimmte Anwendungen muss die Router-Firewall auf eine ganz bestimmte Weise konfiguriert werden, damit sie störungsfrei funktionieren. Hierzu müssen meistens TCP- und UDP-Ports geöffnet und in bestimmten Fällen auch Trigger-Ports gesetzt werden. UPnP-kompatible Anwendungen können mit dem Router kommunizieren und ihm mitteilen, wie die Firewall konfiguriert werden muss. Werkseitig ist die UPnP-Funktion des Routers deaktiviert. Wenn Sie UPnP-kompatible Anwendungen einsetzen und die UPnP-Funktionen nutzen möchten, können Sie die UPnP-Option aktivieren. Wählen Sie hierzu auf der Seite „Utilities“ (Dienstprogramme) im Abschnitt „UPnP Enabling“ (UPnP-Aktivierung) die Option „Enable“ (Aktivieren). Klicken Sie auf „Apply Changes“ (Änderungen übernehmen), um die Änderung zu speichern.

Hinweis: Obwohl manche der folgenden Faktoren die Funktion Ihres Netzwerks beeinträchtigen können, werden Sie Ihr kabelloses Netzwerk nicht völlig funktionsunfähig machen. Wenn Sie vermuten, dass Ihr Netzwerk nicht optimal funktioniert, kann Ihnen diese Kontrollliste helfen.

1. Aufstellung des kabellosen Routers oder Access Points

Stellen Sie Ihren kabellosen Router, den zentralen Verbindungspunkt Ihres Netzwerks, soweit wie möglich in den Mittelpunkt Ihrer kabellosen Netzwerkgeräte. Um den besten Empfang für Ihre „kabellosen Clients“ (d. h. Computer, die mit kabellosen Notebook- oder Desktop-Netzwerkkarten von Belkin oder kabellosen USB-Adaptern ausgestattet sind) zu bekommen:

- Stellen Sie sicher, dass die Antennen des kabellosen Routers (oder Access Points) parallel zueinander ausgerichtet und vertikal aufgestellt sind (mit Ausrichtung auf die Decke). Wenn Ihr kabelloser Router (oder Access Point) vertikal aufgestellt ist, richten Sie die Antennen soweit wie möglich nach oben aus.
- Wenn sich Ihr Wohnraum über mehrere Etagen erstreckt, stellen Sie den kabellosen Router (oder Access Point) in einem Stockwerk auf, das im Gesamtwohnraum so zentral wie möglich gelegen ist. Dies kann bedeuten, dass Sie den kabellosen Router (oder Access Point) in einem der oberen Stockwerke aufstellen müssen.
- Stellen Sie den kabellosen Router (oder Access Point) nicht in der Nähe eines schnurlosen Telefons, das das 2,4-GHz-Band nutzt, auf.

2. Vermeiden Sie Hindernisse und Störungsquellen

Vermeiden Sie es, Ihren kabellosen Router (oder Access Point) in der Nähe von Geräten, die elektromagnetische Strahlung abgeben (z.B. Mikrowellenherde), aufzustellen Objekte, die die kabellose Kommunikation behindern können sind z.B.:

- Kühlschränke

Anhang B: Wichtige Faktoren bei Aufstellung und Einrichtung

- Waschmaschinen und/oder Wäschetrockner
- Aktenschränke aus Metall
- Große Aquarien
- UV-Beschichtung von Fenstern auf Metallbasis

Wenn das Funksignal Ihrer kabellosen Verbindung an manchen Stellen schwach ist, sorgen Sie dafür, dass solche Objekte den Weg des Funksignals nicht blockieren (zwischen Ihren Computern und dem kabellosen Router oder Access Point).

3. Schnurlose Telefone

Wenn die Leistung Ihres kabellosen Netzwerks noch beeinträchtigt wird, nachdem Sie die oben genannten Hinweise beachtet und aber ein schnurloses Telefon haben:

- Versuchen Sie die schnurlosen Telefone aus der Nähe von kabellosen Routern (oder Access Points) und Ihren Computern, die für kabellose Vernetzung ausgerüstet sind, zu entfernen.
- Entfernen Sie die Batterie jedes schnurlosen Telefons, das im Frequenzband 2,4 GHz arbeitet, und ziehen Sie den Stecker am Anschluss heraus (Sehen Sie sich hierzu die Informationen des Herstellers an). Wenn das Problem dadurch behoben wird, ist Ihr Telefon möglicherweise der Auslöser der Störung.
- Wenn Sie Ihr Telefon über eine Kanalauswahl verfügt, wählen Sie einen Kanal für Ihr Telefon aus, der soweit wie möglich von dem Kanal Ihres kabellosen Netzwerks entfernt ist. Stellen Sie z. B. den Kanal Ihres Telefons auf 1 ein und den des kabellosen Routers oder Access Points auf 11. Mehr Informationen hierzu finden Sie im Benutzerhandbuch Ihres Telefons.
- Wenn es nötig ist, überlegen Sie sich, ein schnurloses Telefon anzuschaffen, das mit 900 MHz oder 5 GHz funktioniert.

4. Wählen Sie den „ruhigsten“ Kanal für Ihr kabelloses Netzwerk

An Orten, an denen es eine hohe Konzentration an Wohnräumen und Büros gibt, wie z. B. in Wohnblocks oder Bürogebäuden, kann Ihr kabelloses Netzwerk durch andere Netzwerke gestört werden.

Benutzen Sie die Standortübersicht (Site Survey) Ihres LAN-Programms für kabellose Netzwerke, um andere kabellose Netzwerke ausfindig zu machen, und stellen Sie Ihren kabellosen Router (oder Access Point) und Ihre Computer auf einen Kanal ein, der soweit wie möglich von den anderen Netzwerken entfernt ist.

Probieren Sie mehr als einen der möglichen Kanäle aus, um herauszufinden, welche Verbindung die beste ist, und um Störungen durch schnurlose Telefone oder andere kabellose Geräte in der Umgebung zu vermeiden.

Wenn Sie kabellose Netzwerkprodukte benutzen, die nicht von Belkin sind, benutzen Sie die detaillierte Standortübersicht (Site survey) und die Informationen über Kanäle für kabellose Geräte in Ihrem Benutzerhandbuch.

1

2

3

4

5

6

7

8

9

10

11

Kapitel

Anhang B: Wichtige Faktoren bei Aufstellung und Einrichtung

Diese Richtlinien sollten Ihnen helfen, den größtmöglichen Bereich mit Ihrem kabellosen Router (oder Access Point) abzudecken. Wenn Sie einen größeren Bereich abdecken müssen, empfehlen wir Ihnen den Kabellosen Range Extender/ Access Point von Belkin.

5. Sichere Verbindungen, VPNs und AOL

Sichere Verbindungen sind Verbindungen, für die normalerweise ein Benutzernamen mit Kennwort erforderlich ist. Sie werden überall benutzt, wo großer Wert auf Sicherheit gelegt wird. Zu sicheren Verbindungen zählen folgende:

- Virtual Private Network (VPN) Verbindungen, die oft benutzt werden, um auf Entfernung eine Verbindung mit einem Büronetzwerk herzustellen
- Das „Bring Your Own Access“-Programm von America Online (AOL), das Ihnen die Benutzung von AOL mit Breitband durch Kabel oder DSL-Service ermöglicht
- Die meisten Internetseiten für Bankangelegenheiten
- Viele kommerzielle Internetseiten, für die ein Benutzername und ein Kennwort erforderlich sind, um Ihnen Zugang zu Ihrem Konto zu verschaffen

Sichere Verbindungen können durch die Einstellung der Energieverwaltung (Power Management) eines Computers unterbrochen werden, die den „Ruhezustand“ aktiviert. Die einfachste Möglichkeit, dies zu vermeiden, ist die Herstellung einer neuen Verbindung, indem Sie die VPN- oder AOL-Software neu starten oder sich wieder auf einer sicheren Internetseite einloggen.

Eine zweite Möglichkeit ist die Änderung der Einstellungen der Energieverwaltung, so dass der Ruhezustand deaktiviert ist; dies ist allerdings bei tragbaren Computern weniger angebracht. Wenn Sie die Einstellungen der Energieverwaltung unter Windows ändern wollen, sehen Sie in der Systemsteuerung unter „Power Options“ (Energieoptionen) nach.

Wenn Sie weiterhin Probleme mit sicheren Verbindungen, VPNs oder AOL haben, beachten Sie bitte erneut die Schritte oben, um sicherzustellen, dass Sie die angesprochenen Aspekte berücksichtigt haben.

KONFORMITÄTSERKLÄRUNG ZUR EINHALTUNG DER FCC-BESTIMMUNGEN ÜBER ELEKTROMAGNETISCHE KOMPATIBILITÄT

Wir, Belkin International, Inc., 501 West Walnut Street, Compton, CA 90220, USA, erklären hiermit alleinverantwortlich, dass der Artikel,

F5D7632uk4A

auf den sich diese Erklärung bezieht, Abschnitt 15 der FCC-Bestimmungen entspricht. Der Betrieb unterliegt den beiden folgenden Bedingungen: (1) Dieses Gerät darf schädigende Störungen nicht verursachen, und (2) dieses Gerät muss jedwede Störung annehmen, einschließlich der Störungen, die einen unerwünschten Betrieb verursachen könnten.

Achtung: Hochfrequente Strahlungen

Die Strahlungsleistung dieses Geräts liegt deutlich unter den FCC-Grenzwerten für hochfrequente Strahlungen. Dennoch ist bei der Gerätenutzung darauf zu achten, dass im Normalbetrieb Menschen möglichst wenig schädlichen Strahlungen ausgesetzt werden. Beim Anschluss einer externen Antenne an das Gerät muss die Antenne so aufgestellt werden, dass im Normalbetrieb Menschen möglichst wenig mit schädlichen Strahlungen in Berührung kommen. Um sicherzustellen, dass die FCC-Grenzwerte für Belastungen durch hochfrequente Strahlungen nicht überschritten werden, ist im Normalbetrieb stets ein Abstand von mindestens 20 cm zur Antenne einzuhalten.

FCC-Hinweis

Dieses Gerät entspricht nachweislich den Grenzwerten für digitale Geräte der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte dienen dem angemessenen Schutz vor schädlichen Strahlungen beim Betrieb von Geräten im Wohnbereich.

Das Gerät erzeugt und verwendet hochfrequente Strahlungen und kann sie ausstrahlen. Verursacht dieses Gerät Störungen des Radio- oder Fernsehempfangs (was sich durch Ein- und Ausschalten des Gerätes feststellen lässt), so können Sie versuchen, die Störung auf folgende Weise zu beseitigen:

- Neuausrichtung oder Standortänderung der Empfangsantenne
- Vergrößern des Abstands zwischen Gerät und Empfänger
- Anschluss des Geräts an eine Steckdose in einem anderen Stromkreis als dem des Empfängers
- Den Händler oder einen erfahrenen Rundfunk- und Fernsehtechniker hinzuziehen

Anpassungen

Nach den Vorschriften der FCC muss dem Benutzer mitgeteilt werden, dass Änderungen oder Modifikationen an diesem Gerät, die nicht ausdrücklich von Belkin International, Inc. genehmigt wurden, dazu führen können, dass die Berechtigung des Benutzers zum Betrieb des Geräts erlischt.

Canada-Industry Canada (IC)

Das Funksystem dieses Geräts entspricht den Bestimmungen RSS 139 und RSS 210 von Industry Canada. Dieses digitale Gerät der Klasse B entspricht der kanadischen Norm ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Europa: CE-Hinweis

Die Kennzeichnung von Endeinrichtungen mit dem Zeichen CE 0682 oder dem CE-Hinweis gibt an, dass das Gerät der Richtlinie 1999/5/EG (R&TTE-Richtlinie) der EU-Kommission entspricht.

Aus der Einhaltung dieser Richtlinien geht hervor, dass das Gerät den folgenden europäischen Normen entspricht (in Klammern die entsprechenden internationalen Standards):

- EN 60950 (IEC60950) – Produktsicherheit
 - EN 300 328 Technische Anforderungen an funktechnische Einrichtungen
 - ETS 300 826 Allgemeine EMV-Anforderungen an funktechnische Einrichtungen
- Den Sendertyp finden Sie auf dem Produkterkennungsschild Ihres Belkin-Produkts.

Produkte mit dem CE-Zeichen entsprechen der Richtlinie zur Elektromagnetischen Verträglichkeit (89/336/EWG) und der Niederspannungsrichtlinie

(72/23/EWG) der EU-Kommission. Aus der Einhaltung dieser Richtlinien geht hervor, dass das Gerät den folgenden europäischen Normen entspricht (in Klammern die entsprechenden internationalen Standards).

- EN 55022 (CISPR 22) – Funkstörungen
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) - Elektromagnetische Immunität
- EN 61000-3-2 (IEC610000-3-2) - Oberschwingungsströme
- EN 61000-3-3 (IEC610000) – Grenzwerte für Spannungsschwankungen und Flicker
- EN 60950 (IEC60950) – Produktsicherheit

Produkte mit diesem Sender werden mit dem CE 0682 oder CE-Hinweis versehen und sind ggf. auch mit dem CE-Zeichen gekennzeichnet.



BELKIN.

EC Declaration of Conformity to R&TTE Directive 1999/5/EC

Manufacturer : BELKIN LTD,
EXPRESS BUSINESS PARK,
SHIPTON WAY
,RUSHDEN
NN10 6GL ENGLAND

Representative : Belkin Ltd
(residing in the EC
holding the TCF)

Product / Apparatus : ADSL Modem/Wireless G Router

Type Number : F5D7632-4

Variants include : All Country Variants

Declaration

I declare that above product conforms to all the applicable requirements of EU Directive 1999/5/EC and is CE-marked accordingly:

Article 3.1a: (Standard(s)) used to show compliance with LVD, 73/23/EEC:
IEC 60950-1 2001 Compliant Test Report No: LD931001H03 03 NOV 04

Article 3.1b: (Standard(s)) used to show compliance with EMC Directive, 89/336/EEC:
EN301 489-1 V1.4.1 (2002-08);EN 301 489-17 V1.2.1 (2002-08) Compliant Test Report
No:RM931001H03

Article 3.2: Standard(s) used to show compliance:
...EN300 328 V1.4.1 (2003-04)..... Compliant Test Report No:RC93100H03

Signature : 

Name : K Simpson

Title : European Regulatory Compliance Manager

Date : 20 MAR 2006

Eingeschränkte lebenslange Produktgarantie von Belkin International, Inc.

Garantieleistung.

Belkin International, Inc., garantiert dem ursprünglichen Käufer dieses Belkin-Produkts, dass dieses Produkt frei von Material-, Verarbeitungs-, und Konstruktionsfehlern ist.

Garantiedauer.

Belkin International, Inc. gewährt für dieses Belkin-Produkt eine lebenslange Garantie.

Problembhebung.

Herstellergarantie.

Belkin wird das Produkt nach eigenem Ermessen entweder kostenlos (abgesehen von den Versandkosten) reparieren oder austauschen.

Garantieausschluss.

Alle oben genannten Garantien verlieren ihre Gültigkeit, wenn das Belkin-Produkt von Belkin International, Inc., auf Anfrage nicht auf Kosten des Käufers zur Überprüfung zur Verfügung gestellt wird oder wenn Belkin International, Inc., feststellt, dass das Belkin-Produkt nicht ordnungsgemäß installiert worden ist, und dass unerlaubte Änderungen daran vorgenommen worden sind. Die Herstellergarantie von Belkin gilt nicht für (Natur)gewalten wie Überschwemmungen, Erdbeben und Blitzschlag sowie Krieg, Vandalismus, Diebstahl, normalen Verschleiß, Erosion, Wertminderung, Veralterung, schlechte Behandlung, Beschädigung durch Störungen aufgrund von Unterspannung (z. B. Spannungsabfall oder -Senkung) oder nicht erlaubte Programm- oder Systemänderungen.

Service.

Um Unterstützung von Belkin zu bekommen, gehen Sie nach folgenden Schritten vor:

1. Schreiben Sie an Belkin International, Inc., 501 W. Walnut St., Compton CA 90220, Attn: Customer Service oder wenden Sie sich innerhalb von 15 Tagen nach dem Vorfall telefonisch unter (800)-223-5546 an Belkin. Halten Sie die folgenden Informationen bereit:
 - a. Die Artikelnummer des Belkin-Produkts.
 - b. Wo Sie das Produkt erworben haben.
 - c. Das Kaufdatum.
 - d. Kopie der Originalquittung.
2. Die entsprechenden Mitarbeiter/innen informieren Sie darüber, wie Sie Ihre Rechnung und das Belkin-Produkt versenden müssen und wie Sie fortfahren müssen, um Ihre Ansprüche geltend zu machen.

Belkin International, Inc., behält sich vor, das beschädigte Belkin-Produkt zu überprüfen. Alle Kosten, die beim Versand des Belkin-Produkts an Belkin International, Inc. zum Zweck der Überprüfung entstehen, sind vollständig durch den Käufer zu

tragen. Wenn Belkin nach eigenem Ermessen entscheidet, dass es unpraktisch ist, das beschädigte Gerät an Belkin International, Inc., zu schicken, kann Belkin nach eigenem Ermessen eine Reparaturstelle damit beauftragen, das Gerät zu überprüfen und einen Kostenvoranschlag für die Reparaturkosten des Gerätes zu machen. Die Kosten für den Versand zu einer solchen Reparaturstelle und die eventuellen Kosten für einen Kostenvoranschlag gehen vollständig zu Lasten des Käufers. Beschädigte Geräte müssen zur Überprüfung zur Verfügung stehen, bis das Reklamationsverfahren abgeschlossen ist. Wenn Ansprüche beglichen werden, behält sich Belkin International, Inc. das Recht vor, Ersatzansprüche an eine bestehende Versicherung des Käufers zu übertragen.

Garantiesetze.

DIESE GARANTIE BILDET DIE ALLEINIGE GARANTIE VON BELKIN INTERNATIONAL, INC., WEITERE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNGEN WERDEN NICHT GEGEBEN, SOWEIT NICHT GESETZLICH VORGESCHRIEBEN, EINSCHLIESSLICH DER KONKLUDENTEN ZUSICHERUNG DER QUALITÄT, DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WOBEI ETWAIGE DERARTIGE KONKLUDENTE GEWÄHRLEISTUNGEN AUF DIE LAUFZEIT DIESER GARANTIE BESCHRÄNKT SIND.

In manchen Ländern sind Einschränkungen bezüglich der Dauer der Garantie nicht zulässig. Die oben erwähnten Einschränkungen treffen für Sie dementsprechend nicht zu.

UNTER KEINEN UMSTÄNDEN HAFTET BELKIN INTERNATIONAL, INC. FÜR ZUFÄLLIGEN, BESONDEREN, DIREKTEN, INDIREKTEN, MEHRFACHEN SCHADEN ODER FOLGESCHÄDEN WIE, ABER NICHT AUSSCHLIESSLICH, ENTGANGENES GESCHÄFT ODER PROFITE, DIE IHNEN DURCH DEN VERKAUF ODER DIE BENUTZUNG VON EINEM BELKIN-PRODUKT ENTGANGEN SIND, AUCH WENN SIE AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN AUFMERKSAM GEMACHT WORDEN SIND.

Diese Garantie räumt Ihnen spezifische Rechte ein, die von Land zu Land unterschiedlich ausgestaltet sein können. Da in manchen Ländern der Ausschluss oder die Beschränkung der Haftung für durch Zufall eingetretene oder Folgeschäden nicht zulässig ist, haben die vorstehenden Beschränkungen und Ausschlussregelungen für Sie möglicherweise keine Gültigkeit.



Informationen zur Entsorgung des Produkts finden Sie unter <http://environmental.belkin.com>

ZUR VERWENDUNG IN	AT	BE	CY	CZ	DK	EE	FI	FR	DE	GR	HU	IE		
IT	LV	LT	LU	MT	NL	PL	PT	SK	SI	ES	SE	GB	IS	LI
NO	CH	BG	RO	TR	BETRIEB AUF DEN KANÄLEN 1-13									

In bestimmten Ländern gelten bei der Verwendung Einschränkungen.....
Gerät der Klasse 2

BELKIN®

ADSL2+ Modem mit integriertem kabel- losen G Router

BELKIN®

www.belkin.com

Belkin Technischer Support

GB: 0845 607 77 87

Europa: www.belkin.com/support

Belkin Ltd.

Express Business Park
Shipton Way, Rushden
NN10 6GL, Großbritannien
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 Fax

Belkin SAS

130 rue de Silly
92100 Boulogne-Billancourt,
Frankreich
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 Fax

Belkin GmbH

Hanebergstraße 2
80637 München
Deutschland
+49 (0) 89 143405 0
+49 (0) 89 143405 100 Fax

Belkin Iberia

C/ Anabel Segura, 10 planta baja, Of. 2
28108, Alcobendas, Madrid
Spanien
+34 91 791 23 00
+34 91 490 23 35 Fax

Belkin Italy & Greece

Via Carducci, 7
Mailand 20123
Italien
+39 02 862 719
+39 02 862 719 Fax

Belkin B.V.

Boeing Avenue 333
1119 PH Schiphol-Rijk,
Niederlande
+31 (0) 20 654 7300
+31 (0) 20 654 7349 Fax

© 2007 Belkin International, Inc. Alle Rechte vorbehalten. Alle Produktnamen sind eingetragene Marken der angegebenen Hersteller. Mac, Mac OS, Apple und AirPort sind Marken der Apple, Inc., die in den USA und anderen Ländern eingetragen sind. Windows, NT, Microsoft und Windows Vista sind in den Vereinigten Staaten und/oder in anderen Ländern eingetragene Marken bzw. Marken der Microsoft Corporation.

P74725ea-A

BELKIN®

ADSL2+ modem met ingebouwde draad- loze G router

EN

FR

DE

NL

ES

IT



Handleiding

F5D7632ea4A

Inhoud

1. Inleiding	1
Productkenmerken	1
Voordelen van een netwerk in uw woning	3
Voordelen van een draadloos netwerk van Belkin	3
2. U dient over het volgende te beschikken	4
Inhoud van de verpakking	4
Systeemvereisten	4
Systeemvereisten voor de Setup-Assistent software	4
Internetverbindinginstellingen	4
3 Kennismaken met uw router	5
4 Uw router aansluiten en configureren	8
Stap 1A: Hardware aansluiten – Volg de aanwijzingen in de beknopte installatiehandleiding	8
Stap 1B: Een bestaande modem of modem/router vervangen	9
Stap 2: Installeer de router – Gebruik de Setup-Assistent software	10
5. Handmatige configuratie van de router	13
De werking van de geavanceerde web-based gebruikersinterface	13
LAN-instellingen wijzigen	15
DHCP-cliëntenlijst	16
Internet WAN	17
Type verbinding	17
Draadloos	23
Encryptie/Beveiliging	25
Uitbreiding van het bereik van het draadloze netwerk en bridging	35
Firewall	37
Hulpprogramma's	43
6. Handmatige configuratie van netwerkadapters	51
7. Aanbevolen instellingen van de webbrowser	55
8. Problemen oplossen	57
9. Technische ondersteuning	68
10. Appendices	69
Appendix A: Verklarende woordenlijst	69
Appendix B: Belangrijke factoren die een rol spelen bij plaatsing en installatie	74
11 Informatie	77

Dank u voor het aanschaffen van dit ADSL2+ modem met ingebouwde draadloze G router (de router) van Belkin. Binnen een paar minuten kunt u uw internetaansluiting delen en vormen uw computers met uw nieuwe router een netwerk. Hier volgen enkele productkenmerken die deze router de ideale oplossing maken voor uw netwerk thuis of op kantoor. Wij raden u aan deze handleiding volledig door te lezen en extra aandacht te besteden aan Appendix B, getiteld "Belangrijke factoren die een rol spelen bij plaatsing en setup".

Productkenmerken

Werkt zowel met PC's als Mac®-computers

De router ondersteunt een breed scala aan netwerkomgevingen waaronder Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP en Vista. U heeft een Internetbrowser nodig en een netwerkadaptor die TCP/IP (de standaard internettaal) ondersteunt.

LED-display frontpaneel

LED's aan de voorkant van de router geven aan welke functies zijn ingeschakeld. U kunt in één oogopslag zien of uw router verbinding heeft gemaakt met het Internet. Deze functie maakt gecompliceerde software en statuscontroleprocedures overbodig.

Geavanceerde web-based gebruikersinterface

U kunt de geavanceerde functies van de router eenvoudig instellen via uw webbrowser, zonder dat u extra software moet installeren op de computer. U hoeft geen disks te installeren of in de gaten te houden en bovendien kunt u snel en gemakkelijk wijzigingen aanbrengen en setupfuncties uitvoeren vanaf iedere op het netwerk aangesloten computer.

Geïntegreerde 4-poorts 10/100-switch

De router heeft een ingebouwde 4-poorts netwerkswitch waarmee uw bedrade computers onder meer printers, data, MP3-bestanden en digitale foto's kunnen delen. De switch stelt zich met behulp van auto-sensing automatisch in op de snelheid van de aangesloten apparaten. De switch kan gelijktijdig - zonder onderbrekingen en zonder beslag te nemen op bronnen - data verzenden tussen computers en het Internet.

Geïntegreerd draadloos 802.11g accesspoint

802.11g is een draadloze technologie die overdrachtssnelheden tot 54 Mbps mogelijk maakt. Dat is bijna vijf keer sneller dan 802.11b.

Ingebouwd Dynamic Host Configuration Protocol (DHCP)

Het ingebouwde Dynamic Host Configuration Protocol (DHCP) zorgt voor absoluut probleemloze netwerkverbindingen. De DHCP-server wijst automatisch aan elke computer IP-adressen toe waardoor een gecompliceerde netwerk-setup overbodig is.

NAT IP-adresdeling

Uw router maakt gebruik van Network Address Translation (NAT) voor het delen van het unieke IP-adres dat door uw Internet Service Provider aan u is toegewezen, terwijl u de kosten bespaart van het toevoegen van extra IP-adressen aan uw Internetservice-account.

SPI Firewall

Uw router is uitgerust met een firewall die uw netwerk beschermt tegen een groot aantal veel voorkomende aanvallen van hackers waaronder IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP met lengte nul, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect, en fragment flooding.

MAC-adresfilter

Als extra beveiliging kunt u een lijst aanleggen van Media Access Control (MAC) adressen (unieke cliënten-ID's) die toegang hebben tot uw netwerk. Elke computer heeft een eigen MAC-adres. U stelt eenvoudigweg - met behulp van de web-based gebruikersinterface - een lijst van deze MAC-adressen op en u hebt de toegang tot uw netwerk onder controle.

Compatibel met Universal Plug-and-Play (UPnP)

UPnP (Universal Plug-and-Play) is een technologie die naadloze werking van voice messaging, video messaging, games en andere applicaties mogelijk maakt die voldoen aan UPnP.

Ondersteuning voor VPN Pass-Through

Als u met behulp van een VPN-aansluiting van huis uit verbinding maakt met uw bedrijfsnetwerk, dan maakt uw router het mogelijk dat uw met VPN-functionaliteit uitgeruste computer via de router contact maakt met uw bedrijfsnetwerk.

Voordelen van een netwerk in uw woning

Als u de volgende eenvoudige installatie-instructies volgt, kunt u met uw thuisnetwerk van Belkin het volgende doen:

- Een high-speed Internetverbinding met alle computers in huis delen
- Bronnen als bestanden en harde schijven delen met alle aangesloten computers in huis
- Een printer met het hele gezin delen
- Documenten, muziek, videomateriaal en digitale foto's delen
- Bestanden opslaan, ophalen en kopiëren van de ene naar de andere computer
- Samen on-line games spelen, uw e-mail ophalen en bekijken en chatten

Voordelen van een draadloos netwerk van Belkin

Mobiliteit — een speciale computerruimte is voortaan overbodig; u kunt nu overal binnen de draadloze reikwijdte op een laptop- of desktopcomputer binnen het netwerk werken

Eenvoudige installatie — de Setup-Wizard van Belkin maakt installatie heel eenvoudig

Flexibiliteit — toegang tot printers, computers en andere netwerkapparatuur vanaf elke plek in uw woning

Eenvoudige uitbreiding — Belkin biedt u keus uit een complete reeks netwerkproducten die het u mogelijk maken uw netwerk uit te breiden met apparaten als printers en game-consoles

Bekabeling is niet nodig — u bespaart uzelf de kosten en de moeite die komen kijken bij het aanleggen van Ethernet-bekabeling in uw woning of kantoor

Algemeen aanvaard — keuze uit een groot aanbod van interoperabele netwerkproducten

U dient over het volgende te beschikken

Inhoud van de verpakking

- ADSL2+ modem met ingebouwde draadloze G router
- RJ11-telefoonkabel – grijs
- RJ45 Ethernet-netwerkkabel – geel
- ADSL-microfilter*
- Voedingsadapter
- Handleiding en Belkin Setup-Assistent software op cd

*Benodigde ADSL-microfilter verschilt per land en wordt niet in elk land meegeleverd. Als geen filter is meegeleverd, dient u er zelf een aan te schaffen.

Systeemvereisten

- Een actieve ADSL-lijn in combinatie met een telefoonaansluiting aan de muur, voor het aansluiten van de router
- Ten minste één computer met een netwerkinterfacekaart (NIC) en een internetbrowser die op de juiste wijze zijn geïnstalleerd en geconfigureerd
- TCP/IP-netwerkprotocol geïnstalleerd op alle computers die zijn aangesloten op de router
- Geen andere DHCP-server op uw lokale netwerk die IP-adressen aan computers en apparatuur toekent

Systeemvereisten voor de Setup-Assistent software

- Een PC met Windows® 2000, XP of Vista™ als besturingssysteem
- Minimaal een 500MHz-processor en 128 MB RAM
- Internetbrowser

Internetverbindinginstellingen

De Setup-Assistent bevat een database van Internet Service Providers (ISP's) in elke land, wat een snelle installatie van uw router mogelijk maakt. Als uw ISP niet in de lijst staat, vraag dan de volgende informatie bij uw ISP op voordat u de router installeert.

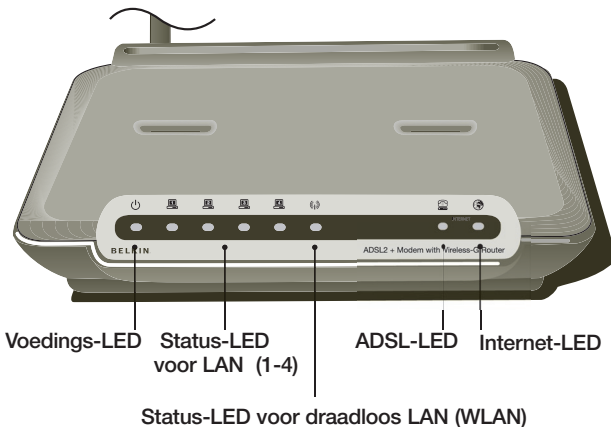
- Internetverbindingprotocol: (PPPoE, PPPoA, Dynamic IP, Static IP)
- Multiplexing-methode of encapsulatie: (LLC of VC MUX)
- Virtueel circuit: VPI (Virtual Path Identifier) _____
(een getal tussen 0 en 255)
- VCI (Virtual Channel Identifier) _____
(een getal tussen 1 and 65535)
- Voor PPPoE- en PPPoA-gebruikers: Gebruikersnaam en wachtwoord van uw ADSL-account _____
- Voor gebruikers van een statisch IP: IP Address ____ . ____ . ____ . ____
Subnetmasker ____ . ____ . ____ . ____
Standaard-gatewayserver ____ . ____ . ____ . ____
- IP-adres voor Domain Name Server ____ . ____ . ____ . ____
(Indien verstrekt door uw Internet Service Provider)

Kennismaken met uw router

De router is ontworpen voor plaatsing op een bureau of werktafel. Met het oog op praktische bruikbaarheid lopen alle kabels via de achterzijde van de router naar uw apparatuur. De LED's aan de bovenzijde van de router zijn goed zichtbaar en geven u informatie over de netwerkactiviteit en de status.

Voorzijde router




De afbeelding geeft het vooraanzicht van de router weer.



LED's

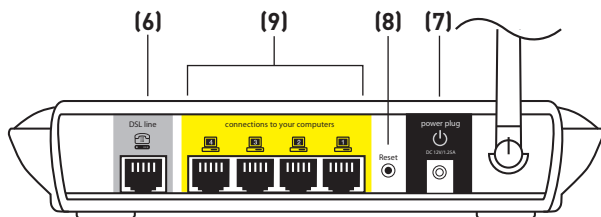
Het frontpaneel van de router is voorzien van negen LED's, zoals omschreven op de volgende bladzijde (van links naar rechts):

Kennismaken met uw router

LED	Kleur	Status	Beschrijving
ADSL			
	Groen	UIT	Voeding uitgeschakeld of ADSL-lijn niet aangesloten
		Knippert	Handshaking of training wordt uitgevoerd
		Brandt continu	ADSL-verbinding is OK
Draadloos			
	Groen	UIT	Voeding uitgeschakeld of geen radiosignaal (WLAN-kaart niet aanwezig of werkt niet goed)
		Knippert	Verkeer loopt via de WLAN-interface
		Brandt continu	WLAN-interface klaar voor gebruik
Internet			
	Groen	UIT	Geen Internetverbinding
		Knippert	Er worden gegevens verzonden of ontvangen
		Brandt continu	Er is een verbinding met het Internet tot stand gebracht
LAN 1 tot LAN 4			
LAN 1 - 4	Groen	UIT	Voeding uitgeschakeld of geen Ethernet-kaart aanwezig
		Knippert	Ethernet-kaart aanwezig en gebruikersgegevens gaan via Ethernet-poort
		Brandt continu	Ethernet-kaart aanwezig
Power (Voeding)			
	Groen	UIT	Voeding uitgeschakeld
		Brandt continu	Voeding ingeschakeld

Achterzijde router

De volgende afbeelding geeft het achterpaneel van de router weer.



Power Plug (Voedingsaansluiting) – Sluit de meegeleverde voedingsadapter aan op deze poort. Als u het verkeerde type voedingsadapter gebruikt, kunt u uw router beschadigen.

Ethernet-poorten – De Ethernet-poorten zijn RJ45, 10/100 auto-negotiation-poorten. De poorten worden aangeduid met de cijfers 1 t/m 4. Deze cijfers corresponderen met genummerde LED's aan de voorkant van de router. Sluit de netwerkcomputers of andere netwerkapparatuur aan op deze poorten.

ADSL Line – Deze poort is voor de verbinding met uw ADSL-aansluiting. Verbind uw ADSL-lijn met deze poort.

Resetknop – De resetknop kan gebruikt worden in het zeldzame geval dat de router niet goed functioneert. Door de router te resetten, herstelt u de normale werking van de router terwijl de geprogrammeerde instellingen in behoud blijven. Met de resetknop kunt u ook de fabrieksinstellingen van het draadloze accesspoint terugroepen. U kunt de optie "Restore" (Herstellen) gebruiken wanneer u uw persoonlijke wachtwoord bent vergeten.

a. De router resetten

Druk de resetknop een seconde lang in en laat hem daarna los. Wanneer de LED voor "Voeding/Gereed" weer continu brandt, is de resetprocedure voltooid.

b. Fabriekswaarden herstellen

Hou de resetknop gedurende 20 seconden ingedrukt en laat hem daarna los. Wanneer de LED voor "Voeding/Gereed" weer continu brandt, is de resetprocedure voltooid.

Uw router aansluiten en configureren

Setup-Assistent

Met de meegeleverde Setup-Assistent software is het installeren van de router erg eenvoudig. Hiermee hebt u uw router binnen een paar minuten aan de praat. Om de Setup-Assistent te kunnen gebruiken moet uw Windows 2000-, XP- of Vista™-computer rechtstreeks zijn aangesloten op de ADSL-lijn en moet de internetverbinding tijdens de installatie actief en operationeel zijn. Is dat niet het geval, ga dan te werk volgens het hoofdstuk “Alternatieve installatiemethode” in deze handleiding om uw router te configureren. Bij gebruik van een ander besturingssysteem dan Windows 2000, XP, Vista of Mac OS X, dient u gebruik te maken van het hoofdstuk “Alternatieve installatiemethode” in deze handleiding.

Stap 1A: Hardware aansluiten – Volg de aanwijzingen in de beknopte installatiehandleiding

Eerste installatie

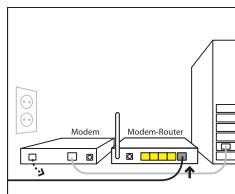
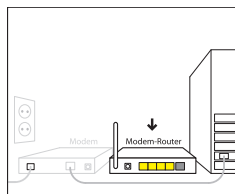
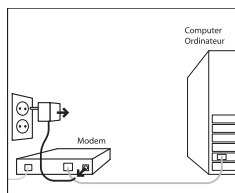
Volg deze stappen als u geen bestaande modem vervangt. Indien u een bestaande modem vervangt, ga dan verder op bladzijde 9 bij “Een bestaande modem of modem/router vervangen”.

1A.1 Haal uw nieuwe router uit de verpakking en zet hem naast uw computer. Zet de antenne van de router in verticale stand.

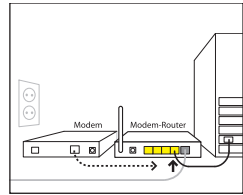
1A.2 Pak de gele RJ45-kabel die met uw router is meegeleverd. +Sluit eerst het ene uiteinde van deze kabel aan op een gele poort aangeduid met “Wired Computers” (Bedrade computers) op de achterkant van uw router. Sluit vervolgens het andere uiteinde aan op de netwerkpoort aan de achterkant van uw computer. [Insert Ethernet logo]

1A.3 Pak de meegeleverde RJ11-telefoonkabel. Sluit het ene uiteinde aan op de grijze poort die wordt aangeduid met “DSL” aan de achterkant van uw router. Sluit vervolgens het andere uiteinde aan op de ADSL-aansluiting (op een aansluiting aan de wand of op een ADSL-splitter).

Opmerking: Sommige ADSL-aansluitingen vereisen een microfilter. Uw ADSL-provider kan u vertellen of u een microfilter nodig hebt. Belkin levert een microfilter mee met het product in die regio's waarin ze doorgaans nodig zijn. Raadpleeg de handleiding die u van uw ADSL-provider hebt gekregen om vast te stellen of u een microfilter nodig hebt.



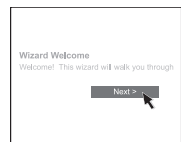
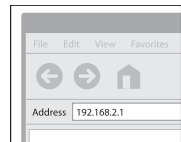
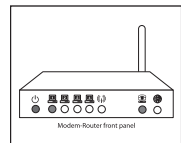
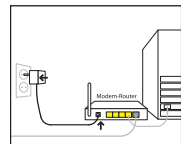
- 1A.4** Sluit de voedingsadapter van uw router aan op de zwarte poort die wordt aangeduid met “Power”, aan de achterkant van de router. Het kan 20 seconden duren tot de router is opgestart. Kijk naar het display aan de voorzijde van de router. De pictogrammen “Wired” (bedraad) en “Modem-Router” moeten groen oplichten. Als dit niet het geval is, controleer dan de verbindingen.



Stap 1B: Een bestaande modem of modem/router vervangen

Volg deze stappen als u nu al een modem of een modem/router gebruikt en u deze wilt vervangen door uw nieuwe router van Belkin.

- 1B.1** Haal uw nieuwe router uit de verpakking en zet hem naast uw oude modem. Zet de antenne van de router in verticale stand. Maak de voedingskabel los van het oude modem.
- 1B.2** Lokaliseer de kabel die uw oude modem met uw computer verbindt. Koppel die kabel los van uw oude modem en sluit hem aan op de gele poort, aangeduid met “Wired Computers” (Bedrade computers) aan de achterkant van uw nieuwe router.
- 1B0.3** Zoek de kabel op die uw oude modem met de ADSL-aansluiting aan de wand verbindt. Maak deze kabel los van uw oude modem en sluit hem aan op de grijze poort, aangeduid met “ADSL” (ADSL) aan de achterkant van uw nieuwe router.
- 1B.4** Sluit de voedingsadapter van uw router aan op de zwarte poort die wordt aangeduid met “Power”, aan de achterkant van de router.
- 1B.5** **Wait** Het kan 20 seconden duren tot de router is opgestart. Kijk naar het display aan de voorzijde van de router. Controleer of de LED's voor “ADSL” en “LAN” branden. Als dit niet het geval is, controleer dan de verbindingen.



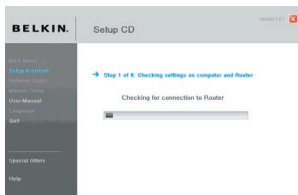
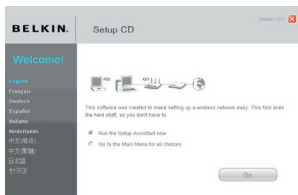
Stap 2: Installeer de router – Gebruik de Setup-Assistent software

- 2.1 Sluit alle programma's af die momenteel op uw computer geopend zijn. Schakel op uw computer alle software voor firewalls of het delen van een internetverbinding uit.
- 2.2 Plaats de cd in het cd-romstation van uw computer. De Setup-assistent zal binnen 15 seconden automatisch op uw beeldscherm verschijnen. Klik op "Go" (Starten) om de Setup-Assistent te starten. Volg de instructies op het scherm.

BELANGRIJK: Draai de Setup-Assistent op de computer die rechtstreeks is aangesloten op de router (Stap 1A).

Opmerking voor Windows-gebruikers: Als de Setup-Assistent niet automatisch opstart, selecteer dan uw cd-romstation onder "My computer" (Deze computer) en dubbelklik op het bestand met de naam "SetupAssistant" om de Setup-Assistent te starten.

- 2.3 Selecteer een land. Selecteer uw land in het dropdown-menu. Klik op "Begin" (Beginnen) om door te gaan.
- 2.4 Bevestigingsscherm Bevestig dat u alle stappen van de beknopte installatiehandleiding hebt doorlopen door het vakje naast de pijl aan te vinken. Klik op "Next" (Volgende) om door te gaan.
- 2.5 Voortgangsscherm. Er zal een voortgangsscherm verschijnen zodra er een stap in de setup is afgerond.
- 2.6 Controle van de instellingen. De Setup-Assistent controleert nu de netwerkinstellingen van uw computer en verzamelt de informatie die benodigd is voor het voltooien van de verbinding van de router met het Internet.



2.7 Controle van de hardwareverbindingen
De Setup-Assistent zal nu de hardwareverbindingen controleren.

2.8 Uw draadloze netwerk een naam geven

De Setup-Assistent toont de standaardnaam (of Service Set Identifier (SSID)) voor een draadloos netwerk. De SSID is de naam van het draadloze netwerk waarmee uw computer of apparaten met draadloze netwerkadapters verbinding zullen maken. U kunt de standaard naam gebruiken of ervoor kiezen de naam te wijzigen. Noteer deze naam ergens, zodat u weet welke naam u hebt gekozen. Klik op "Next" (Volgende) om verder te gaan.

2.9 Internetaccountinformatie opvragen (indien nodig)

Indien uw internetaccount een gebruikersnaam en wachtwoord vereist, verschijnt er een scherm als op de onderstaande afbeelding. Selecteer uw land of provider in het dropdown-menu.

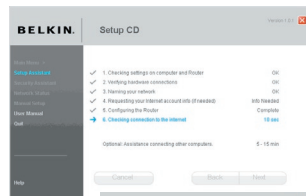
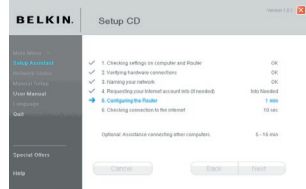
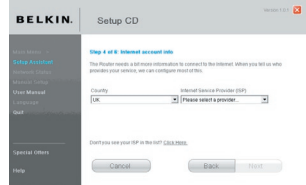
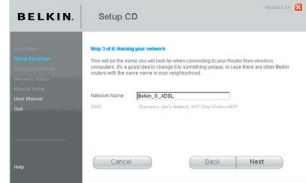
2.10 2.10 Configuratie van de router

De Setup-Assistent configureert nu de router door gegevens naar de router te versturen en hem te herstarten. Daarna hoeft u slechts de aanwijzingen op uw scherm te volgen.

Opmerking: U mag tijdens het herstarten van de router de kabels of de voeding niet ontkoppelen. Als u dit wel zou doen, kan de router onbruikbaar worden.

2.11 Controle van de Internetverbinding

U bent bijna klaar. De Setup-Assistent zal nu de verbinding met het Internet controleren.



1
2
3
4
5
6
7
8
9
10
11

Uw router aansluiten en configureren

Gefeliciteerd!

De installatie van uw nieuwe router van Belkin is klaar. Dit scherm zal verschijnen als uw router verbinding heeft kunnen maken met het Internet. U kunt nu op het Internet gaan surfen door uw browser te openen en een website te bezoeken.

U kunt de Setup-Assistent gebruiken voor het instellen van uw andere bedrade en draadloze computers zodat deze ook verbinding kunnen maken met het internet. Als u dit wilt doen, klik dan op “Next” (Volgende). Als u pas later computers wilt toevoegen, selecteer dan “Exit the Assistant” (Sluit de Assistent) en klik op “Next” (Volgende).

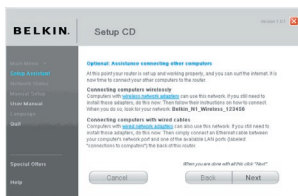


Problemen oplossen

Als de Setup-Assistent geen verbinding met het Internet kan maken, verschijnt het volgende scherm. Volg de aanwijzingen op het scherm om de oorzaak van het probleem te achterhalen.

2.12 Optioneel: Assistentie bij het aansluiten van andere computers.. Deze optionele stap helpt u bij het aansluiten van meer bedrade en draadloze computers op uw netwerk. Volg de aanwijzingen op het beeldscherm op.

Zodra u hebt gecontroleerd of uw andere bedrade en draadloze computers correct zijn aangesloten, is uw netwerk klaar voor gebruik. U kunt nu op surfen op het Internet. Klik op “Next” (Volgende) om terug te gaan naar het hoofdmenu.



Handmatige configuratie van de router

1
2
3
4
5
6
7
8
9
10
11

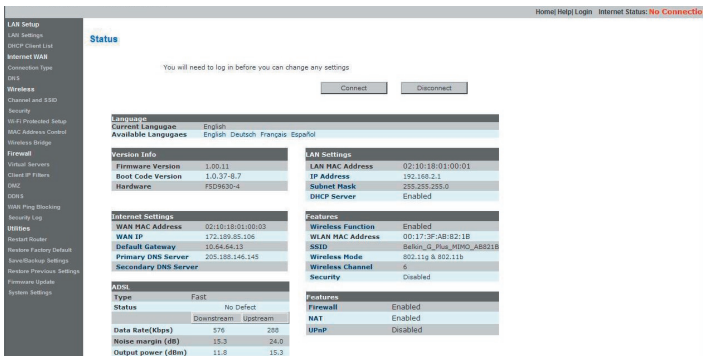
Hoofdstuk

De werking van de geavanceerde web-gebruikersinterface

Deze homepage geeft u een beknopt overzicht van de status en de instellingen van de router. Alle pagina's voor geavanceerde installatie zijn vanaf deze pagina bereikbaar.

Gebruik maken van web-based beheer

Zodra uw host-PC op de juiste wijze is geconfigureerd, start u uw webbrowser en typt u het IP-adres van de router, "192.168.2.1", in in het URL-veld. Vervolgens klikt u op "Enter".



1. Snelnavigatiekoppelingen

U kunt rechtstreeks naar elke pagina van de gebruikersinterface van de router gaan door rechtstreeks op deze koppelingen te klikken. Om het opzoeken van een bepaalde instelling te vergemakkelijken, zijn de koppelingen onderverdeeld in logische categorieën en gegroepeerd op tabbladen. Als u klikt op de koptekst van een tabblad krijgt u een beknopte beschrijving van de functie van het tabblad.

2. Home-knop

De "Home"-knop is beschikbaar op elke pagina van de gebruikersinterface. Met een druk op deze knop gaat u terug naar de homepage.

3. Helpknop

Door middel van de helpknop kunt u de helppagina's van de router openen. Op veel pagina's kunt u ook om hulp vragen met een klik op "More Info" (Meer informatie).

4. Login/Logout-knop

Met één druk op deze knop kunt u op de router in- en uitloggen. Wanneer u bent ingelogd, verandert de tekst op de knop in "Logout". Door op de router in te loggen, gaat u naar een afzonderlijke inlogpagina waar u een wachtwoord moet invoeren. Als u bent ingelogd, kunt u wijzigingen aanbrengen in de instellingen. Wanneer u klaar bent met het aanbrengen van wijzigingen, kunt u uitloggen door te klikken op de knop "Logout" (Afmelden). Meer informatie over inloggen op de router vindt u in het hoofdstuk "Inloggen op de router".

5. Indicator Internetstatus

Deze indicator is zichtbaar op alle pagina's van de router en geeft de verbindingstatus van de router weer. Wanneer de indicator in het GROEN "Connection OK" (Verbinding OK) aangeeft, dan is er een verbinding met Internet tot stand gebracht. Wanneer de indicator in het rood "No Connection" (Geen verbinding) aangeeft, is er geen verbinding met Internet tot stand gebracht. De indicator wordt automatisch aangepast wanneer u wijzigingen aanbrengt in de instellingen van de router.

6. LAN-instellingen

Toont u de instellingen van de LAN-kant van de router. U kunt deze instellingen wijzigen door op de LAN-snelnavigatiekoppeling links in het scherm te klikken.

7. Productkenmerken

Hiermee wordt de status getoond van de NAT, firewall, en draadloze functies van de router. U kunt deze instellingen wijzigen door te klikken op een van de koppelingen of door te klikken op de snelnavigatiekoppelingen aan de linkerzijde van het scherm.

8. Internetinstellingen

Toont de instellingen van de internet/WAN-kant van de router die verbinding maakt met het internet. U kunt deze instellingen wijzigen door te klikken op de "Internet/WAN"-snelnavigatiekoppeling aan de linkerzijde van het scherm.

9. Versie-informatie

Toont de firmwareversie, bootcode-versie, hardwareversie, en het serienummer van de router.

10. Paginanaam

De pagina waarop u zich bevindt, is herkenbaar aan deze naam. Deze handleiding verwijst soms naar de naam van de pagina's. "LAN > LAN Settings" verwijst bijvoorbeeld naar de pagina "LAN Settings" (LAN-instellingen).

LAN-instellingen wijzigen

Hier kunt u alle instellingen van de interne LAN-setup van de router bekijken en aanpassen.

LAN-instellingen

Als u klikt op de header van de LAN-tab (A) gaat u naar die pagina van de LAN-tab. Hier vindt u een beknopte beschrijving van de functies. Om de instellingen te bekijken of één van de LAN-instellingen te wijzigen, klikt u op "LAN Settings" (LAN-instellingen) (B). Als u een lijst van de aangesloten computers wilt bekijken, klikt u op "DHCP Client List" (C).

(A) points to the 'LAN Setup' header in the navigation menu.

(B) points to the 'LAN Settings' option in the navigation menu.

(C) points to the 'DHCP Client List' option in the navigation menu.

The main content area shows the following text:

BELKIN Wireless ADSL Modem Router Setup Utility

LAN >

Your Router is equipped with a DHCP server that will automatically assign IP addresses to each computer on your network. The factory default settings for the DHCP server will work in most any application. If you need to make changes to the settings, you can do so.

The changes that you can make are:

- Change the Internal IP address of the Router. The default = 192.168.2.1
- Change the Subnet Mask. The default = 255.255.255.0
- Enable/Disable the DHCP Server Function. Default = On (Enabled)
- Specify the Starting and Ending IP Pool Address. Default = Starting: 2 / Ending: 100
- Specify the IP address Lease Time. Default = Forever
- Specify a local Domain Name. Default = Belkin

To make changes, click "LAN Settings" on the LAN tab to the left.

The Router will also provide you with a list of all client computers connected to the network. To view the list, click "DHCP client list" on the LAN tab to the left.

IP-adres

Het "IP adres" is het interne IP-adres van de router. Het standaard IP-adres is "192.168.2.1". Om de geavanceerde installatie-interface te openen, moet u dit adres in de adresbalk van uw browser typen. U kunt dit adres indien nodig wijzigen. Om het IP-adres te wijzigen, typt u het nieuwe IP-adres in en klikt u op "Apply Changes" (Wijzigingen aanbrengen). Het IP-adres dat u kiest, moet een niet-routeerbaar IP zijn. Hieronder ziet u een paar voorbeelden van een niet-routeerbaar IP:

192.168.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)

10.x.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)

Subnetmasker

Het subnetmasker hoeft niet te worden veranderd. Dit is een unieke, geavanceerde eigenschap van uw router van Belkin.

DHCP-server

De DHCP-serverfunctie maakt het installeren van een netwerk bijzonder gemakkelijk omdat aan elke computer in het netwerk automatisch een IP-adres wordt toegekend. De standaardinstelling is “On” (Ingeschakeld). Indien nodig kan de DHCP-server worden uitgeschakeld, maar om dit te doen moet u voor iedere computer in uw netwerk handmatig een statisch IP-adres instellen. Om de DHCP-server uit te schakelen, selecteert u “Off” (Uitgeschakeld) en klikt u op “Apply Changes” (Wijzigingen aanbrengen).

IP-pool

Dit is een voorraad IP-adressen die u in reserve houdt voor dynamische toewijzing aan de computers in uw netwerk. Als u dit aantal wilt veranderen, voert u een nieuw start- en eind-IP-adres in en klikt u op “Apply Changes” (Wijzigingen aanbrengen). Het start-IP-adres moet altijd een lagere waarde hebben dan het eind-IP-adres.

Leasetijd

De tijd gedurende welke de DHCP-server het IP-adres voor elke computer bewaart. Het is beter dat de leasetijd ingesteld blijft op “Forever” (Altijd). Ook de standaard-instelling is “Forever” (Altijd). Dit betekent dat het door de DHCP-server aan een computer toegewezen IP-adres voor die bepaalde computer nooit verandert. Door het instellen van kortere leasetijden zoals een dag of een uur komen IP-adressen na de gespecificeerde tijdsduur vrij. Dit betekent ook dat het IP-adres van een bepaalde computer na verloop van tijd zou kunnen veranderen. Als u één van de andere geavanceerde functies van de router heeft ingesteld zoals DMZ of cliënt IP-filters, dan zijn deze afhankelijk van het IP-adres. Daarom is het niet waarschijnlijk dat u het IP-adres wilt wijzigen.

Lokale domeinnaam

U kunt een lokale domeinnaam (netwerknnaam) voor uw netwerk instellen. Het is niet nodig deze instelling te wijzigen tenzij daar een specifieke reden voor is. U kunt het netwerk elke naam geven die u wilt zoals “MIJN NETWERK”.

DHCP-cliëntlijst

U kunt een overzicht bekijken van de computers die zijn aangesloten op uw netwerk. U krijgt een overzicht met het IP-adres van de computer, de hostnaam (naam van de computer in uw netwerk) en het MAC-adres van de netwerkkinterfacaekaart (NIC) van de computer. Wanneer u de knop “Refresh” (Vernieuwen) indrukt, wordt het overzicht bijgewerkt. Als er dingen zijn gewijzigd, wordt de lijst bijgewerkt.

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing “Refresh” will update the list.

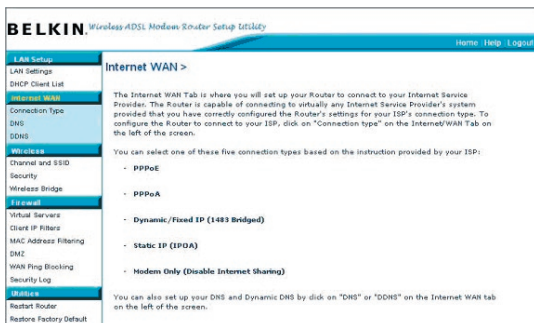
IP Address	Host Name	MAC Address
192.168.2.11	Ericd-XP	00-30-BD-3D-AB-09

[Refresh](#)

Internet WAN

Via het tabblad “Internet/WAN” stelt u uw router zo in dat deze verbinding kan maken met uw Internet Service Provider (ISP). De router kan met vrijwel elke ADSL-serviceprovider verbinding maken mits u de instellingen van de router hebt afgestemd op het type verbinding dat uw ISP gebruikt. Uw ISP verstrekt u de benodigde gegevens.

Om de router te configureren volgens de gegevens die uw ISP heeft verstrekt, klikt u op “Connection Type” (Verbindingstype) (1) links op het scherm. Selecteer het type verbinding dat u gebruikt. Als uw ISP u DNS-gegevens heeft gegeven, kunt u door op “DNS” (2) te klikken DNS-adresinformatie invoeren voor ISP’s die specifieke instellingen vereisen. Als u klaar bent met het aanbrengen van instellingen, geeft de internetstatusindicator aan dat de verbinding is gemaakt als de setup van uw router correct is verlopen.



Verbindingstype

Via de pagina “Connection Type” (Verbindingstype), kunt u een van deze vijf verbindingstypes selecteren afhankelijk van de instructies die uw ISP u heeft gegeven:

PPPoE

PPPoA

Dynamic IP (1483 Bridged) (Dynamisch IP)

Static IP (IPoA) (Statisch IP)

Modem Only (Disable Internet Sharing) (Alleen modem (Internet delen uitschakelen))

Opmerking: Als u niet zeker weet welk verbindingstype u moet gebruiken, raden wij u aan contact op te nemen met uw ISP.

Selecteer het type verbinding dat u gebruikt door op het keuzerondje naast uw type verbinding te klikken en vervolgens te klikken op “Next” (Volgende).

Handmatige configuratie van de router

WAN > Connection type

The following information is usually provided by your ISP.
Please select the Internet sharing protocol.

- PPPoE
- PPPoA
- Dynamic/Fixed IP (488 Bridged)
- Static IP (1PoA)
- Modem Only (Disable Internet Sharing)

Next

Uw ISP-verbindingstype instellen op PPPoE of PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) is de standaardmethode voor het aansluiten van netwerkapparatuur. Een gebruikersnaam en wachtwoord zijn vereist om toegang tot het netwerk van uw ISP te verkrijgen en om een verbinding met Internet tot stand te kunnen brengen. PPPoA (PPP over ATM) is vergelijkbaar met PPPoE, maar wordt voornamelijk in het Verenigd Koninkrijk gebruikt. Selecteer PPPoE of PPPoA en klik op “Next” (Volgende). Voer vervolgens de informatie in die u van uw ISP gekregen hebt en klik op “Apply Changes” (Wijzigingen aanbrengen) om de instellingen te activeren.

WAN > Connection Type > PPPoE Interface

More Info
ATM Interface

(1)	Username	<input type="text"/>
(2)	Password	<input type="password"/>
(3)	Retype Password	<input type="password"/>
(4)	IP assigned by ISP >	Yes <input checked="" type="checkbox"/>
	IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
	Subnet Mask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
	Default Gateway	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
(5)	VPI/VCI	<input type="text"/> / <input type="text"/>
(6)	Encapsulation	LLC <input checked="" type="checkbox"/>
(7)	Dial on Demand >	<input type="checkbox"/>
(8)	Idle Time (Minute) >	<input type="text"/>
(9)	MTU >	1456

Clear Changes Apply Changes

1. Gebruikersnaam - Typ de gebruikersnaam in. (Toegekend door uw ISP.)
2. Password (Wachtwoord) - Voer uw wachtwoord in. (Toegekend door uw ISP.)
3. Retype Password (Wachtwoord opnieuw intypen) - Typ het wachtwoord opnieuw in. (Toegekend door uw ISP.)
4. IP toegekend door ISP – Laat “Yes” (Ja) staan indien uw ISP automatisch een IP-adres toekent. Indien uw ISP u een vast IP-adres toekent, selecteert u “No” (Nee) en voert u de aan u verstrekte waarden in.

5. VPI/VCI - Vul uw Virtual Path Identifier (VPI) en Virtual Circuit Identifier (VCI) parameter hier in. (Toegekend door uw ISP.)
6. Encapsulatie - Selecteer uw encapsulatietype (verstrek door uw ISP) om aan te geven hoe meerdere protocols verwerkt moeten worden bij de ATM-transportlaag. VC-MUX: PPPoA Virtual Circuit Multiplexer (null encapsulation) laat slechts een protocol per virtueel circuit toe, met minder overheads. LLC: PPPoA Logical Link Control staat meerdere protocols toe op een virtueel circuit (meer overhead).
7. Dial on Demand — Als u “Dial on Demand” selecteert, zal uw router automatisch verbinding maken met het Internet zodra een gebruiker de webbrowser opent.
8. Niet-actieve tijd (minuten) — Voer de maximale niet-actieve tijd in voor de Internet-verbinding. Nadat deze tijd is verstreken, zal de verbinding verbroken worden.
9. MTU — De MTU (Maximum Transmission Unit) waarde mag nooit worden gewijzigd tenzij uw provider een specifieke MTU-waarde vereist. Door wijziging van de MTU-instelling kunnen problemen met uw internetverbinding ontstaan zoals verbreking van de verbinding, trage toegang tot het Internet en een gebrekkige werking van internetapplicaties.

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

IP assigned by ISP > Yes

IP Address 0 0 0 0

Subnet Mask 0 0 0 0

Default Gateway 0 0 0 0

VPI / VCI 0 / 35

Encapsulation LLC

Clear Changes Apply Changes

Uw type internetverbinding instellen op Dynamic IP (1483 Bridged)

Deze verbindingmethode verbindt uw netwerk met dat van uw ISP. Aan de router zal automatisch een IP-adres worden toegekend door de DHCP-server van uw ISP.

Handmatige configuratie van de router

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

(1) IP assigned by ISP > Yes

IP Address
0 0 0 0

Subnet Mask
0 0 0 0

(2) Default Gateway > 0 0 0 0

VPI/VCI
0 / 35

(3) Encapsulation
LLC

Clear Changes Apply Changes

1. IP toegekend door ISP – Laat “Yes” (Ja) staan indien uw ISP automatisch een IP-adres toekent. Indien uw ISP u een vast IP-adres toekent, selecteert u “No” (Nee) en voert u de aan u verstrekte waarden in.

2. VPI/VCI - Voer hier de VPI- en VCI-parameters in. Deze gegevens worden door uw ISP verstrekt.

3. Encapsulatie - Selecteer LLC of VC MUX afhankelijk van wat uw ISP gebruikt.

Het verbindingstype van uw ISP instellen op Static IP (IPoA) (Statisch IP).

Dit type verbinding wordt ook wel “Classical IP over ATM” of “CLIP” genoemd.

Hierbij voorziet uw ISP u van een vast IP voor de verbinding van uw router met het Internet.

WAN > Connection Type > Static IP(IPoA)

More Info
ATM Interface

(1) IP Address > 0 0 0 0

(2) Subnet Mask > 0 0 0 0

(3) Default Gateway > 0 0 0 0

(4) VPI/VCI > 0 / 35

(5) Encapsulation > LLC

Clear Changes Apply Changes

1. IP-adres — Voer het IP-adres in dat u van uw ISP gekregen hebt voor de WAN-interface van de router.

2. Subnetmasker - Vul het door uw ISP verstrekte subnetmasker in.

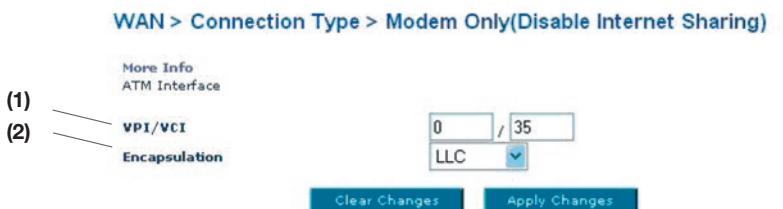
3. Standaard gateway — Voer een standaard gateway IP-adres in. Indien de router binnen het lokale netwerk geen bestemmingsadres kan vinden, zal hij de pakketten doorsturen naar de standaard gateway die uw ISP heeft toegekend.

4. VPI/VCI - Voer hier de VPI- en VCI-parameters in. Deze gegevens worden door uw ISP verstrekt.

5. Encapsulatie - Selecteer LLC of VC MUX afhankelijk van wat uw ISP gebruikt.

Het verbindingstype instellen op Modem Only (Disable Internet Sharing) (Alleen modem ("Internet delen" uitschakelen)).

In deze modus fungeert de router uitsluitend als een bridge (brug) voor de overdracht van pakketten via de DSL-poort. Om een verbinding met het Internet tot



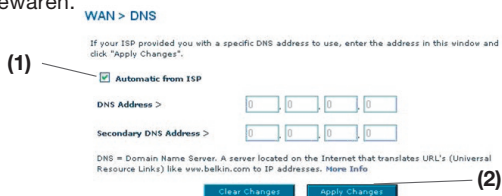
stand te kunnen brengen, moet echter wel extra software op uw computer worden geïnstalleerd.

1. VPI/VCI — Voer hier de VPI- en VCI-parameters in. (Toegekend door uw ISP.)
2. Encapsulatie — Selecteer LLC of VC MUX. (Toegekend door uw ISP.)

Instellingen DNS (Domain Name Server)

Een "Domain Name Server" is een server op het Internet die URL's (Universal Resource Links) als "www.belkin.com" vertaalt in IP-adressen. De meeste ISP's verlangen niet van u dat u deze informatie in de router invoert. Selecteer de optie "Automatic from ISP" (1) als uw Internet Service Provider u geen specifiek DNS-adres heeft gegeven. Als u een statische IP gebruikt, moet u waarschijnlijk een specifiek DNS-adres en een secundair DNS-adres invullen om ervoor te zorgen dat uw verbinding correct functioneert. Als u een dynamische verbinding of PPPoE gebruikt, hoeft u waarschijnlijk geen DNS-adres in te vullen.

Laat het vakje behorend bij "Automatic from ISP" (Automatisch van ISP) aangevinkt. Om de gegevens van het DNS-adres in te voeren, verwijdert u het vinkje voor de optie "Automatic from ISP" en vult u uw DNS-gegevens in de daarvoor bestemde ruimte in. Klik op "Apply Changes" (Wijzigingen aanbrengen) (2) om de instellingen te bewaren.



Handmatige configuratie van de router

Gebruik maken van DDNS (Dynamic DNS)

De DDNS-service staat statische hostnamen toe voor dynamische IP-adressen in een van de vele domeinen van DynDNS.org, waardoor toegang tot uw netwerkcomputers vanaf verschillende plaatsen op het Internet eenvoudiger is. DynDNS.org biedt deze service, voor een maximum van vijf hostnamen, als een gratis dienst voor de internetgemeenschap. TZO.com is een alternatief voor DynDNS.org. De DDNS-service is ideaal voor een privé-website, bestandsserver, maar ook als u vanaf uw werk toegang wilt krijgen tot uw pc thuis en de bestanden die erop staan. Indien u gebruik maakt van deze service verzekert u zich ervan dat uw hostnaam altijd verwijst naar uw IP-adres, zelfs als uw ISP dit adres wijzigt. Indien uw IP-adres wijzigt, kunnen uw vrienden en zakenrelaties u altijd vinden via yourname.dyndns.org! U kunt zich gratis aanmelden voor een Dynamische DNS-host-naam via <http://www.dyndns.org>.

De Dynamic DNS Update Client van de router installeren.

Voordat u van deze functionaliteit gebruik kunt maken, dient u zich aan te melden voor de gratis update-service van DynDNS.org. Zodra u dit gedaan hebt, kunt u verder. Volg daartoe onderstaande aanwijzingen.

1. Voer uw DynDNS.org-gebruikersnaam in in het veld "Account / E-mail" (1).
2. Voer uw DynDNS.org-wachtwoord in in het veld "Password / Key" (2).
3. Voer de DynDNS.org domeinnaam die u met DynDNS.org hebt opgezet in in het veld "Domain Name" (3).
4. Klik op "Apply Changes" (Wijzigingen aanbrengen) om uw IP-adres bij te werken. Indien het door uw provider aan u toegewezen IP-adres wijzigt, zal de router uw nieuwe IP-adres automatisch doorspelen aan de DynDNS.org-servers. U kunt dit ook handmatig doen door te klikken op de knop "Apply Changes" (Wijzigingen aanbrengen) (4).

Via de pagina "Connection Type" (Verbindingstype), kunt u het door u gebruikte verbindingstype selecteren.

WAN > DDNS

DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP address is dynamic. You must Register for DDNS service at one of the listed DDNS Services.

DDNS Service >

DDNS Status >

(1) Account / E-mail >

(2) Password / Key >

(3) Domain Name >

(4)

Draadloos

Op het tabblad “Wireless” (Draadloos) kunt u veranderingen aanbrengen in de instellingen van het draadloze netwerk. Op dit tabblad kunt u de naam van het draadloze netwerk (SSID), het gebruikte kanaal en de encryptie-instellingen aanpassen.

Wireless > Channel and SSID

This page allows you to enter the Wireless Network Name (SSID in Wi-Fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as an wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. More Info

SSID >	<input type="text" value="Belkin54g"/>
ESSID Broadcast >	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode >	<input type="text" value="Mixed (11b+11g)"/>
Wireless Channel >	<input type="text" value="Auto"/>

Kanaal en SSID

1. De naam van het draadloze netwerk (SSID) wijzigen

Om uw draadloze netwerk te identificeren, wordt een naam gebruikt die bekend is als SSID (Service Set Identifier). U kunt deze naam veranderen in alles wat u maar wilt of u kunt hem onveranderd laten. Als er andere draadloze netwerken in uw omgeving actief zijn, stelt u het waarschijnlijk op prijs dat uw SSID uniek is (dus niet hetzelfde is als die van een ander draadloos netwerk in uw omgeving). Als u de SSID wil veranderen, typ dan de SSID die u wilt gebruiken in het SSID-veld in en klik op “Apply Changes” (Wijzigingen aanbrengen). De verandering gaat onmiddellijk in. Als u de SSID verandert, moeten ook uw draadloos werkende computers opnieuw worden geconfigureerd om verbinding te kunnen maken met uw nieuwe netwerknaam. Zie de handleiding van uw draadloze netwerkadapter voor meer informatie over hoe u deze verandering moet aanbrengen.

2. Gebruik maken van de ESSID Broadcast-functie

Om veiligheidsredenen kunt u ervoor kiezen de SSID van uw netwerk niet uit te zenden. Daardoor blijft de naam van uw netwerk verborgen voor computers die de ether aftasten naar de aanwezigheid van draadloze netwerken. Om de uitzending van het SSID stop te zetten, selecteert u “DISABLE” (Uitschakelen) en klikt u op “Apply Changes” (Wijzigingen aanbrengen). De verandering gaat onmiddellijk in. Elke computer moet nu worden ingesteld op het maken van verbinding met uw specifieke SSID; een SSID in de vorm van “ANY” (Elke) wordt niet langer geaccepteerd. Zie de handleiding van uw draadloze netwerkadapter voor meer informatie over hoe u deze verandering moet aanbrengen.

Opmerking: Deze geavanceerde functie mag uitsluitend door ervaren gebruikers worden toegepast.

3. Wisselen van draadloze modus

Uw router kan in drie verschillende draadloze modi werken: “Mixed (11b+11g)”, “11g Only” en “11b Only”. De verschillende modi worden hieronder toegelicht.

Mixed (11b+11g) modus

In deze modus is de router zowel compatibel met 802.11b als met 802.11g draadloze cliënten. Deze modus is de standaard-fabrieksinstelling die ervoor zorgt dat u volledige compatibiliteit geniet met alle met Wi-Fi® compatibele apparaten. Als zowel 802.11b- als 802.11g-clieënten in uw netwerk zijn opgenomen, raden wij u aan de standaard instelling te gebruiken. Deze instelling mag alleen gewijzigd worden als u daarvoor een specifieke reden heeft.

11g-Only-modus

“802.11g-Only”-modus werkt alleen met 802.11g-clieënten. Gebruik van deze modus wordt aangeraden als u wilt voorkomen dat 802.11b-clieënten zich toegang verschaffen tot uw netwerk. Als u van modus wilt wisselen, selecteert u de gewenste modus in het dropdown-menu “Wireless Mode” (Draadloze modus). Klik vervolgens op “Apply Changes” (Wijzigingen aanbrengen).

11b-Only-modus

Wij raden u aan om deze modus NIET te gebruiken als u daar geen specifieke reden voor heeft. Deze modus is uitsluitend bedoeld om unieke problemen op te lossen die zouden kunnen voorkomen bij het gebruik van 802.11b-clieëntadapters en hoeft niet gebruikt te worden voor interoperabiliteit van de 802.11g- en 802.11b-standaard.

4. Van draadloos kanaal wisselen

U kunt kiezen uit verschillende kanalen. In de Verenigde Staten zijn 11 kanalen beschikbaar. In het grootste deel van Europa, waaronder het Verenigd Koninkrijk, zijn 13 kanalen beschikbaar. Een klein aantal andere landen stelt andere eisen aan het kanaalgebruik. Uw router is zo ingesteld dat hij actief kan zijn op de juiste kanalen voor het land waarin u zich bevindt. Standaard is “Auto”. Indien nodig kan dit adres worden gewijzigd. Als er meer draadloze netwerken in uw gebied actief zijn, moet uw netwerk op een ander kanaal worden ingesteld dan de andere draadloze netwerken. U bereikt het beste resultaat door een kanaal te kiezen dat minstens vijf kanalen verwijderd is van een ander draadloos netwerk. Als een ander netwerk bijvoorbeeld kanaal 11 gebruikt, stel uw netwerk dan in op kanaal 6 of lager. Om het kanaal te veranderen, kiest u een kanaal in het dropdown-menu. Klik op “Apply Changes” (Wijzigingen aanbrengen). De verandering gaat onmiddellijk in.

Encryptie/Beveiliging

Beveiliging van uw WiFi-netwerk

Hier zijn een aantal manieren om de beveiliging van uw draadloze netwerk te verhogen en uw data voor nieuwsgierige ogen en oren af te schermen. Dit overzicht is van toepassing voor de privé- of kleinzakelijke gebruiker. Op het moment van publicatie van deze handleiding, zijn er drie encryptiemethodes beschikbaar.

Naam	64-Bit Wired Equivalent Privacy	128-Bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acroniem	64-bits WEP	128-bits WEP	WPA-TKIP/AES (of alleen WPA)	WPA2-AES (of alleen WPA2)
Beveiliging	Goed	Beter	Uitstekend	Uitstekend
Productkenmerken	Statische sleutels	Statische sleutels	Dynamische encryptiesleutels en tweezijdige authenticatie	Dynamische encryptiesleutels en tweezijdige authenticatie
	Encryptiesleutels gebaseerd op het RC4-algoritme (meestal 40-bits sleutels)	Veiliger dan 64-bits WEP-encryptie met een sleutellengte van 104 bits plus 24 extra bits van door het systeem gegenereerde data.	TKIP (Temporal Key Integrity Protocol); ter verhoging van de veiligheid worden de sleutels continu gewijzigd	AES (Advanced Encryption Standard) beveiligt zonder snelheidsverlies

Wired Equivalent Privacy (WEP)

WEP is een protocol dat beveiliging van draadloze producten die voldoen aan de Wi-Fi-standaard mogelijk maakt. WEP werd ontwikkeld om draadloze netwerken dezelfde mate van privacybescherming te bieden als vergelijkbare bekabelde netwerken.

64-bits WEP-encryptie

64-bits WEP werd als eerste geïntroduceerd met 64-bits encryptie, bestaande uit een sleutel met een lengte van 40 bits plus 24 extra bits van door het systeem gegenereerde data (totaal 64 bits). Er zijn hardwarefabrikanten die 64-bits 40-bits encryptie noemen. Kort na de introductie van deze technologie ontdekten onderzoekers dat 64-bits encryptie te gemakkelijk te decoderen is.

1
2
3
4
5
6
7
8
9
10
11

128-bits WEP-encryptie

Aangezien beveiliging via 64-bits WEP-encryptie mogelijkwerijs niet toereikend zou zijn, werd een veiligere methode ontwikkeld, namelijk 128-bits WEP-encryptie. Bij 128-bits encryptie is er sprake van een sleutellengte van 104 bits plus 24 extra bits van door het systeem gegenereerde data (128 bits in totaal). Er zijn hardwarefabrikanten die 128-bits 104-bits encryptie noemen. De meeste nieuwe draadloze apparatuur die momenteel op de markt is, ondersteunt zowel 64-bits als 128-bits WEP-encryptie wat niet uitsluit dat u oudere apparatuur bezit die alleen 64-bits WEP-encryptie ondersteunt. Alle draadloze apparatuur van Belkin ondersteunt zowel 64-bits als 128-bits WEP-encryptie.

Encryptiesleutels

Nadat u de 64-bits of 128-bits WEP-encryptiemodus hebt gekozen, dient u een encryptiesleutel te genereren. Als de encryptiesleutel niet consequent in uw gehele draadloze netwerk gebruikt wordt, kunnen de op het netwerk aangesloten apparaten niet goed met elkaar communiceren. U kunt de sleutel invoeren door de hexadecimale sleutel handmatig in te typen of u kunt een "Passphrase" (Meervoudig wachtwoord) intypen in het daarvoor bestemde veld en klikken op "Generate" (Genereren) om een sleutel te genereren. Een hexadecimale sleutel bestaat uit een combinatie van cijfers en letters van A tot F en van 0 tot 9. Voor 64-bits WEP-encryptie dient u 10 hexadecimale sleutels in te voeren. Voor 128-bits WEP-encryptie dient u 26 hexadecimale sleutels in te voeren.

Bijvoorbeeld:

AF 0F 4B C3 D4 = 64-bits WEP-sleutel

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bits WEP-sleutel

Een WEP-passphrase (meervoudig wachtwoord) is NIET hetzelfde als een WEP-sleutel. Uw draadloze netwerkkaart gebruikt deze passphrase om uw WEP-sleutels te genereren, maar de methode voor het aanmaken van sleutels verschilt per hardwarefabrikant. Als uw netwerk uit apparaten van verschillende leveranciers is opgebouwd, kunt u het beste de hexadecimale WEP-sleutel van uw router of accesspoint aanhouden en deze met de hand invoeren in de tabel voor de hexadecimale WEP-sleutel in het configuratiescherm van uw draadloze kaart.

Wi-Fi Protected Access (WPA)

WPA is een nieuwe Wi-Fi-standaard die is ontwikkeld ter verbetering van de beveiliging die geboden wordt door WEP-encryptie. De stuurprogramma's en software van uw draadloze apparatuur ondersteunen WPA slechts na een upgrade. Updates kunt u vinden op de website van de leverancier van uw draadloze product. Er zijn twee soorten WPA-beveiliging: WPA-PSK (zonder server) en WPA (met 802.1x radiusserver).

WPA-PSK (zonder server)

Deze methode maakt gebruik van een zogenaamde “pre-shared key” als netwerksleutel. Een netwerksleutel is een wachtwoord dat tussen de 8 en 63 tekens lang is. Dit wachtwoord kan zijn opgebouwd uit een combinatie van letters, cijfers en andere tekens. Elke cliënt gebruikt dezelfde sleutel om toegang te krijgen tot het netwerk. Dit is de modus die doorgaans gebruikt wordt in woningen.

WPA (met 802.1x radiusserver)

Bij dit systeem wordt er door een radiusserver automatisch een netwerksleutel aan de cliënten toegekend. Van deze modus wordt doorgaans op kantoren gebruik gemaakt.

WPA2

De router maakt beveiliging van uw netwerk mogelijk via WPA2. WPA2 is de tweede generatie WPA die gebaseerd is op de 802.11i-standaard en maakt een betere beveiliging van uw draadloze netwerk mogelijk doordat geavanceerde netwerkauthenticatie en complexere AES encryptietechnieken gecombineerd worden.

Systeemvereisten voor WPA2

BELANGRIJK: Om WPA2-beveiliging te kunnen gebruiken moeten al uw computers en netwerkadapters geüpgraded zijn en beschikken over stuurprogramma's en software die WPA2 ondersteunen. Ten tijde van de publicatie van deze handleiding kunt kosteloos u een aantal beveiligingspatches van Microsoft® downloaden. Deze patches werkt alleen onder het Windows XP-besturingssysteem. Andere besturingssystemen worden op dit moment nog niet ondersteund.

Voor een computer met Windows XP zonder Service Pack 2 (SP2) kan via <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91> gratis een bestand van Microsoft genaamd “Windows XP Support Patch for Wireless Protected Access (KB 826942)” gedownload worden.

Voor Windows XP met Service Pack 2 heeft Microsoft een gratis download uitgebracht voor het bijwerken van uw draadloze cliëntcomponenten ter ondersteuning van WPA2 (KB893357). De update kunt u downloaden via: <http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en>.

BELANGRIJK: U moet ook controleren of al uw draadloze netwerkkaarten en adapters WPA2 ondersteunen en of u de nieuwste stuurprogramma's hebt gedownload en geïnstalleerd. Voor de meeste draadloze netwerkkaarten van Belkin is er een stuurprogramma-update beschikbaar op de website van Belkin: www.belkin.com/networking. Ga voor een overzicht van de draadloze producten van Belkin die WPA/WPA2 ondersteunen naar onze website: www.belkin.com/networking.

Netwerksleutels delen

De meeste Wi-Fi-producten worden geleverd met uitgeschakelde beveiliging. Dus zodra u uw netwerk hebt geïnstalleerd, dient u WEP- of WPA-beveiliging te activeren en ervoor te zorgen dat al uw draadloze apparatuur dezelfde netwerksleutel delen.

Gebruik maken van een hexadecimale sleutel

Een hexadecimale sleutel is een combinatie van cijfers en letters van A t/m F en van 0 t/m 9. 64-bits sleutels bestaan uit vijf tweecijferige getallen. 128-bits sleutels bestaan uit 13 tweecijferige getallen.

Bijvoorbeeld:

AF 0F 4B C3 D4 = 64-bits sleutel

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bits sleutel

Stel in de onderstaande vakken uw sleutel samen door twee letters en/of twee cijfers van A t/m F en 0 t/m 9 in te vullen. U gebruikt deze sleutel om de encryptie-instellingen van uw router en uw draadloze computers te programmeren.

Opmerking voor Mac-gebruikers: De oorspronkelijke Apple AirPort®-producten ondersteunen uitsluitend 64-bits encryptie. Apple AirPort 2-producten kunnen 64-bits en 128-bits encryptie ondersteunen. Controleer dus eerst welk type apparaat u gebruikt. Als het u niet lukt uw netwerk met 128-bits encryptie te configureren, probeer dan 64-bits encryptie.

WEP-setup

1. Selecteer “WEP” in de dropdown-menu.
2. Selecteer een “WEP Mode” van 64-bits of 128-bits.
3. Nadat u de WEP-modus hebt geselecteerd, kunt u uw sleutel invoeren door de hexadecimale sleutel handmatig in te typen.

Een hexadecimale sleutel bestaat uit een combinatie van cijfers en letters van A tot F en van 0 tot 9. Voor 64-bits WEP-encryptie dient u 10 hexadecimale sleutels in te voeren. Voor 128-bits WEP-encryptie dient u 26 hexadecimale sleutels in te voeren.

Bijvoorbeeld:

AF 0F 4B C3 D4 = 64-bits sleutel

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bits sleutel

Wireless > Security

The router can transmit your data securely over the wireless network. Having security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	<input type="radio"/> WEP
WEP Mode >	<input checked="" type="radio"/> 64 bit <input type="radio"/> 128 bit
Key Entry Method >	<input type="radio"/> HEX <input checked="" type="radio"/> ASCII
Key Provisioning >	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Key 1 >	<input type="text"/>
Key 2 >	<input type="text"/>
Key 3 >	<input type="text"/>
Key 4 >	<input type="text"/>
Default Key ID >	<input type="text" value="1"/>
Password >	<input type="checkbox"/>

[Apply Changes](#) [Cancel Changes](#)

3. Klik op “Apply Changes” (Wijzigingen toepassen) om te eindigen. De encryptie in de router is nu ingesteld. Iedere computer binnen uw draadloze netwerk moet nu worden geconfigureerd met dezelfde beveiligingsinstellingen.

WAARSCHUWING: Als u de draadloze router op een computer met een draadloze cliënt configureert, moet u ervoor zorgen dat de beveiliging voor deze draadloze cliënt is ingeschakeld. Als dat niet zo is, zal de draadloze verbinding namelijk verbroken worden.

De beveiligingsinstellingen van het draadloze netwerk wijzigen

Uw router is uitgerust met WPA/WPA2, de nieuwste beveiligingsstandaard voor draadloos netwerkverkeer. Hij ondersteunt tevens de WEP-beveiligingsstandaard. Beveiliging van uw draadloze netwerk is standaard uitgeschakeld. Om beveiliging mogelijk te maken, dient u eerst te bepalen welke standaardinstelling u wilt gebruiken. Om de beveiligingsinstellingen te wijzigen, klik op “Security” (Beveiliging) op het tabblad “Wireless” (Draadloos).

WPA-setup

Opmerking: Om WPA-beveiliging te kunnen gebruiken moeten al uw cliënten geüpgraded zijn naar stuurprogramma’s en software die WPA ondersteunen. U kunt ook gratis een beveiligingspatch van Microsoft downloaden. Deze patch werkt alleen onder het Windows XP-besturingssysteem. U dient tevens van de website van Belkin het nieuwste stuurprogramma te downloaden voor uw draadloze G desktop- of notebookkaart. Andere besturingssystemen worden op dit moment nog niet ondersteund. De patch van Microsoft ondersteunt uitsluitend apparaten zoals 802.11g-producten van Belkin met stuurprogramma’s die WPA ondersteunen.

Er zijn twee soorten WPA-beveiliging: WPA-PSK (zonder server) en WPA (met radiusserver). WPA-PSK (zonder server) gebruikt een zogenaamde “Pre-shared key” (PSK) als beveiligingssleutel. Een pre-shared key is een wachtwoord dat tussen de 8 en 63 tekens lang is. Dit wachtwoord kan zijn opgebouwd uit een combinatie van letters, cijfers en andere tekens. Elke cliënt maakt gebruik van dezelfde sleutel om toegang te krijgen tot het netwerk. Deze modus wordt doorgaans in een woonomgeving gebruikt. WPA (met radiusserver) is een configuratie waarin een radiusserver automatisch de sleutels aan de cliënten toekent. Van deze modus wordt doorgaans in bedrijfsomgevingen gebruik gemaakt. WPA2 is de tweede generatie WPA die gebruik maakt van een complexere encryptietechniek dan WPA.

WPA/WPA2-PSK (zonder server) activeren

1. Selecteer “WPA/WPA2” in het dropdown-menu “Allowed Client Type” (Toegestaan cliënttype).

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >

WPA/WPA2

Authentication >

802.1X Pre-shared Key

Pre-shared Key >

Apply Changes

Clear Changes

2. Voor "Authentication" (Authenticatie), selecteer "Pre-Shared Key" bij standaard gebruik in uw woning of een klein kantoor. Deze instelling moet voor al uw cliënten hetzelfde zijn.
3. Voer uw pre-shared sleutel in. Deze bestaat uit 8 tot 63 tekens, dit kunnen letters, cijfers of symbolen zijn. U dient bij al uw cliënten dezelfde sleutel te gebruiken. Uw pre-shared key kan er als volgt uitzien: "Netwerksleutel familie Jansen".
4. Klik op "Apply Changes" (Wijzigingen toepassen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.

WPA/WPA2 (met radiusserver) instellen

Als uw netwerk een radiusserver gebruikt om de sleutels aan de cliënten toe te wijzen, gebruik dan deze instelling.

1. Selecteer "WPA/WPA2" in het dropdown-menu "Allowed Client Type" (Toegestaan cliënttype).
2. Selecteer "802.1x" als "encryptietechniek" voor omgevingen met RADIUS-servers. Deze instelling moet voor al uw cliënten hetzelfde zijn.
3. Voer de "Session idle timeout" (Maximale niet-actieve tijd) van de radiusserver in in het daarvoor bestemde veld.
4. Voer het sleutelinterval, de frequentie waarmee de sleutels worden verdeeld (in pakketten), in in het veld "Re-Authentication Period" (Re-authenticatieperiode).
5. Voer de wachttijd na authenticatie in in het veld "Quiet Period".
6. Voer het IP-adres en het poortnummer van de radiusserver in in de velden voor "Server-IP" en "Server-Port".
7. Voer de radiussleutel in in het veld "Secret Key" (Geheime sleutel).
8. Klik op "Apply Changes" (Wijzigingen toepassen) om te eindigen. Stel nu al uw cliënten op deze manier in.

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	<input type="text" value="WPA/WPA2"/>
Authentication >	<input checked="" type="radio"/> 802.1X <input type="radio"/> Pre-shared Key
Session Idle Timeout >	<input type="text" value="300"/> seconds (0 for no timeout checking)
Re-Authentication Period >	<input type="text" value="3600"/> seconds (0 for no re-authentication)
Quiet Period >	<input type="text" value="60"/> seconds after authentication failed
Server-IP >	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="2"/> . <input type="text" value="1"/>
Server-Port >	<input type="text" value="1812"/>
Secret Key >	<input type="text"/>
NAS-ID >	<input type="text"/>

Opmerking: Zorg ervoor dat uw draadloze computers geüpdatet zijn, WPA2 ondersteunen en voorzien zijn van de juiste instellingen die een verbinding met de router mogelijk maken.

Uw draadloze G netwerkkaarten van Belkin configureren voor gebruik met beveiliging

Opmerking: Deze paragraaf informeert u over hoe u uw draadloze G netwerkkaarten van Belkin kunt configureren voor gebruik met beveiliging. Op dit moment zou u uw draadloze router of draadloos accesspoint al zo moeten hebben ingesteld dat deze gebruik maakt van WPA of WEP. Om een draadloze verbinding tot stand te kunnen brengen dient u uw draadloze notebook- en desktopkaart te configureren met dezelfde beveiligingsinstellingen.

Uw computer aansluiten op een draadloos netwerk dat een 64-bits of 128-bits WEP-sleutel vereist.

1. Dubbelklik op het signaalindicatorpictogram om het venster “Wireless Network Utility” te laten verschijnen. Als u op de knop “Advanced” (Geavanceerd) drukt, kunt u meer opties van de draadloze netwerkkaart bekijken en configureren.
2. Op het tabblad “Wireless Network Properties” (Eigenschappen draadloos netwerk) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op “Configure” (Configureren).
3. Selecteer “WEP” onder “Data Encryption” (Dataencryptie)
4. Zorg ervoor dat het selectievakje voor “Network key is provided for me automatically” (Netwerksleutel wordt automatisch toegekend), onderaan, niet is aangevinkt. Als u deze computer gebruikt om in te loggen op een bedrijfsnetwerk, vraag dan aan uw netwerkbeheerder of deze optie aangevinkt moet zijn of niet.
5. Typ de WEP-sleutel in in het daarvoor bestemde vakje voor “Network Key” (Netwerksleutel).

1

2

3

4

5

6

7

8

9

10

11

Wireless > Security

Security Mode

Key 1

Key 2

Key 3

Key 4

(hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, input it here

PassPhrase

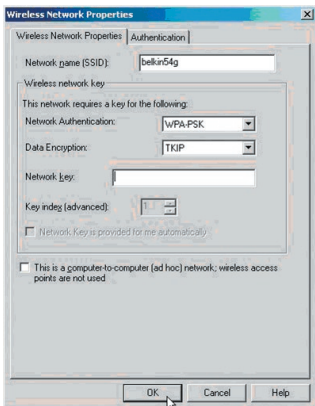
Belangrijk: Een WEP-sleutel is een combinatie van cijfers en letters van A tot F en 0 tot 9. Voor 128-bits WEP-encryptie dient u 26 hexadecimale sleutels in te voeren. Voor 64-bits WEP-encryptie dient u 10 hexadecimale sleutels in te voeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw router.

6. Klik op “OK” om de instellingen op te slaan.

Uw computer aansluiten op een draadloos netwerk dat WPA-PSK vereist (zonder server)

1. Dubbelklik op het signaalindicatorpictogram om het venster “Wireless Network Utility” te laten verschijnen. Als u op de knop “Advanced” (Geavanceerd) drukt, kunt u meer opties van de draadloze netwerkkaart bekijken en configureren.
2. Op het tabblad “Wireless Networks” (Draadloze netwerken) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op “Configure” (Configureren).
3. Selecteer “WPA-PSK (no server)” (WPA-PSK (geen server)) onder “Network Authentication” (Netwerkauthenticatie).
4. Typ de WPA-sleutel in in het daarvoor bestemde vakje voor “Network Key” (Netwerksleutel).

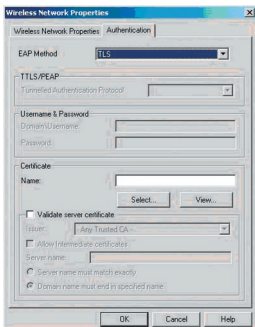
Belangrijk: WPA-PSK is opgebouwd uit een combinatie van cijfers en letters van A tot Z en 0 tot 9. Voor WPA-PSK kunt u 8 tot 63 sleutels invoeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw router.



5. Klik op “OK” om de instellingen op te slaan.

Uw computer aansluiten op een draadloos netwerk dat WPA (met radiusserver) vereist

1. Dubbelklik op het signaalindicatorpictogram om het venster “Wireless Network Utility” te laten verschijnen. Als u op de knop “Advanced” (Geavanceerd) drukt, kunt u meer opties van de draadloze netwerkkaart bekijken en configureren.
2. Op het tabblad “Wireless Networks” (Draadloze netwerken) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op “Configure” (Configureren).
3. Selecteer “WPA” onder “Network Authentication” (Netwerkauthenticatie).
4. Selecteer op het tabblad “Authentication” (Authenticatie) de door uw netwerkbeheerder bepaalde instellingen.
5. Klik op “OK” om de instellingen op te slaan.



WPA instellen voor draadloze desktop- en notebookkaarten die NIET door Belkin zijn gemaakt.

Voor niet-Belkin WPA draadloze desktop- en notebookkaarten die niet zijn voorzien van WPA-enabled software, kunt u gratis van de website van Microsoft een bestand downloaden met de naam “Windows XP Support Patch for Wireless Protected Access”.

Opmerking: Dit bestand van Microsoft werkt alleen met Windows XP. Andere besturingssystemen worden op dit moment nog niet ondersteund.

Belangrijk: U dient ook te controleren of de kaartfabrikant WPA ondersteunt en of u het nieuwste stuurprogramma van hun support site hebt gedownload.

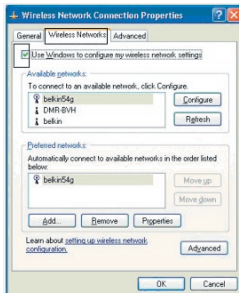
Ondersteunde besturingssystemen:

- Windows XP Professional
- Windows XP Home Edition

De Windows XP Wireless Network Utility instellen voor gebruik met WPA-PSK

Om WPA-PSK te kunnen gebruiken, dient u ervoor te zorgen dat u Windows Wireless Network Utility gebruikt. Dit doet u als volgt:

1. Om WPA-PSK te kunnen gebruiken, dient u ervoor te zorgen dat u Windows Wireless Network Utility gebruikt. Dit doet u als volgt:
2. Klik met de rechter muisknop op “Wireless Network Connection” (Verbinding met draadloos netwerk) en selecteer “Properties” (Eigenschappen).
3. Klik op het tabblad “Wireless Networks” (Draadloze netwerken). Het volgende venster zal verschijnen. Zorg ervoor dat het vakje “Use Windows to configure my wireless network settings” (Gebruik Windows om de instellingen van mijn draadloze netwerk te configureren) is aangevinkt.
4. Klik op het tabblad “Wireless Networks” op de knop “Configure” (Configureren). Het volgende venster zal verschijnen.



5. Voor een netwerk voor thuis- of klein zakelijk gebruik selecteert u onder “Network Authentication” (Netwerkauthenticatie) “WPA-PSK”.

Opmerking: Selecteer “WPA” als u deze computer gebruikt om verbinding te maken met een bedrijfsnetwerk dat een authenticatieserver ondersteunt, zoals bijvoorbeeld een radiusserver. Neem voor meer informatie contact op met uw netwerkbeheerder.



6. Selecteer onder “Data Encryption” (Data-encryptie) “TKIP” of “AES”. Deze instelling moet gelijk zijn aan die van de router.

7. Typ de encryptiesleutel in het vakje voor de netwerksleutel (Network Key) in.

Belangrijk: Voer uw pre-shared sleutel in. Deze bestaat uit 8 tot 63 tekens, dit kunnen letters, cijfers of symbolen zijn. U dient bij al uw cliënten dezelfde sleutel te gebruiken.

8. Klik op “OK” om de instelling te voltooien.

Uitbreiding van het netwerkbereik en bridging

Wat is een draadloze bridge?

Een draadloze bridge is eigenlijk een modus waarvan u gebruik kunt maken. U kunt de bridging-modus gebruiken om het bereik van uw draadloze netwerk uit te breiden of om uw netwerk uit te breiden naar een ander deel van uw kantoor of woning zonder dat u kabels hoeft aan te leggen.

Opmerking: Wij kunnen niet garanderen dat deze functie werkt als u gebruik maakt van hardware van andere fabrikanten.

Opmerking: Ten behoeve van optimale prestaties van uw netwerk, raden wij u aan de meest recente firmware voor de router te downloaden via: <http://web.belkin.com/support>.

Draadloos en nieuw netwerksegment toevoegen

Het aansluiten van een switch of een hub op de RJ45-aansluiting van de router geeft een aantal computers dat aangesloten is op de switch toegang tot de rest van het netwerk.

Zorgen voor een bridge (brug) tussen uw draadloze router en een secundair accesspoint

Als u een “bridge” (brug) tot stand wil brengen tussen uw router van Belkin en een secundair accesspoint, dan dient u het geavanceerde setup-hulpprogramma van de router te starten en het MAC-adres van het accesspoint in te vullen op de daarvoor bestemde plaats. Er zijn nog een paar andere vereisten.

VOLG NAUWGEZET DE VOLGENDE STAPPEN.

1. Stel uw accesspoint in op hetzelfde kanaal als de router. Voor meer informatie over het wijzigen van kanalen verwijzen wij u naar het hoofdstuk “Draadloos - Kanaal en SSID” in deze handleiding.
2. Lokaliseer het MAC-adres van het accesspoint aan de onderzijde van het apparaat. Er staan twee MAC-adressen op het label aan de onderzijde. U heeft het MAC-adres genaamd “WLAN MAC Address” nodig. Het MAC-adres begint met “0030BD”. Hierachter staan zes andere cijfers of letters (i.e. 0030BD-XXXXXX). Schrijf het MAC-adres hieronder op. Ga verder met de volgende stap.
3. Plaats uw secundaire accesspoint binnen het bereik van uw router en dichtbij het gebied waarnaar u uw bereik wilt uitbreiden of waar het netwerksegment dat u wil toevoegen zich bevindt. Binnenshuis ligt het bereik doorgaans tussen de 30 en 60 meter.
4. Sluit uw accesspoint op het elektriciteitsnet aan. Controleer of het accesspoint gevoed wordt en ga verder met de volgende stap.
5. Start het geavanceerde setup-hulpprogramma (Advanced Setup Utility) door uw browser te openen vanaf een computer die al op uw router is aangesloten. In de adresbalk typt u het volgende in: 192.168.2.1. Typ hiervoor geen “www” of “http://” in. Opmerking: Als u het IP-adres van uw router hebt gewijzigd, maak dan gebruik van het nieuwe IP-adres.

Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

1) Wireless Channel must match between Router and AP.
2) Security Settings (WEP) must match between Router and AP.
3) If MAC Filtering is enabled, user must be sure to add the WLAN MAC address(es) of the Router/AP in order to allow communication with each other.

Enable Wireless Bridging. (enabling this feature allows other Access Points to connect to this Access Point.)

Enable ONLY specific Access Points to connect. (enter Wireless MAC Address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Hint: the MAC address can be found using a site survey on a wireless client card.)

AP 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP 3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
AP 4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Disable ability for Wireless CLIENT to connect. (This feature should only be used when the AP is used exclusively to other APs.)

- In uw browservenster verschijnt nu de gebruikersinterface van de router. Klik op “Wireless Bridge” (2) aan de linkerkant van het scherm. U krijgt nu het volgende venster te zien.
- Selecteer de optie “Enable ONLY specific Access Points to connect” (Laat ALLEEN specifieke accesspoints verbinding maken) (1).
- In het veld genaamd “AP1” (3) typt u het MAC-adres van uw secundaire accesspoint in. Nadat u het adres hebt ingetypt, klikt u op “Apply Changes” (Wijzigingen aanbrengen).
- De bridging (brug) is nu opgezet.

Opmerking: Het kan een minuut duren voordat de brug (bridge) gecreëerd is. In sommige gevallen moet u het accesspoint of de router herstarten om de brug tot stand te brengen.

Firewall

Uw router is voorzien van een firewall die uw netwerk beschermt tegen uiteenlopende hackeraanvallen zoals:

- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP met lengte nul
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

De firewall schermt ook gewone poorten af die vaak gebruikt worden om netwerken aan te vallen. Deze poorten zijn dan onzichtbaar gemaakt waardoor zij voor hackers eenvoudigweg niet lijken te bestaan. U kunt de firewallfunctie eventueel uitschakelen hoewel het aanbeveling verdient de firewall ingeschakeld te laten. Het uitschakelen van de firewall laat uw netwerk niet volledig onbeschermd tegen een aanval van hackers, maar wij raden u toch aan de firewall geactiveerd te houden.

Firewall >

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable / Disable > Enable Disable

Virtuele servers

Via “Virtual Servers” kunt u externe (Internet)verbindingen voor diensten zoals een webserver (poort 80), FTP-server (poort 21), of andere applicaties, via uw router doorsturen naar uw interne netwerk. Aangezien uw interne computers beschermd worden door een firewall, kunnen computers buiten uw netwerk (via het Internet) de interne computers niet bereiken omdat ze niet “zichtbaar” zijn. Als u de functie “virtuele server” voor een specifieke applicatie dient te configureren, neem dan contact op met de leverancier van de applicatie om geïnformeerd te worden over welke poortinstellingen u nodig hebt. U kunt deze poortinformatie handmatig in de router vastleggen.

Firewall > Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. [View Info](#)

ID	LAN IP address	Description	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.1.1		TCP			<input type="checkbox"/>	Set Clear
2	192.168.1.1		TCP			<input type="checkbox"/>	Set Clear
3	192.168.1.1		TCP			<input type="checkbox"/>	Set Clear

Applicaties kiezen

Selecteer de applicatie in het dropdown-menu. Klik op “Add” (Toevoegen). De instellingen worden overgebracht naar de eerste beschikbare regel. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de instelling voor deze applicatie op te slaan. Om een applicatie te verwijderen, selecteert u het nummer van de regel die u wilt verwijderen en vervolgens klikt u op “Clear” (Leeg maken).

Instellingen handmatig in de virtuele server invoeren

Om instellingen handmatig in te voeren, typt u het IP-adres in het vak voor de interne (server) computer in, geeft u de poort(en) op die vrijgegeven moeten worden, selecteert u het poorttype (TCP of UDP) en klikt u op “Apply Changes” (Wijzigingen aanbrengen). Voor elke binnenkomende poort zijn er twee velden in elk waarvan u maximaal 5 karakters kunt invoeren waarmee u begin en eind van het poortbereik kunt aangeven, bijvoorbeeld: [xxxxx]-[xxxxx]. Voor elke invoerpoort kunt u een enkele waarde invoeren door in de twee velden dezelfde waarde te typen (bijv. [7500]-[7500]) of kiezen voor een breed poortbereik (bijv. [7500]-[9000]). Als u meerdere enkelvoudige poortwaarden nodig heeft of een combinatie van bereiken en een enkelvoudige waarde, dient u meervoudige invoeren tot een maximum van 20 te gebruiken (bijv. 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). U kunt per intern IP-adres slechts één poort vrijgeven. U neemt een zeker risico door poorten in uw firewall te openen. U kunt instellingen zeer snel in- en uitschakelen. Het is beter de instellingen uit te schakelen wanneer u een specifieke applicatie niet gebruikt.

IP-filters cliënt

De router kan zo worden geconfigureerd dat toegang tot het Internet, e-mail of andere netwerkdiensten op bepaalde dagen en tijden beperkt is. Deze beperking kan worden ingesteld voor één computer, een groep computers of verscheidene computers.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [View Info](#)

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function > Enable Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
Go To URL Blocking Rule ID				

> Add PC

Apply Changes

Toegangscontrole

Access control (toegangscontrole) stelt gebruikers in staat te definiëren welk uitgaand dataverkeer wel en niet toegaan tot de WAN-interface krijgt. De standaardinstelling is dat al het uitgaande verkeer wordt doorgelaten. Om toegang voor uw computers te beperken, gaat u als volgt te werk:

1. Klik op “Add PC” (PC toevoegen) op het scherm “Access Control” (Toegangscontrole).
2. Definieer de juiste instelling voor cliënt PC services (zoals getoond op het volgende scherm).

Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [View Info](#)

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PC's, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Rule" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address > -

> Client PC Service:

Service Name	Default Description	Blocking
globe	HTTP, TCP Port 80, 110, 8080, 8081, 8082	<input checked="" type="checkbox"/>
WWW with URL Blocking	HTTP (with URL Blocking Rule Page)	<input checked="" type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input checked="" type="checkbox"/>
Open Forum	HTTP, TCP Port 113	<input checked="" type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input checked="" type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input checked="" type="checkbox"/>
Web Messenger	TCP Port 1863	<input checked="" type="checkbox"/>
Other Services	TCP Port 22	<input checked="" type="checkbox"/>

3. Klik op “OK” en vervolgens op “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan.

URL Blocking (URL-blokking)

Om de functie URL-blokking te configureren, specificceert u de websites (www.eenbepaaldesite.com) en/of trefwoorden waarop gefilterd dient te worden. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijziging te activeren. Om de configuratie te voltooien, dient u een toegangsregel te creëren of te wijzigen in het “Client IP filters” deel. Om een bestaande regel te wijzigen, klikt u op de knop “Edit” (Wijzigen) naast de regel die u wenst te wijzigen. Om een nieuwe regel te creëren, klikt u op de “Add PC” (PC toevoegen) optie. Via “Access Control > Add PC”, kunt u de optie voor “WWW with URL Blocking” (WWW met URL-blokking) in de “Client PC Service”-tabel aanvinken, zodat u op de websites en trefwoorden die u hebt opgegeven, kunt filteren.

Handmatige configuratie van de router

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

To configure the URL Blocking feature, use the table below to specify the websites ([www.somewhere.com](#)) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section. To modify an existing rule, click the "Edit" option next to the rule you want to modify. To create a new rule, click on the "Add PC" option.

From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below...

Rule Number	URL / Keyword
SNL_1	
SNL_2	
SNL_3	
SNL_4	
SNL_5	

Schemaregel

U kunt op basis van regels filteren en zo bepalen welke lokale cliënten wel en niet internettoegang krijgen. Elke toegangscontroleregels kan op een specifiek moment worden geactiveerd. Bepaal het schema "Schedule Rule" (Schemaregel) en pas de regel toe op de pagina "Access Control" (Toegangscontrole).

Volg deze stappen om een schema toe te voegen:

1. Klik op "Add Schedule Rule" (Schemaregel toevoegen).
2. U krijgt nu het volgende venster te zien.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Rule Name	Rule Comment	Configure
	No Valid Schedule Rule ID	

> Add Schedule Rule

[Clear Changes](#) [Apply Changes](#)

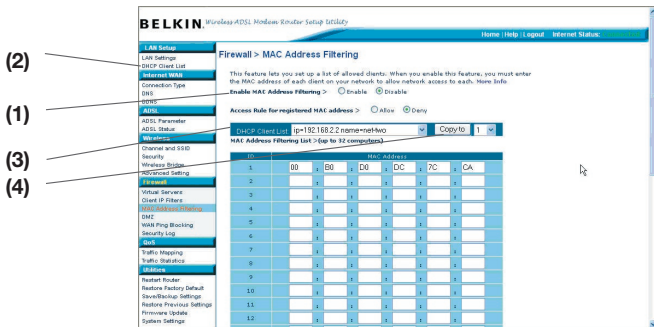
3. Om de schemaregel te configureren, specificeert u de naam, opmerking, begintijd en eindtijd waarop u wilt filteren binnen uw netwerk.
4. Klik op "OK" en vervolgens op "Apply Changes" (Wijzigingen aanbrengen) om de instellingen op te slaan.
5. Om de configuratie te voltooien, dient u een toegangsregel te creëren of te wijzigen in het "Client IP filters" deel. Zo wordt het schema geactiveerd waarvan gebruik wordt gemaakt op de "Access Control"-pagina.

MAC-adressenfilter instellen

Het MAC-adressenfilter is een krachtig beveiligingsinstrument waarmee u kunt aangeven welke computers toegang hebben tot het netwerk. Elke computer die probeert het netwerk binnen te komen maar die niet in de filterlijst voorkomt, wordt de toegang geweigerd. Wanneer u deze functie aanzet, dient u het MAC-adres in te voeren van iedere cliënt (computer) op uw netwerk om ieder van deze computers toegang te geven tot het netwerk. Met de functie “Block” (Blokkeren) kunt u de toegang tot het netwerk voor elke computer eenvoudig in- en uitschakelen zonder dat u verplicht bent het MAC-adres van deze computer aan de lijst toe te voegen of daaruit te verwijderen. Om deze functie te activeren, selecteert u “Enable MAC Address Filtering” (1) (MAC-adres-filter activeren). Selecteer vervolgens “Allow” (Toelaten) of “Deny” (Weigeren) voor de toegangsregel.

Voer vervolgens het MAC-adres van elke computer binnen uw netwerk, door ze een voor een te selecteren in het dropdown-menu “DHCP Client List” (2) en te klikken op “Copy to”. Zorg ervoor dat u niet twee keer hetzelfde adres kopieert. U kunt ook klikken op de gegeven ruimte (4) en het MAC-adres van de computer die u aan het overzicht wilt toevoegen, invoeren. Klik op “Apply Changes” (Wijzigingen aanbrengen) (5) om de instellingen op te slaan. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan.

Opmerking: Het MAC-adres van de computer waarmee u toegang hebt tot de beheerfuncties van de router (dus de computer die u nu gebruikt) kunt u niet verwijderen.



DMZ (Gedemilitariseerde zone)

Indien een van uw cliënten van achter de firewall geen internetapplicatie kan draaien, kunt u deze cliënt onbeperkte tweewegs internettoegang verstrekken. Dit kan nodig zijn wanneer de NAT-functie problemen veroorzaakt met applicaties als games en videoconferenties. Het is raadzaam deze functie alleen tijdelijk te gebruiken. De computer in de gedemilitariseerde zone wordt namelijk niet beschermd tegen hackeraanvallen.

Handmatige configuratie van de router

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** [More Info](#)

DMZ > ENABLE DISABLE

> IP Address of Virtual DMZ Host

Static IP	Static IP
1	192.168.2.0
2	192.168.2.0
3	192.168.2.0
4	192.168.2.0
5	192.168.2.0
6	192.168.2.0
7	192.168.2.0
8	192.168.2.0

Om een computer in de gedemilitariseerde zone te plaatsen, vult u de laatste cijfers van het IP-adres van die computer in in het IP-veld. Vervolgens selecteert u “Enable” (Activeren). Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijziging te activeren. Als u meerdere statische WAN IP-adressen gebruikt, kunt u aangeven aan welk WAN IP-adres de DMZ-host wordt gericht. Vul het WAN IP-adres in waaraan de DMZ-host moet worden gericht, voer de laatste twee cijfers in van het IP-adres van de DMZ-hostcomputer, selecteer “Enable” (Activeren) en klik op “Apply Changes” (Wijzigingen aanbrengen).

ICMP-pings blokkeren

Computerhackers maken gebruik van een techniek die bekend is onder de naam “pingen” om potentiële slachtoffers op het Internet te vinden. Door naar een bepaald IP-adres te pingen en een reactie te ontvangen van het IP-adres, kan een



hacker vaststellen of zich daar misschien iets interessants bevindt. De router kan zo worden ingesteld dat hij niet op ICMP-pings van buiten reageert. Hierdoor wordt de veiligheidsmarge van uw router verhoogd.

Om het ping-antwoordbericht uit te schakelen, selecteert u “Block ICMP Ping” (ICMP-ping blokkeren) (1) en klikt u op “Apply Changes” (Wijzigingen aanbrengen). De router reageert nu niet meer op een ICMP-ping.

Hulprogramma's

In het scherm "Utilities" (Hulprogramma's), kunt u verschillende parameters van de router beheren en bepaalde beheerfuncties uitvoeren.

Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Restart Router**
Sometimes it may be necessary to Reset or Reboot the Router if it begins working improperly. Resetting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Defaults**
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Current Settings**
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Saved Settings**
This option will allow you to restore a previously saved configuration.
- **Firmware Update**
From time to time, Linksys may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
- **System Settings**
The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the NAT function of the Router.

De router herstarten

Als de werking van de router niet meer optimaal is, kan het soms nodig zijn de router opnieuw te starten. De configuratie-instellingen van de router worden door opnieuw starten NIET gewist.

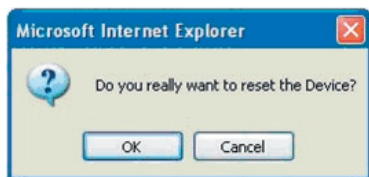
Utilities > Restart Router

Sometimes it may be necessary to Restart or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.

Restart Router

De router opnieuw starten om de normale werking te herstellen

1. Klik op de knop "Restart Router" (Herstart de router).
2. Nu verschijnt het volgende bericht. Klik op "OK" om uw router te herstarten.



Fabrieksinstellingen herstellen

Wanneer u deze optie gebruikt, worden alle instellingen in de router naar de (standaard) fabrieksinstellingen teruggezet. Het is verstandig eerst van uw eigen instellingen een reservekopie te maken voordat u de standaardinstellingen herstelt.

Utilities > Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.

Restore Defaults

Handmatige configuratie van de router

1. Klik op de knop "Restore Defaults" (standaardinstellingen herstellen).
2. Nu verschijnt het volgende bericht. Klik op "OK" om de standaard fabrieksinstellingen te herstellen.

Huidige instellingen opslaan/als backupbestand opslaan

Van deze functie kunt u de huidige configuratie opslaan. Door een reservekopie te maken van uw huidige configuratie kunt u deze in het geval van verlies of beschadiging herstellen. Het is raadzaam een reservekopie te maken van uw huidige configuratie voordat u uw firmware bijwerkt.

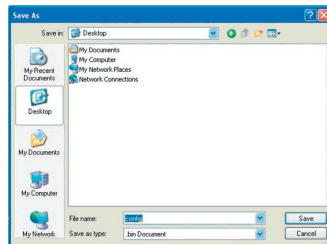
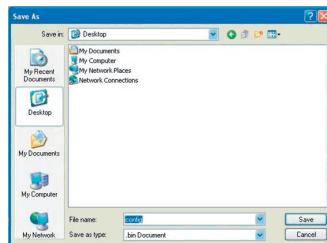
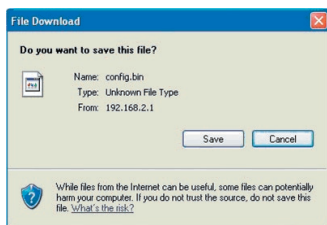
1. Klik op "Save" (Opslaan). Er gaat een venster open met de naam "File Download" (Bestand downloaden). Klik op "Save" (Opslaan).
2. Een scherm wordt geopend waarin u de locatie kunt selecteren waar u het configuratiebestand wilt opslaan. Selecteer een locatie. U kunt zelf bepalen hoe u het bestand noemt. Wij raden u echter aan er bij de naamgeving rekening mee te houden dat u het bestand nog wel terug moet kunnen vinden. Wanneer u de locatie hebt geselecteerd en de naam van het bestand hebt ingevoerd, klikt u op "Save" (Opslaan).



UTILITIES > Save/Backup current settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

OK



3. Als het bestand is opgeslagen, ziet u het onderstaande scherm. Klik op “Close” (Sluiten). De configuratie is nu bewaard.

Utilities > Restore Previous Settings

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the “Restore” button below.



Vorige instellingen herstellen

Met deze optie kunt u een eerder opgeslagen configuratie herstellen.

1. Klik op “Browse” (Zoeken). Er gaat een venster open waarin u de locatie van het configuratiebestand kunt selecteren. Zoek het configuratiebestand “config.bin” op en dubbelklik erop.
2. Klik vervolgens op “Open” (Openen).

Firmware bijwerken

Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click here](#) to go to the Save/Backup current settings page.



Af en toe brengt Belkin een nieuwe versie uit van de firmware voor de router. Nieuwe firmwareversies bevatten verbeteringen van functies en oplossingen voor eventuele problemen. Wanneer Belkin nieuwe firmware publiceert, kunt u de firmware downloaden van de Belkin update-website en de firmware van de router bijwerken tot en met de nieuwste versie.

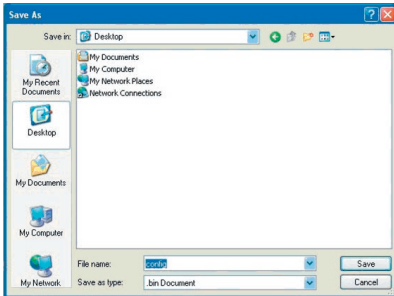
Beschikbaarheid van nieuwe firmwareversies nagaan

Met de knop “Check Firmware” (Firmware controleren) (1) kunt u onmiddellijk nagaan of er eventueel een nieuwe firmwareversie beschikbaar is. Als u op de knop klikt, verschijnt er een browservenster waarin wordt aangegeven dat er geen nieuwe firmware beschikbaar is, of dat er een nieuwe versie beschikbaar is. Als er een nieuwe versie beschikbaar is, kunt u deze downloaden.

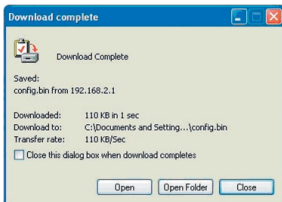
Een nieuwe firmwareversie downloaden

Als u op de knop “Check Firmware” (Firmware controleren) klikt en er een nieuwe firmwareversie beschikbaar is, verschijnt er een scherm dat lijkt op onderstaande afbeelding.

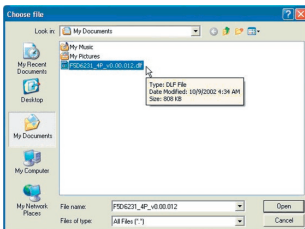
Handmatige configuratie van de router



1. Om de nieuwe firmwareversie te downloaden, klikt u op “Download”.
2. Er gaat een venster open waarin u de locatie kunt aangeven waar u het firmwarebestand wilt opslaan. Selecteer een locatie. U kunt het bestand elke naam geven die u wilt, of gewoon de standaard naam gebruiken. Zorg ervoor dat u het bestand later ook weer terug kunt vinden. Zodra u een locatie hebt geselecteerd, klikt u op “Save” (Opslaan).



3. Als het bestand is opgeslagen, ziet u het onderstaande scherm. Klik op “Close” (Sluiten). De firmware is gedownload. Om de firmware bij te werken, gaat u te werk als aangegeven in het volgende hoofdstuk “Firmware van de router bijwerken”.



Firmware van de router bijwerken

1. Op de pagina “Firmware Update” (Firmware bijwerken) klikt u op “Browse” (Zoeken) (2). Er gaat een venster open waarin u de locatie van het bijgewerkte firmwarebestand kunt selecteren.
2. Blader naar het firmwarebestand dat u hebt gedownload. Selecteer het bestand door dubbel te klikken op de bestandsnaam.

3. Het venster “Update Firmware” (Firmware bijwerken) toont nu de locatie en de naam van het firmwarebestand dat u zojuist hebt geselecteerd. Klik op “Update” (Bijwerken).

Utilities > Firmware Update

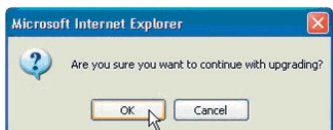
From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click Here](#) to go to the Save/Backup current settings page.

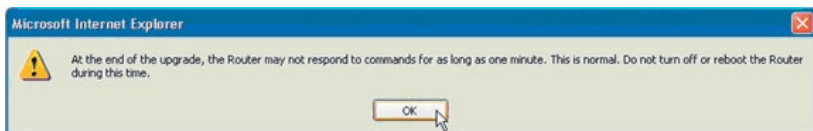
Firmware Version > 3.01.05
Check for new firmware version >

Update Firmware >

4. U krijgt de vraag of u zeker weet dat u wilt doorgaan. Klik op "OK".



5. U krijgt nu nog een bericht te zien. Dit bericht laat u weten dat de router mogelijk pas na één minuut reageert tijdens het laden van de firmware en dat de router opnieuw wordt opgestart. Klik op "OK".



Op het scherm wordt van 60 seconden naar 0 seconden afgeteld. Zodra de nul bereikt is, zal de firmware van de router zijn bijgewerkt. De homepage van de router zou nu automatisch moeten verschijnen. Als dat niet gebeurt, typ dan het adres van de router in de navigatiebalk van uw browser in (standaard = 192.168.2.1).

Systeminstellingen

Op de pagina "System Settings" (Systeminstellingen) kunt u een nieuw wachtwoord invoeren voor de systeembeheerder, de tijdzone instellen, beheer op afstand inschakelen en de UPnP-functie van de router in- en uitschakelen.

Het wachtwoord voor de systeembeheerder instellen of wijzigen

De router wordt geleverd ZONDER vooraf geprogrammeerd wachtwoord. Als u een wachtwoord wilt toevoegen voor meer beveiliging, dan kunt u hier een wachtwoord instellen. Schrijf het wachtwoord op en bewaar het op een veilige plaats, aangezien u het nodig hebt als u in de toekomst wilt inloggen op de router. Het is ook verstandig een wachtwoord in te stellen als u van plan bent de mogelijkheid van extern beheer van uw router te gebruiken.

Utilities > System Settings

Administrator Password:

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

De inlog-timeoutinstelling wijzigen

Met de optie inlog-timeout kunt u de maximale tijdsduur instellen waarbinnen u ingelogd kunt blijven op de Advanced Setup Interface (Geavanceerde setup-interface) van de router. De timer start als er geen activiteit is geweest. U hebt bijvoorbeeld een aantal wijzigingen in de geavanceerde gebruikersinterface aangebracht en daarna uw computer alleen gelaten zonder op “Logout” (Afmelden) te klikken. Als de timeout is ingesteld op 10 minuten, dan loopt de inlogsessie 10 minuten nadat u de router alleen hebt gelaten af. Als u nog meer wijzigingen wilt aanbrengen, moet u zich opnieuw aanmelden bij de router. Deze inlog-timeoutoptie is bedoeld als extra beveiliging en staat standaard ingesteld op 10 minuten. Opmerking: Er kan slechts één computer tegelijk ingelogd zijn op de geavanceerde Setup-Interface van de router.

Tijd en tijdzone instellen

De tijd klok van de router wordt geregeld via de aansluiting op een SNTP (Simple Network Time Protocol) server. Hierdoor loopt de systeemklok van de router synchroon met de tijd van het wereldwijde Internet. De gesynchroniseerde klok in de router wordt gebruikt voor de registratie van de beveiligingslog en de aansturing van de cliëntfilter. Selecteer de tijdzone waarin u zich bevindt. Als u in een land woont dat de zomer- en wintertijd volgt, selecteer dan de optie “Enable Daylight Saving” (Zomer/wintertijd inschakelen). De systeemklok geeft niet onmiddellijk na inschakeling de juiste tijd aan. De router heeft ten minste 15 minuten nodig om een verbinding op te bouwen met de tijdservers op het Internet en voor het ontvangen van een antwoordsignaal. U kunt de klok niet zelf

instellen. U heeft nu de mogelijkheid een primaire en een back-up NTP-server te selecteren zodat de klok van uw router synchroon loopt met de verschillende NTP-tijdservers op het Internet. Selecteer de gewenste NTP-server in het dropdown-menu's, of gebruik de huidige instelling.

The screenshot shows the 'Time and Time Zone' configuration page. At the top, it displays the current time as 'August 1, 2003 4:26:00 AM'. Below this, there is a section for 'Daylight Savings' with an unchecked checkbox. The 'Set Time Zone' dropdown menu is set to '(GMT-08:00)Pacific Time (US & Canada), Tijuana'. Under 'Configure Time Server (NTP)', the 'Enable Automatic Time Server Maintenance' checkbox is checked. The 'Primary Server' dropdown is set to '132.163.4.102 - North America' and the 'Secondary Server' dropdown is set to '192.5.41.41 - North America'. An 'Apply Changes' button is located at the bottom of the form.

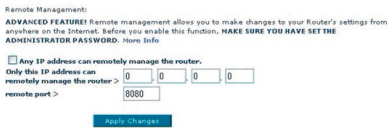
Beheer op afstand mogelijk maken

ZORG ERVOOR DAT U HET BEHEERDERSWACHTWOORD HEBT INGESTELD voordat u deze geavanceerde functie van uw router inschakelt. De functie “Remote Management” (Beheer op afstand) biedt u de mogelijkheid vanaf elke internetlocatie ter wereld de instellingen van uw router te wijzigen.

Er zijn twee methoden voor het op afstand beheren van de router. Met de eerste kunt u de router vanaf elke internetlocatie openen door het selecteren van “Any IP address can remotely manage the Router” (Elk IP-adres kan de router op afstand beheren). Wanneer u uw WAN IP-adres intypt vanaf iedere willekeurige computer op het Internet, dan krijgt u een inlogscherm te zien waarin u het wachtwoord van uw router moet invoeren. De tweede methode is een specifiek IP-adres uitsluitend te bestemmen voor het op afstand beheren van de router. Deze methode is veiliger, maar minder praktisch. Bij deze methode vult u in de daarvoor bestemde ruimte het IP-adres in van de computer waarmee u toegang tot de router wilt hebben en selecteert u “Only this IP address can remotely manage the Router” (Uitsluitend dit IP-adres kan de router op afstand beheren).

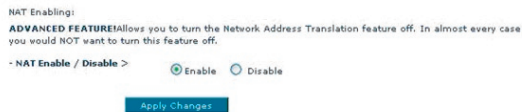
Voordat u deze functie inschakelt, RADEN WIJ U TEN ZEERSTE AAN uw systeembeheerderwachtwoord in te stellen. Als u geen wachtwoord gebruikt, loopt uw router het risico van indringers. De “Remote Access”-poort (poort voor toegang op afstand) is standaard poort 8080. U kunt een andere poort opgeven door een nieuw

poortnummer in te vullen in het veld voor de “remote port” (Poort op afstand). Klik op de knop “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan.



Network Address Translation (NAT) inschakelen/uitschakelen

Opmerking: Deze geavanceerde functie mag uitsluitend door ervaren gebruikers worden toegepast. ZORG ERVOOR DAT U HET BEHEERDERSWACHTWOORD HEBT INGESTELD voordat u deze functie inschakelt. NAT is de methode waarvan de router gebruik maakt voor het delen van het enkele IP-adres dat uw ISP heeft toegekend met de andere computers binnen uw netwerk. Deze functie dient uitsluitend te worden gebruikt als uw provider u meerdere IP-adressen toekent of als u NAT moet uitschakelen in verband met een geavanceerde systeemconfiguratie. Als u slechts een enkel IP-adres heeft en u schakelt NAT uit, dan zullen de computers binnen uw netwerk geen gebruik kunnen maken van het Internet. Andere problemen kunnen ook voorkomen. Door het uitschakelen van NAT worden uw firewallfuncties niet uitgeschakeld.



Universal Plug-and-Play (UPnP) in/uitschakelen.

UPnP is weer een andere geavanceerde mogelijkheid van uw router van Belkin. Het is een technologie die naadloze voice- en video-messaging, games en andere applicaties mogelijk maakt die voldoen aan UPnP.

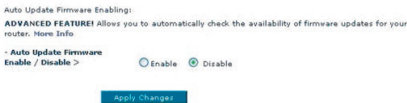
Sommige applicaties vereisen dat de firewall van de router op een bepaalde manier is geconfigureerd om correct te functioneren. Hiervoor moeten doorgaans de TCP- en UDP-poorten worden geopend en in sommige gevallen triggerpoorten worden ingesteld. Applicaties die voldoen aan UPnP kunnen met de router communiceren, in principe om de router te “vertellen” op welke wijze de firewall moet worden geconfigureerd. Bij levering van de router is de UPnP-functie gedeactiveerd. Als u applicaties gebruikt die voldoen aan UPnP en u wilt profiteren van de mogelijkheden van UPnP dan heeft het zin de UPnP-functie in te schakelen. U selecteert eenvoudigweg “Enable” (Inschakelen) in de paragraaf



“UPnP Enabling” (UPnP inschakelen) van de pagina “Utilities” (Hulpprogramma’s). Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijziging op te slaan.

Automatische firmware-update activeren/deactiveren

Deze vernieuwing geeft de router de ingebouwde mogelijkheid automatisch te controleren of er een nieuwe versie bestaat van de firmware en u te waarschuwen als de nieuwe firmware beschikbaar is. Als u inlogt op de geavanceerde web-based gebruikersinterface van de router, zal de router controleren of er nieuwe firmware beschikbaar is. Als er nieuwe firmware gedownload kan worden, wordt u daarvan op de hoogte gesteld. U kunt er dan voor kiezen de nieuwe versie te downloaden



of verder te gaan met hetgene waar u mee bezig was. Bij levering van de router is deze functie gedeactiveerd. Als u deze functie wilt activeren, selecteert u “Enable” (Activeren) en klikt u op “Apply Changes” (Wijzigingen aanbrengen).

Configuratie van uw computers

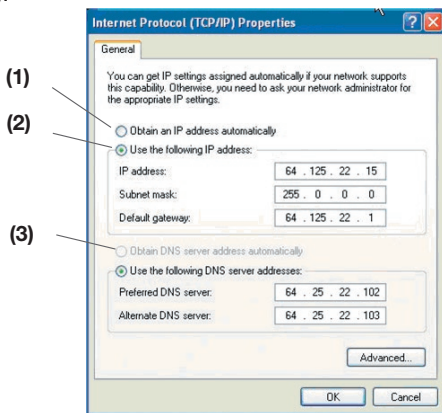
Om ervoor te zorgen dat uw computer correct met uw router kan communiceren, dient u de “TCP/IP/Ethernet”-instellingen van uw computer te wijzigen in: “Obtain an IP address automatically/Using DHCP” (IP-adres automatisch ophalen/Gebruik maken van DHCP) Dit is de standaardinstelling voor de meeste homecomputers.

Handmatige configuratie van netwerkadapters

Installeer EERST de computer die is verbonden met het ADSL-modem. Volg daarbij de volgende stappen. U kunt deze stappen ook gebruiken om computers aan uw router toe te voegen nadat de router geconfigureerd is voor aansluiting op het Internet.

Windows XP, 2000 of NT

1. Klik op “Start”, “Settings” (Instellingen) en vervolgens “Control Panel” (Configuratiescherm).
2. Dubbelklik op het pictogram “Network and dial-up connections” (Netwerk- en inbelverbindingen) (Windows 2000) of het pictogram “Network” (Netwerk) (Windows XP).



3. Klik met uw rechter muisknop op de “Local Area Connection” (Lokale verbinding) die is gekoppeld aan uw netwerkadapter en selecteer “Properties” (Eigenschappen) in het dropdown-menu.
4. In het venster “Local Area Connection Properties” klikt u op “Internet Protocol (TCP/IP)” en klik u op de knop “Properties” (Eigenschappen). Nu verschijnt het volgende scherm:
5. Als “Use the following IP address” (Gebruik het volgende IP-adres) (2) is geselecteerd, moet uw router worden geconfigureerd voor een statisch type IP-verbinding. Noteer de adresinformatie in de afgebeelde tabel. U dient deze informatie in de router in te voeren.

1
2
3
4
5
6
7
8
9
10
11

Handmatige configuratie van netwerkadapters

- Als dit niet al is geselecteerd, selecteert u “Obtain an IP address automatically” (1) en “Obtain DNS server address automatically” (3). Klik op “OK”. Uw netwerkadapter(s) is (zijn) nu geconfigureerd voor gebruik met de router.

Windows 98SE of Me

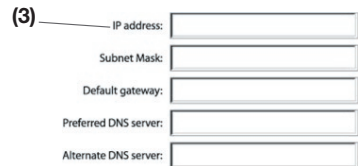
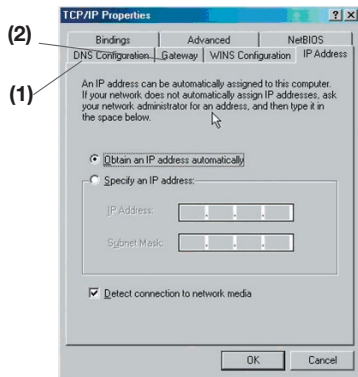
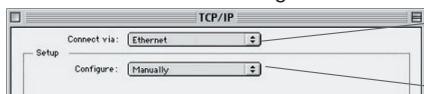
- Klik in het dropdown-menu met uw rechter muisknop op “My Network Neighbourhood” (Mijn netwerkomgeving).
- Selecteer “TCP/IP -> settings” (TCP/IP-instellingen) voor uw geïnstalleerde netwerkadapter. Het volgende venster zal verschijnen.
- Als “Specify an IP address” (IP-adres specificeren) is geselecteerd, moet u de router configureren voor verbinding met een statisch IP. Noteer de adresinformatie in de afgebeelde tabel. U dient deze informatie in de router in te voeren.
- Schrijf het IP-adres en subnetmasker over van het tabblad “IP Address” (IP-adres) (3).

- Klik op het tabblad “Gateway” (2). Vul het gatewayadres in het diagram in.
- Klik op het tabblad “DNS Configuration” (DNS-configuratie) (1). Schrijf het DNS-adres/de DNS-adressen in het diagram.
- Als dit niet al is geselecteerd, selecteert u op het tabblad voor IP-adressen “Obtain an IP address automatically” (IP-adres automatisch ophalen). Klik op “OK”. Start de computer opnieuw. Wanneer de computer opnieuw is opgestart, zijn uw netwerkadapters geconfigureerd voor gebruik met de router. Installeer EERST de computer die is verbonden met het kabel- of DSL-modem. Volg daarbij de volgende stappen. U kunt deze stappen ook gebruiken om computers aan uw router toe te voegen nadat de router geconfigureerd is voor aansluiting op het Internet.

Mac OS tot 9.x

Om ervoor te zorgen dat uw computer correct met uw router kan communiceren, dient u de TCP/IP-instellingen van uw Mac-computer in te stellen op DHCP.

- Open het “Apple”-menu. Selecteer “Control Panels” (Configuratieschermen) en dan “TCP/IP”.
- U ziet nu het TCP/IP-configuratiescherm. Selecteer “Ethernet Built-In” (Ethernet ingebouwd) of “Ethernet” in het dropdown-menu “Connect via:” (Verbinding maken via) (1).

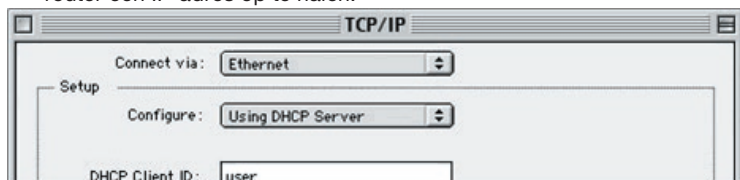


Handmatige configuratie van netwerkadapters

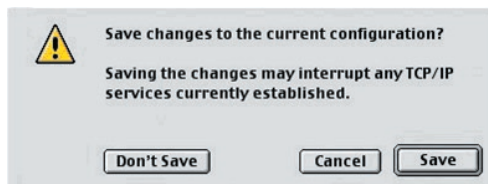
3. Als naast “Configure” (Configureren) (2), “Manually” (Handmatig) is geselecteerd, moet uw router worden geconfigureerd voor een verbinding met een statisch IP. Noteer de adresinformatie in de afgebeelde tabel. U zal deze informatie in de router moeten invoeren.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

4. Als dit niet al bij “Configure:” is ingesteld, kiest u “Using DHCP Server” (Gebruikt DHCP-server). Hierdoor geeft u de computer de opdracht bij de router een IP-adres op te halen.



5. Sluit het venster. Als u veranderingen hebt aangebracht, verschijnt het volgende venster. Klik op “Save” (Opslaan).



Start de computer opnieuw. Wanneer de computer opnieuw is opgestart, zijn uw netwerkinstellingen geconfigureerd voor gebruik met de router.

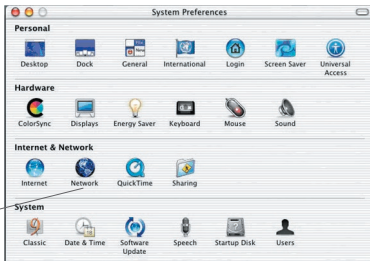
Mac® OS X

1. Klik op het pictogram “System Preferences” (Systeemvoorkeuren).

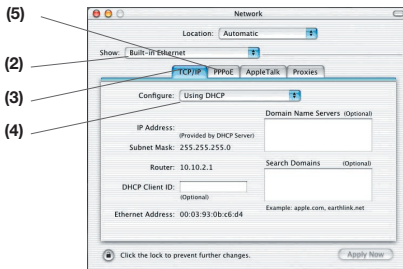


Handmatige configuratie van netwerkadapters

2. Selecteer “Network” (Netwerk) (1) in het menu “System Preferences” (Systeemvoorkeuren).



3. Selecteer “Built-in Ethernet” (Ingebouwd Ethernet) (2) naast “Show” (Tonen) in het “Network”(Netwerk)-menu.
4. Selecteer het tabblad “TCP/IP” (3). Naast “Configure” (Configureren) (4) moet nu “Manually” (Handmatig) of “Using DHCP” (Gebruikt maken van DHCP) te zien zijn. Is dat niet het geval, ga dan naar het tabblad PPPoE (5) en zorg ervoor dat “Connect using PPPoE” (Met behulp van PPPoE verbinding maken) NIET is geselecteerd. Als dit wel het geval is, dan moet u uw router configureren voor een verbinding van het type PPPoE met behulp van uw gebruikersnaam en wachtwoord.



5. Als “Manually” (Handmatig) is geselecteerd, moet uw router worden geconfigureerd voor een statisch type IP-verbinding. Noteer de adresinformatie in de afgebeelde tabel. U zal deze informatie in de router moeten invoeren.
6. Als dit niet al is geselecteerd, selecteert u naast “Configure” (Configureren) (4) “Using DHCP” (DHCP gebruiken) en klikt u vervolgens op “Apply Now” (Nu toepassen).

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

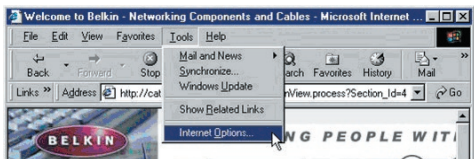
Uw netwerkadapter(s) is/zijn nu geconfigureerd voor gebruik met de router.

Aanbevolen instellingen van de webbrowser

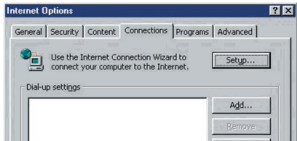
Meestal hoeft u aan de instellingen van uw webbrowser niets te veranderen. Als u problemen hebt met de toegang tot het Internet of de geavanceerde web-based gebruikersinterface, wijzig dan de huidige instellingen van uw browser in de aanbevolen instellingen die u in dit hoofdstuk vindt.

Microsoft Internet Explorer 4.0 of hoger

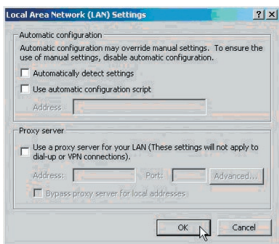
1. Start uw webbrowser. Selecteer “Tools” (Extra) en vervolgens “Internet Options” (Internetopties).



2. In het scherm “Internet Options” (Internetopties) vindt u drie keuzemogelijkheden. “Never dial a connection” (Nooit een verbinding maken), “Dial whenever a network connection is not present” (Maak verbinding indien er geen netwerkverbinding aanwezig is) en “Always dial my default connection” (Altijd mijn standaardverbinding gebruiken). Als u een keus kunt maken, selecteer dan “Never dial a connection” (Nooit een verbinding maken). Als u geen keus kunt maken, ga dan naar de volgende stap.



3. Klik onder het scherm “Internet Options” (Internetopties) op “Connections” (Aansluitingen) en selecteer “LAN Settings...” (LAN-instellingen).
4. Zorg ervoor dat er geen selectievakjes aangevinkt zijn naast de geboden opties: “Automatically detect settings” (Instellingen automatisch detecteren), “Use automatic configuration script” (Script voor automatische configuratie gebruiken) en “Use a proxy server” (Proxyserver gebruiken). Klik op “OK”. Klik vervolgens op de pagina “Internet Options” (Internetopties) opnieuw op “OK”.

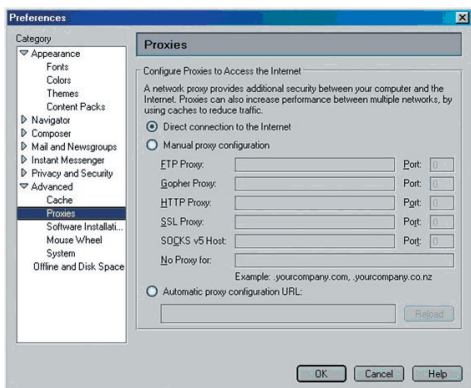


1
2
3
4
5
6
7
8
9
10
11

Hoofdstuk

Netscape® Navigator® 4.0 of hoger

1. Start Netscape. Klik op “Edit” (Bewerken) en vervolgens op “Preferences” (Voorkeurstellingen).
2. Klik in het venster “Preferences” (Voorkeurstellingen) op “Advanced” (Geavanceerd) en selecteer vervolgens “Proxies”. In het venster “Proxies” selecteert u “Direct connection to the Internet” (Rechtstreekse verbinding met het Internet).



Problemen oplossen

Probleem:

De ADSL-LED brandt niet.

Oplossing:

1. Controleer de verbinding tussen de router en de ADSL-lijn. Zorg ervoor dat de kabel van de ADSL-lijn is aangesloten op de poort van de router die wordt aangeduid met "DSL line".
2. Zorg ervoor dat de router van stroom wordt voorzien. De LED voor Voeding op het frontpaneel zou nu moeten branden.

Probleem:

De Internet-LED brandt niet.

Oplossing:

1. Zorg ervoor dat de kabel van de ADSL-lijn is aangesloten op de poort van de router die wordt aangeduid met "DSL line".
2. Zorg ervoor dat u over de juiste, door uw Internet Service Provider verstrekte, gegevens voor VPI/VCI, gebruikersnaam en wachtwoord beschikt.

Probleem:

Mijn type verbinding is "Static IP Address" (Statisch IP-adres). Ik kan geen verbinding met het Internet tot stand brengen

Oplossing:

Omdat uw type verbinding dat van een statisch IP-adres is, moet uw Internet Service Provider u een IP-adres, een subnetmasker en een gateway-adres toewijzen. In plaats van gebruik te maken van de Wizard, gaat u naar "Connection Type" (Verbindingstype) en selecteert u het type verbinding. Klik op "Next" (Volgende) en selecteer "Static IP" (Statisch IP). Vervolgens voert u het IP-adres, subnetmasker en de standaard gateway-informatie in.

Probleem:

Ik ben mijn wachtwoord kwijt of vergeten.

Oplossing:

Druk de "Reset"-knop op het achterpaneel gedurende tenminste zes seconden in om de standaard fabrieksinstellingen te herstellen.

1

2

3

4

5

6

7

8

9

10

11

Probleem:

Mijn draadloze PC kan geen verbinding maken met de router.

Oplossing:

1. Zorg ervoor dat de draadloze PC dezelfde SSID-instellingen heeft als de router en dat de beveiligingsinstellingen voor de cliënten, zoals WPA-beveiliging of WEP-encryptie, hetzelfde zijn.
2. Zorg ervoor dat de afstand tussen de router en de draadloze PC niet te groot is.

Probleem:

Het draadloze netwerkverbinding wordt vaak onderbroken.

Oplossing:

1. Zet uw draadloze PC dichterbij de router voor een beter signaal.
2. Er kan ook sprake zijn van interferentie, mogelijk veroorzaakt door de aanwezigheid van een magnetron of 2,4GHz draadloze telefoon. Wijzig de locatie van de router of maak gebruik van een ander draadloos kanaal.

Probleem:

Ik kan geen draadloze verbinding met het Internet tot stand brengen.

Oplossing:

Indien u met een draadloze computer geen verbinding met het Internet tot stand kunt brengen, ga dan als volgt te werk:

1. Kijk naar de lampjes op uw router. Indien u gebruik maakt van een router van Belkin geldt het volgende voor de lampjes:
 - De LED voor de voeding moet nu oplichten.
 - De LED voor “Connected” (Verbinding gemaakt) moet constant branden en niet knipperen.
 - De LED voor “WAN” moet constant branden of knipperen.
2. Open de “wireless utility”-software door te klikken op het pictogram rechts onderin het scherm. Indien u een draadloze kaart van Belkin gebruikt, zou het pictogram in de taakbalk er als volgt uit moeten zien (het pictogram kan rood of groen zijn):
3. Het precieze venster dat geopend wordt, is afhankelijk van het type draadloze kaart waarvan u gebruik maakt; onderdeel van alle hulpprogramma's is echter een overzicht van “Available Networks” (Beschikbare netwerken) de draadloze netwerken waarmee verbinding gemaakt kan worden.

Komt de naam van uw draadloze netwerk in dit overzicht voor?

Ja, mijn netwerknaam is opgenomen in het overzicht—ga naar de oplossing voor het probleem “Ik kan geen draadloze verbinding met internet tot stand brengen, maar de naam van mijn netwerk is bekend” in het hoofdstuk “Problemen oplossen”.

Nee, de naam van mijn netwerk wordt niet vermeld — ga naar de probleemoplossing “Ik kan geen draadloze verbinding met het internet maken en de naam van mijn netwerk wordt niet vermeld”.

Probleem:

Ik kan geen draadloze verbinding met het Internet tot stand brengen, maar de naam van mijn netwerk is bekend.

Oplossing:

Indien de juiste netwerknaam is opgenomen in het overzicht van “Available Networks” (Beschikbare netwerken), volg dan de onderstaande stappen om een draadloze verbinding tot stand te brengen.

1. Klik op de juiste netwerknaam in het overzicht met beschikbare netwerken. Indien voor het netwerk beveiligingsinstellingen (encryptie) zijn geactiveerd, dient u de netwerksleutel in te voeren. Meer informatie over beveiliging vindt u in het hoofdstuk “Instellingen voor beveiliging van uw draadloze netwerk wijzigen”.
2. Binnen enkele seconden wordt het pictogram in de taakbalk, links onderin uw scherm groen, om aan te geven dat u verbinding heeft met het netwerk.

Probleem:

Ik kan geen draadloze verbinding met het Internet tot stand brengen en de naam van mijn netwerk is niet bekend.

Oplossing:

Doorloop onderstaande stappen als de naam van uw netwerk niet is opgenomen in het overzicht “Available Networks” (Beschikbare netwerken) in de utility:

1. Verplaats, indien mogelijk, de computer tijdelijk op een afstand van tussen anderhalve en drie meter van de router vandaan. Sluit de utility en heropen hem. Als de naam van uw netwerk nu wel verschijnt in het overzicht “Available Networks” (beschikbare netwerken), heeft u wellicht een probleem met het bereik of last van storing. Wij verwijzen u ook naar Appendix B, getiteld “Belangrijke factoren die een rol spelen bij plaatsing en setup”.
2. Gebruik een computer die via een netwerkkabel op de router is aangesloten (in plaats van een draadloze verbinding) en zorg dat “Broadcast SSID” (SSID uitzenden) is ingeschakeld. Deze instelling vindt u op de pagina voor het configureren van “Channel and SSID” (Kanaal en SSID).

Als u nog steeds geen toegang tot Internet kunt krijgen nadat u deze stappen heeft doorlopen, neem dan contact op met de afdeling Technische Ondersteuning van Belkin.

Probleem:

De prestaties van mijn draadloze netwerk zijn wisselvallig.

De gegevensoverdracht geschiedt soms traag.

Het signaal is zwak.

Problemen bij het tot stand brengen/behouden van een Virtual Private Network-verbinding.

Oplossing:

Draadloze technologie is gebaseerd op radiogolven. Dit betekent dat de connectiviteit en de doorvoersnelheid afnemen naarmate de afstand tussen de apparaten groter is. Andere factoren die een vermindering van de signaalkwaliteit veroorzaken (metaal is meestal de grootste boosdoener) zijn muren en metalen apparaten. Hierdoor is het bereik van uw draadloze apparatuur binnenshuis meestal zo'n 30 tot 60 meter. Hou er verder rekening mee dat de snelheid van de verbinding af zal nemen naarmate de afstand tot de router of het accesspoint groter wordt.

Om vast te stellen of problemen met draadloze gegevensoverdracht te maken hebben met afstand, adviseren we u uw computer tijdelijk te verplaatsen, indien mogelijk, op een afstand van 1,5 tot 3 meter van de router.

Het draadloze kanaal wijzigen - Het wijzigen van het kanaal kan een positief effect hebben op de prestaties en betrouwbaarheid van uw draadloze netwerk indien ander draadloos verkeer in uw omgeving en interferentie de prestaties van uw netwerk negatief beïnvloeden. Het kanaal waarop de router standaard is ingesteld is kanaal 11. Afhankelijk van uw regio kunt u voor verschillende andere kanalen kiezen. Raadpleeg op pagina XX het hoofdstuk "Het kanaal voor draadloze communicatie wijzigen" voor meer informatie over het kiezen van een kanaal.

De overdrachtssnelheid verlagen - Het verlagen van de overdrachtssnelheid kan het draadloze bereik en de stabiliteit van de verbinding verhogen. Bij de meeste draadloze netwerkkaarten kan de overdrachtssnelheid aangepast worden. Als u deze eigenschap wilt wijzigen, gaat u naar "Control Panel" (Configuratiescherm) in Windows, opent u de "Network connections" (Netwerkverbindingen) en dubbelklikt u op de verbinding van uw draadloze kaart. Onder "Properties" (Eigenschappen) selecteert u de knop "Configure" (Configureren) op het tabblad "General" (Algemeen). (Gebruikers van Windows 98 dienen de draadloze kaart te selecteren en op "Properties" (Eigenschappen) te klikken.) Vervolgens selecteert u op het tabblad "Advanced" (Geavanceerd) de overdrachtssnelheid. Draadloze cliëntkaarten regelen doorgaans automatisch de draadloze overdrachtssnelheid voor u, maar dit kan periodiek onderbreking van de verbinding veroorzaken als het draadloze signaal te zwak is; in de regel zijn langzamere overdrachtssnelheden betrouwbaarder. Experimenteer met verschillende verbindingssnelheden totdat u de beste verbinding voor uw netwerkomgeving gevonden hebt; de beschikbare overdrachtssnelheden zouden allemaal geschikt moeten zijn voor internetgebruik. Raadpleeg voor meer informatie de handleiding bij uw netwerkkaart.

Probleem:

Hoe ver groot ik het bereik van mijn draadloze netwerk?

Oplossing:

Belkin adviseert gebruik van één van onderstaande producten om het bereik van uw draadloze netwerk te vergroten:

- **Draadloos accesspoint:** Een draadloos accesspoint kan het dekkingsgebied van uw draadloze netwerk verdubbelen. Een accesspoint wordt meestal geplaatst in het gebied dat niet door uw draadloze router wordt bestreken en wordt middels een Ethernet-kabel of via de elektriciteitskabels in het pand met twee Powerline Ethernet-adapters met de router verbonden.
- Voor 802.11g (54g) draadloze netwerken biedt Belkin een draadloze range extender/accesspoint die draadloos op een draadloze 802.11g router van Belkin wordt aangesloten, zonder gebruik van een Ethernet-kabel of Powerline-Ethernet-adapters.

Deze producten zijn verkrijgbaar bij uw plaatselijke Belkin dealer of zijn rechtstreeks bij Belkin te bestellen.

Ga voor meer informatie over het uitbreiden van draadloze netwerken en het bereik ervan naar www.belkin.com/networking en lees meer over de volgende producten:

Draadloze G Range Extender/Accesspoint van Belkin (F5D7132)

Probleem:

Ik heb problemen met het installeren van Wired Equivalent Privacy of WEP-beveiliging op een router of accesspoint van Belkin

Oplossing:

1. Log in op uw draadloze router of accesspoint.
2. Open uw webbrowser en typ het IP-adres van uw router of accesspoint in. (De standaardinstelling voor de router is 192.168.2.1, het 802.11g accesspoint heeft 192.168.2.254.) Log in op uw router door op de knop "Login" in de rechter bovenhoek van uw scherm te drukken. U wordt gevraagd uw wachtwoord in te voeren. Als u geen wachtwoord hebt ingesteld dan vult u dit veld niet in en klikt u op "Submit" (indienen).
3. Klik op het tabblad "Wireless" (Draadloos) links op uw scherm. Selecteer het tabblad "Encryption" (Encryptie) of "Security" (Beveiliging) om naar de instellingenpagina voor beveiliging te gaan.
4. Selecteer "128-bit WEP" in het dropdown-menu.
5. Nadat u een WEP-encryptiemodus hebt geselecteerd, kunt u uw hexadecimale WEP-sleutel handmatig intypen of een passphrase (meervoudig wachtwoord) in het "Passphrase"-veld invoeren en klikken op "Generate" (Genereren) om uit de passphrase een WEP-sleutel te genereren. Klik op "Apply Changes"

(Wijzigingen toepassen) om te eindigen. Zorg er nu voor dat al uw cliënten op deze manier zijn ingesteld. Een hexadecimale sleutel bestaat uit een combinatie van cijfers en letters van A tot F en van 0 tot 9. Voor 128-bits WEP-encryptie dient u 26 hexadecimale sleutels in te voeren.

Bijvoorbeeld:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bits sleutel

6. Klik op “Apply Changes” (Wijzigingen aanbrengen) om te eindigen. De encryptie in de router is nu ingesteld. Iedere computer binnen uw draadloze netwerk moet nu worden geconfigureerd met dezelfde beveiligingsinstellingen.

WAARSCHUWING: Als u de draadloze router of accesspoint vanaf een computer met een draadloze cliënt configureert, dient u ervoor te zorgen dat de beveiliging voor die draadloze cliënt is ingeschakeld. Als dat niet gebeurt, krijgt u geen draadloze verbinding.

Opmerking voor Mac-gebruikers: De oorspronkelijke Apple AirPort-producten ondersteunen uitsluitend 64-bits encryptie. Apple AirPort 2-producten kunnen 64-bits en 128-bits encryptie ondersteunen. Controleer dus eerst het type Apple AirPort-product dat u gebruikt. Als het u niet lukt uw netwerk met 128-bits encryptie te configureren, probeer dan 64-bits encryptie.

Probleem:

Ik heb problemen met het installeren van Wired Equivalent Privacy of WEP-beveiliging op een draadloze netwerkkaart van Belkin

Oplossing:

De draadloze netwerkkaart dient dezelfde sleutel te gebruiken als de draadloze router of het draadloze accesspoint. Als uw draadloze router of accesspoint de sleutel 00112233445566778899AABBCC gebruikt, dan moet de draadloze kaart exact dezelfde sleutel krijgen.

1. Dubbelklik op het signaalindicatorpictogram om het venster “Wireless Network Utility” te laten verschijnen.
2. Met de knop “Advanced” (Geavanceerd) kunt u meer opties van de kaart bekijken en deze configureren.
3. Nadat u op “Advanced” (Geavanceerd) hebt geklikt, verschijnt de Belkin Wireless LAN Utility. Met dit hulpprogramma kunt u alle geavanceerde functies van de draadloze kaart van Belkin beheren.
4. Op het tabblad “Wireless Networks Properties” (Eigenschappen draadloze netwerken) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op de knop “Properties” (Eigenschappen).

5. Selecteer “WEP” onder “Data Encryption” (Dataencryptie)
6. Zorg ervoor dat de optie “The key is provided for me automatically” (De sleutel wordt automatisch verstrekt) niet is aangevinkt. Als u deze computer gebruikt om in te loggen op een bedrijfsnetwerk, vraag dan aan uw netwerkbeheerder of deze optie aangevinkt moet zijn of niet.
7. Typ de WEP-sleutel in in het daarvoor bestemde veld naast “Network Key” (Netwerksleutel).

Belangrijk:Een WEP-sleutel is een combinatie van cijfers en letters van A tot F en 0 tot 9. Voor 128-bits WEP-encryptie dient u 26 hexadecimale sleutels in te voeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw draadloze router of accesspoint.

Bijvoorbeeld: C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bits sleutel

8. Klik op “OK” en vervolgens op “Apply” (Toepassen) om de instellingen op te slaan.

Indien u GEEN draadloze netwerkkaart van Belkin gebruikt, raden wij u aan de handleiding die u van de fabrikant van uw netwerkkaart hebt gekregen, te raadplegen.

Probleem:

Ondersteunen de producten van Belkin WPA?

Oplossing:

Opmerking: Om WPA-beveiliging te kunnen gebruiken moeten al uw cliënten geüpgraded zijn naar stuurprogramma's en software die WPA ondersteunen. U kunt gratis een beveiligingspatch van Microsoft downloaden. Deze patch werkt alleen onder het Windows XP-besturingssysteem.

U kunt deze patch hier downloaden:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

U dient tevens van de website van Belkin het nieuwste stuurprogramma te downloaden voor uw draadloze 802.11g desktop- of notebooknetwerkkaart van Belkin. Andere besturingssystemen worden op dit moment nog niet ondersteund. De patch van Microsoft ondersteunt uitsluitend apparaten zoals 802.11g-producten van Belkin met stuurprogramma's die WPA ondersteunen.

Download de nieuwste stuurprogramma's van <http://www.belkin.com/uk/support/tech/index.asp>

Probleem:

Ik heb problemen met het installeren van Wi-Fi Protected Access (WPA) beveiliging op een draadloze router / accesspoint van Belkin voor een thuisnetwerk.

1

2

3

4

5

6

7

8

9

10

11

Oplossing:

1. Selecteer “WPA-PSK (zonder server)” in het dropdown-menu “Security Mode” (Beveiligingsmodus).
2. Selecteer “TKIP” of “AES” als Encryption Technique (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.
3. Voer uw “pre-shared key” (PSK) in. Deze kan bestaan uit 8 tot 63 karakters en wordt opgebouwd uit letters, cijfers, symbolen en spaties. U dient bij al uw cliënten dezelfde sleutel te gebruiken. Uw PSK kan er als volgt uitzien: “Netwerksleutel familie Jansen”.
4. Klik op “Apply Changes” (Wijzigingen aanbrengen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.

Probleem:

Ik heb problemen met het installeren van Wi-Fi Protected Access (WPA) beveiliging op een draadloze router of een draadloos accesspoint van Belkin in een bedrijfsomgeving.

Oplossing:

Als uw netwerk een radiusserver gebruikt om de sleutels aan de cliënten toe te wijzen, gebruik dan deze instelling. Van deze modus wordt doorgaans op kantoren gebruik gemaakt.

1. Selecteer “WPA (met server)” in het dropdown-menu “Security Mode” (Beveiligingsmodus).
2. Selecteer “TKIP” of “AES” als Encryption Technique (Encryptietechniek). Deze instelling moet voor al uw cliënten hetzelfde zijn.
3. Voer het IP-adres van de radiusserver in in de daarvoor bestemde velden.
4. Voer de radius-sleutel in in het veld “Radius Key”.
5. Voer het sleutelinterval in. Het sleutelinterval geeft aan hoe vaak de sleutels worden verdeeld (in pakketten).
6. Klik op “Apply Changes” (Wijzigingen aanbrengen) om te eindigen. Ken nu aan al uw cliënten deze instellingen toe.

Probleem:

Ik heb problemen met het installeren van Wi-Fi Protected Access (WPA) beveiliging op een draadloze netwerkkaart van Belkin voor een thuisnetwerk.

Oplossing:

Cliënten moeten dezelfde sleutel gebruiken als de draadloze router / accesspoint. Als bijvoorbeeld de sleutel “Netwerksleutel familie Jansen” door de draadloze router of het draadloze accesspoint wordt gebruikt, moeten de cliënten ook van diezelfde sleutel gebruik maken.

1. Dubbelklik op het signaalindicatorpictogram om het venster “Wireless Network Utility” te laten verschijnen.
2. Met de knop “Advanced” (Geavanceerd) kunt u meer opties van de kaart bekijken en deze configureren.
3. Nadat u op “Advanced” (Geavanceerd) hebt geklikt, verschijnt de Belkin Wireless LAN Utility. Met dit hulpprogramma kunt u alle geavanceerde functies van de draadloze kaart van Belkin beheren.
4. Op het tabblad “Wireless Networks Properties” (Eigenschappen draadloze netwerken) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op de knop “Properties” (Eigenschappen).
5. Selecteer “WPA-PSK (no server)” (WPA-PSK (zonder server)) onder “Network Authentication” (Netwerkauthenticatie).
6. Typ de WPA-sleutel in in het daarvoor bestemde veld naast “Network Key” (Netwerksleutel).

Belangrijk:WPA-PSK is opgebouwd uit een combinatie van cijfers en letters van A tot Z en 0 tot 9. Voor WPA-PSK kunt u 8 tot 63 tekens invoeren. Deze netwerksleutel dient overeen te komen met de sleutel die u toekent aan uw draadloze router of accesspoint.

7. Klik op “OK” en vervolgens op “Apply” (Toepassen) om de instellingen op te slaan.

Probleem:

Ik heb problemen met het installeren van Wi-Fi Protected Access (WPA) beveiliging op een draadloze netwerkkaart van Belkin voor een kantoor netwerk.

Oplossing:

1. Dubbelklik op het signaalindicatorpictogram om het venster “Wireless Network Utility” te laten verschijnen.
2. Met de knop “Advanced” (Geavanceerd) kunt u meer opties van de kaart bekijken en deze configureren.
3. Nadat u op “Advanced” (Geavanceerd) hebt geklikt, verschijnt de Belkin Wireless LAN Utility. Met dit hulpprogramma kunt u alle geavanceerde functies van de draadloze kaart van Belkin beheren.
4. Op het tabblad “Wireless Networks Properties” (Eigenschappen draadloze netwerken) selecteert u een netwerknaam uit de lijst “Available networks” (Beschikbare netwerken) en vervolgens klikt u op de knop “Properties” (Eigenschappen).
5. Selecteer “WPA” onder “Network Authentication” (Netwerkauthenticatie).
6. Selecteer op het tabblad “Authentication” (Authenticatie) de door uw netwerkbeheerder bepaalde vereiste instellingen.
7. Klik op “OK” en vervolgens op “Apply” (Toepassen) om de instellingen op te slaan.

1

2

3

4

5

6

7

8

9

10

11

Probleem:

Ik heb problemen bij het instellen van Wi-Fi Protected Access (WPA) beveiliging voor een draadloze cliëntkaart van een andere fabrikant dan Belkin in een thuisnetwerk.

Oplossing:

Als u geen draadloze desktop- of notebooknetwerkaart van Belkin gebruikt en uw kaart niet voorzien is van software die WPA ondersteunt, dan kunt u van de website van Microsoft kosteloos een bestand downloaden met de naam "Windows XP Support Patch for Wireless Protected Access". De patch van Microsoft kunt u downloaden door de knowledge base voor Windows XP WPA te doorzoeken.

Opmerking: Dit bestand van Microsoft werkt alleen met Windows XP. Andere besturingssystemen worden op dit moment nog niet ondersteund. U dient ook te controleren of de kaartfabrikant WPA ondersteunt en of u het nieuwste stuurprogramma van hun support site hebt gedownload.

Ondersteunde besturingssystemen:

- Windows XP Professional
- Windows XP Home Edition

Inschakelen WPA-PSK (zonder server)

1. In Windows XP klikt u op "Start > Control Panel > Network Connections" (Start > Configuratiescherm > Netwerkverbindingen).
2. Klik met uw rechter muisknop op het tabblad "Wireless Networks" (Draadloze netwerken). Het volgende venster zal verschijnen. Zorg ervoor dat de optie "Use Windows to configure my wireless network settings" (Gebruik Windows om de instellingen van mijn draadloze netwerk te configureren) is aangevinkt.
3. Klik in het tabblad "Wireless Networks" (Draadloze netwerken) op de knop "Configure" (Configureren).
4. Voor gebruik in uw woning of op een klein kantoor, selecteert u onder "Network Administration" (Netwerkbeheer) "WPA-PSK".

Opmerking: Selecteer "WPA (with radius server)" (WPA met radiusserver) als u deze computer gebruikt om verbinding te maken met een bedrijfsnetwerk dat een authenticatieserver ondersteunt zoals een radiusserver. Neem contact op met uw netwerkbeheerder voor meer informatie.

5. Selecteer onder "Data Encryption" (Data-encryptie) "TKIP" of "AES". Deze instelling moet gelijk zijn aan die van de draadloze router of het draadloze accesspoint.
6. Typ de encryptiesleutel in in het daarvoor bestemde vakje bij "Network Key" (Netwerksleutel).

Belangrijk: Voer uw PSK in. Deze sleutel bestaat uit 8 tot 63 tekens, dit kunnen letters, cijfers of symbolen zijn. U dient bij al uw cliënten dezelfde sleutel te gebruiken.

7. Klik op "OK" om de instellingen op te slaan.

Wat is het verschil tussen 802.11b, 802.11g, 802.11a en Pre-N?

Op dit moment zijn er vier standaarden voor draadloze netwerken, waartussen grote verschillen in overdrachtssnelheden bestaan. Elke norm is gebaseerd op de aanduiding 802.11(x), een benaming die is vastgesteld door het IEEE (Institute of Electrical and Electronic Engineers), het Amerikaanse instituut dat verantwoordelijk is voor de ontwikkeling en goedkeuring van ondermeer netwerknormen. De meest gebruikte standaard voor draadloos netwerkverkeer, 802.11b, maakt een gegevensoverdracht van 11 Mbps mogelijk; 802.11a en 802.11g maken snelheden tot 54 Mbps mogelijk; en Pre-N snelheden tot 108Mbps. Pre-N, de voorloper van 802.11n, belooft snelheden te realiseren die boven die van 802.11g-producten ligt, met een reikwijdte die twee keer zo groot is. Zie voor nadere informatie de onderstaande tabel.

Vergelijkend overzicht van draadloze technologieën

Draadloze technologie	G (802.11g)	G+ MIMO (802.11g met MIMO MRC)	N MIMO (draft 802.11n met MIMO)	N1 MIMO (draft 802.11n met MIMO)
Snelheid/gegevenssnelheid*	Tot 54 Mbps*	Tot 54 Mbps*	Tot 300 Mbps*	Tot 300 Mbps*
Frequentie	De vrije 2,4 GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons.	De vrije 2,4 GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons.	De vrije 2,4 GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons.	De vrije 2,4 GHz-band is gevoelig voor interferentie door stoorsignalen van huishoudelijke apparatuur als draadloze telefoons en magnetrons.
Compatibiliteit	Compatibel met 802.11b/g	Compatibel met 802.11b/g	Compatibel met draft 802.11n** en 802.11b/g	Compatibel met draft 802.11n** en 802.11b/g
Bereik*	Tot 120 m*	Tot 300 m*	Tot 365 m*	Tot 425 m*
Voordeel	Veel gebruikt – vooral voor het delen van internetaansluitingen	Betere dekking en bereik en constante snelheden	Groter bereik en hogere snelheden	Geavanceerd – beste reikwijdte en doorvoer

*Bereik en verbindingssnelheid afhankelijk van netwerkomgeving.

**Deze router is compatibel met producten die gebaseerd zijn op dezelfde 802.11n-specificaties en vereisen mogelijk erwijs een software-upgrade ten behoeve van optimale resultaten.

Technische ondersteuning

Gratis technische ondersteuning* *tegen lokaal telefoontarief **www.belkin.com**

Aanvullende informatie over technische ondersteuning is beschikbaar op onze website **www.belkin.com** onder "Ondersteuning". Als u telefonisch contact wilt opnemen met onze afdeling voor technische ondersteuning, kunt u gebruik maken van het voor u van toepassing zijnde telefoonnummer uit onderstaande lijst.

LAND	NUMMER	INTERNETADRES
OOSTENRIJK	0820 200766	www.belkin.com/uk/networking/
BELGIË	07 07 00 073	www.belkin.com/nl/networking/
TSJECHIË	239 000 406	www.belkin.com/uk/networking/
DENEMARKEN	701 22 403	www.belkin.com/uk/networking/
FINLAND	097 25 19 123	www.belkin.com/uk/networking/
FRANKRIJK	08 - 25 54 00 26	www.belkin.com/fr/networking/
DUITSLAND	0180 - 500 57 09	www.belkin.com/de/networking/
GRIEKENLAND	00800 - 44 14 23 90	www.belkin.com/uk/networking/
HONGARIJE	06 - 17 77 49 06	www.belkin.com/uk/networking/
IJSLAND	800 8534	www.belkin.com/uk/networking/
IERLAND	0818 55 50 06	www.belkin.com/uk/networking/
ITALIË	02 - 69 43 02 51	www.belkin.com/it/support/tech/issues_more.asp
LUXEMBURG	34 20 80 85 60	www.belkin.com/uk/networking/
NEDERLAND	0900 - 040 07 90 € 0,10 per minuut	www.belkin.com/nl/networking/
NOORWEGEN	81 50 0287	www.belkin.com/uk/networking/
POLEN	00800 - 441 17 37	www.belkin.com/uk/networking/
PORTUGAL	707 200 676	www.belkin.com/uk/networking/
RUSLAND	495 580 9541	www.belkin.com/networking/
ZUID-AFRIKA	0800 - 99 15 21	www.belkin.com/uk/networking/
SPANJE	902 - 02 43 66	www.belkin.com/es/support/tech/networkingsupport.asp
ZWEDEN	07 - 71 40 04 53	www.belkin.com/se/support/tech/networkingsupport.asp
ZWITSERLAND	08 - 48 00 02 19	www.belkin.com/uk/networking/
VERENIGD KONINKRIJK	0845 - 607 77 87	www.belkin.com/uk/networking/
OVERIGE LANDEN	+44 - 1933 35 20 00	

Appendix A: Verklarende woordenlijst

IP-adres

Het "IP address" is het interne IP-adres van de router. Om de geavanceerde installatie-interface te openen, typt u dit adres in de adresbalk van uw browser in. U kunt dit adres indien nodig wijzigen. Om het IP-adres te wijzigen, typt u het nieuwe IP-adres in en klikt u op "Apply Changes" (Wijzigingen aanbrengen). Het IP-adres dat u kiest, moet een niet-routeerbaar IP zijn. Hieronder ziet u een paar voorbeelden van een niet-routeerbaar IP:

192.168.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)
10.x.x.x (waarbij x elke waarde kan hebben tussen 0 en 255)

Subnetmasker

Sommige netwerken zijn veel te groot om, waardoor niet al het verkeer in alle uithoeken terecht komt. Deze netwerken moeten worden opgedeeld in kleinere, werkbare delen, subnets genaamd. Het subnetmasker is het netwerkadres plus de informatie die identificatie van het "subnetwerk" mogelijk maakt.

DNS

DNS is de afkorting van Domain Name Server. Een "Domain Name Server" is een server op het Internet die URL's (Universal Resource Links) als "www.belkin.com" vertaalt naar IP-adressen. De meeste ISP's verlangen niet van u dat u deze informatie in de router invoert. Als u een statische IP gebruikt, moet u waarschijnlijk een specifiek DNS-adres en een secundair DNS-adres invullen om ervoor te zorgen dat uw verbinding correct functioneert. Als u een dynamische verbinding of PPPoE gebruikt, hoeft u waarschijnlijk geen DNS-adres in te vullen.

PPPoE

De meeste ADSL-providers maken gebruik van PPPoE als type verbinding. Als u gebruik maakt van een ADSL-modem voor het maken van een verbinding met het Internet, dan gebruikt uw ISP mogelijk PPPoE om u aan te melden.

Uw type verbinding is PPPoE als:

1. Uw Internet Service Provider u een gebruikersnaam en wachtwoord heeft gegeven die noodzakelijk zijn om de verbinding met het Internet tot stand te brengen.
2. Uw provider u software als WinPoET of Enternet300 heeft verstrekt om de internetverbinding tot stand te brengen.
3. U op een ander desktoppictogram dan uw browser moet dubbelklikken om op Internet te kunnen.

Om de router geschikt te maken voor het gebruik van PPPoE, moet u uw gebruikersnaam en wachtwoord invoeren in de daarvoor bestemde vakken.

1
2
3
4
5
6
7
8
9
10
11

Hoofdstuk

Appendix A: Verklarende woordenlijst

Nadat u alle noodzakelijke informatie hebt ingevoerd, klikt u op “Apply Changes” (Wijzigingen aanbrengen).

Nadat u de noodzakelijke wijzigingen hebt aangebracht, geeft de internetstatusindicator de melding “Connection OK” (Verbinding OK), als uw router correct is geïnstalleerd.

PPPoA

Voer de PPPoA-informatie in de daarvoor bestemde ruimtes en klik op “Next” (Volgende). Klik op “Apply” (Toepassen) om de instellingen te activeren.

1. User name (Gebruikersnaam) - Voer de gebruikersnaam in. (Toegekend door uw ISP.)
2. Password (Wachtwoord) - Voer uw wachtwoord in. (Toegekend door uw ISP.)
3. Retype Password (Wachtwoord opnieuw intypen) - Typ het wachtwoord opnieuw in. (Toegekend door uw ISP.)
4. VPI/VCI - Vul uw Virtual Path Identifier (VPI) en Virtual Circuit Identifier (VCI) parameter hier in. (Toegekend door uw ISP.)

Verbinding verbreken na X...

Deze functie wordt gebruikt om automatisch de verbinding van uw router met het internet te verbreken als er gedurende bepaalde tijd geen activiteit is. Als u bijvoorbeeld deze optie aanvinkt en het cijfer 5 in het minutenveld invult, wordt de verbinding van de router met het Internet automatisch verbroken als er gedurende vijf minuten geen Internetactiviteit is geweest.

Gebruik deze optie als u voor gebruik van het Internet per minuut moet betalen.

Kanaal en SSID

U kunt het kanaal waarvan de router gebruik maakt wijzigen door in het uitrolmenu het gewenste kanaal te selecteren en uw kanaal te kiezen. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan. U kunt eveneens de SSID wijzigen. De SSID is het equivalent van de naam van uw draadloze netwerk. U kunt de SSID elke naam geven die u maar wilt. Als er zich nog andere draadloze netwerken in uw omgeving bevinden, moet u uw draadloze netwerk een unieke naam geven. Klik in het vakje voor de SSID en typ een nieuwe naam in. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijzigingen door te voeren.

ESSID Broadcast (ESSID-uitzending)

Veel draadloze netwerkadapters die momenteel op de markt verkrijgbaar zijn, beschikken over een functie genaamd site survey. Deze functie scant naar beschikbare netwerken en stelt elke computer in staat automatisch een netwerk uit de survey te selecteren. Dit gebeurt als de SSID van de computer is ingesteld op “ANY”. Uw router van Belkin kan deze willekeurige zoektocht naar een netwerk blokkeren. Indien u de “ESSID Broadcast”-functie uitschakelt, kan een computer het

netwerk alleen vinden als u de SSID van de computer op de specifieke naam van het netwerk (zoals WLAN) instelt. Zorg er wel voor dat u uw SSID (netwerknamen) kent voordat u deze functie inschakelt. U kunt uw draadloze netwerk zo goed als onzichtbaar maken. Wanneer u de optie SSID-uitzending uitzet, verschijnt uw netwerk niet in een site-survey. Door het uitschakelen van de SSID-uitzending, helpt u de veiligheid te verhogen.

Encryptie

Door het gebruik van encryptie zorgt u voor een betere beveiliging van uw netwerk. De router maakt gebruik van Wired Equivalent Privacy (WEP) om uw gegevens te beschermen en biedt twee encryptiemogelijkheden: 64-bits en 128-bits encryptie. Encryptie werkt met een sleutelsysteem. De sleutel op de computer moet overeen komen met de sleutel van de router. Er zijn twee manieren om een sleutel te creëren. Bij de eenvoudigste methode laat u de router's software een passphrase (meervoudig wachtwoord) converteren naar een sleutel. Een geavanceerde methode is het handmatig invoeren van de sleutels.

Applicatiegateways

Met applicatiegateways kunt u bepaalde poorten aanwijzen die open moeten zijn voor bepaalde applicaties om correct met de Network Address Translation (NAT)-functie van de router samen te kunnen werken. Een overzicht van veel gebruikte applicaties is hier opgenomen. In het dropdown-menu met veel gebruikte keuzes kunt u een applicatie selecteren. Uw keuze zal in de router worden ingeprogrammeerd. Selecteer in het dropdown-menu de regel waarvan u de instellingen wilt kopiëren en de regel waarnaar u de gegevens wilt kopiëren en klik op "Copy To" (Kopiëren naar). De instellingen worden overgebracht naar de regel die u hebt opgegeven. Klik op "Apply Changes" (Wijzigingen aanbrengen) om de instelling voor deze applicatie op te slaan. Als uw applicatie hier niet bij staat, neem dan contact op met de leverancier van de applicatie om vast te stellen welke poorten u moet configureren. U kunt deze poortinformatie handmatig in de router invoeren.

Virtuele servers

De functie Virtuele Servers biedt u de mogelijkheid externe (internet)verbindingen voor diensten zoals een webserver (poort 80), FTP-server (poort 21) of andere applicaties via uw router door te sturen naar uw interne netwerk. Aangezien uw interne computers beschermd worden door een firewall, kunnen computers buiten uw netwerk (via het Internet) de interne computers niet bereiken omdat ze niet "zichtbaar" zijn. Als u de functie "virtual server" voor een specifieke applicatie dient te configureren, neem dan contact op met de leverancier van de applicatie om geïnformeerd te worden welke poortinstellingen u nodig hebt.

Om instellingen handmatig in te voeren, typt u het IP-adres in het vak voor de interne computer in, geeft u het poorttype (TCP of UDP) op en de LAN- en publieke poort(en) die gepasseerd moeten worden. Selecteer vervolgens “Enable” (Activeren) en klik op “Set” (Instellen). U kunt per intern IP-adres slechts één poort vrijgeven. U neemt een zeker risico door poorten in uw firewall te openen. U kunt instellingen zeer snel in- en uitschakelen. Het verdient aanbeveling de instellingen te deactiveren wanneer u een bepaalde toepassing niet gebruikt.

IP-filters cliënt

De router kan zo worden geconfigureerd dat toegang tot het Internet, e-mail of andere netwerkdiensten op bepaalde dagen en tijden beperkt is. De beperking kan worden ingesteld voor één enkele computer, een groep computers, of meerdere computers.

URL Blocking (URL-blokking)

Om de functie URL-blokking te configureren, specificeert u de websites (www.eenbepaaldesite.com) en/of trefwoorden waarop gefilterd dient te worden. Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijziging te activeren. Om de configuratie te voltooiën, dient u een toegangsregel te creëren of te wijzigen in het “Client IP filters” deel. Om een bestaande regel te wijzigen, klikt u op de knop “Edit” (Wijzigen) naast de regel die u wenst te wijzigen. Om een nieuwe regel te creëren, klikt u op de “Add PC” (PC toevoegen) optie. Via “Access Control > Add PC”, kunt u de optie voor “WWW with URL Blocking” (WWW met URL-blokking) in de “Client PC Service”-tabel aanvinken, zodat u op de websites en trefwoorden die u hebt opgegeven, kunt filteren.

Schemaregel

Om de schemaregel te configureren, specificeert u de naam, opmerking, begin- en eindtijd waarop u wilt filteren binnen uw netwerk. Zo wordt het schema geactiveerd waarvan gebruik wordt gemaakt op de “Access Control”-pagina.

MAC-adressenfilter

Het MAC-adressenfilter is een krachtig beveiligingsinstrument waarmee u kunt aangeven welke computers toegang hebben tot het netwerk. Computers die proberen toegang te krijgen tot het netwerk maar die niet op de filterlijst voorkomen, worden niet toegelaten. Wanneer u deze functie activeert, moet u het MAC-adres invoeren van iedere cliënt op uw netwerk om elk van deze computers toegang te geven tot het netwerk. U kunt ook het MAC-adres kopiëren door de naam van de computer te selecteren in het “DHCP Client List”-overzicht. Om deze functie te activeren, selecteert u “Enable” (Activeren). Klik vervolgens op “Apply Changes” (Wijzigingen aanbrengen) om de instellingen op te slaan.

DMZ (Gedemilitariseerde Zone)

Indien een van uw cliënten van achter de firewall geen internetapplicatie kan draaien, kunt u deze cliënt onbeperkte tweewegs internettoegang verstrekken. Dit kan nodig zijn wanneer de NAT-functie problemen veroorzaakt met applicaties zoals games of videoconferenties. Het is raadzaam deze functie alleen tijdelijk te activeren. De computer in de gedemilitariseerde zone wordt namelijk niet beschermd tegen hackeraanvallen. Om een computer in de gedemilitariseerde zone te plaatsen, dient u het LAN IP-adres van deze computer in het “Static IP”-veld in te vullen en te klikken op “Apply Changes” (Wijzigingen aanbrengen).

Als u slechts een publiek (WAN) IP-adres hebt, kunt u het publieke IP laten staan op “0.0.0.0”. Als u meerdere publieke WAN IP-adressen gebruikt, kunt u aangeven op welk publiek WAN IP-adres de DMZ-host gericht zal zijn. Vul het (WAN) IP-adres in waaraan de DMZ-host moet worden gericht, voer de laatste twee cijfers in van het IP-adres van de DMZ-hostcomputer en klik op “Apply Changes” (Wijzigingen aanbrengen).

Beheerderswachtwoord

De router wordt geleverd ZONDER vooraf geprogrammeerd wachtwoord. Als u een wachtwoord wilt toevoegen voor meer beveiliging, dan kunt u via de web-based gebruikersinterface van uw router een wachtwoord instellen. Bewaar uw wachtwoord op een veilige plek, want u zal het nodig hebben als u in de toekomst op de router wilt inloggen. Wij raden u TEN ZEERSTE aan een wachtwoord in te stellen als u van plan bent de functie “beheer op afstand” van uw router te gebruiken. Met de optie inlog-timeout kunt u de maximale tijdsduur instellen waarbinnen u ingelogd kunt blijven op de Advanced Setup Interface (Geavanceerde setup-interface) van de router. De timer start als er geen activiteit is geweest. U hebt bijvoorbeeld een aantal wijzigingen in de geavanceerde gebruikersinterface aangebracht en daarna uw computer alleen gelaten zonder op “Logout” (Afmelden) te klikken.

Als de timeout is ingesteld op 10 minuten, dan loopt de inlogsessie af 10 minuten nadat u de router alleen hebt gelaten. Als u meer wijzigingen wilt aanbrengen, dient u opnieuw op de router in te loggen. Deze inlog-timeoutoptie is bedoeld als extra beveiliging en staat standaard ingesteld op 10 minuten. Let op: er kan slechts één computer tegelijk ingelogd zijn op de Advanced Setup-interface van de router.

Tijd en tijdzone

De tijd klok van de router wordt geregeld via de aansluiting op een SNTP (Simple Network Time Protocol) server. Hierdoor loopt de systeemklok van de router synchroon met de tijd van het wereldwijde Internet. De gesynchroniseerde klok in de router wordt gebruikt voor de registratie van het beveiligingslog en de aansturing van het cliëntfilter. Selecteer de tijdzone waarin u gevestigd bent. Als u in een land woont dat de zomer- en wintertijd volgt, vink dan de optie “Enable Daylight Saving” (Zomer/wintertijd inschakelen) aan. De systeemklok geeft niet onmiddellijk na inschakeling de juiste tijd aan.

1
2
3
4
5
6
7
8
9
10
11

Appendix B: Belangrijke factoren die een rol spelen bij plaatsing en installatie.

De router heeft ten minste 15 minuten nodig om een verbinding op te bouwen met de tijdservers op het Internet en voor het ontvangen van een antwoordsignaal. U kunt de klok niet zelf instellen.

Beheer op afstand

Voordat u deze functie inschakelt, DIENT U HET BEHEERDERSWACHTWOORD IN TE STELLEN De functie “Remote Management” (Beheer op afstand) biedt u de mogelijkheid vanaf elke internetlocatie ter wereld de instellingen van uw router te wijzigen.

UPnP

UPnP (Universal Plug-and-Play) is een technologie die naadloze werking van voice messaging, video messaging, games en andere applicaties mogelijk maakt die voldoen aan UPnP. Voor sommige applicaties dient de firewall van de router op een specifieke manier geconfigureerd te zijn voor een juiste werking. Hiervoor moeten doorgaans de TCP- en UDP-poorten worden geopend en in sommige gevallen triggerpoorten worden ingesteld. Applicaties die voldoen aan UPnP kunnen met de router communiceren, in principe om de router te “vertellen” op welke wijze de firewall moet worden geconfigureerd. De router wordt geleverd met uitgeschakelde UPnP-functie. Als u applicaties gebruikt die voldoen aan UPnP en u wilt profiteren van de mogelijkheden van UPnP dan heeft het zin de UPnP-functie te activeren. U selecteert eenvoudigweg “Enable” (Activeren) in de paragraaf “UPnP Enabling” (UPnP activeren) van de pagina “Utilities” (Hulpprogramma’s). Klik op “Apply Changes” (Wijzigingen aanbrengen) om de wijziging op te slaan.

Opmerking: Ondanks dat onderstaande factoren de prestaties van uw netwerk nadelig kunnen beïnvloeden, zullen zij er niet voor zorgen dat uw draadloze netwerk niet meer functioneert. Als u vermoedt dat uw netwerk niet optimaal presteert kan deze checklist uitkomst bieden.

1. Plaatsing van uw draadloze router (of accesspoint)

Plaats uw draadloze router (of accesspoint), het centrale verbindingspunt binnen uw netwerk, op een centrale plek tussen uw draadloze netwerkkaparaatuur.

De beste netwerkdekking voor uw “draadloze cliënten” (d.w.z. computers aangestuurd door draadloze notebook- en desktopnetwerkkarten en draadloze USB-adapters van Belkin) bereikt u als volgt:

- Zorg er voor dat de netwerkantennes van uw draadloze router (of accesspoint) parallel aan elkaar en in verticale stand staan (naar het plafond wijzen). Als de draadloze router (of het draadloze accesspoint) zelf al verticaal is gepositioneerd, laat de antennes dan zo recht mogelijk naar het plafond wijzen.
- In woningen met meer verdiepingen plaatst u de draadloze router (of accesspoint) op de verdieping die zich het dichtst bij het midden van de woning bevindt. Dit kan betekenen dat u de draadloze router (of accesspoint) op een hogere verdieping moet plaatsen.
- Plaats de draadloze router (of accesspoint) niet in de buurt van een draadloze 2,4GHz-telefoon.

Appendix B: Belangrijke factoren die een rol spelen bij plaatsing en installatie.

2. Vermijd obstakels en interferentie

Plaats uw draadloze router (of accesspoint) bij voorkeur niet in de buurt van apparaten die radiogolven uitzenden, zoals magnetrons. De volgende ondoordringbare objecten kunnen draadloze communicatie hinderen:

- Koelkasten
- Wasmachines en/of drogers
- Metalen kasten
- Grote aquaria
- Gemetalliseerde UV-werende ruiten

Indien uw draadloze signaal op sommige plaatsen zwakker lijkt te zijn, zorg er dan voor dat dit soort objecten het signaal niet kunnen hinderen, dat wil zeggen dat ze niet tussen uw computers en uw draadloze router (of accesspoint) in staan.

3. Draadloze telefoons

Ga als volgt te werk als de prestaties van het draadloze netwerk niet beter worden nadat u de bovenstaande wenken hebt opgevolgd én u een draadloze telefoon bezit:

- Kijk wat er gebeurt als u uw draadloze telefoon uit de buurt houdt van uw draadloze routers (of accesspoints) en uw computers die geschikt zijn voor draadloze communicatie.
- Verwijder de batterij uit alle draadloze telefoons die gebruik maken van de 2,4 GHz-band (zie de informatie van de fabrikant). Als het probleem hiermee is opgelost, is(/zijn) uw telefoon(s) de storingsbron.
- Als u voor uw telefoon ook andere kanalen kunt kiezen, kies dan voor het kanaal dat het verst verwijderd is van het kanaal dat door uw draadloze netwerk wordt gebruikt. Verander bijvoorbeeld het kanaal van uw telefoon in kanaal 1 en stel het kanaal van uw draadloze router (of accesspoint) in op kanaal 11. Raadpleeg de handleiding van uw telefoon voor gedetailleerde instructies.
- Gebruik zo nodig voortaan een draadloze telefoon van 900 MHz of 5 GHz.

4. Kies het “stilste” kanaal voor het draadloze netwerk

Op plaatsen waar meerdere woningen of kantoren dicht bij elkaar liggen, zoals appartementen- of kantoorgebouwen, kunnen draadloze netwerken in de omgeving problemen veroorzaken voor uw netwerk.

Maak gebruik van de Site Survey-mogelijkheid (site-overzicht) van de Wireless LAN Utility (hulpprogramma voor draadloos LAN) om andere draadloze netwerken te lokaliseren en verplaats uw router en computers naar een kanaal dat zo ver mogelijk verwijderd is van andere netwerken.

Experimenteer met de verschillende beschikbare kanalen om de beste verbinding te vinden en storing door draadloze telefoons en andere draadloze apparaten in de omgeving te voorkomen.

1

2

3

4

5

6

7

8

9

10

11

Appendix B: Belangrijke factoren die een rol spelen bij plaatsing en installatie.

Gebruik voor niet van Belkin afkomstige draadloze netwerkproducten het gedetailleerde site-overzicht en de informatie over draadloze kanalen in de handleiding.

Bovenstaande suggesties en richtlijnen helpen u bij het optimaliseren van het bereik van uw draadloze router (of accesspoint). Indien u een nog groter bereik nodig hebt, raden wij u aan een draadloze range extender/accesspoint van Belkin aan te schaffen.

5. Veilige verbindingen, VPN's en AOL

Veilige verbindingen zijn verbindingen waarvoor een gebruikersnaam en een wachtwoord vereist zijn. Hiervan wordt gebruik gemaakt in situaties waar beveiliging van belang is. Veilige verbindingen zijn o.a.:

- Virtual Private Network (VPN)-verbindingen, vaak gebruikt om op afstand verbinding te maken met een kantoor netwerk
- Het "Bring Your Own Access"-programma van America Online (AOL) - met dit programma kunt u AOL gebruiken via een breedbandverbinding die door een andere kabel- of DSL-service beschikbaar wordt gesteld.
- De meeste websites voor Internetbankieren
- Veel commerciële websites die alleen te openen zijn nadat een gebruikersnaam en een wachtwoord zijn ingevuld.

Veilige verbindingen kunnen worden onderbroken als het energiebeheer van de computer de computer naar de slaapstand overschakelt. U kunt opnieuw verbinding maken door de VPN of AOL-software te draaien, of door opnieuw op de beveiligde website in te loggen.

Een tweede alternatief is het veranderen van de energiebeheerinstelling van de computer, zodat deze niet overgaat op de slaapstand. Dit is niet noodzakelijkerwijs van toepassing voor draagbare computers. Om de energiebeheerinstellingen te wijzigingen in Windows, gaat u naar "Power Options" (Energiebeheer) in het "Control Panel" (Configuratiescherm).

Als u moeilijkheden blijft houden met de beveiligde verbindingen, VPN en AOL, raden wij u aan de bovenstaande stappen te doorlopen om te zien of u hiermee rekening gehouden hebt.

FCC-verklaring

VERKLARING VAN CONFORMITEIT MET DE FCC-VOORSCHRIFTEN VOOR ELEKTROMAGNETISCHE COMPATIBILITEIT

Wij, Belkin International, Inc., gevestigd 501 West Walnut Street, Compton, CA 90220, Verenigde Staten van Amerika, verklaren hierbij dat wij de volledige verantwoordelijkheid aanvaarden dat het product met het artikelnummer

F5D7632uk4A

waarop deze verklaring betrekking heeft, voldoet aan Deel 15 van de FCC-Voorschriften. Het gebruik ervan is onderworpen aan de beide volgende voorwaarden: (1) het apparaat mag geen schadelijke storingen opwekken en (2) het apparaat moet elke ontvangen interferentie accepteren, waaronder storingen die een ongewenste werking kunnen veroorzaken.

Waarschuwing: Blootstelling aan radiofrequente straling.

Het door dit apparaat afgegeven uitgangsvermogen ligt ver beneden de hiervoor in de FCC-voorschriften vastgelegde grenswaarden voor stralingsfrequenties.

Niettemin dient dit apparaat zodanig te worden gebruikt dat bij normaal gebruik de mogelijkheid van persoonlijk contact tot een minimum beperkt blijft.

Ook bij het aansluiten van een externe antenne op dit apparaat moet de antenne zodanig worden geplaatst dat bij normaal gebruik de kans op aanraking tot een minimum beperkt blijft. Ter voorkoming van overschrijding van de in de FCC-voorschriften aangegeven grenswaarden voor de blootstelling aan radiofrequente straling, mogen personen de werkende antenne niet dichter naderen dan tot op een afstand van 20 centimeter.

Kennisgeving van de Federal Communications Commission (FCC)

Deze apparatuur is getest en voldoet aan de grenswaarden voor digitale apparaten van Klasse B zoals vastgelegd in Deel 15 van de FCC-voorschriften. Deze normen zorgen bij de installatie in een woonomgeving voor een aanvaardbare bescherming tegen schadelijke interferentie.

Deze apparatuur genereert en gebruikt radiofrequente energie en kan deze tevens uitzenden. Als deze apparatuur de radio- of televisie-ontvangst stoort, wat u kunt vaststellen door de apparatuur in- en uit te schakelen, kunt u proberen de storing op te heffen met een of meer van de volgende maatregelen:

- Door de ontvangende antenne in een andere richting te draaien of de antenne op een andere plaats te zetten.
- Vergroot de afstand tussen de apparatuur en het ontvangende apparaat.
- Sluit de apparatuur aan op een stopcontact van een andere groep dan die waarop de ontvanger is aangesloten.
- Neem contact op met de verkoper of een deskundig radio/televisietechnicus.

Veranderingen

De Federal Communications Commission eist dat de gebruiker ervoor wordt gewaarschuwd dat elke verandering aan het apparaat die niet uitdrukkelijk door Belkin International, Inc. is goedgekeurd de bevoegdheid van de gebruiker om het apparaat te bedienen teniet kan doen.

Canada-Industry Canada (IC)

De draadloze radio van dit apparaat voldoet aan RSS 139 & RSS 210 Industry Canada. This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B conforme á la norme NMB- 003 du Canada.

Kennisgeving betreffende de Europese Unie

Radioproducten die voorzien zijn van de CE 0682- of de CE-aanduiding voldoen aan de R&TTE-richtlijn (1995/5/EC) van de Commissie van de Europese Gemeenschap.

Het voldoen aan deze richtlijn houdt in dat de betreffende apparatuur beantwoordt aan de volgende Europese normen (de overeenkomstige internationale normen zijn tussen haakjes vermeld).

- EN 60950 (IEC60950) – Productveiligheid
 - EN 300 328 Technische eisen voor radioapparatuur
 - ETS 300 826 Algemene EMC-vereisten voor radioapparatuur.
- U kunt het zendertype vaststellen op het identificatie-etiket van uw apparaat van Belkin.

Producten die voorzien zijn van het CE-merk voldoen aan de Richtlijn voor Elektromagnetische Compatibiliteit (89/336/EEC) en aan de Richtlijn voor Laagspanningsapparatuur (72/23/EEC) van de Commissie van de Europese Economische Gemeenschap.

Apparaten die aan deze richtlijn voldoen beantwoorden aan de volgende Europese normen (tussen haakjes zijn de overeenkomstige internationale normen vermeld).

- EN 55022 (CISPR 22) – Elektromagnetische interferentie
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Elektromagnetische immuniteit
- EN 61000-3-2 (IEC610000-3-2) – Harmonischen in elektrische leidingen
- EN 61000-3-3 (IEC610000) – Spanningsfluctuaties in elektrische leidingen
- EN 60950 (IEC60950) – Productveiligheid

Producten die een radiozender bevatten zijn voorzien van de CE 0682- of CE-aanduiding en kunnen tevens zijn voorzien van het CE-logo.



BELKIN.

EC Declaration of Conformity to R&TTE Directive 1999/5/EC

Manufacturer : BELKIN LTD,
EXPRESS BUSINESS PARK,
SHIPTON WAY
,RUSHDEN
NN10 6GL ENGLAND

Representative : Belkin Ltd
(residing in the EC
holding the TCF)

Product / Apparatus : **ADSL Modem/Wireless G Router**

Type Number : **F5D7632-4**

Variants include : **All Country Variants**

Declaration

I declare that above product conforms to all the applicable requirements of EU Directive 1999/5/EC and is CE-marked accordingly:

Article 3.1a: (Standard(s)) used to show compliance with LVD, 73/23/EEC:

IEC 60950-1 2001 Compliant Test Report No: LD931001H03 03 NOV 04

Article 3.1b: (Standard(s)) used to show compliance with EMC Directive, 89/336/EEC:

EN301 489-1 V1.4.1 (2002-08);EN 301 489-17 V1.2.1 (2002-08) Compliant Test Report No:RM931001H03

Article 3.2: Standard(s) used to show compliance:

...EN300 328 V1.4.1 (2003-04)..... Compliant Test Report No:RC93100H03

Signature : 

Name : K Simpson

Title : European Regulatory Compliance Manager

Date : 20 MAR 2006

Beperkte levenslange productgarantie van Belkin International, Inc.

Deze garantie dekt het volgende:

Belkin International, Inc. garandeert de oorspronkelijke koper van dit Belkin-product dat het product vrij is van ontwerp-, assemblage-, materiaal- en fabricagefouten.

De geldigheidsduur van de dekking

Belkin International, Inc., garandeert het Belkin-product voor de levensduur van het product.

Hoe worden problemen opgelost?

Productgarantie.

Belkin zal het product dat een defect vertoont naar eigen keus kosteloos (met uitzondering van verzendkosten) repareren of vervangen.

Wat valt buiten deze garantie?

Alle hierin versterkte garanties zijn niet van toepassing als het product van Belkin op verzoek van Belkin niet op kosten van de koper voor onderzoek aan Belkin International, Inc., ter beschikking is gesteld of als Belkin International, Inc. constateert dat het product van Belkin verkeerd is geïnstalleerd, op enige wijze is veranderd of vervalst. De Belkin productgarantie biedt geen bescherming tegen van buiten komend onheil, zoals blikseminslag, overstromingen, aardbevingen en oorlogsmolest, vandalisme, diefstal, normale slijtage, afslijting, depletie, veroudering, misbruik, beschadiging door netspanningsdalingen (z.g. "brown-outs" en "sags"), ongeoorloofde programmering en/of wijziging van de systeemapparatuur.

Hoe wordt service verleend?

Om voor serviceverlening door Belkin in aanmerking te komen, moet u het volgende doen:

1. Neem binnen 15 dagen na het voorval schriftelijk contact op met de afdeling Customer Service (Klantenservice) van Belkin International, Inc., 501 W. Walnut St., Compton CA 90220, Verenigde Staten, of bel (800)-223-5546. U moet de volgende gegevens kunnen verstrekken:
 - a. Het artikelnummer van het Belkin-product.
 - b. Waar u het product hebt gekocht.
 - c. Wanneer u het product hebt gekocht.
 - d. Het originele aankoopbewijs.
2. De medewerker/ster van de klantenservice van Belkin zal u vervolgens instructies geven hoe u het aankoopbewijs en het product moet verzenden en uitleggen hoe de claim verder afgewikkeld wordt.

Belkin International, Inc. behoudt zich het recht voor het defecte Belkin-product te onderzoeken. De kosten voor verzending van het Belkin-product naar Belkin

International, Inc. komen volledig voor rekening van de koper. Als Belkin naar eigen bevinding tot de conclusie komt dat het onpraktisch is de defecte apparatuur naar Belkin International, Inc. te verzenden, kan Belkin naar eigen goeddunken een deskundige reparatie-inrichting aanwijzen en deze opdragen de betreffende apparatuur te inspecteren en de reparatiekosten ervan te begroten. De eventuele verzendkosten van het product naar de reparatie-inrichting en van de terugzending naar de koper en van de kostenbegroting komen geheel voor rekening van de koper. Het beschadigde product moet voor onderzoek beschikbaar blijven totdat de claim is afgehandeld. Belkin International, Inc. behoudt zich bij de vereffening van claims het recht voor tot in-de-plaatstreding bij alle geldige verzekeringspolissen waarover de koper van het product beschikt.

De garantie en de wet.

DEZE GARANTIE OMVAT DE ENIGE GARANTIE VAN BELKIN INTERNATIONAL, INC. EN ER ZIJN GEEN ANDERE GARANTIES, NADRUKKELIJK OF TENZIJ WETTELIJK BEPAALD IMPLICIET, MET INBEGRIIP VAN IMPLICIETE GARANTIES OF VOORZIENINGEN VAN VERHANDELBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL, EN ZULKE IMPLICIETE GARANTIES, MITS VAN TOEPASSING, ZIJN WAT HUN GELDIGHED BETREFT TOT DE DUUR VAN DEZE GARANTIE BEPERKT.

In sommige staten of landen is het niet toegestaan de duur van impliciete garanties te beperken in welk geval de bovenstaande garantiebeperkingen wellicht niet voor u gelden.

ONDER TOEPASSELIJK RECHT IS BELKIN INTERNATIONAL, INC. NIET AANSPRAKELIJK VOOR INCIDENTELE, BIJZONDERE, DIRECTE, INDIRECTE, BIJKOMENDE OF MEERVOUDIGE SCHADE WAARTOE ZONDER ENIGE BEPERKING TE REKENEN SCHADE TEN GEVOLGE VAN GEDERFDE WINST EN/OF GEMISTE OPBRENGSTEN VOORTKOMEND UIT DE VERKOOP OF HET GEBRUIK VAN BELKIN PRODUCTEN, ZELFS ALS DE BETROKKENE VAN MOGELIJKHEID VAN ZULKE SCHADE TEVOREN OP DE HOOGTE WAS GESTELD.

Deze garantie verleent u specifieke wettelijke rechten en wellicht hebt u andere rechten die van staat tot staat kunnen verschillen. In sommige staten en landen is het niet toegestaan incidentele schade, gevolgschade en andere schade uit te sluiten, daarom is het mogelijk dat de bovenstaande garantiebeperkingen voor u niet gelden.



Voor informatie over de verwijdering van afgedankte apparatuur verwijzen wij u naar <http://environmental.belkin.com>

VOOR GEBRUIK IN	AT	BE	CY	CZ	DK	EE	FI	FR	DE	GR	HU	IE		
IT	LV	LT	LU	MT	NL	PL	PT	SK	SI	ES	SE	GB	IS	LI
NO	CH	BG	RO	TR	WERKT OP DE KANALEN 1-13									

In sommige landen gelden gebruiksbeperkingen.....Klasse 2-apparaat

BELKIN®

ADSL2+ modem met ingebouwde draad- loze G router

BELKIN®

www.belkin.com

Technische ondersteuning

Verenigd Koninkrijk: 0845 607 77 87

Europa: www.belkin.com/support

Belkin Ltd.

Express Business Park
Shipton Way, Rushden
NN10 6GL, Verenigd Koninkrijk
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin SAS

130 rue de Silly
92100 Boulogne-Billancourt,
Frankrijk
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH

Hanebergstraße 2
80637 München
Duitsland
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

Belkin Iberia

C/ Anabel Segura, 10 planta baja, Of. 2
28108, Alcobendas, Madrid
Spanje
+34 91 791 23 00
+34 91 490 23 35 fax

Belkin Italy & Greece

Via Carducci, 7
20123 Milaan
Italië
+39 02 862 719
+39 02 862 719 fax

Belkin B.V.

Boeing Avenue 333
1119 PH Schiphol-Rijk,
Nederland
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

© 2007 Belkin International, Inc. Alle rechten voorbehouden. Alle handelsnamen zijn gedeponeerde handelsmerken van de betreffende rechthebbenden. Mac, Mac OS, Apple en AirPort zijn handelsmerken van Apple Inc. die geregistreerd zijn in de Verenigde Staten en in andere landen. Microsoft, NT, Windows en Windows Vista zijn in de Verenigde Staten en/of andere landen geregistreerde handelsmerken of handelsmerken van Microsoft Corporation.

P74725ea-A

BELKIN®

Módem ADSL2+ con router inalámbrico G

EN

FR

DE

NL

ES

IT



Manual del usuario

F5D7632ea4A

Índice de contenidos

1. Introducción	1
Características del producto	1
Ventajas de una red doméstica	3
Ventajas de una red inalámbrica de Belkin.....	3
2. Asegúrese de tener lo siguiente	4
Contenido del paquete	4
Requisitos del sistema	4
Requisitos del sistema para el programa del asistente de instalación	4
Ajustes para la conexión a Internet	4
3. Presentación de su router	5
4. Conexión y configuración de su router	8
Paso 1A: Conexiones de hardware: siga las instrucciones de la guía de instalación rápida	8
Paso 1B: Sustitución de su módem o módem router ya existente	9
Paso 2: Configuración del router: ejecute el software del asistente de instalación	10
5. Configuración manual del router	13
Utilización de la interfaz de usuario a través de Internet	13
Modificación de los ajustes LAN	15
Lista de clientes DHCP	16
Internet WAN	17
Tipo de conexión	17
Inalámbrico	23
Encriptación/seguridad	25
Extensión del alcance inalámbrico y puenteo inalámbrico	35
Firewall	37
Utilidades	43
6. Configuración manual de los adaptadores de red	51
7. Ajustes recomendados para el navegador de Internet	55
8. Solución de problemas	57
9. Información sobre la asistencia técnica	68
10. Apéndices	69
Anexo A: Glosario	69
Anexo B: Factores importantes de colocación e instalación	74
11 Información	77

Gracias por la adquisición del módem ADSL+ con router inalámbrico G de Belkin (el router). En pocos minutos podrá compartir su conexión a Internet y establecer una red entre sus ordenadores con su nuevo router. A continuación presentamos una lista de características que convierten su nuevo router en la solución ideal para su red de oficina pequeña o del hogar. Lea atentamente el presente manual del usuario y preste especial atención al Anexo B titulado “Factores importantes para la colocación y configuración”.

Características del producto

Compatibilidad con ordenadores PC y Mac®

El router soporta una gran variedad de entornos de red, incluyendo Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP, Vista y otros. Todo lo que se necesita es un navegador de Internet y un adaptador de red que soporte TCP/IP (el idioma estándar de Internet).

Indicadores LED del panel frontal

Los LEDs del panel frontal del router que se encuentran iluminados indican qué funciones están activas. De un vistazo podrá saber si su router se encuentra conectado a Internet. Esta característica elimina la necesidad de disponer de software avanzado y procedimientos de control de estado.

Interfaz de usuario avanzado mediante el navegador de Internet

Puede configurar las funciones avanzadas del router de forma sencilla a través de su navegador de Internet, sin necesidad de instalar software adicional en su ordenador. No es preciso instalar discos y, lo que es aún mejor, puede efectuar cambios y llevar a cabo funciones de configuración desde cualquier ordenador de la red de forma rápida y sencilla.

Conmutador de 4 puertos 10/100 integrado

El Router dispone de un conmutador de red de 4 puertos incorporado que permite a los ordenadores conectados en red compartir impresoras, datos y archivos MP3, fotos digitales y mucho más. El conmutador cuenta con la función de detección automática, de forma que se adaptará a la velocidad de los dispositivos conectados. El conmutador transferirá datos entre los ordenadores e Internet simultáneamente sin interrumpir o consumir recursos.

Punto de acceso inalámbrico 802.11g integrado

802.11g es una nueva tecnología inalámbrica que alcanza velocidades de transmisión de datos de hasta 54Mbps, casi cinco veces más rápida que 802.11b.

Protocolo de configuración de host dinámico incorporado (DHCP)

El Protocolo de configuración de host dinámico (DHCP, Dynamic Host Configuration Protocol) incorporado garantiza la conexión más sencilla posible a una red. El servidor de DHCP asignará direcciones IP a cada ordenador de forma automática, de forma que no sea necesario configurar una interconexión en red compleja.

Compartir dirección IP con NAT

Su router emplea NAT (Network Address Translation, Traducción de direcciones de red) para compartir la única dirección IP que le ha asignado su Proveedor de Servicios de Internet, evitando así los costes que supondría el empleo de direcciones IP adicionales para su cuenta de servicios de Internet.

Firewall SPI

Su router está equipado con un firewall que protege su red de una amplia gama de ataques habituales de piratas informáticos, incluidos IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP with zero length, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect y fragment flooding.

Filtrado de direcciones MAC

Para lograr una seguridad adicional, puede configurar una lista de direcciones MAC (identificadores exclusivos de los clientes) que dispongan de permiso para acceder a su red. Cada ordenador cuenta con su propia dirección MAC. Simplemente deberá introducir dichas direcciones MAC en una lista utilizando la interfaz de usuario a través de Internet y podrá controlar el acceso a su red.

Compatibilidad con Plug-and-Play universal (UPnP)

El UPnP (Universal Plug-and-Play, Plug-and-Play universal) es una tecnología que ofrece un funcionamiento perfecto de las opciones de mensajes de voz, mensajes de vídeo, juegos y otras aplicaciones compatibles con UPnP.

Soporta paso a través de VPN

Si se conecta desde casa a su red de oficina utilizando una conexión VPN, su router permitirá a su ordenador equipado con VPN pasar por el router y llegar a la red de la oficina.

Ventajas de una red doméstica

Siguiendo nuestras sencillas instrucciones de instalación, podrá utilizar en casa su red de Belkin para:

- Compartir una conexión de Internet de alta velocidad con todos los ordenadores de su hogar
- Compartir recursos, como archivos y discos duros, entre todos los ordenadores conectados en su hogar
- Compartir una única impresora con toda la familia
- Compartir documentos, música, vídeo e imágenes digitales
- Almacenar, recuperar y copiar archivos de un ordenador a otro
- Participar en juegos on-line, consultar su correo electrónico y chatear de forma simultánea

Ventajas de una red inalámbrica de Belkin

Movilidad: ya no necesitará una “sala de ordenadores” específica, ahora podrá trabajar en cualquier parte dentro de su alcance inalámbrico con un ordenador de sobremesa o portátil conectado en red

Instalación sencilla: el asistente de instalación sencilla de Belkin facilita la instalación

Flexibilidad: instale y acceda a impresoras, ordenadores y otros dispositivos de red desde cualquier punto de su hogar

Fácil ampliación: la extensa gama de productos de interconexión en red de Belkin le permite ampliar su red para incluir dispositivos como, por ejemplo, impresoras y videoconsolas de juegos

Sin necesidad de cableado: podrá ahorrarse los gastos y las complicaciones de colocar cableado Ethernet por todo su hogar u oficina

Aceptación general en el sector : seleccione entre una amplia gama de productos de interconexión en red compatibles

Asegúrese de tener los siguientes elementos al alcance de la mano

Contenido del paquete

- Módem ADSL2+ con router inalámbrico G
- Cable de teléfono RJ11 (de color gris)
- Cable de red Ethernet RJ45: amarillo
- Microfiltro ADSL*
- Adaptador de alimentación
- Manual de usuario y software de asistente de instalación en CD-ROM

*El microfiltro ADSL varía según el país. Si éste no está incluido, necesitará adquirir uno.

Requisitos del sistema

- Un servicio ADSL activo con un enchufe de pared para el teléfono para conectar el router
- Al menos un ordenador con una tarjeta de interfaz de red (NIC, Network Interface Card) y un navegador de Internet instalado y configurado correctamente
- Protocolo de red TCP/IP instalado en todos los ordenadores conectados al router
- Ningún otro servidor de su red local debe asignar las direcciones IP a ordenadores y dispositivos

Requisitos del sistema del software del asistente de instalación

- Un PC que ejecute Windows® 2000, XP o Vista™
- Como mínimo un procesador de 500MHz y 128MB RAM
- Navegador Internet

Ajustes para la conexión a Internet

El asistente de instalación contiene una base de datos de los proveedores de Internet (ISP) de cada país para ayudarle a que configure su router rápidamente. Si su proveedor ISP no se encuentra en la lista, solicite a su ISP la siguiente información antes de configurar router .

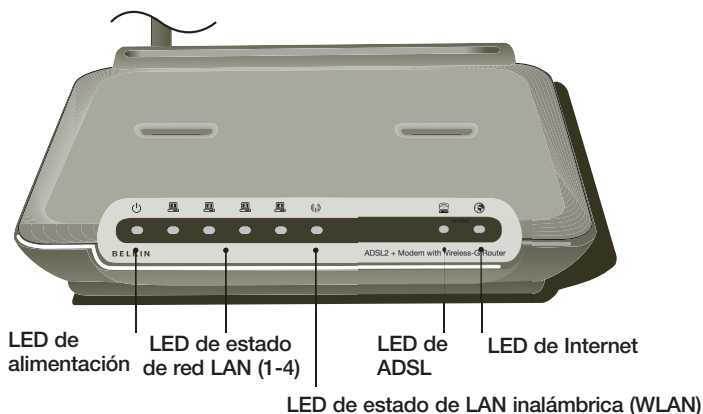
- Protocolo de conexión a Internet: (PPPoE, PPPoA, IP dinámica, IP estática)
- Método múltiplex o encapsulamiento: (LLC o VC MUX)
- Circuito virtual: VPI (Identificador virtual de ruta) _____
(un número entre 0 y 255)
- VCI (Identificador virtual de canal) _____
(un número entre 1 y 65535)
- Para usuarios PPPoE y PPPoA: Nombre de usuario y contraseña de la cuenta ADSL _____
- Para usuarios de IP estática: Dirección IP. ____ . ____ . ____ . ____
Máscara de subred ____ . ____ . ____ . ____
Servidor de Puerta de enlace predeterminada ____ . ____ . ____ . ____
- Dirección IP para el servidor de nombres de dominio ____ . ____ . ____ . ____ (si ha sido suministrado por su ISP)

Presentación de su router

El router ha sido diseñado para su colocación sobre un escritorio. Todos los cables salen de la parte posterior del router para lograr una mejor organización y utilidad. Los indicadores LED se encuentran fácilmente visibles en la parte frontal del router para proporcionar información acerca de la actividad y el estado de la red.

Panel frontal

La siguiente ilustración muestra el panel frontal del router:






Indicadores LED

El router está equipado con nueve LEDs en el panel frontal tal y como se describe en la tabla de la página siguiente (de izquierda a derecha):

1
2
3
4
5
6
7
8
9
10
11

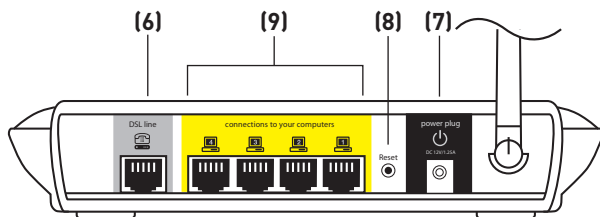
sección

Presentación de su router

LED	Color	Estado	Descripción
ADSL			
	Verde	APAGADO	Sin alimentación o la conexión de la línea ADSL está físicamente desconectada
		Intermitente	Establecimiento de enlace en progreso
		Permanente	La conexión de la línea ADSL está bien
Inalámbrico			
	Verde	APAGADO	Apagado o sin señal de radio (la tarjeta WLAN no está o no funciona)
		Intermitente	El tráfico va a través de la interfaz LAN inalámbrica
		Permanente	Interfaz LAN inalámbrica lista para funcionar
Internet			
	Verde	APAGADO	Sin conexión Internet
		Intermitente	Transmisión o recepción de datos
		Permanente	Conectado a Internet
De LAN 1 a LAN 4			
LAN 1 -4	Verde	APAGADO	Sin alimentación o ningún operador Ethernet está presente
		Intermitente	Un operador Ethernet está presente y los datos del usuario se transmiten a través del puerto Ethernet
		Permanente	Está presente un operador Ethernet
Alimentación			
	Verde	APAGADO	Desconectado
		Permanente	Encendido

Panel posterior

La siguiente ilustración muestra el panel posterior de su router.



Enchufe de alimentación: — conecte el suministro de alimentación incluido a esta toma. Si utiliza un adaptador de alimentación incorrecto, podrá causar daños irreversibles a su router.

Puertos Ethernet—Los puertos Ethernet son RJ45, 10/100 de negociación automática. Los puertos presentan etiquetas con números del 1 al 4. Dichos puertos se corresponden con los LEDs numerados de la parte frontal del router. Conecte sus ordenadores de red o cualquier otro dispositivo de red a uno de estos puertos.

Línea ADSL :Este puerto es para la conexión de la línea ADSL. Conecte su línea ADSL a este puerto.

Botón de reinicio :El botón de “Reset” (Reinicio) se emplea en casos excepcionales cuando el router puede estar funcionando mal. Al reiniciar el router se restablecerá el funcionamiento normal del mismo manteniendo los ajustes programados. También puede restablecer los ajustes de fábrica utilizando el botón de reinicio. Emplee la función de restablecimiento en casos como cuando haya olvidado su contraseña personal.

a. Reinicio del router

Mantenga pulsado el botón de Reinicio durante un segundo y suéltelo después. Cuando la luz de Encendido obtenga de nuevo un color permanente, el reinicio habrá sido completado.

b. Restablecimiento de los ajustes por defecto de fábrica

Mantenga pulsado el botón de Reinicio durante veinte segundos y suéltelo después. Cuando la luz de encendido/listo parpadee de nuevo, se habrán restablecido los ajustes.

Conexión y configuración de su router

Asistente de configuración

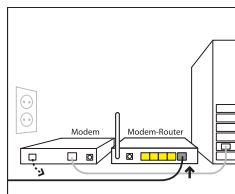
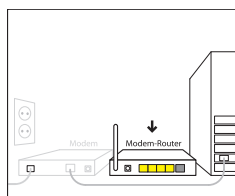
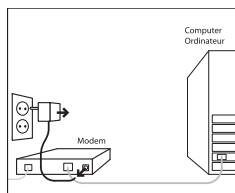
Belkin le suministra el software de nuestro asistente de instalación sencilla para facilitarle la tarea de instalar su router. Al utilizarlo, logrará que su router esté listo y funcionando en pocos minutos. El asistente de instalación requiere que su ordenador con Windows 2000, XP o Vista™ esté conectado directamente a la línea de ADSL y que la conexión a Internet se encuentre activa y funcionando en el momento de la instalación. En caso contrario, deberá utilizar la sección “Método alternativo de configuración” de este manual del usuario para configurar su router. Además, si está utilizando un sistema operativo diferente a Windows 2000, XP o Vista o Mac OS X, debe utilizar la sección de “Método Alternativo de Configuración” de este manual del usuario.

Paso 1A: Conexiones de hardware: siga las instrucciones de la Guía de instalación rápida

Instalación de un router nuevo

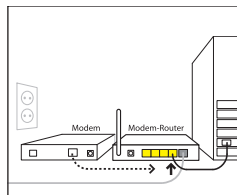
Siga estos pasos si NO está reemplazando un módem ya existente. Si está reemplazando un módem ya existente, pase a la siguiente sección, “Sustitución de un módem o módem router ya existente”, en la página 9.

- 1A.1** Saque su nuevo router del paquete y colóquelo junto a su ordenador. Levante la antena del router.
- 1A.2** Recupere el cable amarillo RJ45 incluido en el router. En primer lugar, conéctelo a cualquiera de los puertos amarillos con la indicación “Wired Computers” (ordenadores por cable) en la parte trasera de su router. A continuación conecte el otro extremo al puerto de red en la parte trasera del ordenador. [Inserte el logotipo Ethernet]
- 1A.3** Recupere el cable telefónico gris RJ11 incluido. Conecte un extremo al puerto gris con la indicación “DSL” de la parte trasera de su router. Después conecte el otro extremo a su conexión ADSL (o bien a una toma de pared o a un distribuidor ADSL).



Nota: Algunas conexiones ADSL requieren un microfiltro. Su proveedor de ADSL puede informarle sobre si necesita uno. Belkin incluye un microfiltro para las zonas en las que es necesario. Para determinar si necesita un microfiltro, remítase al manual del usuario de su proveedor de ADSL.

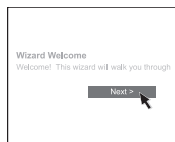
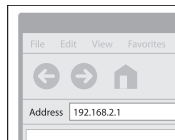
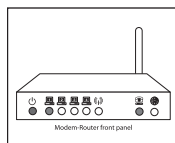
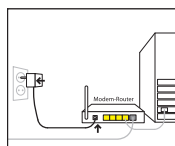
- 1A.4** Conecte el suministro de alimentación del router en el puerto negro de la parte trasera por la indicación “Power” (Alimentación). Espere 20 segundos para que el router arranque. Compruebe los indicadores de la parte delantera del Router. Asegúrese de que los iconos “Wired” (cableado) y “Módem Router” estén iluminados en verde. En caso contrario, vuelva a comprobar sus conexiones.



Paso 1B: Sustitución de su módem o módem router ya existente

Siga estos pasos si actualmente tiene un módem o un módem router que va a sustituir por su nuevo router.

- 1B.1** Saque su nuevo router del paquete y colóquelo junto a su módem antiguo. Levante la antena del router. Desconecte el cable de alimentación de su módem antiguo.
- 1B.2** Localice el cable que conecta el módem antiguo a su ordenador. Desenchufe este cable de su módem antiguo y conéctelo en cualquiera de los puertos amarillos con la indicación “Wired Computers” (ordenadores por cable) de la parte trasera del nuevo router.
- 1B.3** Localice el cable que conecta su antiguo módem a la toma ADSL. Desenchúfelo de su viejo módem y a continuación conéctelo al puerto gris marcado como “DSL” de la parte trasera del router.
- 1B.4** Conecte el suministro de alimentación del router en el puerto negro de la parte trasera por la indicación “Power” (Alimentación).
- 1B.5** Espere 20 segundos para que el router arranque. Compruebe los indicadores de la parte delantera del Router. Compruebe que los LEDs de “ADSL” y “LAN” estén iluminados en verde. En caso contrario, vuelva a comprobar sus conexiones.



Paso 2: Configuración del router: ejecute el software del asistente de instalación

2.1 Apague cualquier programa que esté funcionando en el ordenador en ese momento. Apague cualquier firewall o software para compartir conexiones a Internet.

2.2 Introduzca el CD en el ordenador. El asistente de instalación aparecerá de manera automática en la pantalla de su ordenador en un plazo de 15 segundos. Haga clic en “Go” (Comenzar) para ejecutar el asistente de instalación. Siga las instrucciones.

IMPORTANTE: Ejecute el asistente de instalación en el ordenador que está conectado directamente al Router desde el paso 1A.2.

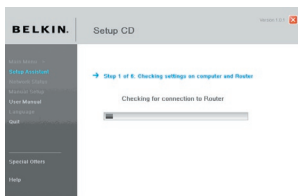
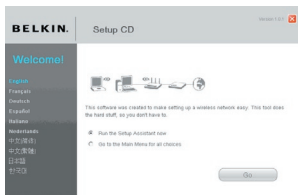
Advertencia para usuarios de Windows: Si el asistente de instalación no se inicia de forma automática, seleccione su unidad de CD-ROM en “Mi PC” y haga doble clic sobre el archivo con el nombre “SetupAssistant” (asistente de instalación) en la unidad de CD-ROM.

2.3 Seleccione un país. Seleccione su país de la lista desplegable. Haga clic en “Next” (Siguiente) para continuar.

2.4 Pantalla de confirmación. Confirme que ha completado todos los pasos de la guía de instalación rápida marcando el recuadro que se encuentra a la derecha de la flecha. Haga clic en “Next” (Siguiente) para continuar.

2.5 El asistente de configuración le mostrará la pantalla de progreso cada vez que se haya completado un paso de la instalación.

2.6 Comprobación de los ajustes. El asistente procederá ahora a examinar las configuraciones de red de su ordenador y a recopilar la información precisa para completar la conexión a Internet del router.



2.7 Verificación de las conexiones del hardware El asistente de instalación ahora comprobará las conexiones de su hardware.

2.8 Denominación de la red inalámbrica.

El asistente de instalación mostrará el nombre de la red inalámbrica por defecto o el SSID (Service Set Identifier) Este es el nombre de la red inalámbrica a la que se conectarán sus ordenadores o dispositivos con adaptadores de red inalámbrica. Puede utilizar este nombre predeterminado o cambiarlo por otro exclusivo. Escriba el nombre por si lo necesita en el futuro. Haga clic en “Next” (siguiente) para continuar.

2.9 Requerimiento de la información de la cuenta Internet (si es necesario)

Si su cuenta de Internet requiere de un nombre de usuario y de una contraseña, se abrirá una ventana parecida a la siguiente. Seleccione su país o su ISP del listado de los recuadros desplegados.

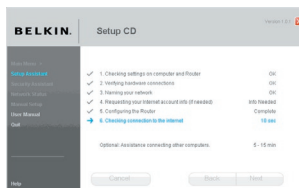
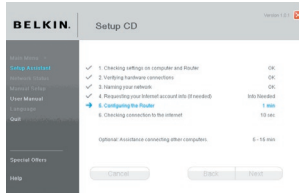
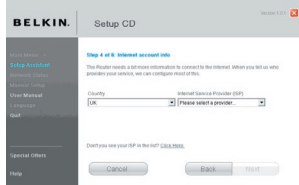
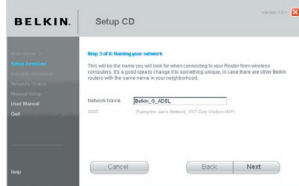
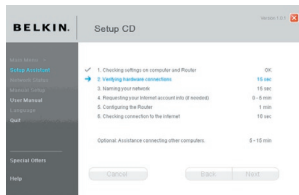
2.10 Configuración del router

El asistente de instalación a continuación configurará su router enviando datos al router y reiniciándolo. Espere a que aparezcan las instrucciones en la pantalla.

Nota: No desconecte ningún cable ni apague el router cuando éste se esté reiniciando. Si lo hace podría dañar el router dejándolo inoperativo.

2.11 Comprobación de la conexión Internet

Casi hemos terminado. El asistente de instalación ahora comprobará su conexión a Internet.



1
2
3
4
5
6
7
8
9
10
11

Enhorabuena

Ha terminado de instalar su nuevo router de Belkin. Cuando su router pueda conectarse a Internet, verá la pantalla de enhorabuena. Puede comenzar a navegar por Internet abriendo su navegador y dirigiéndose a cualquier la página web.

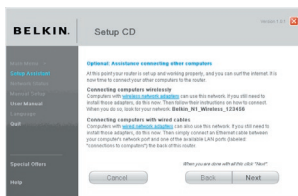
Puede utilizar el asistente de instalación para configurar sus otros ordenadores y que se conecten a Internet de forma inalámbrica o mediante cables, haciendo clic en “Next” (Siguiente). Si prefiere añadir ordenadores a su router más adelante, seleccione “Exit the Assistant” (Salir del Asistente) y, a continuación, haga clic en “Next” (Siguiente).

Solución de problemas

Si el asistente de instalación no puede conectarse a Internet, aparecerá esta pantalla. Siga las instrucciones para llevar a cabo los pasos de resolución de problemas.

2.12 Opcional: Asistencia para conectar otros ordenadores. Este paso opcional le ayudará a conectar los ordenadores a la red mediante cables y los ordenadores inalámbricos. Siga las instrucciones que aparecen en la pantalla.

Si ha verificado que todos los ordenadores conectados mediante cables e inalámbricos se encuentran conectados correctamente, su red está configurada y en funcionamiento. Ahora puede navegar por Internet. Haga clic en “Next” (Siguiente) para volver al menú principal.

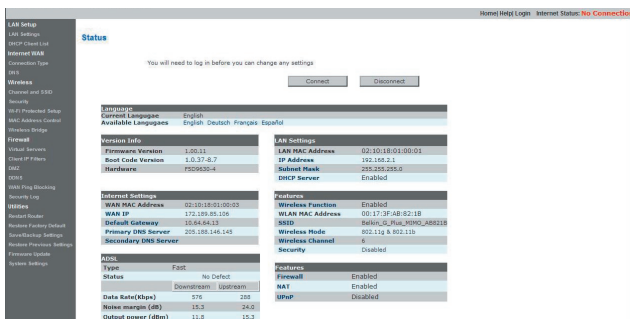


Utilización de la interfaz de usuario a través de Internet

La página principal le ofrece una imagen rápida del estado y los ajustes del router. Desde esta página es posible acceder a todas las páginas de configuración avanzada.

Empleo de la interfaz de instalación a través de Internet

Una vez que el PC está configurado convenientemente, inicie el navegador de red e introduzca la dirección IP privada del router en el campo URL: “192.168.2.1” y después haga clic en “Enter” (intro).



1. Vínculos de navegación rápida

Puede ir directamente a cualquiera de las páginas de la UI del router haciendo clic directamente en estos vínculos. Los vínculos se encuentran divididos en categorías lógicas y agrupados por pestañas para facilitar la búsqueda de un ajuste concreto. Al hacer clic sobre el encabezamiento de color morado de cada pestaña aparecerá una breve descripción de la función de la misma.

2. Botón de Inicio (“Home”)

El botón de inicio se encuentra disponible en todas las páginas de la UI. Al pulsar este botón, regresará a la página principal.

3. Botón de ayuda

El botón de ayuda (“Help”) le permite acceder a las páginas de ayuda del router. La opción de ayuda se encuentra disponible asimismo en muchas páginas haciendo clic en la opción “more info” (más información) situada junto a determinadas secciones de cada página.

4. Botón de “Login”/“Logout” (Acceder/Salir)

Este botón le permite acceder y salir del router pulsando un solo botón. Cuando ha accedido al router, este botón mostrará la palabra “Logout” (Salir). El acceso al router le llevará a una página independiente de acceso en la que será preciso introducir una contraseña. Cuando haya accedido al router podrá efectuar cambios en los ajustes. Cuando haya terminado de realizar los cambios, podrá salir del router haciendo clic sobre el botón de “Logout” (Salir). Para obtener más información acerca del acceso al router, consulte la sección “Logging into the Router” (Acceso al router).

5. Indicador del estado de Internet

Este indicador está visible en todas las páginas del router, indicando el estado de la conexión del mismo. Cuando el indicador muestra “connection OK” (Conexión en buen estado) en VERDE, el router se encuentra conectado a Internet. Cuando el router no está conectado a Internet, el indicador mostrará el mensaje “no connection” (sin conexión) en ROJO. El indicador es actualizado automáticamente cuando usted efectúe cambios en las configuraciones del router.

6. Ajustes LAN

Le muestra los ajustes de la red LAN del router. Pueden hacerse cambios en los ajustes haciendo clic en el enlace “LAN” y “Quick Navigation” (navegación rápida) en la parte izquierda de la pantalla.

7. Prestaciones

Le muestra el estado del NAT, firewall y características inalámbricas del Router. Es posible efectuar cambios en los ajustes haciendo clic en cualquiera de los vínculos o haciendo clic en los vínculos de “Quick Navigation” (Navegación rápida) de la parte izquierda de la pantalla.

8. Ajustes de Internet

Muestra los ajustes de la parte de Internet/WAN del router que se conecta a Internet. Es posible efectuar cambios en cualquiera de estos ajustes haciendo clic en cualquiera de los vínculos o haciendo clic en el vínculo de Navegación rápida “Internet/WAN” de la parte izquierda de la pantalla.

9. Información sobre la versión

Muestra la versión del firmware, la versión del código de arranque, la versión del hardware y el número de serie del router.

10. Nombre de la página

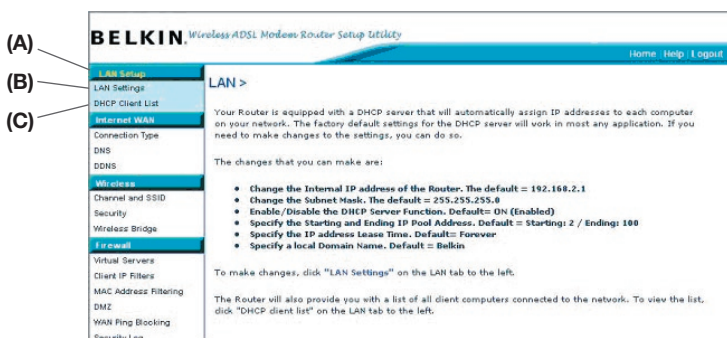
La página en la que se encuentra puede ser identificada con este nombre. El presente manual se referirá en ocasiones a las páginas por el nombre. Por ejemplo, “LAN > LAN Settings” se refiere a la página “LAN Settings” (Ajustes LAN).

Modificación de los ajustes LAN

Todos los ajustes para la configuración de la LAN interna del Router pueden ser visualizados y modificados aquí.

Ajustes LAN

Al hacer clic en el encabezamiento de la pestaña LAN (A) accederá a la página de encabezamiento de la pestaña LAN. Aquí se puede encontrar una breve descripción de las funciones. Para visualizar los ajustes o realizar cambios en alguno de los ajustes LAN, haga clic en “LAN Settings” (Ajustes LAN) (B), y para visualizar la lista de ordenadores conectados, haga clic en “DHCP Client List” (Lista de clientes DHCP) (C).



Dirección IP

La “IP address” (dirección IP) es la dirección IP interna del router. La dirección IP por defecto es “192.168.2.1”. Para acceder a la interfaz de configuración avanzada, escriba esta dirección IP en la barra de direcciones de su buscador. Esta dirección puede ser modificada en caso necesario. Para modificar la dirección IP, introduzca la nueva dirección IP y haga clic en “Apply Changes” (Aplicar cambios). La dirección IP seleccionada será un IP no enrutable. Ejemplos de IP no enrutable son:

192.168.x.x (donde x es una cifra entre el 0 y el 255)

10.x.x.x (donde x es una cifra entre el 0 y el 255)

Máscara de subred

No es necesario modificar la máscara de subred. Esta es una característica exclusiva y avanzada de su adaptador de Belkin.

Servidor DHCP

La función de servidor DHCP facilita en gran medida la tarea de establecer una red asignando direcciones IP a cada ordenador de la red de forma automática. El ajuste por defecto es “On” (Encendido). El servidor DHCP puede ser APAGADO en caso necesario; sin embargo, para hacerlo deberá establecer de forma manual una dirección IP estática para cada ordenador de su red. Para apagar el servidor DHCP, seleccione “Off” (Apagado) y haga clic en “Apply Changes” (Aplicar cambios).

“IP Pool” (Conjunto de IP)

La gama de direcciones IP reservadas para la asignación dinámica a los ordenadores de su red. Si desea modificar este número, puede hacerlo introduciendo una nueva dirección IP de inicio y final y haciendo clic en “Apply Changes” (Aplicar cambios). La dirección IP de inicio deberá ser inferior en su número a la dirección IP de final.

“Lease Time” (Tiempo límite de concesión)

La cantidad de tiempo que el servidor DHCP reservará la dirección IP para cada ordenador. Le recomendamos dejar la configuración del tiempo de mantenimiento en “Forever” (Para siempre). La configuración por defecto es “Forever” (Para siempre), lo que significa que cada vez que el servidor DHCP asigne una dirección IP a un ordenador, la dirección IP no cambiará para ese ordenador concreto. Si configura el tiempo límite de concesión en intervalos menores como un día o una hora, las direcciones IP serán liberadas una vez transcurrido dicho periodo específico de tiempo. Esto significa además que la dirección IP de un ordenador determinado puede cambiar a lo largo del tiempo. Si ha establecido cualquier otra de las características avanzadas del router, como filtros IP de clientes o DMZ, éstas dependerán de la dirección IP. Por esta razón, no es deseable para usted que cambie la dirección IP.

Nombre de dominio local

Puede establecer un nombre de dominio local (nombre de red) para su red. No es necesario modificar este ajuste a no ser que tenga una necesidad avanzada específica para hacerlo. Puede dar a la red el nombre que quiera como “MI RED”.

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing “Refresh” will update the list.

IP Address	Host Name	MAC Address
192.168.2.11	Ericd-XP	00-30-BD-3D-AB-09

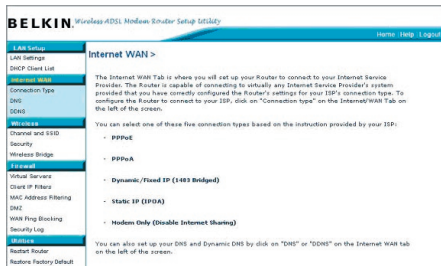
[Refresh](#)

Lista de clientes DHCP

Puede visualizar una lista de los ordenadores que se encuentran conectados a su red. Puede visualizar la dirección IP del ordenador, el nombre de host (si se ha asignado uno al ordenador) y la dirección MAC de la tarjeta de interfaz de red (NIC, network interface card) del ordenador. Al pulsar el botón “Refresh” (Actualizar) se actualizará la lista. Si se han producido cambios, la lista se actualizará.

Internet WAN

En la pestaña “Internet/WAN” configurará su router para conectar con su proveedor de servicios de Internet (ISP, Internet Service Provider). El router es capaz de conectarse a prácticamente cualquier sistema de Proveedor de servicios de ADSL siempre que hayan sido configurados correctamente los ajustes del router para su tipo de conexión al ISP. Los ajustes de su conexión le son suministrados por su ISP. Para configurar el router con los ajustes que le ha proporcionado su ISP, haga clic en “Connection Type” (Tipo de conexión) (1) en la parte izquierda de la pantalla. Seleccione el tipo de conexión que emplea. Si su ISP le ha proporcionado ajustes DNS, al hacer clic sobre “DNS” (2) podrá introducir entradas de direcciones DNS para ISPs que requieran ajustes específicos. Cuando haya finalizado de realizar los ajustes, el indicador de “Internet Status” (Estado de Internet) mostrará el mensaje “Connected” (Conectado) si su router ha sido configurado correctamente.



Tipo de conexión

En la página “Connection Type” (Tipo de conexión), podrá seleccionar uno de los cinco tipos de conexiones basadas en las instrucciones proporcionadas por su ISP.

PPPoE

PPPoA

IP dinámica (1483 Bridged)

IP estática (IPoA)

Sólo módem (Desactivar Compartir Internet)

Nota: Si tiene dudas sobre qué tipo de conexión seleccionar, consulte a su ISP.

Seleccione el tipo de conexión que emplea haciendo clic en el botón situado junto a su tipo de conexión y después haciendo clic en “Next” (Siguiente).

Configuración manual del router

WAN > Connection type

The following information is usually provided by your ISP. Please select the Internet sharing protocol.

- PPPoE
- PPPoA
- Dynamic/Fixed IP (1481 Bridge)
- Static IP (PPPoA)
- Modem Only (Disable Internet Sharing)

Next

Establecimiento del tipo de conexión de su ISP como PPPoE o PPPoA

PPPoE (Protocolo punto a punto a través de Ethernet) es el método estándar de conexión de dispositivos de red. Requiere un nombre de usuario y una contraseña para acceder a la red de su ISP y conectarse a Internet. PPPoA (PPP sobre ATM) es similar a PPPoE. Es muy frecuente en el Reino Unido. Seleccione PPPoE o PPPoA y haga clic en “Next” (Siguiente). Luego, ingrese la información que le ha proporcionado su ISP y haga clic en “Apply Changes” (Aplicar cambios) para activar los ajustes.

WAN > Connection Type > PPPoE Interface

More Info
ATM Interface

(1)	Username	<input type="text"/>
(2)	Password	<input type="password"/>
(3)	Retype Password	<input type="password"/>
(4)	IP assigned by ISP >	Yes <input checked="" type="checkbox"/>
	IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
	Subnet Mask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
	Default Gateway	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
(5)	VPI/VCI	<input type="text" value="0"/> / <input type="text" value="35"/>
(6)	Encapsulation	LLC <input checked="" type="checkbox"/>
(7)	Dial on Demand >	<input type="checkbox"/>
(8)	Idle Time (Minute) >	<input type="text" value="0"/>
(9)	MTU >	<input type="text" value="1456"/>

Clear Changes Apply Changes

1. Nombre de usuario: introduzca el nombre de usuario. (Asignado por su ISP).

2. Contraseña: introduzca su contraseña. (Asignada por su ISP).

3. Confirmación de la contraseña: vuelva a introducir la contraseña.

(Asignada por su ISP).

4. IP asignada por su ISP: deje “Yes” (sí) si su ISP le asigna automáticamente una dirección IP. Si su ISP le ha asignado una dirección IP estática, seleccione “No” e ingrese la dirección correspondiente.

5. VPI/VCI introduzca aquí los parámetros de su identificador de ruta virtual (VPI) y del identificador de circuito virtual (VCI). (Asignados por su ISP).
6. Encapsulamiento seleccione el tipo de encapsulamiento correspondiente (suministrado por su ISP) para especificar cómo manejar múltiples protocolos en la capa de transporte ATM. VC-MUX: PPPoA Circuito Virtual Multiplexeado (encapsulamiento anulado) permite sólo un protocolo por circuito virtual con poca sobrecarga. LLC: PPPoA Control de Enlace Lógico permite múltiples protocolos sobre un único circuito virtual (con más sobrecarga).
7. Conexión telefónica por demanda: al seleccionar “Dial on Demand” (Conexión telefónica por demanda), su router se conectará automáticamente a Internet cuando un usuario abra el navegador de red.
8. Tiempo límite de inactividad:: introduzca aquí el tiempo límite de inactividad para la conexión a Internet. Cuando haya transcurrido este período de tiempo, la conexión será finalizada.
9. MTU : el ajuste MTU no debería ser modificado nunca a no ser que su ISP le

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

IP assigned by ISP >

IP Address

Subnet Mask

Default Gateway

VPI/VCI

Encapsulation

Yes				
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	/	35		
LLC				

Clear Changes

Apply Changes

proporcione un ajuste MTU específico. Si se efectúan cambios en el ajuste MTU, pueden surgir problemas con su conexión a Internet, incluyendo la desconexión, un acceso lento a Internet y problemas para el correcto funcionamiento de las aplicaciones de Internet.

Establecimiento del tipo de conexión como IP dinámica (1483 Bridged)

Este método de conexión crea un puente entre su red y la de su ISP. El router obtendrá automáticamente una dirección de IP del servidor DHCP de su ISP.

Configuración manual del router

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

(1) IP assigned by ISP > Yes

(2) IP Address > 0 0 0 0

Subnet Mask > 0 0 0 0

(2) Default Gateway > 0 0 0 0

VPI/VCI > 0 / 35

(3) Encapsulation > LLC

Clear Changes Apply Changes

1. IP asignada por su ISP: deje “Yes” (sí) si su ISP le asigna automáticamente una dirección IP. Si su ISP le ha asignado una dirección IP estática, seleccione “No” e ingrese la dirección correspondiente.

2. VPI/VCI : introduzca aquí los parámetros de VPI y VCI. Estos identificadores le serán suministrados por su ISP.

3. Encapsulamiento: seleccione LLC o VC MUX que utiliza su ISP.

Establecimiento de su tipo de conexión al ISP como IP estático (IPoA)

Este tipo de conexión también se denomina “Clásico IP sobre ATM” o “CLIP”, en el cual su ISP le proporciona un IP fijo para que su router se conecte al Internet.

WAN > Connection Type > Static IP(IPoA)

More Info
ATM Interface

(1) IP Address > 0 0 0 0

(2) Subnet Mask > 0 0 0 0

(3) Default Gateway > 0 0 0 0

(4) VPI/VCI > 0 / 35

(5) Encapsulation > LLC

Clear Changes Apply Changes

1. Dirección IP: introduzca la dirección de IP que le ha asignado su ISP para la interfaz WAN de su router.

2. Máscara de subred WAN : introduzca la máscara de subred que le ha asignado su ISP.

3. Pasarela predeterminada : introduzca una dirección IP de pasarela predeterminada. Si el router no puede encontrar la dirección de destino dentro de la red local, reenviará los paquetes a la pasarela por defecto que le ha asignado su ISP.

4. VPI/VCI : introduzca aquí los parámetros de VPI y VCI. Estos identificadores le serán suministrados por su ISP.

5. Encapsulamiento: seleccione LLC o VC MUX que utiliza su ISP.

Establecimiento del tipo de conexión como “Sólo módem” (Desactivar compartido de Internet)

En este modo, el router actúa sólo como puente por el que pasan los paquetes hacia el puerto DSL. Requiere la instalación de software adicional que debe ser instalado en su ordenador para poder acceder a Internet.

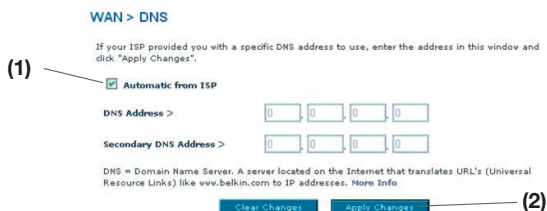


1. VPI/VCI: introduzca aquí los parámetros de VPI y VCI. (Asignados por su ISP).
2. Encapsulamiento: seleccione LLC o VC MUX. (Asignados por su ISP).

Ajustes de DNS (Servidor de nombres de dominio)

Un “Domain Name Server” es un servidor ubicado en Internet que convierte los Universal Resource Locator (URL, Localizador de recursos universales) como “www.belkin.com” en direcciones IP. Muchos ISPs no precisan que usted introduzca esta información en el router. El recuadro “Automatic from ISP” (Automáticamente desde el ISP) (1) [Diseñador: consúltelo en el siguiente pantallazo] deberá encontrarse marcado si su ISP no la ha proporcionado ninguna dirección DNS específica. Si está utilizando un tipo de conexión de IP estática, es posible que deba introducir una dirección DNS específica y una dirección DNS secundaria para que su conexión funcione correctamente. Si su tipo de conexión es dinámica o PPPoE, es probable que no sea necesario introducir ninguna dirección DNS.

Deje marcado el recuadro “Automatic from ISP” (Automáticamente desde el ISP). Para introducir los ajustes de la dirección DNS, retire la marca del recuadro “Automatic from ISP” (Automáticamente desde el ISP) e introduzca sus entradas DNS en los espacios previstos. Haga clic en “Apply Changes” (Aplicar cambios) (2) [Diseñador: consúltelo en el siguiente pantallazo] para guardar los ajustes.



Opción DDNS (DNS dinámico)

El servicio DDNS le permite otorgar a una dirección IP dinámica uno de los muchos nombres de host estático que ofrece la lista de dominios de DynDNS.org; de esta manera, podrá acceder a sus ordenadores en red de manera más sencilla desde varias ubicaciones en Internet. DynDNS.org ofrece a la comunidad de Internet este servicio para hasta cinco nombres de host en forma gratuita. TZO.com es otra alternativa a DynDNS.org. El servicio DDNS es ideal para una página web personal, un servidor de archivos o para facilitar el acceso a su PC del hogar y los archivos guardados cuando está en el trabajo. Mediante la utilización de este servicio puede estar seguro de que el nombre de host siempre indicará a su dirección IP, independientemente de cuántas veces su ISP la cambie. Cuando su dirección IP cambia, sus amigos y socios pueden ubicarlo siempre visitando sunombre.dyndns.org. Puede registrarse de manera gratuita para obtener su nombre de host DNS dinámico en <http://www.dyndns.org>.

Configuración del cliente de actualización para DNS dinámico del router

Debe registrarse para el servicio gratuito de actualización de DynDNS.org antes de poder utilizar esta función. Una vez que se haya registrado, siga las instrucciones a continuación.

1. Ingrese su nombre de usuario de DynDNS.org en el campo “Account / E-mail” (Cuenta de usuario / E-mail) (1).
2. Ingrese la contraseña de DynDNS.org en el campo “Password / Key” (Contraseña / Palabra clave) (2).
3. Introduzca el nombre del dominio DynDNS.org que ha establecido en el campo “Domain Name” (nombre del dominio) (3).
4. Haga clic en “Apply Changes” (Aplicar cambios) para actualizar la dirección IP. Si la dirección IP dinámica que le ha asignado su ISP cambia, el router actualizará automáticamente los servidores de DynDNS.org con la dirección IP nueva. También puede hacer esto de manera manual presionando el botón “Apply Changes” (Aplicar cambios) (4).

En la página “Connection Type” (tipo de conexión), podrá seleccionar el tipo de conexión que quiera utilizar seleccionándolo de la lista desplegable.

WAN > DDNS

DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP address is dynamic. You must Register for DDNS service at one of the listed DDNS Services.

DDNS Service >

DDNS Status >

(1) Account / E-mail >

(2) Password / Key >

(3) Domain Name >

(4)

Tecnología inalámbrica

La pestaña “Wireless” (Inalámbrico) le permite realizar cambios en los ajustes de red inalámbrica. Desde esta pestaña puede efectuar cambios en el nombre de red inalámbrica (SSID), el canal de funcionamiento y en los ajustes de seguridad en la encriptación.

Wireless > Channel and SSID

This page allows you to enter the Wireless Network Name (SSID in Wi-Fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as a wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. [More Info](#)

SSID >	<input type="text" value="Belkin54g"/>
ESSID Broadcast >	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode >	<input type="button" value="Mixed (11b+11g)"/>
Wireless Channel >	<input type="button" value="Auto"/>
<input type="button" value="Clear Changes"/> <input type="button" value="Apply Changes"/>	

Canal y SSID

1. Modificación del Nombre de red inalámbrica (SSID)

Para identificar su red inalámbrica, se emplea un nombre conocido como SSID (Service Set Identifier, Identificador del conjunto de servicios). Puede cambiar este nombre por el que desee o puede dejarlo sin modificar. Si existen otras redes inalámbricas operando en su área, deberá asegurarse de que su SSID sea exclusivo (no coincida con el de otra red inalámbrica en la zona). Para modificar el SSID, introduzca en el campo SSID el SSID que desee utilizar y haga clic en “Apply Changes” (Aplicar cambios). La modificación es inmediata. Si modifica el SSID, es posible que sus ordenadores de equipamiento inalámbrico deban ser configurados de nuevo con su nuevo nombre de red. Consulte la documentación de su adaptador de red inalámbrica para obtener información acerca de cómo realizar esta modificación.

2. Utilización de la función de ESSID Broadcast

Para garantizar la seguridad máxima, deberá optar por no emitir el SSID de su red. Al hacerlo así, mantendrá su nombre de red oculto a los ordenadores que estén rastreando la presencia de redes inalámbricas. Para desactivar la emisión del SSID, seleccione “DISABLE” (desactivar) y luego haga clic en “Apply Changes” (Aplicar cambios). La modificación es inmediata. Ahora será preciso configurar cada ordenador para conectar con su SSID específico; ya no se aceptará la opción “ANY” (Cualquiera) para el SSID. Consulte la documentación de su adaptador de red inalámbrica para obtener información acerca de cómo realizar esta modificación.

Nota: Esta característica avanzada deberá ser empleada exclusivamente por usuarios avanzados.

3. Utilización del Conmutador en Modo Inalámbrico

Su router puede funcionar en tres modos inalámbricos diferentes: “Mixed (11b+11g)” (Modo mixto: 11b+11g), “11g Only” (Sólo 11g), y “11b Only” (Sólo 11b). Los diferentes modos son explicados a continuación.

Modo combinado (11b+11g)

En este modo, el Router es compatible con clientes inalámbricos 802.11b y 802.11g de forma simultánea. Este es el modo por defecto y garantiza el perfecto funcionamiento con todos los dispositivos compatibles con Wi-Fi®. Si cuenta con una combinación de clientes 802.11b y 802.11g en su red, le recomendamos que mantenga el ajuste predeterminado. Este ajuste sólo deberá ser modificado si tiene una razón determinada para hacerlo.

Modo “11g-Only”

El modo “802.11g-Only” sólo funciona con clientes 802.11g. Se recomienda este modo si desea evitar que los clientes 802.11b accedan a su red. Para conmutar los modos, seleccione el modo deseado del recuadro desplegable “Wireless Mode” (Modo inalámbrico). Y luego, haga clic sobre “Apply Changes” (Aplicar cambios).

Modo 11b-Only

Recomendamos NO emplear este modo a menos que tenga una razón muy concreta para hacerlo. Este modo sólo existe para resolver problemas específicos que pueden producirse con algunos adaptadores de clientes 802.11b y NO es necesario para la interoperabilidad de los estándares 802.11g y 802.11b.

4. Modificación del canal inalámbrico

Existe una serie de canales de funcionamiento entre los que puede elegir. En Estados Unidos, existen 11 canales. En Reino Unido y la mayor parte de Europa, existen 13 canales. Un pequeño número de países presentan otros requisitos respecto a los canales. Su router está configurado para funcionar en los canales apropiados para el país en el que reside. El nombre por defecto es “Auto”. Este canal puede ser modificado en caso necesario. Si existen otras redes inalámbricas operando en su área, su red deberá ser configurada para funcionar en un canal diferente que el resto de redes inalámbricas. Para lograr un mejor rendimiento, utilice un canal que se encuentre al menos a cinco canales de distancia del de la otra red inalámbrica. Por ejemplo, si la otra red está funcionando en el canal 11, configure su red en el canal 6 o inferior. Para modificar el canal, selecciónelo de la lista desplegable. Haga clic sobre “Apply Changes” (Aplicar cambios). La modificación es inmediata.

Encriptación/seguridad

Cómo proteger su red Wi-Fi

Presentamos diferentes formas de potenciar la seguridad de su red inalámbrica y de proteger sus datos de intrusiones no deseadas. Esta sección está pensada para el usuario en el hogar, de oficina doméstica y pequeña oficina. Al momento de la publicación de este manual, se encuentran disponibles tres métodos de encriptación.

Nombre	Privacidad equivalente a la del cable de 64 bits	Privacidad equivalente a la del cable de 128 bits	Acceso protegido Wi-Fi-TKIP	Acceso Protegido Wi-Fi 2
Acrónimo	WEP de 64 bits	WEP de 128 bits	WPA-TKIP/AES (o solamente WPA)	WPA2-AES (o solamente WPA2)
Seguridad	Buena	Mejor	La mejor	El mejor
Prestaciones	Claves estáticas	Claves estáticas	Encriptación de clave dinámica y autenticación mutua	Encriptación de clave dinámica y autenticación mutua
	Claves de encriptación basadas en el algoritmo RC4 (habitualmente claves de 40 bits)	Mayor seguridad que la WEP de 64 bits empleando una longitud de clave de 104 bits, más 24 bits adicionales de datos generados por el sistema	TKIP (Protocolo de integridad de clave temporal) adicional para permitir la rotación de las claves y el fortalecimiento de la encriptación	El AES (Estándar de encriptación avanzada) no causa ninguna pérdida de rendimiento

Wired Equivalent Privacy, (Privacidad equivalente a la del cable), WEP

La WEP (Wired Equivalent Privacy, privacidad equivalente a la del cable) es un protocolo común que añade seguridad a todos los productos inalámbricos compatibles con Wi-Fi. La WEP ha sido diseñada para aportar a las redes inalámbricas un nivel de protección de la privacidad equivalente al de una red por cable.

WEP de 64 bits

WEP de 64 bits se introdujo en un principio con encriptación de 64 bits, que incluye una longitud de clave de 40 bits más 24 bits adicionales de datos generados por el sistema (64 bits en total). Algunos fabricantes de hardware llaman encriptación de 40 bits a la encriptación de 64 bits. Poco después de que se introdujese esta tecnología, los investigadores descubrieron que la encriptación de 64 bits era demasiado fácil de decodificar.

WEP de 128 bits

Como resultado de una debilidad potencial en la seguridad WEP de 64 bits, se creó un método más seguro de encriptación de 128 bits. La encriptación de 128 bits incluye una longitud de clave de 104 bits, más 24 bits adicionales de datos generados por el sistema (128 bits en total). Algunos fabricantes de hardware llaman encriptación de 104 bits a la encriptación de 128 bits. La mayoría de equipos inalámbricos actualmente en el mercado es compatible con la encriptación WEP tanto de 64 bits como de 128 bits, pero es posible que usted disponga de equipos más antiguos que sólo sean compatibles con la encriptación WEP de 64 bits. Todos los productos inalámbricos de Belkin son válidos para la WEP de 64 bits y de 128 bits.

Claves de encriptación

Después de seleccionar el modo de encriptación WEP de 64 bits o de 128 bits, es esencial generar una clave de encriptación. Si la clave de encriptación no es igual para el conjunto de la red inalámbrica, sus dispositivos de interconexión en red inalámbrica no podrán comunicarse entre sí dentro de su red y usted no podrá comunicarse con éxito dentro de la misma. Puede introducir su clave hexadecimal de forma manual, o introducir una frase de paso en el campo "Passphrase" (frase de paso) y hacer clic en "Generate" (generar) para crear una clave. Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9. Para WEP de 64 bits deberá introducir 10 claves hexadecimales. Para WEP de 128 bits, deberá introducir 26 claves hexadecimales.

Por ejemplo:

AF 0F 4B C3 D4 = clave WEP de 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clave WEP de 128 bits

La frase de paso WEP NO es lo mismo que la clave WEP. Su tarjeta inalámbrica utiliza esta contraseña para generar sus claves WEP, pero es posible que los diferentes fabricantes de hardware dispongan de diferentes métodos para generar las claves. Si cuenta en su red con equipos de diferentes vendedores, lo más sencillo será utilizar la clave WEP hexadecimal de su router o punto de acceso e introducirla manualmente en la tabla de claves WEP hexadecimales de la pantalla de configuración de su tarjeta.

Acceso protegido Wi-Fi (WPA)

El WPA (Wi-Fi Protected Access, Acceso Wi-Fi protegido) es un nuevo estándar Wi-Fi que mejora las propiedades de seguridad de la WEP. Para utilizar la seguridad WPA, los controladores y el software de su equipo inalámbrico deben actualizarse para que sean compatibles con WPA. Estas actualizaciones se encontrarán en la página web del vendedor de su equipo inalámbrico. Existen dos tipos de seguridad WPA: WPA-PSK (sin servidor) y WPA (con servidor Radius 802.1x).

Configuración de WPA-PSK (sin servidor)

Este método emplea como clave de red lo que se conoce como “clave precompartida”. Una clave de red es una contraseña que contiene entre ocho y 63 caracteres. Se compone de una combinación de letras, números o caracteres. Todos los clientes utilizan la misma clave de red para acceder a la red. Normalmente, éste es el modo que se utilizará en un entorno de hogar.

WPA (con servidor Radius 802.1x)

Con este sistema, un servidor Radius distribuye la clave de red automáticamente a los clientes. Esto está vinculado habitualmente a un entorno empresarial.

WPA2

El router incorpora WPA2, la segunda generación de WPA, basada en el estándar 802.11i. Ofrece un nivel más alto de seguridad inalámbrico ya que combina una autenticación de red avanzada con métodos de encriptación AES más sólidos.

Requisitos para WPA2

IMPORTANTE: Para utilizar la seguridad WPA2, todos sus ordenadores y clientes inalámbricos deberán haber actualizado los parches, drivers y software que son compatibles con WPA. En el momento de la publicación de este manual, se puede descargar, de forma gratuita, una serie de parches de seguridad de Microsoft®. Estos parches sólo funcionan con el sistema operativo Windows XP. En la actualidad no existe soporte para otros sistemas operativos.

Si tiene un ordenador con Windows XP que no tiene el Service Pack 2 (SP2), puede descargar un archivo de Microsoft llamado “Windows XP Support Patch for Wireless Protected Access (KB 826942)” que está disponible en <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91>

Para Windows XP con Service Pack 2, Microsoft ofrece una descarga gratuita para actualizar los clientes inalámbricos de modo que éstos puedan soportar WPA2 (KB893357). Puede descargar la actualización de: <http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en>.

IMPORTANTE: Debe también asegurarse de que todas las tarjetas o adaptadores inalámbricos de los clientes admitan WPA2 y de haber descargado e instalado el controlador más reciente. La mayoría de las tarjetas inalámbricas de Belkin tienen drivers actualizados que puede descargarse de la página de soporte de Belkin: www.belkin.com/networking Para obtener una lista de los productos inalámbricos de Belkin que son compatibles con WPA/WPA2, visite nuestro sitio web www.belkin.com/networking.

Compartir las mismas claves de red

La mayoría de productos Wi-Fi se suministran con la seguridad desconectada. Por esta razón, una vez que haya puesto en funcionamiento su red, deberá activar las opciones de seguridad WEP o WPA y asegurarse de que todos sus dispositivos de red inalámbrica compartan la misma clave de red.

Cómo utilizar una clave hexadecimal

Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9. Las claves de 64 bits son cinco cifras de 2 dígitos. Las claves de 128 bits son 13 cifras de 2 dígitos.

Por ejemplo:

AF 0F 4B C3 D4 = clave de 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clave de 128 bits

En las casillas que se muestran a continuación, introduzca la clave en dos caracteres entre A–F y 0–9 en cada casilla. Utilizará esta clave para programar los ajustes de encriptación en su router y en sus ordenadores inalámbricos.

Nota para los usuarios de Mac: Los productos originales Apple® AirPort® admiten exclusivamente la encriptación de 64 bits. Los productos Apple AirPort 2 soportan la encriptación de 64 o de 128 bits. Compruebe qué versión del producto está utilizando. Si no puede configurar su red con una encriptación de 128 bits, pruebe con una encriptación de 64 bits.

Configuración WEP

1. Seleccione “WEP” del menú desplegable.
2. Seleccione el modo WEP (“WEP Mode”) de 64 ó 128 bits.
3. Después de seleccionar su modo WEP, podrá introducir su clave tecleando la clave hexadecimal manualmente.

Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9.

Para WEP de 64 bits deberá introducir 10 claves hexadecimales. Para WEP de 128 bits, deberá introducir 26 claves hexadecimales.

Por ejemplo:

AF 0F 4B C3 D4 = clave de 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clave de 128 bits

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. Home > Info

Allowed Client Type >	<input checked="" type="checkbox"/> WEP
WEP Mode >	<input checked="" type="radio"/> 64 bit <input type="radio"/> 128 bit
Key Entry Method >	<input type="radio"/> HEX <input checked="" type="radio"/> ASCII
Key Provisioning >	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Key 1 >	<input type="text"/>
Key 2 >	<input type="text"/>
Key 3 >	<input type="text"/>
Key 4 >	<input type="text"/>
Default Key ID >	<input type="text" value="1"/>
Passphrase >	<input type="text"/>

-
-
3. Haga clic en “Apply Changes” (Aplicar cambios) para finalizar. Ahora está establecida la encriptación en el router. Cada ordenador de su red inalámbrica deberá ser configurado ahora con los mismos ajustes de seguridad.

ADVERTENCIA: Si está configurando el router inalámbrico desde un ordenador con un cliente inalámbrico, necesitará asegurarse de que la seguridad esté activada para este cliente inalámbrico. De lo contrario, perderá su conexión inalámbrica.

Modificación de los ajustes de encriptación inalámbrica

Su router está equipado con WPA/WPA2, el estándar de seguridad inalámbrica más moderno. También es compatible con el estándar de seguridad WEP. Por defecto, la seguridad inalámbrica está desactivada. Para activar la seguridad, primero deberá determinar qué estándar desea utilizar. Para acceder a los ajustes de seguridad, haga clic en “Security” (Seguridad) en la pestaña “Wireless “ (Inalámbrico).

Configuración WPA

Nota: Para utilizar la seguridad WPA, todos sus clientes deberán haber actualizado los controladores y el software que son compatibles con WPA. Al momento de la publicación de este manual, se puede descargar de Microsoft un parche de seguridad gratuito. Este parche sólo funciona con el sistema operativo Windows XP. Asimismo, deberá descargar el driver más actualizado para su tarjeta de red inalámbrica G para ordenador de sobremesa o para notebook de Belkin desde la página de servicio de atención al cliente de Belkin. En la actualidad no existe soporte para otros sistemas operativos. El parche de Microsoft sólo es compatible con dispositivos con controladores preparados para WPA, como los productos 802.11g de Belkin.

Existen dos tipos de seguridad WPA: WPA-PSK (sin servidor) y WPA (con servidor Radius). WPA-PSK (sin servidor) emplea como clave de seguridad lo que se conoce como una “clave precompartida” (PSK). Una clave precompartida es una contraseña de entre 63 y 40 caracteres de largo. Se compone de cualquier combinación de letras, números y otros caracteres. Todos los clientes emplean la misma clave para acceder a la red. Normalmente, este modo se utilizará en un entorno de hogar. El WPA (con servidor Radius) es una configuración en la que un servidor Radius distribuye las claves a los clientes de forma automática. Esto se emplea habitualmente en un entorno empresarial. WPA2 es la segunda generación de WPA y ofrece una técnica de encriptación más avanzada que WPA.

Configuración de WPA-PSK (sin servidor)

1. Desde el menú desplegable “Allowed Client Type” (Tipo de cliente permitido), seleccione “WPA/WPA2”.
2. Para la autenticación, seleccione “Pre-shared Key” (Clave precompartida) para el uso en el hogar / pequeña empresa. Este ajuste deberá ser idéntico en todos los clientes que instale.
3. Introduzca su clave precompartida. Puede estar compuesta por entre ocho y 63 caracteres entre letras, números y símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale. Por ejemplo, su clave precompartida podría ser algo así como: “Clave de red familia Pérez”.

Configuración manual del router

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >

Authentication > 802.1X Pre-shared Key

Pre-shared Key >

4. Haga clic en “Apply Changes” (Aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Configuración de los ajustes WPA/WPA2 (con servidor Radius)

Si su red emplea un servidor Radius para distribuir las claves a los clientes, utilice este ajuste.

1. Desde el menú desplegable “Allowed Client Type” (Tipo de cliente permitido), seleccione “WPA/WPA2”.
2. Para la técnica de encriptación, seleccione “802.1x” para un entorno con servidor RADIUS. Este ajuste deberá ser idéntico en todos los clientes que instale.
3. Ingrese el tiempo límite para la detención de la sesión del servidor radius en el campo “Session Idle Timeout”.
4. Ingrese el intervalo de clave, la frecuencia con que se distribuyen las claves (en paquetes), en el campo “Re-Authentication Period” (Intervalo de re-autenticación).
5. Introduzca el tiempo de espera después de una autenticación fallida en el campo “Quiet Period” (Intervalo de espera)
6. Introduzca la dirección IP del servidor Radius en los campos “Server-IP” (Servidor IP) y “Server-Port” (Puerto de servidor).
7. Introduzca la clave radius en el campo “Secret Key” (clave secreta).
8. Haga clic en “Apply Changes” (Aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Nota: Asegúrese de actualizar sus ordenadores inalámbricos con el modo WPA2 y de haber establecido los ajustes correctos para poder establecer una conexión adecuada con el router.

Configuración de sus tarjetas de red inalámbrica G de Belkin para emplear la seguridad

Nota: Esta sección le proporcionará información acerca de cómo configurar sus tarjetas de red inalámbrica G de Belkin para emplear seguridad. En este momento, ya debe tener su router inalámbrico o punto de acceso configurado para utilizar WPA o WEP. Para

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	WPA/WPA2 ▾
Authentication >	<input checked="" type="radio"/> 802.1X <input type="radio"/> Pre-shared Key
Session Idle Timeout >	<input type="text" value="300"/> Seconds (0 for no timeout checking)
Re-Authentication Period >	<input type="text" value="3600"/> Seconds (0 for no re-authentication)
Quiet Period >	<input type="text" value="60"/> Seconds after authentication failed
Server-IP >	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="2"/> . <input type="text" value="1"/>
Server-Port >	<input type="text" value="1812"/>
Secret Key >	<input type="text"/>
NAS-ID >	<input type="text"/>

obtener una conexión inalámbrica, necesitará configurar su tarjeta inalámbrica para ordenador portátil y su tarjeta inalámbrica para ordenador de sobremesa de tal manera que utilicen las mismas configuraciones de seguridad.

Conexión de su ordenador a una red inalámbrica que requiera una clave WEP de 64 bits o de 128 bits:

1. Haga doble clic sobre este icono de “Indicador de señal” para abrir la ventana “Wireless Network” (Red inalámbrica). El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta inalámbrica.
2. En la pestaña “Wireless Networks Properties” (propiedades de las redes inalámbricas), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
3. En la categoría “Data Encryption” (Encriptación de datos), seleccione “WEP”.
4. Asegúrese de que la casilla de verificación “Network key is provided for me automatically” (La clave de red me es proporcionada automáticamente), que se encuentra en la parte inferior, no esté marcada. Si está utilizando este ordenador para conectarse a la red de una empresa, consulte con su administrador de red si es necesario marcar esta casilla.
5. Introduzca su clave WEP en el recuadro “Network key” (Clave de red).

1

2

3

4

5

6

7

8

9

10

11

Wireless > Security

Security Mode

Key 1

Key 2

Key 3

Key 4

(hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, input it here

PassPhrase

Importante: Una clave WEP es una mezcla de números y letras de la A a la F y del 0 al 9. Para WEP de 128 bits, deberá introducir 26 claves. Para WEP de 64 bits, deberá introducir 10 claves. Esta clave de red deberá coincidir con la clave que haya asignado a su router.

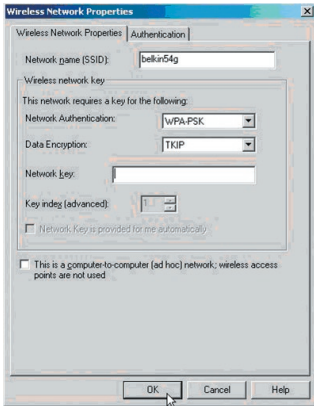
6. Haga clic en “OK” (Aceptar) para guardar los ajustes.

Conexión de su ordenador a una red inalámbrica que requiera WPA-PSK (sin servidor)

1. Haga doble clic sobre este icono de “Indicador de señal” para abrir la ventana “Wireless Network” (Red inalámbrica). El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta inalámbrica.
2. En la pestaña “Wireless Networks” (redes inalámbricas), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
3. En “Network Authentication” (Autenticación de red) seleccione “WPA-PSK (No Server)” (WPA-PSK [sin servidor]).
4. Introduzca su clave WPA en el recuadro “Network key” (Clave de red).

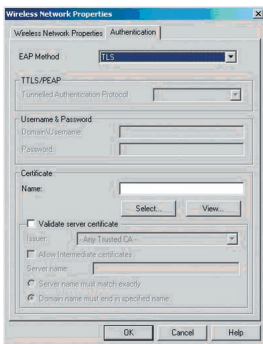
Importante: WPA-PSK es una combinación de números y letras de la A a la Z y del 0 al 9. Para WPA-PSK, puede introducir de ocho a 63 claves. Esta clave de red deberá coincidir con la clave que haya asignado a su router.

5. Haga clic en “OK” (Aceptar) para guardar los ajustes.



Conexión de su ordenador a una red inalámbrica que requiera WPA (con servidor Radius)

1. Haga doble clic sobre este icono de “Indicador de señal” para abrir la ventana “Wireless Network” (Red inalámbrica). El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta inalámbrica.
2. En la pestaña “Wireless Networks” (redes inalámbricas), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
3. En “Network Authentication” (Autenticación de red) seleccione “WPA”.
4. En la pestaña “Authentication” (Autenticación), seleccione las configuraciones indicadas por su administrador de red.
5. Haga clic en “OK” (Aceptar) para guardar los ajustes.



Configuración de WPA para tarjetas de red para ordenador de sobremesa y notebook que NO fueron fabricadas por Belkin.

En el caso de las tarjetas inalámbricas WPA para ordenador de sobremesa y notebook que NO han sido fabricadas por Belkin y que no están equipadas con un software compatible con WPA, se puede descargar de forma gratuita un archivo de Microsoft llamado “Windows XP Support Patch for Wireless Protected Access” (Actualización de Soporte Windows XP para Acceso Inalámbrico Protegido).

Nota: El archivo que Microsoft pone a su disposición sólo funciona con Windows XP. En la actualidad no existe soporte para otros sistemas operativos.

Importante: Asimismo, deberá asegurarse de que el fabricante de la tarjeta inalámbrica soporte WPA y de haber descargado e instalado el driver más actualizado de su página de asistencia.

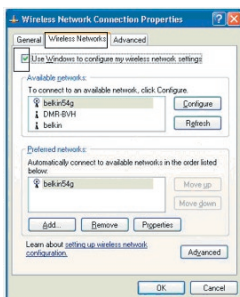
Sistemas operativos soportados:

- Windows XP Professional
- Windows XP Home Edition

Configuración de la utilidad de red inalámbrica de Windows XP para emplear WPA-PSK

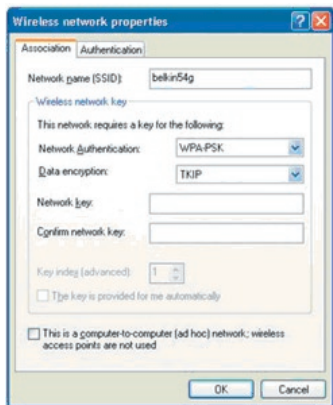
Para utilizar WPA-PSK, asegúrese de que está utilizando la Utilidad de Red Inalámbrica de Windows. Para ello, debe seguir los siguientes pasos:

1. En Windows XP, haga clic sobre “Start > Control Panel > Network Connections” (Inicio > Panel de Control > Conexiones de Red).
2. Haga clic con el botón derecho del ratón sobre “Wireless Network Connection” (Conexión de red inalámbrica) y seleccione “Properties” (Propiedades).
3. Al hacer clic en la pestaña “Wireless Networks” (Redes inalámbricas) aparecerá la siguiente pantalla. Compruebe que esté marcada la casilla “Use Windows to configure my wireless network settings” (Utilizar Windows para configurar mis configuraciones de red inalámbrica)



4. En la pestaña “Wireless Networks” (Redes inalámbricas), haga clic sobre el botón “Configure” (Configurar) y aparecerá la siguiente pantalla.

5. Para usuarios de hogar u oficina pequeña, seleccione “WPA-PSK” en “Network Authentication” (Autenticación de red).



Nota: Seleccione WPA si está utilizando este ordenador para conectarse a una red corporativa que soporte un servidor de autenticación como el servidor Radius. Consulte a su administrador de red para obtener más información.

6. Para la encriptación de datos (“Data Encryption”), seleccione “TKIP” o “AES”. Esta configuración tendrá que ser idéntica a la del router.

7. Introduzca su clave de encriptación en la casilla “Network key” (Clave de red).

Importante: Introduzca su clave precompartida. Puede estar compuesta por entre ocho y 63 caracteres entre letras, números y símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale.

8. Haga clic en “OK” (Aceptar) para aplicar los ajustes.

Extensión del alcance inalámbrico y puenteo inalámbrico

¿Qué es un puente inalámbrico?

Un puente inalámbrico es un modo de funcionamiento para ampliar el alcance de su red inalámbrica o para agregar una extensión de su red en otra área de su hogar u oficina sin necesidad de cables.

Nota: No podemos garantizar que esta función será compatible con el hardware de otros fabricantes de dispositivos inalámbricos.

Nota: Asegúrese de descargar la versión más actualizada de firmware para el router con el fin de lograr el máximo rendimiento: <http://web.belkin.com/support>.

1

2

3

4

5

6

7

8

9

10

11

Cómo añadir otro segmento de red de modo inalámbrico

La conexión de un conmutador de red o hub a la toma RJ45 del router permitirá que varios ordenadores conectados al conmutador accedan al resto de la red.

Configuración de un puente entre su router y un punto de acceso secundario

El puenteo entre su router de Belkin y un punto de acceso secundario requiere el acceso a la utilidad de configuración avanzada del router y la introducción de la dirección MAC del punto de acceso en el lugar apropiado. Existen además otra serie de requisitos.

ASEGÚRESE DE REALIZAR LOS SIGUIENTES PASOS CON TODA ATENCIÓN.

1. Establezca para su punto de acceso el mismo canal que el router. Para obtener más información acerca del cambio de canales, vea la sección “Canal inalámbrico y SSID” del presente manual.
2. Busque la dirección MAC del punto de acceso en la parte inferior del punto de acceso. Existen dos direcciones MAC en la etiqueta de la parte inferior. Usted precisa la dirección MAC llamada “WLAN MAC Address” (Dirección MAC de WLAN). La dirección MAC comienza por “0030BD” y va seguida por otros seis números o letras (p. ej.: 0030BD-XXXXXX). Escriba la dirección MAC a continuación. Vaya al siguiente paso.
3. Coloque su punto de acceso secundario en el margen de alcance de su router y cerca del área en la que desee ampliar el alcance o añadir una red. Normalmente, el alcance en interior deberá ser de entre 30 y 60 metros.
4. Conecte su punto de acceso a la alimentación eléctrica. Asegúrese de que el punto de acceso se encuentre encendido y proceda con el siguiente paso.
5. Desde un ordenador ya conectado a su router, acceda a la Utilidad de Configuración avanzada abriendo su navegador. En la barra de direcciones, escriba “192.168.2.1”. No introduzca “www” ni “http://” delante del número. Nota: Si ha modificado la dirección IP de su router, utilice dicha dirección IP.

Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

1) **Enable Wireless Bridging.** (enabling this feature allows other Access Points to connect to this Access Point.)

2) **Enable ONLY specific Access Points to connect.** (enter Wireless MAC address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Hint: the MAC address can be found using a site survey on a wireless client card.)

3) **Disable ability for Wireless CLIENT to connect.** (This feature should only be used when the AP is used exclusively to other APs.)

AP1

AP2

AP3

AP4

6. La interfaz de usuario del router aparecerá en la ventana del navegador. Haga clic en “Wireless Bridge” (Puente inalámbrico) (2) en la parte izquierda de la pantalla. Aparecerá la siguiente pantalla.
7. Marque la casilla de “Enable ONLY specific Access Points to connect” (Permitir SÓLO la conexión de Puntos de Acceso específicos). (1)
8. En el campo llamado “AP1” (Punto de Acceso 1) (3), escriba la dirección MAC de su punto de acceso secundario. Una vez introducida la dirección, haga clic en “Apply Changes” (Aplicar cambios).
9. El puenteo ha sido configurado.

Nota: Puede ser que tarde hasta un minuto hasta que la conexión de puenteo se termine de establecer. En algunos casos puede ser necesario reiniciar el punto de acceso y el router para iniciar el puente.

Firewall

Su router se encuentra equipado con un firewall que protegerá su red de una amplia gama de ataques habituales de piratas informáticos, incluyendo:

- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP con longitud cero
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

El firewall también protege puertos comunes que son empleados con frecuencia para atacar redes. Estos puertos aparecen como “Stealth” (Invisibles), lo que significa principalmente que estos puertos no existen ante un posible pirata informático. Si lo necesita, puede apagar la función de firewall; sin embargo, se recomienda dejar el firewall activado. Si desactiva la protección por firewall, no dejará su red completamente vulnerable a los ataques de los piratas, pero es recomendable dejar activado el firewall.

Firewall >

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable / Disable > Enable Disable

Clear Changes

Apply Changes

Servidores virtuales

Los servidores virtuales le permiten enrutar llamadas externas (Internet) para servicios como servidor web (puerto 80), servidor FTP (puerto 21) y otras aplicaciones a través de su router hasta su red interna. Gracias a que sus ordenadores internos están protegidos por un firewall, las máquinas fuera de su red (a través de Internet) no pueden acceder a ellos, ya que no pueden ser “detectados”. Si necesita configurar el servidor virtual para una aplicación específica, será preciso que se ponga en contacto con el fabricante de la aplicación para descubrir los ajustes de los puertos precisos. Puede introducir manualmente esta información del puerto en el router.

Firewall > Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (port 21), or other applications through your Router to your internal network. [View Info](#)

No.	List of Address	Description	Protocol Type	Lan Port	Public Port	Status	Action
1	170.148.0		TCP			On	Clear
2	170.148.0		TCP			On	Clear
3	170.148.0		TCP			On	Clear

Selección de una aplicación

Seleccione su aplicación de la lista desplegable. Haga clic sobre “Add” (Añadir). Los ajustes serán transferidos al siguiente espacio disponible en la pantalla. Haga clic en “Apply Changes” (Aplicar cambios) para guardar el ajuste para esta aplicación. Para eliminar una aplicación, seleccione el número de la fila que desea eliminar y haga clic en “Clear” (Borrar).

Introducción manual de los ajustes en el Servidor Virtual

Para introducir las configuraciones de forma manual, introduzca la dirección IP en el espacio provisto para la máquina interna (servidor) y el puerto o los puertos necesarios para pasar, seleccione el tipo de puerto (TCP o UDP) y luego haga clic sobre “Apply Changes” (Aplicar Cambios). Cada celda de puerto de entrada tiene dos campos con cinco caracteres máximo por campo que permite determinar un alcance entre un puerto mínimo y un puerto máximo, por ejemplo; [xxxxx]-[xxxxx]. En cada celda, puede introducir un valor de puerto único completando los dos campos con el mismo valor (por ejemplo; [7500]-[7500]) o un alcance amplio de puertos (por ejemplo; [7500]-[9000]). Si necesita múltiples valores de puerto único o una combinación de alcances y un valor único, debe utilizar entradas múltiples hasta un máximo de 20 entradas (por ejemplo; 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). Únicamente podrá pasar por un puerto por cada dirección IP interna. Abrir los puertos de su firewall puede representar un riesgo para la seguridad. Puede activar y desactivar los ajustes de forma rápida. Se recomienda desactivar las configuraciones cuando no esté utilizando una aplicación específica.

Filtros para IP de clientes

El Router puede ser configurado para restringir el acceso a Internet, al e-mail o a otros servicios de red en determinados días y horas. Puede establecerse una restricción para un ordenador, un nivel de ordenadores o varios ordenadores.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

Access Control allows users to define the traffic type permitted or not-permitted to WAN port services. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function > Enable Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

> Add PC

Apply Changes

Control de acceso

El control de acceso permite a los usuarios definir el tipo de tráfico que será permitido o negado al pasar por la interfaz WAN. Por defecto, todo tráfico está permitido. Para establecer un acceso restringido para sus ordenadores, siga las siguientes instrucciones:

Firewall > Client IP Filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address > -

> Client PC Services:

Service Name	Default Description	Blocking
WWW	HTTP, TCP Port 80, SSL, HTTPS, WWW, WWW	<input checked="" type="checkbox"/>
WWW with URL Blocking	HTTP, WWW, HTTPS, WWW (See Page)	<input checked="" type="checkbox"/>
Client Blocking	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Service	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Blocking	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Service	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Blocking	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Service	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Blocking	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Service	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Blocking	HTTP, TCP Port 80	<input checked="" type="checkbox"/>
Client Service	HTTP, TCP Port 80	<input checked="" type="checkbox"/>

1. Haga clic en "Add PC" (Añadir PC) en la pantalla "Access Control" (Control de acceso).
2. Defina los ajustes apropiados para los servicios de los PC clientes (como se indica en la siguiente pantalla).
3. Haga clic en "OK" y después "Apply Changes" (Aplicar cambios) para guardas los ajustes.

Bloqueo de URL

Para configurar la función de bloqueo de URL, especifique las páginas-web o palabras clave que desea filtrar en su red. Haga clic en "Apply Changes" (Aplicar cambios) para guardar el cambio. Para completar esta configuración, deberá crear o modificar una norma de acceso en la sección de filtros IP del cliente. Para modificar una norma existente, haga clic en "Edit" junto a la norma que desea modificar. Para crear una norma nueva, haga clic en "Add PC" (Añadir PC). En la sección "Access Control Add PC" (Control de acceso, añadir PC), seleccione la opción "WWW with URL Blocking" (WWW con bloqueo de URL) en la tabla "Client PC Service" para filtrar las páginas-web y palabras clave especificadas.

Configuración manual del router

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

To configure the URL Blocking feature, use the table below to specify the websites ([www.somewhere.com](#)) and or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section. To modify an existing rule, click the "Edit" option next to the rule you want to modify. To create a new rule, click on the "Add PC" option.

From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below...

Rule Number	URL / Keyword
504_1	
504_2	
504_3	
504_4	
504_5	

Regla de horario

Es posible filtrar el acceso a páginas de Internet para los clientes de manera basada en una regla. Todas las reglas de control de acceso pueden activarse a una hora programada. Defina el programa o "Schedule Rule" (Programar norma) y aplique la norma en la página "Access Control" (Control de acceso)

Siga los siguientes pasos para añadir una norma:

1. Haga clic en "Add Schedule Rule" (Añadir norma).
2. Aparecerá la siguiente pantalla.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Rule Name	Rule Comment	Configure
Add Schedule Rule		

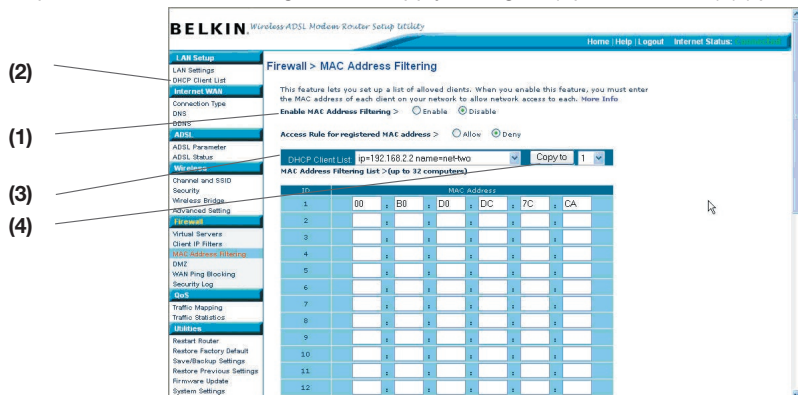
[Clear Changes](#) [Apply Changes](#)

3. Para programar una norma, especifique el nombre, un comentario, hora de comienzo y fin del filtro que desea activar en su red.
4. Haga clic en "OK" y después "Apply Changes" (Aplicar cambios) para guardas los ajustes.
5. Para completar esta configuración, deberá crear o modificar una norma de acceso en la sección de filtros IP del cliente. Así se activará la norma que será utilizada en la página "Access Control" (Control de acceso).

Configuración del filtrado de direcciones MAC

El filtro de direcciones MAC es una potente característica de seguridad que le permite especificar qué ordenadores están permitidos en la red. Cualquier ordenador que trate de acceder a la red y no esté especificado en la lista de filtros no obtendrá permiso para acceder. Cuando active esta propiedad, deberá introducir la dirección MAC de cada cliente (ordenador) de su red para permitir el acceso a la misma de cada uno de ellos. La característica “Block” (Bloquear) le permite encender y apagar el acceso a la red fácilmente para cualquier ordenador, sin tener que añadir y eliminar la dirección MAC del ordenador de la lista. Para activar esta característica, seleccione “Enable MAC Address Filtering” (Activar filtrado de direcciones MAC) (1). A continuación, seleccione para la norma de acceso la opción “Allow” (Permitir) o “Deny” (Negar).

Luego, ingrese la dirección MAC de cada ordenador que se encuentra en su red. Para ello, seleccione la dirección en el recuadro desplegable de clientes DHCP (2) y copie el ID que desea copiar a (3), luego presione “Copy to” (Copiar a). Como método alternativo, pinche sobre el espacio (4) [Designer (diseñador): consúltelo como referencia (4) en el pantallazo] e introduzca la dirección MAC del ordenador que quiera añadir a la lista. Haga clic en “Apply Changes” (Aplicar cambios) (5) para



guardar los ajustes. Haga clic en “Apply Changes” (Aplicar cambios) para guardar los ajustes.

Nota: No podrá borrar la dirección MAC del ordenador que está utilizando para acceder a las funciones administrativas del router (el ordenador que está utilizando ahora mismo).

DMZ (Zona desmilitarizada)

Si uno de los clientes conectados no puede ejecutar una aplicación de Internet correctamente debido al firewall, podrá establecer un acceso a Internet no restringido en ambas direcciones para dicho ordenador. Esto puede ser necesario en el caso de que la propiedad NAT esté causando problemas con una aplicación como, por ejemplo, una aplicación de juegos o de videoconferencia.

Configuración manual del router

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** [More Info](#)

DMZ > ENABLE DISABLE

> IP Address of Virtual DMZ Host

Static IP	Static IP
1	192.168.2.0
2	192.168.2.0
3	192.168.2.0
4	192.168.2.0
5	192.168.2.0
6	192.168.2.0
7	192.168.2.0
8	192.168.2.0

Utilice esta característica de forma temporal. El ordenador que se encuentra en la DMZ no está protegido contra los ataques de piratas informáticos.

Para situar un ordenador en la DMZ, introduzca los dígitos finales de su dirección IP en el campo IP y seleccione “Enable” (Activar). Haga clic en “Apply Changes” (Aplicar cambios) para que los cambios tengan efecto. Si está utilizando múltiples direcciones IP estáticas de WAN, será posible seleccionar a qué dirección IP de WAN será dirigido el host de DMZ. Introduzca la dirección IP de WAN a la que desee dirigir el host de DMZ, introduzca los dos últimos dígitos de la dirección IP del ordenador host de DMZ, seleccione “Enable” (Activar) y haga clic en “Apply Changes” (Aplicar cambios).

Bloqueo de un ICMP Ping

Los piratas informáticos utilizan lo que se conoce como “pinging” (revisar



(1)

actividad) para encontrar posibles víctimas en Internet. Al revisar la actividad de una dirección IP específica y recibir una respuesta de la dirección IP, el pirata informático puede determinar si hay allí algo de interés. El router puede ser configurado de forma que no responda a un ICMP ping proveniente del exterior. Esto eleva el nivel de seguridad de su router.

Para apagar la respuesta al ping, seleccione “Block ICMP” (Bloquear ICMP) (1) y haga clic en “Apply Changes” (Aplicar cambios). El router no responderá a ningún ICMP ping.

Utilidades

La pantalla de “Utilities” (Utilidades) le permite gestionar diferentes parámetros del Router y llevar a cabo determinadas funciones administrativas.

Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Restart Router**
Sometimes it may be necessary to Restart or Reboot the Router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Defaults**
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Current Settings**
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Saved Settings**
This option will allow you to restore a previously saved configuration.
- **Firmware Update**
When the firmware update begins may release new versions of the Router's firmware. Firmware updates can make feature improvements and fixes to problems that may have existed.
- **System Settings**
The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the hot features of the Router.

Reiniciar el router

Algunas veces es posible que sea necesario reiniciar el router en caso de que comience a funcionar mal. Al reiniciar el router NO se borrará ninguno de sus

Utilities > Restart Router

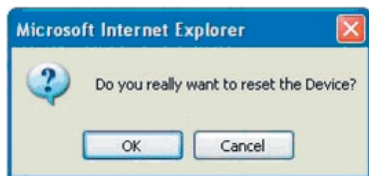
Sometimes it may be necessary to Restart or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.

Restart Router

ajustes de configuración.

Reinicio del router para restablecer el funcionamiento normal

1. Haga clic en el botón “Restart Router” (Reiniciar router).
2. Aparecerá el siguiente mensaje. Haga clic en “Yes” (Sí) para reiniciar su router.



Restablecer las configuraciones por defecto de fábrica

El empleo de esta opción restablecerá los ajustes (predeterminados) de fábrica del router. Se recomienda que realice una copia de seguridad de sus ajustes antes de restablecer todos los ajustes por defecto.

Utilities > Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.

Restore Defaults

1. Haga clic en el botón “Restore Defaults” (Restablecer ajustes predeterminados).
2. Aparecerá el siguiente mensaje. Haga clic en “OK” (Aceptar) para restablecer las configuraciones por defecto de fábrica.



Guardar/Hacer copia de seguridad de los ajustes actuales

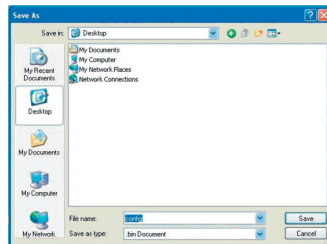
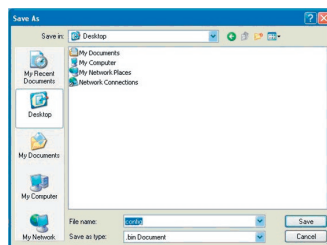
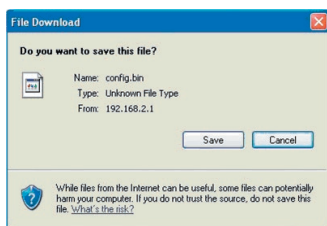
Puede guardar su configuración actual utilizando esta función. Guardar su configuración le permitirá restablecerla posteriormente en caso de que sus ajustes se pierdan o se modifiquen. Se recomienda realizar una copia de seguridad de su configuración actual antes de llevar a cabo una actualización del firmware.

1. Haga clic en “Save” (Guardar). Se abrirá una ventana llamada “File Download” (Descarga de archivos). Haga clic en “Save” (Guardar).
2. Se abrirá una ventana que le permitirá seleccionar la ubicación en la que desea guardar el archivo de configuración. Seleccione una ubicación. No existen restricciones con respecto al nombre del archivo. Sin embargo, asegúrese de dar un nombre al archivo que le permita encontrarlo más tarde. Cuando haya ingresado la ubicación y el nombre del archivo, haga clic en “Save” (Guardar).
3. Cuando el proceso de almacenamiento se haya completado, verá la siguiente ventana. Haga clic en “Close” (Cerrar). La configuración ha sido guardada.

UTILITIES > Save/Backup current settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

Save



“Restore Previous Settings” (Restablecer ajustes anteriores)

Esta opción le permitirá restablecer una configuración guardada anteriormente.

Utilities > Restore Previous Settings

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the “Restore” button below.



1. Haga clic en “Browse” (Examinar). Se abrirá una ventana que le permitirá seleccionar la ubicación del archivo de configuración. Localice el archivo de configuración “config.bin” y haga doble clic sobre él.

2. Haga clic en “Open”. (Abrir).

Actualización del Firmware

Cada cierto tiempo, Belkin publica nuevas versiones del firmware del Router. Las actualizaciones del firmware contienen mejoras de las propiedades y soluciones para los problemas que puedan haber existido. Cuando Belkin publique un nuevo firmware, usted podrá descargarlo de la página web de actualizaciones de Belkin con el fin de instalar la versión más actualizada del firmware de su router.

Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click here to go to the Save/Backup current settings page.](#)



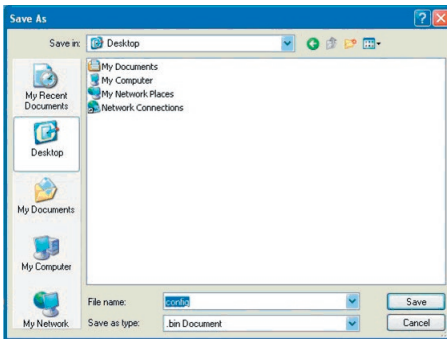
Búsqueda de una nueva versión del Firmware

El botón “Check Firmware” (comprobar firmware) (1) [Designer (diseñador): consúltelo como referencia (1) en el pantallazo] le permite buscar al momento una nueva versión de firmware. Al hacer clic en el botón, aparecerá una nueva ventana de navegador informándole bien de que no existe ningún firmware más moderno que el suyo, o bien que existe una nueva versión disponible. Si está disponible una nueva versión, dispondrá de la opción de descargarla.

Descarga de una nueva versión del firmware

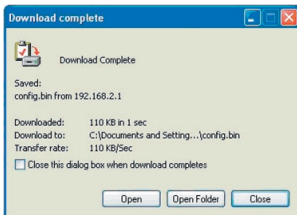
Si hace clic en el botón “Check Firmware” (Búsqueda de firmware) y aparece una nueva versión disponible, aparecerá una ventana como la siguiente.

1. Para descargar la nueva versión del firmware, haga clic en “Download” (Descargar).
2. Se abrirá una ventana que le permitirá seleccionar la ubicación en la que desea guardar el archivo del firmware. Seleccione una ubicación. Puede dar al archivo el nombre que quiera o utilizar el nombre por defecto. Asegúrese de colocar el archivo en una ubicación en la que lo pueda encontrar fácilmente más tarde.



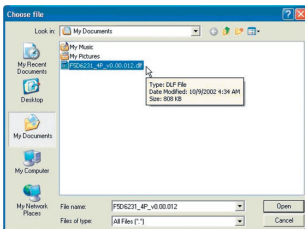
Cuando haya seleccionado la ubicación, haga clic en “Save” (Guardar).

3. Cuando el proceso de almacenamiento se haya completado, verá la siguiente ventana. Haga clic en “Close” (Cerrar). Ha finalizado la descarga del firmware. Para actualizar el firmware, siga los siguientes pasos en “Actualización del firmware del router”.



Actualización del firmware del router

1. En la ventana “Firmware Update” (Actualización del firmware), haga clic en “Browse” (Examinar) (2) Designer (diseñador): consúltelo como referencia (2) en el pantallazo). Se abrirá una ventana que le permitirá seleccionar la ubicación del archivo de actualización del firmware.

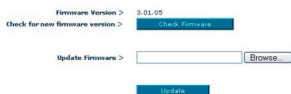


2. Diríjase a la ubicación del archivo de firmware que ha descargado. Seleccione el archivo haciendo doble clic en el nombre del mismo.
3. El recuadro “Update Firmware” (Actualizar firmware) mostrará ahora la ubicación y el nombre del archivo de firmware que acaba de seleccionar. Haga clic en “Update” (Actualizar).

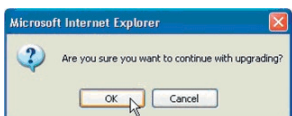
Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

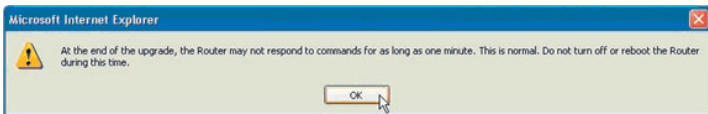
NOTE: Please backup your current settings before updating to a new version of firmware. [Click Here](#) to go to the Save/Backup current settings page.



4. Se le preguntará si está seguro de que desea continuar. Haga clic en “OK” (aceptar).



5. Verá un nuevo mensaje. Este mensaje le indica que es posible que el router no responda durante un minuto, ya que el firmware se carga en el router y éste se reinicia. Haga clic en “OK” (Aceptar).



Aparecerá en pantalla una cuenta atrás de 60 segundos. Cuando la cuenta atrás llegue a cero, la actualización del firmware del router habrá sido completada. La página principal del router deberá aparecer automáticamente. En caso contrario, introduzca la dirección del router (por defecto = 192.168.2.1) en la barra de direcciones de su navegador.

Ajustes del sistema

La página “System Settings” (Ajustes del sistema) es en donde podrá introducir una nueva contraseña de administrador, establecer la zona horaria, activar la gestión a distancia y encender y apagar la función UPnP del router.

Establecimiento o modificación de la contraseña del administrador

El router efectúa el envío SIN necesidad de introducir contraseña. Si desea añadir una contraseña para disfrutar de una mayor seguridad, puede establecerla aquí. Escriba su contraseña y guárdela en un lugar seguro, ya que la necesitará si precisa acceder al router en el futuro. Se recomienda asimismo que establezca una contraseña si prevé utilizar la opción de gestión a distancia de su router.

Modificación del tiempo límite de acceso

Utilities > System Settings

Administrator Password:

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

La opción de tiempo límite de acceso le permite establecer el periodo de tiempo que podrá permanecer en la interfaz de configuración avanzada del router. El temporizador arranca cuando no existe actividad. Por ejemplo, usted ha efectuado algunos cambios en la interfaz de configuración avanzada y después deja su ordenador solo sin hacer clic en “Logout” (Salir). Si suponemos que el tiempo límite es de 10 minutos, entonces 10 minutos después de que abandone el ordenador, la sesión se cerrará. Deberá acceder al router de nuevo para realizar más cambios. La opción del tiempo límite de acceso responde a razones de seguridad y la configuración por defecto es de 10 minutos. Nota: Solamente podrá acceder un ordenador cada vez a la interfaz de configuración avanzada del router.

Establecimiento de la hora y de la zona horaria

El router mantiene la hora conectándose a un servidor SNTP (Simple Network Time Protocol, protocolo horario de red simple). Esto permite al router sincronizar el reloj del sistema con el conjunto de Internet. El reloj sincronizado en el router se emplea para grabar el registro de seguridad y para controlar el filtrado de clientes. Seleccione el zona horaria en la que reside. Si reside en una zona donde se realiza el cambio de hora según el horario de verano, coloque una marca en el recuadro junto a “Daylight Savings” (cambiar la hora automáticamente según el horario de verano). Es posible que el reloj del sistema no se actualice inmediatamente. Espere al menos 15 minutos para que el router contacte con los servidores horarios de Internet y obtenga una respuesta. Usted no podrá configurar el reloj por sí mismo/a. Ahora puede seleccionar un servidor NTP primario y uno de respaldo para que el reloj de su router esté sincronizado con diferentes servidores NTP de Internet. Seleccione el servidor NTP que prefiera de la lista

proporcionada o mantenga el que está seleccionado.

Time and Time Zone: **August 1, 2003 4:26:00 AM**

Please set your time Zone. If you are in an area that observes daylight saving check this box. [More Info](#)

Daylight Savings

Set Time Zone > (GMT-08:00)Pacific Time (US & Canada): Tijuana

Configure Time Server (NTP) > Enable Automatic Time Server Maintenance

Primary Server > 132.163.4.102 - North America

Secondary server > 192.5.41.41 - North America

[Apply Changes](#)

Activación de la gestión a distancia

Antes de activar esta característica avanzada de su Router de Belkin, ASEGÚRESE DE QUE HA ESTABLECIDO LA CONTRASEÑA DE ADMINISTRADOR. La gestión a distancia le permite efectuar cambios en los ajustes de su router desde cualquier parte en Internet.

Existen dos métodos de gestionar el router a distancia. El primero consiste en permitir el acceso al router desde cualquier parte en Internet seleccionando la opción “Any IP address can remotely manage the Router” (cualquier dirección IP puede gestionar el router a distancia). Al introducir su dirección IP de WAN desde cualquier ordenador en Internet, aparecerá una ventana de acceso en la que deberá introducir la contraseña de su router. El segundo método consiste en permitir la gestión a distancia únicamente a una dirección IP específica. Este método es más seguro pero menos cómodo. Para utilizar este método, introduzca la dirección IP desde la que vaya a acceder al router en el espacio previsto y seleccione “Only this IP address can remotely manage the Router” (únicamente esta dirección IP puede gestionar el router a distancia).

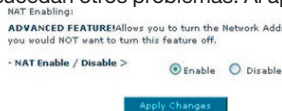
Antes de activar esta función, se RECOMIENDA ENCARECIDAMENTE que establezca su contraseña de administrador. Si deja la contraseña vacía, expondrá potencialmente su router a la intrusión externa. El puerto de acceso remoto se ajusta



por defecto al puerto 8080. Puede elegir un puerto diferente mediante la introducción de un nuevo número de puerto en el campo “remote port” (puerto remoto). Haga clic en “Apply Changes” (Aplicar cambios) para guardar los ajustes.

Activar/Desactivar NAT (Network Address Translation, Traducción de direcciones de red)

Nota: Esta característica avanzada deberá ser empleada exclusivamente por usuarios avanzados. Antes de activar esta función ASEGÚRESE DE HABER ESTABLECIDO LA CONTRASEÑA DEL ADMINISTRADOR. La traducción de direcciones de red (NAT) es el método en el que el Router comparte la única dirección IP asignada por su ISP con el resto de ordenadores de la red. Esta función deberá ser empleada únicamente si su ISP le asigna múltiples direcciones IP o si necesita desactivar NAT para una configuración avanzada del sistema. Si dispone de una sola dirección IP y desactiva NAT, los ordenadores de su red no podrán acceder a Internet. Es posible asimismo que sucedan otros problemas. Al apagar NAT se desactivarán las funciones de su firewall.



Activar/Desactivar el UPnP (Universal Plug-and-Play).

UPnP es otra prestación avanzada de su router. Es una tecnología que ofrece un funcionamiento perfecto de las opciones de mensajes de voz, mensajes de vídeo, juegos y otras aplicaciones compatibles con UPnP.

Para funcionar correctamente, algunas aplicaciones requieren que se configure el firewall del router de forma específica. Normalmente requiere la apertura de puertos TCP y UDP y, en algunos casos, el establecimiento de puertos de activación. Una aplicación compatible con UPnP tiene la capacidad de comunicarse con el router, básicamente “diciendo” al router la forma en que necesita que sea configurado el firewall. El router efectúa los envíos con la opción UPnP desactivada. Si está utilizando cualquier aplicación compatible con UPnP y desea sacar partido de las características UPnP, puede activar la característica UPnP. Simplemente deberá seleccionar “Enable” (Activar) en la sección “UPnP Enabling” (Activación de UPnP) de la página de “Utilities” (Utilidades). Haga clic en “Apply Changes” (Aplicar cambios) para guardar el cambio.



Activar/Desactivar la actualización automática del Firmware

Esta innovación proporciona al router la capacidad incorporada de buscar automáticamente una nueva versión del firmware y de informarle de que está disponible una nueva versión. Cuando acceda a la interfaz avanzada del router, éste efectuará una búsqueda para comprobar si está disponible una nueva versión del firmware. En caso afirmativo, aparecerá una notificación. Puede optar por descargar la nueva versión o por ignorar el mensaje. El router es distribuido con esta función desactivada. Si desea activarla, seleccione “Enable” (Activar) y haga clic en “Apply



Changes” (Aplicar cambios).

Configuración de los ordenadores

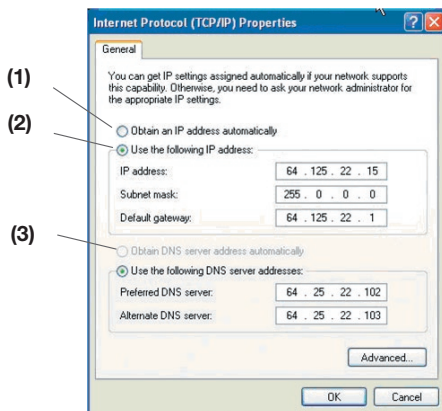
Para que su ordenador se pueda comunicar adecuadamente con su router, necesitará cambiar las configuraciones de “TCP/IP / Ethernet” de su PC a “Obtener una dirección IP automáticamente/ Utilizar DHCP”. Ésta es la configuración por defecto de la mayoría de los ordenadores domésticos.

Configure el ordenador que está conectado al módem DSL utilizando PRIMERO los siguientes pasos. Asimismo, puede emplear estos pasos para añadir ordenadores a su router una vez que éste haya sido configurado para conectarse a Internet.

Configuración manual de los adaptadores de red

Windows XP, 2000 o NT

1. Haga clic en “Start” (Comienzo), “Settings” (Ajustes), y después “Control Panel” (Panel de Control).
2. Haga doble clic en el icono “Network and dial-up connections” (Conexiones telefónicas y de red) (Windows 2000) o en el icono “Network” (Red) (Windows XP).
3. Haga clic con el botón derecho del ratón en la “Local Area Connection” (Conexión de área local) asociada a su adaptador de red y seleccione “Properties” (Propiedades) del menú desplegable.



4. En la ventana de “Local Area Connection Properties” (Propiedades de la conexión de área local), haga clic en “Internet Protocol (TCP/IP)” (Protocolo de Internet [TCP/IP]) y haga clic en el botón de “Properties” (Propiedades). Aparecerá la siguiente pantalla:
5. Si utiliza la siguiente dirección IP, esto es “Use the following IP address” (2) [Designer (diseñador): consúltelo como referencia (2) en el pantallazo] su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.
6. Si no se encuentran seleccionadas, seleccione “Obtain an IP address automatically” (Obtener una dirección IP automáticamente) (1) y “Obtain DNS server address automatically” (Obtener una dirección de servidor DNS automáticamente) (3) Haga clic en “OK” (aceptar). Su(s) adaptador(es) de red está(n) configurado(s) ahora para su uso con el router.

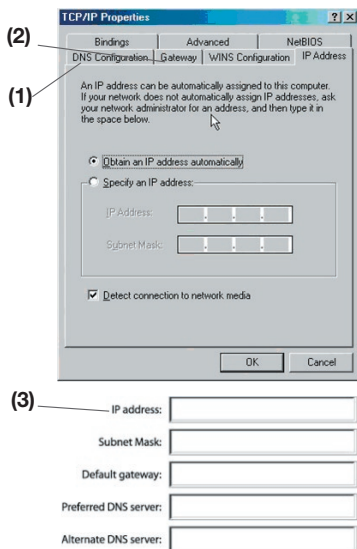
1
2
3
4
5
6
7
8
9
10
11

sección

Configuración manual de los adaptadores de red

Windows 98SE o Me

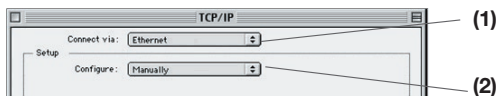
1. Haga clic con el botón derecho del ratón en “My Network Neighborhood” (Mi entorno de red) y seleccione “Properties” (Propiedades) del menú desplegable.
2. Seleccione “TCP/IP -> settings” (TCP/IP -> Ajustes) para su adaptador de red instalado. Aparecerá la siguiente ventana.
3. Si se encuentra seleccionada la opción “Specify an IP address” (Especificar una dirección IP), su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.
4. Escriba la dirección IP y la máscara de subred en la pestaña “IP Address” (Dirección IP) (3).
5. Seleccione la pestaña “Gateway” (Pasarela) (2). Escriba la dirección de gateway (pasarela) en el cuadro.
6. Seleccione la pestaña “DNS Configuration” (Configuración DNS) (1) Escriba la(s) dirección (direcciones) DNS en el cuadro.
7. Si no se encuentra seleccionada, seleccione “Obtain IP address automatically” (Obtener dirección IP automáticamente) en la pestaña de la dirección IP. Haga clic en “OK” (aceptar). Reinicie el ordenador. Una vez reiniciado el ordenador, el adaptador o los adaptadores de su red estarán configurados ahora para su uso con el router. Configure el ordenador que está conectado al módem por cable o DSL utilizando PRIMERO los siguientes pasos. Asimismo, puede emplear estos pasos para añadir ordenadores a su router una vez que éste haya sido configurado para conectar a Internet.



Mac OS hasta 9.x

Para que su ordenador se comunique adecuadamente con su router, necesitará cambiar las configuraciones TCP/IP de su Mac a DHCP.

1. Abra el menú Apple. Seleccione “Control Panels” (Paneles de control) y seleccione “TCP/IP”.
2. Aparecerá el panel de control de TCP/IP. Seleccione “Ethernet Built-In” (Ethernet incorporada) o “Ethernet” en el menú desplegable “Connect via:” (Conectar a través de:); menú desplegable (1).

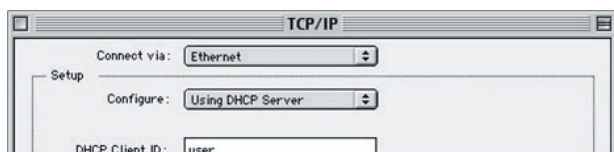


Configuración manual de los adaptadores de red

3. Junto a “Configure” (configurar) (2) [Designer (diseñador): consúltelo como referencia (2) en el pantallazo] si se encuentra seleccionada la opción “Manually” (Manualmente), su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.

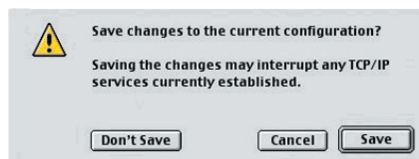
IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

4. Si no está establecido todavía, en “Configure:”, (Configurar:) seleccione “Using DHCP Server” (Empleo de servidor DHCP). Esto indicará al ordenador que debe obtener una dirección IP del router.



5. Cierre la ventana. Si ha efectuado algún cambio, aparecerá la siguiente ventana. Haga clic en “Save” (Guardar).

Reinicie el ordenador. Una vez reiniciado el ordenador, los ajustes de su red estarán configurados ahora para su uso con el router.



Mac OS X

1. Haga clic en el icono de “System Preferences” (Preferencias del sistema).

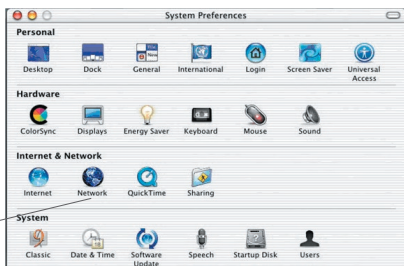


1
2
3
4
5
6
7
8
9
10
11

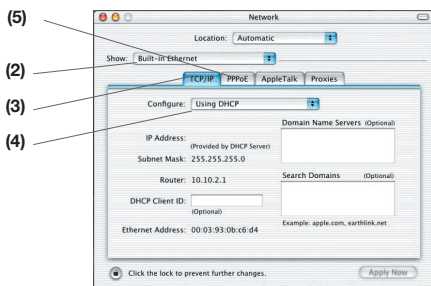
sección

Configuración manual de los adaptadores de red

2. Seleccione “Network” (red) (1) del menú “System Preferences” (Preferencias del sistema).
3. Seleccione “Built-in Ethernet” (Ethernet incorporada) (2) junto a “Show” (Mostrar) en el menú de red.



4. Seleccione la pestaña “TCP/IP” (3). Junto a “Configure” (4), deberá aparecer “Manually” o “Using DHCP”. En caso contrario, compruebe la pestaña PPPoE (5) para asegurarse de que la opción “Connect using PPPoE” (Conectar usando PPPoE) NO esté seleccionada. Si está seleccionada, deberá configurar su router para un tipo de conexión PPPoE utilizando su nombre de usuario y contraseña.



5. Si se encuentra seleccionada la opción “Manually” (Manualmente), su router deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección en la tabla presentada a continuación. Deberá introducir esta información en el router.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

6. Si no está establecido todavía, seleccione “Using DHCP Server” (Empleo de servidor DHCP) junto a “Configure:” (Configurar:) (4), luego haga clic en “Apply Now” (Aplicar ahora).

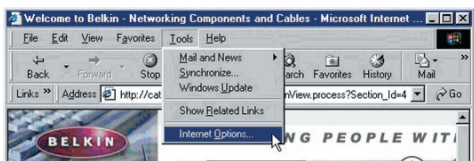
Su(s) adaptador(es) de red está(n) configurado(s) ahora para su uso con el router.

Ajustes recomendados para el navegador de red

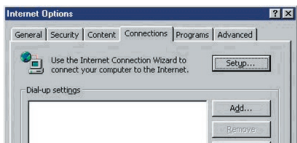
En la mayoría de los casos, no necesitará efectuar ningún cambio en los ajustes de su navegador de Internet. Si tiene problemas para acceder a Internet o a la interfaz de usuario avanzada a través de la red, modifique los ajustes de su navegador e introduzca los ajustes recomendados en la presente sección.

Microsoft Internet Explorer 4.0 o versiones superiores

1. Inicie su navegador de Internet. Seleccione “Tools” (Herramientas) y después “Internet Options” (Opciones de Internet).

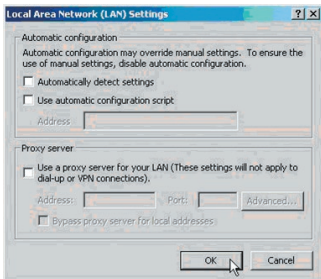


2. En la pantalla de “Internet Options” (Opciones de Internet), existen tres selecciones: “Never dial a connection” (No marcar nunca una conexión), “Dial whenever a network connection is not present” (Marcar cuando no haya ninguna conexión a la red) y “Always dial my default connection” (Marcar siempre la conexión predeterminada). Si puede elegir una opción, seleccione “Never dial a connection” (no marcar nunca una conexión). Si no puede efectuar una selección, vaya al siguiente paso.



3. En la ventana de “Internet Options” (Opciones de Internet), haga clic en “Connections” (Conexiones) y seleccione “LAN Settings...” (Ajustes de LAN...).

4. Asegúrese de que no existan marcas junto a ninguna de las opciones mostradas: “Automatically detect settings” (Detectar la configuración automáticamente), “Use automatic configuration script” (Usar secuencia de configuración automática) y “Use a proxy server” (Utilizar un servidor proxy). Haga clic en “OK” (Aceptar). Después haga clic de nuevo en “OK” (aceptar) en la página de “Internet Options” (opciones de Internet).

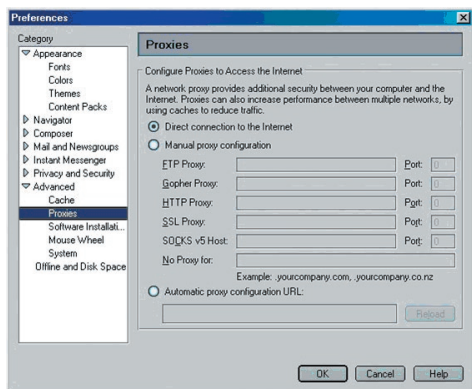


1
2
3
4
5
6
7 **sección**
8
9
10
11

Ajustes recomendados para el navegador de red

Netscape® Navigator® 4.0 o superior

1. Inicie Netscape. Haga clic en “Editar” y seleccione “Preferencias”.
2. En la ventana de “Preferencias”, haga clic en “Avanzadas” y después seleccione “Proxy”. En la ventana de “Proxies” (Proxy), haga clic en “Direct connection to the Internet” (Conexión directa con Internet).



Resolución de problemas

1

Problema:

El LED de ADSL no está encendido.

Solución:

1. Verifique la conexión entre el router y la línea ADSL. Asegúrese de que el cable de la línea ADSL se encuentre conectado al puerto del router con la etiqueta “DSL Line”.
2. Asegúrese de que el router disponga de alimentación. El [Insert (insertar): Power Icon (icono de alimentación)] El LED de la alimentación ubicado en el panel frontal debe estar iluminado.

2

3

4

Problema:

El LED de Internet no está encendido.

Solución:

1. Asegúrese de que el cable de la línea ADSL se encuentre conectado al puerto del router con la etiqueta “DSL Line” y [Insert (insertar): icono ADSL] El LED ADSL está encendido.
2. Asegúrese de haber ingresado los datos correctos para VPI/VCI, nombre del usuario y contraseña, suministrados por su ISP.

5

6

7

8

Problema:

Mi tipo de conexión es “static IP address” (dirección IP estática). No puedo conectar con Internet.

Solución:

Debido a que su tipo de conexión es “static IP address” (dirección IP estática), su ISP deberá asignarle la dirección IP, máscara de subred y dirección de gateway (pasarela). En vez de utilizar el asistente de instalación, vaya al menú de “Connection Type” (Tipo de conexión) y seleccione el tipo de conexión correspondiente. Luego, haga clic en “Next” (Siguiendo), seleccione “Static IP” (IP estática), e ingrese la información de máscara de subred y dirección de gateway (pasarela).

9

10

11

Problema:

He olvidado o perdido mi contraseña.

Solución:

Presione y mantenga presionado el botón “Reset” (Reinicio), ubicado en el panel frontal, durante al menos seis segundos. De esta manera, restablecerá los ajustes de fábrica por defecto.

Problema:

Mi ordenador no puede conectarse de manera inalámbrica al router.

Solución:

1. Asegúrese de que su PC inalámbrico tenga los mismos ajustes SSID que el

router y de tener los mismos ajustes de seguridad, como la encriptación WPA o WEP, en los clientes.

2. Asegúrese de que el router y el PC inalámbrico no estén demasiado lejos el uno del otro.

Problema:

La red inalámbrica es interrumpida con frecuencia.

Solución:

1. Coloque su PC inalámbrico más cerca del router para encontrar una mejor señal.
2. También es posible que haya interferencias, causadas posiblemente por un horno microondas o teléfonos de 2.4GHz. Coloque el router en otro lugar o utilice un canal inalámbrico diferente.

Problema:

No me puedo conectar a Internet de forma inalámbrica.

Solución:

Si no puede conectarse a Internet desde un ordenador inalámbrico, compruebe lo siguiente:

1. Contemple las luces de su router. Si está utilizando un router de Belkin, las luces deberán aparecer como sigue:
 - La luz de alimentación deberá estar encendida.
 - La luz de conexión (“Connected”) deberá estar encendida pero no intermitente.
 - La luz “WAN” deberá estar encendida o intermitente.
2. Abra el software de su utilidad inalámbrica haciendo clic en el icono de la bandeja del sistema en la esquina inferior derecha de la pantalla. Si está utilizando una tarjeta inalámbrica de Belkin, el icono de la bandeja tendrá el siguiente aspecto [INSERT ICON] (el icono puede ser rojo o verde):
3. La ventana exacta que aparece variará dependiendo del modelo de tarjeta inalámbrica del que disponga; sin embargo, todas las utilidades deberán presentar una lista de “Redes Disponibles”; aquellas redes inalámbricas a las que se puede conectar.

¿Aparece en los resultados el nombre de su red inalámbrica?

Sí, el nombre de mi red aparece en la lista: consulte la solución de problemas “No me puedo conectar a Internet de forma inalámbrica pero el nombre de mi red aparece en la lista”.

No, el nombre de mi red no aparece en la lista. Entonces, consulte la solución de problemas “No puedo conectar a Internet de forma inalámbrica y el nombre de mi red no aparece en la lista”.

Problema:

No me puedo conectar a Internet de forma inalámbrica pero el nombre de mi red aparece en la lista.

Solución:

Si el nombre de su red aparece en la lista “Available Networks” (Redes Disponibles), siga los siguientes pasos para realizar la conexión inalámbrica:

1. Haga clic en el nombre correcto de la red en la lista de “Available Networks” (redes disponibles).

Si la red tiene activada la seguridad (encriptación), será preciso que introduzca la clave de red. Para obtener más información acerca de la seguridad, lea la página que lleva el título “Modificación de los ajustes de encriptación inalámbrica”.

2. En pocos segundos, el icono de la bandeja del sistema, en la esquina inferior izquierda de su pantalla, deberá ponerse de color verde indicando la correcta conexión con la red.

Problema:

No me puedo conectar a Internet de forma inalámbrica y el nombre de mi red no aparece en la lista.

Solución:

Si el nombre correcto de la red no aparece en la lista “Available Networks” (Redes Disponibles) en la utilidad inalámbrica, intente realizar los siguientes pasos para la resolución del problema:

1. Desplace temporalmente el ordenador, si es posible, a una distancia de 3 metros del router. Cierre la utilidad inalámbrica y vuelva a abrirla. Si ahora aparece el nombre correcto de la red en la lista “Available Networks” (Redes Disponibles), es posible que tenga un problema de alcance o de interferencia. Consulte las sugerencias incluidas en el Anexo B, “Factores importantes para la colocación y configuración”.

2. Empleando un ordenador que esté conectado al router a través de un cable de red (al contrario que de forma inalámbrica), asegúrese de que esté activado “Broadcast SSID” (emitir SSID). Esta configuración se encuentra en la página de configuración inalámbrica titulada “Channel and SSID” (Canal y SSID).

Si aún no puede acceder a Internet después de completar estos pasos, póngase en contacto con el servicio de asistencia técnica de Belkin.

Problema:

El rendimiento de mi red inalámbrica es irregular.

La transferencia de datos es lenta en ocasiones.

La potencia de la señal es débil.

Dificultad para establecer o mantener una conexión de red privada virtual (VPN, Virtual Private Network).

Solución:

La tecnología inalámbrica está basada en la radioemisión, lo que significa que la conectividad y el rendimiento entre dispositivos descenderán a medida que

aumente la distancia entre los mismos. Otros factores que provocan un debilitamiento de la señal (el metal es habitualmente el responsable) son obstáculos tipo paredes y aparatos metálicos. Como resultado, el alcance habitual de sus dispositivos inalámbricos en interiores se situará entre 30 y 60 metros. Tenga en cuenta, además, que la velocidad de conexión puede verse mermada cuando más se aleje del router o punto de acceso.

Con el fin de determinar si los problemas de conexión inalámbrica están relacionados con el alcance, desplace provisionalmente el ordenador, a ser posible, a una distancia de entre 1,5 y 3 m del Router.

Cambio del canal inalámbrico: según la interferencia y el tráfico inalámbrico del área, cambiar el canal inalámbrico de su red puede mejorar el rendimiento y la fiabilidad. El canal 11 es el canal pre-determinado con el que se suministra el router. Puede elegir entre varios canales dependiendo de su región; consulte la página 37 “modificación del canal inalámbrico” para obtener instrucciones de cómo elegir otros canales.

Limitación de la velocidad de transmisión inalámbrica: limitar la velocidad de transmisión inalámbrica puede ayudar a mejorar la estabilidad de la conexión y el alcance inalámbrico máximo. La mayoría de las tarjetas inalámbricas tiene la capacidad de limitar la velocidad de transmisión. Para modificar esta propiedad, diríjase al panel de control de Windows, abra las conexiones de red y haga doble clic en la conexión de la tarjeta inalámbrica. En el diálogo de propiedades, seleccione el botón “Configure” (Configurar) en la pestaña “General” (los usuarios de Windows 98 deberán seleccionar la tarjeta inalámbrica en el cuadro de lista y luego hacer clic sobre “Properties” [Propiedades]), y luego elija la pestaña “Advanced” (Opciones Avanzadas) y seleccione la propiedad de velocidad. Por lo general, las tarjetas de cliente inalámbrico se configuran de forma automática para ajustar la velocidad de transmisión inalámbrica, pero esto puede causar interrupciones periódicas en la conexión si la señal inalámbrica es demasiado débil. Como regla general, las velocidades de transmisión más lentas son más estables. Experimente con diferentes velocidades de conexión hasta que encuentre la mejor para su entorno, tome nota de que todas las velocidades de transmisión disponibles deben ser aceptables para navegar por Internet. Para obtener mayor asesoría, consulte el manual del usuario de su tarjeta inalámbrica.

Problema:

¿Cómo se amplía el alcance de la red inalámbrica?

Solución:

Belkin recomienda el empleo de los siguientes productos para ampliar la cobertura de la red inalámbrica en hogares u oficinas de gran tamaño:

- **Punto de acceso inalámbrico:** Un punto de acceso inalámbrico puede duplicar de forma efectiva el área de cobertura de su red inalámbrica. Por lo general, se coloca el punto de acceso en un área que su router inalámbrico no cubre actualmente y se conecta al router utilizando ya sea un cable Ethernet o a través de las líneas

eléctricas de su hogar utilizando dos adaptadores Ethernet Powerline.

- Para redes inalámbricas 802.11g (54g), Belkin ofrece un Extensor del alcance inalámbrico/Punto de acceso que puede ser conectado a un router inalámbrico 802.11g de Belkin sin necesidad de cable Ethernet ni de adaptadores de Ethernet Powerline.

Estos productos de Belkin están disponibles en su distribuidor local o los puede solicitar a Belkin directamente.

Para obtener información sobre la ampliación de alcance/red, visite: www.belkin.com/networking para obtener detalles sobre:

Ampliación del alcance inalámbrico G/Punto de acceso (F5D7132)

Problema:

Tengo dificultades para configurar la WEP (Wired Equivalent Privacy, privacidad equivalente a la del cable) en un router de Belkin o punto de acceso de Belkin.

Solución:

1. Acceda a su router inalámbrico o punto de acceso.
2. Abra su navegador de Internet e introduzca la dirección IP del router inalámbrico o punto de acceso. (La dirección IP del router pre-determinado es 192.168.2.1 y la dirección IP del punto de acceso 802.11g es 192.168.2.254). Acceda a su router haciendo clic en el botón "Login" (Acceso) de la parte superior derecha de la pantalla. Se le solicitará la introducción de la contraseña. Si nunca antes ha establecido una contraseña, deje en blanco el campo de contraseña y haga clic sobre "Submit" (Enviar).
3. Haga clic en la pestaña "Wireless" (Inalámbrico) situada en la parte izquierda de su pantalla. Seleccione la pestaña "Encryption" (Encriptación) o "Security" (Seguridad) para acceder a la pantalla de ajustes de seguridad.
4. Seleccione "128-bit WEP" del menú desplegable.
5. Después de seleccionar su modo de encriptación WEP, podrá introducir su clave WEP hexadecimal manualmente, o introducir una frase de paso en el campo "Passphrase" y hacer clic en "Generate" (generar) para crear una clave WEP a partir de la frase de paso. Haga clic en "Apply Changes" (Aplicar cambios) para finalizar. Ahora deberá hacer que todos sus clientes coincidan con estos ajustes. Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9. Para WEP de 128 bits deberá introducir 26 claves hexadecimales.

Por ejemplo:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = clave de 128 bits

6. Haga clic en "Apply Changes" (aplicar cambios) para finalizar. Ahora está establecida la encriptación en el router inalámbrico. Cada ordenador de su red inalámbrica deberá ser configurado ahora con los mismos ajustes de seguridad.

ADVERTENCIA: Si está configurando el router inalámbrico o punto de acceso desde un ordenador con un cliente inalámbrico, necesitará asegurarse de que el modo de seguridad esté activado para este cliente inalámbrico. De lo contrario, perderá su conexión inalámbrica.

Nota para los usuarios de Mac: Los productos originales Apple AirPort admiten exclusivamente la encriptación de 64 bits. Los productos Apple AirPort 2 soportan la encriptación de 64 o de 128 bits. Compruebe qué versión del producto Apple AirPort está utilizando. Si no puede configurar su red con una encriptación de 128 bits, pruebe con una encriptación de 64 bits.

Problema:

Tengo dificultades para configurar la WEP (Wired Equivalent Privacy, privacidad equivalente a la del cable) en una tarjeta inalámbrica de cliente de Belkin.

Solución:

La tarjeta inalámbrica deberá emplear la misma clave que el router inalámbrico o punto de acceso. Por ejemplo, si su router inalámbrico o punto de acceso utilizan la clave 00112233445566778899AABBCC, la tarjeta de cliente debe ser configurada con la misma clave.

1. Haga doble clic sobre este icono de “Signal Indicator” (Indicador de la señal) para abrir la pantalla “Wireless Network” (Red inalámbrica).
2. El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta.
3. Cuando haga clic en el botón “Advanced” (Avanzado) aparecerá la utilidad de LAN inalámbrica de Belkin. Esta utilidad le permitirá gestionar todas las propiedades avanzadas de la tarjeta inalámbrica de Belkin.
4. En la pestaña “Wireless Network Properties” (Redes inalámbricas: propiedades), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
5. En la categoría “Data Encryption” (Encriptación de datos), seleccione “WEP”.
6. Asegúrese de que el recuadro “The key is provided for me automatically” (La clave se me proporciona automáticamente) que se encuentra en la parte inferior no esté marcado. Si está utilizando este ordenador para conectarse a una red corporativa, consulte con su administrador de red si es necesario marcar esta casilla.
7. Introduzca su clave WEP en el recuadro “Network key” (Clave de red).

Importante: Una clave WEP es una mezcla de números y letras de la A a la F y del 0 al 9. Para WEP de 128 bits, deberá introducir 26 claves. Esta clave de red deberá coincidir con la clave que haya asignado a su router inalámbrico o punto de acceso.

Por ejemplo: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = clave de 128 bits

8. Haga clic en “OK” y después “Apply” (Aplicar) para guardar los ajustes.

Si NO está utilizando una tarjeta de cliente inalámbrica de Belkin, consulte el manual del usuario del fabricante de la tarjeta de cliente inalámbrica que esté utilizando.

Problema:

¿Soportan los productos Belkin la seguridad WPA?

Solución:

Atención: Para utilizar la seguridad WPA, todos sus clientes deberán haber

actualizado los controladores y el software que son compatibles con WPA. Al momento de la publicación de esta sección de Preguntas Frecuentemente Preguntadas (FAQ), se puede descargar de Microsoft un parche de seguridad gratuito. Este parche sólo funciona con el sistema operativo Windows XP.

Descargue el parche en la siguiente dirección:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

Asimismo, deberá descargar el driver más actualizado para su tarjeta de red inalámbrica 802.11g para notebook o para ordenador de sobremesa de Belkin desde la página de asistencia de Belkin. En la actualidad no existe soporte para otros sistemas operativos. El parche de Microsoft sólo es compatible con dispositivos con controladores preparados para WPA, como los productos 802.11g de Belkin.

Descargue el último controlador en <http://www.belkin.com/uk/support/tech/index.asp>

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en un router de Belkin o punto de acceso de Belkin para una red doméstica.

Solución:

1. Desde el menú desplegable “Security mode” (modo de seguridad), seleccione “WPA-PSK (no server)” (WPA-PSK, sin servidor).
2. Para “Encryption Technique” (Técnica de encriptación), seleccione “TKIP” o “AES”. Este ajuste deberá ser idéntico en todos los clientes que instale.
3. Introduzca su clave precompartida (PSK). Puede estar compuesta por entre 8 y 63 caracteres entre letras, números y símbolos o espacios. Esta misma clave deberá ser utilizada en todos los clientes que instale. Por ejemplo, su PSK será algo así como esto: “Clave de red familia Pérez”.
4. Haga clic en “Apply Changes” (aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en un router de Belkin o punto de acceso de Belkin para un negocio.

Solución:

Si su red emplea un servidor Radius para distribuir las claves a los clientes, utilice este ajuste. Se emplea habitualmente en un entorno empresarial.

1

2

3

4

5

6

7

8

9

10

11

1. Desde el menú desplegable del modo de seguridad (“Security mode”), seleccione “WPA (with server)” (WPA con servidor).
2. Para “Encryption Technique” (Técnica de encriptación), seleccione “TKIP” o “AES”. Este ajuste deberá ser idéntico en todos los clientes que instale.
3. Introduzca la dirección IP del servidor Radius en los campos de “Radius Server”.
4. Introduzca la clave Radius en el campo “Radius Key”.
5. Introduzca el intervalo de la clave. El intervalo de clave es la frecuencia con la que se distribuyen las claves (en paquetes).
6. Haga clic en “Apply Changes” (aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en una tarjeta de cliente inalámbrico de Belkin para una red de hogar.

Solución:

Los clientes deberán emplear la misma clave que el router inalámbrico G o punto de acceso. Por ejemplo, si la clave es “clave red familia Smith” en el router inalámbrico o punto de acceso, el cliente también debe utilizar esa misma clave.

1. Haga doble clic sobre este icono de “Signal Indicator” (Indicador de la señal) para abrir la pantalla “Wireless Network” (Red inalámbrica).
2. El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta.
3. Cuando haga clic en el botón “Advanced” (Avanzado) aparecerá la utilidad de LAN inalámbrica de Belkin. Esta utilidad le permitirá gestionar todas las propiedades avanzadas de la tarjeta inalámbrica de Belkin.
4. En la pestaña “Wireless Network Properties” (Redes inalámbricas: propiedades), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
5. En “Network Authentication” (Autenticación de red), seleccione “WPA-PSK (No Server)”.
6. Introduzca su clave WPA en el recuadro “Network key” (Clave de red).

Importante:WPA-PSK es una combinación de números y letras de la A a la Z y del 0 al 9. Para WPA-PSK, puede introducir de ocho a 63 caracteres. Esta clave de red deberá coincidir con la clave asignada a su router inalámbrico o punto de acceso.

7. Haga clic en “OK” y después “Apply” (Aplicar) para guardar los ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en una tarjeta de cliente inalámbrico de Belkin para un negocio.

Solución:

1. Haga doble clic sobre este icono de “Signal Indicator” (Indicador de la señal) para abrir la pantalla “Wireless Network” (Red inalámbrica).
2. El botón “Advanced” (Avanzado) le permitirá visualizar y configurar más opciones de su tarjeta.

3. Cuando haga clic en el botón “Advanced” (Avanzado) aparecerá la utilidad de LAN inalámbrica de Belkin. Esta utilidad le permitirá gestionar todas las propiedades avanzadas de la tarjeta inalámbrica de Belkin.
4. En la pestaña “Wireless Network Properties” (Redes inalámbricas: propiedades), seleccione un nombre de red de la lista “Available networks” (Redes disponibles) y haga clic en “Configure” (Configurar).
5. En “Network Authentication” (Autenticación de red), seleccione “WPA”.
6. En la pestaña “Authentication” (Autenticación), seleccione las configuraciones indicadas por su administrador de red.
7. Haga clic en “OK” y después “Apply” (Aplicar) para guardar los ajustes.

Problema:

Tengo dificultades para configurar la seguridad WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) en una tarjeta de cliente que NO es de Belkin para una red de hogar.

Solución:

Si está utilizando una tarjeta inalámbrica para ordenador de sobremesa o para notebook que NO es de Belkin y esta tarjeta no está equipada con un software compatible con WPA, se puede descargar de forma gratuita un archivo de Microsoft llamado “Windows XP Support Patch for Wireless Protected Access” (Actualización de Soporte Windows XP para acceso inalámbrico protegido): Busque el parche de Microsoft en la base de conocimiento para WPA con Windows XP y descárguelo.

Nota: El archivo que Microsoft pone a su disposición sólo funciona con Windows XP. En la actualidad no existe soporte para otros sistemas operativos. Asimismo, deberá asegurarse de que el fabricante de la tarjeta inalámbrica soporte WPA y de haber descargado e instalado el driver más actualizado de su página de asistencia. Sistemas operativos compatibles:

- Windows XP Professional
- Windows XP Home Edition

Activación de WPA-PSK (sin servidor)

1. En Windows XP, haga clic sobre “Start > Control Panel > Network Connections” (Inicio > Panel de Control > Conexiones de Red).
2. Al hacer clic en la pestaña “Wireless Networks” (Redes inalámbricas) con el botón derecho del ratón, aparecerá la siguiente pantalla. Compruebe que esté marcada la casilla “Use Windows to configure my wireless network settings” (Utilizar Windows para configurar mis configuraciones de red inalámbrica).
3. En la pestaña “Wireless Networks” (Redes inalámbricas), haga clic en el botón “Configure” (configurar).
4. Si es un usuario de hogar u oficina pequeña, seleccione “WPA-PSK” en “Network Authentication” (Autenticación de red).

Nota: Seleccione WPA (con servidor Radius) si está utilizando este ordenador para conectarse a una red corporativa que soporte un servidor de autenticación como el servidor Radius. Consulte con su administrador de red para obtener más información.

5. Para la encriptación de datos (“Data Encryption”), seleccione “TKIP” o “AES”. Este ajuste deberá ser idéntico al del router inalámbrico o punto de acceso que haya configurado.

6. Introduzca su clave de encriptación en el recuadro “Network key” (Clave de red).

Importante: Introduzca su PSK. Puede estar compuesta por entre ocho y 63 caracteres entre letras, números y símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale.

7. Haga clic en “OK” para aplicar los ajustes.

¿Cuál es la diferencia entre 802.11b, 802.11g, 802.11a y Pre-N?

Actualmente existen cuatro niveles de estándares de interconexión en red inalámbrica, que transmiten datos a velocidades máximas muy diferentes. Todos se basan en la designación 802.11(x), llamada así por el IEEE, el consejo responsable de certificar los estándares de interconexión en red. El estándar de interconexión en red más común, 802.11b, transmite información a 11Mbps; mientras que 802.11a y 802.11g operan a 54Mbps y Pre-N a 108Mbps. Pre-N, el precursor del lanzamiento del próximo estándar 802.11n, promete velocidades que superan las del 802.11g y un área de cobertura dos veces más amplia. Véase la siguiente tabla para obtener información más detallada.

Tabla de comparación inalámbrica de Belkin

Tecnología inalámbrica	G (802.11g)	G Plus MIMO (802.11g con MIMO MRC)	N MIMO (borrador 802.11n con MIMO)	N1 MIMO (borrador 802.11n con MIMO)
Velocidad/ velocidad datos*	Hasta 54Mbps*	Hasta 54Mbps*	Hasta 300Mbps*	Hasta 300Mbps*
Frecuencia	Los dispositivos domésticos más comunes tales como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2,4 GHz sin licencia	Los dispositivos domésticos más comunes como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2.4 GHz sin licencia	Los dispositivos domésticos más comunes como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2.4 GHz sin licencia	Los dispositivos domésticos más comunes como los teléfonos inalámbricos y los hornos microondas pueden interferir con la banda 2.4 GHz sin licencia
Compatibilidad	Compatible con 802.11b/g	Compatible con 802.11b/g	Compatible con el borrador del estándar 802.11n** y con 802.11b/g	Compatible con el borrador del estándar 802.11n** y con 802.11b/g
Cobertura*	Hasta 120 m*	Hasta 300 m*	Hasta 365,76 m*	Hasta 120 m*
Ventajas	Gran aceptación para el uso compartido de Internet	Mejor cobertura y velocidad y alcance consistentes	Velocidad y cobertura mejoradas	Tecnología punta: mejor cobertura y transmisión

*La distancia y la velocidad de conexión variará según el entorno de red.

**Este Router es compatible con productos que cumplen las especificaciones de la misma versión del borrador para el estándar 802.11n, y puede necesitar una actualización de software para obtener los mejores resultados

Dirección IP

La "IP address" (Dirección IP) es la dirección IP interna del router. Para acceder a la interfaz de configuración avanzada, introduzca esta dirección IP en la barra de direcciones de su navegador. Esta dirección puede ser modificada en caso necesario. Para modificar la dirección IP, introduzca la nueva dirección IP y haga clic en "Apply Changes" (Aplicar cambios). La dirección IP seleccionada será un IP no enrutable. Ejemplos de IP no enrutable son:

192.168.x.x (donde x es una cifra entre el 0 y el 255)

10.x.x.x (donde x es una cifra entre el 0 y el 255)

Máscara de subred

Algunas redes son demasiado grandes como para permitir que el tráfico de datos se extienda por toda la red. Estas redes se dividen en secciones más pequeñas, más sencillas de gestionar, que se denominan subredes. La máscara de subred está compuesta por la dirección de red y por información reservada para identificar la "subred".

DNS

DNS es el acrónimo de Servidor de nombres de dominio. Un Domain Name Server es un servidor ubicado en Internet que convierte los URL ("Universal Resource Links", Vínculos de recursos universales) como, por ejemplo, www.belkin.com en direcciones IP. Muchos ISPs no precisan que usted introduzca esta información en el router. Si está utilizando un tipo de conexión de IP estática, es posible que deba introducir una dirección DNS específica y una dirección DNS secundaria para que su conexión funcione correctamente. Si su tipo de conexión es Dinámica o PPPoE, es probable que no sea necesario introducir ninguna dirección DNS.

PPPoE

La mayoría de proveedores de ADSL emplean PPPoE como tipo de conexión. Si usted emplea un módem ADSL para conectarse a Internet, es posible que su ISP emplee el PPPoE para introducirle en el servicio.

Su tipo de conexión es PPPoE si:

1. Su ISP le proporcionó un nombre de usuario y contraseña que son necesarios para conectarse a Internet
2. Su ISP le proporcionó software como WinPOET o Enternet300, que usted emplea para conectarse a Internet
3. Usted debe hacer doble clic en un icono de escritorio distinto al de su navegador para acceder a Internet.

Para configurar el router de forma que utilice PPPoE, introduzca su nombre de usuario y contraseña en los espacios correspondientes. Una vez introducida la información, haga clic sobre "Apply Changes" (Aplicar cambios).

Una vez aplicados los cambios, el indicador el estado de Internet mostrará el mensaje "connection OK" (Conexión en buen estado) si su router ha sido configurado correctamente.

Asistencia Técnica

Asistencia técnica gratuita* *Pueden aplicarse tarifas de llamada

nacional

www.belkin.com

Dispone de más información sobre asistencia técnica en nuestro website www.belkin.com en el área de -asistencia técnica. Si desea ponerse en contacto con el servicio de asistencia técnica por teléfono, le rogamos que llame al número correspondiente de la siguiente lista*.

PAÍS	NÚMERO	DIRECCIÓN DE INTERNET
AUSTRIA	0820 200766	www.belkin.com/uk/networking/
BÉLGICA	07 07 00 073	www.belkin.com/nl/networking/
REPÚBLICA CHECA	239 000 406	www.belkin.com/uk/networking/
DINAMARCA	701 22 403	www.belkin.com/uk/networking/
FINLANDIA	097 25 19 123	www.belkin.com/uk/networking/
FRANCIA	08 - 25 54 00 26	www.belkin.com/fr/networking/
ALEMANIA	0180 - 500 57 09	www.belkin.com/de/networking/
GRECIA	00800 - 44 14 23 90	www.belkin.com/uk/networking/
HUNGRÍA	06 - 17 77 49 06	www.belkin.com/uk/networking/
ISLANDIA	800 8534	www.belkin.com/uk/networking/
IRLANDA	0818 55 50 06	www.belkin.com/uk/networking/
ITALIA	02 - 69 43 02 51	www.belkin.com/it/support/tech/issues_more.asp
LUXEMBURGO	34 20 80 85 60	www.belkin.com/uk/networking/
PAÍSES BAJOS	0900 - 040 07 90 0,10 € por minuto	www.belkin.com/nl/networking/
NORUEGA	81 50 0287	www.belkin.com/uk/networking/
POLONIA	00800 - 441 17 37	www.belkin.com/uk/networking/
PORTUGAL	707 200 676	www.belkin.com/uk/networking/
RUSIA	495 580 9541	www.belkin.com/networking/
SUDÁFRICA	0800 - 99 15 21	www.belkin.com/uk/networking/
ESPAÑA	902 - 02 43 66	www.belkin.com/es/support/tech/networkingsupport.asp
SUECIA	07 - 71 40 04 53	www.belkin.com/se/support/tech/networkingsupport.asp
SUIZA	08 - 48 00 02 19	www.belkin.com/uk/networking/
REINO UNIDO	0845 - 607 77 87	www.belkin.com/uk/networking/
OTROS PAÍSES	+44 - 1933 35 20 00	

PPPoA

Introduzca la información de PPPoA en el espacio proporcionado y haga clic en “Next” (Siguiente). Haga clic en “Apply” (Aplicar) para activar los ajustes.

1. Nombre de usuario: ingrese el nombre de usuario. (Asignado por su ISP).
2. Contraseña: ingrese su contraseña. (Asignada por su ISP).
3. Confirmación de la contraseña: vuelva a ingresar la contraseña. (Asignada por su ISP).
4. VPI/VCI: introduzca aquí los parámetros de su identificador de ruta virtual (VPI) y del identificador de circuito virtual (VCI). (Asignados por su ISP).

Desconectar después de X...

La propiedad de desconectar se emplea para desconectar automáticamente el router de su ISP cuando no existe actividad durante un periodo determinado de tiempo. Por ejemplo, al colocar una marca junto a esta opción e introducir “5” en el campo para los minutos, el router se desconectará de Internet después de cinco minutos de falta de actividad en Internet.

Debería utilizar esta opción en el caso de que abone sus servicios de Internet por minutos.

Canal y SSID

Para modificar el canal de funcionamiento del router, seleccione el canal deseado del menú desplegable y seleccione su canal. Haga clic en “Apply Changes” (Aplicar cambios) para guardar los ajustes. También puede modificar el SSID. El SSID es el equivalente al nombre de la red inalámbrica. Puede dar al SSID la denominación que desee. Si existen otras redes inalámbricas en su área, deberá dar a su red inalámbrica un nombre exclusivo. Haga clic en el recuadro de SSID e ingrese un nombre nuevo. Haga clic en “Apply Changes” (Aplicar cambios) para efectuar el cambio.

Emisión de ESSID

Muchos adaptadores inalámbricos de red actuales que están disponibles en el mercado cuentan con una función de inspección de la ubicación. Pueden rastrear el entorno en busca de todas las redes disponibles y permitirá al ordenador seleccionar una de las redes localizadas. Esto ocurrirá si el SSID del ordenador tiene el ajuste “ANY” (Cualquier SSID). Su router de Belkin es capaz de bloquear esta búsqueda aleatoria de una red. Si desactiva la función “ESSID Broadcast” (Emitir ESSID), la única forma de que su ordenador se conecte con la red es estableciendo para el SSID del ordenador el nombre específico de la red (como WLAN). Asegúrese de conocer su SSID (nombre de red) antes de activar esta propiedad. Es posible lograr que su red inalámbrica sea prácticamente invisible. Al desactivar la emisión del SSID, su red no aparecerá en una inspección de la ubicación. Desactivar la emisión del SSID contribuirá a elevar la seguridad.

Encriptación

El empleo de la encriptación puede contribuir a mantener su red segura. El router

emplea encriptación WEP para proteger sus datos y dispone de dos modos de encriptación. 64 bits y 128 bits. La encriptación funciona con un sistema de claves. La clave del ordenador debe coincidir con la clave del router. Hay dos formas de crear una clave. La manera más sencilla es que el software del router convierta una contraseña que usted ha ingresado en una clave. El método avanzado consiste en introducir las claves manualmente.

Gateways (pasarelas) de aplicación

Las Gateways (pasarelas) de aplicación le permiten especificar determinados puertos para que se encuentren abiertos con el fin de que determinadas aplicaciones funcionen correctamente con la propiedad NAT (Network Address Translation, Traducción de direcciones de red) del router. Se ha incluido una lista de las aplicaciones más populares. Puede seleccionar una aplicación de entre las opciones que se incluyen en la lista desplegable. Su selección se programará en el router. Seleccione en la lista desplegable la fila de la que desea copiar los ajustes, seleccione la fila a la que desea copiarlos y luego haga clic sobre “Copiar a”. Los ajustes serán transferidos a la fila seleccionada que especifique. Haga clic en “Apply Changes” (Aplicar cambios) para guardar el ajuste de esta aplicación. Si no encuentra aquí su aplicación, necesitará consultar con el proveedor de la aplicación para identificar los puertos que necesitan ser configurados. Puede introducir esta información de forma manual en el router.

Servidores virtuales

Esta función le permitirá enrutar llamadas externas (Internet) para servicios como el servidor web (puerto 80), servidor FTP (puerto 21) y otras aplicaciones a través de su router hasta su red interna. Gracias a que sus ordenadores internos están protegidos por un firewall, las máquinas fuera de su red (a través de Internet) no pueden acceder a ellos, ya que no pueden ser “detectados”. Si necesita configurar el servidor virtual para una aplicación específica, será preciso que se ponga en contacto con el fabricante de la aplicación para descubrir los ajustes de los puertos precisos.

Para introducir las configuraciones de forma manual, introduzca la dirección IP en el espacio provisto para la máquina interna (servidor) y el puerto o los puertos necesarios para pasar, seleccione el tipo de puerto (TCP o UDP) y los puertos LAN y públicos necesarios para pasar. Luego, seleccione “Enable” y haga clic en “Set”. Únicamente podrá pasar por un puerto por cada dirección IP interna. Abrir los puertos de su firewall puede representar un riesgo para la seguridad. Puede activar y desactivar los ajustes de forma rápida. Se recomienda que desactive los ajustes cuando no esté utilizando una aplicación específica.

Filtros para IP de clientes

El Router puede ser configurado para restringir el acceso a Internet, al e-mail o a otros servicios de red en determinados días y horas. La restricción puede ser configurada para un solo ordenador, para una gama de ordenadores o para múltiples ordenadores.

Bloqueo de URL

Para configurar la función de bloqueo de URL, especifique las páginas-web o palabras

clave que desea filtrar en su red. Haga clic en “Apply Changes” (Aplicar cambios) para guardar el cambio. Para completar esta configuración, deberá crear o modificar una norma de acceso en la sección de filtros IP del cliente. Para modificar una norma existente, haga clic en “Edit” junto a la norma que desea modificar. Para crear una norma nueva, haga clic en “Add PC” (Añadir PC). En la sección “Access Control Add PC” (Control de acceso, añadir PC), seleccione la opción “WWW with URL Blocking” (WWW con bloqueo de URL) en la tabla “Client PC Service” para filtrar las páginas-web y palabras clave especificadas.

Regla de horario

Para programar una norma, especifique el nombre, un comentario, hora de comienzo y fin del filtro que desea activar en su red. Esta página define los nombres de normas programadas y las activa para ser utilizadas en la página “Access Control”.

Filtrado de direcciones MAC

El filtro de direcciones MAC es una potente característica de seguridad que le permite especificar qué ordenadores están permitidos en la red. Cualquier ordenador que intente acceder a la red que no esté especificado en la lista de filtrado, no obtendrá permiso para acceder. Cuando active esta propiedad, deberá introducir un nombre de usuario y la dirección MAC de cada cliente de su red para permitir el acceso a la misma de cada uno de ellos o copiar la dirección MAC seleccionando el nombre del ordenador en la lista “DHCP Client List”. Para activar esta función, seleccione “Enable”. Haga clic en “Apply Changes” (Aplicar cambios) para guardar los ajustes.

DMZ

Si uno de los clientes conectados no puede llevar a cabo una aplicación de Internet correctamente debido al firewall, podrá establecer un acceso a Internet no restringido en ambas direcciones para dicho ordenador. Esto puede ser necesario en el caso de que la propiedad NAT esté causando problemas con una aplicación como, por ejemplo, una aplicación de juegos o de videoconferencia. Utilice esta característica de forma temporal. El ordenador que se encuentra en la DMZ no está protegido contra los ataques de piratas informáticos. Para establecer una zona desmilitarizada para uno de los ordenadores, ingrese los últimos dígitos de la dirección IP de LAN en el campo “Static IP” (IP estática) y haga clic en “Apply Changes” (Aplicar cambios) para activar los ajustes.

Si sólo tiene una dirección IP (WAN) pública, deje como IP pública “0.0.0.0”. Si está utilizando múltiples direcciones IP públicas de WAN, será posible seleccionar a qué dirección IP de WAN será dirigido el host de DMZ. Introduzca la dirección IP de WAN a la que desee dirigir el host de DMZ, introduzca los dos últimos dígitos de la dirección IP del ordenador host de DMZ y haga clic en “Apply Changes” (Aplicar cambios).

Contraseña de administrador

El router efectúa el envío SIN necesidad de introducir contraseña. Si desea añadir una contraseña para disfrutar de una mayor seguridad, puede establecerla desde la interfaz de internet del router. Escriba su contraseña y guárdela en un lugar seguro, ya que la necesitará si precisa acceder al router en el futuro. Se recomienda encarecidamente que establezca una contraseña si prevé utilizar la opción de gestión a distancia de su router. La opción de tiempo límite de acceso le permite establecer el periodo de tiempo que podrá permanecer en la interfaz de configuración avanzada del router. El temporizador arranca cuando no existe actividad. Por ejemplo, usted ha efectuado algunos cambios en la interfaz de configuración avanzada y después deja su ordenador solo sin hacer clic en "Logout" (Salir).

Si suponemos que el tiempo límite es de 10 minutos, entonces 10 minutos después de que abandone el ordenador, la sesión se cerrará. Deberá acceder al router de nuevo para realizar más cambios. La opción del tiempo límite de acceso responde a razones de seguridad y la configuración por defecto es de 10 minutos. Solamente podrá acceder un ordenador cada vez a la interfaz de configuración avanzada del router.

Hora y Zona horaria

El router mantiene la hora conectándose a un servidor SNTP (Simple Network Time Protocol, protocolo horario de red simple). Esto permite al router sincronizar el reloj del sistema con el conjunto de Internet. El reloj sincronizado en el router se emplea para grabar el registro de seguridad y para controlar el filtrado de clientes. Seleccione la zona horaria en la que reside. Si reside en una zona que se realiza el cambio de hora según el horario de verano, coloque una marca en el recuadro junto a “Enable Daylight Saving” (Cambiar la hora automáticamente según el horario de verano). Es posible que el reloj del sistema no se actualice inmediatamente.

Espera al menos 15 minutos para que el router contacte con los servidores horarios de Internet y obtenga una respuesta. No podrá cambiar la hora del reloj usted mismo.

Gestión a distancia

Antes de activar esta función **ASEGÚRESE DE HABER ESTABLECIDO LA CONTRASEÑA DEL ADMINISTRADOR**. La gestión a distancia le permite efectuar cambios en los ajustes de su router desde cualquier parte en Internet.

UPnP

El UPnP (Universal Plug-and-Play, Plug-and-Play universal) es una tecnología que ofrece un funcionamiento perfecto de las opciones de mensajes de voz, mensajes de vídeo, juegos y otras aplicaciones compatibles con UPnP. Algunas aplicaciones requieren que el firewall del router sea configurado de una forma específica para funcionar correctamente. Normalmente requiere la apertura de puertos TCP y UDP y, en algunos casos, el establecimiento de puertos de activación. Una aplicación compatible con UPnP tiene la capacidad de comunicarse con el router, básicamente “diciendo” al router la forma en que necesita que sea configurado el firewall. El router efectúa los envíos con la opción UPnP desactivada. Si está utilizando cualquier aplicación compatible con UPnP y desea sacar partido de las características UPnP, puede activar la característica UPnP. Simplemente deberá seleccionar “Enable” (Activar) en la sección “UPnP Enabling” (Activación de UPnP) de la página de “Utilities” (Utilidades). Haga clic en “Apply Changes” (Aplicar cambios) para guardar el cambio.

Nota: Aunque algunos de los elementos enumerados a continuación pueden afectar el rendimiento de la red, estos no impedirán que su red inalámbrica funcione. Si le preocupa que su red no esté funcionando a su máxima potencia, esta lista de verificación puede ser útil.

1. Colocación de su router inalámbrico (o punto de acceso)

Coloque su router inalámbrico (o punto de acceso), el punto central de conexión de su red, lo más cerca posible del centro de sus dispositivos de interconexión en red inalámbricos.

Para lograr la mejor cobertura de red inalámbrica para sus “clientes inalámbricos” (es decir, ordenadores equipados con tarjetas de red inalámbrica

Anexo B: Factores importantes de colocación e instalación

para ordenador portátil, tarjetas de red inalámbrica para ordenador de sobremesa y adaptadores inalámbricos para USB de Belkin):

- Asegúrese de que las antenas de su router inalámbrico (o punto de acceso) estén situadas de forma paralela entre sí y orientadas verticalmente (apuntando hacia el techo). Si su router inalámbrico (o punto de acceso) está colocado en posición vertical, oriente las antenas hacia arriba en la máxima medida posible.
- En las casas de varias plantas, coloque el router inalámbrico (o punto de acceso) en el piso más cercano al centro de la casa. Esto puede implicar la colocación de su router inalámbrico (o punto de acceso) en una de las plantas superiores.
- Intente no colocar el router inalámbrico (o punto de acceso) cerca de un teléfono inalámbrico de 2,4 GHz.

2. Evitar obstáculos e interferencias

Evite colocar su router inalámbrico (o punto de acceso) cerca de dispositivos que puedan emitir “ruido” de radioemisión, como hornos microondas. Los objetos densos que pueden impedir la comunicación inalámbrica incluyen:

- Frigoríficos
- Lavadoras y secadoras
- Armarios de metal
- Acuarios de gran tamaño
- Ventanas con tinte de base metálica contra radiaciones ultravioletas

Si su señal inalámbrica parece debilitarse en algunos puntos, asegúrese de que este tipo de objetos no esté bloqueando la ruta de la señal (entre sus ordenadores y el router inalámbrico o punto de acceso).

3. Teléfonos inalámbricos

Si el rendimiento de su red inalámbrica sigue afectado después de tener en cuenta los aspectos mencionados anteriormente, y usted tiene un teléfono inalámbrico:

- Pruebe a alejar los teléfonos inalámbricos de enrutadores inalámbricos (o puntos de acceso) y de sus ordenadores con equipamiento inalámbrico.
- Desconecte y extraiga la batería de todos los teléfonos inalámbricos que operen dentro de la banda de 2,4 GHz (consulte la información del fabricante). Si se solventa el problema de esta forma, su teléfono probablemente esté causando interferencias.
- Si su teléfono permite la selección de canales, modifique el canal del teléfono para situarlo en el canal más alejado de su red inalámbrica. Por ejemplo, sitúe el teléfono en el canal 1 y su router inalámbrico (o punto de acceso) en el canal 11. Consulte el manual del usuario de su teléfono para obtener instrucciones detalladas.
- En caso necesario, considere la posibilidad de cambiar su teléfono inalámbrico por uno de 900 MHz o 5 GHz.

4. Seleccionar el canal “más tranquilo” para su red inalámbrica

En lugares en los que hay viviendas y oficinas cercanas, como por ejemplo, edificios de apartamentos o complejos de oficinas, es posible que existan redes inalámbricas en los alrededores que puedan entrar en conflicto con la suya.

Emplee la capacidad de inspección de la ubicación de la utilidad de LAN inalámbrica de su adaptador inalámbrico para localizar otras redes inalámbricas disponibles (véase el manual del adaptador inalámbrico), y coloque su router inalámbrico (o punto de acceso) y ordenadores en un canal lo más alejado posible del resto de redes.

Anexo B: Factores importantes de colocación e instalación

Pruebe con más de uno de los canales disponibles con el fin de descubrir la conexión más nítida y de evitar las interferencias de teléfonos inalámbricos cercanos o de otros dispositivos inalámbricos. Para los productos de interconexión en red inalámbrica de Belkin, utilice la información detallada de Inspección de la Ubicación y de canales inalámbricos incluida en su Guía del Usuario

Estas instrucciones deberán permitirle cubrir la zona más extensa posible con su router inalámbrico (o punto de acceso). En caso de que necesite abarcar un área más amplia, le recomendamos el Extensor de Alcance Inalámbrico/Punto de Acceso de Belkin.

5. Conexiones seguras, VPN y AOL

Las conexiones seguras requieren normalmente un nombre de usuario y una contraseña y se utilizan cuando la seguridad es importante. Las conexiones seguras incluyen:

- Conexiones de red virtual privada (VPN), utilizadas con frecuencia para conectar a distancia con una red de oficina
- El programa "Bring Your Own Access" (trae tu propio acceso) de America Online (AOL), que le permite emplear AOL a través de la banda ancha proporcionada por otro servicio por cable o DSL
- La mayoría de las páginas-web de servicios bancarios on-line
- Muchas páginas web comerciales requieren un nombre de usuario y una contraseña para acceder a su cuenta

Las conexiones seguras pueden verse interrumpidas por una configuración de gestión de la alimentación del ordenador que le haga pasar al modo de suspensión. La solución más sencilla para evitarlo es conectar de nuevo ejecutando otra vez el software de VPN o AOL, o accediendo de nuevo al sitio web seguro.

Una segunda alternativa consiste en modificar las configuraciones de gestión de la alimentación de su ordenador, de forma que no pase al modo de suspensión; no obstante, esto puede no ser apropiado para ordenadores portátiles. Para modificar su configuración de gestión de la alimentación en Windows, consulte "Power Options" (Opciones de Alimentación) en el Panel de Control. Si continúa teniendo dificultades con conexiones seguras, VPNs y AOL, revise los anteriores pasos para asegurarse de haber tratado estos temas.

1

2

3

4

5

6

7

8

9

10

11

sección

Anexo B: Factores importantes de colocación e instalación

Declaración de la FCC (Comisión de comunicaciones de EE.UU.)

DECLARACIÓN DE CONFORMIDAD CON LAS NORMATIVAS DE LA FCC SOBRE COMPATIBILIDAD ELECTROMAGNÉTICA

Nosotros, Belkin International, Inc., con sede en 501 West Walnut Street, Compton, CA 90220 (EE.UU.), declaramos bajo nuestra sola responsabilidad que el producto:

F5D7632uk4A

al que hace referencia la presente declaración, cumple con la sección 15 de las normativas de la FCC. Su utilización está sujeta a las siguientes dos condiciones: (1) este dispositivo no debe provocar interferencias nocivas y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan provocar un funcionamiento no deseado.

Advertencia: Exposición a las radiaciones de radiofrecuencia.

La energía de salida emitida por este dispositivo se encuentra muy por debajo de los límites de exposición a radiofrecuencias. No obstante, el dispositivo será empleado de tal forma que se minimice la posibilidad de contacto humano durante el funcionamiento normal. Cuando se conecta una antena externa al dispositivo, dicha antena deberá ser colocada de tal manera que se minimice la posibilidad de contacto humano durante el funcionamiento normal. Con el fin de evitar la posibilidad de superar los límites de exposición a radiofrecuencias establecidos por la FCC, la proximidad del ser humano a la antena no deberá ser inferior a los 20 cm durante el funcionamiento normal.

Declaración sobre interferencias de la Federal Communications Commission (FCC, Comisión de comunicaciones de EEUU)

Las pruebas realizadas con este equipo dan como resultado el cumplimiento con los límites establecidos para un dispositivo digital de la clase B, de acuerdo a la sección 15 de las normativas de la FCC. Los límites se establecen con el fin de proporcionar una protección razonable contra interferencias nocivas en zonas residenciales. Este equipo genera, emplea y puede irradiar energía de radiofrecuencia. Si este equipo provoca interferencias nocivas en la recepción de radio y televisión, las cuales se pueden determinar encendiendo y apagando seguidamente el dispositivo, el mismo usuario puede intentar corregir dichas interferencias tomando una o más de las siguientes medidas:

- Reorientar o colocar en otro lugar la antena de recepción.
- Aumentar la distancia entre el equipo y el receptor.
- Conectar el equipo a la toma de un circuito distinto de aquel al que está conectado el receptor.
- Solicitar la ayuda del vendedor o de un técnico experto en radiotelevisión.

Modificaciones

La FCC exige que el usuario sea notificado de que cualquier cambio o modificación del presente dispositivo que no sea aprobado expresamente por Belkin International, Inc. podría invalidar el derecho del usuario para utilizar este equipo.

Canadá - Industria de Canadá (IC)

La radioemisión inalámbrica de este dispositivo cumple con las especificaciones RSS 139 & RSS 210 de la Industria de Canadá. Este aparato digital de la Clase B cumple con la norma canadiense ICES-003. This Class B digital apparatus complies with Canadian ICES-003.

Este dispositivo digital de la Clase B cumple la norma canadiense NMB-003.

Europa - Declaración de la Unión Europea

Los productos de radioemisión con la indicación CE 0682 ó CE cumplen con la Directiva R&TTE (1995/5/CE) de la Comisión de la Comunidad Europea.

El cumplimiento de esta directiva implica la conformidad con las siguientes Normas Europeas (entre paréntesis

se encuentran los estándares internacionales equivalentes).

- EN 60950 (IEC60950) – Seguridad de los productos
 - EN 300 328 Requisitos técnicos para equipos de radioemisión
 - ETS 300 826 Requisitos generales de la EMC para equipos de radioemisión
- Para determinar el tipo de transmisor, compruebe la etiqueta de identificación de su producto Belkin.

Los productos con la indicación CE cumplen con la directiva EMC (89/336/CEE) y la Directiva de Bajo Voltaje

(72/23/CEE) establecidas por la Comisión de la Comunidad Europea. El cumplimiento de estas directivas implica la conformidad con las siguientes Normas Europeas (entre paréntesis se encuentran las normativas internacionales equivalentes).

- EN 55022 (CISPR 22) – Interferencias electromagnéticas
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11)- Inmunidad electromagnética
- EN 61000-3-2 (IEC610000-3-2) - Movimiento armónico de la línea eléctrica
- EN 61000-3-3 (IEC610000) – Fluctuaciones de la línea eléctrica
- EN 60950 (IEC60950) – Seguridad de los productos

Los productos que contienen el radiotransmisor llevan la etiqueta CE 0682 o CE y es posible que lleven asimismo el logotipo CE.

1

2

3

4

5

6

7

8

9

10

11

Garantía de por vida del producto de Belkin International, Inc.

La cobertura de la presente garantía.

Belkin International, Inc otorga una garantía al comprador original según la cual el producto no tendrá defectos en cuanto a diseño, montaje, materiales o mano de obra.

Cuál es el período de cobertura.

Belkin International, Inc. otorga una garantía a su producto durante toda su vida útil.

¿Cómo resolveremos los problemas?

Garantía del producto.

Belkin reparará o sustituirá, según decida, cualquier producto defectuoso sin ningún tipo de cargo (excepto los gastos de envío del producto).

¿Qué excluye la presente garantía?

Todas las garantías mencionadas anteriormente resultarán nulas y sin valor alguno si el producto Belkin no se le proporciona a Belkin International, Inc para su inspección bajo requerimiento de Belkin con cargo al comprador únicamente, o si Belkin International, Inc determina que el producto Belkin se ha instalado de un modo inadecuado, alterado de algún modo o forzado. La garantía del producto de Belkin no lo protege de los desastres naturales tales como inundaciones, terremotos, rayos, vandalismo, robos, mal uso, erosión, agotamiento, desuso o daño a causa de interrupciones en la alimentación (p. ej. apagones) modificación o alteración no autorizadas de programas o sistemas.

Para obtener asistencia.

Para obtener asistencia sobre algún producto de Belkin, debe seguir los siguientes pasos:

1. Póngase en contacto con Belkin International, Inc en 501 W. Walnut St., Compton CA 90220, a la atención de: Servicio de atención al cliente, o llame al teléfono (800)-223-5546, en un plazo de 15 días desde el momento de la incidencia. Tenga preparada la siguiente información:
 - a. El número de artículo del producto Belkin.
 - b. El lugar de compra del producto.
 - c. Cuándo compró el producto.
 - d. Copia de la factura original.
2. El servicio de atención al cliente de Belkin le informará sobre cómo enviar la factura y el producto Belkin y sobre cómo proceder con su reclamación.

Belkin International, Inc se reserva el derecho a revisar el producto Belkin dañado. Todos los gastos de envío del producto Belkin a Belkin International, Inc para su inspección correrán a cargo del comprador exclusivamente. Si Belkin determina, según su propio criterio, que resulta poco práctico el envío de los equipos dañados



a Belkin International, Inc, Belkin podrá designar, según su propio criterio, una empresa de reparación de equipos para que inspeccione y estime el coste de la reparación de dichos equipos. Los gastos, si existen, de envío del equipo a dicha empresa de reparaciones, y de su valoración, correrán exclusivamente a cargo del comprador. El equipo dañado deberá permanecer disponible para su inspección hasta que haya finalizado la reclamación. Si se solucionan las reclamaciones por negociación, Belkin International, Inc se reserva el derecho a subrogar la garantía por cualquier póliza de seguros del comprador.

Relación de la garantía con la legislación estatal.

ESTA GARANTÍA CONTIENE LA GARANTÍA EXCLUSIVA DE BELKIN INTERNATIONAL INC., NO EXISTE NINGÚN OTRO TIPO DE GARANTÍAS, EXPRESAS O, EXCEPTO LAS REQUERIDAS POR LA LEY, IMPLÍCITAS, INCLUYENDO LA GARANTÍA O CONDICIÓN IMPLÍCITA DE CALIDAD, COMERCIABILIDAD E IDONEIDAD PARA UN FIN PARTICULAR, Y TALES GARANTÍAS, EN CASO DE EXISTIR, ESTÁN LIMITADAS EN DURACIÓN A LOS TÉRMINOS DE LA PRESENTE GARANTÍA.

Algunas jurisdicciones no permiten la limitación de la duración de las garantías implícitas, por lo que cabe la posibilidad de que las anteriores limitaciones no le afecten.

EN NINGÚN CASO BELKIN INTERNATIONAL INC. SERÁ RESPONSABLE DE LOS DAÑOS IMPREVISTOS, ESPECIALES, DIRECTOS, INDIRECTOS, CONSECUENTES O MÚLTIPLES, INCLUYENDO ENTRE OTROS LA PÉRDIDA DE NEGOCIO O BENEFICIOS QUE PUEDA SURGIR DE LA VENTA O EL EMPLEO DE CUALQUIER PRODUCTO BELKIN, INCLUSO SI BELKIN HA SIDO INFORMADA DE LA POSIBILIDAD DE DICHOS DAÑOS.

Esta garantía le proporciona derechos legales específicos y también podría beneficiarse de otros derechos que pueden variar entre las distintas jurisdicciones. Ciertas jurisdicciones no permiten la exclusión o limitación de daños fortuitos, consiguientes o de otro tipo, por lo que tal vez las limitaciones mencionadas no le afecten.

Para obtener información sobre el desecho del producto remítase a <http://environmental.belkin.com>



PARA UTILIZAR EN **AT** **BE** **CY** **CZ** **DK** **EE** **FI**
IT **LV** **LT** **LU** **MT** **NL** **PL** **PT** **SK** **SI**
NO **CH** **BG** **RO** **TR**

FUNCIONA EN LOS CANALES 1-13

Uso restringido en ciertos países.....Equipamiento Clase 2

BELKIN.

EC Declaration of Conformity to R&TTE Directive 1999/5/EC

Manufacturer : BELKIN LTD,
EXPRESS BUSINESS PARK,
SHIPTON WAY
,RUSHDEN
NN10 6GL ENGLAND

Representative : Belkin Ltd
(residing in the EC
holding the TCF)

Product / Apparatus : ADSL Modem/Wireless G Router

Type Number : F5D7632-4

Variants include : All Country Variants

Declaration

I declare that above product conforms to all the applicable requirements of EU Directive 1999/5/EC and is CE-marked accordingly:

Article 3.1a: (Standard(s)) used to show compliance with LVD, 73/23/EEC:

IEC 60950-1 2001 Compliant Test Report No: LD931001H03 03 NOV 04

Article 3.1b: (Standard(s)) used to show compliance with EMC Directive, 89/336/EEC:

EN301 489-1 V1.4.1 (2002-08);EN 301 489-17 V1.2.1 (2002-08) Compliant Test Report No:RM931001H03

Article 3.2: Standard(s) used to show compliance:

...EN300 328 V1.4.1 (2003-04)..... Compliant Test Report No:RC93100H03

Signature : 

Name : K Simpson

Title : European Regulatory Compliance Manager

Date : 20 MAR 2006

BELKIN®

Módem ADSL2+ con router inalámbrico G

BELKIN®

www.belkin.com

Asistencia técnica de Belkin

R.U.: 0845 607 77 87

Europa: www.belkin.com/support

Belkin Ltd.

Express Business Park
Shipton Way, Rushden
NN10 6GL, Reino Unido
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin SAS

130 rue de Silly
92100 Boulogne-Billancourt,
Francia
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH

Hanebergstrasse 2
80637 Múnich
Alemania
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

Belkin Iberia

C/ Anabel Segura, 10 planta baja, Of. 2
28108, Alcobendas, Madrid
España
+34 91 791 23 00
+34 91 490 23 35 fax

Belkin Italy & Greece

Via Carducci, 7
Milán 20123
Italia
+39 02 862 719
+39 02 862 719 fax

Belkin B.V.

Boeing Avenue 333
1119 PH Schiphol-Rijk,
Países Bajos
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

© 2007 Belkin International, Inc. Todos los derechos reservados. Todos los nombres comerciales son marcas registradas de los respectivos fabricantes enumerados. Mac, Mac OS, Apple y AirPort son marcas registradas de Apple Computer, Inc., registrado en EE.UU. y otros países. Windows, NT, Microsoft y Windows Vista son marcas registradas o marcas comerciales de Microsoft Corporation registradas en Estados Unidos y otros países.

P74725ea_A

BELKIN®

Modem ADSL2+ con Router G Wireless

EN

FR

DE

NL

ES

IT



Manuale d'uso

F5D7632ea4A

Indice

1. Introduzione	1
Caratteristiche del prodotto	1
I vantaggi di una rete domestica	3
I vantaggi di una rete wireless Belkin	3
2. Materiale necessario	4
Contenuto della confezione	4
Requisiti di sistema	4
Requisiti di sistema per il software di installazione guidata ..	4
Impostazioni di connessione a Internet	4
3. Conoscere il Router	5
4. Collegamento e configurazione del Router	8
Fase 1A: Collegamento dell'hardware – Leggere la guida di installazione rapida	8
Fase 1B: Sostituzione di un altro modem / modem router ...	9
Fase 2: Installare il router – Avviare il programma di installazione guidata	10
5. Configurazione manuale del router	13
Per una migliore comprensione dell'interfaccia utente avanzata basata sul web	13
Modifica delle impostazioni di sistema	15
Elenco dei client DHCP	16
Internet WAN	17
Connection Type (Tipo di connessione)	17
Wireless	23
Crittografia/Protezione	25
Estensione senza fili del range e bridge	35
Firewall	37
Programmi di utilità	43
6. Configurazione manuale degli adattatori di rete	51
7. Impostazioni del browser web consigliate	55
8. Risoluzione delle anomalie	57
9. Informazioni di assistenza tecnica	68
10. Introduzione.....	69
Allegato A: Glossario	69
Allegato B: Considerazioni importanti per il posizionamento e la configurazione	74
11 Informazioni	77

Grazie per aver scelto il Modem ADSL2+ con Router Wireless G Belkin (il router). Con questo nuovo router sarà possibile condividere in pochi minuti una stessa connessione ad Internet e collegare in rete diversi computer. Di seguito è riportato un elenco delle caratteristiche che fanno di questo nuovo router una soluzione ideale per la creazione di una rete in casa o in un piccolo ufficio. Vi invitiamo a leggere con attenzione questo manuale, in particolare l'Allegato B intitolato "Considerazioni importanti per il posizionamento e la configurazione".

Caratteristiche del prodotto

Compatibilità con i PC e i computer Mac®

Il router supporta diversi ambienti di rete, tra cui Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP, Vista ed altri ancora. Il suo utilizzo richiede la disponibilità di un browser Internet e di un adattatore di rete in grado di supportare la modalità TCP/IP (la lingua standard di Internet).

LED di indicazione di stato sul pannello anteriore

I LED illuminati sul pannello anteriore del router indicano le funzioni in corso e consentono, con un semplice colpo d'occhio, di conoscere lo stato di collegamento del router ad Internet. Questa funzione elimina la necessità di eseguire altre procedure avanzate di monitoraggio stato e software.

Interfaccia utente avanzata basata sul web

Tutte le funzioni avanzate del router si possono impostare facilmente tramite il browser web, senza installare altro software nel computer. Non ci sono dischetti da installare o da conservare e le funzioni di installazione possono essere modificate ed eseguite in modo rapido e semplice da qualsiasi computer collegato in rete.

Switch a 4 porte 10/100 incorporato

In questo router è integrato uno switch di rete a 4 porte, per consentire la condivisione di stampanti, dati e file MP3, foto digitali e ancora di più tra diversi computer cablati. Lo switch prevede una funzione di rilevamento automatico, che consente di regolare la velocità dei dispositivi collegati. Inoltre, trasferisce dati fra i computer ed Internet contemporaneamente, senza interruzioni e senza consumare risorse.

Access point wireless integrato 802.11g

La tecnologia 802.11g è una nuova ed entusiasmante tecnologia wireless che consente la trasmissione dei dati a 54Mbps, quasi cinque volte più velocemente rispetto allo standard 802.11b.

Il protocollo integrato DHCP (Dynamic Host Configuration Protocol)

Il protocollo DHCP (Dynamic Host Configuration Protocol) integrato nella scheda semplifica al massimo la procedura di connessione di una rete. Il server DHCP assegna automaticamente gli indirizzi IP a ciascun computer, eliminando l'esigenza di qualsiasi complicata predisposizione della rete.

Condivisione dell'indirizzo IP NAT

Il Router implementa il servizio Network Address Translation (NAT) per condividere l'unico indirizzo IP assegnato all'utente dal Internet Service Provider, consentendo di risparmiare il costo di eventuali indirizzi IP supplementari per il proprio account di servizio Internet.

La protezione SPI Firewall

Il router è dotato di una protezione firewall che preserva la rete da una vasta gamma di attacchi comuni degli hacker, tra cui IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP with zero length, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect e fragment flooding.

Il filtro indirizzi MAC

Per maggiore sicurezza, è possibile creare un elenco di indirizzi MAC (identificatori unici client) ai quali consentire l'accesso alla propria rete. Ad ogni computer corrisponde un indirizzo MAC specifico, è sufficiente inserire questi indirizzi MAC in un elenco tramite l'interfaccia utente basata sul Web e controllare in questo modo l'accesso alla rete.

Compatibilità UPnP (Universal Plug-and-Play)

La tecnologia UPnP (Universal Plug-and-Play) è in grado di offrire un funzionamento continuo delle opzioni di trasmissione di messaggi vocali, video, giochi e di altre applicazioni conformi agli standard UPnP.

Supporto del servizio VPN Pass-Through

Per chi desidera collegarsi alla propria rete in ufficio da casa utilizzando una connessione VPN, il router consente al computer abilitato al servizio VPN di passare attraverso il router ed arrivare alla rete dell'ufficio.

I vantaggi di una rete domestica

Dopo aver seguito le semplici istruzioni per l'installazione, la rete domestica Belkin vi permetterà di:

- condividere la connessione ad alta velocità a Internet con tutti i computer di casa
- condividere risorse, quali file e dischi rigidi, tra tutti i computer collegati alla rete domestica
- Condividere una sola stampante tra tutta la famiglia
- Condividere documenti, musica, video e fotografie digitali
- Memorizzare, recuperare e copiare i file da un computer all'altro
- giocare online, controllare la posta elettronica e chattare da diversi computer contemporaneamente.

I vantaggi di una rete wireless Belkin

Mobilità – la “stanza per il computer” non è più necessaria: da oggi si può lavorare da un portatile o da un computer desktop collegato in rete da un qualsiasi punto all'interno della propria copertura wireless

Installazione semplice – il programma di impostazione guidata facilita la procedura di configurazione

Versatilità – dopo la configurazione è possibile accedere a stampanti, computer e altri dispositivi di rete dovunque vi troviate all'interno della casa

Facilità di espansione - la vasta copertura dei prodotti di rete Belkin permette di espandere la rete, per comprendere dispositivi quali stampanti e console per videogame

Niente cavi - non è più necessario spendere soldi e perdere tempo per cablare la propria abitazione o l'ufficio per creare una connessione Ethernet

Accettazione incondizionata di altre marche - si ha la possibilità di scegliere tra una vasta gamma di prodotti di rete interoperabili

Materiale necessario

Contenuto della confezione

- Modem ADSL2+ con Router G Wireless
- Cavo telefonico RJ11 - Grigio
- Cavo di rete RJ45 Ethernet - Giallo
- Microfiltro ADSL*
- Adattatore di corrente
- Manuale d'uso Belkin e software di installazione guidata su CD-ROM

*il microfiltro ADSL varia di Paese in Paese. Se non fosse compreso nella fornitura, sarà necessario acquistarne uno.

Requisiti del sistema

- Un servizio ADSL attivo con una presa telefonica a muro per collegare il router
- Almeno un computer con una scheda di interfaccia di rete (NIC) e un browser web installato e configurato correttamente
- Protocollo di rete TCP/IP installato su ogni computer e collegato al router
- Nessun altro server DHCP sulla propria rete locale che assegni gli indirizzi IP ai computer e agli altri dispositivi

Requisiti di sistema per il software di installazione guidata

- Un server dotato di Windows 2000, XP, o Vista™
- Processore da 500 MHz e RAM da 128 MB
- Browser Internet

Impostazioni di connessione a Internet

Il programma di installazione guidata contiene un database di provider di servizi Internet (ISP) in diversi paesi che vi aiuteranno a configurare velocemente il modem router. Se il vostro provider di servizi Internet non figura nell'elenco, raccogliere le seguenti informazioni fornite dal vostro provider prima di installare il modem router.

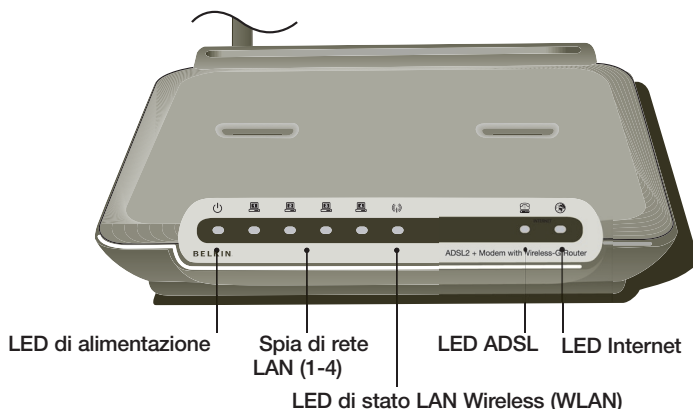
- Protocollo di connessione a Internet: (PPPoE, PPPoA, IP dinamico, IP statico)
- Metodo Multiplexing o incapsulamento: (LLC oppure VC MUX)
- Circuito virtuale: VPI (Virtual Path Identifier) _____
(un numero tra 0 e 255)
- VCI (Virtual Channel Identifier) _____
(un numero tra 1 e 65535)
- Per utenti PPPoE e PPPoA: Nome utente _____
e password _____ dell'account ADSL
- Per utenti con IP statico: Indirizzo IP ____ . ____ . ____ . ____
Subnet Mask ____ . ____ . ____ . ____
Server Gateway predefinito ____ . ____ . ____ . ____
- Indirizzo IP del Domain Name Server ____ . ____ . ____ . ____
_ . ____ (se assegnato dal proprio ISP)

Conoscere il Router

Il router è stato progettato per essere posizionato sulla scrivania. Tutti i cavi escono dal retro del router, consentendo una migliore organizzazione e utilizzabilità. Gli indicatori LED sono facilmente visibili sulla parte anteriore del router per fornire informazioni sull'attività della rete e sul suo stato.

Pannello anteriore

Pannello anteriore – L'illustrazione rappresenta il pannello anteriore del router.






Indicatori LED

Il router è dotato di nove LED sul pannello frontale, come è descritto nella tabella della pagina seguente (da sinistra verso destra)

1
2
3
4
5
6
7
8
9
10
11

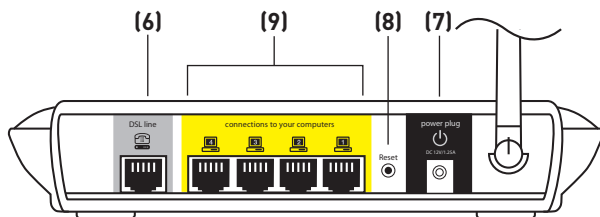
sezione

Conoscere il Router

LED	Colore	Stato	Descrizione
ADSL			
	Verde	SPENTO	Spento o linea ADSL fisicamente scollegata
		Lampeggiante	Collegamento o preparazione in corso
		Fisso	Connessione ADSL attiva
Wireless			
	Verde	SPENTO	Spento o segnale radio assente (scheda WLAN non disponibile o non funzionante)
		Lampeggiante	Il traffico usa l'interfaccia LAN wireless
		Fissa	Interfaccia LAN wireless pronta per il collegamento
Internet			
	Verde	SPENTO	Connessione Internet assente
		Lampeggiante	Trasmissione o ricezione dati in corso
		Fisso	Collegamento a Internet in corso
da LAN 1 a LAN 4			
LAN 1-4	Verde	SPENTO	Alimentazione assente oppure collegamento a Ethernet non attivo
		Lampeggiante	Collegamento alla rete Ethernet attivo e dati utente comunicano tramite la porta Ethernet
		Fisso	Collegamento alla rete Ethernet attivo
Alimentazione			
	Verde	SPENTO	Spento
		Fisso	Alimentato

Pannello posteriore

La seguente illustrazione rappresenta il pannello posteriore del router.



Presa — A questa presa viene collegato l'adattatore di alimentazione fornito. L'utilizzo di un tipo di adattatore di alimentazione sbagliato può danneggiare il router.

Porte Ethernet —Le porte Ethernet sono RJ45, 10/100 auto-negoziante. Queste porte sono contrassegnate con i numeri da 1 a 4 e corrispondono ai LED numerati presenti sulla parte anteriore del router. I propri computer abilitati alla connessione in rete e tutti gli altri dispositivi di rete vanno collegati ad una di queste porte.

Linea ADSL —Questa porta consente di impostare il collegamento con la propria linea ADSL. La linea ADSL deve essere collegata a questa porta.

Pulsante Reset—Il pulsante "Reset" viene utilizzato in alcuni casi rari, quando il router funziona in maniera inadeguata. Resettando il router, si ripristina la normale modalità di funzionamento del router pur mantenendo le impostazioni programmate. Il pulsante di reset consente anche di ripristinare le impostazioni predefinite. L'opzione di ripristino si può utilizzare ad esempio nel caso sia stata dimenticata la password cliente.

a. Reset del router

Premere e tenere premuto il pulsante di reset per un secondo, quindi lasciarlo. Quando la spia "Power/Ready" (alimentazione/pronto) è di nuovo fissa, significa che l'operazione di reset è stata completata.

b. Ripristino delle impostazioni predefinite

Premere e tenere premuto il pulsante di reset per 20 secondi, quindi lasciarlo. Quando la spia "Power/Ready" (alimentazione/pronto) è di nuovo fissa, significa che l'operazione di reset è stata completata.

Collegamento e configurazione del Router

Installazione guidata

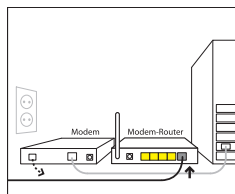
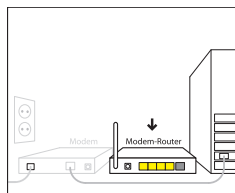
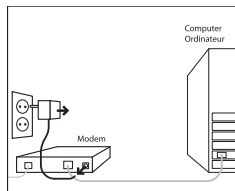
Belkin ha messo a disposizione degli utenti un programma di installazione guidata, con lo scopo di facilitare l'installazione del router. Questo programma consente di installare e utilizzare in pochi minuti il router. Il programma di installazione guidata prevede che il proprio computer funzioni con i programmi Windows 2000, XP o Vista™, che sia collegato direttamente alla linea ADSL e che la connessione a Internet sia attiva e funzionante al momento dell'installazione. In caso contrario, per configurare il router, vedere il capitolo "Metodo di configurazione alternativo" di questo manuale. Inoltre, il router deve essere installato seguendo le indicazioni del capitolo "Metodo di installazione alternativo" di questo manuale se si utilizza un sistema operativo diverso da Windows 2000, XP, Vista o Mac OS X.

Fase 1A: Collegamento dell'hardware – Leggere la guida di installazione rapida

Prima installazione del Router

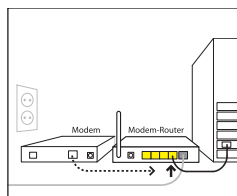
Eseguire le seguenti operazioni solo se NON si dispone già di un modem. Se si dispone già di un modem, passare alla sezione successiva "Sostituzione di un altro modem / modem router" a pagina 9.

- 1A.1** Rimuovere il router dalla confezione e collocarlo affianco al computer. Alzare l'antenna del router.
- 1A.2** Prendere il cavo RJ-45 giallo fornito insieme al router. Collegarlo a una porta gialla marcata "Wired Computers" sul retro del router. Quindi collegare l'altra estremità alla porta di rete sul retro del computer. [Insert Ethernet logo]
- 1A.3** Prendere il cavo telefonico RJ-11 grigio fornito insieme al modem router. Collegarlo alla porta grigia marcata "DSL" sul retro del modem router. Collegare l'altra estremità alla linea ADSL (una presa a muro o uno splitter ADSL).



Nota bene: Alcune linee ADSL richiedono l'uso di un microfiltro. Il proprio fornitore del servizio ADSL sarà in grado di dirvi se ne avete bisogno. Il modem router è venduto insieme al microfiltro in quelle regioni dove occorre utilizzarlo. Per sapere è necessario un microfiltro, consultare il manuale d'uso fornito dalla società che eroga il servizio ADSL.

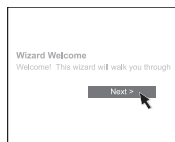
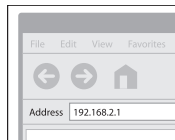
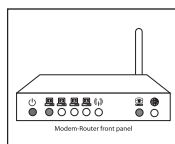
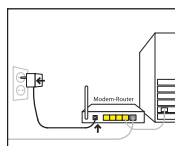
- 1A.4** Collegare l'alimentatore del modem-router alla porta nera sul retro indicata con la scritta "Power". Attendere 20 secondi affinché il modem si avvii. Osservare il display sulla parte anteriore del router. Verificare che le spie "Wired" e "Modem-Router" siano accese ed emettano una luce verde. In caso contrario, controllare di nuovo i collegamenti.



Fase 1B: Sostituzione di un altro modem / modem router

Eseguire le seguenti operazioni se si utilizza il nuovo router per sostituire un altro modem o un altro modem router.

- 1B.1** **Unpack** Rimuovere il modem router dalla confezione e collocarlo affianco al vecchio modem.. Alzare l' antenna del router. Scollegare l'alimentatore del vecchio modem.
- 1B.2** Prendere il cavo di rete che collega il vecchio modem al computer. Scollegare questo cavo dal vecchio modem e inserirlo in una delle porte gialle marcate "Wired Computers" sul retro del nuovo router.
- 1B.3** Prendere il cavo che collega il vecchio modem alla presa a muro ADSL. Scollegarlo dal vecchio modem e collegarlo alla porta grigia marcata "DSL" sul retro del modem router.
- 1B.4** Collegare l'alimentatore del modem-router alla porta nera sul retro indicata con la scritta "Power".
- 1B.5** **Attendere** 20 secondi affinché il modem si avvii. Osservare il display sulla parte anteriore del router. Accertarsi che i LED "ADSL" e "LAN" siano illuminati. In caso contrario, controllare di nuovo i collegamenti.



1
2
3
4

sezione

5

6

7

8

9

10

11

Fase 2: Installare il router Avviare il programma di installazione guidata

2.1 Chiudere tutti i programmi attualmente in esecuzione nel computer. Disattivare qualsiasi protezione firewall o connessione a Internet che condivide uno stesso software nel computer.

2.2 Inserire il CD nel computer. Il sistema eseguirà automaticamente il programma di installazione guidata entro 15 secondi. Fare clic su “Go” per avviare l’installazione guidata. Seguire le istruzioni qui riportate.

IMPORTANTE: Eseguire il programma di installazione guidata dal computer che è collegato direttamente al router della fase 1A.2.

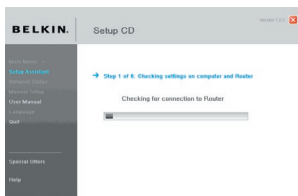
Avviso per gli utenti Windows: Se il programma di installazione guidata non si dovesse avviare automaticamente, aprire l’unità CD-ROM da “Risorse del computer” e fare doppio clic sul file “SetupAssistant” per avviare l’installazione guidata.

2.3 Selezione del paese. Selezionare il proprio paese dall’elenco a discesa. Fare clic su “Begin” (Inizia) per continuare.

2.4 Schermata di conferma. Verificare di aver eseguito tutte le operazioni indicate nella guida di installazione rapida e mettere un segno di spunta nella casella alla destra della freccia. Fare clic su “Next” (Avanti) per continuare.

2.5 Finestra di avanzamento. Il programma visualizza una finestra di avanzamento ogni volta che viene eseguito un passaggio nel corso dell’installazione.

2.6 Verifica delle impostazioni. Il programma di installazione guidata a questo punto procederà con la verifica delle impostazioni del computer e la raccolta delle informazioni necessarie per completare la connessione del router a Internet.



2.7 Verifica del collegamento dell'hardware
Il programma di installazione guidata ora controllerà il collegamento dell'hardware.

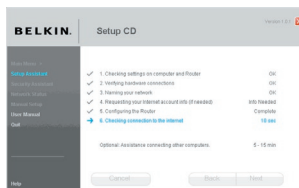
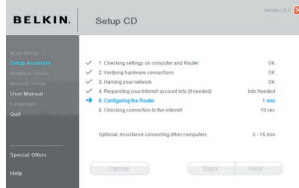
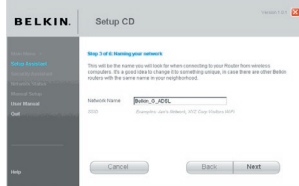
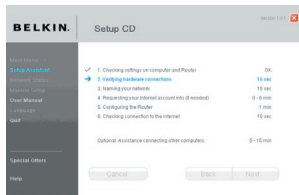
2.8 Denominazione della rete wireless
Il programma di installazione guidata visualizzerà il nome predefinito della rete wireless o Service Set Identifier (SSID). Questo è il nome della rete wireless alla quale i computer o i dispositivi con adattatori di rete wireless si connetteranno. È possibile utilizzare il nome predefinito o scegliere qualcosa di più personale. Annotarsi il nome scelto in modo da non dimenticarlo in futuro. Fare clic su "Next" (Avanti) per continuare.

2.9 Richiesta delle informazioni sull'account Internet (se necessario).
Se il proprio account Internet richiede un nome utente e una password per il login, apparirà una schermata simile a quella illustrata qui sotto. Selezionare la nazione o il provider dal menu a discesa.

2.10 Configurazione del router.
Il programma di installazione guidata ora configurerà il router inviando i dati al router e riavviandolo. Attendere le istruzioni a video.

Nota bene: Non scollegare i cavi né disattivare il router durante la procedura di riavvio. Così facendo, si danneggia il funzionamento del router.

2.11 Verifica della connessione a Internet
L'operazione è quasi terminata. Il programma di installazione guidata ora controllerà la connessione a Internet.



1
2
3
4
5
6
7
8
9
10
11

Congratulazioni

La procedura di installazione del router è terminata. Quando il router potrà connettersi a Internet, apparirà la schermata “Congratulazioni”. Ora è possibile navigare in rete aprendo il browser e visitando qualsiasi sito Internet.

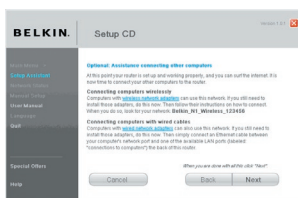
Cliccando su “Next” (Avanti) nel programma di installazione guidata, è possibile configurare altri computer cablati e wireless e connetterli a Internet. Se si decide di aggiungere altri computer in un momento successivo, selezionare “Exit the Assistant” (Esci dal programma) e fare clic su “Next” (Avanti).



Rilevazione e risoluzione delle anomalie

Se il programma di installazione guidata non riesce a collegarsi a Internet, apparirà questa schermata. Seguire le istruzioni a video per risolvere il problema.

2.12 Opzione: Assistenza al collegamento di altri computer. Questa operazione opzionale vi consente di collegare altri computer cablati o wireless alla vostra rete. Seguire le istruzioni a video. volta verificato che i computer cablati e wireless sono collegati in modo corretto, la rete è configurata e funzionante. Ora è possibile navigare in rete. Fare clic su “Next” (Avanti) per tornare al menu principale.



Configurazione manuale del router

1
2
3
4
5
6
7
8
9
10
11

sezione

Per una migliore comprensione dell'interfaccia utente basata sul web

Nella pagina principale viene riportata una breve sintesi dello stato e delle impostazioni del router. Da questa pagina è possibile accedere a tutte le pagine di impostazione avanzata.

Utilizzo dell'interfaccia di gestione basata sul web

Una volta configurato il PC host, avviare l'interfaccia basata sul web e digitare l'indirizzo IP privato del router nel campo URL: "192.168.2.1" quindi fare clic su "Enter" (Invio).

The screenshot shows the 'Status' page of a router's web interface. The page is divided into several sections:

- Language:** Current Language: English, Available Languages: English, Deutsch, Français, Español.
- Version Info:** Firmware Version: 1.00.11, Boot Code Version: 1.0.37-8.7, Hardware: F309432-4.
- WAN Settings:** WAN MAC Address: 02:10:18:01:00:03, WAN IP: 172.19.85.106, Default Gateway: 205.185.141.127, Primary DNS Server: 205.185.144.145, Secondary DNS Server: (empty).
- System Statistics:** Type: Fast, Status: No Default, Data Rate(Kbps): 576 / 200, Noise margin (dB): 15.3 / 29.0, Output power (dBm): 11.8 / 15.3.
- Wireless Function:** Enabled, WLAN MAC Address: 00:17:3F:AD:82:1B, SSID: Serico_Gigaset_HMC_748218, Wireless Mode: 802.11g & 802.11b, Wireless Channel: 6, Security: Disabled.
- Advanced Features:** Firewall: Enabled, NAT: Enabled, UPnP: Disabled.

1. Link di navigazione rapida

Facendo clic su questi link è possibile passare direttamente a qualsiasi altra pagina dell'interfaccia utente del router. I link sono suddivisi per categorie logiche e raggruppati per schede, in questo modo si facilita la ricerca di una particolare impostazione. Facendo clic sul titolo di ogni scheda appare una breve descrizione delle funzioni della scheda scelta.

2. Pulsante Home

Il pulsante "Home" è presente in ogni pagina dell'interfaccia utente. Premendo questo pulsante si ritorna alla home page.

3. Pulsante Help

Il pulsante "Help" consente di accedere alle pagine guida del router. La guida è disponibile anche in molte pagine, è sufficiente fare clic su "more info" (maggiori informazioni) accanto ad alcune sezioni specifiche di ogni pagina.

4. Pulsante Login/Logout

Questo pulsante attiva e disattiva la connessione del router. Quando si è collegati al router, il pulsante riporta l'indicazione "Logout" (Disconnetti). Collegandosi al router si viene condotti in una pagina di connessione a parte dove viene richiesta una password. Una volta collegati al router, è possibile modificare le impostazioni. Una volta terminate le modifiche, per scollegarsi dal router fare clic sul pulsante "Logout" (Disconnetti). Per maggiori informazioni sulla connessione al router, vi rimandiamo al capitolo "Connessione al router".

5. Indicatore di stato Internet

Questo indicatore è presente in tutte le pagine del router ed ha lo scopo di indicare lo stato del collegamento al router. Quando il messaggio “connection OK” (connessione ok) è VERDE, significa che il router è collegato ad Internet. Quando il router non è collegato ad Internet, appare il messaggio “no connection” (nessuna connessione) in ROSSO. L'indicatore viene aggiornato automaticamente modificando le impostazioni del router.

6. LAN settings (Impostazioni LAN)

Visualizza le impostazioni della rete locale LAN (Local Area Network) del router. Per apportare delle modifiche fare clic sul link di navigazione rapida “LAN” nella parte sinistra dello schermo.

7. Features (Caratteristiche)

Visualizza lo stato del servizio NAT, della protezione firewall e delle opzioni wireless del router. Per apportare delle modifiche, è sufficiente fare clic su uno qualsiasi dei link o sul link “Quick Navigation” (Navigazione rapida) nella parte sinistra dello schermo.

8. Internet Settings (Impostazioni Internet)

Visualizza le impostazioni della sezione Internet/WAN del router che si collega ad Internet. Per apportare eventuali modifiche, è sufficiente fare clic sul link di navigazione rapida “Internet/WAN” nella parte sinistra dello schermo.

9. Version Info (Info versione)

Visualizza le informazioni relative alla versione del firmware, del bootcode, dell'hardware ed il numero di serie del router.

10. Page Name (Nome pagina)

Il nome che identifica la pagina in cui ci si trova. Questo manuale a volte farà riferimento alle pagine chiamandole per nome. Ad esempio “LAN > Impostazioni LAN” starà ad indicare la pagina “Impostazioni LAN”.

Modifica delle impostazioni LAN

Da qui possono essere visualizzate o modificate tutte le impostazioni per l'installazione della LAN interna del Router.

“LAN Settings” (Impostazioni LAN)

Facendo clic sul titolo della scheda LAN (A) si entra nella pagina di titolo della scheda LAN che contiene una rapida descrizione delle funzioni. Per visualizzare le impostazioni o modificare una qualsiasi delle impostazioni LAN, fare clic su “LAN Settings” (Impostazioni LAN) (B), o per visualizzare la lista dei computer collegati, fare clic su “DHCP client list” (Lista client DHCP) (C).

Indirizzo IP

Per “Indirizzo IP” si intende l’indirizzo IP interno del router. L’indirizzo IP predefinito è “192.168.2.1”. Per accedere all’interfaccia di impostazione avanzata, digitare l’indirizzo IP nell’apposita barra indirizzi del browser. Questo indirizzo, se necessario, può essere modificato. Per modificare l’indirizzo IP, digitare il nuovo indirizzo IP e fare clic su “Apply Changes” (Esegui modifiche). L’indirizzo IP scelto dovrebbe essere un IP non instradabile. Esempi di indirizzi IP non instradabili sono:

192.168.x.x (dove x indica qualsiasi cifra tra 0 e 255)

10.x.x.x (dove x indica qualsiasi cifra tra 0 e 255)

Subnet Mask (Maschera di sottorete)

Non è necessario modificare la subnet mask. Si tratta di un’opzione unica, avanzata, prevista dal router Belkin.

Server DHCP

La funzione server DHCP semplifica l'impostazione di una rete, in quanto gli indirizzi IP vengono assegnati automaticamente ad ogni computer nella rete. L'impostazione predefinita è "On" (Attiva). Il server DHCP può essere DISATTIVATO, se necessario, ma per farlo è necessario impostare manualmente un indirizzo IP statico per ogni computer in rete. Per disattivare il server DHCP, selezionare "Off" (Inattivo) e fare clic su "Apply Changes" (Esegui modifiche).

Pool di indirizzi IP

La gamma di indirizzi IP mette da parte l'assegnazione dinamica dei computer alla rete. Per modificare questa cifra, digitare un nuovo indirizzo IP di inizio e fine e facendo clic su "Apply Changes" (Esegui modifiche). L'indirizzo IP di partenza deve essere un numero inferiore rispetto all'indirizzo IP finale.

Lease Time

Il lasso di tempo durante il quale il server DHCP assegna un indirizzo IP a ogni computer. È consigliabile lasciare questo intervallo impostato su "Forever" (Per sempre). L'impostazione predefinita "Forever" (Per sempre) sta ad indicare che ogni volta che ad un computer verrà assegnato un indirizzo IP dal server DHCP, l'indirizzo IP per quel particolare computer non cambierà più. Impostando la disponibilità per degli intervalli minori, come un giorno o un'ora, gli indirizzi IP una volta trascorso quello specifico intervallo si liberano. Questo significa anche che l'indirizzo IP di un particolare computer potrebbe cambiare nel corso del tempo. Se fosse stata impostata una qualsiasi delle altre opzioni avanzate del router, tra cui DMZ o filtri IP client, queste dipenderebbero dall'indirizzo IP. Per questo motivo è bene che l'indirizzo IP non cambi.

Local Domain Name (Dominio locale)

Per la propria rete è possibile impostare un dominio locale (nome della rete). Questa impostazione non deve essere necessariamente modificata a meno che non vi sia un'esigenza specifica per farlo. Alla rete può essere assegnato un nome qualsiasi, come ad esempio "MY NETWORK" (LA MIA RETE).

DHCP Client List (Elenco dei Client DHCP)

È possibile visualizzare un elenco dei computer collegati alla rete. È possibile visualizzare l'indirizzo IP del computer, il nome di host (nome del computer in rete) e l'indirizzo MAC della scheda di interfaccia di rete NIC. Premendo il pulsante "Refresh" (Ripristina), l'elenco viene aggiornato. Nel caso fossero state fatte delle modifiche, l'elenco verrà aggiornato.

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing "Refresh" will update the list.

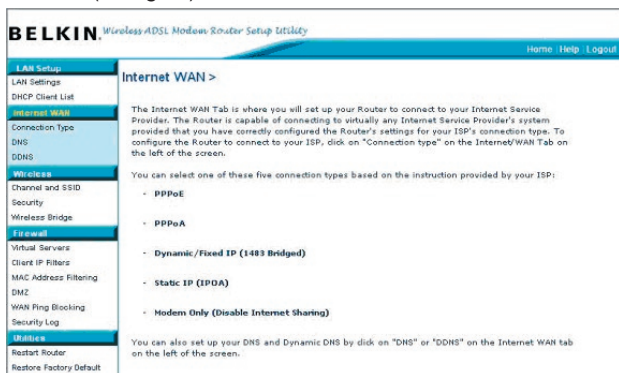
IP Address	Host Name	MAC Address
192.168.2.11	Ericd-XP	00-30-8D-3D-AB-09

[Refresh](#)

Internet WAN

Nella scheda "Internet WAN" è possibile impostare il router per potersi collegare al proprio provider Internet (ISP). Il router è in grado di collegarsi praticamente a qualsiasi sistema di provider ADSL, a condizione che le impostazioni siano state configurate correttamente per il tipo di connessione al provider desiderato. Le impostazioni di connessione sono fornite dal provider stesso.

Per configurare il router con le impostazioni indicate dal provider, fare clic su "Connection Type" (Tipo di connessione) (1) nel lato sinistro dello schermo. Selezionare il tipo di connessione utilizzato. Se il provider avesse fornito le impostazioni DNS, facendo clic su "DNS" (2) si possono inserire le informazioni relative all'indirizzo DNS per quei provider che richiedono alcune specifiche impostazioni. Terminate queste impostazioni, l'indicatore "Internet Status" (Stato Internet), se il router è stato impostato correttamente, visualizzerà il messaggio "Connected" (collegato).



Connection Type (Tipo di connessione)

Nella pagina "Tipo di connessione" è possibile scegliere tra cinque tipi di connessioni sulla base delle istruzioni fornite dal proprio ISP:

PPPoE

PPPoA

IP dinamico (1483 Bridged)

IP statico (IPoA)

Soltanto modem (disattiva condivisione Internet)

Nota bene: Se non si è certi sul tipo di connessione da usare, contattare il proprio ISP.

Selezionare il tipo di connessione utilizzata facendo clic sul pulsante radio accanto al tipo di connessione e facendo quindi clic su "Next" (Avanti).

Configurazione manuale del router

WAN > Connection type

The following information is usually provided by your ISP.
Please select the Internet sharing protocol.

- PPPoE
- PPPoA
- Dynamic/Fixed IP (1483 Bridged)
- Static IP (PPoA)
- Modem Only (Disable Internet Sharing)

Next

Configurazione del proprio tipo di connessione ISP su PPPoE o PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) rappresenta il metodo standard per collegare i dispositivi collegati in rete. Per accedere alla rete del proprio ISP e collegarsi ad Internet questo tipo di connessione richiede un nome utente ed una password. Lo standard PPPoA (PPP over ATM) è simile allo standard PPPoE, ma è utilizzato principalmente nel Regno Unito. Selezionare PPPoE o PPPoA e fare clic su "Next" (Avanti). Quindi inserire le informazioni fornite dal proprio ISP e fare clic su "Apply Changes" (Applica modifiche) per attivare le impostazioni.

WAN > Connection Type > PPPoE Interface

More Info
ATM Interface

(1) Username

(2) Password

(3) Retype Password

(4) IP assigned by ISP > Yes No

IP Address

Subnet Mask

Default Gateway

(5) VPI/VCI /

(6) Encapsulation LLC

(7) Dial on Demand >

(8) Idle Time (Minute) >

(9) MTU >

1. **User Name** - Digitare il nome utente. (forniti dal proprio provider di servizi Internet).
2. **Password** — Digitare la password. (forniti dal proprio provider di servizi Internet).
3. **Retype Password (Ridigita password)**— Conferma la password. (forniti dal proprio provider di servizi Internet).
4. **IP Assigned by ISP (IP assegnato dall'ISP)**— Lasciare "Yes" (Sì) l'ISP assegna automaticamente un indirizzo IP. Se l'ISP assegna un indirizzo IP fisso, selezionare "No" e digitare i dati forniti.

5 VPI/VCI - —. Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio provider di servizi Internet).

6 Encapsulation (Incapsulamento) - Scegliere il tipo di incapsulamento (fornito dal proprio ISP) per specificare come gestire i protocolli multipli sul livello di trasporto ATM. VC-MUX: Lo standard PPPoA Virtual Circuit Multiplexer (incapsulamento nullo) consente di avere un solo protocollo in funzione per ciascun circuito virtuale con un numero inferiore di overhead. LLC: Lo standard PPPoA Logical Link Control consente a diversi protocolli multipli di funzionare su un unico circuito virtuale (maggiore numero di overhead).

7. Dial on Demand (Composizione a richiesta) -- Selezionando l'opzione "Dial on Demand" il router si collegherà automaticamente a Internet ogni volta che un utente apre un browser web.

8. Idle Time (Minutes) (Intervallo di inattività - Minuti) — Indicare il tempo di inattività massimo per la connessione a Internet. Superato questo intervallo, la connessione verrà interrotta.

WAN > Connection Type > Dynamic/Fixed IP (1483 Bridged)

More Info
ATM Interface

IP assigned by ISP >

IP Address

Subnet Mask

Default Gateway

VPI/VCI

Encapsulation

Yes				
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	/	35		
LLC				

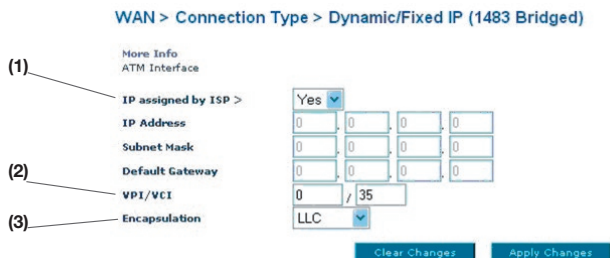
Clear Changes

Apply Changes

9. MTU— L'impostazione MTU non dovrebbe mai essere modificata, sempre che il proprio ISP non fornisca un'impostazione MTU specifica. La modifica delle impostazioni MTU può comportare dei problemi con la propria connessione ad Internet, come disconnessione, rallentamento dell'accesso e problemi relativi al funzionamento corretto delle applicazioni.

Configurazione del tipo di connessione su IP dinamico (1483 Bridged)

Questo metodo di connessione consente di creare un ponte di collegamento tra la propria rete e quella dell'ISP. Il router riceve l'indirizzo IP automaticamente dal server DHCP dell'ISP.



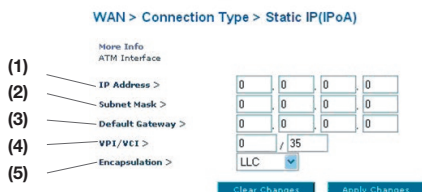
IP Assigned by ISP (IP assegnato dall'ISP) – Lasciare “Yes” (Sì) l'ISP assegna automaticamente un indirizzo IP. Se l'ISP assegna un indirizzo IP fisso, selezionare “No” e digitare i dati forniti.

2. VPI/VCI - —Digitare i propri parametri VPI e VCI. Questi parametri di identificazione vengono assegnati dall'ISP.

3. Encapsulation (Incapsulamento)—Selezionare i parametri LLC o VC MUX utilizzati dall'ISP.

Impostazione del proprio tipo di connessione ISP sull'IP statico (IPoA)

Questo tipo di connessione viene anche chiamato “Classical IP over ATM” o “CLIP”, ed è quello fornito dall'ISP come IP fisso del router da collegare ad Internet.



1. IP Address (Indirizzo IP) – Digitare un indirizzo IP assegnato dal proprio ISP per l'interfaccia WAN del router.

2. Subnet Mask (Maschera di sottorete)— Digitare una subnet mask assegnata dal proprio ISP.

3 Default Gateway (gateway predefinito) —Digitare un indirizzo IP gateway predefinito. Se il router non riesce a trovare l'indirizzo di destinazione entro la propria rete locale, trasmette i pacchetti al gateway predefinito assegnato dal proprio ISP.

4. VPI/VCI - —Digitare i propri parametri VPI e VCI. Questi parametri di identificazione vengono assegnati dall'ISP.

5. Encapsulation (Incapsulamento)—Selezionare i parametri LLC o VC MUX utilizzati dall'ISP.

Impostazione del tipo di connessione su Modem Only (Soltanto modem, disabilita la condivisione a Internet)

In questa modalità, il router agisce semplicemente come ponte per trasferire i pacchetti attraverso la porta DSL. Per accedere ad Internet è necessario disporre di altro software supplementare installato nei propri computer.

WAN > Connection Type > Modem Only(Disable Internet Sharing)

(1) More Info
ATM Interface

(2) VPI/VCI
Encapsulation

0 / 35
LLC

Clear Changes Apply Changes

1. VPI/VCI - Digitare i propri parametri VPI e VCI. (forniti dal proprio provider di servizi Internet).

2. Encapsulation (Incapsulamento)— Selezionare i parametri LLC o VC MUX. (forniti dal proprio provider di servizi Internet).

Impostazioni DNS (Domain Name Server)

Un “Domain Name Server” è un server presente in Internet che traduce gli Universal Resource Link (URL) come “www.belkin.com” in indirizzi IP. Molti ISP non richiedono l'immissione di questa informazione nel router. Se non è stato inserito alcun indirizzo DNS specifico, la casella “Automatic from ISP” dovrebbe essere spuntata. Se si utilizza un tipo di connessione IP statica, perché la propria connessione funzioni correttamente, potrebbe essere necessario inserire uno specifico indirizzo DNS ed un indirizzo DNS secondario. Se il proprio tipo di connessione fosse di tipo dinamico o PPPoE, potrebbe non essere necessario inserire un indirizzo DNS.

Lasciare la casella “Automatic from ISP” (Automatico da ISP) selezionata. Per digitare le impostazioni dell'indirizzo DNS, togliere il segno di spunta dalla casella “Automatic from ISP” (Automatico da ISP) e digitare i propri dati DNS negli spazi disponibili. Fare clic su “Apply Changes” (Applica modifiche) (2). per salvare le impostazioni.

WAN > DNS

If your ISP provided you with a specific DNS address to use, enter the address in this window and click "Apply Changes".

(1) Automatic from ISP

DNS Address > 0 0 0 0

Secondary DNS Address > 0 0 0 0

DNS = Domain Name Server. A server located on the Internet that translates URL's (Universal Resource Links) like www.belkin.com to IP addresses. More Info

(2) Clear Changes Apply Changes

Utilizzo del DNS dinamico

Il servizio Dynamic DNS (DNS dinamico) permette di trasformare un indirizzo IP dinamico in un nome host statico in uno qualsiasi dei domini offerti dalla DynDNS.org. Ciò permette di accedere ai computer di rete più facilmente da varie postazioni Internet. DynDNS.org offre questo servizio, per un massimo di 5 host name, gratuitamente alla comunità Internet. TZO.com, in alternativa a DyDNS.org è un servizio DDNS è ideale per i siti web domestici, file server o per semplificare l'accesso ai file archiviati ed al PC in casa. Con questo servizio si può essere certi che il proprio nome host porti sempre al proprio indirizzo IP, anche se l'ISP lo cambia. Quando l'indirizzo IP cambia, i vostri amici e colleghi saranno sempre in grado di rintracciarvi andando su tuonome.dyndns.org! Per registrarsi gratuitamente al servizio di nome host DNS dinamico, andare su <http://www.dyndns.org>.

Impostazione dell'aggiornamento client del DNS dinamico del router

Prima di poter usufruire del servizio di aggiornamento gratuito, bisogna registrarsi con DynDNS.org. Una volta effettuata la registrazione, seguire le seguenti istruzioni:

1. Inserire il proprio nome utente DynDNS.org nel campo "Account / E-mail" (1).
2. Inserire la propria password DynDNS.org nel campo "Password / Key" (2).
3. Nel campo "Domain Name" (Nome dominio) digitare il nome del dominio DynDNS.org creato con DynDNS.org. (3).
4. Fare clic su "Apply Changes" (Esegui modifiche) per aggiornare l'indirizzo IP. Ogni volta che l'indirizzo IP fornito dall'ISP cambia, il router aggiornerà automaticamente i server di DynDNS.org con il nuovo indirizzo IP. È possibile effettuare questa operazione anche manualmente, facendo clic sul pulsante "Apply Changes" (Esegui modifiche) (4).

Dalla pagina "Connection Type" (tipo di connessione), è possibile selezionare il tipo di connessione che si vuole utilizzare dalla voce "Connection Type" dal menu a discesa.

WAN > DDNS

DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP address is dynamic. You must Register for DDNS service at one of the listed DDNS Services.

DDNS Service >

DDNS Status >

(1) Account / E-mail >

(2) Password / Key >

(3) Domain Name >

(4)

Wireless

Nella scheda “Wireless” è possibile modificare le impostazioni di configurazione di rete. Da questa scheda è possibile modificare il nome della rete wireless (SSID), il canale operativo e le impostazioni di protezione crittografata.

Canale e SSID

Wireless > Channel and SSID

This page allows you to enter the Wireless Network Name (SSID in Wi-Fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as an wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. [More Info](#)

SSID >	<input type="text" value="Belkin54g"/>
ESSID Broadcast >	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode >	<input type="text" value="Mixed (11b+11g)"/>
Wireless Channel >	<input type="text" value="Auto"/>
<input type="button" value="Clear Changes"/> <input type="button" value="Apply Changes"/>	

1. Modifica del nome della rete wireless (SSID)

Per identificare la propria rete wireless, si utilizza un nome chiamato SSID (Service Set Identifier). È possibile sostituire questo nome con un altro qualsiasi o lasciarlo invariato. In presenza di altre reti wireless nella stessa area, è consigliabile utilizzare un SSID unico (diverso da quello di un'eventuale altra rete wireless in zona). Per modificare il nome SSID, digitare il nuovo SSID che si desidera utilizzare nel campo SSID e fare clic su “Apply Changes” (Esegui modifiche). La modifica è immediata. Nel caso il nome SSID venga modificato, è necessario riconfigurare anche i computer wireless per consentirne il collegamento al nuovo nome della rete. Per ulteriori indicazioni su come eseguire le modifiche necessarie, vedere la documentazione relativa alla scheda di rete wireless.

2. Utilizzo del servizio di trasmissione ESSID

Per questioni di sicurezza si può scegliere di non trasmettere la propria SSID di rete. In questo modo, il proprio nome di rete rimarrà nascosto a quei computer che eseguiranno un'analisi per rilevare la presenza di eventuali reti wireless. Per disattivare la trasmissione SSID, selezionare “DISABLE” (disattiva) e fare clic su “Apply Changes” (Esegui modifiche). La modifica è immediata. A questo punto, tutti i computer devono essere impostati in modo da potersi collegare al proprio SSID specifico; un SSID “QUALSIASI” non sarà più accettato. Per ulteriori indicazioni su come eseguire le modifiche necessarie, vedere la documentazione relativa alla scheda di rete wireless.

Nota bene: Questa funzione avanzata dovrebbe essere implementata soltanto dagli utenti esperti.

3. Utilizzo dello switch di modalità wireless

Il router può funzionare in tre diverse modalità wireless: “Mixed (11b+11g)”, “11g Only” e “11b Only”. Le diverse modalità sono spiegate di seguito.

Modalità mista (11b+11g)

In questa modalità, il router è compatibile contemporaneamente con i client wireless 802.11b e 802.11g. Questa modalità è impostata dal produttore e garantisce un corretto funzionamento con tutti i dispositivi Wi-Fi®. Se nella propria rete sono presenti client 802.11b e 802.11g, è consigliabile impostare il router sulla modalità predefinita. Questa impostazione andrà modificata soltanto per motivi ben specifici.

Modalità solo 11g

La modalità 802.11g-Only funziona esclusivamente con i client 802.11g. Questa modalità è consigliata soltanto nel caso si desideri impedire ai client 802.11b di accedere alla propria rete. Per cambiare modalità, selezionare quella desiderata dall'elenco a discesa “Wireless Mode” (Modalità wireless). Quindi fare clic su “Apply Changes” (Esegui modifiche).

Modalità solo 11b

Consigliamo di NON utilizzare questa modalità, a meno che non se ne abbia un motivo specifico. Questa modalità è stata creata per risolvere problematiche uniche che si possono verificare con alcuni adattatori per client 802.11b e NON è necessaria per garantire l'interoperabilità tra gli standard 802.11g e 802.11b.

4. Modifica del canale wireless

Esistono numerosi canali operativi tra cui scegliere. Negli Stati Uniti i canali sono 11. Nel Regno Unito e in gran parte d'Europa i canali sono 13. In pochi altri paesi ancora i requisiti per i canali sono diversi. Il router è stato configurato per funzionare sui canali adatti del paese di residenza dell'utente. L'impostazione predefinita è “Auto”. Questo canale, se necessario, può essere cambiato. In presenza di altre reti wireless nella stessa area, la rete dovrà essere impostata in modo da funzionare su un canale diverso dalle altre reti wireless. Per ottenere prestazioni migliori, utilizzare un canale che sia almeno a cinque canali di distanza dalla rete wireless. Ad esempio, in presenza di un'altra rete che funziona sul canale 11, impostare la propria rete sul canale 6 o su un canale minore. Per cambiare canale, selezionare il canale desiderato dall'elenco a tendina. Fare clic su “Apply Changes” (Esegui modifiche). La modifica è immediata.

Crittografia/Sicurezza

Protezione della rete Wi-Fi

Di seguito sono descritte alcune soluzioni per rendere più efficiente la rete wireless e per proteggere i propri dati da intrusioni indesiderate. Questo capitolo è dedicato agli utenti che usano la rete da casa, dall'ufficio in casa e da piccoli uffici. Al momento della stampa di questo manuale, i tipi di crittografia disponibili sono tre.

Nome	Wired Equivalent Privacy a 64 bit	Wired Equivalent Privacy a 128 bit	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronimo	64-bit WEP	128-bit WEP	WPA-TKIP/AES (oppure soltanto WPA)	WPA2-AES (oppure soltanto WPA2)
Protezione	Buona	Migliore	Ottima	Ottimo
Caratteristiche	Chiavi statiche	Chiavi statiche	Crittografia a chiavi dinamiche e autenticazione reciproca	Crittografia a chiavi dinamiche e autenticazione reciproca
	Chiavi di crittografia basate sull'algoritmo RC4 (generalmente chiavi a 40 bit)	Più sicura rispetto alla protezione WEP a 64 bit con una chiave lunga 104 bit, più 24 bit aggiuntivi dei dati generati dal sistema	Protocollo TKIP (temporal key integrity protocol) aggiunto per permettere la rotazione delle chiavi e il potenziamento della crittografia	La crittografia AES (Advanced Encryption Standard) non provoca alcuna perdita di trasferimento dati

Wired Equivalent Privacy (WEP)

WEP è un protocollo che aggiunge protezione a tutti i prodotti wireless conformi allo standard Wi-Fi. Questo protocollo comune offre alle reti wireless lo stesso livello di protezione della privacy di una rete cablata simile.

WEP a 64 bit

La protezione 64-bit WEP fu introdotta per la prima volta con la crittografia da 64 bit, che prevedeva una lunghezza di chiave di 40 bit più altri 24 bit supplementari di dati generati dal sistema (per un totale di 64 bit). Alcuni produttori di hardware si riferiscono alla crittografia a 64 bit come crittografia a 40 bit. Poco tempo dopo l'introduzione della tecnologia, i ricercatori scoprirono che la crittografia a 64 bit poteva essere decodificata molto facilmente.

WEP a 128 bit

Per riparare alle potenziali debolezze della crittografia WEP 64 bit, fu progettato un metodo più sicuro a 128 bit. La crittografia a 128 bit comprende una chiave da 104 bit più 24 bit aggiuntivi di dati generati dal sistema (128 bit in totale). Alcuni produttori di hardware si riferiscono alla crittografia a 128 bit come crittografia a 104 bit. La maggior parte delle apparecchiature wireless attualmente in commercio supporta entrambi i tipi di crittografia, a 64 e 128 bit, tuttavia alcune apparecchiature più vecchie supportano solo la WEP a 64 bit. Tutti i prodotti wireless Belkin supportano entrambi i tipi di crittografia, a 64 e 128 bit.

Codici di crittografia

Dopo aver scelto tra la modalità di crittografia “64-bit” oppure “128-bit WEP” è fondamentale generare una chiave di crittografia. La chiave di crittografia dovrà essere sempre la stessa per tutta la rete wireless, altrimenti i dispositivi di rete wireless non saranno in grado di comunicare tra loro e l'utente non sarà in grado di comunicare all'interno della rete. La chiave di crittografia può essere inserita manualmente in modalità esadecimale, oppure inserendo una frase di accesso nel campo “Passphrase” (frase di accesso) e cliccando quindi sulla richiesta di generare la chiave. Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 64 bit è necessario inserire una chiave composta da 10 caratteri esadecimali. Per la protezione WEP a 128 bit, bisogna inserire 26 codici esadecimali.

Ad esempio:

AF 0F 4B C3 D4 = codice WEP a 64 bit

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = codice WEP a 128 bit

La frase di accesso WEP NON è la stessa cosa della chiave WEP. La scheda wireless fornita utilizza la frase di accesso per generare le chiavi WEP, ma i metodi per generare le chiavi potrebbero cambiare a seconda del produttore. Se nella rete sono presenti dispositivi di varie marche, la cosa più semplice da fare è usare la chiave WEP esadecimale del router o dell'access point wireless ed inserirlo manualmente nella tabella dei codici esadecimali WEP nella schermata di configurazione della scheda.

Wi-Fi Protected Access (WPA)

WPA è un nuovo standard Wi-Fi che è stato progettato per offrire maggiore sicurezza rispetto alla WEP. Per poter utilizzare la protezione WPA, i driver ed il software dell'apparecchiatura wireless devono essere aggiornati in maniera adatta a supportarla. Tali aggiornamenti sono disponibili nel sito web del rivenditore dei dispositivi wireless. Esistono due tipi di protezione WPA: WPA-PSK (senza server) e WPA (con server radius 802.1x).

WPA-PSK (no server)

Questo metodo si avvale di una chiave pre-condivisa come chiave di rete. Un codice di rete è una password di una lunghezza che va dagli 8 ai 63 caratteri, tra lettere, numeri ed altri caratteri. Ogni client usa la stessa chiave di accesso alla rete. Generalmente, questa è la modalità che viene utilizzata in un ambiente domestico.

WPA (con server radius 802.1x)

Questo sistema consente ad un radius server di distribuire automaticamente la chiave di rete ai client. Generalmente, questa modalità viene utilizzata in un ambiente di lavoro.

WPA2

Il Router è provvisto della protezione WPA2, la seconda generazione della crittografia WPA basata sullo standard 802.11i. Offre un maggiore livello di protezione wireless, combinando un'autenticazione di rete avanzata ed un metodo di crittografia AES rafforzato.

Requisiti WPA2

IMPORTANTE: Per utilizzare la protezione WPA2, tutti i computer e gli adattatori di rete devono essere aggiornati con patch, driver e software utility client che supportano la WPA2. Al momento della pubblicazione di questo manuale, è possibile scaricare gratuitamente un paio di security patch da Microsoft®. Questi patch sono adatti soltanto al sistema operativo Windows XP. Attualmente gli altri sistemi operativi non sono supportati.

Per i computer con Windows XP che non hanno Service Pack 2 (SP2), è possibile scaricare gratuitamente un file da Microsoft chiamato "Windows XP Support Patch for Wireless Protected Access (KB 826942)" dal sito: <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91>.

Per Windows XP con Service Pack 2, Microsoft mette a disposizione un download gratuito per aggiornare i componenti del client wireless in modo da poter supportare la protezione WPA2 (KB893357). L'aggiornamento può essere scaricato dal sito: <http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en>.

IMPORTANTE: è necessario accertarsi inoltre che le schede/adattatori wireless supportino la protezione WPA2 e di aver scaricato e installato il driver più recente. Per la maggior parte delle schede wireless Belkin è possibile scaricare un driver di aggiornamento dal sito Belkin: www.belkin.com/networking. Un elenco dei prodotti wireless Belkin che supportano le protezioni WPA/WPA2 è riportato al sito web www.belkin.com/networking.

Condivisione dei codici di rete

Nella maggior parte dei prodotti Wi-Fi la sicurezza è disattivata. Dopo aver installato la rete e quando questa è in funzione, bisognerà attivare la protezione WEP o WPA ed assicurarsi che tutti i dispositivi wireless usino la stessa chiave di rete.

Utilizzo di una chiave esadecimale

Un codice esadecimale è composto da numeri e lettere che vanno dalla A alla F e dallo 0 al 9. I codici a 64-bit sono composti da cinque numeri a due cifre. I codici 128-bit sono composti da 13 numeri a due cifre.

Ad esempio:

AF 0F 4B C3 D4 = codice a 64-bit

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = codice a 128 bit

Nelle caselle riportate di seguito è possibile creare la propria chiave inserendo due caratteri

tra A ed F e tra 0 e 9. Questa chiave verrà usata per programmare le impostazioni di crittografia del vostro router e dei propri computer wireless.

Nota per gli utenti Mac: I prodotti originali Apple AirPort® supportano soltanto la crittografia a 64 bit. I prodotti Apple Airport 2 possono supportare la modalità di crittografia a 64 o 128 bit. Verificare quale sia la versione utilizzata. Non potendo configurare la rete con una crittografia a 128 bit, provare una crittografia a 64 bit.

Configurazione WEP

1. Selezionare “WEP” dal menu a tendina.
2. Scegliere “WEP Mode” (modalità WEP) a 64 bit o 128-bit.
3. Una volta selezionata la modalità WEP, sarà possibile inserire la propria chiave esadecimale digitandola manualmente.

Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la sicurezza WEP a 64 bit, bisogna inserire una chiave composta da 10 chiavi esadecimali. Per la protezione WEP a 128 bit, bisogna inserire 26 codici esadecimali.

Ad esempio:

AF 0F 4B C3 D4 = codice a 64-bit

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = codice a 128-bit

Wireless > Security

The router can transmit your data securely over the wireless network. Making security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. Home >

Allowed Client Type >	WEP <input checked="" type="checkbox"/>
WEP Mode >	<input checked="" type="radio"/> 64 bit <input type="radio"/> 128 bit
Key Entry Method >	<input type="radio"/> HEX <input checked="" type="radio"/> ASCII
Key Provisioning >	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Key 1 >	<input type="text"/>
Key 2 >	<input type="text"/>
Key 3 >	<input type="text"/>
Key 4 >	<input type="text"/>
Default Key ID >	1 <input type="text"/>
Password >	<input type="text"/>

[Cancel](#) [Apply](#)

-
-
3. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. La crittografia del router è impostata. Ogni computer presente nella rete wireless deve essere configurato con le medesime impostazioni di protezione.

AVVERTENZA: se si stesse eseguendo la configurazione del router wireless da un client wireless, sarà necessario accertarsi che la protezione per questo client wireless sia ATTIVA. In caso contrario si perderà la connessione wireless.

Modifica delle impostazioni di protezione della rete wireless

Il vostro router è corredato del WPA/WPA2, il più recente standard di protezione wireless. Supporta inoltre gli standard di sicurezza WEP. L'impostazione predefinita prevede che la protezione wireless sia disattivata. Per abilitare la protezione, è necessario stabilire prima lo standard che si desidera utilizzare. Per accedere alle impostazioni di protezione, fare clic su “Security” (Protezione) nella pagina “Wireless”.

Configurazione WPA

Nota bene: per utilizzare la protezione WPA, tutti i client devono disporre dei driver e del software in grado di supportarla. Al momento della pubblicazione di questo manuale, un security patch di Microsoft è disponibile gratuitamente, adatto soltanto al sistema operativo Windows XP. È necessario inoltre scaricare dal sito di supporto Belkin il driver più recente per la scheda di rete G wireless Belkin per computer desktop o laptop. Attualmente gli altri sistemi operativi non sono supportati. Il patch Microsoft supporta esclusivamente i dispositivi che prevedono driver con la funzione WPA abilitata, tra cui i prodotti 802.11g Belkin.

Esistono due tipi di protezione WPA: WPA-PSK (senza server) e WPA (con server radius). La protezione WPA-PSK (senza server) sfrutta il cosiddetto codice pre-condiviso come codice di protezione. Un codice pre-condiviso è una password la cui lunghezza varia tra otto e 63 caratteri, tra lettere, numeri ed altri caratteri. Ogni client usa lo stesso codice per accedere alla rete. Generalmente, questa modalità viene utilizzata in un ambiente domestico. La protezione WPA (con server radius) è una configurazione nell'ambito della quale un server radius distribuisce automaticamente i codici ai client. Questa soluzione viene generalmente utilizzata nell'ambiente lavorativo. La protezione WPA2 è la seconda generazione della WPA ed offre una tecnica di crittografia più avanzata rispetto alla WPA..

Impostazione della protezione WPA/WPA2-PSK (senza server)

1. Dal menu a discesa “Allowed Client Type”, selezionare “WPA/WPA2”.
2. Come autenticazione, scegliere “Pre-shared Key” per un uso domestico o in un piccolo ufficio. Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare la propria chiave pre-condivisa. che può essere lunga da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati. Ad esempio, la propria pre-shared key (Chiave pre-condivisa) potrebbe essere qualcosa del tipo: “Chiave di rete famiglia Rossi”.

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >

WPA/WPA2 ▾

Authentication >

802.1X Pre-shared Key

Pre-shared Key >

Apply Changes

Clear Changes

4. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Configurazione delle impostazioni WPA/WPA2 (con server radius)

Se la vostra rete utilizza un radius server per distribuire le chiavi ai client, utilizzare questa impostazione.

1. Dal menu a discesa “Allowed Client Type”, selezionare “WPA/WPA2”.
2. Come tecnica di crittografia, scegliere “802.1x” se si tratta di ambienti con server radius. Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare l'intervallo di inattività del server radius nel campo “Session Idle Timeout” (Interruzione della connessione).
4. Digitare l'intervallo della chiave, ovvero ogni quanto le chiavi sono distribuite (in pacchetti), nel campo “Re-Authentication Period”
5. Digitare l'intervallo di attesa dopo la fallita autenticazione nel campo “Quiet Period”.
6. Digitare l'indirizzo IP e il numero della porta del server radius nei campi “Server-IP” e “Server-Port”.
7. Digitare la chiave radio nel campo “Secret Key” (chiave segreta).
8. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. Ora devono essere configurati tutti i client in modo da essere adattati a queste impostazioni.

Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

Allowed Client Type >	WPA/WPA2
Authentication >	<input checked="" type="radio"/> 802.1X <input type="radio"/> Pre-shared Key
Session Idle Timeout >	300 Seconds (0 for no timeout checking)
Re-Authentication Period >	3600 Seconds (0 for no re-authentication)
Quiet Period >	60 Seconds after authentication failed
Server-IP >	192 . 168 . 2 . 1
Server-Port >	1812
Secret Key >	<input type="text"/>
NAS-ID >	<input type="text"/>

[Apply changes](#) [Clear changes](#)

Nota bene: accertarsi che i computer wireless siano stati aggiornati in modo tale da poter funzionare con la protezione WPA2 e che le impostazioni siano corrette per poter effettuare la connessione con il router.

Configurazione delle Schede di Rete Wireless G Belkin in modalità sicura

Nota bene: questa sezione contiene le informazioni su come configurare le schede di rete wireless G di Belkin per utilizzare la protezione. A questo punto il router e l'access point wireless dovrebbero essere stati già configurati per l'utilizzo della crittografia WPA o WEP. Per ottenere una connessione wireless, bisognerà configurare le schede di rete wireless notebook e desktop con le medesime impostazioni di protezione.

Collegamento del computer ad un router o wireless access point che richiede una chiave WEP a 64 o 128 bit

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Avanzate" consente di visualizzare e configurare diverse opzioni della scheda wireless.
2. Nella scheda "Wireless Network Properties", selezionare un nome dall'elenco "Available networks" (Reti disponibili) e fare clic su "Configure" (configura).
3. In "Data Encryption", selezionare "WEP".
4. Disattivare la casella in basso "Network key is provided for me automatically" (Fornisci automaticamente la chiave di rete). Se si usa il computer per collegarsi ad una rete aziendale, chiedere al proprio amministratore di rete se la casella deve essere attivata.
5. Digitare il codice WEP nella casella "Network key" (Codice rete).

Wireless > Security

Security Mode

Key 1

Key 2

Key 3

Key 4

(hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, input it here

PassPhrase

Importante: una chiave WEP è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit, vanno inseriti 26 caratteri. Per la protezione WEP a 64 bit, bisogna inserire 10 codici. Questo codice di rete deve essere uguale a quello assegnato al router.

6. Fare clic su “OK” per salvare le impostazioni.

Collegamento del computer ad una rete wireless che usa la protezione WPA-PSK (senza server)

1. Fare doppio clic sull' icona “Signal Indicator” per aprire la schermata “Wireless Network” (Rete wireless). Il pulsante “Avanzate” consente di visualizzare e configurare diverse opzioni della scheda wireless.
2. Nella scheda “Wireless Network”, selezionare un nome dall'elenco “Available networks” (Reti disponibili) e fare clic su “Configure” (configura).
3. In “Network Authentication” (Autenticazione di rete) selezionare “WPA-PSK (No Server)”.
4. Digitare la chiave WPA nella casella “Network key” (Chiave di rete).

Importante: una chiave WPA-PSK è composta da numeri e lettere, da 0 a 9 e dalla A alla Z. Per la protezione WPA-PSK, si possono inserire da 8 a 63 chiavi. Questo codice di rete deve essere uguale a quello assegnato al router.

1

2

3

4

5

6

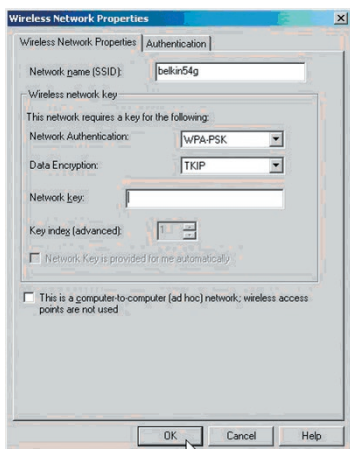
7

8

9

10

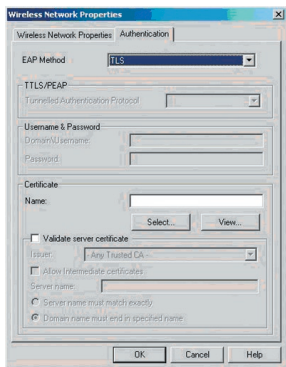
11



5. Fare clic su “OK” per salvare le impostazioni.

Collegamento del computer ad una rete wireless che usa la protezione WPA (con radius server)

1. Fare doppio clic sull’ icona “Signal Indicator” per aprire la schermata “Wireless Network” (Rete wireless). Il pulsante “Avanzate” consente di visualizzare e configurare diverse opzioni della scheda wireless.
2. Nella scheda “Wireless Network”, selezionare un nome dall’elenco “Available networks” (Reti disponibili) e fare clic su “Configure” (configura).
3. In “Network Authentication” (Autenticazione di rete) selezionare “WPA”.
4. Nella scheda “Authentication” (Autenticazione), selezionare le impostazioni indicate dall’amministratore di rete.



5. Fare clic su “OK” per salvare le impostazioni.

Impostazione della protezione WPA per schede di rete wireless di altre marche.

Per le schede di rete wireless WPA per computer desktop e notebook di altre marche provviste del software WPA, è possibile scaricare gratuitamente un file da Microsoft chiamato “Windows XP Support Patch for Wireless Protected Access”.

Nota bene: il file messo a disposizione da Microsoft funziona soltanto con Windows XP. Attualmente gli altri sistemi operativi non sono supportati.

Importante: È necessario accertarsi inoltre che il produttore della scheda wireless supporti la protezione WPA e di aver scaricato e installato il driver più recente dal suo sito.

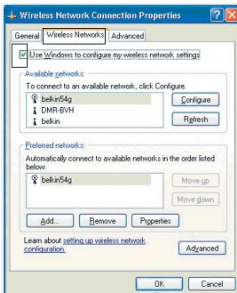
Sistemi operativi supportati:

- Windows XP Professional
- Windows XP Home Edition

Impostazione dell'utilità di rete wireless Windows XP per utilizzare la protezione WPA-PSK

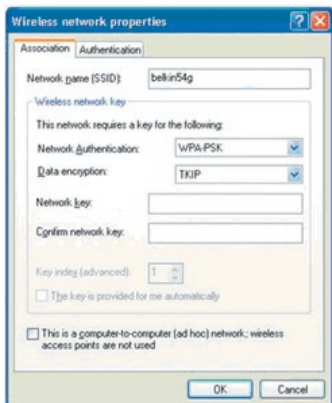
Per utilizzare la protezione WPA-PSK, accertarsi di utilizzare la utility di rete wireless Windows nel seguente modo:

1. In Windows XP, fare clic su “Start > Control Panel (Pannello di controllo) > Network Connections (Connessioni di rete)”.
2. Con il tasto destro del mouse, fare clic sull'opzione “Wireless Network Connection” (Connessione rete wireless), e selezionare “Properties” (Proprietà).
3. Cliccando sulla scheda “Wireless Networks” (Reti wireless) si aprirà la seguente schermata. Accertarsi che l'opzione “Utilizza Windows per configurare le impostazioni di rete wireless” sia spuntata.
4. Nella scheda “Wireless Networks” (Reti wireless), cliccare il pulsante “Configure” (Configura) e sarà visualizzata la seguente schermata.



5. Nel caso di una rete domestica o simile, selezionare “WPA-PSK” da “Network Authentication” (Autenticazione rete).

Nota bene: selezionare “WPA” se si sta utilizzando il computer per collegarsi ad una rete aziendale che supporta un server di autenticazione come può essere un radius server. Per ulteriori informazioni, rivolgersi all'amministratore di rete.



6. Selezionare “TKIP” o “AES” da “Data Encryption” (Crittografia dati). Questa impostazione deve essere identica a quella del Router.

7. Digitare la propria chiave di crittografia nella casella “Network key” (Chiave di rete).

Importante: Inserire la propria chiave precondivisa che può essere lunga da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati.

8. Fare clic su “OK” per confermare le impostazioni.

Modalità di estensione range wireless e bridging

Cos'è un Bridge Wireless?

La modalità bridge wireless può essere utilizzata per ampliare la portata della propria rete wireless o per aggiungere un'estensione della propria rete in un'altra zona del proprio ufficio o a casa senza dover ricorrere all'uso dei cavi.

Nota bene: non possiamo garantire che questa opzione funzionerà con hardware wireless di altre marche.

Nota bene: Per avere prestazioni eccellenti, accertarsi di aver scaricato la più recente versione firmware per il router o access point: <http://web.belkin.com/support>

Aggiunta di un altro segmento di rete wireless

La connessione di uno switch o un hub di rete al jack R45 dell'access point consente a numerosi computer collegati allo switch di accedere al resto della rete.

Impostazione di una connessione bridge tra il proprio router wireless ed un access point secondario

Per creare una connessione di tipo bridge tra il proprio router Belkin e un access point secondario aprire il programma di configurazione guidata del router e digitare l'indirizzo MAC dell'access point nello spazio apposito. Si devono inoltre osservare alcune altre indicazioni.

SEGUIRE CON ATTENZIONE QUESTI PUNTI.

1. Impostare il proprio access point sullo stesso canale del router. Per ulteriori informazioni sulla variazione dei canali, vedere il capitolo "Canale wireless e SSID".
2. Trovare l'indirizzo MAC dell'access point sull'etichetta prevista sotto l'access point. Nell'etichetta sono riportati due indirizzo MAC. Fare riferimento all'indirizzo MAC "WLAN MAC Address". L'indirizzo MAC inizia con 0030BD ed è seguito da altri sei numeri o lettere (ad es. 0030BD-XXXXXX). Scrivere di seguito l'indirizzo MAC. Passare alla fase successiva.
3. Posizionare l'access point secondario entro il raggio di azione del router wireless e vicino all'area dove si desidera estendere la portata o aggiungere il segmento di rete. Normalmente, la portata in un ambiente chiuso dovrebbe essere compresa tra 30 e 70 metri circa.
4. Collegare l'access point alla fonte di alimentazione. Accertarsi che l'access point sia acceso e procedere alla fase successiva.
5. Da un computer già collegato al router, accedere alla utility di configurazione avanzata aprendo il proprio browser. Nella barra indirizzi digitare "192.168.2.1". Non digitare "www" o "http://" prima del numero. Nota: Se il proprio indirizzo IP del router è stato modificato, usare quell'indirizzo IP.
6. Nella finestra del browser compare l'interfaccia utente del router. Fare clic su "Wireless Bridge" (2) sul lato sinistro dello schermo. La seguente finestra sarà visualizzata.

Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

1) Wireless Channel must match between Router and AP.
2) Security Settings (WEP) must match between Router and AP.
3) If MAC Filtering is enabled, user must be sure to add the WLAN MAC address(es) of the Router/AP in order to allow communication with each other.

Enable Wireless Bridging. (enabling this feature allows other Access Points to connect to this Access Point.)

Enable ONLY specific Access Points to connect. (enter Wireless MAC Address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Hint: the MAC address can be found using a site survey on a wireless client card.)

AP1

AP2

AP3

AP4

Disable ability for Wireless CLIENT to connect. (This feature should only be used when the AP is used exclusively to other APs.)

- Spuntare la casella che dice “Enable ONLY specific Access Points to connect” (Abilita alla connessione SOLTANTO da access point specifici) (1).
- Nel campo “AP1” (3), digitare l’indirizzo MAC del proprio access point secondario. Dopo aver inserito l’indirizzo, fare clic su Apply Changes (Esegui modifiche).
- La connessione di tipo bridge è stata impostata.

Nota bene:Prima di stabilire la connessione di tipo bridge potrebbe trascorrere un minuto. In alcuni casi potrebbe essere necessario riavviare l’access point ed il router per poter avviare la connessione di tipo bridge.

Firewall

Il router è dotato di una protezione firewall che salvaguardia la rete da una vasta gamma di comuni attacchi degli hacker, tra cui:

- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

La protezione firewall inoltre maschera le porte comuni generalmente utilizzate per attaccare le reti. Queste porte appaiono “nascoste”, il che significa che un potenziale hacker non le rileva. Se necessario, la funzione di protezione firewall può essere disattivata, ma è consigliabile lasciarla attiva. Disattivando la protezione firewall, la rete non rimarrà completamente vulnerabile agli attacchi degli hacker, ma è comunque indicato lasciare la protezione firewall attiva.

Firewall >

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Firewall Enable / Disable > Enable Disable

Clear Changes

Apply Changes

Server virtuali

I server virtuali consentono di instradare eventuali richieste di servizio esterne (di Internet), tra cui le richieste di vari servizi come quello di un server web (porta 80), server FTP (porta 21) o altre applicazioni attraverso il proprio router nella rete interna. Poiché i computer interni sono protetti da una protezione firewall, i computer di Internet non possono accedervi perché non li “vedono”. Se fosse necessario configurare una funzione di server virtuale per una specifica applicazione, si dovrà contattare il fornitore dell'applicazione per conoscere le impostazioni delle porte necessarie. Le informazioni su questa porta possono essere immesse manualmente nel router.

Firewall > Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (port 21), or other applications through your Router to your internal network. [View Info](#)

No.	LAN IP Address	Description	Protocol Type	LAN Port	Public Port	Enable	Action
1	192.168.0.2		TCP			<input checked="" type="checkbox"/>	Clear
2	192.168.0.2		TCP			<input checked="" type="checkbox"/>	Clear
3	192.168.0.2		TCP			<input checked="" type="checkbox"/>	Clear

Scelta di un'applicazione

Selezionare la propria applicazione dall'elenco a discesa. Fare clic su “Add” (Aggiungi). Le impostazioni saranno trasferite nel successivo spazio disponibile nello schermo. Fare clic su “Apply Changes” (Esegui modifiche) per salvare le impostazioni per quella specifica applicazione. Per eliminare un'applicazione, selezionare il numero della riga che si desidera eliminare e fare clic su “Clear” (Cancella).

Immissione manuale delle impostazioni nel server virtuale

Per immettere manualmente le impostazioni, inserire l'indirizzo IP nello spazio previsto per la macchina interna (server), le porte da cui passare, selezionare il tipo di porta (TCP o UDP) e fare clic su “Esegui modifiche”. Ciascuna voce relativa alle porte in entrata prevede due campi di massimo 5 caratteri che consentono di stabilire un punto di partenza e di arrivo della portata (ad es. [xxxxx]-[xxxxx]). Per ciascuna voce si può inserire un valore porta unico compilando i due campi con il medesimo valore (ad es. [7500]-[7500]) oppure una vasta gamma di porte (ad es. [7500]-[9000]). Se si desidera utilizzare diversi valori porta unici o diversi range ed un solo valore, è necessario ricorrere ad un massimo di 20 voci (ad es. 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). È possibile passare soltanto attraverso una porta per ciascun indirizzo IP interno. L'apertura delle porte nella protezione firewall può comportare un rischio per la sicurezza. Le impostazioni possono essere attivate e disattivate molto rapidamente. È consigliabile disattivare le impostazioni quando non si utilizza un'applicazione specifica.

Filtri IP Client

Il router può essere configurato in modo da limitare l'accesso ad Internet, alla posta elettronica o ad altri servizi di rete in particolari giorni o momenti. La limitazione di accesso ai servizi può essere impostata per uno o più computer.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

Access Control allows users to define the traffic type permitted or not-permitted to WAN port services. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function > Enable Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

> Add PC

Apply Changes

Controllo dell'accesso

Il controllo dell'accesso permette agli utenti di definire il traffico in uscita, sia esso consentito o negato, mediante l'interfaccia WAN. Per impostazione predefinita è permesso il traffico in uscita. Per limitare l'accesso ai computer, seguire il seguente procedimento:

1. Nella schermata "Access Control" (controllo dell'accesso) fare clic su "Add PC" (aggiungi un PC).
2. Stabilire le impostazioni corrette per i servizi del client PC (come indicato nella seguente schermata).

Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address > -

> Client PC Service:

Service Name	External Description	Blocked
Any	ANY, TCP Port 0, UDP, 8000, 8000	<input checked="" type="checkbox"/>
Any with URL Blocking	ANY (with URL Blocking Site Page)	<input checked="" type="checkbox"/>
Email Sending	SMTP, TCP Port 25	<input checked="" type="checkbox"/>
Newsvs Feeds	NNTP, TCP Port 110	<input checked="" type="checkbox"/>
Email Receiving	POP3, TCP Port 110	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input checked="" type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input checked="" type="checkbox"/>
SMTP Messenger	SMTP, TCP Port 25	<input checked="" type="checkbox"/>
Instant Services	TCP/UDP 80	<input checked="" type="checkbox"/>

3. Fare clic su "OK" e, quindi, su "Apply Changes" (Esegui modifiche) per salvare le impostazioni.

Blocco di URL

Per poter configurare il blocco URL, specificare i siti web (www.sitoweb.com) e/o le parole che si vuole filtrare dalla rete. Fare clic su "Apply Changes" (Esegui modifiche) per salvare la modifica. Per completare la configurazione bisognerà creare o modificare la regola dell'accesso nella sezione "Client IP filters" (Filtri IP Client).. Per modificare una regola esistente, fare clic sull'opzione "Edit" vicina alla regola che si vuol modificare. Per creare una nuova regola, fare clic su "Add PC" (Aggiungi PC). Dalla sezione "Access Control > Add PC", inserire il segno di spunta accanto all'opzione "WWW with URL Blocking" (www con blocco URL) nella scheda "Client PC Service" per eliminare i siti web e le parole specificate.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

To configure the URL Blocking feature, use the table below to specify the websites ([www.somewhere.com](#)) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section. To modify an existing rule, click the "Edit" option next to the rule you want to modify. To create a new rule, click on the "Add PC" option.

From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below...

Rule Number	URL / Keyword
SN_1	
SN_2	
SN_3	
SN_4	
SN_5	

Regola di pianificazione

Si può filtrare l'accesso ad Internet per clienti locali servendosi delle regole. Ogni controllo di accesso può essere pianificato. Programmare attraverso l'opzione "Schedule Rule" (Norma di pianificazione) e confermarla nella pagina "Access

Control"(Controllo accesso).

Per aggiungere un'altra pianificazione, seguire queste fasi:

1. Fare clic su "Add Schedule

Rule" (Aggiungi pianificazione).

2. Si apre questa finestra.

3. Per configurare la regola di pianificazione, specificare il nome, il commento, l'orario di inizio e di fine del filtraggio della rete.

4. Fare clic su "OK" e, quindi, su "Apply Changes" (Esegui modifiche) per salvare le impostazioni.

5. Per completare la configurazione bisognerà creare o modificare la regola dell'accesso nella sezione "Client IP filters" (Filtri IP Client). In questo modo si attiva la pianificazione dell'accesso nella pagina "Access Control" (Controllo accesso).

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Rule Name	Rule Comment	Configure
	No Valid Schedule Rule In	

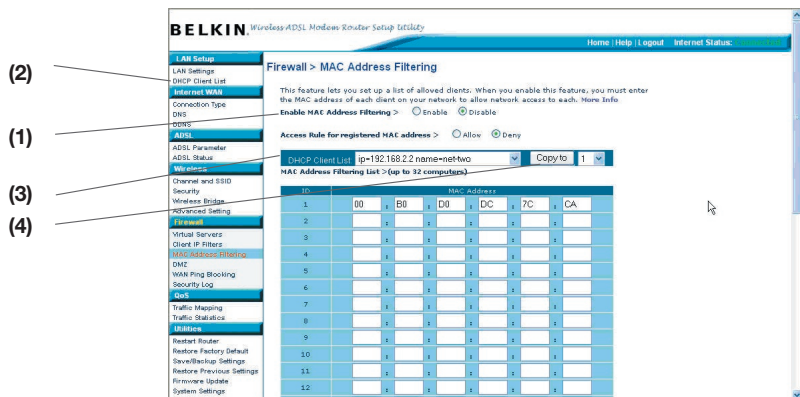
> Add Schedule Rule

[Clear Changes](#) [Apply Changes](#)

Impostazione del filtro indirizzi MAC

Il filtro indirizzi MAC è un potente mezzo per specificare quali sono i computer che possono accedere alla rete. Sarà negato l'accesso a qualsiasi computer che dovesse tentare di accedere alla rete e che non fosse specificato nell'elenco dei filtri. Quando questa opzione viene attivata, per consentirne l'accesso alla rete, è necessario digitare l'indirizzo MAC di ogni client (computer) presente nella propria rete. L'opzione "Block" (Blocca) consente di disattivare ed attivare facilmente l'accesso alla rete per qualsiasi computer senza dover aggiungere e togliere l'indirizzo MAC del computer dalla lista. Per attivare questa opzione, selezionare "Enable MAC Address Filtering" (Attiva filtro indirizzi MAC) (1). Successivamente, scegliere quale regola si vuole applicare: "Allow" (Permetti) o "Deny" (Nega).

Quindi inserire l'indirizzo MAC per ogni computer della rete, selezionandolo dal menu a discesa (2) l'opzione "DHCP Client List". Copiare l'ID da inserire, (3) quindi fare clic su "Copy to". In alternativa, fare clic nello spazio previsto (4) e inserire l'indirizzo MAC del computer che si desidera aggiungere all'elenco. Fare clic su "Apply Changes" (Esegui modifiche) (5) per salvare le impostazioni. Fare clic su "Apply Changes" (Applica modifiche) per salvare le impostazioni.



Nota bene: L'indirizzo MAC del computer utilizzato per accedere alle funzioni amministrative del router (il computer utilizzato in questo momento) non può essere cancellato.

DMZ (Demilitarized Zone)

Se si ha un PC client che non è in grado di gestire adeguatamente un'applicazione Internet da una protezione firewall, il client può aprire un accesso a Internet illimitato a due vie. Questa operazione potrebbe rivelarsi necessaria nel caso l'opzione NAT stesse causando problemi ad un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Questa opzione va sfruttata solo provvisoriamente. Il computer nella DMZ non è protetto dagli attacchi degli hacker.

Configurazione manuale del router

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** [More Info](#)

DMZ > ENABLE DISABLE

> IP Address of Virtual DMZ Host

Static IP	Static IP
1	192.168.2.0
2	192.168.2.0
3	192.168.2.0
4	192.168.2.0
5	192.168.2.0
6	192.168.2.0
7	192.168.2.0
8	192.168.2.0

Per inserire un computer nella DMZ, inserire le ultime cifre del suo indirizzo IP nel campo IP e selezionare “Enable” (Abilita). Fare clic su “Apply Changes” (Esegui modifiche) perché le modifiche abbiano effetto. Qualora si utilizzino diversi indirizzi statici WAN IP, è possibile selezionare a quale indirizzo WAN IP dirigere l’host DMZ. Digitare l’indirizzo WAN IP al quale si desidera indirizzare l’host DMZ, digitare le ultime due cifre dell’indirizzo IP del computer host DMZ, selezionare “Attiva” e fare clic su “Applica modifiche”.

Arresto di un Ping ICMP

Gli hacker informatici utilizzano quello che è noto come “pinging” per scoprire le potenziali vittime in Internet. Colpendo uno specifico indirizzo IP e ricevendo una risposta da detto indirizzo IP, un hacker è in grado di stabilire se ci sia qualcosa di interessante o meno. Il router può essere impostato in modo da non rispondere ad



un ping ICMP proveniente dall’esterno. In questo modo, il livello di protezione del proprio router aumenta.

Per disattivare la risposta al ping, selezionare “Block ICMP Ping” (Blocca ping ICMP) (1) e fare clic su “Apply Changes” (Esegui modifiche). Il router in questo modo non reagirà se colpito da un ping ICMP.

Utility

La schermata “Utility” consente di gestire diversi parametri del router ed eseguire alcune specifiche funzioni amministrative.

Utilities >

This screen lets you manage different parameters of the Router and perform certain administrative functions.

- **Restart Router**
Sometimes it may be necessary to Reset or Reboot the Router if it begins working improperly. Resetting or Rebooting the Router will not delete any of your configuration settings.
- **Restore Factory Defaults**
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults.
- **Save/Backup Current Settings**
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.
- **Restore Previous Saved Settings**
This option will allow you to restore a previously saved configuration.
- **Firmware Update**
From time to time, Linksys may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed.
- **System Settings**
The System Settings page is where you can enter a new administrator password, set the time zone, enable remote management and turn on and off the NAT function of the Router.

Riavvio del router

Potrebbe essere necessario riavviare il router in caso di malfunzionamento. Se il router dovesse essere riavviato, le impostazioni di configurazione NON saranno cancellate.

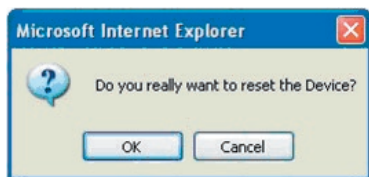
Utilities > Restart Router

Sometimes it may be necessary to Restart or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the "Restart Router" button below to Restart the Router.

Restart Router

Riavvio del router per ripristinare il normale funzionamento

1. Fare clic sul pulsante “Restart Router” (Riavvia il router).
2. Compare il seguente messaggio. Fare clic su “OK” per riavviare il router.



Restore Factory Defaults (Ripristina impostazioni predefinite)

Con questa opzione è possibile ripristinare tutte le impostazioni eseguite dal produttore del router. È consigliabile fare una copia di tutte le impostazioni prima di ripristinare quelle predefinite.

Utilities > Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.

Restore Defaults

Configurazione manuale del router

1. Fare clic sul pulsante “Restore Default” (Ripristina impostazioni predefinite).
2. Comparire il seguente messaggio. Fare clic su “OK” per ripristinare le impostazioni predefinite.

Salvataggio/Creazione di una copia di back up delle impostazioni correnti

Questa opzione consente di salvare la configurazione attuale. Il salvataggio della propria configurazione consente di ripristinarla in un momento successivo nel caso le impostazioni andassero perdute o venissero modificate. È consigliabile fare una copia della configurazione corrente prima di eseguire un aggiornamento del firmware.

1. Fare clic su “Save” (Salva). Comparire una finestra chiamata “File Download” (Scaricamento file). Fare clic su “Save” (Salva).
2. Si apre una finestra che consente di selezionare la posizione in cui salvare il file di configurazione. Selezionare una posizione. Non ci sono limiti rispetto al nome del file, tuttavia è necessario assegnare un nome che si è certi di ricordare successivamente. Una volta selezionata la posizione ed il nome del file, fare clic su “Salva”.

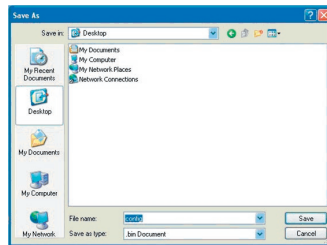
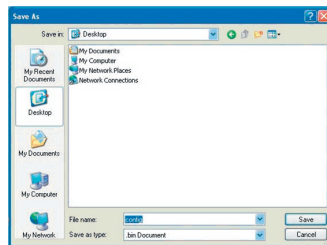
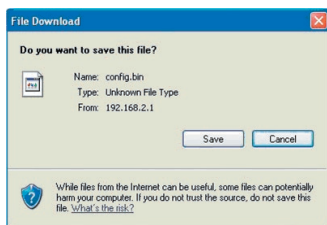
3. A salvataggio terminato, comparire la finestra illustrata di seguito. Selezionare “Close” (Chiudi). La configurazione è stata salvata.



UTILITIES > Save/Backup current settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

OK



Restore Previous Settings (Ripristina impostazioni precedenti)

Questa opzione consente di ripristinare qualsiasi configurazione salvata in precedenza.

Utilities > Restore Previous Settings

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the "Restore" button below.



1. Fare clic su "Browse" (Sfoglia). Si apre una finestra che consente di selezionare la posizione del file di configurazione. Cercare il file di configurazione "config.bin" ed eseguire doppio clic.
2. Quindi, fare clic su "Open" (Apri).

Aggiornamento del firmware

Di tanto in tanto, Belkin potrebbe pubblicare nuove versioni del firmware del router. Gli aggiornamenti del firmware contengono alcuni miglioramenti e consentono di risolvere possibili problemi esistenti nelle versioni precedenti. Quando la Belkin pubblica un nuovo firmware, questo può essere scaricato dal sito di aggiornamento Belkin, aggiornando in questo modo il firmware del router alla versione più recente.

Utilities > Firmware Update

Please click to view, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have occurred.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click here](#) to go to the backup/restore current settings page.



Controllo di una nuova versione del firmware

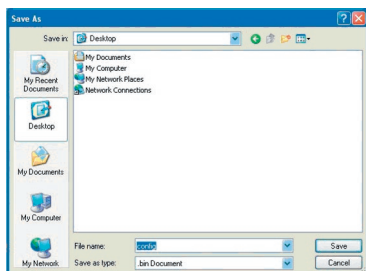
Il pulsante "Check Firmware" (Verifica firmware) (1) consente di verificare istantaneamente se esiste una nuova versione del firmware. Facendo clic su questo pulsante, compare una nuova finestra di browser che informa che non è disponibile nessun nuovo firmware o che esiste una nuova versione. Se esiste una nuova versione, è necessario scaricarla.

Download di una nuova versione del firmware

Facendo clic su "Check Firmware" (Verifica firmware), e se una nuova versione è disponibile, compare una schermata simile alla seguente.

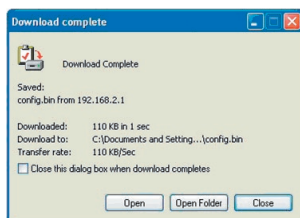
1. Per scaricare la nuova versione di firmware, fare clic su "Download".
2. Si apre una finestra che consente di selezionare la posizione in cui salvare il file firmware. Selezionare una posizione. A questo file può essere assegnato qualsiasi nome si desideri, oppure si può utilizzare il nome predefinito. Accertarsi di collocare il file in una posizione tale da consentirne il ritrovamento in un momento successivo. Una volta selezionata la posizione, fare clic su "Save" (Salva).
3. A salvataggio terminato, compare la finestra illustrata di seguito. Selezionare "Chiudi". Il download del firmware è terminato. Per aggiornare il firmware, seguire le indicazioni riportate di seguito in "Aggiornamento del firmware del router".

Configurazione manuale del router

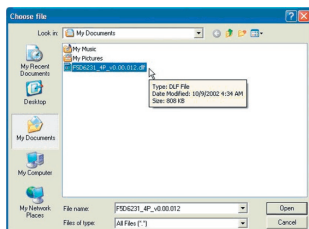


Aggiornamento del firmware del router

1. Dalla pagina “Firmware Update” (Aggiornamento firmware), fare clic su “Browse” (Sfoglia) (2). pls callout (2) in the screenshot]. Si apre una finestra che consente di selezionare la posizione del file di aggiornamento firmware.
2. Andare al file di firmware scaricato. Selezionarlo facendo doppio clic sul nome del file.



3. La casella “Update Firmware” (Aggiornamento firmware) ora visualizza la posizione ed il nome del file di firmware appena selezionato. Fare clic su “Update” (Aggiorna).



Utilities > Firmware Update

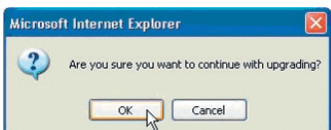
From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed.

NOTE: Please backup your current settings before updating to a new version of firmware. [Click Here](#) to go to the Save/Backup current settings page.

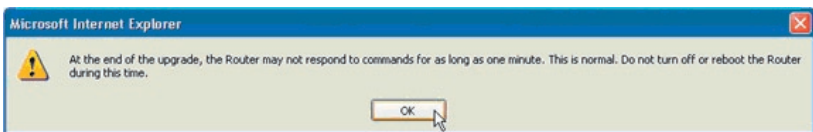
Firmware Version > 3.01.05
Check for new firmware version >

Update Firmware >

4. Vi verrà chiesto se si è certi di voler continuare. Fare clic su “OK”.



5. Compare un ulteriore messaggio. Questo messaggio dice che il router potrebbe non rispondere per un massimo di un minuto, in quanto il firmware è stato caricato nel router ed il router viene riavviato. Fare clic su “OK”.



Sullo schermo compare un conto alla rovescia di 60 secondi. Quando il conto alla rovescia raggiunge lo zero, l'aggiornamento del firmware del router è completo. La home page del router dovrebbe apparire automaticamente. In caso contrario, digitare l'indirizzo del router (predefinito = 192.168.2.1) nella barra di navigazione del proprio browser.

System Settings (Impostazioni del sistema)

Nella pagina “System Settings” è possibile inserire una nuova password per l'amministratore, impostare il fuso orario, attivare la gestione a distanza ed attivare e disattivare la funzione UPnP del router.

Impostazione o modifica della password amministratore

Il router viene fornito SENZA password. Se si desidera impostare una password per avere una maggiore protezione, lo si può fare da qui. La password deve essere annotata e custodita in un posto sicuro, in quanto sarà necessaria per connettersi al router in futuro. È anche consigliabile inserire una password nel caso si intenda utilizzare l'opzione di gestione a distanza del router.

Utilities > System Settings

Administrator Password:

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

Modifica della durata di connessione

L'opzione di durata connessione consente di impostare un intervallo di tempo di connessione all'interfaccia avanzata di impostazione del router. Il timer parte dal momento in cui non si rileva alcuna attività. Ad esempio, se fosse stata apportata qualche modifica all'interfaccia di impostazione avanzata, il computer si gestirà da solo senza dover fare clic su "Logout". Supponendo che la durata di connessione sia stata impostata su 10 minuti, dopo 10 minuti di mancato utilizzo del computer, la sessione di connessione verrà interrotta. Si deve allora effettuare un nuovo "login" all'adattatore per poter apportare altre modifiche. L'opzione di durata della connessione è prevista a scopo cautelativo ed è preimpostata su 10 minuti. Nota bene: è possibile connettere un computer alla volta all'interfaccia avanzata delle impostazioni del router.

Impostazione dell'ora e del fuso orario

Il router aggiorna l'orario collegandosi ad un server SNTP (Simple Network Time Protocol). In questo modo il router è in grado di sincronizzare l'orologio del sistema con la rete Internet mondiale. L'orologio sincronizzato presente nel router viene utilizzato per registrare l'elenco di protezione e controllare il filtro client. Selezionare il fuso orario della zona in cui si risiede. Se si vive in una zona che osserva l'ora legale, inserire un segno di spunta nella casella accanto a "Enable Daylight Saving" (Attiva ora legale). L'orologio del sistema potrebbe non aggiornarsi immediatamente. Attendere almeno 15 minuti perché il router contatti i server dell'orario su Internet e riceva una risposta. L'utente non può impostare autonomamente l'orologio. Viene data la possibilità di scegliere un server NTP primario e uno di backup per poter mantenere l'orologio del

router sincronizzato con diverso server di orario su Internet. Selezionare il server NTP dal menu a tendina o semplicemente non apportare modifiche.

Time and Time Zone: **August 1, 2003 4:26:00 AM**

Please set your time zone. If you are in an area that observes daylight saving check this box. [More Info](#)

Daylight Savings

Set Time Zone > (GMT-08:00)Pacific Time (US & Canada), Tijuana

Configure Time Server (NTP) > Enable Automatic Time Server Maintenance

Primary Server > 132.163.4.102 - North America

Secondary Server > 192.5.41.41 - North America

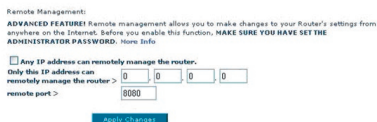
[Apply Changes](#)

Attivazione della gestione a distanza

Prima di attivare questa funzione avanzata del router Belkin, ACCERTARSI DI AVER IMPOSTATO LA PASSWORD AMMINISTRATORE. La gestione a distanza consente di modificare le impostazioni del router da qualsiasi punto di Internet.

Esistono due metodi per gestire a distanza il router. Il primo consente di accedere al router da qualsiasi punto di Internet selezionando “Any IP address can remotely manage the Router” (Qualsiasi indirizzo IP può gestire a distanza il router). Digitando il proprio indirizzo WAN IP da qualsiasi computer in Internet, compare una schermata di connessione nella quale è necessario digitare la password del proprio router. Il secondo metodo consiste nel consentire ad uno specifico indirizzo IP di gestire soltanto a distanza il router. Questo metodo è più sicuro, ma meno comodo. Per utilizzare questo metodo, digitare l’indirizzo IP dal quale si sa di accedere al router nello spazio previsto e selezionare “Only this IP address can remotely manage the Router” (Soltanto questo indirizzo IP può gestire a distanza il router).

Prima di attivare questa funzione è FORTEMENTE CONSIGLIATO aver impostato la propria password amministratore. Lasciando la password vuota, potenzialmente si apre il router ad eventuali intrusioni esterne. Per impostazione predefinita la porta di accesso remoto è 8080. Si può scegliere un’altra porta digitando un nuovo numero nel campo “remote port” (porta remota). Fare clic su “Apply Changes” (Esegui modifiche) per salvare le proprie impostazioni.



Enabling/Disabling NAT (Network Address Translation) (Abilitazione/Disabilitazione NAT)

Nota bene: Questa funzione avanzata dovrebbe essere implementata soltanto dagli utenti esperti. Prima di attivare questa funzione, ACCERTARSI DI AVER IMPOSTATO LA PASSWORD AMMINISTRATORE. Il NAT (Network Address Translation) è il metodo attraverso il quale il router condivide un unico indirizzo IP assegnato dal proprio ISP con gli altri computer presenti nella rete. Utilizzare questa funzione soltanto se l'ISP assegna all'utente diversi indirizzi IP o se si desidera che l'opzione NAT venga disattivata per una configurazione avanzata del sistema. Se si ha un solo indirizzo IP e si disattiva l'opzione NAT, i computer all'interno della rete non sono in grado di

accedere ad Internet. Si potrebbero verificare anche altri problemi. La disattivazione dell'opzione NAT disattiva le funzioni della protezione firewall.



Abilitare/disabilitare il servizio Universal Plug-and-Play (Universal Plug-and-Play).

Il servizio UPnP (Universal Plug-and-Play) è un'altra opzione avanzata messa a disposizione dal router Belkin. Si tratta di una tecnologia in grado di offrire un funzionamento diretto delle opzioni di trasmissione di messaggi vocali, video, giochi ed altre applicazioni conformi agli standard UPnP.

Per funzionare correttamente, alcune applicazioni richiedono che la protezione firewall del router sia configurata in maniera specifica. Per farlo è generalmente necessario aprire le porte TCP e UDP e, in alcuni casi, impostare le porte trigger. Un'applicazione conforme al servizio UPnP ha la capacità di comunicare con il router, fondamentalmente "dicendo" al router come configurare la protezione firewall. Il router viene fornito con l'opzione UPnP disabilitata. Se si sta utilizzando una qualsiasi applicazione conforme al servizio UPnP, e si desidera utilizzare le opzioni UPnP, queste

si possono attivare. È sufficiente selezionare "Enable" (Abilita) nella sezione "UPnP Enabling" (Abilitazione UPnP) della pagina "Utilities" (Utility). Fare clic su "Apply Changes" (Applica modifiche) per salvare la modifica.

UPnP Enabling:
ADVANCED FEATURE! Allows you to turn the UPnP feature of the Router on or off. If you use applications that support UPnP, enabling UPnP will allow these applications to automatically configure the router. [Home Info](#)

UPnP Enable / Disable > Enable Disable

[Apply Changes](#)

Abilitazione / disabilitazione del servizio Auto Firmware Update

Questa novità mette a disposizione del router la capacità integrata di ricercare automaticamente una nuova versione di firmware ed avvisare l'utente della disponibilità del nuovo firmware. Nel momento in cui avviene la connessione con l'interfaccia utente avanzata basata sul web del router, il router esegue un controllo per verificare la disponibilità di nuovo firmware. In questo caso, si viene avvisati. È possibile scegliere se scaricare la nuova versione o ignorarla. Il router

viene fornito con questa opzione disabilitata. Per abilitarla, selezionare "Enable" (abilita) e fare clic su "Apply Changes" (Esegui modifiche).

Auto Update Firmware Enabling:
ADVANCED FEATURE! Allows you to automatically check the availability of firmware updates for your router. [Home Info](#)

Auto Update Firmware Enable / Disable > Enable Disable

[Apply Changes](#)

Configurazione dei computer

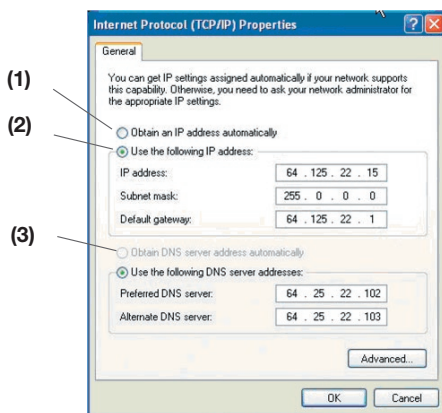
Per consentire al computer di comunicare correttamente con il router, è necessario modificare le impostazioni "TCP/IP Ethernet" e impostarle su "Obtain an IP address automatically/Using DHCP" (Ottieni un indirizzo IP automaticamente/Utilizzando DHCP). Si tratta dell'impostazione normalmente predefinita nella maggior parte dei computer d'uso domestico.

INNANZITUTTO, impostare il computer collegato al modem ADSL seguendo queste fasi. Le stesse operazioni si possono eseguire anche per aggiungere altri computer al router dopo aver impostato il router in modo da collegarlo ad Internet.

Configurazione manuale degli adattatori di rete

Windows XP, 2000, o NT

1. Fare clic su “Start”, “Settings” (Impostazioni) e quindi su “Control Panel” (Pannello di controllo).
2. Fare doppio clic sull'icona “Network and dial-up connections” (Connessione di rete ed accesso remoto) (Windows 2000) o sull'icona “Network” (Rete) (Windows XP).
3. Fare clic con il tasto destro del mouse sull'opzione “Local Area Connection” (Connessione locale) associata alla propria scheda di rete e selezionare “Properties” (Proprietà) dal menu a tendina.



4. Dalla finestra “Local Area Connection Properties” (Proprietà connessione locale) fare clic su “Internet Protocol (TCP/IP) (Protocollo Internet (TCP/IP) e fare clic sul pulsante “Properties” (Proprietà). Comparare la seguente schermata.
5. Se l'opzione “Use the following IP address” (2) (Specifica l'indirizzo IP), il router deve essere impostato per un tipo di connessione IP statica. Scrivere le informazioni relative all'indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.

1
2
3
4
5
6
7
8
9
10
11

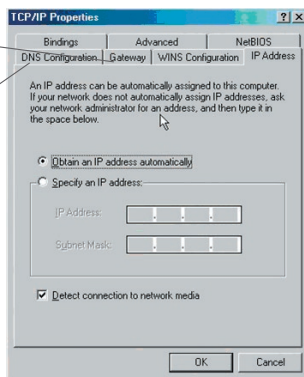
sezione

Configurazione manuale degli adattatori di rete

- Se non fosse già selezionata, selezionare l'opzione "Obtain an IP address automatically" (Ottieni automaticamente un indirizzo IP) (3) e Obtain DNS server address automatically" (Ottieni automaticamente un indirizzo server DNS) (3). Fare clic su "OK". L'adattatore di rete è ora configurato per consentire l'utilizzo del router.

Per gli utenti di Windows 98SE o Millennium Edition:

- Con il tasto destro del mouse, fare clic su "My Network Neighborhood" e selezionare "Properties" (Proprietà).
- Selezionare "TCP/IP -> settings" (Impostazioni TCP/IP) per l'adattatore di rete installato. Si apre questa finestra.
- Se è stata selezionata l'opzione "Specify an IP address" (Specifica l'indirizzo IP), il router deve essere impostato per un tipo di connessione IP statica. Scrivere le informazioni relative all'indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.
- Annotare l'indirizzo IP e la subnet mask dalla scheda "IP Address" (Indirizzo IP) (3).
- Fare clic sulla scheda "Gateway" (2). Trascrivere l'indirizzo gateway nella tabella.
- Fare clic sulla scheda "DNS Configuration" (Configurazione DNS)(1). Trascrivere l'indirizzo (gli indirizzi) DNS nello schema.
- Se non fosse già selezionata, selezionare l'opzione "Obtain an IP address automatically" (Ottieni automaticamente un indirizzo IP) (1) dalla scheda di indirizzo IP. Fare clic su "OK". Riavviare il computer. Quando il computer verrà riavviato, gli adattatori di rete saranno configurati per essere utilizzati con il router. INNANZITUTTO, impostare il computer collegato al modem via cavo o ADSL seguendo queste fasi. Le medesime operazioni si possono eseguire anche per aggiungere altri computer al router dopo averne impostato il collegamento ad Internet.



(2)
(1)

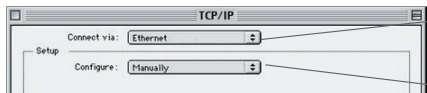
(3)

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

Mac OS 9.0 – 9.x

Per consentire al computer di comunicare correttamente con il router, è necessario modificare le impostazioni TCP/IP del computer Mac in DHCP.

- Aprire il menu "Apple" Selezionare dapprima "Control Panels"(Pannelli di controllo) e quindi "TCP/IP".



(1)
(2)

- Compare il pannello di controllo TCP/IP. Dal menu a tendina "Connect via" (Collega via),

Configurazione manuale degli adattatori di rete

selezionare “Ethernet Built In” (Ethernet Integrato) o “Ethernet”. dal menu a tendina (1).

IP address:

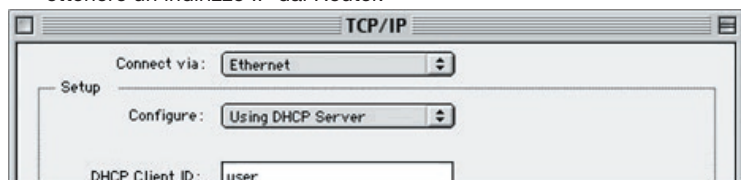
Subnet Mask:

Default gateway:

Preferred DNS server:

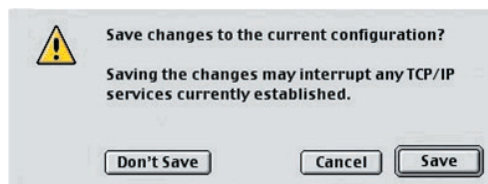
Alternate DNS server:

3. Accanto a “Configure” se è stato selezionato “Manually” (Manualmente), il router deve essere impostato in modo da eseguire un tipo di connessione IP statico. Scrivere le informazioni relative all’indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.
4. Se non fosse già impostato, in “Configure:” (Configura), selezionare “Using DHCP Server” (Utilizzando server DHCP). Questo indicherà al computer di ottenere un indirizzo IP dal Router.



5. Chiudere la finestra. Nel caso fossero state fatte alcune modifiche, compare la seguente videata: Fare clic su “Save” (Salva).

Riavviare il computer. Quando il computer verrà riavviato, le impostazioni di rete saranno configurate per essere utilizzate con il router.



Mac OS X

1. Fare clic sull'icona “System Preferences” (Preferenze del sistema).



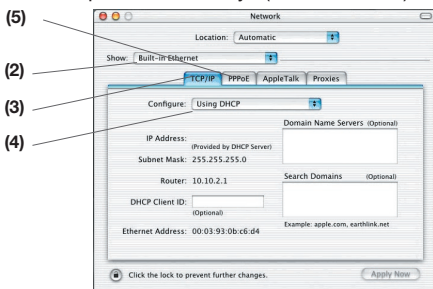
1
2
3
4
5
6 sezione
7
8
9
10
11

Configurazione manuale degli adattatori di rete

2. Selezionare “Network” (Rete) (1) dal menu “System Preferences” (Preferenze del sistema).



3. Selezionare “Built-in Ethernet” (2) accanto all’opzione “Show” (Mostra) nel menu Network (Rete).
4. Selezionare la scheda “TCP/IP” (3). Accanto a “Configure” (Configura) (4), dovrebbero comparire “Manually” (Manualmente) o “Using DHCP” (Utilizzando



l’opzione DHCP). In caso contrario, verificare nella scheda PPPoE (5) che l’opzione “Connect using PPPoE” (Connetti utilizzando PPPoE) NON sia selezionata. Se lo fosse, il router deve essere configurato per un tipo di connessione PPPoE, usando il proprio nome utente e password.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

5. Se è stato selezionato “Manually” (Manualmente), il router deve essere impostato in modo da eseguire un tipo di connessione IP statico. Scrivere le informazioni relative all’indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.
6. Se non fosse già selezionato, selezionare “Using DHCP Server” (Utilizzando server DHCP) accanto a “Configure” (Configura) (4), quindi fare clic su “Apply Now” (Esegui ora).

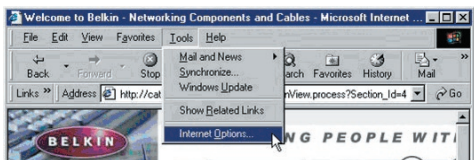
L’adattatore è ora configurato per consentire l’utilizzo del router.

Impostazioni del browser web consigliate

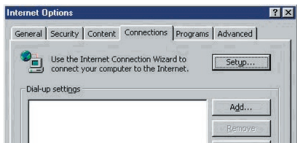
Nella maggior parte dei casi non è necessario eseguire molte modifiche alle impostazioni del browser web. Nel caso l'accesso a Internet o l'utilizzo dell'interfaccia utente avanzata basata sul web creassero qualche problema, modificare le impostazioni del browser in base alle impostazioni consigliate in questo capitolo.

Microsoft Internet Explorer 4.0 o successivo

1. Avviare il browser Web. Selezionare “Tools” (Strumenti) e “Internet Options” (Opzioni Internet)

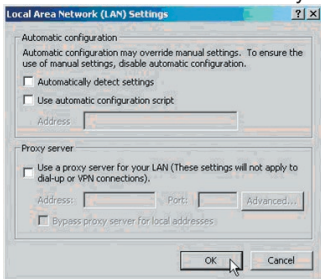


2. Nella schermata “Internet Options” (Opzioni Internet) compaiono tre selezioni. “Never dial a connection” (Non utilizzare mai connessioni remote), “Dial whenever a network connection is not present” (Usa connessione remota se non è disponibile una connessione di rete) e “Always dial my default connection” (Utilizza sempre la connessione remota predefinita). Se è possibile, selezionare “Non utilizzare mai connessioni remote”. Nel caso non fosse possibile eseguire una selezione, passare alla fase successiva.



3. Nella finestra “Internet Options” (Opzioni Internet), cliccare su “Connections” (Connessioni) e selezionare “LAN Settings...” (Impostazioni LAN).

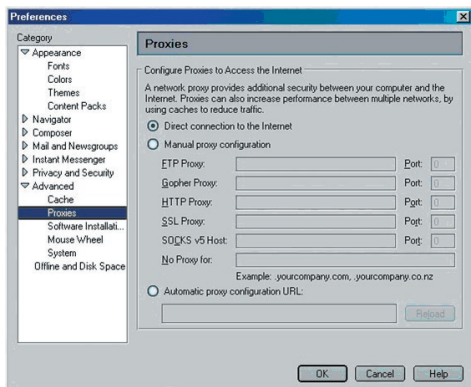
4. Accertarsi che non vi siano segni di spunta vicino a nessuna delle opzioni visualizzate: “Automatically detect settings” (Rileva automaticamente impostazioni) e “Use a proxy server” (Utilizza un server proxy). Fare clic su “OK”. Ancora un clic su “OK” nella pagina delle “Opzioni Internet”.



1
2
3
4
5
6
7 sezione
8
9
10
11

Netscape®Navigator® versione 4.0 o successiva.

1. Avviare Netscape. Clic su “Modifica”, quindi su “Preferenze”.
2. Nella finestra delle preferenze, cliccare su “Advanced” (Avanzate), quindi selezionare “Proxies”. Nella finestra “Proxies”, selezionare “Direct connection to the Internet” (Connessione diretta a Internet).



Risoluzione delle anomalie

Problema:

Il LED ADSL è spento.

Soluzione:

1. Controllare lo stato della connessione tra il router e la linea ADSL. Accertarsi che il cavo della linea ADSL sia collegato alla porta del router marcata “DSL Line”.
2. Assicurarsi che il router sia alimentato. Il LED Power (Alimentazione) sul pannello anteriore dovrebbe essere illuminato.

Problema:

Il LED Internet è spento.

Soluzione:

1. Accertarsi che il cavo della linea ADSL sia collegato alla porta del router marcata “DSL Line” e che il LED ADSL sia acceso.
2. Accertarsi di aver ricevuto i parametri VPI/VCI, nome utente e password corretti dal proprio ISP.

Problema:

Il mio tipo di connessione è “un indirizzo IP statico”. Non riesco a connettermi a Internet.

Soluzione:

Se la vostra connessione prevede un indirizzo IP statico, il vostro ISP deve assegnarvi un indirizzo IP, una subnet mask e l'indirizzo gateway. Al posto di usare il programma di impostazione guidata, andare in “Connection Type” (Tipo di connessione) e selezionare il proprio tipo di connessione. Fare clic su “Next” (Avanti), selezionare “Static IP” (IP statico) e digitare il proprio indirizzo IP, la subnet mask e le informazioni relative al gateway predefinito.

Problema:

Ho dimenticato o smarrito la password.

Soluzione:

Premere per almeno 6 secondi il pulsante “Reset” sul pannello posteriore per ripristinare le impostazioni predefinite.

Problema:

Il mio PC wireless non riesce a collegarsi al router.

Soluzione:

1. Accertarsi che le impostazioni SSID del PC wireless siano le stesse del router e che le impostazioni di sicurezza, come ad esempio la crittografia WPA o

1

2

3

4

5

6

7

8

9

10

11

sezione

WEP, siano uguali per tutti i client.

2. Accertarsi che il router e il PC wireless non siano troppo distanti tra loro.

Problema:

La rete wireless si interrompe spesso.

Soluzione:

1. Avvicinare il PC wireless al router per ottenere un segnale migliore.
2. Ci potrebbero essere anche alcune interferenze, causate da un forno a microonde o dai telefoni cordless da 2,4 GHz. Spostare il router o utilizzare un canale wireless diverso.

Problema:

Non si riesce ad impostare un collegamento a Internet in modalità wireless.

Soluzione:

Nell'impossibilità di collegarsi a Internet, si consiglia di controllare quanto segue:

1. Controllare le spie del router. Se si sta usando un Router Belkin, le spie dovrebbero essere così:
 - La spia "Power" (Alimentazione) dovrebbe essere accesa.
 - La spia di collegamento (Connected) dovrebbe essere accesa e non lampeggiante.
 - La spia "WAN" dovrebbe essere accesa o lampeggiante.
2. Aprire il software della utility wireless facendo clic sull'icona nel desktop di sistema nell'angolo in basso a destra dello schermo. Se si sta usando una scheda wireless Belkin, l'icona nel desktop di sistema dovrebbe essere così (l'icona può essere rossa o verde):
3. La finestra che si apre può cambiare secondo il modello della scheda wireless; tuttavia, una delle utility dovrebbe contenere un elenco con le "Reti disponibili": le reti wireless disponibili alle quali è possibile collegarsi.

Il nome della rete wireless appare nei risultati?

Sì, il nome della mia rete è in elenco – passare alla soluzione dal titolo "Non riesco a collegarmi ad internet in modalità wireless, ma il nome della mia rete è in elenco".

No, il nome della mia rete non è in elenco. Passare alla soluzione delle anomalie dal titolo "Non riesco a collegarmi ad Internet in modalità wireless e il nome della mia rete non è in elenco".

Problema:

Non riesco a collegarmi ad Internet in modalità wireless, ma il nome della mia rete è in elenco.

Soluzione:

Se il nome della rete appare nell'elenco "Reti disponibili", seguire le seguenti indicazioni per collegarsi in modalità wireless:

1. Fare clic sul nome corretto della rete nell'elenco "Reti disponibili".

Se la protezione (crittografia) della rete è stata attivata, bisognerà digitare la chiave di rete. Per ulteriori informazioni sulla protezione, vedere la pagina "Modifica delle impostazioni di protezione della rete wireless".

2. In pochi secondi, l'icona di sistema nell'angolo in basso a sinistra dello schermo dovrebbe diventare verde, indicando la corretta connessione alla rete.

Problema:

Non riesco a collegarmi ad internet in modalità wireless e il nome della mia rete non è in elenco

Soluzione:

Se il nome corretto della rete non appare nell'elenco "Reti disponibili", seguire le seguenti indicazioni per risolvere il problema:

1. Se possibile, spostare provvisoriamente il computer a 1,5 / 3 m dal router.

Chiudere la utility Wireless ed aprirla di nuovo. Se il nome corretto della rete ora appare nell'elenco "Available Networks", potrebbe trattarsi di un problema di copertura o di interferenza. Vedere i suggerimenti nell'allegato B intitolato "Considerazioni importanti per il posizionamento e la configurazione".

2. Se si sta usando un computer collegato al router mediante un cavo di rete (anziché in modalità wireless), assicurarsi che la funzione "Broadcast SSID" (Trasmetti SSID) sia abilitata. Questa impostazione può essere trovata nella pagina di configurazione wireless "Channel and SSID" (Canale e SSID).

Se, dopo aver seguito queste istruzioni, non fosse ancora possibile accedere a Internet, contattare l'Assistenza Tecnica Belkin.

Problema:

Il livello delle prestazioni della rete wireless non è buono

Il trasferimento dei dati a volte è lento.

Il segnale è debole.

Si incontrano difficoltà nell'impostare e/o mantenere una connessione con una rete VPN (Virtual Private Network)

Soluzione:

La tecnologia wireless è basata sulla tecnologia radio. Ciò significa che la connettività e le prestazioni di trasmissione tra i dispositivi diminuiscono con l'aumentare della distanza. Altri fattori che possono causare un indebolimento del segnale (il metallo è generalmente l'indiziato numero uno) sono gli ostacoli

quali muri e apparecchiature in metallo. Di conseguenza, la copertura tipica per i dispositivi wireless in un ambiente chiuso è compresa tra i 30 e i 60 metri. Inoltre, se ci si allontana ulteriormente dal router o dall'access point wireless, la velocità della connessione diminuisce.

Per determinare se i problemi wireless siano dovuti a fattori di copertura, provare a posizionare il computer a 1,5 metri e 3 metri di distanza dal router.

Cambiare il canale wireless - A seconda del traffico wireless locale e delle interferenze, cambiare il canale wireless della rete può migliorarne le prestazioni e l'affidabilità. Il canale predefinito del router è l'11, tuttavia, si possono scegliere altri canali, a seconda del paese nel quale ci si trova. Consultare il capitolo intitolato "Modifica del canale wireless" a pagina XX per le istruzioni su come scegliere altri canali wireless.

Limitazione della trasmissione dati wireless - Limitare la trasmissione dati può aiutare a migliorare la copertura wireless e la stabilità della connessione. La maggior parte delle schede di rete offre la possibilità di limitare la trasmissione dati. Per cambiare questa proprietà, andare sul pannello di controllo di Windows, aprire le Connessioni di rete e fare doppio clic sulla connessione della scheda wireless. Nella finestra di dialogo "Properties" (Proprietà), nella tabella "General" (Generale) selezionare il pulsante "Configure" (Configura) (gli utenti Windows 98 dovranno selezionare la scheda wireless nell'elenco e quindi fare clic su "Properties" (Proprietà), quindi fare clic su la tabella "Advanced" (Avanzate) e selezionare le caratteristiche di trasmissione. Le velocità di trasmissione delle schede di rete dei client wireless sono generalmente preimpostate, tuttavia si possono verificare periodiche disconnessioni quando il segnale wireless è troppo basso. Generalmente, le velocità di trasmissione più lente sono le più stabili. Provare varie velocità fino a trovare la migliore per la propria rete; notare che tutte le trasmissioni di rete disponibili dovrebbero essere accettabili per la navigazione in Internet. Per maggiori chiarimenti consultare il manuale della scheda wireless.

Problema:

Come posso estendere la portata della rete wireless?

Soluzione:

Per estendere la copertura della rete nel caso di abitazioni o uffici di grandi dimensioni, Belkin consiglia di utilizzare uno dei seguenti prodotti:

- **Access Point Wireless** Un access point wireless può effettivamente raddoppiare la copertura di una rete wireless. Un Access point viene generalmente collocato nella zona non attualmente coperta dal proprio router wireless e collegato al router usando un cavo Ethernet, oppure attraverso le linee di alimentazione domestiche utilizzando due adattatori Powerline Ethernet.

- Per le reti wireless 802.11g (54g), Belkin offre un Range Extender/Access Point Wireless da collegare in modalità wireless al router wireless Belkin 802.11g senza bisogno di un cavo Ethernet o di adattatori Powerline Ethernet.

Questi prodotti Belkin sono disponibili presso i punti vendita locali o si possono ordinare direttamente da Belkin.

Per ulteriori informazioni sull'estensione della rete/portata, potete visitare il sito: www.belkin.com/networking per saperne di più su:

Range Extender/Access Point G Wireless (F5D7132)

Problema:

Si incontrano alcune difficoltà nell'impostare la protezione Wired Equivalent Privacy (WEP) in un router o access point Belkin

Soluzione:

1. Collegarsi al router o all'access point wireless.
2. Aprire il browser web e digitare l'indirizzo IP del router o dell'access point wireless. (Il router è preimpostato su 192.168.2.1, l'access point 802.11g su 192.168.2.254). Collegarsi al router cliccando il pulsante "Login" nell'angolo in alto a destra dello schermo. Viene richiesto di inserire una password. Se non fosse mai stata impostata alcuna password, lasciare il campo password in bianco e cliccare "Submit" (Inoltra).
3. Fare clic sulla scheda "Wireless" sul lato sinistro dello schermo. Selezionare la scheda "Encryption" (Crittografia) o "Security" (Protezione) per accedere alla pagina delle impostazioni di sicurezza.
4. Selezionare "128-bit WEP" dal menu a tendina.
5. Dopo aver selezionato la propria modalità di crittografia WEP, si può digitare a mano la propria chiave esadecimale WEP, oppure si può digitare una frase di accesso nel campo "Passphrase" e fare clic su "Generate" per creare una chiave WEP dalla frase di accesso. Fare clic su "Apply Changes" (Esegui modifiche) per terminare. Ora tutti i propri client vanno adattati a queste impostazioni. Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit è necessario inserire una chiave composta da 26 caratteri esadecimali.

Ad esempio:

C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = chiave a 128 bit

6. Fare clic su "Applica modifiche" per terminare. La crittografia del router wireless è impostata. Ogni computer presente nella rete wireless deve essere configurato con le medesime impostazioni di protezione.

AVVERTENZA: se si stesse eseguendo la configurazione del router o dell'access point wireless da un computer con un client wireless, sarà necessario accertarsi che la protezione per questo client wireless sia attiva. In caso contrario si perderà la connessione wireless.

1

2

3

4

5

6

7

8

9

10

11

Nota per gli utenti Mac: i prodotti originali Apple AirPort supportano soltanto la crittografia a 64 bit. I prodotti Apple Airport 2 possono supportare le modalità di crittografia a 64 o 128 bit. Verificare quale sia la versione utilizzata nel proprio prodotto Apple AirPort. Non potendo configurare la rete con una crittografia a 128 bit, provare una crittografia a 64 bit.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wired Equivalent Privacy (WEP) in una scheda wireless Belkin.

Soluzione:

La scheda wireless deve utilizzare la stessa chiave del router wireless o dell'access point. Ad esempio, se il router wireless o l'access point utilizza la chiave 00112233445566778899AABBCC, la scheda client deve essere impostata esattamente con la stessa chiave.

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Rete wireless".
2. Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
3. Dopo aver premuto il pulsante "Advanced", appare la Utility LAN Wireless Belkin. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda "Proprietà di rete wireless", selezionare un nome dall'elenco "Reti disponibili" e fare clic su "Proprietà".
5. In "Data Encryption" (Crittografia dati), selezionare "WEP".
6. Disattivare la casella in basso "The key is provided for me automatically" (Fornisci automaticamente la chiave di rete). Se si usa il computer per collegarsi ad una rete aziendale, chiedere al proprio amministratore di rete se la casella deve essere attivata.
7. Digitare la chiave WEP nella casella "Network key" (Chiave di rete).

Importante:una chiave WEP è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit, vanno inseriti 26 caratteri. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

Ad esempio: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = codice a 128 bit

8. Fare clic su "OK" e, quindi, su "Esegui" per salvare le impostazioni.

Se NON si utilizza una scheda wireless Belkin, richiedere al produttore il manuale d'uso per la scheda client wireless utilizzata.

Problema:

I prodotti Belkin supportano la modalità WPA?

Soluzione:

Nota bene: Per utilizzare la protezione WPA, tutti i client devono disporre dei driver e del software in grado di supportarla. Al momento della pubblicazione di questo elenco di domande e risposte, è possibile scaricare gratuitamente un security patch da Microsoft, adatto soltanto al sistema operativo Windows XP.

Il patch può essere scaricato al sito:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

Dal sito di assistenza Belkin è necessario anche scaricare il driver più recente per la propria scheda di rete wireless 802.11g per computer desktop o notebook Belkin. Attualmente gli altri sistemi operativi non sono supportati. Il patch di Microsoft supporta esclusivamente i dispositivi che prevedono driver con la funzione WPA abilitata, tra cui i prodotti 802.11g Belkin.

Scaricare il driver più recente da: <http://www.belkin.com/uk/support/tech/index.asp>

Problema:

Si incontrano difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in un router o access point Belkin per una rete domestica.

Soluzione:

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA-PSK (no server)".
2. Per "Encryption Technique", scegliere "TKIP" o "AES". Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare la propria chiave precondivisa, che può essere composta da una combinazione di lettere, numeri o caratteri o spazi, da un minimo di 8 a un massimo di 63. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati. Ad esempio, la propria PSK potrebbe essere qualcosa del tipo: "Chiave di rete famiglia Rossi".
4. Fare clic su "Applica modifiche" per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in un router o access point Belkin per una rete aziendale.

1

2

3

4

5

6

7

8

9

10

11

Soluzione:

Se la vostra rete utilizza un radius server per distribuire le chiavi ai client, utilizzare questa impostazione. Questa soluzione viene generalmente utilizzata nell'ambiente lavorativo.

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA-PSK (with server)".
2. Per "Encryption Technique", scegliere "TKIP" o "AES". Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare l'indirizzo IP del radius server nei campi "Radius Server".
4. Digitare la chiave radio nel campo "Radius Key".
5. Digitare l'intervallo chiave. L'intervallo chiave indica la frequenza di distribuzione delle chiavi (in pacchetti).
6. Fare clic su "Applica modifiche" per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless Belkin per una rete domestica.

Soluzione:

I client devono utilizzare la stessa chiave del router wireless o dell'access point. Ad esempio, se la chiave nel router wireless o nell'access point è "Codice rete famiglia Rossi", anche i client devono utilizzare la stessa chiave.

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Rete wireless".
2. Il pulsante "Avanzate" consente di visualizzare e configurare diverse opzioni della scheda.
3. Dopo aver premuto il pulsante "Advanced", appare la Utility LAN Wireless Belkin. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda "Proprietà di rete wireless", selezionare un nome dall'elenco "Reti disponibili" e fare clic su "Proprietà".
5. In "Network Authentication" (Autenticazione di rete) selezionare "WPA-PSK (No Server)".
6. Digitare la chiave WEP nella casella "Chiave di rete".

Importante: una chiave WPA-PSK è composta da numeri e lettere, da 0 a 9 e dalla A alla Z. Per la protezione WPA-PSK, si possono inserire da 8 a 63 chiavi. Questo codice di rete deve essere uguale a quello assegnato al router wireless (o all'access point).

7. Fare clic su "OK" e, quindi, su "Esegui" per salvare le impostazioni.

Problema:

Si incontrano difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless Belkin per una rete aziendale.

Soluzione:

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Rete wireless".
2. Il pulsante "Avanzate" consente di visualizzare e configurare diverse opzioni della scheda.
3. Dopo aver premuto il pulsante "Advanced", appare la Utility LAN Wireless Belkin. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda "Proprietà di rete wireless", selezionare un nome dall'elenco "Reti disponibili" e fare clic su "Proprietà".
5. In "Autenticazione di rete" selezionare "WPA".
6. Nella scheda "Autenticazione", selezionare le impostazioni indicati dall'amministratore di rete.
7. Fare clic su "OK" e, quindi, su "Esegui" per salvare le impostazioni.

Problema:

Ho difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless NON Belkin per una rete domestica.

Soluzione:

Per le schede di rete wireless per computer desktop e notebook di altre marche, sprovviste del software WPA, si può scaricare gratuitamente un file da Microsoft chiamato "Windows XP Support Patch for Wireless Protected Access". Scaricare il patch da Microsoft ricercando nei dati base per Windows XP WPA.

Nota bene: il file messo a disposizione da Microsoft funziona soltanto con Windows XP. Attualmente gli altri sistemi operativi non sono supportati. È necessario accertarsi inoltre che il produttore della scheda wireless supporti la protezione WPA e di aver scaricato e installato il driver più recente dal suo sito.

Sistemi operativi supportati:

- Windows XP Professional
- Windows XP Home Edition

Attivazione dell'opzione WPA-PSK (senza server)

1. In Windows XP, fare clic su Start > Pannello di controllo > Connessioni di rete.
2. Cliccando sulla scheda "Reti wireless" si aprirà la seguente schermata. Accertarsi che l'opzione "Use Windows to configure my wireless network settings" (Utilizza Windows per configurare le impostazioni di rete wireless) sia attivata.

1

2

3

4

5

6

7

8

9

10

11

3. Nella scheda “Reti wireless”, fare clic su “Configura”.
4. Nel caso di una rete domestica o di un piccolo ufficio, selezionare “WPA-PSK” da “Amministrazione rete”.

Nota bene: selezionare “WPA (with radius server)” se si sta utilizzando il computer per collegarsi ad una rete aziendale che supporta un server di autenticazione come può essere un radius server. Per ulteriori informazioni, rivolgersi all'amministratore di rete.

5. Selezionare “TKIP” o “AES” da “Data Encryption” (Crittografia dati). Questa impostazione deve essere identica a quella del router wireless o dell'access point configurato.
6. Digitare il codice di crittografia nella casella “Codice rete”.

Importante: Inserire la propria chiave precondivisa (PSK), che può essere lunga da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati.

7. Fare clic su “OK” per confermare le impostazioni.

Qual è la differenza tra 802.11b, 802.11g, 802.11a, e Pre-N?

Attualmente esistono quattro livelli di standard di rete wireless, che trasferiscono dati a velocità massime molto diverse tra loro. Ognuno di loro inizia per 802.11(x), nome dato loro dall' IEEE, l'ente responsabile della certificazione degli standard di rete. Lo standard di rete più comune, l'802.11b, trasferisce dati a 11 Mbps, gli standard 802.11a e 802.11g trasferiscono i dati a 54 Mbps e Pre-N a 108 Mbps. Pre-N, il precursore dell'imminente versione 802.11n promette velocità superiori a 802.11g e fino al doppio dell'area di copertura wireless. Per ulteriori informazioni vedere la tabella di seguito riportata.

Tabella di confronto wireless

Tecnologia wireless	G (802.11g)	G+ MIMO (802.11g con MIMO MFC)	N MIMO (bozza 802.11n con MIMO)	N1 MIMO (bozza 802.11n con MIMO)
Velocità/Trasferimento dati	Fino a 54 Mbps*	Fino a 54 Mbps*	Fino a 300 Mbps*	Fino a 300 Mbps*
Frequenza	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz
Compatibilità	Compatibile con 802.11b/g	Compatibile con 802.11b/g	Compatibile con la bozza 802.11n** e 802.11b/g	Compatibile con la bozza 802.11n** e 802.11b/g
Copertura*	Fino a 120 m *	Fino a 300 metri*	Fino a 60 metri*	Fino a 420 metri*
Vantaggi	Comune - ampio utilizzo della condivisione Internet	Copertura maggiore e velocità costante	Velocità e copertura maggiori	Leader nel settore - ottima copertura ed efficienza

*La distanza e le velocità di connessione variano in funzione dell'ambiente di rete.

**Questo router è compatibile con i prodotti conformi alle specifiche della bozza 802.11n e potrebbe richiedere degli aggiornamenti del software per offrire prestazioni migliori.

Informazioni sul supporto tecnico

Assistenza tecnica gratuita* *Si applica solo la tariffa della chiamata locale

www.belkin.com

Per maggiori informazioni sull'assistenza tecnica, visitare il nostro sito web **www.belkin.com** nell'area assistenza tecnica. Per contattare telefonicamente il servizio di assistenza tecnica, chiamare uno dei seguenti numeri*.

NAZIONE	NUMERO	INDIRIZZO INTERNET
AUSTRIA	0820 200766	www.belkin.com/uk/networking/
BELGIO	07 07 00 073	www.belkin.com/nl/networking/
REPUBBLICA CECA	239 000 406	www.belkin.com/uk/networking/
DANIMARCA	701 22 403	www.belkin.com/uk/networking/
FINLANDIA	097 25 19 123	www.belkin.com/uk/networking/
FRANCIA	08 - 25 54 00 26	www.belkin.com/fr/networking/
GERMANIA	0180 - 500 57 09	www.belkin.com/de/networking/
GRECIA	00800 - 44 14 23 90	www.belkin.com/uk/networking/
UNGHERIA	06 - 17 77 49 06	www.belkin.com/uk/networking/
ISLANDA	800 8534	www.belkin.com/uk/networking/
IRLANDA	0818 55 50 06	www.belkin.com/uk/networking/
ITALIA	02 - 69 43 02 51	www.belkin.com/it/support/tech/issues_more.asp
LUSSEMBURGO	34 20 80 85 60	www.belkin.com/uk/networking/
PAESI BASSI	0900 - 040 07 90	<small>€0.10 al minuto</small> www.belkin.com/nl/networking/
NORVEGIA	81 50 0287	www.belkin.com/uk/networking/
POLONIA	00800 - 441 17 37	www.belkin.com/uk/networking/
PORTOGALLO	707 200 676	www.belkin.com/uk/networking/
RUSSIA	495 580 9541	www.belkin.com/networking/
SUDAFRICA	0800 - 99 15 21	www.belkin.com/uk/networking/
SPAGNA	902 - 02 43 66	www.belkin.com/es/support/tech/networkingsupport.asp
SVEZIA	07 - 71 40 04 53	www.belkin.com/se/support/tech/networkingsupport.asp
SVIZZERA	08 - 48 00 02 19	www.belkin.com/uk/networking/
REGNO UNITO	0845 - 607 77 87	www.belkin.com/uk/networking/
ALTRI PAESI	+44 - 1933 35 20 00	

Indirizzo IP

Per “Indirizzo IP” si intende l’indirizzo IP interno del router. Per accedere all’interfaccia di impostazione avanzata, digitare l’indirizzo IP nell’apposita barra indirizzi del browser. Questo indirizzo, se necessario, può essere modificato. Per modificare l’indirizzo IP, digitare il nuovo indirizzo IP e fare clic su “Apply Changes” (Esegui modifiche). L’indirizzo IP scelto dovrebbe essere un IP non instradabile. Esempi di indirizzi IP non instradabili sono:

192.168.x.x (dove x indica qualsiasi cifra tra 0 e 255)
10.x.x.x (dove x indica qualsiasi cifra tra 0 e 255)

Subnet Mask (Maschera di sottorete)

Alcune reti sono troppo grandi per consentire che il traffico scorra in tutte le loro parti. Queste reti devono essere suddivise quindi in sezioni più piccole, meglio gestibili, dette sottoreti. La subnet mask (maschera di sottorete) è l’indirizzo accompagnato da altre informazioni necessarie ad identificare la “sottorete”.

DNS

DNS è l’acronimo di Domain Name Server. Un “Domain Name Server” è un server presente in Internet che traduce gli URL (Universal Resource Links) come “www.belkin.com” in indirizzi IP. Molti ISP non richiedono l’immissione di questa informazione nel router. Se si utilizza un tipo di connessione IP statica, perché la propria connessione funzioni correttamente, potrebbe essere necessario inserire uno specifico indirizzo DNS ed un indirizzo DNS secondario. Se il proprio tipo di connessione fosse dinamico o PPPoE, è probabile che non sia necessario inserire un indirizzo DNS.

PPPoE

La maggior parte dei provider ADSL utilizza un tipo di connessione PPPoE. Nel caso si utilizzasse un modem ADSL per collegarsi ad Internet, il proprio ISP potrebbe utilizzare il tipo di connessione PPPoE per collegarsi al servizio.

Il proprio tipo di connessione è PPPoE se:

1. Il proprio ISP ha fornito un nome utente e una password per collegarsi a Internet.
2. Il proprio ISP ha fornito un software del tipo WinPOET o Enternet300 da utilizzare per collegarsi a Internet
3. Per entrare in Internet, è necessario fare doppio clic su un’icona del desktop diversa dal proprio browser.

Per impostare il router in modo da utilizzare il servizio PPPoE, digitare il proprio nome utente e la password negli appositi spazi. Dopo aver inserito i propri dati, fare clic su “Apply Changes” (Esegui modifiche).

Una volta eseguite le modifiche, l'indicatore "Internet Status" (Stato Internet) visualizzerà il messaggio "Connection OK", se il router è stato impostato correttamente.

PPPoA

Digitare le informazioni PPPoA negli appositi spazi e fare clic su "Next" (Avanti). Fare clic su "Apply" (Applica) per attivare le impostazioni.

1. User name (Nome utente) - Digitare il nome utente. (forniti dal proprio provider di servizi Internet).
2. Password - Digitare la propria password (forniti dal proprio provider di servizi Internet).
3. Retype Password (Ridigita password) - Confermare la password. (forniti dal proprio provider di servizi Internet).
4. . VPI/VCI Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio provider di servizi Internet).

Disconnetti dopo X...

Questa opzione viene utilizzata per disconnettere automaticamente il router dall'ISP quando non vi sono attività in corso per un intervallo di tempo specifico. Ad esempio, posizionando un segno di spunta accanto a questa opzione e digitando "5" nello spazio riservato ai minuti, si farà in modo che il router si disconnetta da Internet dopo cinque minuti di inattività di Internet.

Questa opzione va utilizzata nel caso il servizio di Internet venga pagato a minuti.

Canale e SSID

Per cambiare canale, selezionare il canale di funzionamento del router dal menu a discesa e selezionare il proprio canale. Fare clic su "Apply Changes" (Esegui modifiche) per salvare le impostazioni. È possibile modificare anche i parametri SSID. I parametri SSID sono l'equivalente del nome della rete wireless. I parametri SSID possono essere di qualsiasi tipo si desidera. In presenza di altre reti wireless nella propria area, assegnare alla propria rete wireless un nome univoco. Fare clic nella casella SSID e digitare un nuovo nome. Fare clic su "Apply Changes" (Applica modifiche) per salvare la modifica.

Trasmissione ESSID

Molte schede di rete wireless attualmente sul mercato prevedono una funzione detta "site survey". Essa consente di esaminare attorno per rilevare qualsiasi rete disponibile e consentire al computer di selezionare la rete tramite la funzione di descrizione generale del sito. Questa condizione si verifica se l'SSID è impostato su "ANY" (QUALSIASI). Il router Belkin può bloccare questa ricerca casuale di una rete. Disattivando la funzione di trasmissione "ESSID Broadcast", l'unico modo in cui un computer è in grado di entrare nella rete è tramite la propria SSID impostata con il nome specifico della rete (WLAN ad esempio). Accertarsi di conoscere i propri

parametri SSID (nome della rete) prima di attivare questa opzione. È possibile rendere la propria rete wireless quasi invisibile. Disattivando la trasmissione SSID, la rete non sarà rilevata. Naturalmente, disattivando la trasmissione SSID, la protezione aumenta.

Crittografia

Utilizzando la funzione di crittografia, la rete viene resa più sicura. Per proteggere i vostri dati, il router sfrutta la crittografia Wired Equivalent Privacy (WEP) e prevede due gradi di crittografia: a 64 bit e a 128 bit. La crittografia si basa su un sistema di chiavi. La chiave inserita nel computer deve corrispondere alla chiave del router ed esistono due modi per creare una chiave. Il più semplice consiste nel consentire al software del router di convertire una frase di accesso creata dall'utente in una chiave. Il metodo avanzato prevede l'inserimento manuale delle chiavi.

Gateway applicativi

I gateway applicativi consentono di selezionare le porte da aprire per consentire ad alcune applicazioni specifiche di funzionare in maniera adatta con l'opzione Network Address Translation (NAT) del router. È disponibile un elenco delle applicazioni tradizionali. È possibile selezionare un'applicazione dall'elenco a discesa, programmando in questo modo le impostazioni nel router. Selezionare il rigo in cui copiare le impostazioni dal menu a tendina e fare clic su Invia a. Le impostazioni saranno trasferite al rigo specificato. Fare clic su "Apply Changes" (Esegui modifiche) per salvare le impostazioni per quella specifica applicazione. Se non si trova l'applicazione desiderata, è necessario contattare il rivenditore dell'applicazione per individuare quali porte devono essere configurate. Questa informazione può essere inserita nel router manualmente.

Server virtuali

Questa funzione consente di instradare eventuali richieste di servizio esterne (di Internet), tra cui server web (porta 80), server FTP (porta 21) o altre applicazioni attraverso il proprio router nella rete interna. Poiché i computer interni sono protetti da una protezione firewall, i computer di Internet non possono accedervi perché non li "vedono". Se fosse necessario configurare una funzione di server virtuale per una specifica applicazione, si dovrà contattare il fornitore dell'applicazione per conoscere le impostazioni delle porte necessarie.

Per digitare manualmente le impostazioni, inserire l'indirizzo IP nello spazio previsto per la macchina interna, il tipo di porta (TCP o UDP) e la(e) porta(e) pubbliche da superare. Quindi selezionare "Enable" (Abilita) e fare clic su "Set" (Imposta). È possibile passare soltanto attraverso una porta per ciascun indirizzo IP interno. L'apertura delle porte nella protezione firewall può comportare un

1

2

3

4

5

6

7

8

9

10

11

rischio per la sicurezza. Le impostazioni possono essere attivate e disattivate molto rapidamente. È consigliabile disattivare le impostazioni quando non si utilizza un'applicazione specifica.

Filtri IP Client

Il router può essere configurato in modo da limitare l'accesso ad Internet, alla posta elettronica o ad altri servizi di rete in particolari giorni o momenti. Il limite può essere impostato per un solo computer, una serie di computer o numerosi computer.

Blocco di URL

Per poter configurare il blocco URL, specificare i siti web (www.sitoweb.com) e/o le parole che si vuole filtrare dalla rete. Fare clic su "Apply Changes" (Esegui modifiche) per salvare la modifica. Per completare la configurazione bisognerà creare o modificare la regola dell'accesso nella sezione "Client IP filters" (Filtri IP Client). Per modificare una regola esistente, fare clic sull'opzione "Edit" vicina alla regola che si vuol modificare. Per creare una nuova regola, fare clic su "Add PC" (Aggiungi PC). Dalla sezione "Access Control > Add PC", apporre il segno di spunta accanto all'opzione "WWW with URL Blocking" (www con blocco URL) nella scheda "Client PC Service" per eliminare i siti web e le parole specificate.

Regola di pianificazione

Per configurare la regola di pianificazione, specificare il nome, il commento, l'orario di inizio e di fine del filtraggio della rete. Questa pagina definisce i nomi delle regole di pianificazione e attiva la pianificazione dell'accesso della pagina "Access Control".

Filtraggio degli indirizzi MAC

Il filtro indirizzi MAC è un potente mezzo per specificare quali sono i computer che possono accedere alla rete. I computer che tentano di accedere senza essere specificati nell'elenco del filtro non saranno autorizzati. Attivando questa funzione, è necessario inserire l'indirizzo MAC per ciascun client nella propria rete per consentire l'accesso della rete ad ognuno oppure copiare l'indirizzo MAC selezionando il nome del computer dal "DHCP Client List" (Elenco Client DHCP). Per attivare questa funzione, selezionare "Enable" (Abilita). Quindi, fare clic su "Apply Changes" (Esegui modifiche) per salvare le impostazioni.

DMZ

Se si ha un PC client che non è in grado di gestire adeguatamente un'applicazione Internet da dietro una protezione firewall, per il client è possibile aprire un accesso a Internet illimitato a due vie. Questa operazione potrebbe rivelarsi necessaria nel caso l'opzione NAT stesse causando problemi con un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Questa opzione va sfruttata solo provvisoriamente. Il computer nella DMZ non è protetto dagli attacchi degli hacker. Per collocare il computer nella DMZ, digitare le ultime cifre del rispettivo indirizzo

IP LAN nel campo “Static IP” (IP Statico) e fare clic su “Apply Changes” (Esegui modifiche) affinché la modifica venga attivata.

Se si dispone di un unico indirizzo IP pubblico (WAN), l'IP pubblico può essere lasciato su “0.0.0.0”. Se si stessero utilizzando diversi indirizzi pubblici (WAN) IP, è possibile selezionare a quale indirizzo pubblico (WAN) IP dirigere l'host DMZ. Digitare l'indirizzo pubblico (WAN) IP al quale si desidera indirizzare l'host DMZ, digitare le ultime due cifre dell'indirizzo IP del computer host DMZ e fare clic su “Apply Changes” (Esegui modifiche).

1

2

3

4

5

6

7

8

9

10

11

Allegato B: Considerazioni importanti per il posizionamento e l'installazione

Password Amministratore

Il router viene fornito SENZA password. Se si desidera aggiungere una password per maggiore sicurezza, la password può essere impostata dall'interfaccia utente basata sul server del router. Conservare la password in un posto sicuro, in quanto sarà necessaria per accedere al router in futuro. È anche VIVAMENTE CONSIGLIATO inserire una password nel caso si intenda utilizzare l'opzione di gestione a distanza. L'opzione di durata della connessione consente di impostare un intervallo di tempo di connessione all'interfaccia avanzata di impostazione del router. Il timer parte dal momento in cui non si rileva alcuna attività. Ad esempio, se fosse stata apportata qualche modifica all'interfaccia di impostazione avanzata, il computer si gestirà da solo senza dover fare clic su "Logout".

Supponendo che la durata di connessione sia stata impostata su 10 minuti, dopo 10 minuti di mancato utilizzo del computer, la sessione di connessione verrà interrotta. Per apportare ulteriori modifiche sarà quindi necessario connettersi di nuovo al router. L'opzione di durata della connessione è prevista a scopo cautelativo ed è preimpostata su 10 minuti. Va ricordato che è possibile connettere all'interfaccia avanzata di impostazione del router soltanto un computer alla volta.

Orario e fuso orario

Il router aggiorna l'orario collegandosi ad un server SNTP (Simple Network Time Protocol). In questo modo il router è in grado di sincronizzare l'orologio del sistema con la rete Internet mondiale. L'orologio sincronizzato presente nel router viene utilizzato per registrare l'elenco di protezione e controllare il filtro client. Selezionare il proprio fuso orario. Se si vive in una zona che osserva l'ora legale, inserire un segno di spunta nella casella accanto a "Enable Daylight Saving" (Attiva ora legale). L'orologio del sistema potrebbe non aggiornarsi immediatamente. Attendere almeno 15 minuti perché il router contatti i server dell'orario su Internet e riceva una risposta. L'utente non può impostare autonomamente l'orologio.

Gestione a distanza

Prima di abilitare questa funzione, ACCERTARSI DI AVER IMPOSTATO LA PASSWORD DELL'AMMINISTRATORE. La gestione a distanza consente di modificare le impostazioni del router da qualsiasi punto di Internet.

UPnP

La tecnologia UPnP (Universal Plug-and-Play) è in grado di offrire un funzionamento continuo delle opzioni di trasmissione di messaggi vocali, video, giochi e di altre applicazioni conformi agli standard UPnP. Per funzionare correttamente, alcune applicazioni richiedono che la protezione firewall del router sia configurata in maniera specifica. Per farlo è generalmente necessario aprire le porte TCP e UDP e, in alcuni casi, impostare le porte trigger. Un'applicazione conforme al servizio UPnP ha la capacità di comunicare con il router, fondamentalmente "dicendo" al router come configurare la protezione firewall. Il router viene fornito con l'opzione

Allegato B: Considerazioni importanti per il posizionamento e l'installazione

UPnP disabilitata. Se si sta utilizzando una qualsiasi applicazione conforme al servizio UPnP, e si desidera utilizzare le opzioni UPnP, queste si possono attivare. È sufficiente selezionare “Enable” (Abilita) nella sezione “UPnP Enabling” (Abilitazione UPnP) della pagina “Utilities” (Utility). Fare clic su “Apply Changes” (Esegui modifiche) per salvare la modifica.

Nota bene: sebbene alcuni dei fattori elencati di seguito possano compromettere le prestazioni della rete, non ne impediscono il funzionamento. Se ritenete che la vostra rete non funzioni efficientemente, la seguente lista di controllo potrebbe rivelarsi utile.

1. Collocazione del router o dell'access point wireless

Posizionare il router (o l'access point) wireless, che rappresenta il punto di connessione centrale della rete, il più vicino possibile al centro del raggio d'azione dei dispositivi wireless.

Per ottenere la migliore connessione per i “clienti wireless” (computer provvisti delle schede di rete wireless per notebook, schede di rete per computer desktop ed adattatori USB wireless Belkin):

- Assicurarsi che le antenne di rete del router wireless o dell'access point siano parallele e verticali (rivolte verso il soffitto). Se il router wireless (o l'access point) è in posizione verticale, puntare le antenne il più possibile verso l'alto.
- Negli edifici a più piani, posizionare il router wireless o l'access point su un piano che sia il più vicino possibile al centro dell'edificio. Ad esempio sul pavimento di un piano superiore.
- Non posizionare il Router Wireless (o l'Access Point) vicino a telefoni senza filo da 2,4 GHz.

2. Evitare ostacoli e interferenze

Evitare di posizionare il router wireless (o l'access point) vicino a dispositivi che possono trasmettere “interferenze”, come nel caso dei forni a microonde. Tra gli oggetti che possono impedire la comunicazione wireless sono compresi:

- Frigoriferi
- Lavatrici e/o asciugabiancheria
- Armadietti in metallo
- Acquari grandi
- Finestre verniciate con vernice a base metallica di protezione dai raggi UV

Se il segnale wireless dovesse sembrare più debole in alcuni punti, assicurarsi che oggetti di questo tipo non ostacolino il segnale tra i computer e il router (o l'access point) wireless.

3. Telefoni cordless

Se le prestazioni della rete wireless dovessero continuare ad essere inadeguate, dopo aver verificato i punti sopra riportati, e se si ha un telefono cordless:

- Allontanare il telefono cordless dal Router (o dall'Access Point) Wireless e dai computer provvisti di tecnologia wireless.

1
2
3
4
5
6
7
8
9
10
11

sezione

Allegato B: Considerazioni importanti per il posizionamento e l'installazione

- Staccare la spina e rimuovere la batteria da eventuali telefoni cordless che utilizzano la banda 2,4 GHz (consultare le informazioni del produttore). Se il problema si risolve, ciò era probabilmente dovuto ad un'interferenza del telefono.
- Se il telefono supporta la selezione dei canali, e se possibile, cambiare il canale sul telefono e scegliere il canale più lontano dalla rete wireless. Per esempio, spostare il telefono sul canale 1 e il Router Wireless (o Access Point) sull'11. Vedere il manuale utente per maggiori informazioni.
- Se necessario, passare ad un telefono cordless da 900 MHz o 5 GHz.

4. Scegliere il canale “più tranquillo” per la propria rete wireless

Negli edifici dove sono presenti sia abitazioni che uffici, una rete vicina potrebbe entrare in conflitto con la vostra.

Usare le capacità “Site Survey” (analisi del sito) della utility LAN wireless del proprio adattatore wireless per localizzare eventuali reti wireless disponibili (vedere il manuale di istruzioni dell'adattatore wireless) e spostare il router wireless (o access point) ed i computer su un canale che sia il più lontano possibile da altre reti.

Provare con più canali, in modo da individuare la connessione più chiara ed evitare in questo modo interferenze da altri telefoni cordless o da altri dispositivi di rete wireless.

Per i prodotti wireless Belkin, consultare l'opzione Site Survey e le informazioni sui canali wireless riportate nel manuale utente.

Queste indicazioni dovrebbero consentire di ottenere la migliore copertura possibile con il router wireless (o l'access point). Per coprire un'area più estesa, si consiglia di usare il Range Extender/Access Point Wireless Belkin.

5. Connessioni protette, VPN e AOL

Le connessioni protette generalmente richiedono un nome utente e una password e sono usate quando sono richieste condizioni di sicurezza. Le connessioni sicure comprendono:

- Le connessioni Virtual Private Network (VPN), spesso usate per il collegamento remoto a una rete di un ufficio
- Il programma di America Online (AOL) “Bring Your Own Access”, che permette di usare AOL mediante la banda larga fornita da un altro servizio via cavo o DSL
- La maggior parte dei servizi bancari online
- Molti siti commerciali che richiedono un nome utente e una password per accedere all'account

Le connessioni protette si possono interrompere configurando la gestione dell'alimentazione del computer facendole entrare in modalità di sospensione. La soluzione più semplice per evitare che questo accada consiste nell'effettuare nuovamente il collegamento riavviando il software VPN o AOL o eseguendo di nuovo il login nel sito protetto.

Un'alternativa è cambiare le configurazioni della gestione dell'alimentazione del computer, in modo da non rimandare alla modalità di sospensione; tuttavia, ciò potrebbe non essere raccomandabile per i portatili. Per modificare le configurazioni della gestione dell'alimentazione in Windows, vedere in "Power Options" (Opzioni risparmio energia) nel pannello di controllo.

Se si dovessero ancora avere difficoltà con la connessione sicura, con VPN e AOL, rivedere i passi sopra riportati per assicurarsi di aver identificato il problema.

1

2

3

4

5

6

7

8

9

10

11

Dichiarazione FCC

DICHIARAZIONE DI CONFORMITÀ CON LE LEGGI FCC PER LA COMPATIBILITÀ' ELETTROMAGNETICA

Noi sottoscritti, Belkin International, Inc., con sede al 501 West Walnut Street, Compton, CA 90220, dichiariamo sotto la nostra piena responsabilità che il prodotto:

F5D7632uk4A

, cui questa dichiarazione fa riferimento, è conforme alla sez. 15 delle norme FCC. Le due condizioni fondamentali per il funzionamento sono le seguenti: (1) il dispositivo non deve causare interferenze dannose e (2) il dispositivo deve accettare qualsiasi interferenza ricevuta, comprese eventuali interferenze che possano causare un funzionamento anomalo.

Attenzione: esposizione alle radiazioni di radiofrequenza.

La potenza in uscita irradiata da questo dispositivo è molto inferiore ai limiti di esposizione alla radiofrequenza FCC. Tuttavia, la periferica dovrà essere utilizzata in modo da ridurre al minimo il potenziale rischio di contatto umano nel corso del suo funzionamento.

Se il dispositivo venisse collegato con un'antenna esterna, l'antenna dovrà essere posizionata in modo da ridurre al minimo il potenziale rischio di contatto umano nel corso del suo funzionamento. Per evitare la possibilità di un eventuale superamento dei limiti di esposizione alle radiofrequenze FCC, non è consentito avvicinarsi all'antenna di oltre 20 cm nel corso del suo normale funzionamento.

Informazione della Commissione Federale per le Comunicazioni

Questa apparecchiatura è stata testata ed è risultata conforme ai limiti per i dispositivi digitali di Classe B, ai sensi della Parte 15 delle normative FCC. Questi limiti hanno lo scopo di offrire una protezione ragionevole dalle interferenze dannose in un'installazione domestica.

Questo dispositivo genera, utilizza e può emettere energia in radiofrequenza.

Se questo dispositivo causasse interferenze dannose per la ricezione delle trasmissioni radiotelevisive determinabili spegnendo o riaccendendo l'apparecchio stesso, si suggerisce all'utente di cercare di rimediare all'interferenza ricorrendo ad uno o più dei seguenti provvedimenti:

- Cambiare l'orientamento o la posizione dell'antenna ricevente.
- Aumentare la distanza tra il dispositivo ed il ricevitore.
- Collegare il dispositivo a una presa di un circuito diverso da quello a cui è collegato il ricevitore
- Consultare il rivenditore o un tecnico radio/TV specializzato.



Modifiche

Le indicazioni FCC prevedono che l'utente venga informato che eventuali variazioni o modifiche apportate a questo dispositivo, non espressamente approvate da Belkin, potrebbero annullare la facoltà dell'utente di utilizzare il dispositivo.

Canada- Industry Canada (IC)

L'apparecchio radio wireless di questo dispositivo è conforme alle indicazioni RSS 139 & RSS 210 Industry Canada. Questo apparecchio digitale di Classe B è conforme allo standard canadese ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Europa -Comunicato dell'Unione Europea

I prodotti radio con la sigla di avvertenza CE 0682 o CE sono conformi alla direttiva R&TTE (1995/5/EC) emessa dalla Commissione della Comunità Europea.

La conformità a queste Direttive comporta l'osservanza delle seguenti Norme Europee (fra parentesi le sono indicati i rispettivi standard internazionali).

- EN 60950 (IEC 60950) – Sicurezza del prodotto
- EN 300 328 Requisiti tecnici per apparecchiature radio
- ETS 300 826 Indicazioni generali di compatibilità elettromagnetica per le apparecchiature radio.

Per stabilire il tipo di trasmettitore utilizzato, verificare la targhetta di identificazione del proprio prodotto Belkin.

I prodotti con il marchio CE sono conformi alla Direttiva EMC (89/336/CEE) e alla Direttiva per la Bassa Tensione

(72/23CEE) emesse dalla Commissione della Comunità Europea. La conformità a tale direttiva implica la conformità alle seguenti norme europee (tra parentesi sono indicati i rispettivi standard internazionali).

- EN 55022 (CISPR 22) Interferenze elettromagnetiche
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) - Immunità elettromagnetica
- EN 61000-3-2 (IEC610000-3-2)- Armoniche della linea di alimentazione
- EN 61000-3-3 (IEC610000) – Sfarfallamento della linea di alimentazione
- EN 60950 (IEC 60950) – Sicurezza del prodotto

I prodotti che contengono un trasmettitore radio presentano le etichette di avvertimento CE 0682 o CE, e possono anche esibire il logotipo CE.

1

2

3

4

5

6

7

8

9

10

11

Garanzia a vita limitata sul prodotto Belkin International Inc.

Oggetto della garanzia.

Belkin International, Inc. garantisce all'acquirente di questo prodotto Belkin che tale prodotto è esente da difetti di progettazione, montaggio, materiale e lavorazione.

Periodo di copertura della garanzia.

Belkin International garantisce il prodotto Belkin per tutto il ciclo di vita di tale prodotto.

Risoluzione di eventuali problemi

Garanzia sul prodotto.

Belkin provvederà a riparare o sostituire gratuitamente, a sua discrezione, qualsiasi prodotto che dovesse risultare difettoso (escluse le spese di trasporto).

Condizioni non coperte dalla garanzia.

Tutte le garanzie di cui sopra saranno rese nulle qualora il prodotto Belkin non fosse fornito alla Belkin International, Inc. per essere sottoposto alle necessarie verifiche dietro espressa richiesta di Belkin e a spese del cliente, oppure nel caso in cui la Belkin International, Inc. dovesse stabilire che il prodotto non è stato correttamente installato o che sia stato in qualche modo alterato o manomesso. La garanzia sul prodotto Belkin non copre danni da imputarsi a calamità naturali, tra cui allagamenti, terremoti, fulmini, guerre, atti di vandalismo, furti, usura, erosione, assottigliamento, obsolescenza, abusi, danni dovuti ad interferenze di bassa tensione (tra cui parziali oscuramenti o abbassamenti di tensione), programmazione non autorizzata oppure modifiche o alterazioni all'apparecchiatura dell'impianto.

Come ottenere l'assistenza.

Per usufruire dell'assistenza per il proprio prodotto Belkin, è necessario:

1. Contattare la Belkin International, Inc. all'indirizzo 501 W. Walnut St., Compton CA 90220, att.: Customer Service, oppure chiamare il numero (800)-223-5546, entro 15 giorni dall'evento. Vi sarà richiesto di fornire le seguenti informazioni:
 - a. Il codice del prodotto Belkin.
 - b. Il luogo di acquisto del prodotto.
 - c. La data di acquisto del prodotto.
 - d. Copia della ricevuta originale.
2. Il rappresentante del Servizio Clienti Belkin vi spiegherà come inviare la ricevuta e il prodotto Belkin e come procedere al reclamo.

Belkin International, Inc. si riserva il diritto di riesaminare il prodotto Belkin danneggiato. Tutte le spese di spedizione per il prodotto Belkin restituito alla Belkin International, Inc. sono a carico dell'acquirente. Qualora Belkin ritenga, a sua discrezione, difficoltoso il rinvio dell'apparecchio danneggiato alla Belkin International, Inc., quest'ultima potrebbe decidere, a sua discrezione, di farlo ispezionare e determinare il costo della riparazione. In caso ci fossero delle spese di spedizione

per inviare e ricevere l'apparecchio dopo l'ispezione, queste saranno a carico dell'acquirente. Eventuali apparecchi danneggiati dovranno essere mantenuti disponibili per eventuali verifiche fino alla risoluzione della richiesta di indennizzo. Qualora si raggiunga un accordo, Belkin International, Inc. si riserva il diritto di essere surrogata da eventuali polizze assicurative dell'acquirente.

La garanzia e le leggi vigenti in materia.

LA PRESENTE GARANZIA COSTITUISCE L'UNICA GARANZIA, ESPLICITA O IMPLICITA, DELLA BELKIN INTERNATIONAL, INC. SI ESCLUDE QUALSIASI GARANZIA IMPLICITA, DI COMMERCIALIZZABILITÀ E DI IDONEITÀ A SCOPI PARTICOLARI CHE VADANO OLTRE LA PRESENTE GARANZIA ESPLICITA SCRITTA.

Alcune giurisdizioni non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, pertanto i limiti di esclusione di cui sopra potrebbero non fare al caso vostro.

IN NESSUN CASO BELKIN INTERNATIONAL, INC. POTRÀ ESSERE CONSIDERATA RESPONSABILE DI ALCUN DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIFICO O DANNI MULTIPLI TRA I QUALI, MA NON SOLO, EVENTUALI DANNI DI MANCATI AFFARI O MANCATO GUADAGNO DERIVANTI DALLA VENDITA O UTILIZZO DI QUALSIASI PRODOTTO BELKIN, ANCHE NEL CASO IN CUI SI FOSSE STATI INFORMATI DELLA POSSIBILITÀ DI TALI DANNI.

Questa garanzia consente di godere di diritti legali specifici e di eventuali altri diritti che possono variare di stato in stato. Alcune giurisdizioni non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, pertanto i limiti di esclusione di cui sopra potrebbero non fare al caso vostro.

L'apparecchiatura può essere liberamente utilizzata per uso personale o per attività di propria pertinenza solo all'interno di edifici o di aree di esclusiva proprietà privata (Decreto legislativo 259/03, art. 105). Se non si verificano queste condizioni, l'uso per scopi privati è consentito solo previa autorizzazione, da chiedersi al Ministero delle Comunicazioni – Ispettorato Territoriale competente per Regione (Decreto legislativo 259/03, art. 104).

L'apparecchiatura può essere utilizzata anche da Operatori pubblici di Telecomunicazione, per consentire l'accesso alle rispettive reti / servizi (D.M. 28.5.03 e D.M. 4.10.05). In questo caso, l'installazione e l'esercizio dell'apparecchiatura è soggetto ad autorizzazione del Ministero delle Comunicazioni, Direzione Generale – Roma.

Nota: per ulteriori informazioni relative alle Autorizzazioni consultare l'indirizzo web <http://www.urpcomunicazioni.it>, alla voce "utilità per il cittadino".

Per informazioni sullo smaltimento del prodotto consultare il sito:
<http://environmental.belkin.com>



PER L'USO IN	AT	BE	CY	CZ	DK	EE	FI	FR	DE	GR	HU	IE		
IT	LV	LT	LU	MT	NL	PL	PT	SK	SI	ES	SE	GB	IS	LI
NO	CH	BG	RO	TR										

FUNZIONA SUI CANALI 1-13

Utilizzo non è consentito in alcuni paesi...Apparecchiatura di classe2

BELKIN®

EC Declaration of Conformity to R&TTE Directive 1999/5/EC

Manufacturer : BELKIN LTD,
EXPRESS BUSINESS PARK,
SHIPTON WAY
RUSHDEN
NN10 6GL ENGLAND

Representative : Belkin Ltd
(residing in the EC
holding the TCF)

Product / Apparatus : ADSL Modem/Wireless G Router

Type Number : F5D7632-4

Variants include : All Country Variants

Declaration

I declare that above product conforms to all the applicable requirements of EU Directive 1999/5/EC and is CE-marked accordingly:

Article 3.1a: (Standard(s)) used to show compliance with LVD, 73/23/EEC:

IEC 60950-1 2001 Compliant Test Report No: LD931001H03 03 NOV 04

Article 3.1b: (Standard(s)) used to show compliance with EMC Directive, 89/336/EEC:

EN301 489-1 V1.4.1 (2002-08); EN 301 489-17 V1.2.1 (2002-08) Compliant Test Report No: RM931001H03

Article 3.2: Standard(s) used to show compliance:

...EN300 328 V1.4.1 (2003-04)..... Compliant Test Report No: RC93100H03

Signature :



Name :

K Simpson

Title :

European Regulatory Compliance Manager

Date :

20 MAR 2006

d of c f5d7632

BELKIN®

Modem ADSL2+ con Router G Wireless

BELKIN®

www.belkin.com

Assistenza tecnica Belkin

REGNO UNITO: 0845 607 77 87

Europa: www.belkin.com/support

Belkin Ltd.

Express Business Park
Shipton Way, Rushden
NN10 6GL, Regno Unito
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin SAS

130 rue de Silly
92100 Boulogne-Billancourt,
Francia
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH

Hanebergstrasse 2
80637 Monaco di Baviera
Germania
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

Belkin Iberia

C/ Anabel Segura, 10 planta baja, Of. 2
28108, Alcobendas, Madrid
Spagna
+34 91 791 23 00
+34 91 490 23 35 fax

Belkin Italy & Greece

Via Carducci, 7
20123 Milano
Italia
+39 02 862 719
+39 02 862 719 fax

Belkin B.V.

Boeing Avenue 333
1119 PH Schiphol-Rijk,
Paesi Bassi
+31 (0) 20 654 7300
+31 (0) 20,654 7349 fax

© 2007 Belkin International, Inc. Tutti i diritti riservati. Tutti i nomi commerciali sono marchi registrati dai rispettivi produttori elencati. Mac, Mac OS, Apple e AirPort sono marchi commerciali della Apple, Inc., registrati negli USA e in altri Paesi. Windows, NT, Microsoft e Windows Vista sono marchi commerciali o marchi registrati della Microsoft Corporation negli Stati Uniti e/o in altri Paesi.

P74725ea-A