

[Note from proofing: keep changes tracked at each revision, this is a uk manual]
[insert title page per branding standard] [needs updated image]
G+MIMO Modem router

User Manual
F5D9631-4

Splash Screen [update with new N background]

[double check the page # and titles]

Table of Contents

1 IntroductionX
Advantages of a Wireless Network	
Placement of your G+MIMO Modem routerX
2 Product OverviewX
Product FeaturesX
3 Knowing your Modem RouterX
Package ContentsX
System RequirementsX
Setup Assistant Software System RequirementsX
4 Connecting and Configuring your Modem RouterX
5 Alternate Setup MethodX
6 Using the Web-Based Advanced User InterfaceX
Changing LAN SettingsX
Viewing the DHCP Client List PageX
Configuring the Wireless Network SettingsX
Setting WPA SecurityX
Setting WEP EncryptionX
Setting MAC Address ControlX
Configuring the FirewallX
Using Dynamic DNS	
UtilitiesX
Restarting the RouterX
Updating the FirmwareX
7 Manually Configuring Network SettingsX
8 Recommended Web Browser SettingsX
9 TroubleshootingX
10 InformationX

Introduction

Thank you for purchasing the Belkin G+MIMO Modem router (the Router). Following are two short sections—the first discusses the benefits of home networking, and the other outlines best practices that maximize your wireless home network range and performance. Please be sure to read through this User Manual completely, and pay special attention to the section entitled “Placement of your Wireless Networking Hardware for Optimal Performance” on page 2. (double check the page #)

Benefits of a Home Network

- 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 Wireless Network

Here are some of the advantages of setting up 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 Assistant application 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.

[Introduction]

Thank you for purchasing the Belkin G+MIMO Wireless Modem Router (the Router). Following are two short sections—the first discusses the benefits of home networking, and the other outlines best practices that maximize your wireless home network range and performance. Please be sure to read through this User Manual completely, and pay special attention to the section entitled “Placement of your Wireless Networking Hardware for Optimal Performance” on page #(double check the page#). 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 Wireless Network

Here are some of the advantages of setting up 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 our wireless range

Easy installation – Belkin’s Setup Assistant software 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

Placement of your Wireless Networking Hardware for Optimal Performance

Important Factors for Placement and Setup

Your wireless connection will be stronger the closer your computer is to your Router. Typical indoor operating range for wireless devices is between 100 and 200 feet.

In the same way, your wireless connection and performance will degrade somewhat as the distance between your Router and connected devices increases. This may or may not be noticeable to you. As you move further from your Router, connection speed may decrease. Factors that can weaken signals simply by getting in the way of your network's radio waves are metal appliances or obstructions, and walls.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between five and 10 feet from the Router in order to see if distance is the problem. If difficulties persist even at close range, please contact Belkin Technical Support.

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. Router Placement

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

2. Avoid Obstacles and Interference

Avoid placing your Router 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 Router).

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 your Router 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 phone to channel 1 and move your Router 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 Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter’s user manual), and move your Router 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 with your wireless network card. See your network card’s user guide for more information.

These guidelines should allow you to cover the maximum possible area with your Router. Should you need to cover an even wider area, we suggest the Belkin Wireless Universal 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.

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.

Product Overview

Product Features

In minutes you will be able to share your Internet connection and network your computers. The following is a list of features that make your new Belkin G+MIMO Wireless Modem router an ideal solution for your home or small office network.

Works with Both PCs and Mac[®] Computers

The Router supports a variety of networking environments including Mac OS[®] 8.x, 9.x, X v10.x, Linux[®], Windows[®] 98, Me, NT[®], 2000, XP, and Vista[™]. All that is needed is an Internet browser and a network adapter that supports TCP/IP (the standard language of the Internet).

Network Status 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.

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.

Integrated 10/100 4-Port Switch

The Router has a built-in, four-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.

Universal Plug and Play (UPnP)

UPnP 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.

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.

Setup Assistant

The Setup Assistant, second generation of Belkin's renowned Easy Install Wizard, takes the guesswork out of setting up your Router. This automatic software determines your network settings for you and sets up the Router for connection to your Internet Service Provider (ISP). In a matter of minutes, your Router will be up and running on the Internet.

Note: Setup Assistant software is compatible with Windows 2000, XP, and Vista, Mac OS X v10.4 and v10.5. If you are using another operating system, the Router can be set up using the Alternate Setup Method described in this User Manual (see page xx) **[VERIFY PAGE NUMBER]**.

Integrated G+MIMO Wireless Access Point

G+MIMO is an exciting new wireless technology that achieves data rates up to 54Mbps. Actual throughput is typically lower than the connected data rate and will vary depending on your networking environment.

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 Advanced User Interface and you can control access to your network.

Knowing your Modem Router

Package Contents

- Belkin G+MIMO Wireless Modem router
- Quick Installation Guide
- Belkin Personal Network Assistant Software CD with User Manual
- RJ11 Telephone Cord
- RJ45 Ethernet Networking Cable
- ADSL (Asymmetric Digital Subscriber Line) Micro filter*
- Power Supply
- User Manual in CD
- Network Status Display Guide

*ADSL Micro filter 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 an installed network interface adapter
- TCP/IP networking protocol installed on each computer
- No other DHCP server on your local network assigning IP addresses to computers and devices
- Internet browser

Setup Assistant Software System Requirements

- A computer running Windows 2000, XP, or Vista; or Mac OS X v10.4 and v10.5
- Minimum 1GHz processor and 512MB RAM
- Internet browser

Internet Connection Settings

The Setup Assistant contains a database of Internet Service Providers (ISP) 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 ____ . ____ . ____ . ____

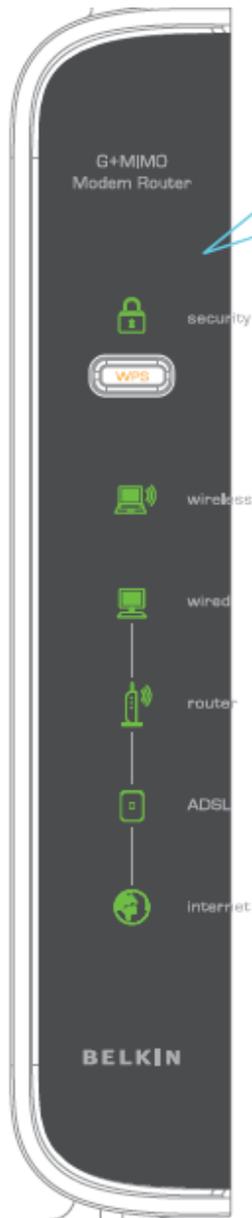
Subnet Mask ____ . ____ . ____ . ____

Default Gateway Server ____ . ____ . ____ . ____

• IP address for Domain Name Server ____ . ____ . ____ . ____ (If given by your ISP)

Knowing your Router

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 Network Status Display is easily visible on the FRONT of the Router to provide you with information about network activity and status. See the Network Status Display Guide for more detailed information.



[Reference only]

- A. Security [insert Lock Icon]



OFF	Wireless security is OFF
-----	--------------------------

Solid Blue	Wireless security is ON
Flashing Blue	WPS sync is in progress



● **B. Wireless-Computer Status [insert Laptop Icon]**

Off	Wireless computer is not present
Solid Blue	Wireless computer is connected to the Router
Blinking Amber	Problem with wireless computer connecting properly to the Router



● **C. Wired-Computer Status [Computer Icon]**

Off	Wired computer is not present
Solid Blue	Wired computer is connected to the Router
Blinking Amber	Problem with wired computer connecting to the Router currently



● **D. Router/Power Status [insert Router Icon]**

When you apply power to the Router or restart it, a short period of time elapses while the Router boots up. During this time, the “router” icon blinks. When the Router has completely booted up, the “router” icon becomes a solid light, indicating the Router is ready for use.

Off	Router is off
Blinking Blue	Router is booting up
Solid Blue	Router is on and ready



● **E. ADSL Line Status [insert ADSL Icon]**

This icon lights in blue to indicate that your Router is connected properly to the ADSL. It turns amber when problem is detected.

Off	Router is NOT connected to a functioning ADSL line
Blinking Blue	Router is attempting to connect to the ADSL line
Solid Blue	Router is connected to an ADSL service and is functioning properly
Blinking Amber	Problem with ADSL line



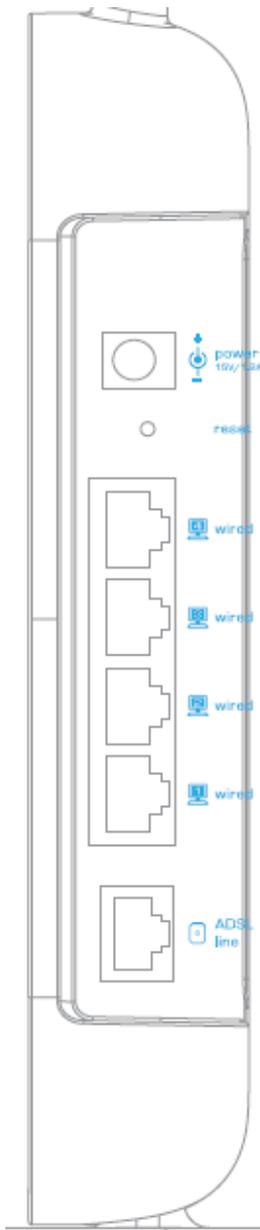
● **F. Internet Status [insert Globe Icon]**

This unique icon shows you when the Router is connected to the Internet. When the light is off, the Router is NOT connected to the Internet. When the light is blinking amber, the Router is attempting to connect to the Internet. When the light is solid blue, the Router is connected to the Internet. When using the “Disconnect after x minutes” feature, this icon becomes extremely useful in monitoring the status of your Router’s connection.

Off	Router is NOT connected to the Internet
Blinking Blue	Router is attempting to connect to the Internet
Solid Blue	Router is connected to the Internet

Blinking Amber	Router is not connected to the Internet
----------------	---

[insert router rear-panel line art with H to K line up to the ports, below is an example for reference only]



G. Connection to ADSL (insert ADSL icon) – Gray

This port is for connection to your ADSL. Connect your ADSL to this port. An RJ11 telephone cord is provided in the package.

H. Connections to Wired Computers (insert Wired Computer icon) – Yellow

Connect your wired (non-wireless) computers to these ports. These ports are RJ45, 10/100 auto-negotiation, auto-uplinking ports for standard UTP category 5 or 6 Ethernet cable. The ports are labeled 1 through 4, with onboard LEDs on the connectors.

I. 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.

i. Resetting the Router

Push and release the “Reset” button. The lights on the Router will momentarily flash. The “Router” light will begin to blink. When the “Router” light becomes solid again, the reset is complete.

ii. Restoring the Factory Defaults

Press and hold the “Reset” button for at least 10 seconds, then release it. The lights on the Router will momentarily flash. The “Router” light will begin to blink. When the “Router” light becomes solid again, the restore is complete.

J. Power Jack – Black

Connect the included 15V/.08A DC power supply to this jack.

K. WPS Push Button (insert the security lock icon) – xxxx (double check)

This button is for [the](#) Wi-Fi Protected Setup™ feature. Refer to the “Changing the Wireless Security Settings” section for more details.

Connecting and Configuring your Modem Router

Verify the contents of your box. You should have the following:

- Belkin G+MIMO Wireless Modem router
- RJ11 Telephone Cord
- RJ45 Ethernet Networking Cable
- Power Supply
- Belkin Personal Network Assistant CD
- User Manual on CD
- Micro Filter (if your ISP line requires)

Setup Assistant

Belkin has provided our 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 or XP 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 v10.4 and v10.5, you must set up the Router using the “Alternate Setup Method” section of this User Manual.

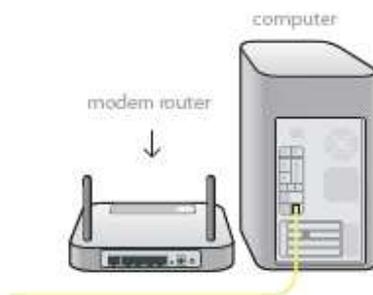
Step 1: Hardware Connections

1.1 Brand-New 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 20. (verify the page number)

- A. Unpack your new Router from the box and place it next to your computer. Raise the Router’s antennas.

[insert line art from QIG]



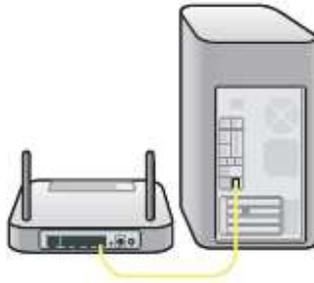
(Modem Router illustrate needs to be modified.)

- B. Retrieve the yellow RJ45 cable that was included with your Router. First, connect one end to any yellow port labeled “Wired” on the back of your Router. Then, connect the other end to the networking

port on the back of your computer. [Insert Ethernet logo]



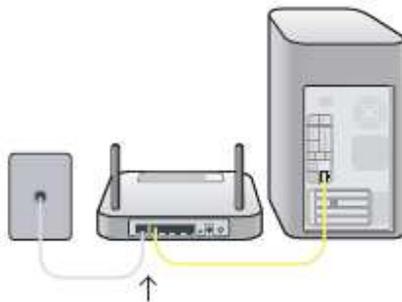
[insert line art from QIG]



(Modem Router illustrate needs to be modified.)

- C. Retrieve the included gray RJ11 phone cord. Connect one end to the gray port labeled “ADSL line” on the back of your Router. Then connect the other end to your ADSL connection (either a wall jack or an ADSL splitter).

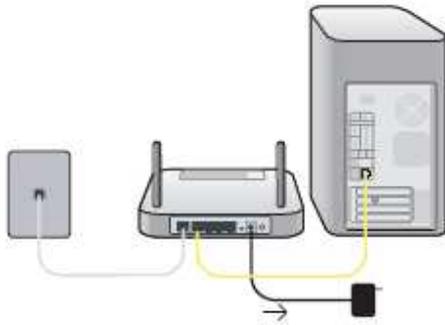
[insert line art from QIG]



(Modem Router illustrate needs to be modified.)

Note: Some ADSL connections require a micro filter. Your ADSL provider can tell you if you need one. Belkin includes a micro filter in regions known to use them. You may or may not have received one in your box.

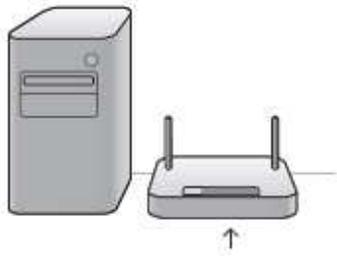
- D. Plug your Router’s power supply into the black port labeled “Power” on the back of your Router. [insert line art from QIG]



modified.)

(Modem Router illustrate needs to be

- E. Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the “Wired” and “Router” icons are lit up in blue. If they are not, recheck your connections.
[insert line art from QIG]



modified.)

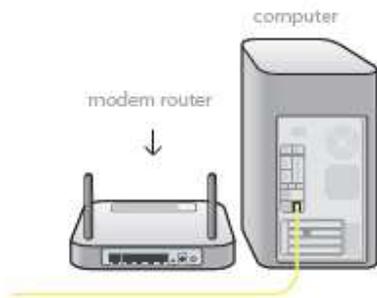
(Modem Router illustrate needs to be

1.2 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.

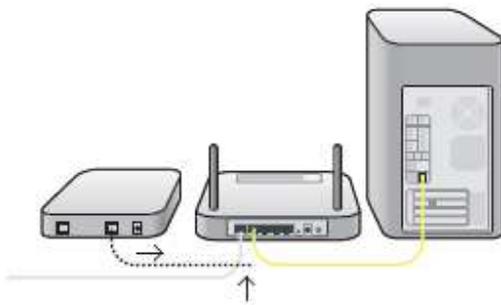
Important: Please unplug the power adapter of your old modem from your wall outlet first.

- A. Unpack your new Router from the box and place it next to your old modem. Raise the Router’s antennas. Unplug your old modem’s power cord.
[insert line art from QIG]



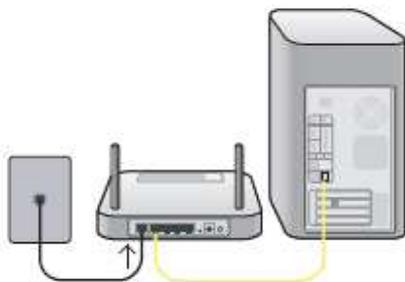
(Modem Router illustrate needs to be modified.)

- B. 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” on the back of your new Router.
[insert line art from QIG]



(Modem Router illustrate needs to be modified.)

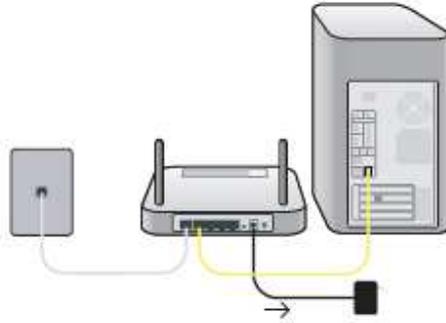
- C. Locate the cable that connects your old modem to the ADSL wall jack. Unplug it from your old modem and then connect it to the gray port labeled “ADSL line” on the back of your Router.
[insert line art from QIG]



(Modem Router illustrate needs to be modified.)

- D. Plug your Router's power supply into the black port labeled "Power" on the back of your Router.

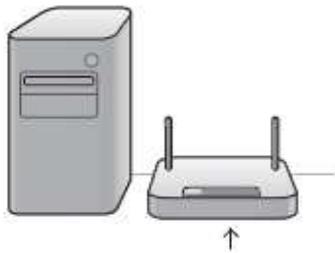
[insert lineart from QIG]



(Modem Router illustrate needs to be modified.)

- E. Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the "Wired" and "Router" icons are lit in blue. If they are not, recheck your connections.

[insert lineart from QIG]



modified.)

(Modem Router illustrate needs to be

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

A. 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.

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

[insert lineart from QIG]



modified.) (Modem Router illustrate needs to be

IMPORTANT: Run the Setup Assistant from the computer that is directly connected to the Router from Step 1.1B.

[Note, all EZI screenshots are updated]

<Insert: EZI1.tif>



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.

Select Country

Select your country from the drop-down box. Click “Begin” to continue.

[insert EZI2b.tif]

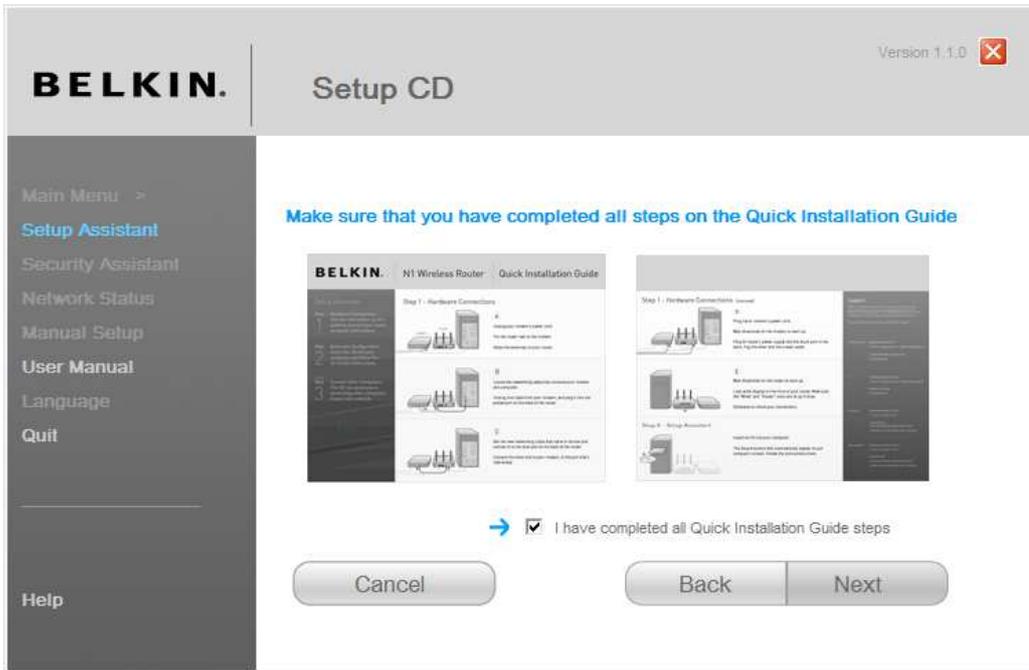


Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only

Confirmation Screen

Verify that you have completed all QIG steps by checking the box to the right of the arrow. Click “Next” to continue.

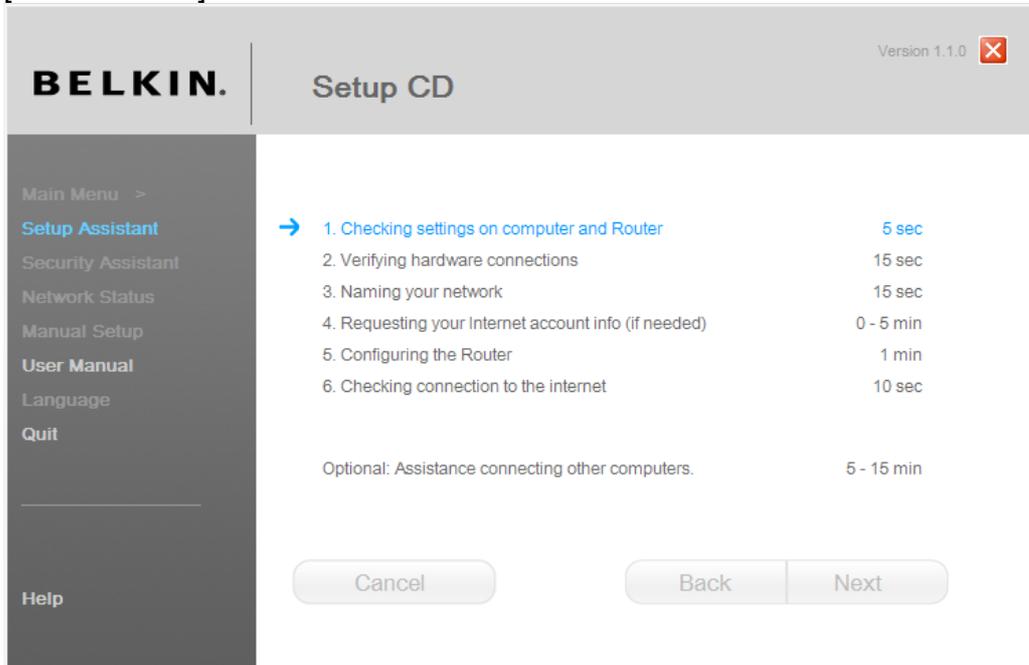
[insert EZI3.tif]



Progress Screen

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

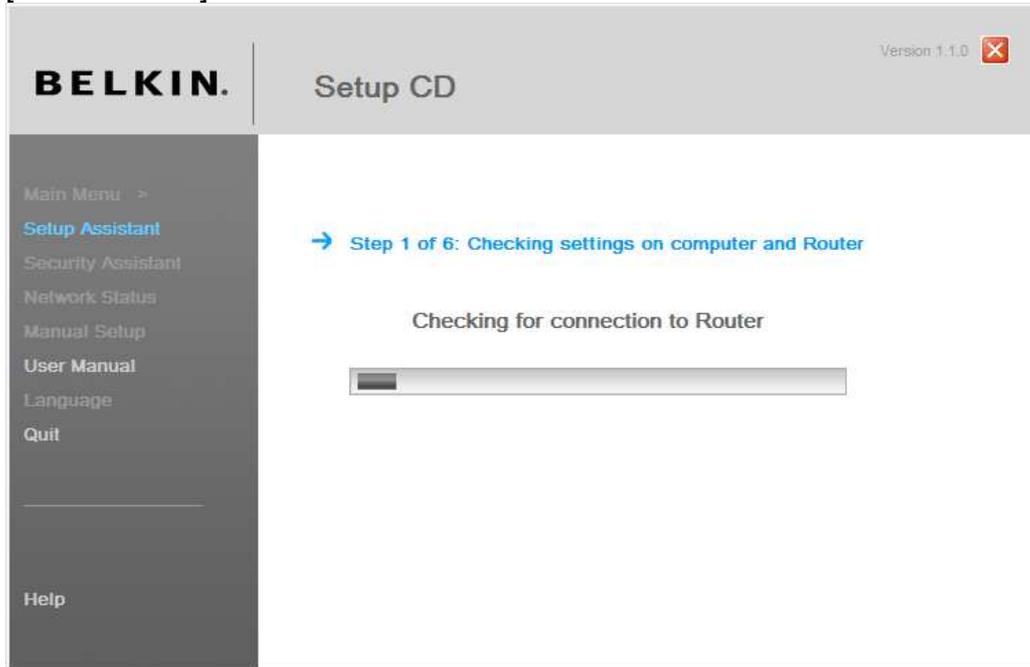
[insert EZI4.tif]



2.1 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.

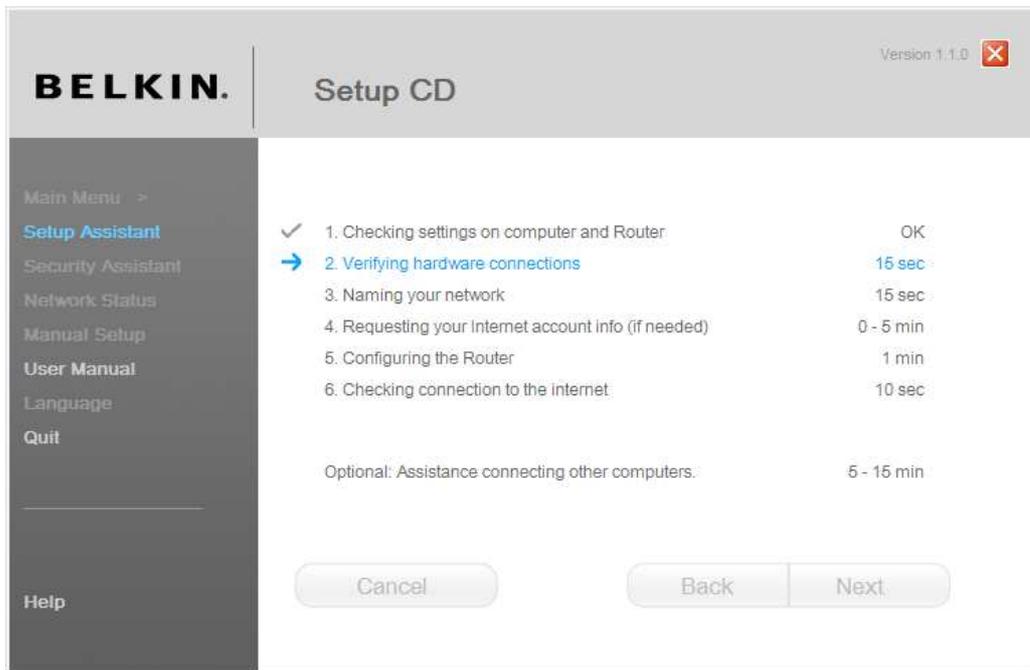
[insert EZI5.tif]



2.2 Verifying Hardware Connections

The Setup Assistant will now verify your hardware connection.

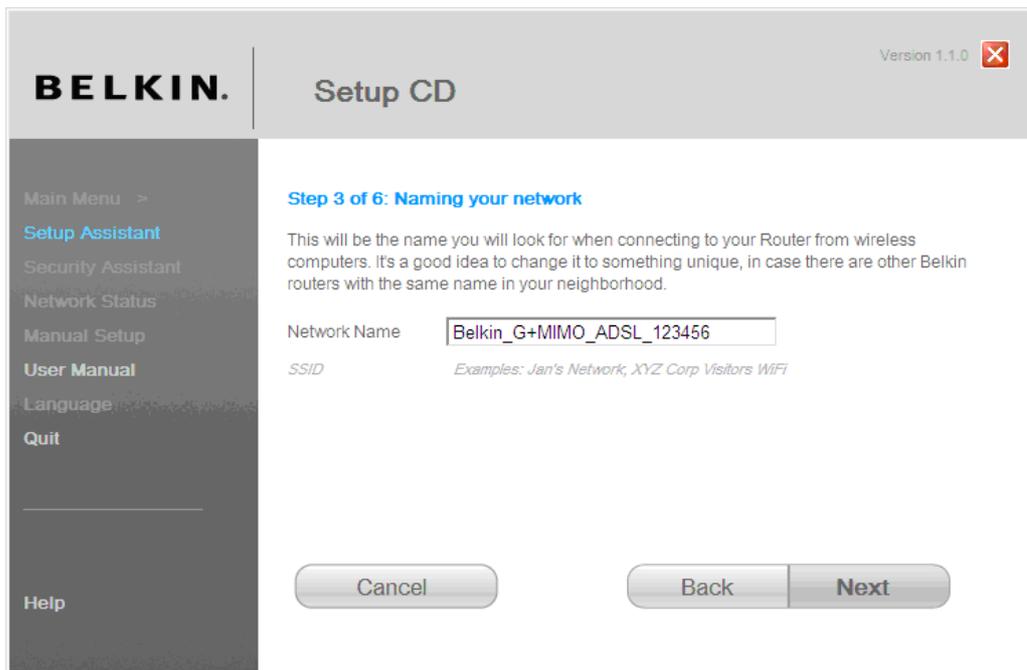
[insert EZI6.tif]



2.3 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.

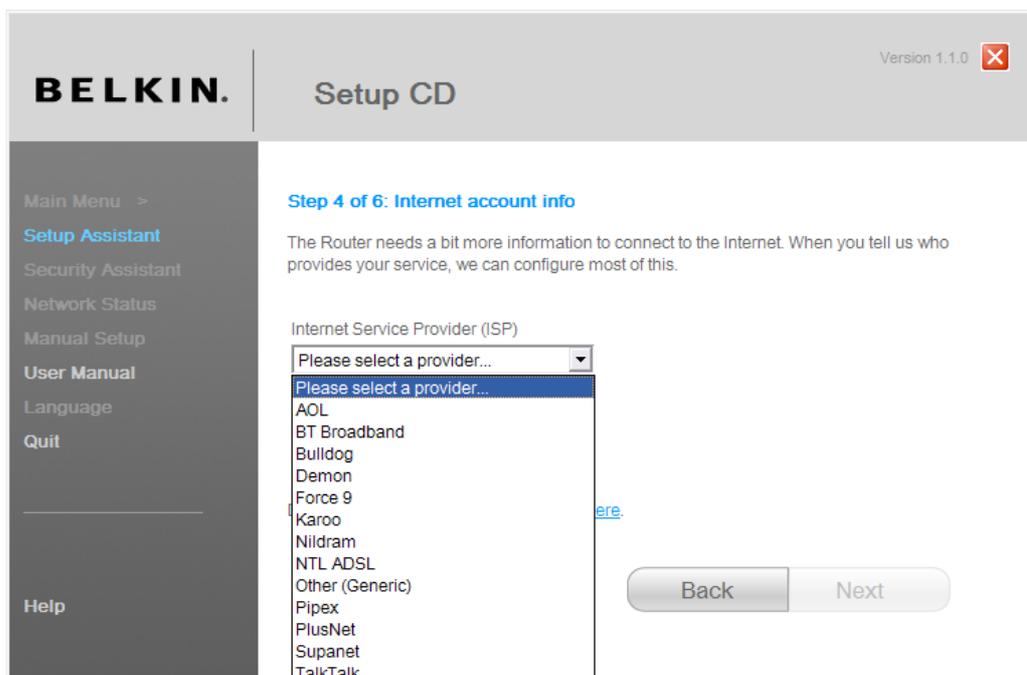
[insert EZI8.tif]



2.4 Requesting Internet Account Info (if needed)

Select your ISP from the drop-down boxes.

[insert EZI10.tif]



If your Internet account requires a login and password, you will be prompted with a screen similar to the illustration below. Click “Next” to continue.

[insert EZI11.tif]

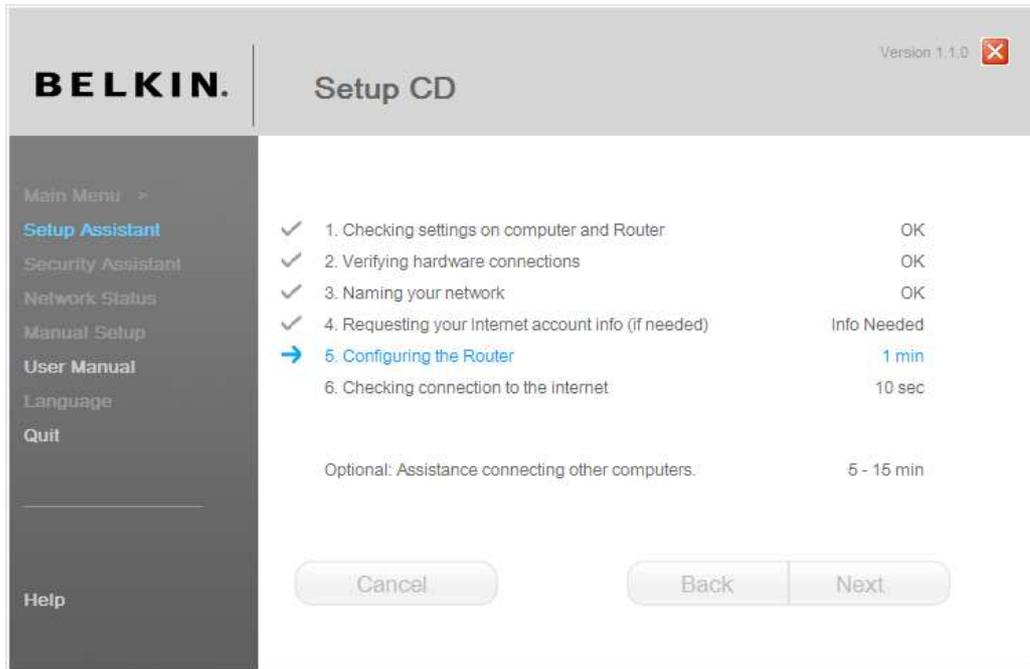
The screenshot shows a web-based setup interface for a Belkin router. The top left corner features the 'BELKIN.' logo. The top right corner displays 'Version 1.1.0' and a close button. The main header reads 'Setup CD'. On the left side, there is a vertical navigation menu with the following items: 'Main Menu >', 'Setup Assistant' (highlighted in blue), 'Security Assistant', 'Network Status', 'Manual Setup', 'User Manual', 'Language', 'Quit', and 'Help'. The main content area is titled 'Step 4 of 6: Internet account info - manual entry'. Below the title, it instructs the user to 'Enter the following information needed for the connection type you chose on the last screen. Your ISP provided this information.' The connection type is identified as 'AOL'. There are two input fields: 'User Name' with the value 'John@MyISP.net' and a subtext example 'Example: username@planet.nl', and 'Password' which is currently masked with seven dots. A checkbox labeled 'View Password' is located below the password field. At the bottom of the form, there are three buttons: 'Cancel', 'Back', and 'Next'.

2.5 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.

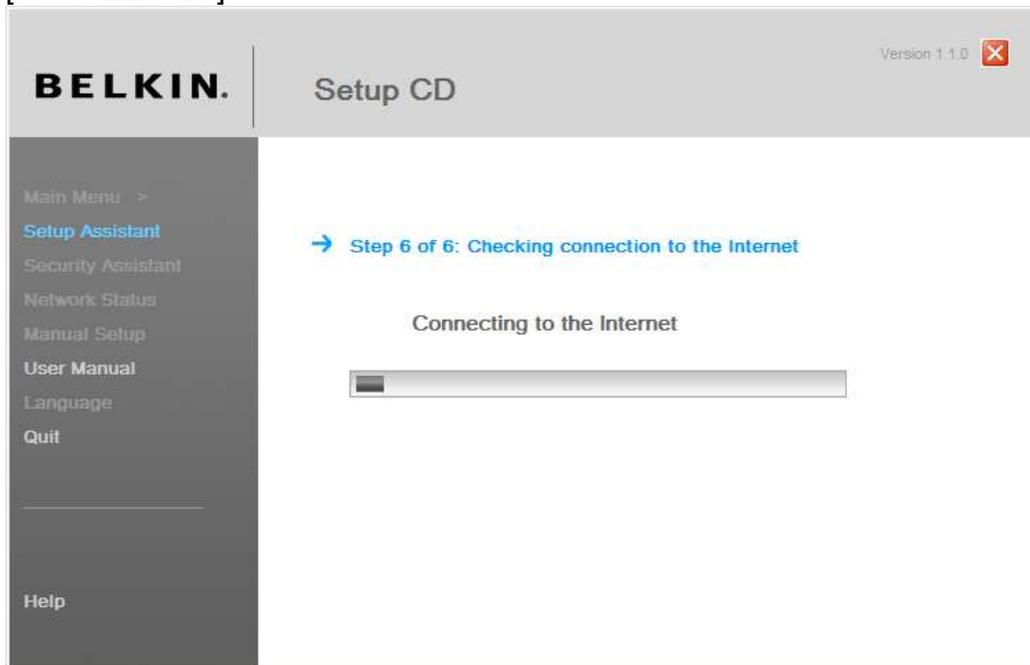
[insert EZI12.tif]



2.6 Checking Internet Connection

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

[insert EZI14.tif]

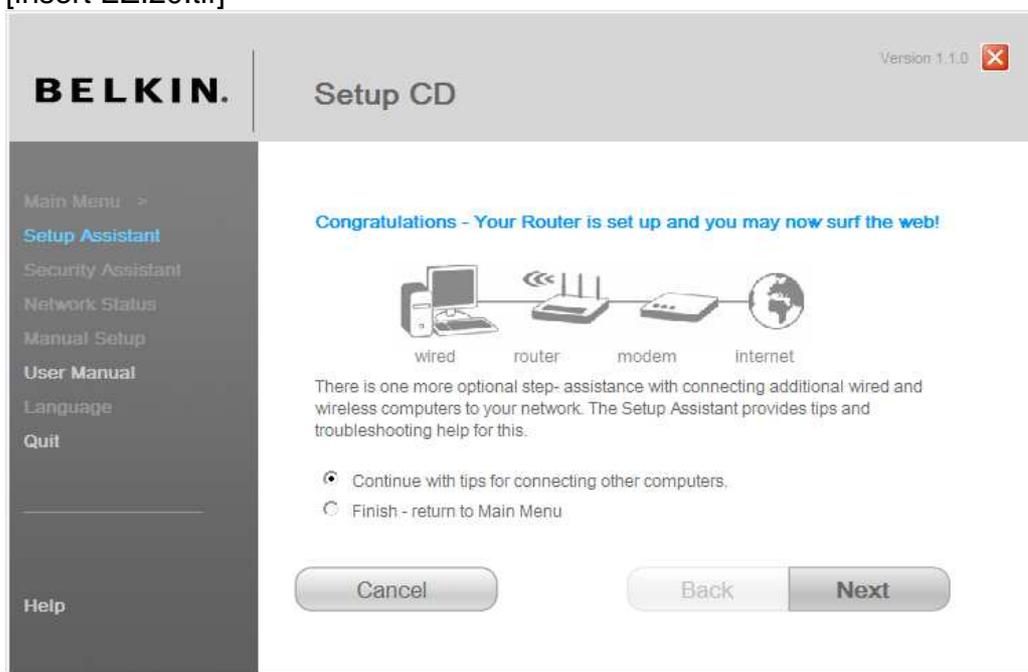


Congratulations

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 “Finish—return to Main Menu” and then click “Next”.

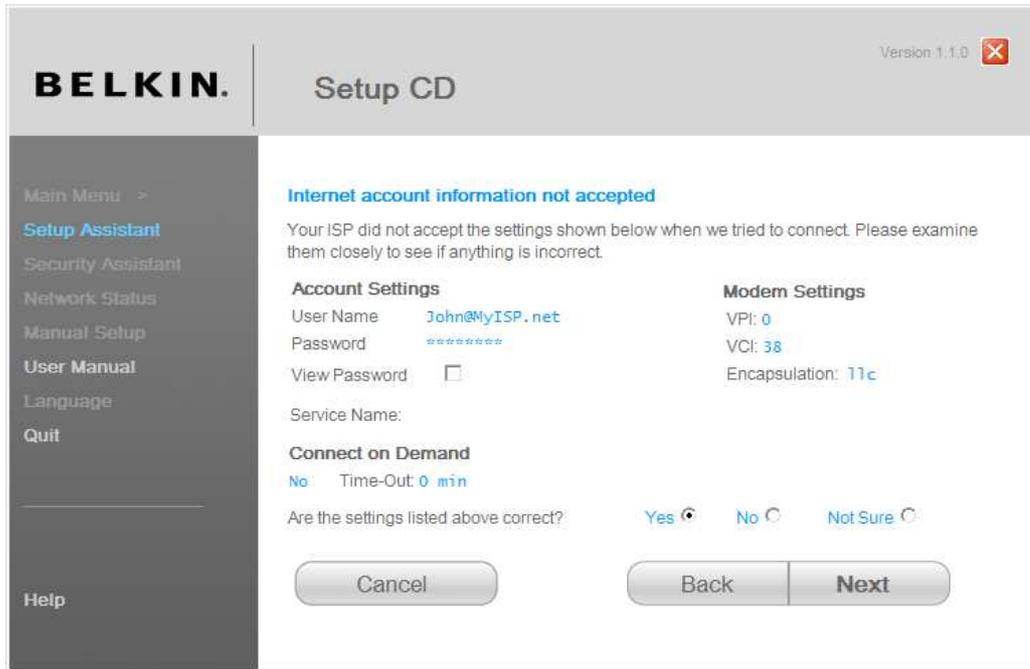
[insert EZI20.tif]



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.

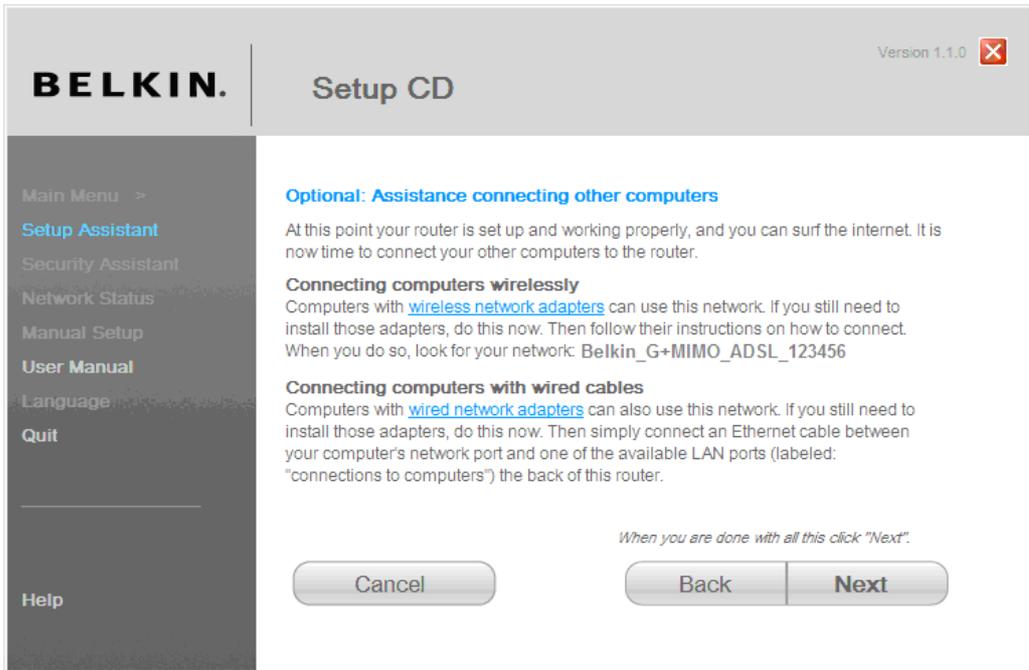
[insert EZI15.tif]



2.7 Optional: Assistance Connecting Other Computers

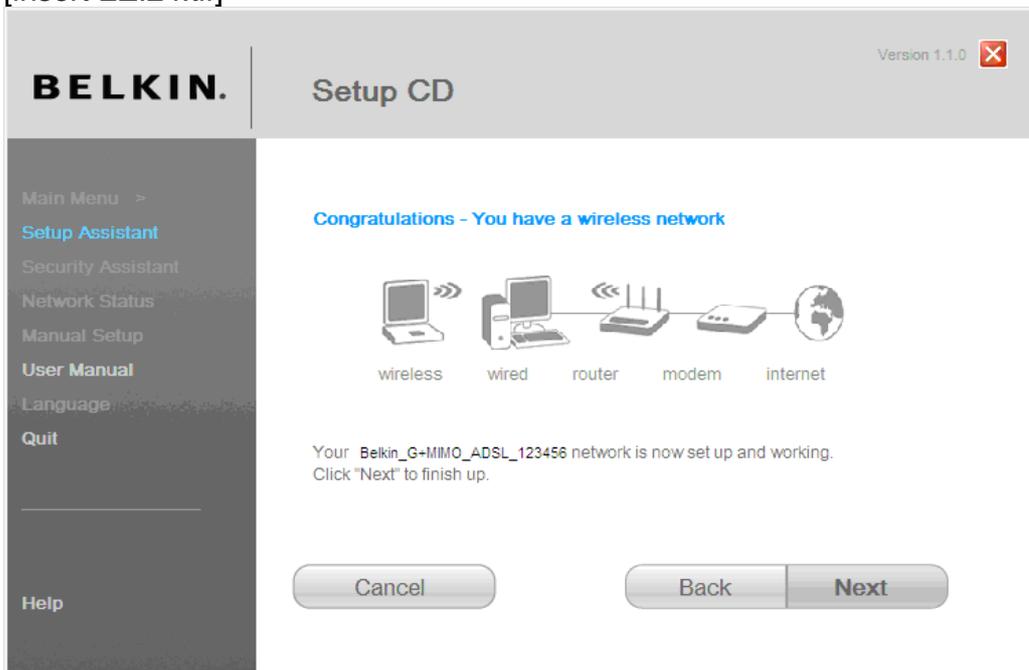
This optional step will help you to connect additional wired and wireless computers to your network. Follow the on-screen instructions.

[insert EZI23.tif]



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 return to the main menu.

[insert EZI24.tif]

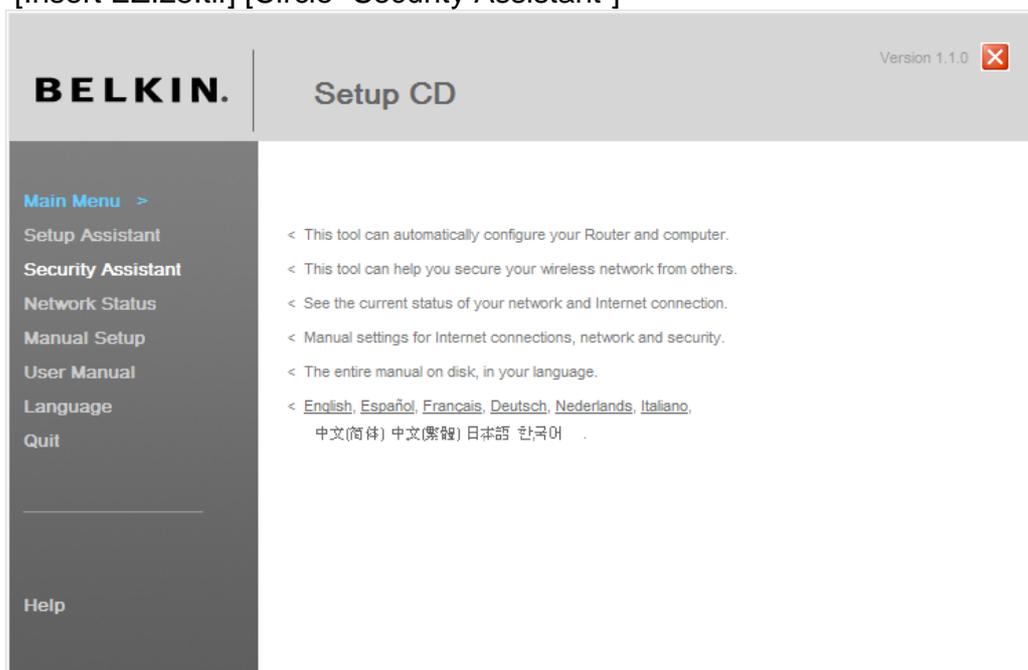


Step 3: Set Up Wireless Security – Run the Security Assistant Software

Now that your network is set up and working, it is recommended that you turn on wireless security to prevent unauthorized access to your network from neighboring wireless-enabled computers. The Security Assistant will guide you through the process. Click “Security Assistant” and follow the on-screen instructions.

IMPORTANT: Run the Setup Assistant from the computer that is directly connected to the Router from Steps 1.1B and 1.2B.

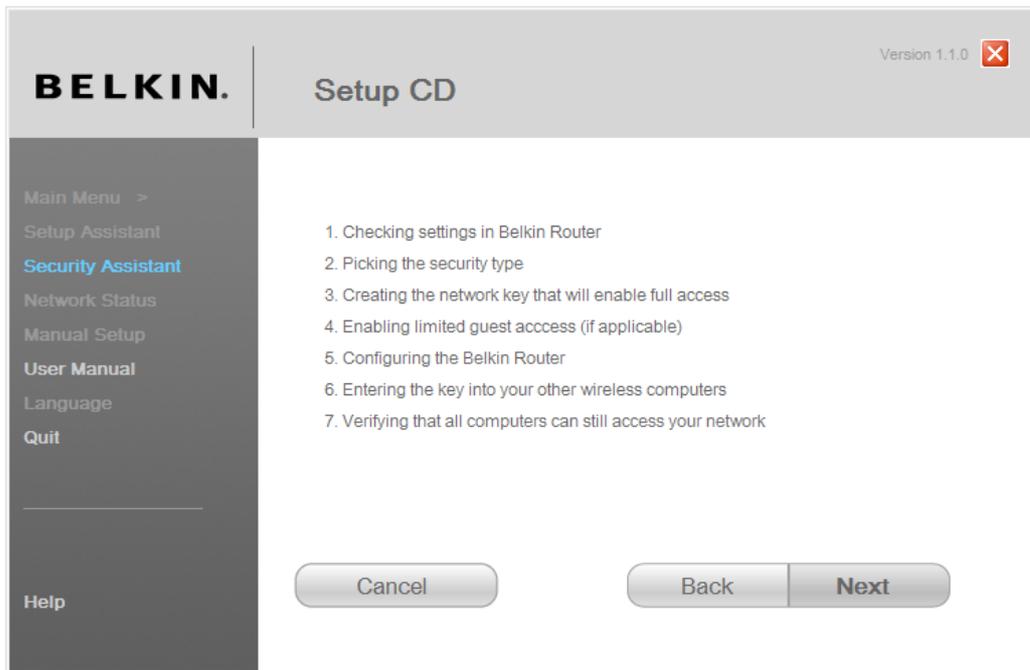
[Insert EZI25.tif] [Circle “Security Assistant”]



Progress Screen

The Security Assistant will show you a progress screen each time a step has been completed.

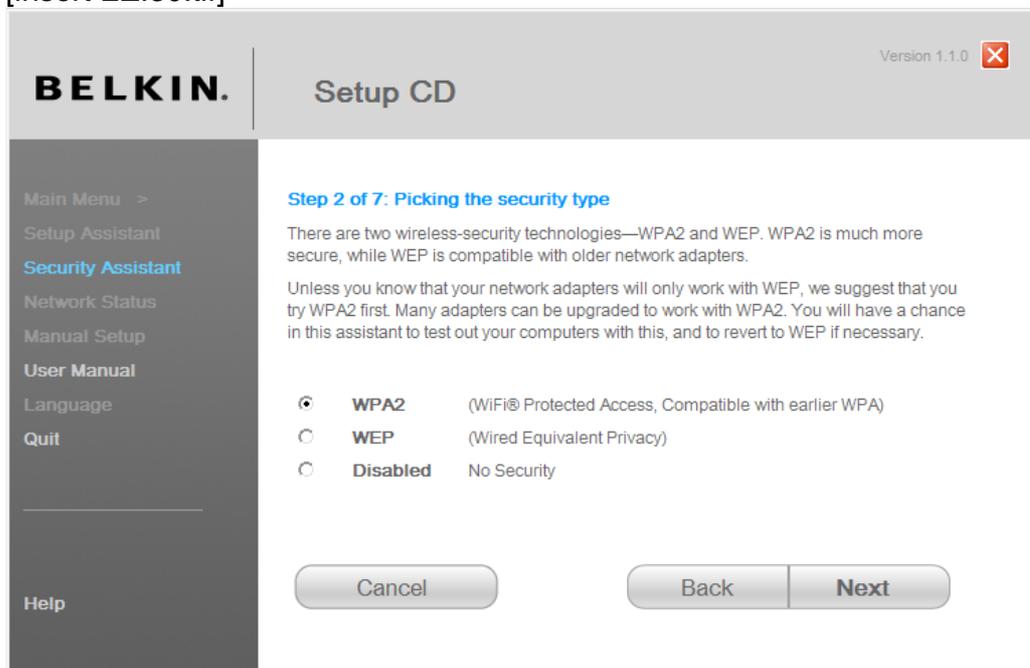
[insert EZI28.tif]



3.1 Picking the Security Type

Select the security type for your wireless network and click “Next” to continue.

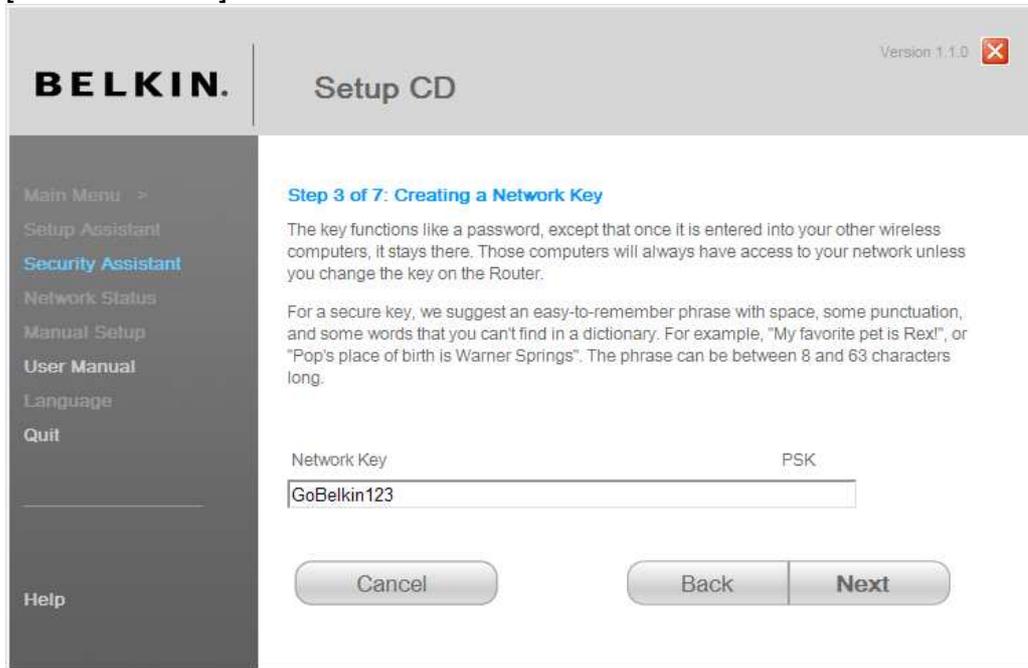
[insert EZI30.tif]



3.2 Creating a Network Key

Enter a network key (PSK) for your wireless network and click “Next” to continue.

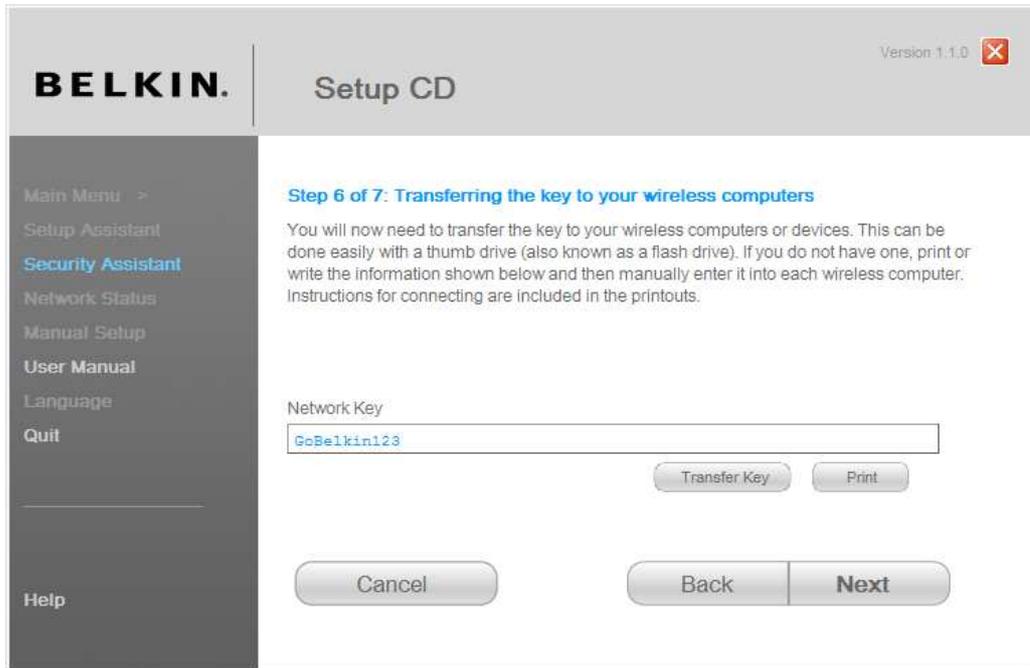
[Insert EZI31.tif]



3.3 Transferring the Key

After setting up your wireless security, you will have to transfer the network key to each of your wireless computers. Click on “Transfer Key” if you have a USB flash drive. Follow the on-screen instructions, or click on “Print” to print the information. Manually enter it to each wireless computer. Then, click “Next” to continue.

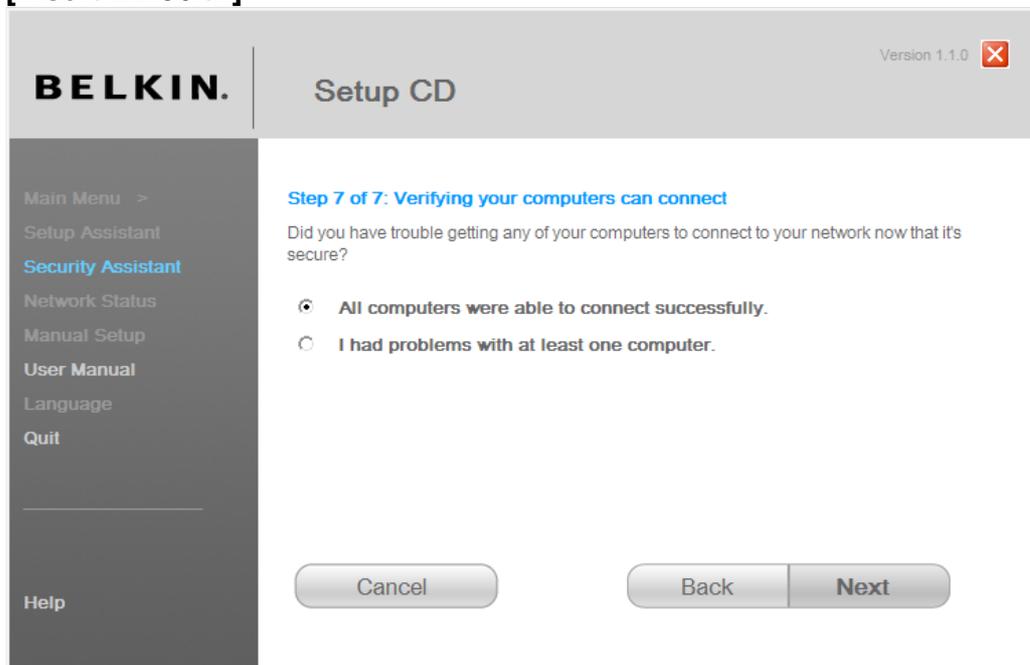
[insert EZI33.tif]



3.4 Verifying the Connection

If all your wireless computers are able to connect to the Router, click "Next". If you are having trouble, select "I had problem with at least one computer" and click "Next". Then, follow on-screen instructions.

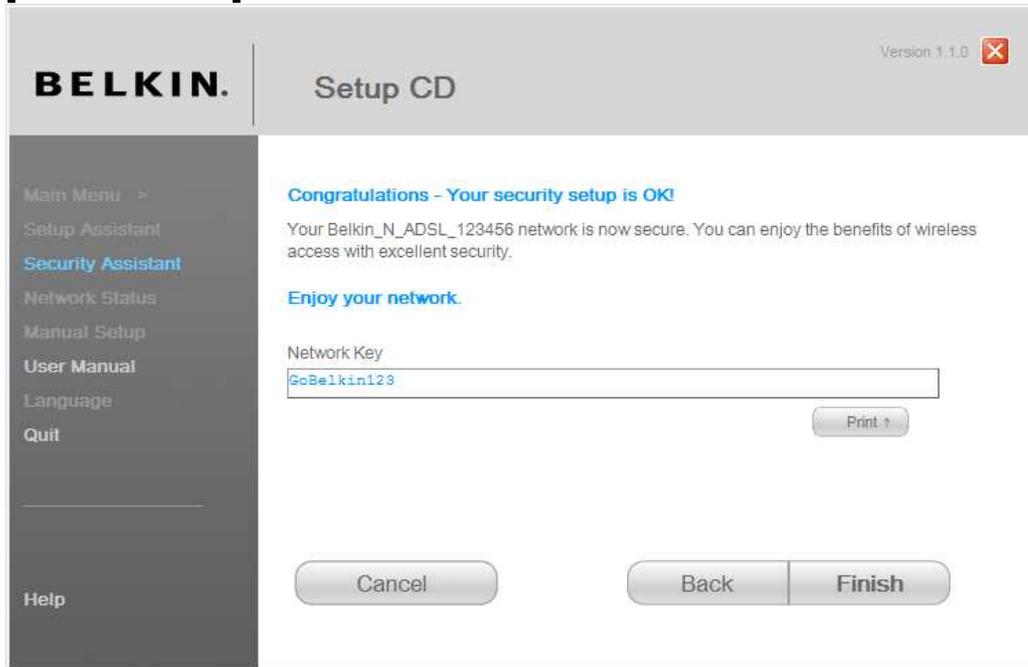
[insert EZI36.tif]



Congratulations

Once you have verified that your wireless computers are properly connected, your wireless network is set up and secured. You now can run your network wirelessly and securely. Click “Finish” to take you back to the main menu.

[insert EZI37.tif]



Alternate Setup Method

Step 1: Hardware Connections – Follow the Quick Installation Guide

See the QIG or Step 1: Hardware Connections from the previous section.

Step 2: Set your Computer’s Network Settings to Work with a DHCP Server

See the section in this User Manual called “Manually Configuring Network Settings” for directions.

Step 3: Configuring the Router Using the Web-Based Advanced User Interface

Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (do not type in anything else such as "http://" or "www"). Then press the "Enter" key.

Address 192.168.2.1

[insert IP_Address.tif]

Logging into the Router

You will see the Router's home page in your browser window. The home page is visible to any user who wants to see it. To make any changes to the Router's settings, you have to log in. Clicking the "Login" button or clicking on any one of the links on the home page will take you to the login screen. The Router ships with no password entered. In the login screen, leave the password blank and click the "Submit" button to log in.

Login

Before you can change any settings, you need to login with a password. If you have not yet set a custom password, then leave this field blank and click "Submit."

Password

Default = leave blank

Clear

Submit

[FW01.tif]

Logging out of the Router

One computer at a time can log into the Router for the purposes of making changes to the settings of the Router. Once a user has logged in to make changes, there are two ways that the computer can be logged out. Clicking the “Logout” button will log the computer out. The second method is automatic. The login will time out after a specified period of time. The default login time-out is 10 minutes. This can be changed from one to 99 minutes. For more information, see the section in this manual titled “Changing the Login Time-Out Setting”.

Understanding the Web-Based Advanced User Interface

The home page is the first page you will see when you access the Advanced User Interface (UI). 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.

[FW02.tif]

BELKIN Router Setup

Home | Help | Login | Internet Status: Connection

Status (10) (9) (2) (5) (4) (3)

You will need to log in before you can change any settings.

Language	
Current Language	English
Available Languages	English Français Deutsch Español Nederlands Italiano

Version Info	
Firmware Version	0.00.07R3 (Jul 6 2007 14:37:05)
Boot Version	V0.05
Hardware	F5D8633-4 v1 (01)
Serial No.	J724318983

LAN Settings	
LAN/WLAN MAC	00-1A-2A-C2-0D-F0
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled (1 LAN, 1 WLAN Clients)

Internet Settings	
WAN MAC Address	00-17-31-47-3E-D1 (Clone MAC)
Connection Type	PPPoE
Subnet Mask	255.0.0.0
WAN IP	69.226.88.206
Default Gateway	192.0.2.100
DNS Address	68.94.156.1

Features	
NAT	Enabled
Firewall Settings	Enabled
SSID	Belkin_N_ADSL_123456
Security	WPA-Personal (PSK)
UPnP	Disabled
Remote Management	Disabled
WPS	Enabled

ADSL	
Type	Fast Path
Status	SHOWTIME
	Downstream Upstream
Data rate(Kbps)	1536kb 384kb
Noise Margin	31 22
Output power(dBm)	8 67
Attenuation(dB)	27 12

1. Quick-Navigation Links

You can go directly to any of the Router’s advanced 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 purple 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, indicating the connection status of the Router. When the indicator says “Connected” in blue, the Router is connected to the Internet. When the Router is not connected to the Internet, the indicator will read “Not Connected” in RED. The indicator is automatically updated when you make changes to the settings of the Router.

6. Connect/Disconnect Buttons

Use these buttons to manually connect or disconnect your ADSL connection as needed.

7. Language

Shows the active language for the Advanced User Interface. Select a desirable language by clicking one of the available languages.

8. Version Info

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

9. 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 on any one of the links (IP Address, Subnet Mask, DHCP Server) or by clicking the “LAN” quick-navigation link on the left side of the screen.

10. 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 links or by clicking on the “Internet/WAN” quick-navigation link on the left side of the screen.

11. Features

Shows the status of the Router’s firewall, wireless, and UPnP, Remote Management 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.

The screenshot shows the Belkin Router Setup interface. The top navigation bar includes the Belkin logo, "Router Setup", and links for Home, Help, Login, and Internet Status (No Connection). A left sidebar lists various setup categories like LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled "Status" and contains several information panels:

- Language:** Current Language: English; Available Languages: English, Français, Deutsch, Español, Nederlands, Italiano.
- Version Info:** Firmware Version: 1.00.01 (May 30 2008 18:50:12); Boot Version: V0.01; Hardware: F5D9631-4 v1 (0A); Serial No.: 12820963100025.
- Internet Settings:** WAN MAC Address: 00-1C-DF-E6-60-C2; Connection Type: PPPoA; WAN IP: NULL; Subnet Mask: NULL; Default Gateway: NULL; DNS Address: NULL.
- LAN Settings:** LAN/WLAN MAC: 00-1C-DF-E6-60-C1; IP Address: 192.168.2.1; Subnet Mask: 255.255.255.0; DHCP Server: Enabled (1 LAN, 0 WLAN Client).
- Features:** Firewall Settings: Enabled; SSID: Belkin_G_Plus_MIMO_ADSL_E660C1; Security: Disabled; UPnP: Enabled; Remote Management: Disabled; WPS: Enabled.
- ADSL:** Type: ---; Status: READY; Data rate(Kbps): 0 Downstream, 0 Upstream; Noise Margin: 0; Output power(dBm): 0; Attenuation(dB): 0.

[9631_”FW01.tif”]

12. ADSL Info

Shows the ADSL status and transmission rates.

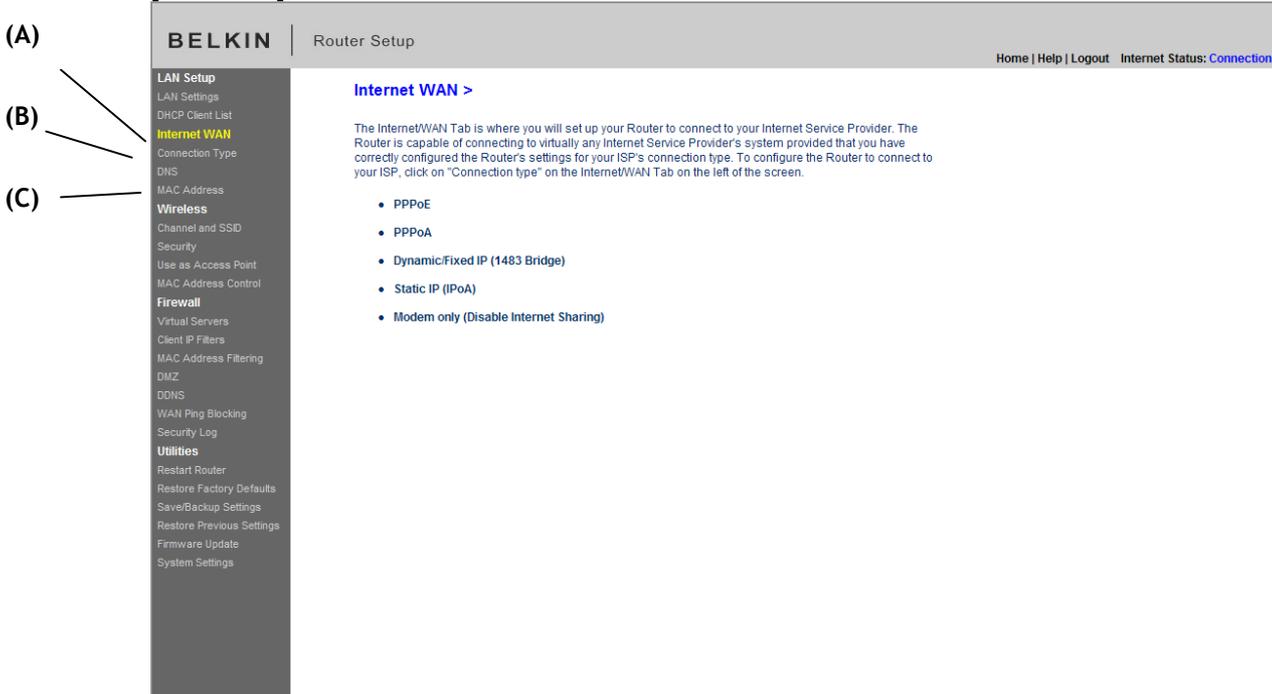
13. Page Name

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

Step 4: Configuring your Router for Connection to your Internet Service Provider (ISP)

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 ISP’s system provided you have correctly configured the Router’s settings for your ISP’s connection type. Your ISP connection settings are provided to you by your ISP. To configure the Router with the settings that your ISP gave you, click “Connection Type” **(A)** on the left side of the screen. Select the connection type you use. If your ISP gave you DNS settings, clicking “DNS” **(B)** allows you to enter DNS address entries for ISPs that require specific settings. Clicking “MAC Address” **(C)** will let you clone your computer’s MAC address or type in a specific WAN MAC address, if required by your ISP. When you have finished making settings, the “Internet Status” indicator will read “connection OK” if your Router is set up properly.

[FW03.tif]



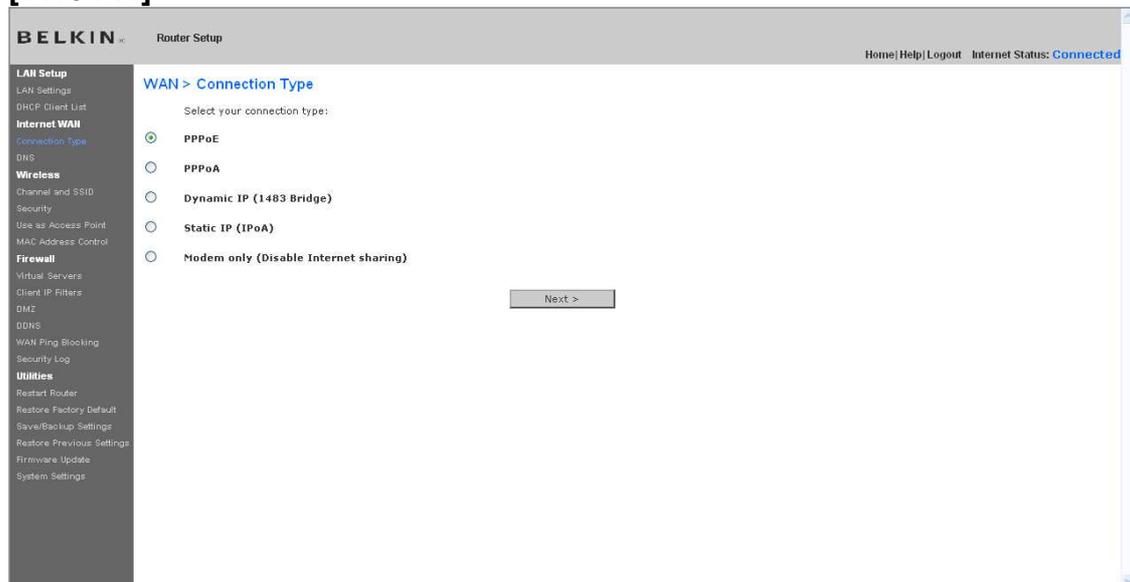
Connection Type

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/Fixed IP (1483 Bridged)**
- **Static IP (IPoA)**
- **Modem Only (Disable Internet Sharing)**

Select the type of connection you use by clicking the radio button (1) next to your connection type and then clicking “Next”.

[FW04.tif]



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.

BELKIN Router Setup Home | Help | Logout | Internet Status

LAN Setup
LAN Settings
DHCP Client List

Internet WAN
Connection Type
DNS
MAC Address

Wireless
Channel and SSID
Security
Wi-Fi Protected Setup
MAC Address Control

Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log

Utilities
Restart Router
Restore Factory Defaults
Save/Backup Settings
Restore Previous Settings

WAN > Connection Type > PPPoE

To enter your PPPoE settings, type in your information below and click "Apply changes". [More Info](#)

Username >

Password >

Retype Password

Service Name (Optional)

IP assigned by ISP Yes

VPI/VCI /

Encapsulation LLC

MTU (500-1500) >

Do not make changes to the MTU setting unless your ISP specifically requires a different setting than 1454. [More Info](#)

Disconnect after minutes of no activity. [More Info](#)

[FW05.tif]

- 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. Service Name (Optional)** - A service name is rarely required by an ISP. If you are not sure if your ISP requires a service name, leave this blank.

5. IP assigned by ISP

- 1) For the Dynamic IP connection - Select "Yes" if your ISP instructed you to use Dynamic IP.
- 2) For the Static IP connection – Select "No" if your ISP instructed you to use Static IP.

- **IP Address** – Enter an IP address assigned by your ISP for the Router WAN interface.

IP assigned by ISP No

IP address . . .

(FW05-1.tif)

- 6. VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier

(VCI) parameter here. (Assigned by your ISP).

7. 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).

8. MTU – Enter the MUT value for your ISP.

9. Disconnect after of x minutes of no activity – Checking the box and enter the number of minute that you want the modem router to auto disconnect after no activity. After this time has been exceeded, the connection will be terminated.

Click “Apply Changes” to save and activate your settings. To go back to the original settings before saving, click “Clear Changes”. Or click any of the Quick-Navigation links for other options. Your new settings will not be saved unless your click “Apply Changes”.

Setting your Connection Type to Dynamic/Fixed IP (1483 Bridged)

This connection method bridges your network and ISP’s network together. The Router can obtain an IP address automatically from your ISP’s DHCP server or accept a fixed IP address assigned by your ISP.

The screenshot shows the Belkin Router Setup interface. The top navigation bar includes the Belkin logo, 'Router Setup', and links for 'Home | Help | Logout' and 'Internet Status: Connection'. A left sidebar lists various setup categories: LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled 'WAN > Connection Type > Dynamic/Fixed IP (1483 Bridge)'. Below the title, there is a instruction: 'To enter your Dynamic IP settings, type in your information below and click "Apply changes".' The settings are as follows: 'IP assigned by ISP' is set to 'Yes'; 'Use static Default Gateway' is unchecked; 'Default Gateway' is set to '0.0.0.0'; 'VPI/VCI' is set to '0/35'; and 'Encapsulation' is set to 'LLC'. At the bottom of the settings area are two buttons: 'Clear Changes' and 'Apply Changes'.

[FW06.tif]

For Dynamic IP connection:

- 1. IP assigned by ISP** – Select “Yes” if your ISP instructed you to use Dynamic IP.
- 2. VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. These identifiers are assigned by your ISP.
- 3. Encapsulation** - Select LLC or VC MUX your ISP uses.

Click “Apply Changes” to save and activate your settings. To go back to the original settings before saving, click “Clear Changes”; or click any of the Quick-Navigation links for other options. Your new settings will not be saved unless you click “Apply Changes”.

The screenshot shows the BELKIN Router Setup interface. The left sidebar contains a navigation menu with categories: LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled 'WAN > Connection Type > Dynamic/Fixed IP (1483 Bridge)'. It includes a sub-header 'To enter your Dynamic IP settings, type in your information below and click "Apply changes".' and several configuration fields: 'IP assigned by ISP' (dropdown menu set to 'No'), 'IP Address' (four input boxes), 'Subnet Mask' (four input boxes), 'Default Gateway' (four input boxes), 'VPI/VCI' (two input boxes with a slash separator, showing '0 / 35'), and 'Encapsulation' (dropdown menu set to 'LLC'). Below the fields are two buttons: 'Clear Changes' and 'Apply Changes'. A link 'Click here to enter your DNS Settings' is also present.

[FW07.tif]

For Static IP connection:

- 1. IP assigned by ISP** – Select “No” if your ISP instructed you to use fixed IP.
- 2. IP Address** – Enter an IP address assigned by your ISP for the Router WAN interface.
- 3. Subnet Mask** – Enter a subnet mask assigned by your ISP.
- 4. Default Gateway** – Enter a default gateway IP address assigned by your ISP.
- 5. VPI/VCI** – Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameters here. These identifiers are assigned by your ISP.
- 6. Encapsulation** – Select the LLC or VC MUX your ISP uses.

Click “Apply Changes” to save and activate your settings. To go back to the original settings before saving, click “Clear Changes”. Or click any of the Quick-Navigation links for other options. Your new settings will not be saved unless you click “Apply Changes”.

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.

The screenshot shows the Belkin Router Setup interface. The top navigation bar includes 'BELKIN Router Setup' and 'Home | Help | Logout | Internet Status: Connection'. The left sidebar lists various setup categories: LAN Setup, Internet WAN, Wireless, Security, Firewall, and Utilities. The main content area is titled 'WAN > Connection Type > Static IP (IPoA)'. It contains the following fields and options:

- WAN IP Address >**: Four input boxes for IP address.
- Subnet Mask >**: Four input boxes for subnet mask.
- Use static Default Gateway:**
- Default Gateway >**: Four input boxes for default gateway.
- VPI/VCI >**: Two input boxes, one with '0' and the other with '35'.
- Encapsulation >**: A dropdown menu with 'LLC' selected.

At the bottom of the form are two buttons: 'Clear Changes' and 'Apply Changes'. A link 'Click here to enter your DNS Settings' is also present.

[FW08.tif]

- 1. WAN 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. Use Static 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 Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. These identifiers are assigned by your ISP.
- 5. Encapsulation** - Select LLC or VC MUX your ISP uses.

Click “Apply Changes” to save and activate your settings. To go back to the original settings before saving, click “Clear Changes”. Or click any of the Quick-Navigation links for other options. Your new settings will not be saved unless you click “Apply Changes”.

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.

The screenshot shows the Belkin Router Setup interface. The top navigation bar includes 'BELKIN Router Setup' and links for 'Home | Help | Logout | Internet Status: Connection'. The left sidebar lists various setup categories: LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled 'WAN > Connection Type > Modem only (Disable Internet Sharing)'. It contains a sub-header 'WAN > Connection Type > Modem only (Disable Internet Sharing)', a note 'To enter your Modem settings, type in your information below and click "Apply changes".', and two input fields: 'VPI/VCI >' with values '0' and '35', and 'Encapsulation >' with a dropdown menu set to 'LLC'. At the bottom of the form are two buttons: 'Clear Changes' and 'Apply Changes'.

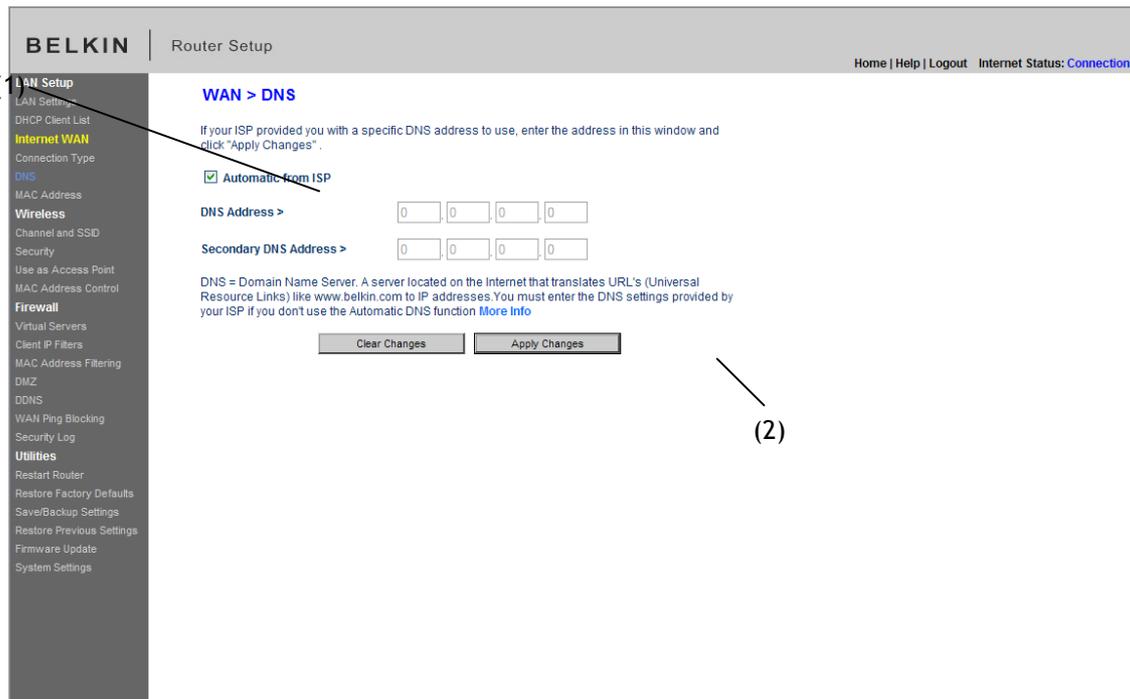
[FW09.tif]

1. **Enable Bridge Service** – Check this box to enable bridge service
2. **VPI/VCI** – Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameters here. (Assigned by your ISP).
3. **Encapsulation** – Select the LLC or VC MUX your ISP uses.

Click “Apply Changes” to save and activate your settings. To go back to the original settings before saving, click “Clear Changes”. Or click any of the Quick-Navigation links for other options. Your new settings will not be saved unless you click “Apply Changes”.

Setting Custom Domain Name Server (DNS) Settings

A “Domain Name Server” is a server located on the Internet that translates Universal Resource Locaters (URLs) like “www.belkin.com” to IP addresses. Many Internet Service Providers (ISPs) do not require you to enter this information into the Router. The “Automatic from ISP” box **(1)** 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)** to save the settings.



[FW10.tif]

Using the Web-Based Advanced User Interface

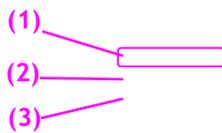
Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (do not type in anything else such as "http://" or "www") then press the "Enter" key.

Address 192.168.2.1 [insert IP_Address.tif] Use the same screenshot

You will see the Router's home page in your browser window.

Viewing the LAN Settings

Clicking on the header of the LAN tab (1) 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" (2) or to view the list of connected computers, click on "DHCP client list" (3).



BELKIN Router Setup Home | Help | Logout | Internet Status: [Connection](#)

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Defaults
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings

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

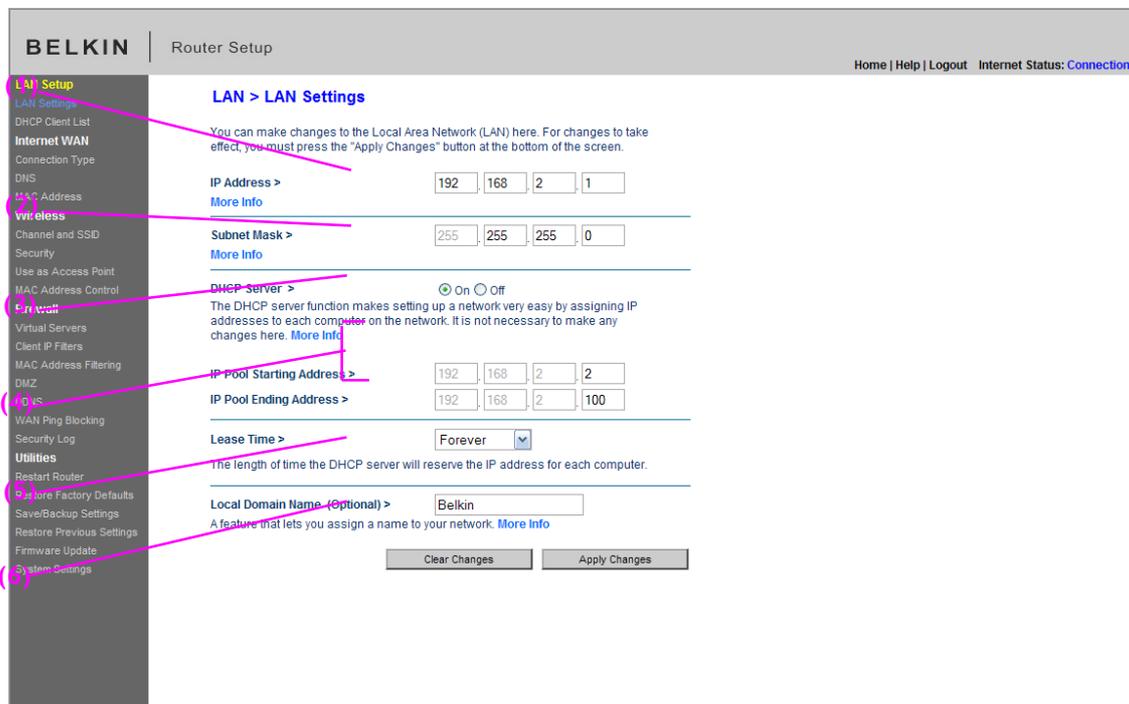
To make changes, click "LAN Settings" on the LAN tab to the left.

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.

[FW11.tif]

Changing LAN Settings

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



[FW12.tif]

1. 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)

2. Subnet Mask

There is no need to change the subnet mask. This is a unique, advanced feature of your Belkin Router. It is possible to change the subnet mask if necessary; however, do NOT make changes to the subnet mask unless you have a specific reason to do so. The default setting is "255.255.255.0".

3. 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”.

4. IP Pool

The range of IP addresses set aside for dynamic assignment to the computers on your network. The default is 2–100 (99 computers). 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 DHCP server can assign 100 IP addresses automatically. This means that you cannot specify an IP address pool larger than 100 computers. For example, starting at 50 means you have to end at 150 or lower so as not to exceed the 100-client limit. The starting IP address must be lower in number than the ending IP address.

5. Lease Time

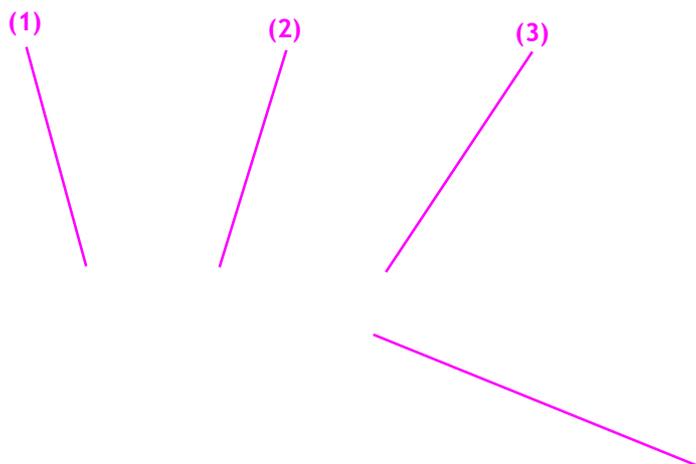
The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to “Forever”. The default setting is “Forever”, meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular 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.

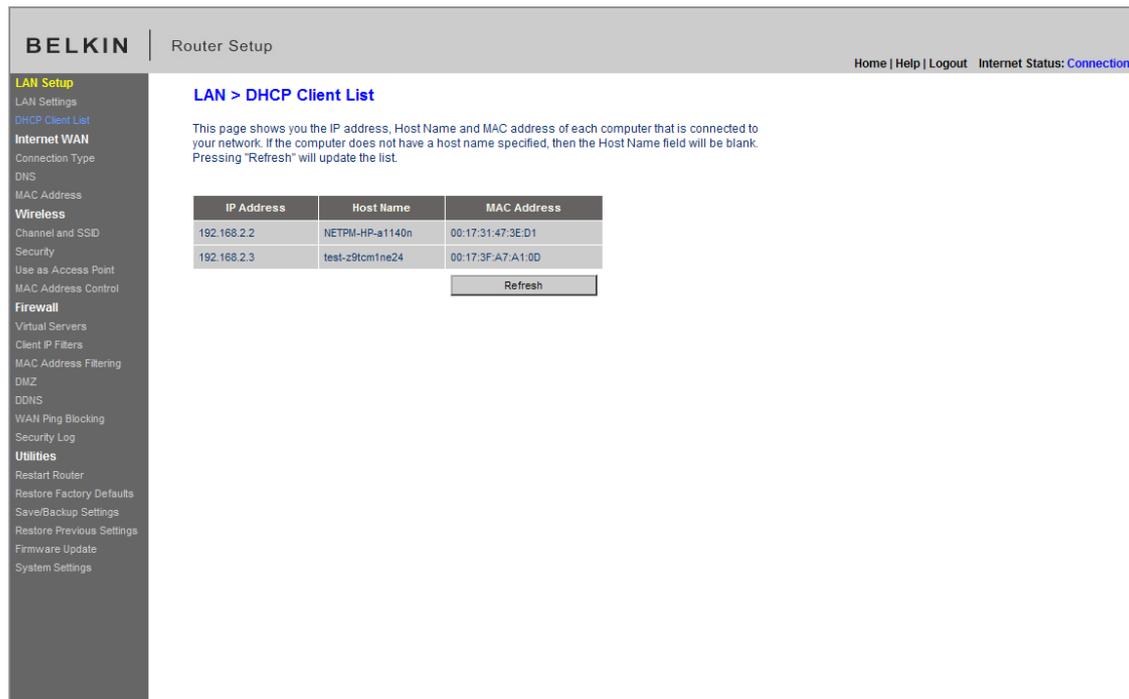
6. Local Domain Name (Optional)

The default setting is “Belkin”. 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”.

Viewing the DHCP Client List Page

You can view a list of the computers (known as clients), which are connected to your network. You are able to view the IP address **(1)** of the computer, the host name **(2)** (if the computer has been assigned one), and the MAC address **(3)** of the computer’s network interface card (NIC). Pressing the “Refresh” **(4)** button will update the list. If there have been any changes, the list will be updated.





[FW13.tif]

Configuring the Wireless Network Settings

The "Wireless" tab lets you make changes to the wireless network settings. From this tab you can make changes to the wireless network name or Service Set Identifier (SSID), operating channel, encryption security settings, and configure the Router to be used as an access point.

Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID is used. The SSID is your network name. The default network name of the Router is "Belkin_G+MIMO_" followed by six digits that are unique to your Router. Your network name will look something like "Belkin_G+MIMO_123456". You can change this to anything you choose, or you can leave it unchanged. Keep in mind, if you decide to change your wireless network name, and there are other wireless networks operating in your area, your network name needs to be different from other wireless networks that may be operating in your area. To change the SSID, type in the SSID that you want to use in the SSID field **(1)** and click "Apply Changes" **(2)**. 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.

(1)



[9631_”FW02.tif”]

Note: Please periodically check for new Router firmware updates from the “Utilities > Firmware update” page. Newer firmware can fix problems, add wireless features, and/or improve wireless performance (see page 69).
[Designer, Please match page number to the firmware update section]

Changing the Wireless Channel

There are a number of operating channels from which you can choose—in the United Kingdom (and most of Europe), Australia, and most of Asia, there are 13. In other countries, there are other channel requirements. Your Router is configured to operate on the proper channels for the country in which you reside. 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.

Using the Wireless Mode Switch

This switch allows you to set the Router’s wireless modes. There are several modes.

Note: Some modes may require firmware updates to be enabled.

802.11b&802.11g 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 Wi-Fi-compatible devices. If you have a mix of 802.11b and 802.11g clients in your network, we recommend setting the Router to g and b mode. This setting should only be changed if you have a specific reason to do so.

802.11g Mode

802.11g 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”.

802.11b 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.

off Mode

This option will off the wireless functionality.

When to use b only Mode

In some cases, older 802.11b clients may not be compatible with 802.11g wireless. These adapters tend to be of inferior design and may use older drivers or technology. Switching to this mode can solve problems that sometimes occur with these clients. If you suspect that you are using a client adapter that falls into this category of adapters, first check with the adapter vendor to see if there is a driver update. If there is no driver update available, switching to b only mode may fix your problem. **Please note that switching to b only mode will decrease 802.11g performance.**

Using the Broadcast SSID Feature

Note: This advanced feature should be employed by advanced users only. For security, 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, remove the check mark from the box next to “Broadcast SSID”, 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.

Protected Mode Switch

Protected mode ensures proper operation of G+MIMO, 802.11g-compliant devices on your wireless network when 802.11g or 802.11b devices are present or when there is heavy 802.11g or 802.11b traffic in the operating environment. Use protected mode if your network consists of a mix of Belkin G+MIMO Wireless Cards and 802.11g or 802.11b cards on your network. If you are in an environment that includes little to no 802.11g or 802.11b wireless network traffic,

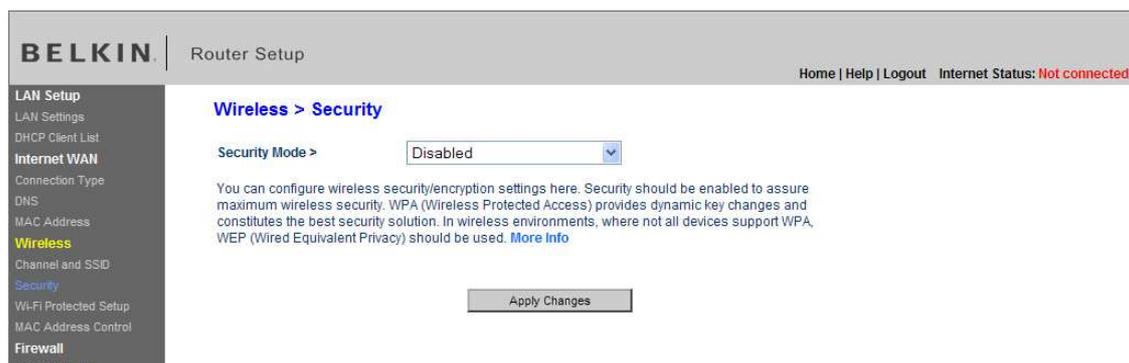
you will achieve the best G+MIMO wireless performance with protected mode OFF. Conversely, in an environment with HEAVY 802.11g or 802.11b traffic or interference, you will achieve the best G+MIMO wireless performance with protected mode ON. This will ensure G+MIMO wireless performance is not affected.

802.11e/WMM (Wi-Fi® Multimedia) QoS

WMM, based on 802.11e QoS (Quality of Service), prioritizes important data on your network, such as multimedia content and voice-over-IP (VoIP), so it will not be interfered with by other data being sent over the network. This feature requires other wireless devices, such as Wi-Fi phones or wireless laptops, to support WMM for best results.

Changing the Wireless Security Settings

Your Router is equipped with the latest security standard called Wi-Fi Protected Access™ 2 (WPA2™) and the legacy security standard called Wired Equivalent Privacy (WEP). Your Router also supports the Wi-Fi Protected Setup (WPS) specification, which simplifies the setup of a wireless network. WPS uses familiar methodologies, such as typing in a Personal Identification Number (PIN) or pushing a button, to enable users to automatically configure network names and strong WPA2 data encryption and authentication. By default, your Router does not ship with security enabled. You may automatically configure the security settings using WPS. To change the security settings manually, you will need to determine which standard you want to use. To access the security settings, click “Security” on the “Wireless” tab.



(FW15.tif)

Using Wi-Fi Protected Setup

WPS uses WPA2 (described below) for encryption. It does not provide additional security, but rather, standardizes the method for securing your wireless network.

You may use either the Push Button Configuration (PBC) method or PIN method to allow a device access to your wireless network. Conceptually, the two methods work as follows:

PBC: Push and hold the WPS button located on the back of your Router for three seconds. Then initiate the WPS procedure on the client device within two minutes. Refer to your client's documentation on this procedure. Pushing the PBC button will automatically enable WPS. The client has now been securely added to your wireless network.

PIN: The client device has a PIN number (either four or eight digits) that is associated with WPS. Enable WPS through the GUI shown below. Enter the client's PIN into the Router's internal registrar (accessed through this GUI). The client will be automatically enrolled into your wireless network within two minutes.

(FW16.tif)

The screenshot shows the Belkin Router Setup interface. The top navigation bar includes the Belkin logo, 'Router Setup', and links for 'Home | Help | Logout'. The 'Internet Status' is shown as 'Not connect'. The left sidebar contains a menu with categories: LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled 'Wireless > Wi-Fi Protected Setup (WPS)'. It features a dropdown menu for 'Wi-Fi Protected Setup (WPS)' set to 'Enabled' and an 'Apply Changes' button. Below this, three methods are detailed: 1) Personal Information Number (PIN) Method, which includes an 'Enter Client Device PIN' field and an 'Enroll' button; 2) Push Button Configuration (PBC) Method, which includes a 'Start PBC' button; and 3) Manual Configuration Method, which lists network settings: Network Name (SSID) as 'Belkin_N_ADSL_E35387' and Wireless Security as 'No Security'. A note at the bottom of the manual method section says 'Please configure wireless security'.

1. Wi-Fi Protected Setup (WPS): Enabled or Disabled.
2. Personal Identification Number (PIN) Method: In this method, a wireless client wishing to access your network must supply an 8-digit PIN to the

- Router. After clicking “Enroll”, you must start the WPS handshaking procedure from the client within two minutes.
3. Router PIN: If an external registrar is available, you may enter in the Router’s PIN to the registrar. Click “Generate New PIN” to change the PIN from the default value. Click “Restore Default PIN” to reset the PIN value.
 4. Push Button Configuration (PBC) Method: PBC is an alternate method to connect to a WPS network. Push the PBC button located on the back of the Router for three seconds, and then initiate the PBC on the client device. Alternatively, push the “Start PBC” soft button to start this process.
 5. Manual Configuration Method: This section lists the default security settings if not using WPS.

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 Advanced Encryption Standard (AES) encryption methods.

WPA2 Requirements

IMPORTANT: In order to use WPA2 security, all your computers and wireless client adapters must be upgraded with patches, driver, and client utility software that supported 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 Windows XP computers that do 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://support.microsoft.com/kb/826942>

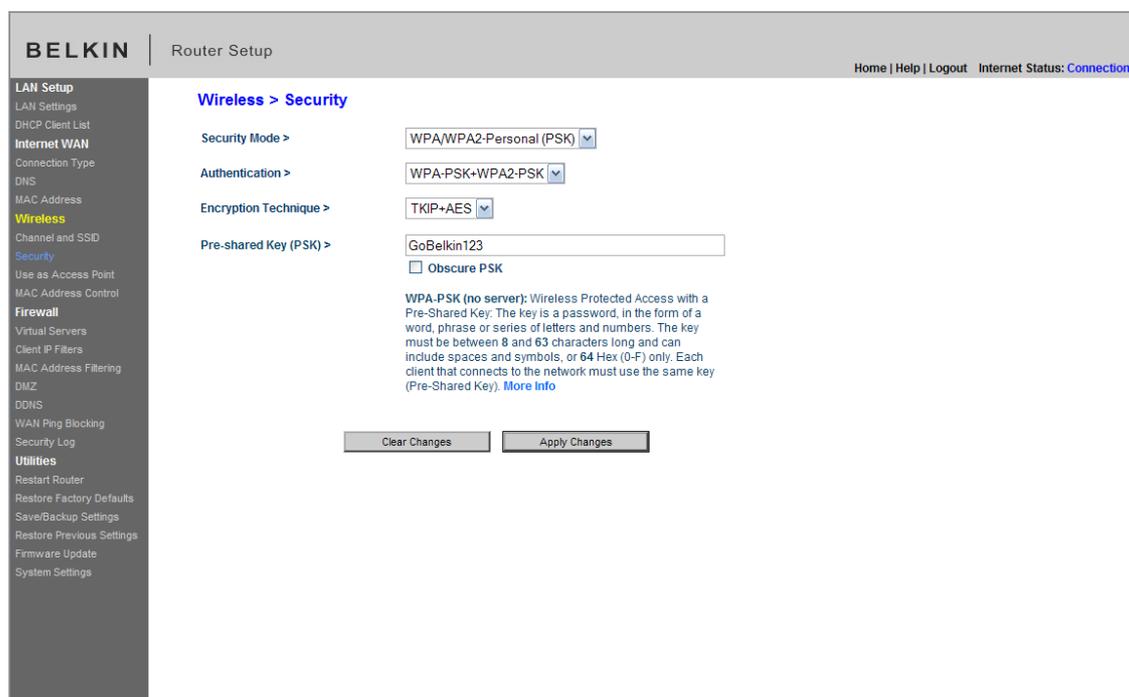
For Windows XP with Service Pack 2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB971021). The update is available from: <http://support.microsoft.com/kb/917021>

IMPORTANT: You also need to ensure that all your wireless client cards/adapters support WPA2, and that you have downloaded and installed the latest driver. Most of the Belkin wireless cards have driver updates available for download from the Belkin support site: www.belkin.com/networking.

Setting WPA/WPA2-Personal (PSK)

Like WPA security, WPA2 is available in WPA2-Personal (PSK) mode. Typically, WPA2-Personal (PSK) is the mode that will be used in a home environment. Please refer to the User Manual for more information about wireless security and different types of wireless security.

1. After you've set up your Router, go to the "Security" page under "Wireless" and select "WPA/WPA2-Personal (PSK)" from the "Security Mode" drop-down menu.
2. For "Authentication", select "WPA-PSK", "WPA2-PSK", or "WPA-PSK + WPA2-PSK". This setting will have to be identical on the wireless clients that you set up. "WPA-PSK + WPA2-PSK" mode will allow the Router to support clients running either WPA or WPA2 security.
3. For "Encryption Technique", select "TKIP", "AES", or "TKIP+AES". This setting will have to be identical on the wireless clients that you set up.
4. Enter your pre-shared key (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 wireless clients that you set up. For example, your PSK might be something like: "Smith family network key". Click "Apply Changes" to finish. You must now set all wireless clients to match these settings.



[FW17.tif]

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

Setting WPA Security

Note: To use WPA security, your wireless network cards must be equipped with software that supports WPA. At the time this User Manual was published, a security patch from Microsoft is available for free download. This patch works only with Windows XP.

Your Router supports WPA-PSK. WPA-PSK uses what is known as a pre-shared key as the security key. A pre-shared key is basically a password that is between eight and 39 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same key to access the network. Typically this is the mode that will be used in a home environment.

Setting WPA-PSK

1. From the “Security Mode” drop-down menu, select “WPA-PSK”.
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. This can be from eight to 39 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.
4. Click “Apply Changes” to finish. You must now set all clients to match these settings.

The screenshot shows the Belkin Router Setup interface. The page title is "Router Setup" and the breadcrumb is "Wireless > Security". The left sidebar contains a navigation menu with categories: LAN Setup, Internet WAN, Wireless (highlighted), Firewall, and Utilities. The main content area shows the following settings:

- Security Mode >: WPA/WPA2-Personal (PSK)
- Authentication >: WPA-PSK
- Encryption Technique >: TKIP
- Pre-shared Key (PSK) >: GoBelkin123
- Obscure PSK

Below the settings is a note: "WPA-PSK (no server): Wireless Protected Access with a Pre-Shared Key: The key is a password, in the form of a word, phrase or series of letters and numbers. The key must be between 8 and 63 characters long and can include spaces and symbols, or 64 Hex (0-F) only. Each client that connects to the network must use the same key (Pre-Shared Key). [More Info](#)"

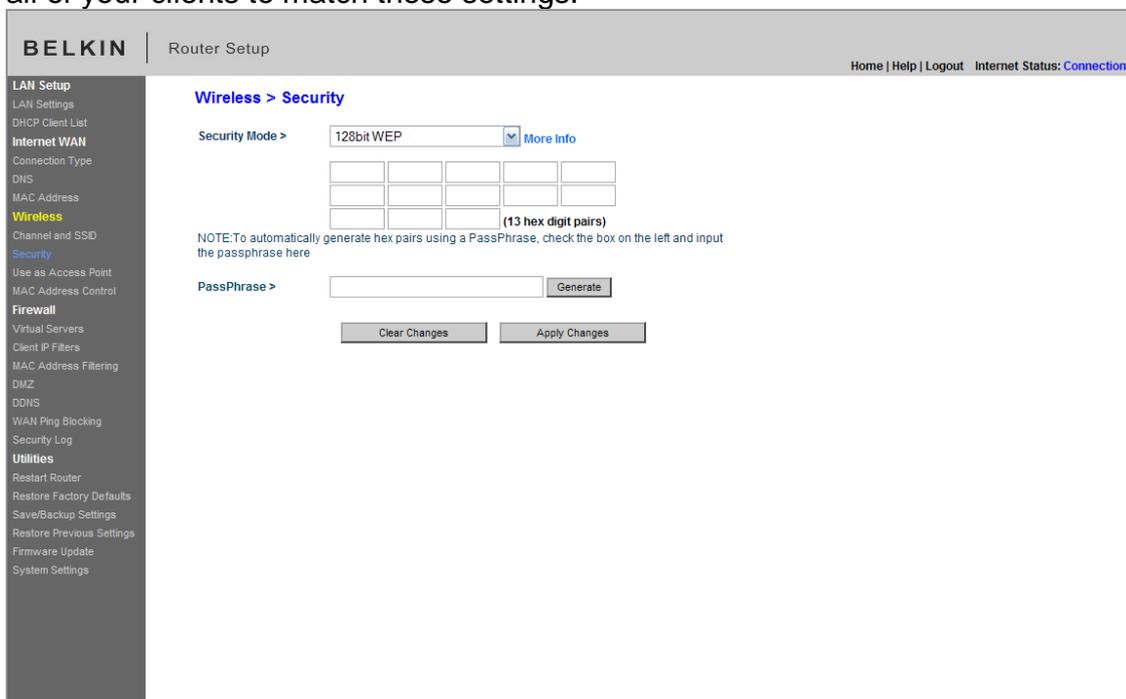
At the bottom of the settings area are two buttons: "Clear Changes" and "Apply Changes".

[FW18.tif]

Setting WEP Encryption

Note to Mac users: The “Passphrase” option will not operate with Apple® AirPort®. To configure encryption for your Mac computer, set the encryption using the manual method described in the next section.

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



The screenshot shows the Belkin Router Setup interface. The left sidebar contains a navigation menu with categories like LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled "Wireless > Security". Under "Security Mode >", a dropdown menu is set to "128bit WEP" with a "More Info" link. Below this is a grid of 13 empty boxes for entering hex pairs. A note states: "NOTE: To automatically generate hex pairs using a PassPhrase, check the box on the left and input the passphrase here". To the left of the note is a checkbox. Below the note is a "PassPhrase >" field with a "Generate" button. At the bottom are "Clear Changes" and "Apply Changes" buttons.

[FW19.tif]

3. Encryption in the Router is now set. Each of your computers on your wireless network will now need to be configured with the same passphrase. Refer to the documentation of your wireless network adapter for information on making this change.

Using a Hexadecimal Key

A hexadecimal key is a mixture of numbers and letters from A–F and 0–9. 64-bit keys are 10 digits long and can be divided into five two-digit numbers. 128-bit keys are 26 digits long and can be divided into 13 two-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. You will use this key to program the encryption settings on your Router and your wireless computers.

Example:

AF	IF	4B	C3	D4
----	----	----	----	----

64-bit:

--	--	--	--	--

128-bit:

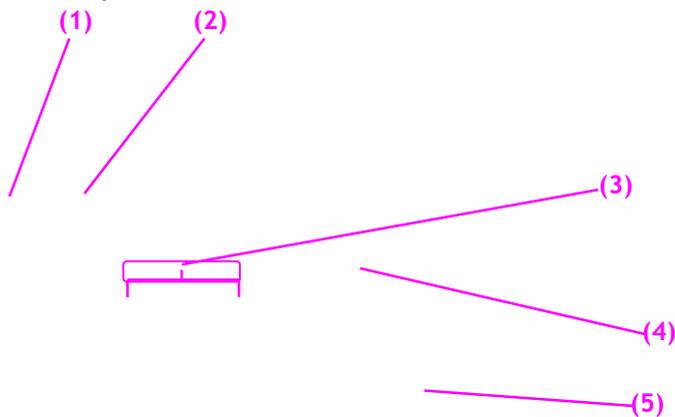
--	--	--	--	--	--	--	--	--	--	--	--	--

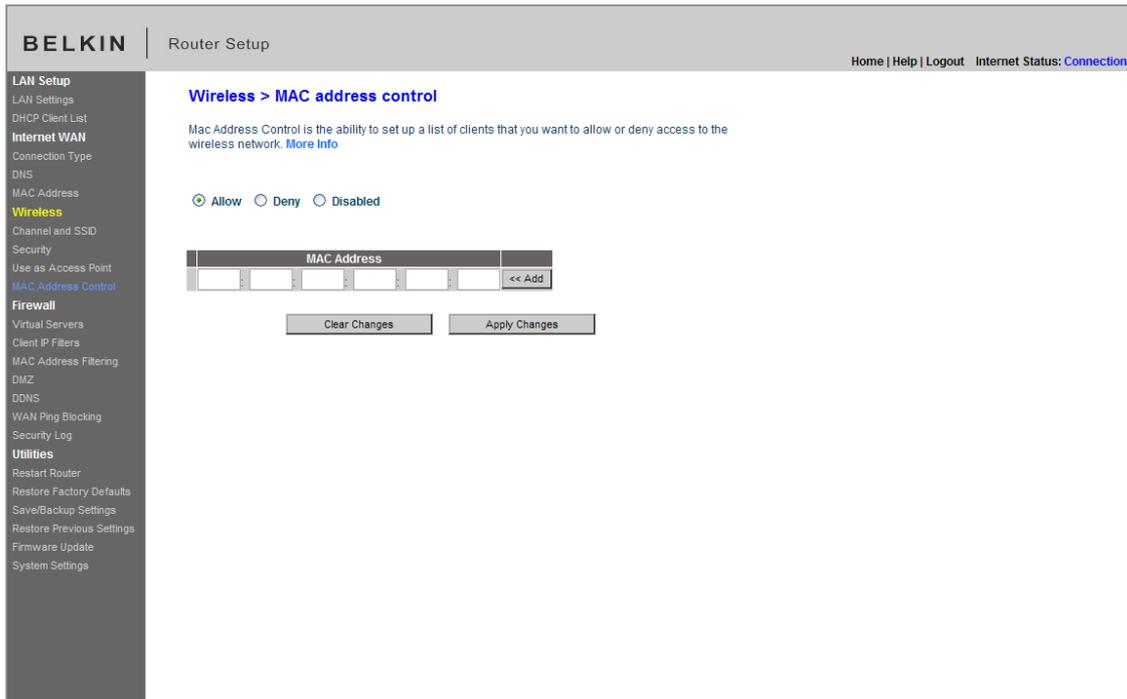
[\[encryption chart.tif\]](#)[\[use current image\]](#)Use the same image

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.

Setting MAC Address Control

The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the wireless network. **Note:** This list applies only to wireless computers. This list can be configured so any computer attempting to access the wireless 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) to which you want to allow network access. 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.





[FW20.tif]

Setting up an Allow Access List

1. Select the “Allow” radio button **(1)** to begin setting up a list of computers allowed to connect to the wireless network.
2. Next, in the “MAC Address” field that is blank **(2)**, type in the MAC address of the wireless computer you want to be able to access the wireless network, then click “<<Add” **(3)**.
3. Continue to do this until all of the computers you want to add have been entered.
4. Click “Apply Changes” **(4)** to finish.



[FW21.tif]

Setting up a Deny Access List

The “Deny Access” list lets you specify computers that you DO NOT want to access the network. Any computer in the list will not be allowed access to the wireless network. All others will.

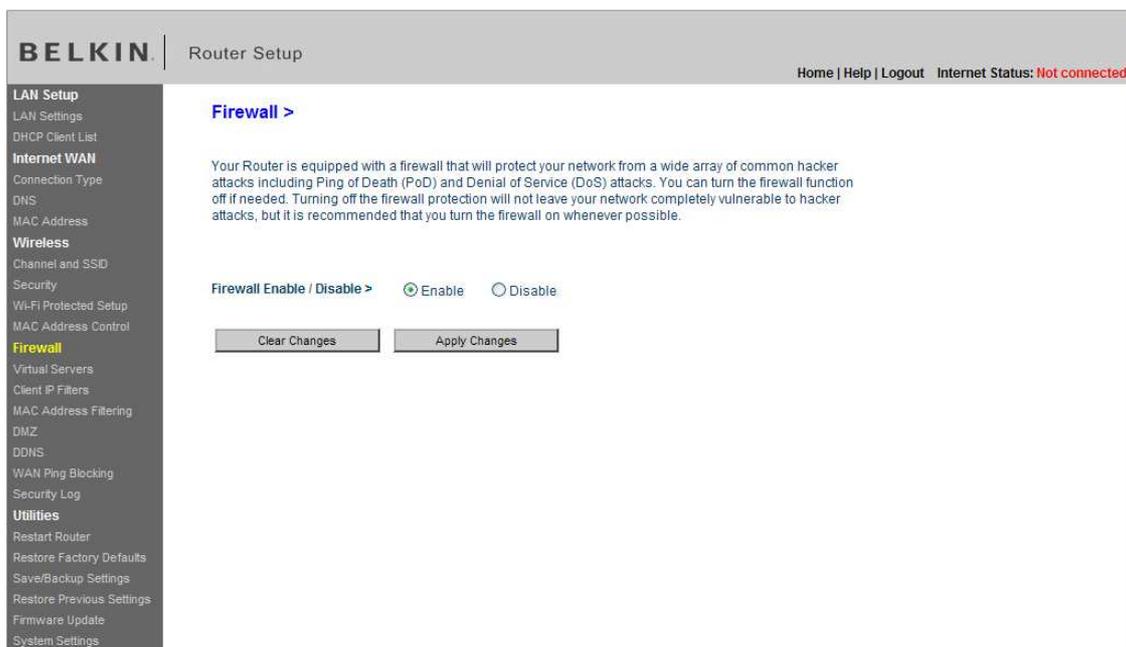
1. Select the “Deny” radio button **(1)** to begin setting up a list of computers to be denied access to the wireless network.
2. Next, in the “MAC Address” field that is blank **(2)**, type in the MAC address of the wireless computer you want to deny access to the wireless network, then click “<<Add” **(3)**.
3. Continue to do this until all of the computers you want to deny access to have been entered.
4. Click “Apply Changes” **(4)** to finish.

Configuring the 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 for all intents and purposes, 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.



The screenshot shows the Belkin Router Setup interface. The top navigation bar includes the Belkin logo, "Router Setup", and links for "Home | Help | Logout". The "Internet Status" is shown as "Not connected". A left sidebar lists various setup categories: LAN Setup, Internet WAN, Wireless, Firewall (highlighted), and Utilities. The main content area is titled "Firewall >" and contains the following text: "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." Below this text, there is a "Firewall Enable / Disable >" section with two radio buttons: "Enable" (which is selected) and "Disable". At the bottom of this section are two buttons: "Clear Changes" and "Apply Changes".

[FW22.tif]

Configuring Internal Forwarding Settings

The Virtual Servers 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, computers outside your network (over the Internet) cannot get to them because they cannot be “seen”. A list of common applications has been provided in case you need to configure the Virtual Server function for a specific application. If your application is not listed, you will need to contact the application vendor to find out which port settings you need.

The screenshot shows the Belkin Router Setup interface. The main content area is titled "Firewall > Virtual Servers". Below the title, there is a text box explaining the function: "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](#)".

Below the text box, there are two buttons: "Clear Changes" and "Apply Changes".

Below the buttons, there is a form with the following fields:

- "Add" button
- Drop-down menu: "Active Worlds"
- "Add" button
- "Clear" button
- "Clear entry" button
- Drop-down menu: "1"

Below the form, there is a table with 15 rows and 6 columns:

	Enable	Description	Inbound port	Type	Private IP address	Private port
1	<input type="checkbox"/>			TCP	192.168.2	
2	<input type="checkbox"/>			TCP	192.168.2	
3	<input type="checkbox"/>			TCP	192.168.2	
4	<input type="checkbox"/>			TCP	192.168.2	
5	<input type="checkbox"/>			TCP	192.168.2	
6	<input type="checkbox"/>			TCP	192.168.2	
7	<input type="checkbox"/>			TCP	192.168.2	
8	<input type="checkbox"/>			TCP	192.168.2	
9	<input type="checkbox"/>			TCP	192.168.2	
10	<input type="checkbox"/>			TCP	192.168.2	
11	<input type="checkbox"/>			TCP	192.168.2	
12	<input type="checkbox"/>			TCP	192.168.2	
13	<input type="checkbox"/>			TCP	192.168.2	
14	<input type="checkbox"/>			TCP	192.168.2	
15	<input type="checkbox"/>			TCP	192.168.2	

[FW23.tif]

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 (use a comma between multiple ports), select the port type (TCP or UDP), and click “Apply Changes”. 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.

Setting 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.

BELKIN Router Setup Home | Help | Logout Internet Status: **Connection**

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities
Restart Router
Restore Factory Defaults
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings

Firewall > Client IP filters

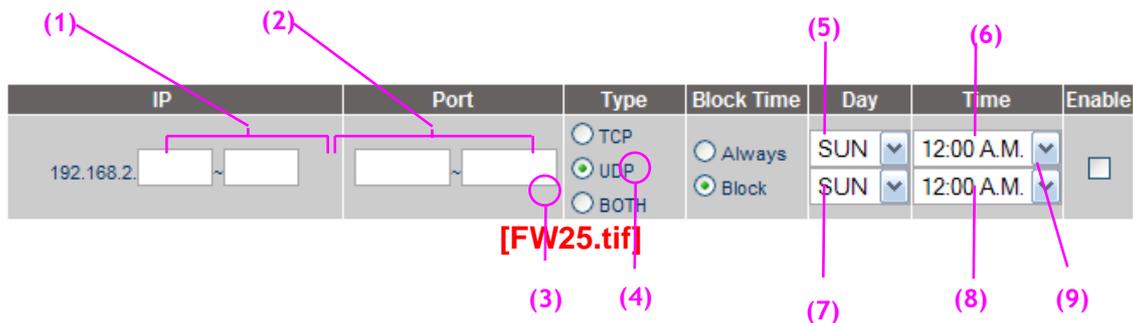
The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

IP	Port	Type	Block Time	Day	Time	Enable
192.168.2. []	[]	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN	12:00 A.M.	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN	12:00 A.M.	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN	12:00 A.M.	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN	12:00 A.M.	<input type="checkbox"/>
192.168.2. []	[]	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> BOTH	<input type="radio"/> Always <input checked="" type="radio"/> Block	SUN	12:00 A.M.	<input type="checkbox"/>

[FW24.tif]



To restrict Internet access to a single computer for example, enter the IP address of the computer you wish to restrict access to in the IP fields (1). Next, enter “80” in both the port fields (2). Select “Both” (3). Select “Block” (4). You can also select “Always” to block access all of the time. Select the day to start on top (5), the time to start on top (6), the day to end on the bottom (7), and the time to stop (8) on the bottom. Select “Enable” (9). Click “Apply Changes”. The computer at the IP address you specified will now be blocked from Internet access at the times you specified. **Note:** Be sure you have selected the correct time zone under “Utilities> System Settings> Time Zone”.



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.

Firewall > MAC address filtering

This feature lets you set up a list of allowed clients. When you enable this feature, you must enter the MAC address of each client on your network to allow network access to each. [More Info](#)

Enable MAC Address Filtering >

MAC Address Filtering List >

Block	Host	MAC Address	
<input type="checkbox"/>		[]	<< Add

Clear Changes Apply Changes

(FW26.tif)

To enable this feature, select “MAC Address Filtering” and click “Enable MAC Address Filtering” (1). Next, enter the MAC address of each computer on your network by clicking in the space provided (2) and entering the MAC address of the computer you want to add to the list. Click “Add” (3), then “Apply Changes” (4) to save the settings. You can have a MAC-address-filtering list of up to 32 computers.

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).

Enabling the Demilitarized Zone (DMZ)

The DMZ feature allows you to specify one computer on your network to be placed outside of the firewall. This may be necessary if the firewall 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.

[FW27.tif]

BELKIN Router Setup Home | Help | Logout | Internet Status: [Connection](#)

LAN Setup
LAN Settings
DHCP Client List

Internet WAN
Connection Type
DNS
MAC Address

Wireless
Channel and SSID
Security
Use as Access Point
MAC Address Control

Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log

Utilities
Restart Router
Restore Factory Defaults
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings

Firewall > DMZ

The DMZ feature allows you to specify one computer on your network to be placed outside of the NAT firewall. 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 IP address in the field below and select "Enable". Click "Apply Changes" for the change to take effect. [More Info](#)

IP Address of Virtual DMZ Host >

	Static IP	Private IP	Enable
1	69.226.88.206	192.168.2.0	<input type="checkbox"/>

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 which WAN IP address the DMZ host will be directed to. Type in the 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, select "Enable" and click "Apply Changes".

Using Dynamic DNS

The Dynamic DNS 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.

The Dynamic DNSSM 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!

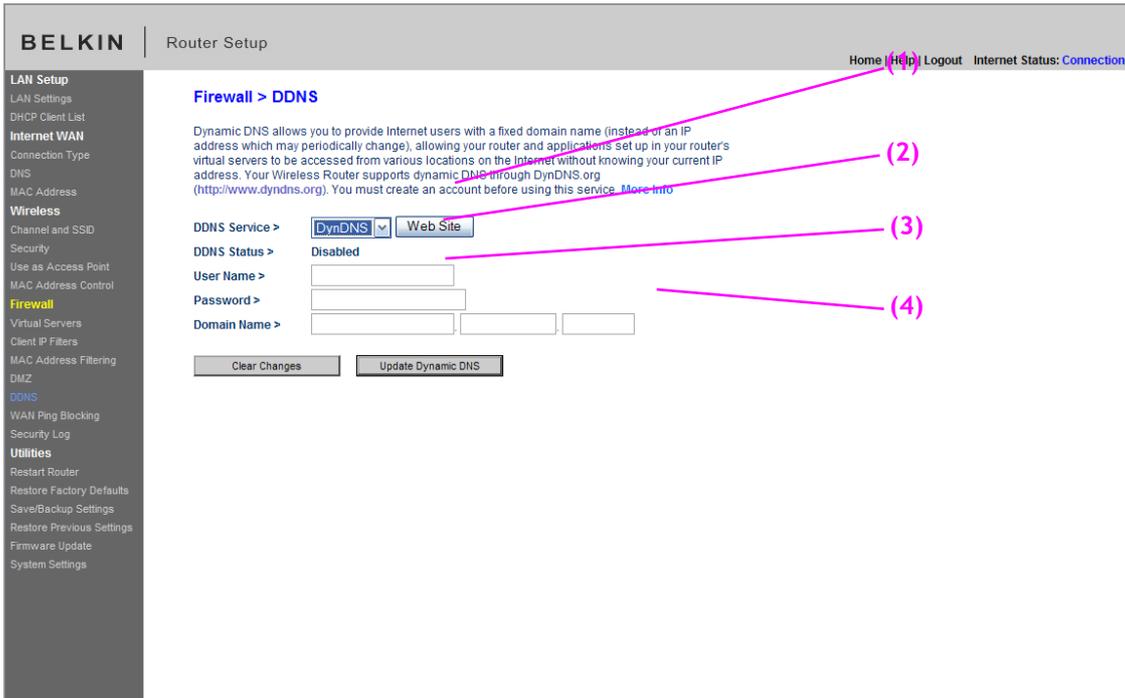
To register free for your Dynamic DNS host name, please visit <http://www.dyndns.org>.

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. Select DynDNS.org from the "DNS Service" drop-down box **(1)**.
2. Enter your DynDNS.org user name in the "User Name" field **(2)**.
3. Enter your DynDNS.org password in the "Password" field **(3)**.
4. Enter the DynDNS.org domain name you set up with DynDNS.org in the "Domain Name" field **(4)**.
5. Click "Update Dynamic DNS" to update your IP address **(5)**.

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 "Update Dynamic DNS" button **(5)**.

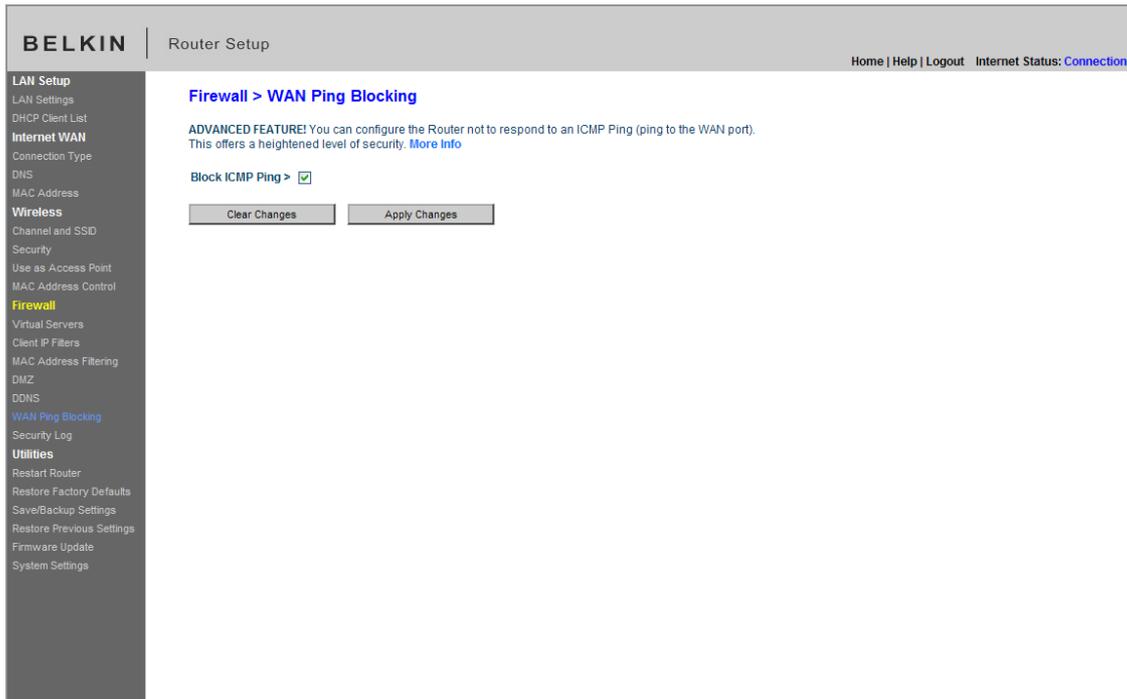


[FW28.tif]

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 your Router’s security level.

(1)



[Fw29.tif]

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.

The screenshot shows the Belkin Router Setup interface. The top navigation bar includes the Belkin logo, 'Router Setup', and links for Home, Help, Logout, and Internet Status (Connection). A left sidebar lists various setup categories: LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The Utilities section is expanded, showing options like Restart Router, Restore Factory Defaults, Save/Backup Current Settings, Restore Previous Saved Settings, Firmware Update, and System Settings. The main content area is titled 'Utilities >' and contains a descriptive paragraph and a list of utility functions with their respective descriptions.

[FW30.tif]

Restarting the 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.

This screenshot shows the 'Restart Router' page within the Belkin Router Setup interface. The top navigation bar is identical to the previous screenshot, but the Internet Status is now 'Not connected'. The left sidebar is also the same. The main content area is titled 'Utilities > Restart Router' and contains a paragraph explaining the purpose of the restart function. A prominent 'Restart Router' button is centered on the page.

[FW31.tif]

Restarting the Router to Restore Normal Operation

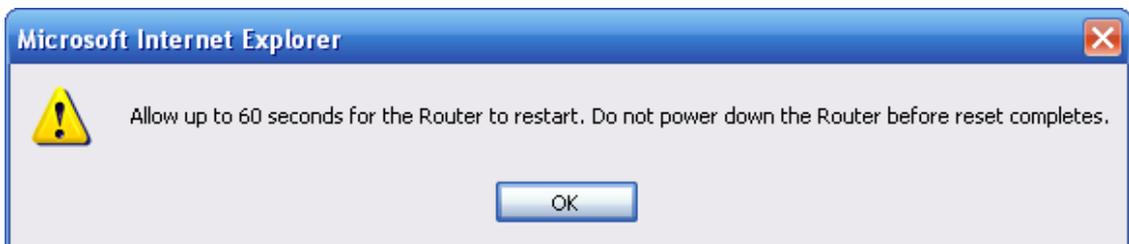
1. Click the "Restart Router" button.

2. The following message will appear. Click "OK".



[FW32.tif]

3. The following message will appear. Restarting the Router can take up to 60 seconds. It is important not to turn off the power to the Router during the restart.

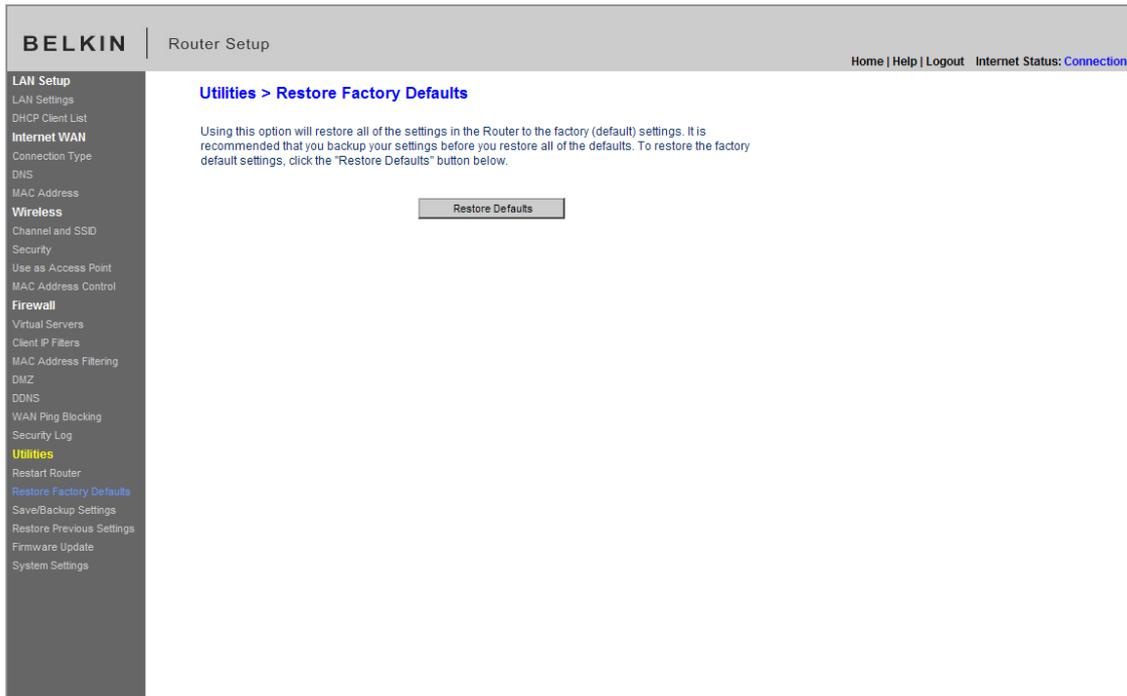


[FW33.tif]

4. A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router will be restarted. 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.

Restoring Factory Default Settings

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.



[FW34.tif]

1. Click the "Restore Defaults" button.
2. The following message will appear. Click "OK".



[FW35.tif]

3. The following message will appear. Restoring the defaults includes restarting the Router. It can take up to 60 seconds. It is important not to turn the power to the Router off during the restart.

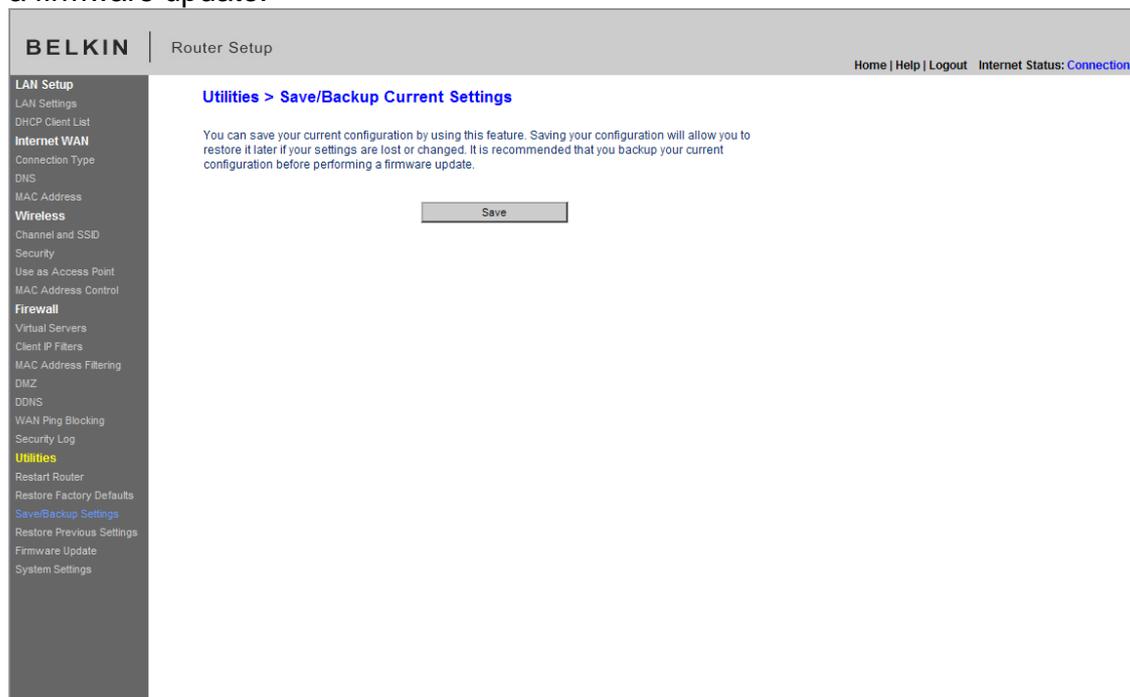


[FW36.tif]

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

Saving a Current Configuration

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.



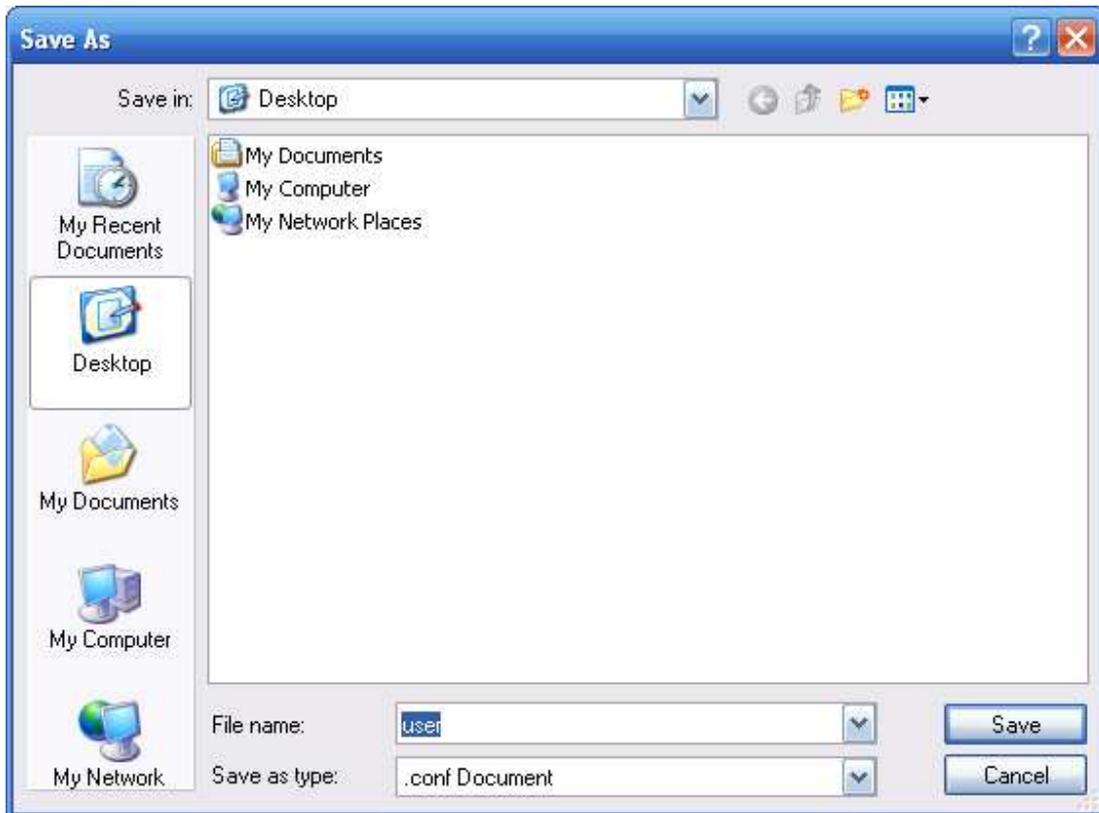
[FW37.tif]

1. Click "Save". A window called "File Download" will open. Click "Save".



[FW38.tif]

2. A window will open that allows you to select the location where you want to save the configuration file. Select a location. You can name the file anything you want, or use the default name “user.conf”. Be sure to name the file so you can locate it yourself later. When you have selected the location and name of the file, click “Save”.



[FW39.tif]

3. When the save is complete, you will see the window below. Click "Close".



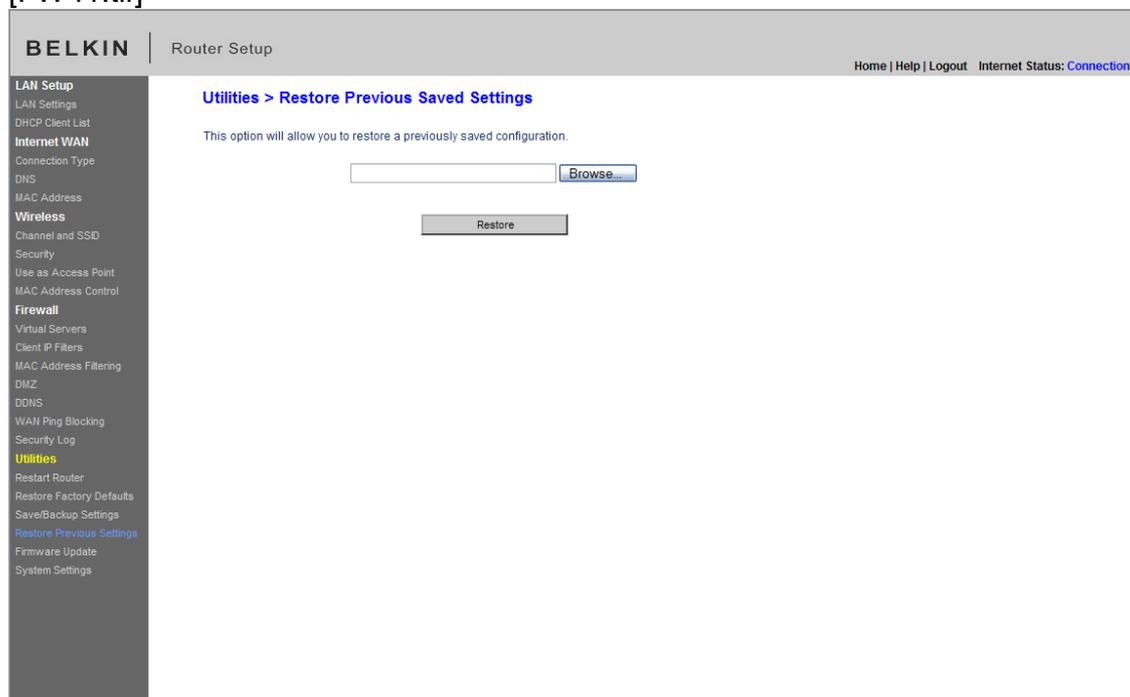
[FW40.tif]

4. The configuration is now saved.

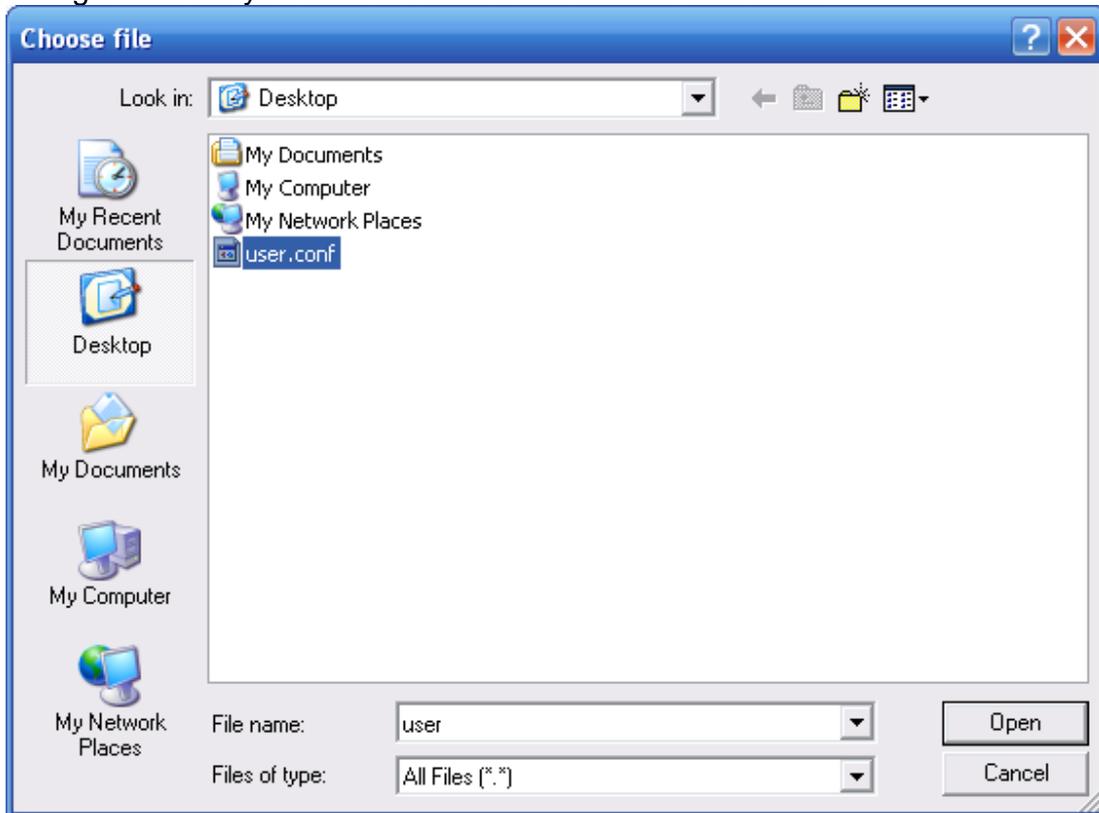
Restoring a Previous Configuration

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

[FW41.tif]



1. Click “Browse”. A window will open that allows you to select the location of the configuration file. All configuration files end with a “.conf”. Locate the configuration file you want to restore and double-click on it.



[FW42.tif]

2. You will be asked if you want to continue. Click “OK”.



[FW43.tif]

3. A reminder window will appear. It will take up to 60 seconds for the configuration restoration to complete. Click “OK”.

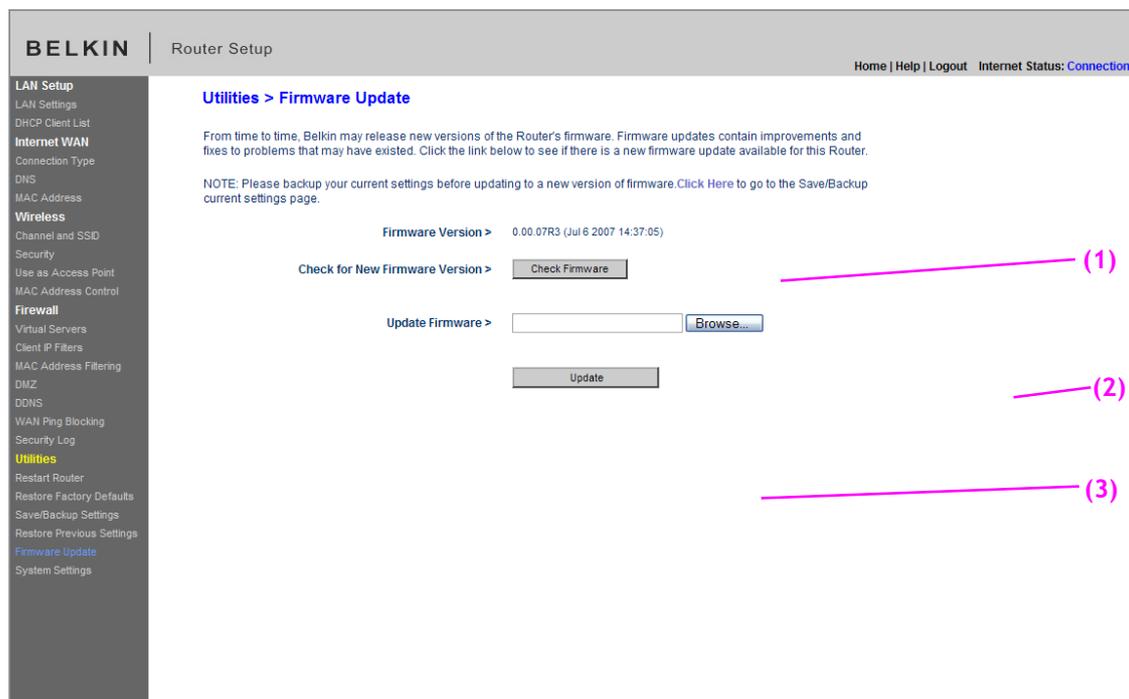


[FW44.tif]

4. A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router's configuration will be restored. The Router's 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.

Updating the 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 update website and update your Router's firmware to the latest version.



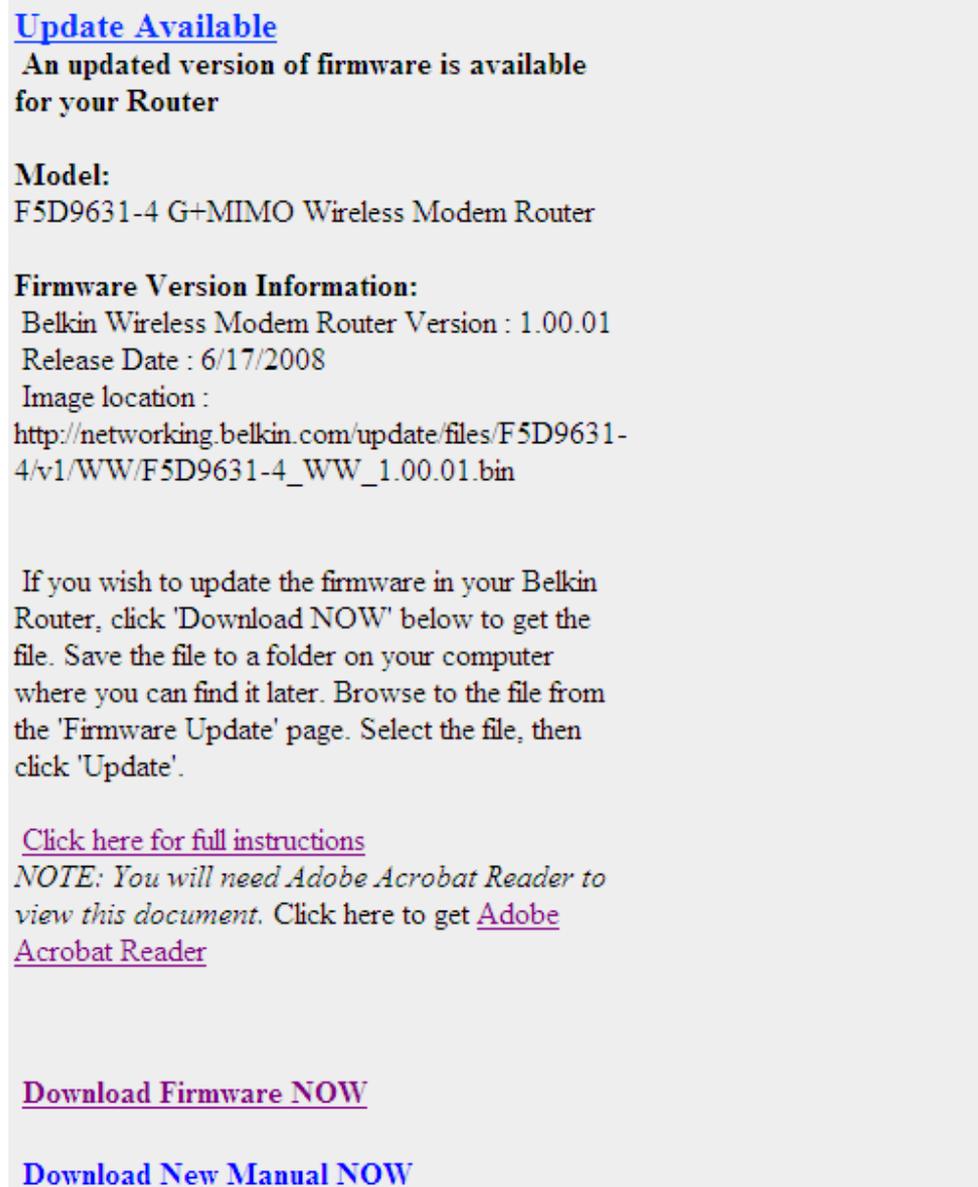
[FW45.tif]

Checking for a New Version of Firmware

The “Check Firmware” **(1)** 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:



[Update Available](#)
An updated version of firmware is available for your Router

Model:
F5D9631-4 G+MIMO Wireless Modem Router

Firmware Version Information:
Belkin Wireless Modem Router Version : 1.00.01
Release Date : 6/17/2008
Image location :
http://networking.belkin.com/update/files/F5D9631-4/v1/WW/F5D9631-4_WW_1.00.01.bin

If you wish to update the firmware in your Belkin Router, click 'Download NOW' below to get the file. Save the file to a folder on your computer where you can find it later. Browse to the file from the 'Firmware Update' page. Select the file, then click 'Update'.

[Click here for full instructions](#)
NOTE: You will need Adobe Acrobat Reader to view this document. Click here to get [Adobe Acrobat Reader](#)

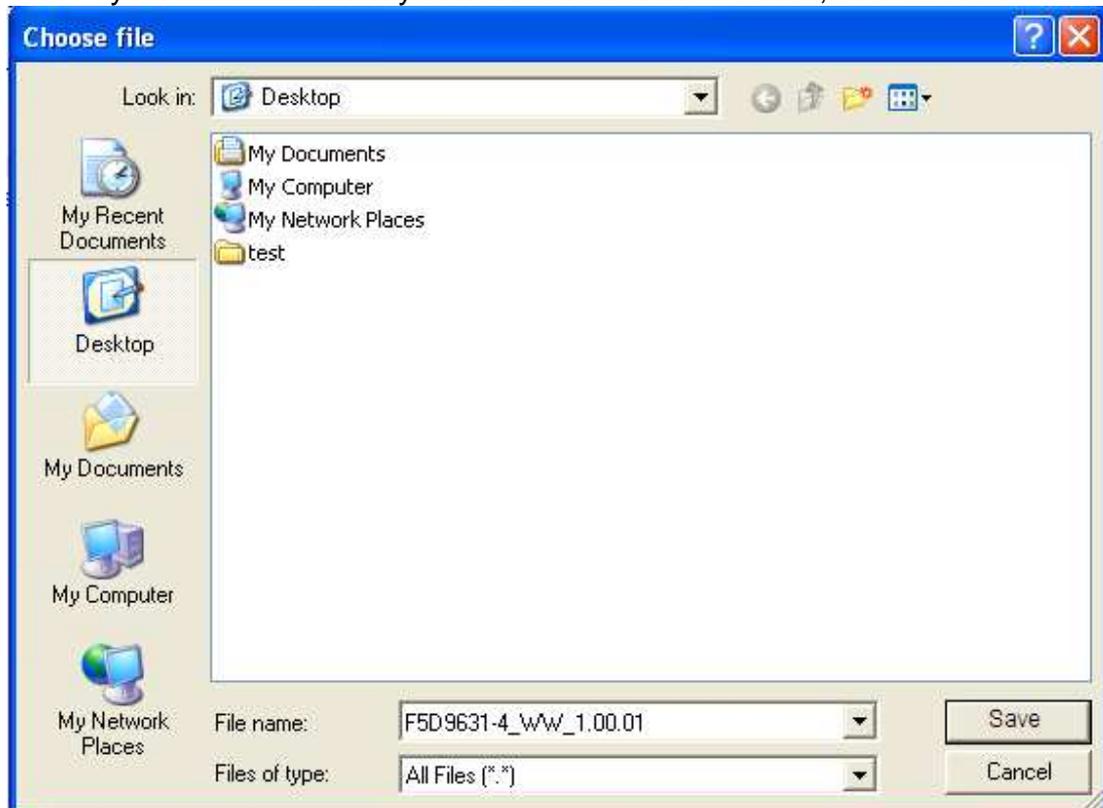
[Download Firmware NOW](#)

[Download New Manual NOW](#)

[FWUP05.tif]

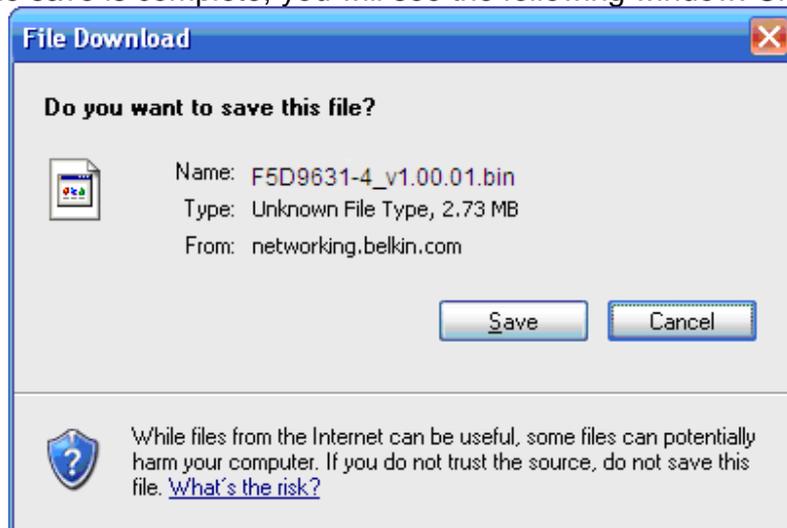
1. To download the new version of firmware, click “Download”.

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”.



[FWUP06.tif]

2. When the save is complete, you will see the following window. Click “Close”.

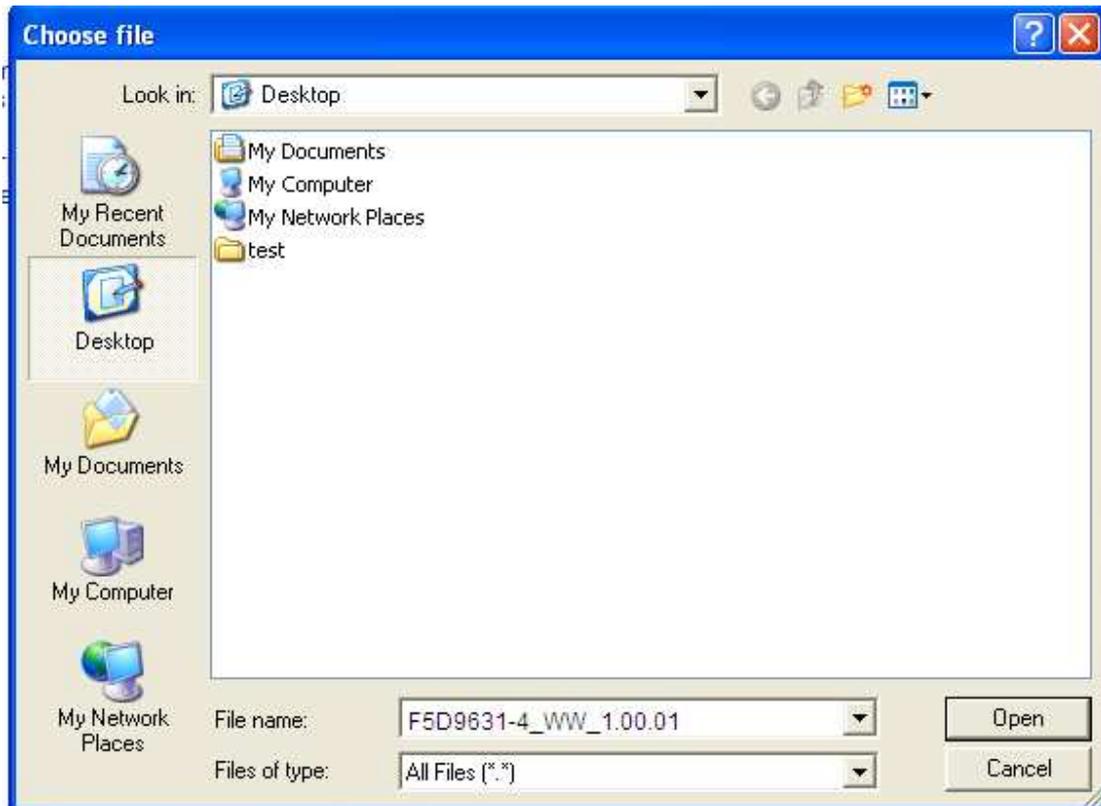


[FWUP07.tif]

3. 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

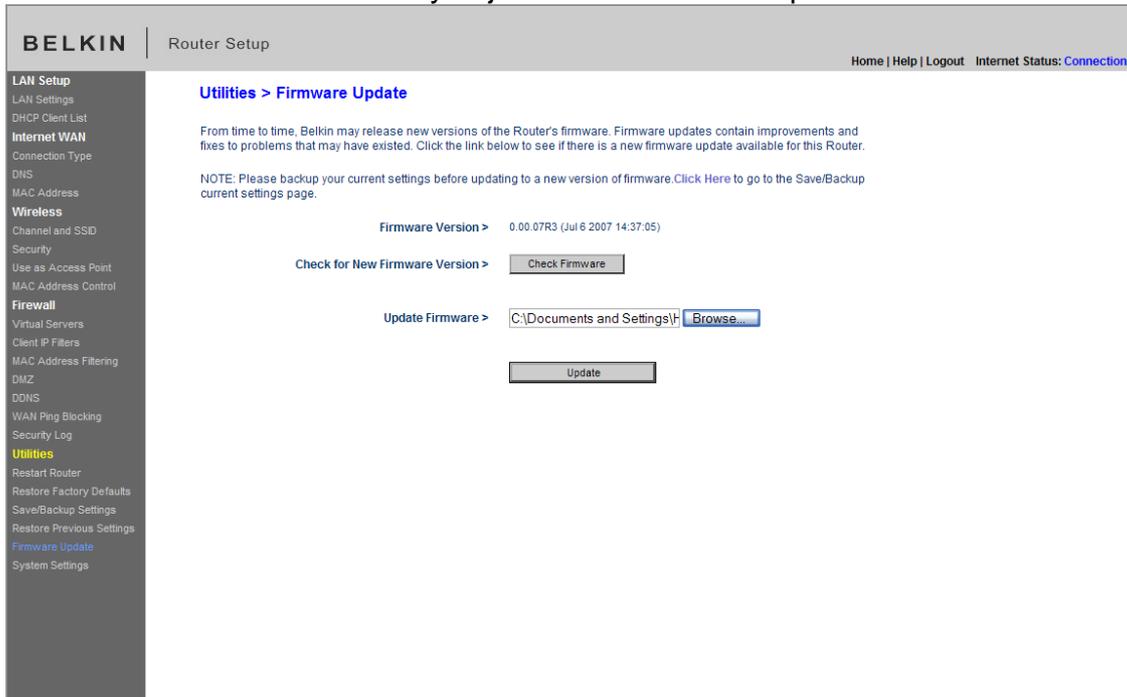
1. In the “Firmware Update” page, click “Browse”. A window will open that allows you to select the location of the firmware update file.



[FWUP08.tif]

2. Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.

The “Update Firmware” box will now display the location and name of the firmware file you just selected. Click “Update”.



[FW46.tif]

3. You will be asked if you are sure you want to continue. Click “OK”.



[FW47.tif]

4. 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”.



[FW48.tif]

5. 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.

Changing 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.

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 into 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](#)

- Type in current Password >	<input type="text"/>
- Type in new Password >	<input type="text"/>
- Confirm new Password >	<input type="text"/>
- Login Timeout >	<input type="text" value="10"/> (1-99 minutes)

[FW49.tif]

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, imagine 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, 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 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 that you reside in. You have the option to select a primary and a backup NTP server to keep your Router's clock synchronized. Select your desired NTP server from the drop-down box, or simply keep it as is.

If you reside in an area that observes daylight saving, 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.

Time and Time Zone: **June 26, 2008 2:58:56 PM**

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

- Time Zone > (GMT) Greenwich Mean Time: Lisbon, London ▼

- Daylight Savings > Automatically Adjust Daylight Saving

- Primary NTP Server > 129.132.2.21-Europe ▼

- Backup NTP Server > 130.149.17.8-Europe ▼

[FW49.tif]

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 you know you will be accessing the Router from 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.

Advanced Feature: The “Remote Access Port” option allows you to configure the desired “Remote Access Port for Remote Management” feature. The default access port is set to port 8080.

Remote Management:

ADVANCED FEATURE! Remote management allows you to make changes to your Router's settings from anywhere on the Internet. Before you enable this function, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD.** [More Info](#)

Any IP address can remotely manage the router.

- Only this IP address can remotely manage the router >

 . . .

- Remote Access Port >

[FW49.tif]

Enabling/Disabling UPnP

UPnP (Universal Plug-and-Play) 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. [More Info](#)

- UPNP Enable / Disable >

Enable Disable

[FW49.tif]

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 advanced 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.

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

Clear Changes

Apply Changes

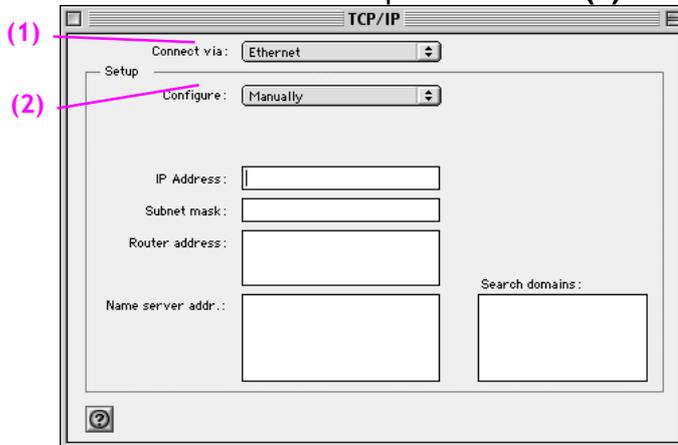
[FW49.tif]

Manually Configuring Network Settings

Set up the computer that is connected to the cable or DSL 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 Settings in Mac OS up to 9.x

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)**.



[xxxxxxx][use current image]

[keep]

3. Next to "Configure" **(2)**, 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"/>
Router Address:	<input type="text"/>
Name Server Address:	<input type="text"/>

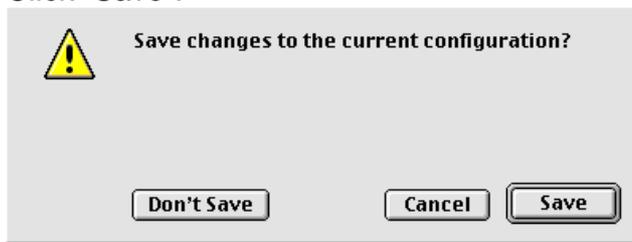
[MacOS9 chart.tif] [use current image] [keep]

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



[xxxxxxx] [use current image] [keep]

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



[xxxxxxx] [use current image] [keep]

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

Manually Configuring Network Settings in Mac OS X

1. Click on the “System Preferences” icon.



[xxxxxxx] [use current image] [keep]

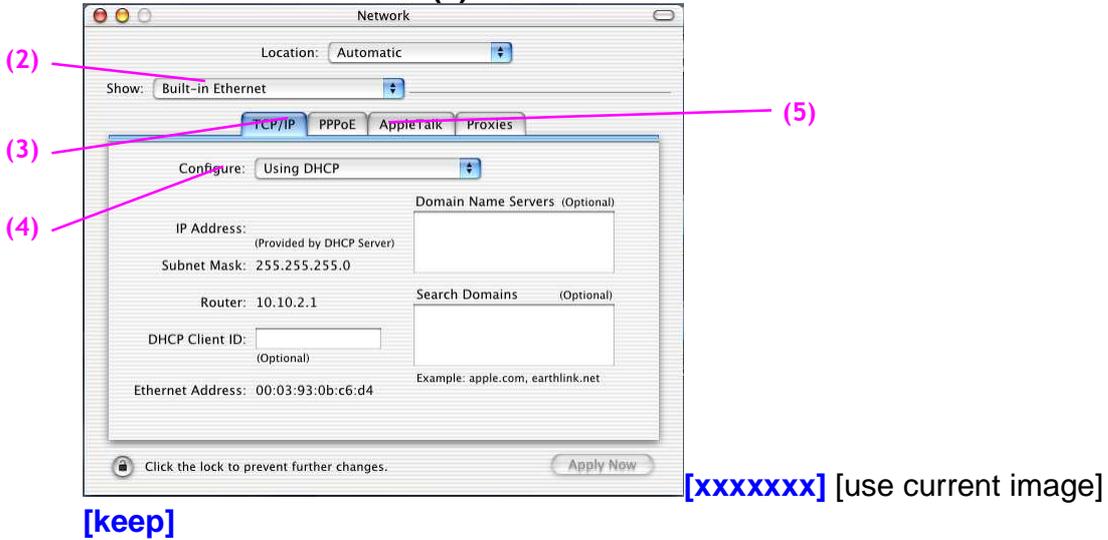
2. Select “Network” (1) from the “System Preferences” menu.



[xxxxxxx] [use current image]

[keep]

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.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Router Address:	<input type="text"/>
Name Server Address:	<input type="text"/>

[MacOS9 chart.tif] [use current image] [keep]

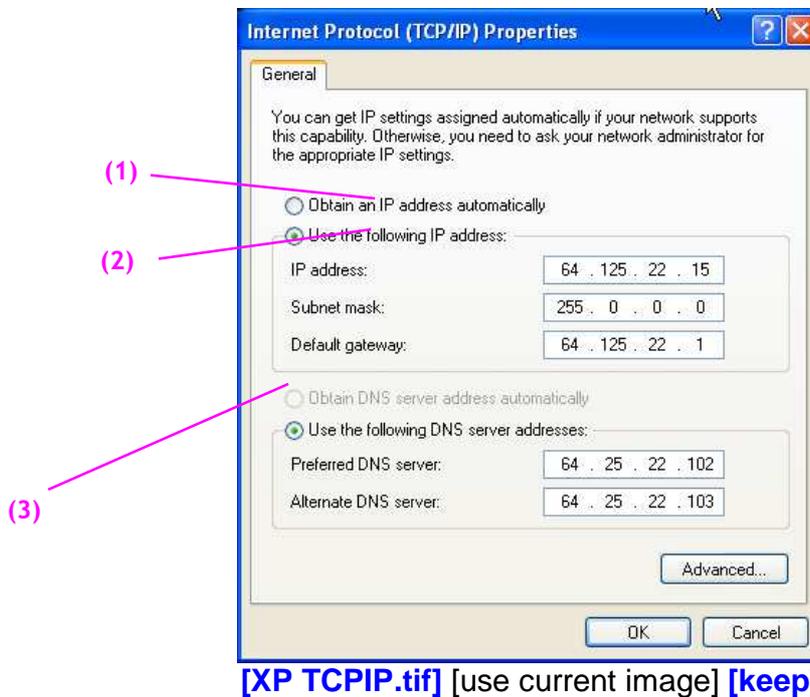
6. If not already selected, select "Using DHCP" next to "Configure" (4), then click "Apply Now".

Your network settings are now configured for use with the Router.

Manually Configuring Network Settings in Windows 2000, NT, or XP

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) is selected, your Router will need to be set up for a static IP connection type. Write the address information 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"/>

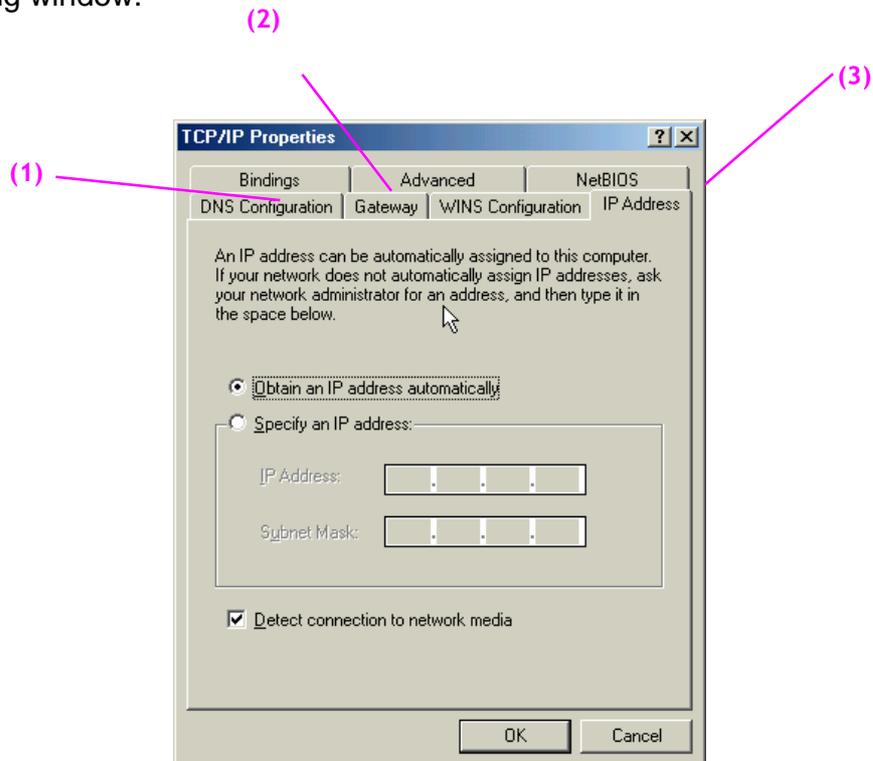
[win2k settings chart.tif] [use current image] [keep]

6. If not already selected, select “Obtain an IP address automatically” (1) and “Obtain DNS server address automatically” (3). Click “OK”.

Your network settings are now configured for use with the Router.

Manually Configuring Network Settings in Windows 98 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.



[98 Me IP properties.tif] [use current image] [keep]

3. If “Specify and 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 the IP address and subnet mask from the “IP Address” tab **(3)**.
5. Click the “Gateway” tab **(2)**. Write the gateway address down in the chart.
6. Click the “DNS Configuration” tab **(1)**. Write the DNS address(es) in the chart.

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"/>

[\[win2k settings chart.tif\]](#) [\[keep\]](#)

[use current image]

7. If not already selected, select "Obtain IP address automatically" on the IP address tab. Click "OK".

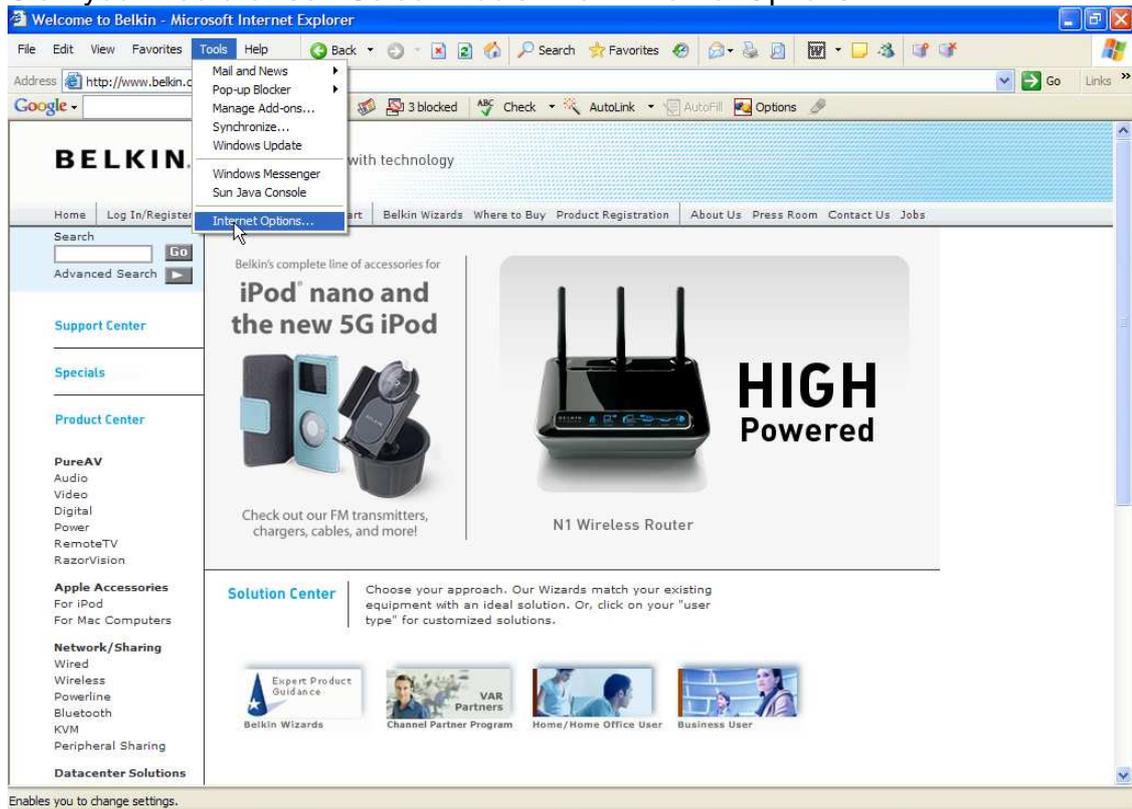
Restart the computer. When the computer restarts, your network settings are now configured for use with the Router.

Recommended Web Browser Settings

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".



Enables you to change settings.
[insert Internet_options.tif]

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.

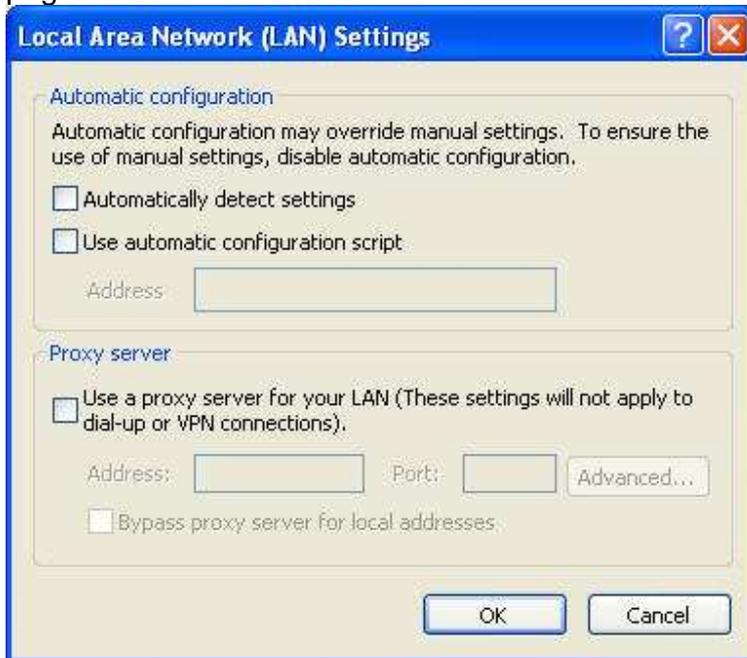


[IE6_Internet_Option

ns_Connections.jpg

3. Under the "Internet Options" screen, click on "Connections" and select "LAN Settings...".

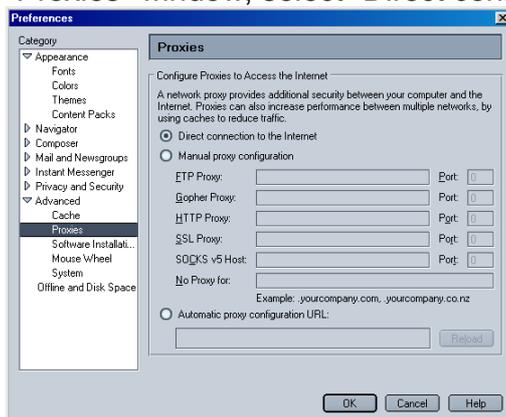
4. Make sure there are no check marks next to any of the displayed options: “Automatically detect settings”, “Use automatic configuration script”, and “Use a proxy server”. Click “OK”. Then click “OK” again in the “Internet Options” page.



[IE6_Internet_Options_Connections_LAN_Settings.jpg]

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”.



[NS6 Setup 1.tif]

Troubleshooting

Problem:

Installation CD does not automatically start.

Solution:

If the CD-ROM does not start the Setup Assistant automatically, it could be that the computer is running other applications that are interfering with the CD drive.

1. If the Setup Assistant screen does not appear within 15–20 seconds, open up your CD-ROM drive by double-clicking on the “My Computer” icon that is located on your desktop.



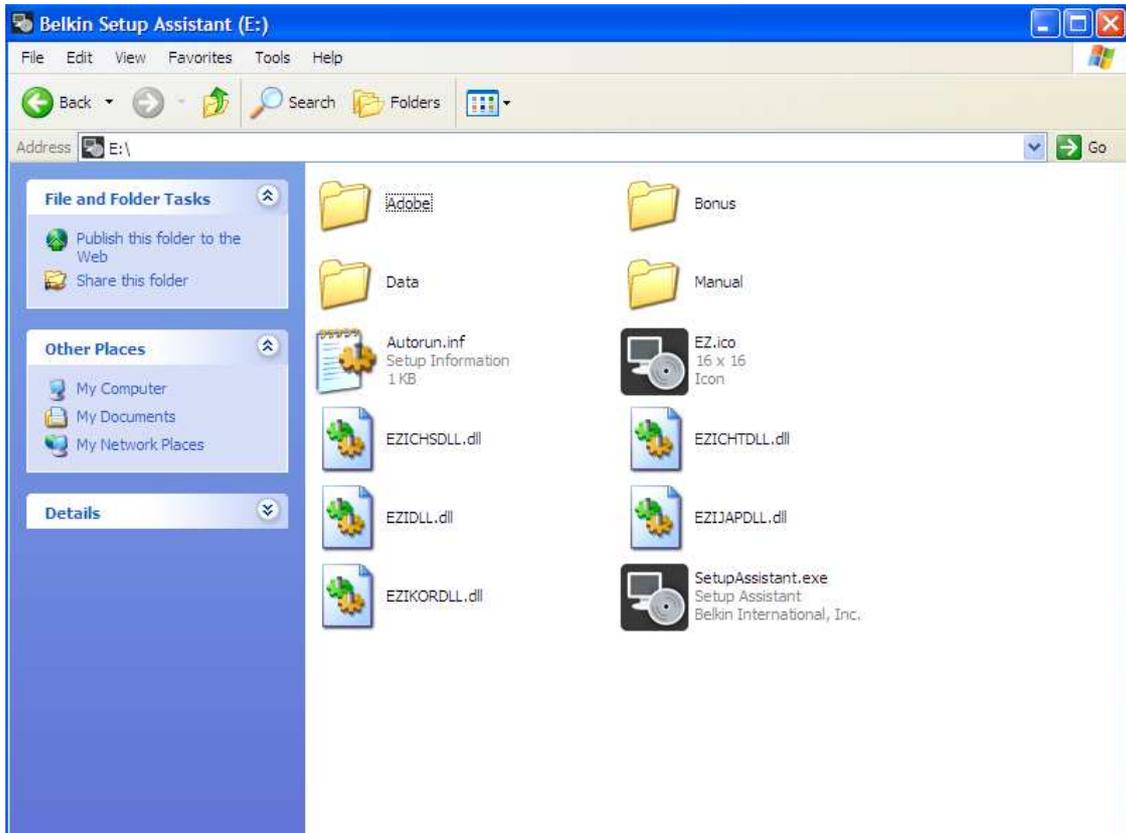
2. Next, double-click on the CD-ROM drive that the Setup Assistant Software CD has been placed in to start the installation.

[encircle on “Belkin Setup Assistant” icon.]



3. The Setup Assistant should start within a few seconds. If, instead, a window appears showing the files on the CD, double-click on the icon labeled “SetupAssistant.exe”.

[encircle on “SetupAssistant.exe” icon.]



4. If the Setup Assistant still does not start, reference the section titled "Manually Configuring Network Settings" (page 86 of this User Manual)(verify the page #) for an alternate setup method.

Problem:

The Setup Assistant cannot find my Router.

Solution:

If the Setup Assistant is not able to find the Router during the installation process, please check the following items:

1. If the Setup Assistant is not able to find the Router during the installation process, there may be third-party firewall software installed on the computer attempting to access the Internet. Examples of third-party firewall software are ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, and Norton Personal Firewall.

If you do have firewall software installed on your computer, please make sure that you properly configure it. You can determine if the firewall software is preventing Internet access by temporarily turning it off. If, while the firewall is disabled, Internet access works properly, you will need to change the firewall settings to function properly when it is turned on.

Please refer to the instructions provided by the publisher of your firewall software for instructions on configuring the firewall to allow Internet access.

2. Unplug power to the Router for 10 seconds, and then plug the power back into the Router. Ensure that the Router's Power light is on; it should be solid green. If not, check to make sure that the AC adapter is correctly connected to the Router and plugged into a wall outlet.
3. Ensure that you have a cable (use the cable included with the Router) connected between (1) the network (Ethernet) port on the back of the computer and (2) one of the LAN ports, labeled "1" through "4", on the back of the Router.

Note: The computer should NOT be connected to the port labeled "Modem" on the back of the Router.
4. Try shutting down and restarting your computer, then rerunning the Setup Assistant.

If the Setup Assistant is still unable to find the Router, reference the section titled "Manually Configuring Network Settings" for installation steps.

Problem:

The Setup Assistant cannot connect my Router to the Internet.

Solution:

If the Setup Assistant is not able to connect the Router to the Internet, please check the following items:

1. Use the troubleshooting suggestions within the Setup Assistant. If the troubleshooting screen does not open automatically, click on the "Troubleshoot" button in the lower, right-hand corner of the Setup Assistant window.
2. If your ISP requires a user name and password, make sure that you have typed in your user name and password correctly. Some user names require that the ISP's domain be at the end of the name. Example: "myname@myisp.com". The "@myisp.com" part of the user name may need to be typed as well as your user name.

If you continue to have no Internet connection, reference the section titled "Manually Configuring Network Settings" (page 86 of this User Manual)(verify the page #) for alternate setup method.

Problem:

- The Setup Assistant completed installation, but my web browser doesn't work.
- I am unable to connect to the Internet. The Router's "Internet" light is off and the "Modem" light is blinking.

Solution:

If you cannot connect to the Internet, the "Internet" light is off, and the "Modem" light is blinking, the problem may be that your modem and Router are not connected properly.

1. Make sure the network cable between the modem and the Router is connected. We strongly recommend using the cable that was supplied with your cable or DSL modem for this purpose. The cable should be connected at one end to the Router's "Modem" port, and at the other end to the network port on your modem.
2. Unplug the cable or DSL modem from its power source for three minutes. After three minutes, plug the modem back into its power source. This may force the modem to properly recognize the Router.
3. Unplug the power to your Router, wait 10 seconds, and then reconnect the power. This will cause the Router to reattempt communication with the modem.

If the "Modem" light on the Router is not lit after completing these steps, please contact Belkin Technical Support.

4. Try shutting down and restarting your computer.

Problem:

- The Setup Assistant completed installation, but my web browser doesn't work.
- I am unable to connect to the Internet. The Router's "Modem" light is on and the "Internet" light is blinking.

Solution:

If you cannot connect to the Internet, the "Modem" light is on, and the "Internet" light is blinking, the problem may be that your connection type may not match the ISP's connection.

- If you have a "static IP address" connection, your ISP must assign you the IP address, subnet mask, and gateway address. Please refer to the section entitled "Alternate Setup Method" for details on changing this setting.
- If you have a "PPPoE" connection, your ISP will assign you a user name and password and sometimes a service name. Make sure the Router connection type is configured to PPPoE and the settings are entered properly. Please refer to the section entitled "Alternate Setup Method" for details on changing this setting.
- You may need to configure your Router to meet the specific requirements of your ISP. To search our Knowledge Base for ISP-specific issues, go to: <http://web.belkin.com/support> and type in "ISP"

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

Problem:

- The Setup Assistant completed, but my web browser doesn't work.
- I am unable to connect to the Internet. The "Modem" light on my Router is blinking and the "Internet" light is solid.

Solution:

If the “Modem” light is blinking and the “Internet” light is solid, but you are unable to access the Internet, there may be third-party firewall software installed on the computer attempting to access the Internet. Examples of third-party firewall software are ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, and Norton Personal Firewall.

If you do have firewall software installed on your computer, please make sure that you properly configure it. You can determine if the firewall software is preventing Internet access by temporarily turning it off. If, while the firewall is disabled and Internet access works properly, you will need to change the firewall settings to function properly when it is turned on.

Please refer to the instructions provided by the publisher of your firewall software for instructions on configuring the firewall to allow Internet access.

If you are still unable to access the Internet after disabling any firewall software, please contact Belkin Technical Support.

Problem:

I can't connect to the Internet wirelessly.

Solution:

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

1. Look at the lights on your Router. Your Belkin Router's lights should be as follows:
 - The “Power” light should be on.
 - The “Internet” light should be on and not blinking.
 - The “Modem” 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 are also using a Belkin Wireless Card or Adapter with this Router, the tray icon should look like this



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.
2. If the network has security (encryption) enabled, you will need to enter the network key. For more information regarding security, see the section entitled “Securing your Wi-Fi Network” in this User Manual.
3. 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 configuration utility, please attempt the following troubleshooting steps:

1. Temporarily move your computer, if possible, five to 10 feet away from the Router. Close the wireless configuration utility, and reopen 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 the section titled “Placement of your Router for Optimal Performance” in this User Manual.
2. Using a computer that is connected to the Router through 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.

I am having 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 away 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 away 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 titled "Changing the Wireless Channel" on page 48 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 G Wireless Router, and is 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 G Range Extender/Access Point that can be connected wirelessly to a Belkin G 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 (F5D7130)
Powerline Ethernet Adapter (F5D4070)
Powerline USB Adapter (F5D4050)

Problem:

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

Solution:

1. Log into your Wireless Router or Access Point.

Open your web browser and type in the IP address of the Wireless Router or Access Point. (The Router's default is 192.168.2.1, the Access Point's default 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".

Click the "Wireless" tab on the left of your screen. Select the "Encryption" or "Security" tab to get to the security settings page.

2. Select "128-bit WEP" from the drop-down menu.
3. 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 combination 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

4. 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.

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 client card (Wireless Network Card or Adapter).

Solution:

The client card must use the same key as the G Wireless Router or access point. For instance, if your Wireless Router or access point uses the key 00112233445566778899AABBCC, then the client card must be set to the exact same key.

1. Double-click the "Signal Indicator" icon to bring up the "Wireless Network Utility" screen. The "Advanced" button will allow you to view and configure more options of your client card.
2. 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 client card.
3. Under the "Wireless Network Properties" tab, select a network name from the "Available Networks" list and click the "Properties" button.
4. Under "Data Encryption", select "WEP".
5. Ensure the 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.
6. Type your WEP key in the "Network key" box.

Important: A WEP key is a combination of numbers and letters from A–F and 0–7. For 128-bit WEP, you need to enter 26 keys. This network key needs to match the key you assign to your G Wireless Router or access point.

For example: C3030FAF4BB2C3D44BC3D4E7E4 = 128-bit key

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

If you are NOT using a Belkin wireless client card, please consult the manufacturer's user manual for that wireless client card.

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 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>

[keep hyperlink since this will be on CD]

You also need to download the latest driver for your Belkin Wireless 802.11g Desktop 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://web.belkin.com/support>

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".
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. This can be from eight to 63 characters and can be letters, numbers, 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 client card (Wireless Network Card or Adapter) for a home network.

Solution:

Clients must use the same key that the G Wireless Router or access point uses. For instance, if the key is "Smith Family Network Key" in the G 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 Utility" screen. The "Advanced" button will allow you to view and configure more options of your client card.

2. 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 client card.

3. Under the "Wireless Network Properties" tab, select a network name from the "Available Networks" list and click the "Properties" button.

4. Under "Network Authentication", select "WPA-PSK".
5. Type your WPA key in the "Network key" box.

Important: WPA-PSK is a combination 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 G Wireless Router or access point.

6. Click "OK", then "Apply" to save the settings.

Problem:

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

Solution:

1. Double-click the "Signal Indicator" icon to bring up the "Wireless Network Utility" screen. The "Advanced" button will allow you to view and configure more options of your client card.

2. 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 client card.

3. Under the "Wireless Network Properties" tab, select a network name from the "Available Networks" list and click the "Properties" button.

4. Under "Network Authentication", select "WPA".

5. In the "Authentication" tab, select the settings that are indicated by your network administrator.

6. 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 client card for a home network.

Solution:

If you are NOT using a Belkin WPA Wireless Desktop or Wireless Notebook Network Card and it 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:

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

[keep hyperlink since this is on CD]

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

1. In systems running Windows XP, click “Start > Control Panel > Network Connections”.
2. Right-click on the “Wireless Networks” tab. The “Wireless Network Connection Properties” screen appears. Ensure the “Use Windows to configure my wireless network settings” box is checked.
3. Under the “Wireless Networks” tab, click the “Configure” button, and you will see the client card properties screen.
4. For a home or small business user, select “WPA-PSK” under “Network Administration”.
 5. Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the G Wireless Router or access point that you set up.
6. 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.
7. Click “OK” to apply settings.

What’s the difference between 802.11b, 802.11g, 802.11a, and draft 802.11n?

Currently there are four levels of wireless networking standards, which transmit data at very different maximum speeds. Each is based on the designation for certifying network standards. The most common wireless networking standard, 802.11b, transmits information at 11Mbps; 802.11a and 802.11g work at 54Mbps; and draft 802.11n works at 300Mbps. See the following chart for more detailed information.

Wireless Comparison Chart [Use same chart as 8233]

Wireless	G	G Plus	N MIMO	N1 MIMO
----------	---	--------	--------	---------

Technology	(802.11g)	MIMO (802.11g with MIMO MRC)	(draft 802.11n with MIMO)	(draft 802.11n with MIMO)
Speed*	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.

Technical Support

You can find technical-support information on our website, www.belkin.com, by navigating to the tech-support section.

If you want to contact technical support by phone, please call the number you need from the list below*:

*Local rates apply.

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

Information

FCC Statement

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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into 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.

This device 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2.4GHz operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

FCC PART68 STATEMENT

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: BKCDL01BF5D9631A. If requested, this number must be provided to the telephone company.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:

BKCDL01BF5D9631A. The digits represented by 01 are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Contact information in the USA

COMPANY: Belkin International, Inc.

ADDRESS: 501 West Walnut Street, Compton, CA 90220-5221, USA

TEL NO: 1-310-604-2448

CONTACT PERSON: Candy Campbell

Add CE statement to below.

[This device can be operated in the EU without restrictions indoor.](#)

[However, operated outdoors in France is restricted to 2400 ~ 2454 MHz \(Channel 1 ~ 7\).](#)

Belkin International, Inc., Limited Lifetime Product Warranty

What this warranty covers.

Belkin International, Inc. ("Belkin") 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 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 for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin 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 Tech Support at the number listed on page 99 **[Need to verify this page #]**, 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 reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin 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, 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 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, 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 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.

Belkin Tech Support

US: 877-736-5771
800-223-5546 ext. 2263310-898-1100 ext. 2263
UK: 0845 607 77 87
Australia: 1800 235 546
New Zealand: 0800 235 546
Singapore: 65 64857620
Europe: www.belkin.com/support

Belkin International, Inc.

501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.

Express Business Park, Shipton Way
Rushden, NN10 6GL, United Kingdom

F5D9631-4_man updated by ARC
Page 120 of 120

+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.

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

Belkin Ltd.

4 Pioneer Avenue
Tuggerah Business Park
Tuggerah, NSW 2259, Australia
+61 (0) 2 4350 4600
+61 (0) 2 4350 4700 fax

© 2008 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 Computer, Inc., registered in the U.S. and other countries. Windows, Microsoft, and NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Pxxxxx
F5D8633-4