

BELKIN®

Wireless G Plus MIMO Router



User Manual

F5D9230-4

Table of Contents

| | |
|---|-----|
| 1. Introduction | |
| Advantages of a Wireless Network | 1 |
| Placement of your Wireless G Plus MIMO Router | 2 |
| 2. Product Overview | 6 |
| Product Features | 6 |
| 3. Knowing your Router | 9 |
| Package Contents | 9 |
| System Requirements | 9 |
| Easy Install Wizard Software System Requirements | 9 |
| 4. Connecting and Configuring your Router | 14 |
| 5. Alternate Setup Method | 29 |
| 6. Using the Web-Based Advanced User Interface | 47 |
| Changing LAN Settings | 48 |
| Viewing the DHCP Client List Page | 50 |
| Configuring the Wireless Network Settings | 51 |
| Setting WPA Security | 58 |
| Setting WEP Encryption | 60 |
| Using the Access Point Mode | 64 |
| Setting MAC Address Control | 65 |
| Setting Up Wireless Bridging | 67 |
| Configuring the Firewall | 71 |
| Using Dynamic DNS | 76 |
| Utilities | 79 |
| Restarting the Router | 80 |
| Updating the Firmware | 88 |
| 7. Manually Configuring Network Settings | 98 |
| 8. Recommended Web Browser Settings | 106 |
| 9. Troubleshooting | 111 |
| 10. Information | 123 |

Introduction

Thank you for purchasing the Belkin Wireless G Plus MIMO 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 the next 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 your wireless range

Easy installation – Belkin’s Easy Installation Wizard makes setup simple

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

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

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

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

Placement of your Wireless G Plus MIMO Router

Important Factors for Placement and Setup

Your wireless connection will be stronger the closer your computer is to your Router (or access point). 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 (or access point) and connected devices increases. This may or may not be noticeable to you. As you move farther from your Router (or access point), 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 (or access point) 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. Wireless Router (or Access Point) Placement

Place your Router (or access point), the central connection point of your network, as close as possible to the center of your wireless network devices.

To achieve the best wireless network coverage for your "wireless clients" (i.e., computers enabled by Belkin Wireless Notebook Network Cards, Wireless Desktop Network Cards, and Wireless USB Adapters):

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

2. Avoid Obstacles and Interference

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

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

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

3. Cordless Phones

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

- Try moving cordless phones away from your Router (or access point) 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 (or access point) to channel 11. See your phone’s user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

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

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

Use the Site Survey capabilities found in the Wireless 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 (or access point) and computers to a channel as far away from other networks as possible.

- Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices.
- For Belkin wireless networking products, use the detailed Site Survey and wireless channel information included 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 (or access point). Should you need to cover an even wider area, we suggest the Belkin Wireless Range Extender/Access Point.

5. Secure Connections, VPNs, and AOL

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

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

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

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.

Introduction

For more information regarding our networking products, visit our website at **www.belkin.com/networking** or call Belkin Technical Support at:

USA: 877-736-5771

310-898-1100 ext. 2263

UK: 0845 607 77 87

Australia: 1800 235 546

New Zealand: 0800 235 546

Singapore: 800 616 1790

Europe: www.belkin.com/support

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 Wireless G Plus MIMO 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, and XP, and others. All that is needed is an Internet browser and a network adapter that supports TCP/IP (the standard language of the Internet).

Front-Panel LED Display

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

Web-Based Advanced User Interface

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

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.

Product Overview

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.

Easy Install Wizard

The 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: Easy Install Wizard software is compatible with Windows 98SE, Me, 2000, XP, and Mac OS X. 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 29).

Product Overview

Integrated G Plus MIMO Wireless Access Point

G Plus 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 Router

Package Contents

- Belkin Wireless G Plus MIMO Router
- Quick Installation Guide
- Belkin Easy Install Wizard Software CD
- Belkin RJ45 Ethernet Networking Cable
- Power Supply
- User Manual

System Requirements

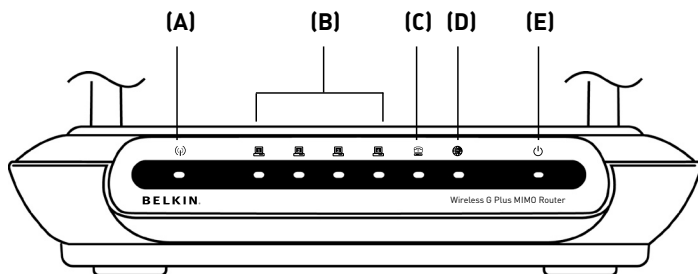
- Broadband Internet connection such as a cable or DSL modem with RJ45 (Ethernet) connection
- At least one computer with an installed network interface adapter
- TCP/IP networking protocol installed on each computer
- RJ45 Ethernet networking cable
- Internet browser

Easy Install Wizard Software System Requirements

- A PC running Windows® 98SE, Me, 2000, or XP, or a Mac® computer running Mac OS® X
- Minimum 64MB RAM
- Internet browser

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 LED indicators are easily visible on the TOP of the Router to provide you with information about network activity and status.



A. Wireless Network LED (📶)

| | |
|----------|-----------------------------|
| OFF | Wireless network is OFF |
| Green | Wireless network is ready |
| Blinking | Indicates wireless activity |

B. Wired Computer Status LEDs



These LEDs are labeled 1–4 and correspond to the numbered ports on the rear of the Router. When a computer is properly connected to one of the wired computer ports on the rear of the Router, the LED will light. When information is being sent over the port, the LED blinks rapidly.

| | |
|----------|---------------------------------|
| OFF | No device is linked to the port |
| Green | 10Base-T device connected |
| Blinking | Port activity |

C. Modem/WAN Status LED

This LED lights in GREEN to indicate that your modem is connected properly to the Router. It blinks rapidly when information is being sent over the port between the Router and the modem.

| | |
|----------------|---------------|
| OFF | No WAN link |
| Solid Green | Good WAN link |
| Blinking Green | WAN activity |

D. Internet/Connected LED

This unique LED 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, the Router is attempting to connect to the Internet. When the light is solid GREEN, the Router is connected to the Internet. When using the “Disconnect after x minutes” feature, this LED becomes extremely useful in monitoring the status of your Router’s connection.

| | |
|----------------|---|
| OFF | Router is not connected to the Internet |
| Blinking Green | Router is attempting to connect to the Internet |
| Solid Green | Router is connected to the Internet |

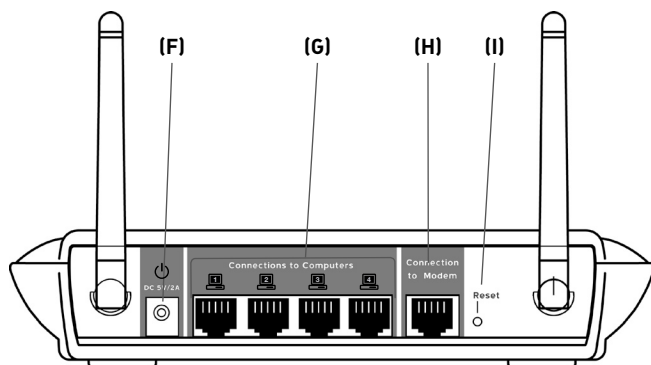
E. Power/Ready LED

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 “Power/Ready” LED blinks. When the Router has completely booted up, the “Power/Ready” LED becomes a SOLID light, indicating the Router is ready for use.

| | |
|----------------|----------------------|
| OFF | Router is OFF |
| Blinking Green | Router is booting up |
| Solid Green | Router is ready |

Knowing your Router

Rear Panel



F. Power Jack – GRAY

Connect the included 12V/0.5A DC power supply to this jack.

G. Connections to Computers (Wired Computer Ports) – 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. These ports correspond to the numbered LEDs on the front of the Router.

H. Connection to Modem (Modem Port) – BLUE

This port is for connection to your cable or DSL modem. Use the cable that was provided with the modem to connect the modem to this port. Use of a cable other than the cable supplied with the cable modem may not work properly.

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.

(a) Resetting the Router

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

(b) 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 “Power/Ready” light will begin to blink. When the “Power/Ready” light becomes solid again, the restore is complete.

Connecting and Configuring your Router

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

- Belkin Wireless G Plus MIMO Router
- Category 5 Networking Cable (for connecting the Router to the computer)
- Power Supply
- Belkin Easy Install Wizard Software CD
- User Manual

Modem Requirements

Your cable or DSL modem must be equipped with an RJ45 Ethernet port. Many modems have both an RJ45 Ethernet port and a USB connection. If you have a modem with both Ethernet and USB, and are using the USB connection at this time, you will be instructed to use the RJ45 Ethernet port during the installation procedure. If your modem has only a USB port, you can request a different type of modem from your ISP, or you can, in some cases, purchase a modem that has an RJ45 Ethernet port on it.



Ethernet



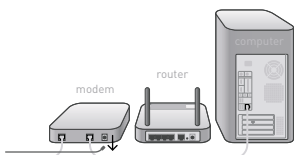
USB

Easy Install Wizard

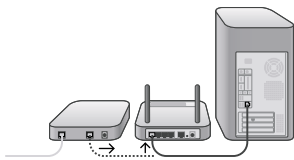
Belkin has provided our Easy Install Wizard software to make installing your Router a simple and easy task. You can use it to get your Router up and running in minutes. The Easy Install Wizard requires that your Windows 98SE, Me, 2000, or XP computer be connected directly to your cable or DSL modem and 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 98SE, Me, 2000, or XP, you must set up the Router using the “Alternate Setup Method” section of this User Manual.

Connecting and Configuring your Router

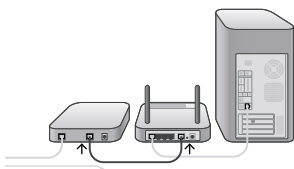
Step 1 | Hardware Connections – Follow the Quick Installation Guide (QIG)



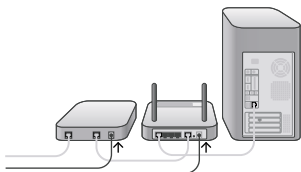
- 1.1** Unplug your modem's power cord. Place the Router next to the modem with the antennas raised.



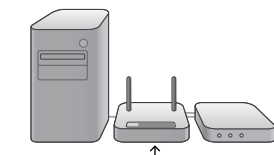
- 1.2** Locate the networking cable that connects your modem and computer. Unplug that cable from your modem, and plug it into any gray port on the back of the Router.



- 1.3** Find your new networking cable (included in the box with your Router) and connect it to the yellow port on the back of the Router. Connect the other end to your modem, in the port that's now free.



- 1.4** Plug in your modem's power cord. Wait 60 seconds for the modem to start up. Plug the Router's power supply into the black port on the back. Plug the other end into the wall outlet.

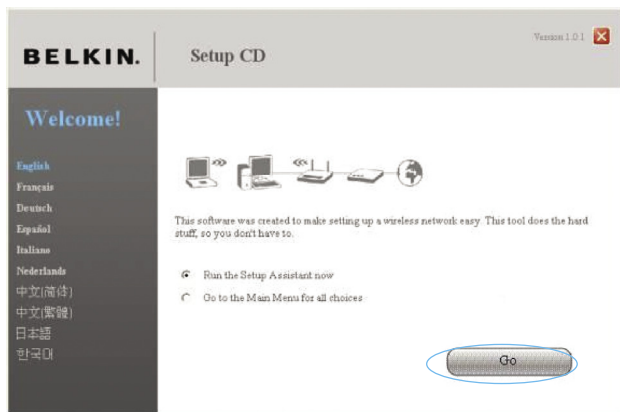


- 1.5** Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the "Wired" and "Router" icons are lit up in blue. If they are not, recheck your connections.

Connecting and Configuring your Router

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

- 2.1 Shut down any programs that are running on your computer at this time. Turn off any firewall or Internet-connection-sharing software on your computer.
- 2.2 Insert the CD into your computer. The Setup Assistant will automatically appear on your computer's screen within 15 seconds. Click on "Go" to run the Setup Assistant. Follow the instructions there.

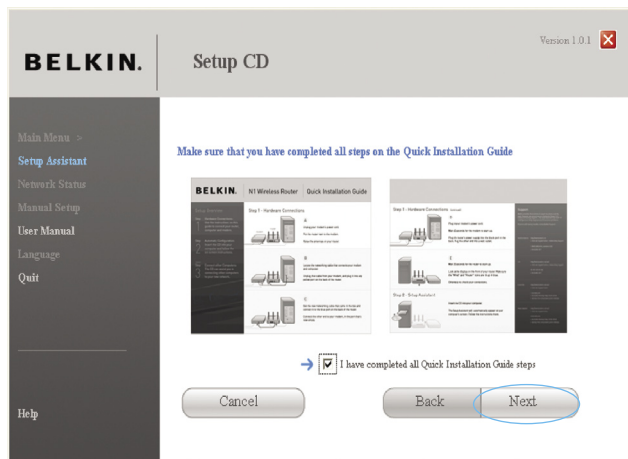
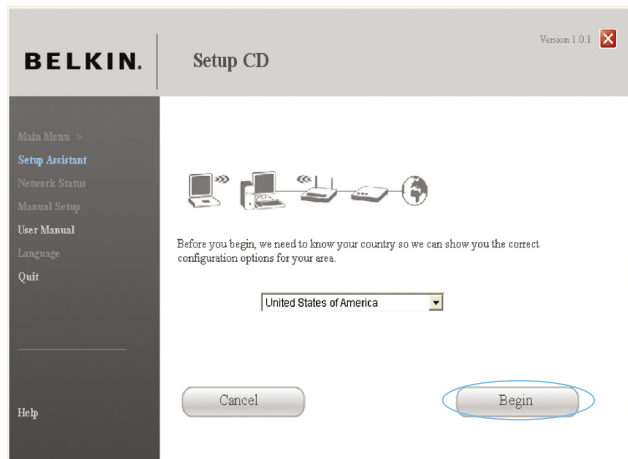


IMPORTANT: Run the Setup Assistant from the computer that is directly connected to the Router from Step 1.2.

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

2.3 Confirmation Screen

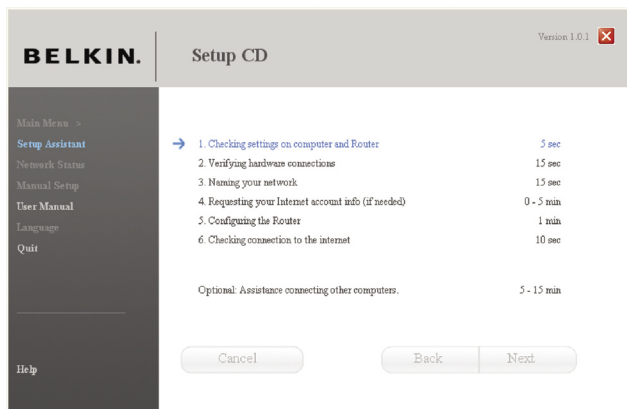
Verify that you have completed all setup steps by checking the box to the right of the arrow. Click “Next” to continue.



Connecting and Configuring your Router

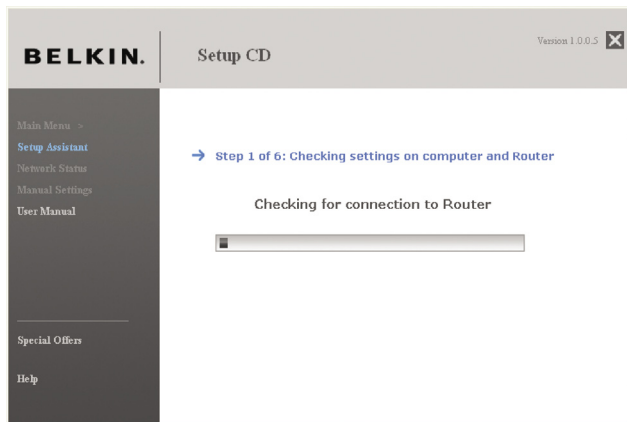
2.4 Progress Screen

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



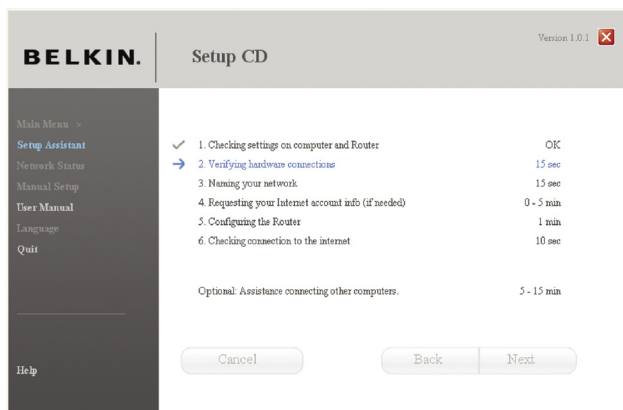
2.5 Checking Settings

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



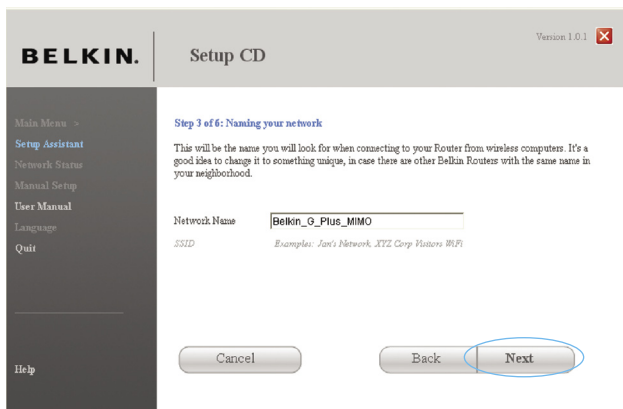
2.6 Verifying Hardware Connections

The Setup Assistant will now verify your hardware connection.



2.7 Naming your Wireless Network

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



Connecting and Configuring your Router

2.8 Requesting Internet Account Info (if needed)

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

BELKIN. Setup CD Version 1.0.1

Main Menu >
Setup Assistant
Network Status
Manual Setup
User Manual
Language
Quit

Help

| | | |
|---|--|----------|
| ✓ | 1. Checking settings on computer and Router | OK |
| ✓ | 2. Verifying hardware connections | OK |
| ✓ | 3. Naming your network | OK |
| → | 4. Requesting your Internet account info (if needed) | Checking |
| | 5. Configuring the Router | 1 min |
| | 6. Checking connection to the internet | 10 sec |

Optional: Assistance connecting other computers. 5 - 15 min

Cancel Back Next

BELKIN. Setup CD Version 1.0.1

Main Menu >
Setup Assistant
Network Status
Manual Setup
User Manual
Language
Quit

Help

Step 4 of 6: Internet account info

The Router needs a bit more information in order to be able to connect to the Internet.
When you tell us who provides your service, we can configure most of it.

Country Internet Service Provider (ISP)
United States of America Please select a provider...

Don't you see your ISP in the list? [Click Here.](#)

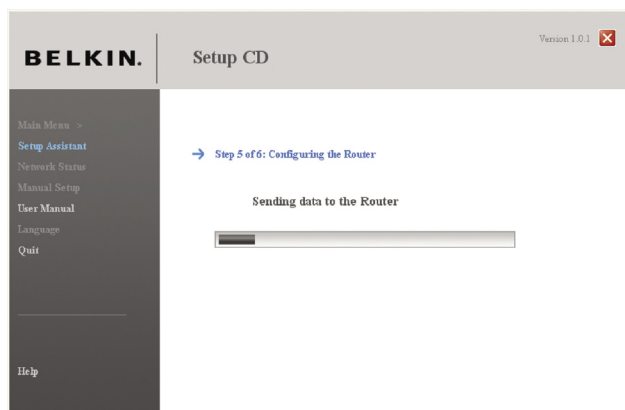
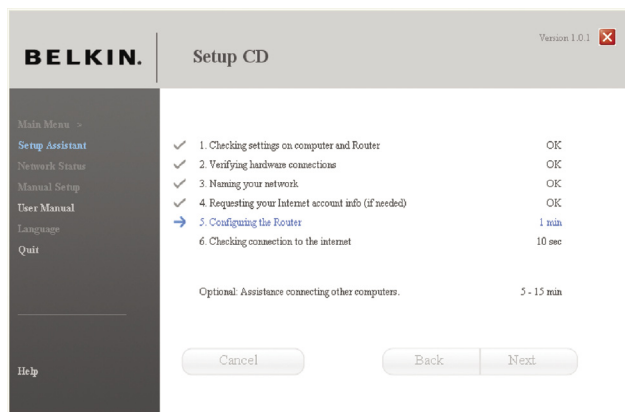
Cancel Back Next

Connecting and Configuring your Router

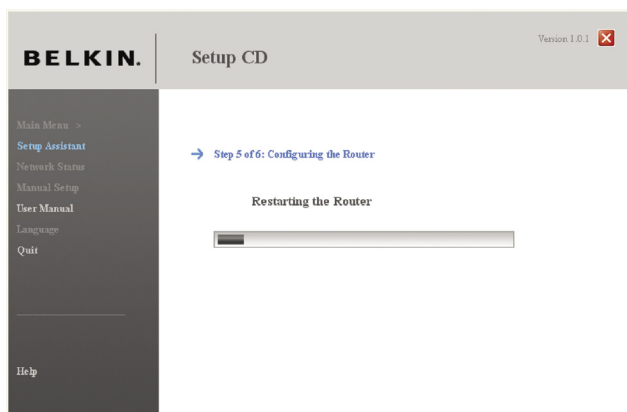
2.9 Configuring the Router

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.

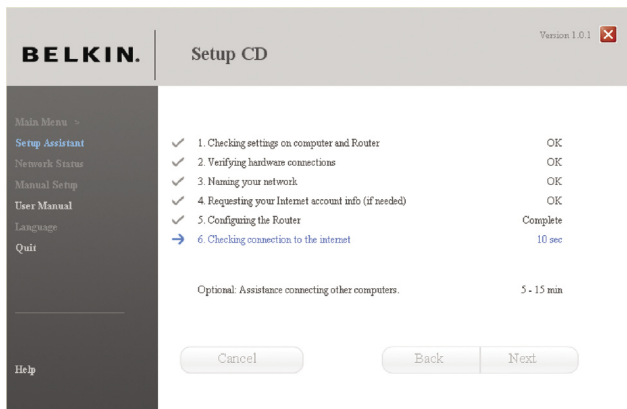


Connecting and Configuring your Router



2.10 Checking Internet Connection

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



Connecting and Configuring your Router

1

2

3

4

5

6

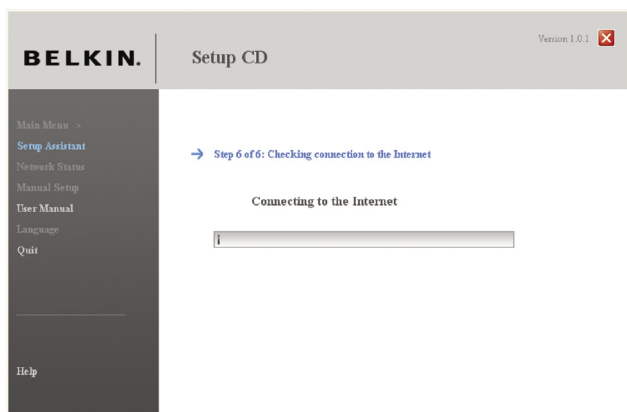
7

8

9

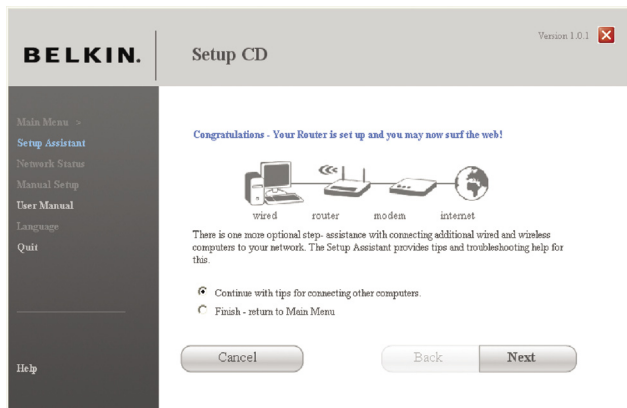
10

section

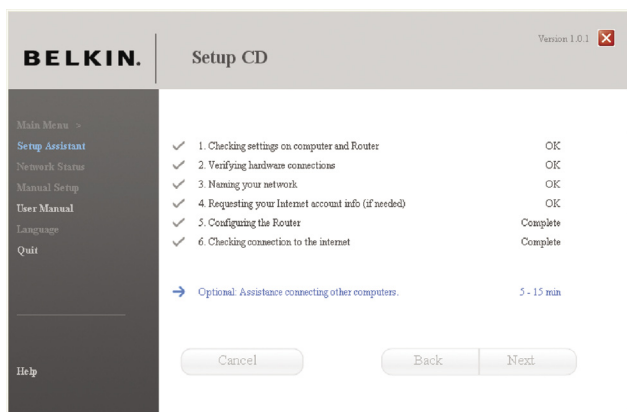


Congratulations

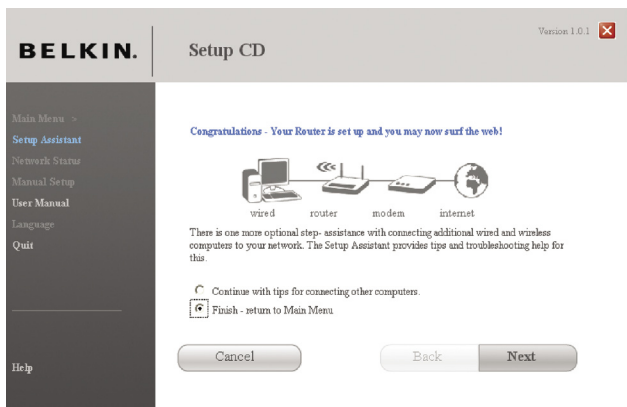
You have finished installing your new Belkin Router. You will see the “Congratulations” screen when your Router can connect to the Internet. You can begin surfing by opening your browser and going to any website.



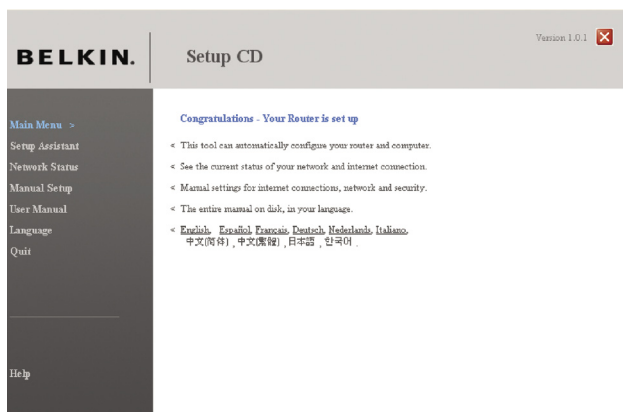
Connecting and Configuring your Router



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

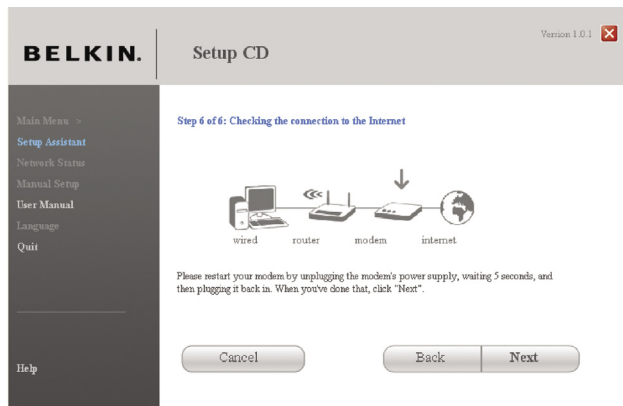


Connecting and Configuring your Router



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.



1

2

3

4

5

6

7

8

9

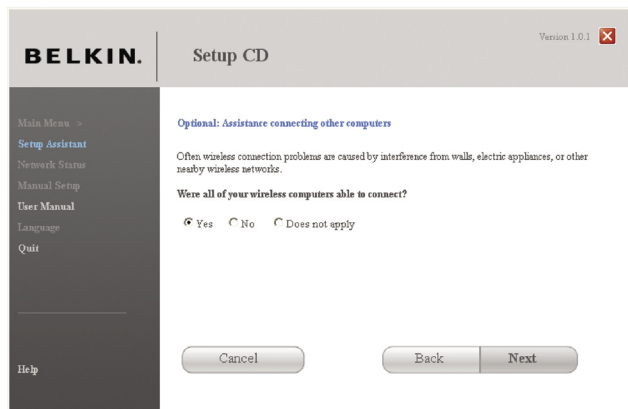
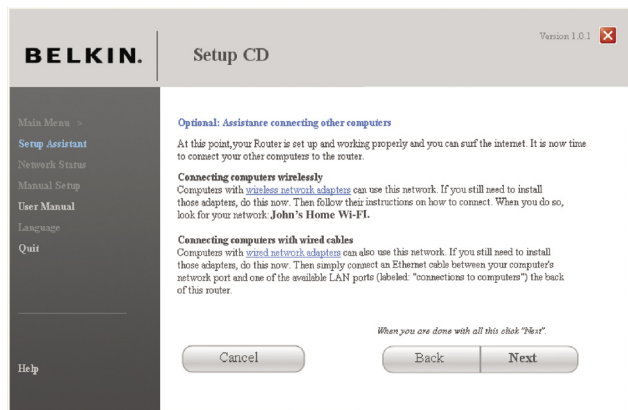
10

section

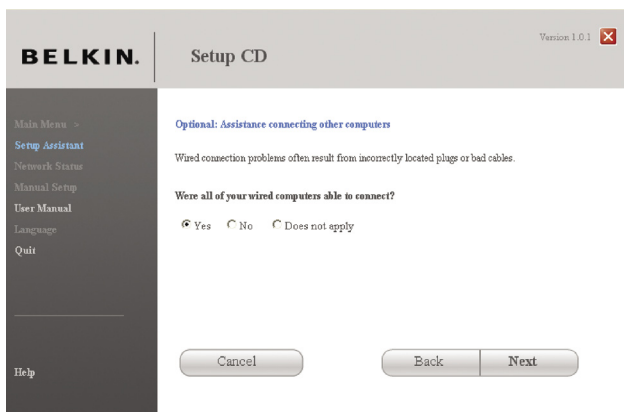
Connecting and Configuring your Router

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.

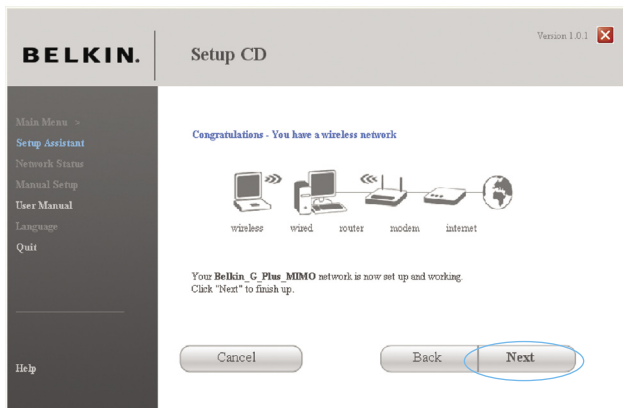


Connecting and Configuring your Router

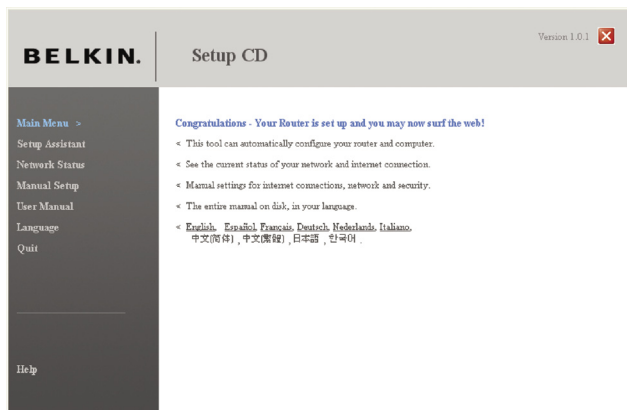


Congratulations

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



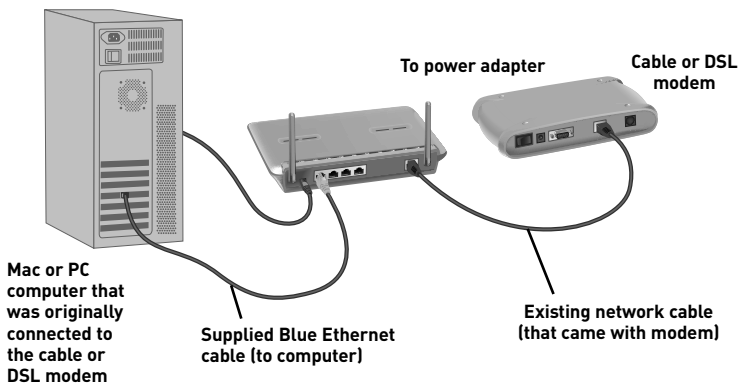
Connecting and Configuring your Router



Alternate Setup Method

Step 1 | Connecting your Gateway Router

- 1.1 Turn off the power to your modem by unplugging the power supply from the modem.
- 1.2 Locate the network cable that is connected between your modem and your computer and unplug it from your computer, leaving the other end connected to your modem.
- 1.3 Plug the loose end of the cable you just unplugged into the port on the back of the Router labeled “Internet/WAN”.
- 1.4 Connect the included network cable from the back of the computer to one of the ports labeled “1–4”.
Note: It does not matter which numbered port you choose.
- 1.5 Turn your cable or DSL modem on by reconnecting the power supply to the modem.
- 1.6 Before plugging the power cord into the Router, plug the cord into the wall, then plug the cord into the Router’s power jack.



Alternate Setup Method

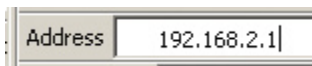
- 1.7 Verify that your modem is connected to the Router by checking the lights on the TOP of the Router. The green light labeled “WAN” should be ON if your modem is connected correctly to the Router. If it is not, recheck your connections.
- 1.8 Verify that your computer is connected properly to the Router by checking the lights labeled “LAN 1,2,3,4”. The light which corresponds to the numbered port connected to your computer should be ON, if your computer is connected properly. If it is not, recheck your connections.

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.

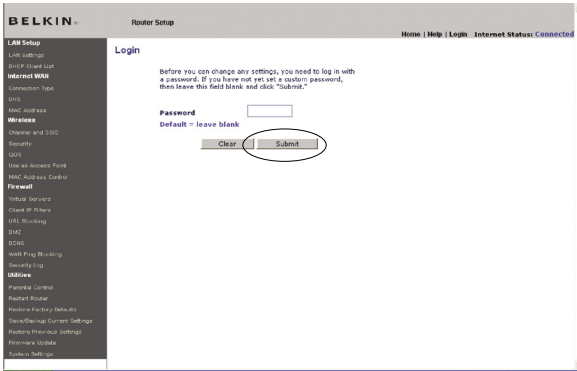
Step 3: Configuring the Router Using the Web-Based Advanced User Interface

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.



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.



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".

1

2

3

4

5

6

7

8

9

10

section

Alternate Setup Method

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.

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. Internet Status Indicator

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

The screenshot shows the Belkin Router Setup page. The interface includes a left sidebar with navigation links, a top navigation bar, and a main content area with several status and configuration sections. Numbered callouts identify the following elements:

- (1) Left sidebar navigation menu.
- (2) Home button in the top navigation bar.
- (3) Internet Status: Connected indicator in the top navigation bar.
- (4) Help button in the top navigation bar.
- (5) Login button in the top navigation bar.
- (6) WAN Settings section, including LAN/WLAN MAC, IP Address, Subnet Mask, and DHCP server.
- (7) Firewall Settings section, including NAT, Firewall Settings, SSID, Security, and UPnP.
- (8) Language section, showing Current Language (English) and Available Languages.
- (9) Status section, showing Action Info (Firmware Version, Hardware, Serial No.) and Internet Settings (WAN MAC Address, Connection Type, Subnet Mask, WAN IP, Default Gateway, DNS Address, Remaining Lease Time).
- (10) Router Setup title in the top navigation bar.

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. 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.

6. LAN Settings

Shows you the settings of the Local Area Network (LAN) side of the Router. Changes can be made to the settings by clicking 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.

7. Features

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

8. Internet Settings

Shows the settings of the Internet/WAN side of the Router that connects to the Internet. Changes to any of these settings can be made by clicking on the links or by clicking on the “Internet/WAN” quick-navigation link on the left side of the screen.

9. Version Info

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

10. Page Name

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

1

2

3

4

5

6

7

8

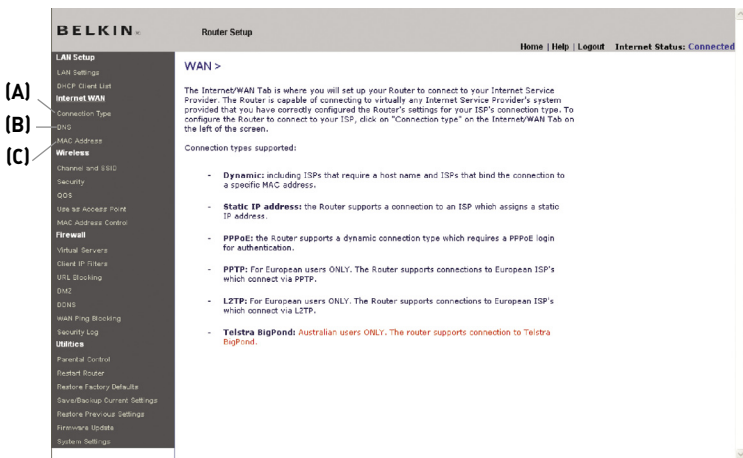
9

10

Alternate Setup Method

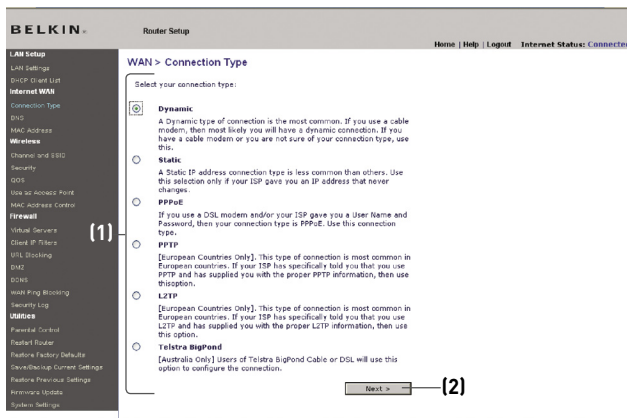
Step 4: Configuring your Router for Connection to your Internet Service Provider (ISP)

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.



Setting your Connection Type

From the “Connection Type” page, you can select the type of connection you use. Select the type of connection you use by clicking the button **(1)** next to your connection type and then clicking “Next” **(2)**.



1

2

3

4

5

6

7

8

9

10

Setting your Internet Service Provider (ISP) Connection Type to Dynamic IP

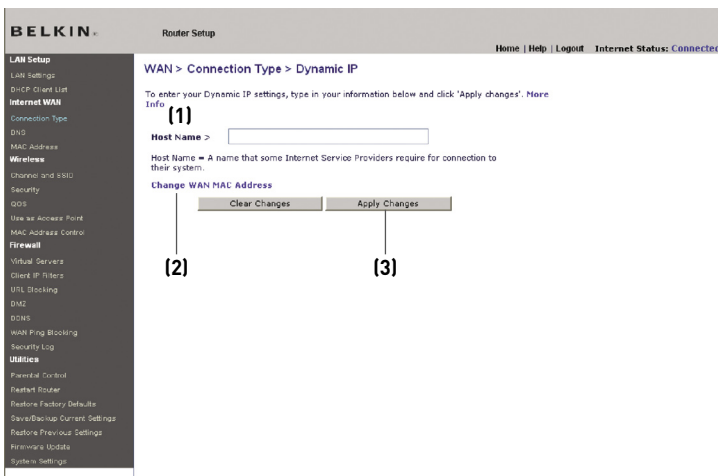
A dynamic connection type is the most common connection type found with cable modems. Setting the connection type to “dynamic” in many cases is enough to complete the connection to your ISP. Some dynamic connection types may require a host name. You can enter your host name in the space provided if you were assigned one. Your host name is assigned by your ISP. Some dynamic connections may require that you clone the MAC address of the PC that was originally connected to the modem.

1. Host Name

This space is provided to enter a host name that needs to be visible to your ISP. Enter your host name here and click “Apply Changes” **(3)**. If your ISP did not assign you a host name, or you are not sure, leave this blank.

2. Change WAN MAC Address

If your ISP requires a specific MAC address to connect to the service, you can enter a specific MAC address or clone the current computer's MAC address through this link.



Setting your Internet Service Provider (ISP) Connection Type to Static IP

A static IP address connection type is less common than other connection types. If your ISP uses static IP addressing, you will need your IP address, subnet mask, and ISP gateway address. This information is available from your ISP or on the paperwork that your ISP left with you. Type in your information, then click “Apply Changes” (5). After you apply the changes, the Internet Status indicator will read “connection OK” if your Router is set up properly.

1. IP Address

Provided by your ISP. Enter your IP address here.

2. Subnet Mask

Provided by your ISP. Enter your subnet mask here.

3. ISP Gateway Address

Provided by your ISP. Enter the ISP gateway address here.

4. My ISP Provides More Than One Static IP Address

If your ISP assigns you more than one static IP address, your Router is capable of handling up to five static WAN IP addresses. Select “My ISP provides more than one static IP address” and enter your additional addresses.

BELKIN Router Setup Home | Help | Logout Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
WPS
Use as Access Point
Host Address Control
Firewall
Virtual Servers
Guest IP Filter
URL Blocking
DMZ
STAS
Web Ping Blocking
Security Log
Utilities
Parental Control
Restart Router
Restore Factory Defaults
Revert/Restore Current Settings
Restore Previous Settings
Firmware Update
System Settings

WAN > Connection Type > Static IP

To enter your Static IP settings, type in your information below and click 'Apply changes'. Note: Info

IP Address > (1)

Subnet Mask > (2)

ISP Gateway Address > (3)

My ISP Provides more than one Static IP address? > (4)

Click here to enter your DNS Settings

Clear Changes Apply Changes (5)

Alternate Setup Method

Setting your ISP Connection Type to PPPoE

Most DSL providers use PPPoE as the connection type. If you use a DSL modem to connect to the Internet, your ISP may use PPPoE to log you into the service. If you have an Internet connection in your home or small office that doesn't require a modem, you may also use PPPoE.

Your connection type is PPPoE if:

- 1) Your ISP gave you a user name and password, which is required to connect to the Internet.
- 2) Your ISP gave you software such as WinPOET or Eternet300 that you use to connect to the Internet.
- 3) You have to double-click on a desktop icon other than your browser to get on the Internet.

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

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
WAN
MAC Address
Wireless
Channels and SSID
Security
WDS
Wireless Access Point
MAC Address Control
Firewall
Virtual Servers
Stateful Firewall
URL Blocking
DMZ
QoS
WAN Ping Blocking
Security Log
Utilities
Firewall Control
Restore Router
Restore Factory Defaults
Save/Revert Settings
Restore Previous Settings
Firmware Update
System Settings

WAN > Connection Type > PPPoE

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

User Name > (1)

Password > (2)

Retype Password >

Service Name (Optional) > (3)

MTU (576-1492) > (4)

Do not make changes to the MTU setting unless your ISP specifically requires a different setting than 1492. [More Info](#)

☐ Disconnect after minutes of no activity: (5)

[More Info](#)

Alternate Setup Method

1. **User Name**

This space is provided to type in your user name that was assigned by your ISP.

2. **Password**

Type in your password and retype it into the “Retype Password” box to confirm it.

3. **Service Name**

A service name is rarely required by an ISP. If you are not sure if your ISP requires a service name, leave this blank.

4. **MTU**

The MTU setting should never be changed unless your ISP gives you a specific MTU setting. Making changes to the MTU setting can cause problems with your Internet connection including disconnection from the Internet, slow Internet access, and problems with Internet applications working properly.

5. **Disconnect after X...**

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

1

2

3

4

5

6

7

8

9

10

section

Alternate Setup Method

Setting your Internet Service Provider (ISP) Connection Type to Point-to-Point Tunneling Protocol (PPTP) [European Countries Only]

Some ISPs require a connection using PPTP protocol, a type of connection most common in European countries. This sets up a direct connection to the ISP's system. Type in the information provided by your ISP in the space provided. When you have finished, click "Apply Changes" (9). After you apply the changes, the Internet Status indicator will read "connection OK" if your Router is set up properly.

BELKIN Router Setup Home | Help | Logout | Internet Status: Connected

LAN Setup
Link Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
QoS
Use Set Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filter
URL Blocking
DMZ
DDNS
Web Page Blocking
Security Log
Utilities
Parental Control
Restart Router
Restore Factory Defaults
Save/Revert Current Settings
Restore Previous Settings
Firmware Updates
System Settings

WAN > Connection Type > PPTP

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

PPTP Account > (1)

PPTP Password > (2)

Retype Password >

Host Name > (3)

Server IP Address > (4)

My IP Address > (5)

My Subnet Mask > (6)

Connection ID (optional) > (optional) (7)

☐ Disconnect after minutes of no activity (8)

[Click here to enter your DNS Settings](#)

(9)

1. PPTP Account

Provided by your ISP. Enter your PPTP account name here.

2. PPTP Password

Type in your password and retype it into the "Retype Password" box to confirm it.

3. Host Name

Provided by your ISP. Enter your host name here.

4. Server IP Address

Provided by your ISP. Enter your server IP address here.

5. My IP Address

Provided by your ISP. Enter the IP address here.

6. **My Subnet Mask**

Provided by your ISP. Enter the IP address here.

7. **Connection ID (optional)**

Provided by your ISP. If your ISP did not give you a connection ID, leave this blank.

8. **Disconnect after X....**

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

1

2

3

4

5

6

7

8

9

10

section

Setting your Internet Service Provider (ISP) Connection Type to Point-to-Point Tunneling Protocol (L2TP)

[European Countries Only]

Some ISPs require a connection using L2TP protocol, a type of connection most common in European countries. This sets up a direct connection to the ISP's system. Type in the information provided by your ISP in the space provided. When you have finished, click "Apply Changes" (9). After you apply the changes, the Internet Status indicator will read "connection OK" if your Router is set up properly.

BELKIN Router Setup Home | Help | Logout | Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
WAN Address
Wireless
Channel and SSID
Security
QoS
Web Air Access Point
WAN Address Control
Firewall
Virtual Servers
Client IP Filter
VPN Tunneling
DMZ
WAN Ping Browsing
Security Log
Utilities
Powerful Control
Restart Router
Restore Factory Default
Download/Upload Current Settings
Restore Previous Settings
Firmware Updates
System Settings

WAN > Connection Type > L2TP

To enter your L2TP settings, type in your information below and click "Apply changes". [More Info](#)

L2TP Account > (1)

L2TP Password > (2)

Retype Password > (3)

Host Name > (4)

Server IP Address > (5)

My IP Address > 0.0.0.0 (6)

My Subnet Mask > 255.255.255.0 (7)

Connection ID (optional) > (optional) (8)

☐ Disconnect after 5 minutes of no activity

[Click here to enter your DNS Settings](#)

Clear Changes Apply Changes (9)

1. L2TP Account

Provided by your ISP. Enter your L2TP account name here.

2. L2TP Password

Type in your password and retype it into the "Retype Password" box to confirm it.

3. Host Name

Provided by your ISP. Enter your host name here.

4. Server IP Address

Provided by your ISP. Enter your server IP address here.

5. My IP Address

Provided by your ISP. Enter the IP address here.

6. My Subnet Mask

Provided by your ISP. Enter the IP address here.

7. **Connection ID (optional)**

Provided by your ISP. If your ISP did not give you a connection ID, leave this blank.

8. **Disconnect after X....**

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

1

2

3

4

5

6

7

8

9

10

section

Alternate Setup Method

Setting your Connection Type if You Are a Telstra® BigPond User [Australia Only]

Your user name and password are provided to you by Telstra BigPond. Enter this information below. Choosing your state from the drop-down menu **(6)** will automatically fill in your login server IP address. If your login server address is different than one provided here, you may manually enter the login server IP address by placing a check in the box next to “User decide login server manually” **(4)** and type in the address next to “Login Server” **(5)**. When you have entered all of your information, click “Apply Changes” **(7)**. After you apply the changes, the Internet Status indicator will read “connection OK” if your Router is set up properly.

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

LAN Setup
LAN Settings
WAN Setup
Internet WAN
Connection Type
WAN
MAC Address
Wireless
Channel and SSID
Security
SSID
Step-by-Step Wizard
Internet Address Control
Firewall
Virtual Servers
Client IP Filter
URL Blocking
QoS
DHCP
Web Page Blocking
Security Log
Utilities
Parental Control
Router Status
Restore Factory Defaults
Restore Factory Defaults
Restore Previous Settings
Restore Previous Settings
Restore Previous Settings
Restore Previous Settings

WAN > Connection Type > Telstra BigPond

If your Internet service is provided by Telstra BigPond in Australia, you will need to enter your information below. This information is provided by Telstra BigPond. Please Refer:

Select Your State - **(1)** --> **(6)**

User Name -> **(2)**

Password -> **(3)**

Retype Password ->

User decide login server manually -> **(4)**

Login Server -> **(5)**

Clear Changes Apply Changes **(7)**

1. Select your State

Select your state from the drop-down menu **(6)**. The “Login Server” box will automatically be filled in with an IP address. If for some reason this address does not match the address that Telstra has given, you can manually enter the login server address. See “User decide login server manually” **(4)**.

2. User Name

Provided by your ISP. Type in your user name here.

3. Password

Type in your password and retype it into the “Retype Password” box to confirm it.

4. User Decide Login Server Manually

If your login server IP address is not available in the “Select Your State” drop-down menu **(6)**, you may manually enter the login server IP address by placing a check in the box next to “User decide login server manually” and type in the address next to “Login Server” **(5)**.

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.

The screenshot shows the Belkin Router Setup interface. On the left is a navigation menu with categories: LAN Setup, Wireless, Firewall, and Utilities. The main content area is titled 'WAN > DNS'. It contains instructions: 'If your ISP provided you with a specific DNS address to use, enter the address in this window and click "Apply Changes".' Below this is a checkbox labeled 'Automatic from ISP' with a callout **(1)** pointing to it. There are two text input fields: 'DNS Address >' and 'Secondary DNS Address >'. At the bottom are two buttons: 'Clear Changes' and 'Apply Changes' with a callout **(2)** pointing to it. A footer note explains: 'DNS = Domain Name Server. A server located on the Internet that translates URL's (Universal Resource Links) like www.belkin.com to IP addresses. More Info'.

Alternate Setup Method

Configuring your WAN Media Access Controller (MAC) Address

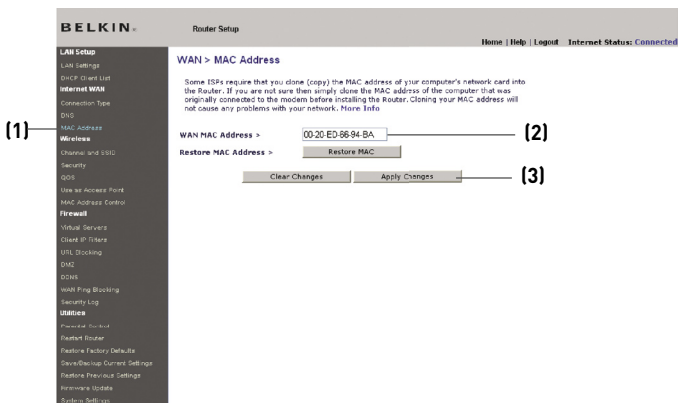
All network components including cards, adapters, and routers, have a unique “serial number” called a MAC address. Your Internet Service Provider (ISP) may record the MAC address of your computer’s adapter and only let that particular computer connect to the Internet service. When you install the Router, its own MAC address will be “seen” by the ISP and may cause the connection not to work. Belkin has provided the ability to clone (copy) the MAC address of the computer into the Router. This MAC address, in turn, will be seen by the ISP’s system as the original MAC address and will allow the connection to work. If you are not sure whether your ISP needs to see the original MAC address, simply clone the MAC address of the computer that was originally connected to the modem. Cloning the address will not cause any problems with your network.

Cloning your MAC Address

To clone your MAC address, make sure that you are using the computer that was **ORIGINALLY CONNECTED** to your modem before the Router was installed. Click the “Mac Address” button **(1)**. Click “Apply Changes” **(3)**. Your MAC address is now cloned to the Router.

Entering a Specific MAC Address

In certain circumstances you may need a specific WAN MAC address. You can manually enter one in the “MAC Address” page. Type in a MAC address in the spaces provided **(2)** and click “Apply Changes” **(3)** to save the changes. The Router’s WAN MAC address will now be changed to the MAC address you specified.



Using the Web-Based Advanced User Interface

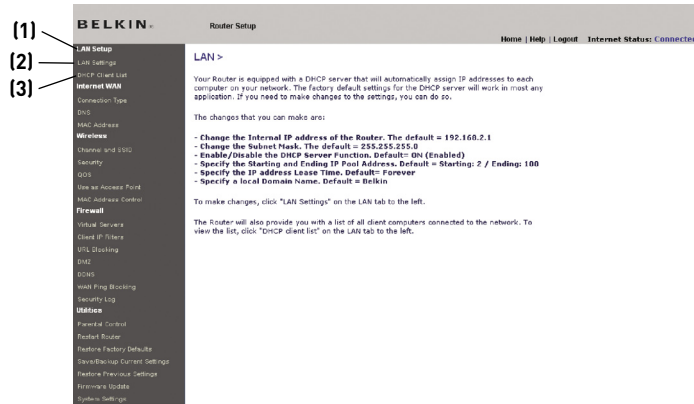
Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (do not type in anything else such as "http://" or "www") then press the "Enter" key.



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).



Using the Web-Based Advanced User Interface

Changing LAN Settings

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

BELKIN Router Setup Home | Help | Logout | Internet Status: Connected

LAN Setup

- LAN Settings
- Dynamic WAN
- Connection Type
- DNS
- MAC Address
- Wireless
- Channel and SSID
- Security
- QoS
- Virtual Access Point
- MAC Address Control
- Firewall
- Virtual Servers
- Client Firewall
- URL Filtering
- DHCP
- IGMP
- Link Ping Monitoring
- Security Log
- Utilities
- Parental Control
- Restart Router
- Restore Factory Defaults
- Specify/Reset Current Settings
- Restore Previous Settings
- Firmware Updates
- System Settings

LAN > LAN Settings

You can make changes to the Local Area Network (LAN) here. For changes to take effect, you must press the "Apply Changes" button at the bottom of the screen.

IP Address > **(1)**
[More Info](#)

Subnet Mask > **(2)**
[More Info](#)

DHCP server > ☒ On ☐ Off **(3)**
The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network. It is not necessary to make any changes here. [More Info](#)

IP Pool Starting Address > **(4)**
IP Pool Ending Address >

Lease Time > **(5)**
The length of time the DHCP server will reserve the IP address for each computer.

Local Domain Name > **(6)**
(Optional)
A feature that lets you assign a name to your network. [More Info](#)

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

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”.

Using the Web-Based Advanced User Interface

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.

The screenshot shows the Belkin Router Setup web interface. The left sidebar contains navigation links for LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled "LAN > DHCP Client List". It includes a descriptive paragraph and a table with three columns: IP Address, Host Name, and MAC Address. The table lists two clients. Below the table is a "Refresh" button. Numbered callouts (1) through (4) point to the IP Address, Host Name, MAC Address, and the Refresh button, respectively.

LAN Setup
List Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
WDS
Virtual Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filter
URL Blocking
DMZ
IDS/IPS
Web Page Blocking
Security Log
Utilities
Firmware Control
Restart Router
Restore Factory Defaults
Specify Backup Config Settings
Restore Previous Settings
Firmware Update
System Settings

Router Setup Home | Help | Logout Internet Status: Connected

LAN > DHCP Client List

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

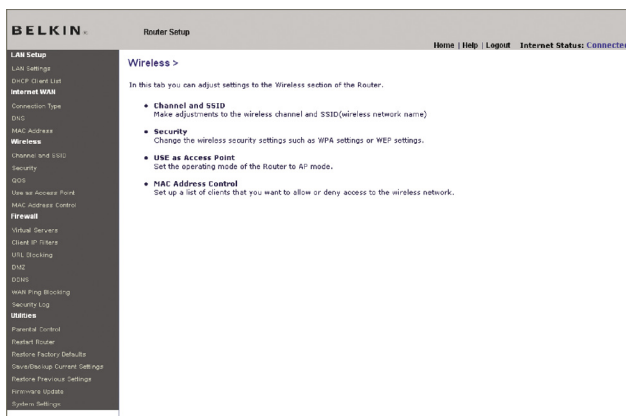
| IP Address | Host Name | MAC Address |
|--------------|---------------|-------------------|
| 192.168.1.20 | you~7218239e7 | 90-13-94-52-18-50 |
| 192.168.1.48 | marian_wan | 00-16-93-26-00-37 |

(1) (2) (3) (4)

Refresh

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 (SSID), operating channel, encryption security settings, and configure the Router to be used as an access point.



1

2

3

4

5

6

7

8

9

10

section

Using the Web-Based Advanced User Interface

Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. The SSID is your network name. The default network name of the Router is “Belkin G Plus MIMO_” followed by six digits that are unique to your Router. Your network name will look something like “Belkin G Plus MIMO_012345”. 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.

The screenshot shows the Belkin Router Setup web interface. On the left is a navigation menu with categories: LAN Setup, Internet WDM, Wireless, Firewall, and Utilities. The 'Wireless' section is expanded, showing options like Channel and SSID, Security, QoS, and Wireless Network Point. The main content area is titled 'Wireless > Channel and SSID'. It contains a message: 'To make changes to the wireless settings of the router, make the changes here. Click "Apply Changes" to save the settings. More Info'. Below this are several settings: 'Wireless Channel' set to 'Auto' (Current Channel = 11), 'SSID' set to 'Belkin_G_Plus_MIMO', 'Wireless Mode' set to '802.11g & 802.11b' (More Info), 'Broadcast SSID' checked (More Info), and 'Protected Mode' set to 'Off' (More Info). At the bottom are two buttons: 'Clear Changes' and 'Apply Changes'. The 'Apply Changes' button is highlighted with a line and the label **(2)**. The label **(1)** points to the SSID text field.

Using the Wireless Mode Switch

This switch allows you to set the Router's wireless modes. There are three modes.

1) 802.11g only

Setting the Router to this mode will allow only G Plus MIMO and 802.11g-compliant devices to join the network, keeping out any slower 802.11b devices.

2) 802.11g & 802.11b

Setting the Router to this mode will let G Plus MIMO-, 802.11g-, and 802.11b-compliant devices to join the network.

3) Off

This mode will turn OFF the Router's access point, so no wireless devices can join the network. Turning off the wireless function of your Router is a great way to secure your network when you are away from home for a long period of time, or don't want to use the wireless feature of the Router at a certain time.

The image displays two screenshots of the Belkin Router Setup web interface, specifically the 'Wireless > Channel and SSID' configuration page. The interface includes a left sidebar with navigation links and a main content area with settings for wireless channel, SSID, mode, broadcast SSID, and protected mode. Buttons for 'Clear Changes' and 'Apply Changes' are at the bottom of the settings area.

Top Screenshot: The 'Wireless Mode' is set to '802.11g & 802.11b' (labeled 2), and 'Protected Mode' is set to 'Off' (labeled 3). The 'Wireless Channel' is set to 'Auto' with 'Current Channel = 11'. The 'SSID' is 'Belkin_G_Plus_MIMO'. The 'Broadcast SSID' checkbox is checked.

Bottom Screenshot: The 'Wireless Mode' is set to '802.11g only' (labeled 1). The 'Wireless Channel' is set to 'Auto' with 'Current Channel = 11'. The 'SSID' is 'Belkin_G_Plus_MIMO'. The 'Broadcast SSID' checkbox is checked.

Using the Web-Based Advanced User Interface

Changing the Wireless Channel

There are a number of operating channels you can choose from. In the United States, there are 11 channels. In the United Kingdom and most of Europe, there are 13 channels. In a small number of other countries, there are other channel requirements. Your Router is configured to operate on the proper channels for the country you reside in. 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.

Auto Channel Selection Feature and Changing the Channel

For best performance, your Router should use a channel that is at least five channels away from the other wireless networks in the area. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. The auto channel selection mode will choose the clearest channel to operate on when the Router is first powered up. Your Router ships from the factory with the auto channel feature enabled. You can manually select a channel if you wish; however, it is recommended to use the auto channel mode. To change the channel, select the channel from the drop-down list. Click “Apply Changes”. The change is immediate.

Wireless > Channel and SSID

To make changes to the wireless settings of the router, make the changes here. Click “Apply Changes” to save the settings. [More Info](#)

Wireless Channel > Auto Current Channel = 11

SSID >

Wireless Mode > 802.11b More Info

Broadcast SSID > Info

Protected Mode > More Info

Clear Channel Apply Changes

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 will ensure proper operation of 802.11g devices on your G Plus MIMO network when 802.11b devices are present or when there is heavy 802.11b traffic in the operating environment. If you are using a mix of Belkin G Plus MIMO Wireless Cards and 802.11b or 802.11g cards on your network, protected mode should be used. If you are in an environment where there is no other (or very little) 802.11b wireless network traffic, best 802.11g performance may be achieved with protected mode OFF. If you are operating in an environment with HEAVY 802.11b traffic or interference, best 802.11g performance may be achieved with protected mode ON. Wireless G Plus MIMO performance is not affected by this setting.

Changing the Wireless Security Settings

Your Router is equipped with the latest security standard called Wi-Fi Protected Access (WPA). It also supports the legacy security standard called Wired Equivalent Privacy (WEP). By default, wireless security is disabled. To enable security, you will need to determine which standard you want to use. To access the security settings, click "Security" on the "Wireless" tab.

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/?kbid=826942>

For Windows XP with Service Pack 2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB893357). The update is available from: <http://support.microsoft.com/default.aspx?scid=kb;en-us;893357>

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 both WPA2-Personal (PSK) mode and WPA2-Enterprise (RADIUS) mode. Typically, WPA2-Personal (PSK) is the mode that will be used in a home environment, while WPA2-Enterprise (RADIUS) is implemented in a business environment where an external radius server distributes the network key to the clients automatically. This guide will focus on WPA2-Personal (PSK) usage. 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.

Using the Web-Based Advanced User Interface

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.

BELKIN Router Setup Home | Help | Logout Internet Status: Connected

LAN Setup
 LAN Settings
 Setup Wireless
Internet WAN
 Connection Type
 DNS
 MAC Address
Wireless
 Channels and SSID
 Security
 QoS
 Basic Access Point
 WAN Address Control
Firewall
 Virtual Servers
 Client IP Filters
 DMZ Blocking
 NAT
 IGMP
 WAN Ping Blocking
 Security Log
Utilities
 Password Control
 Restart Router
 Restore Factory Defaults
 Save/Backup Current Settings
 Restore Previous Settings
 Firmware Update
 System Settings

Wireless > Security

Security Mode WPA(With Radius Server)

WPA(with server)
Advanced Setting: Wireless Protected Access using a server to distribute keys to the clients. This option requires that a Radius server is running on the network. [More Info](#)

Authentication WPA-RADIUS+WPA2-RADIUS

Encryption Technique TKIP

| | |
|------------------------|------|
| RADIUS Server | |
| RADIUS port | 1812 |
| RADIUS Key | |
| Re-Key Interval | 900 |

Clear Changes
Apply Changes

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 (no server). 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 (no server)”.
2. For “Encryption Technique”, select “TKIP” or “AES”. This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key. 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.

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

Wireless > Security

Security Mode: WPA-PSK (no server) (circled in blue)

Authentication: WPA-PSK

Encryption Technique: TKIP (Default is TKIP)

Pre-shared Key(PSK):

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 (0-9, A-F) only. Each client that connects to the network must use the same key (Pre-Shared Key). [More Info](#)

☐ Obsolete PSK

[Clear Changes](#) [Apply Changes](#) (circled in blue)

Using the Web-Based Advanced User Interface

BELKIN Router Setup Home | Help | Logout | Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
WAN Address
MAC Address
Wireless
Channel and SSID
Security
QoS
Web Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
URL Blocking
DMZ
DOCS
WAN Ping Blocking
Security Log
Utilities
Parental Control
Restart Router
Restore Factory Defaults
Backup/Restore Current Settings
Restore Previous Settings
Firmware Updates
System Settings

Wireless > Security

Security Mode: WPA-PSK(no server)
Authentication: WPA2-PSK
Encryption Technique: AES
Pre-shared Key(PSK):

☐ Obsolete PSK

Clear Changes Apply Changes

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](#)

BELKIN Router Setup Home | Help | Logout | Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
WAN Address
MAC Address
Wireless
Channel and SSID
Security
QoS
Web Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
URL Blocking
DMZ
DOCS
WAN Ping Blocking
Security Log
Utilities
Parental Control
Restart Router
Restore Factory Defaults
Backup/Restore Current Settings
Restore Previous Settings
Firmware Updates
System Settings

Wireless > Security

Security Mode: WPA-PSK(no server)
Authentication: WPA-PSK+WPA2-PSK
Encryption Technique: TKIP
Pre-shared Key(PSK):

☐ Obsolete PSK

Clear Changes Apply Changes

TKIP(AES 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](#)

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

Wireless > Security

Security Mode

You can configure wireless security/encryption. WPA (Wireless Protected Access) provides dynamic security, but not all devices support WPA. WEP (Wired Equivalent Privacy) should be enabled to assure maximum wireless security. WPA (with Radius Server) is the best security solution. In wireless environments, WEP should be used. [More Info](#)

Disabled
WPA-PSK(no server)
128bit WEP
64bit WEP
WPA(with Radius Server)

Apply Changes

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.

Wireless > Security

Security Mode

128bit WEP [More Info](#)

(13 hex digit pairs)

NOTE: To automatically generate hex pairs using a PassPhrase, check the box on the left and input the passphrase here

PassPhrase

generate

Clear Changes [Apply Changes](#)

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 the Web-Based Advanced User Interface

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 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:

| | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|

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.

1

2

3

4

5

6

7

8

9

10

section

Using the Web-Based Advanced User Interface

QOS

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

LAN Setup
Link Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
QOS
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
URL Blocking
DND
QoS
WAN Ping Blocking
Security Log
Utilities
Parental Control
Reboot Router
Restore Factory Defaults
Save/Backup Current Settings
Restore Previous Settings
Firmware Update
System Settings

Wireless > QOS

WMM Mode >

ACK Mode >

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

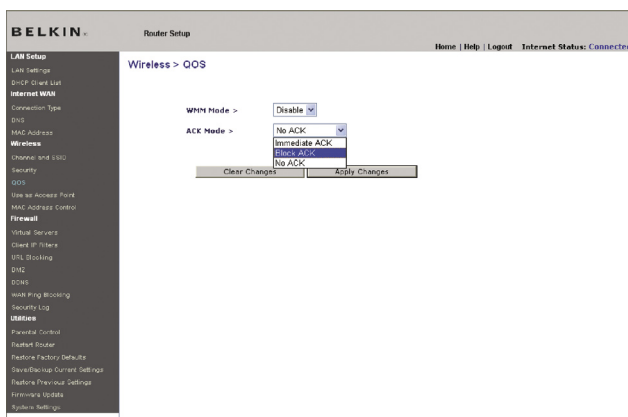
LAN Setup
Link Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
QOS
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
URL Blocking
DND
QoS
WAN Ping Blocking
Security Log
Utilities
Parental Control
Reboot Router
Restore Factory Defaults
Save/Backup Current Settings
Restore Previous Settings
Firmware Update
System Settings

Wireless > QOS

WMM Mode >

ACK Mode >

Using the Web-Based Advanced User Interface

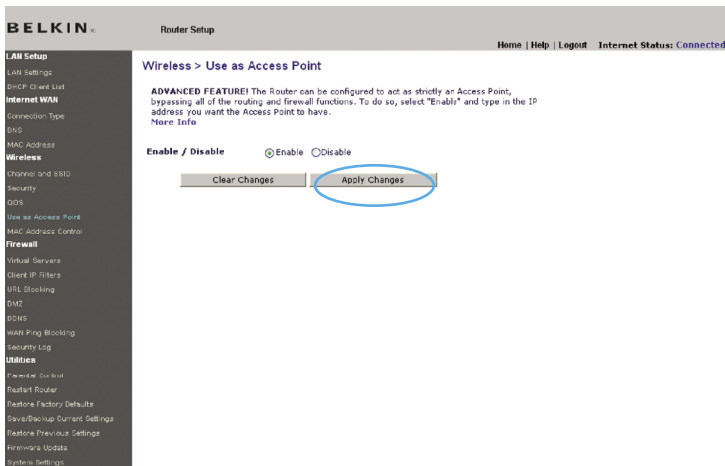


Using the Access Point Mode

Note: This advanced feature should be employed by advanced users only. The Router can be configured to work as a wireless network access point. Using this mode will defeat the NAT IP sharing feature and DHCP server. In AP mode, the Router will need to be configured with an IP address that is in the same subnet as the rest of the network that you will bridge to. The default IP address is 192.168.2.254 and subnet mask is 255.255.255.0. These can be customized for your need.

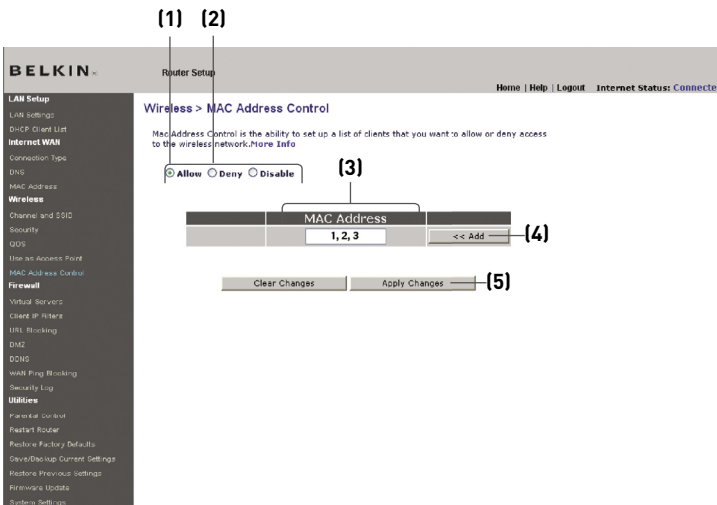
1. Enable the AP mode by selecting “Enable” in the “Use as Access Point only” page. When you select this option, you will be able to change the IP settings.
2. Set your IP settings to match your network. Click “Apply Changes”.
3. Connect a cable from the LAN port on the Router to your existing network.

The Router is now acting as an access point. To access the Router advanced user interface again, type the IP address you specified into your browser's navigation bar. You can set the encryption settings, MAC address filtering, SSID, and channel normally.



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.



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 (3), type in the MAC address of the wireless computer you want to be able to access the wireless network, then click “<<Add” (4).
3. Continue to do this until all of the computers you want to add have been entered.
4. Click “Apply Changes” (5) to finish.

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 **(2)** 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 **(3)**, type in the MAC address of the wireless computer you want to deny access to the wireless network, then click “<<Add” **(4)**.
3. Continue to do this until all of the computers you want to deny access to have been entered.
4. Click “Apply Changes” **(5)** to finish.

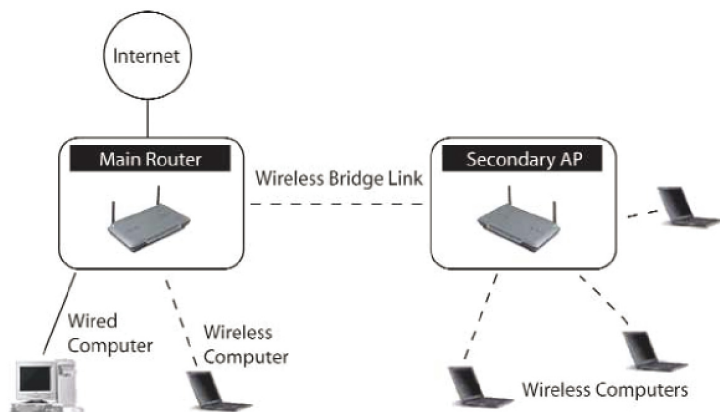
Setting Up Wireless Bridging

What is a Wireless Bridge?

A wireless bridge is actually a “mode” in which your Wireless Router can directly connect to a secondary wireless access point. Note that you can bridge your Wireless G Plus MIMO Router (model F5D9230-4) only to certain access points. Contact your technical-support representative for compatibility updates. You can use the bridge mode to extend the range of your wireless network, or add an extension of your network in another area of your office or home without running cables.

Range Extension

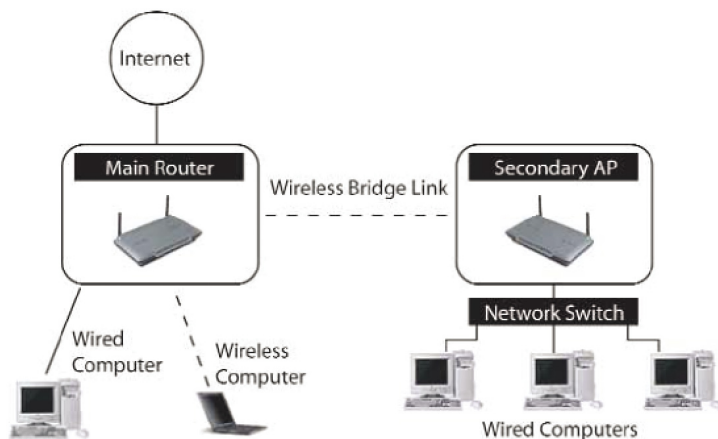
Range extension will extend the wireless-coverage area in your home or office. The example below illustrates use of bridging to extend the range of your wireless network. In this example, the Router is set up to connect to an access point located in another area. Laptops can roam, or move between the two wireless-coverage areas.



Using the Web-Based Advanced User Interface

Adding Another Network Segment Wirelessly

Bridging an access point to your Wireless Router allows you to add another network segment in another area in the home or office without running wires. Connecting a network switch or hub to the access point's RJ45 jack will allow a number of computers connected to the switch access to the rest of the network.

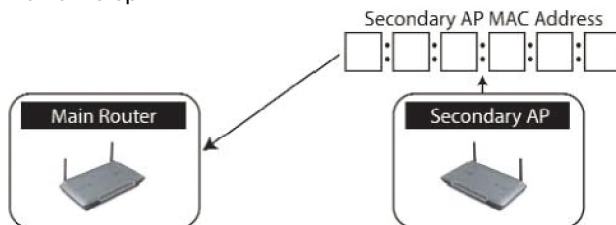


Setting Up a Bridge Between your Wireless Router and a Secondary Access Point

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

PLEASE BE SURE TO FOLLOW THE STEPS BELOW CAREFULLY.

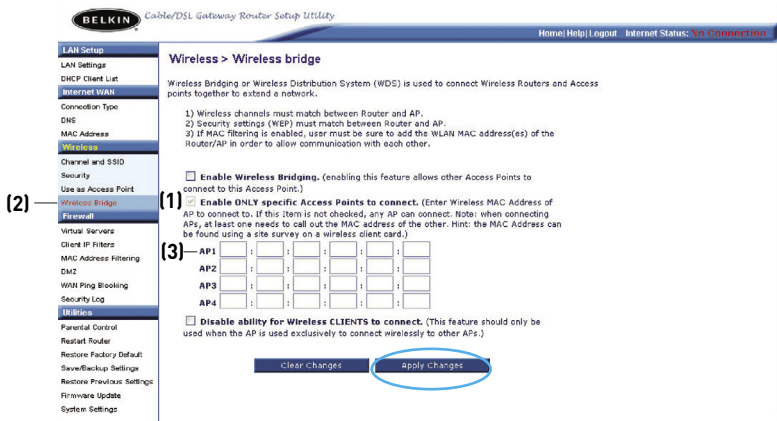
1. Set your access point to the same channel as the Router. By default, the Router and access-point channels are set to channel 11 at the factory. If you have never changed the channel, you don't need to do anything.
2. Find the access point's MAC address on the bottom label of the access point. There are two MAC addresses on the bottom label. You will need the MAC address named "WLAN MAC Address". The MAC address starts with 0030BD and is followed by six other numbers or letters (i.e., 0030BD-XXXXXX). Write the MAC address below. Go to the next step.



Enter the Secondary AP's MAC address into the Router

3. Place your secondary access point within range of your Wireless Router and near the area where you want to extend the range or add the network segment. Typically, indoor range should be between 50 and 150 feet.
4. Connect power to your access point. Make sure the access point is on and proceed to the next step.
5. From a computer already connected to your Router, access the Advanced Setup Utility by opening your browser. In the address bar, type in "192.168.2.1". Do not type in "www" or "http://" before the number. **Note: If you have changed your Router's IP address, use that IP address.**
6. You will see the Router's user interface in the browser window. Click "Wireless Bridge" (2) on the left-hand side of the screen. You will see the following screen.

Using the Web-Based Advanced User Interface



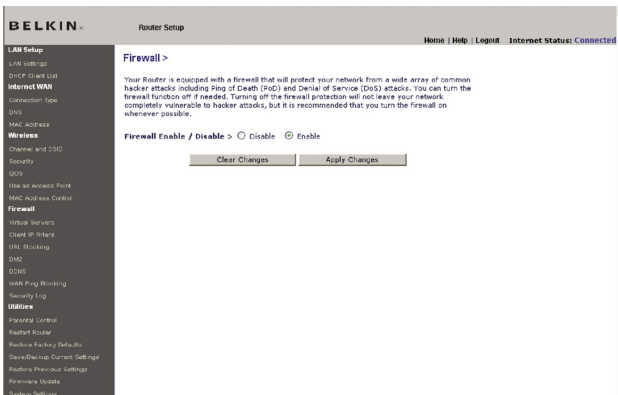
7. Check the box that says “Enable ONLY specific Access Points to connect” **(1)**.
8. In the field named “AP1” **(3)**, type in the MAC address of your secondary access point. When you have typed in the address, click “Apply Changes”.
9. Bridging is now set up.

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.



Using the Web-Based Advanced User Interface

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 web interface. The left sidebar contains a navigation menu with options like LAN Setup, DHCP Client List, Internet WAN, Connection Type, DNS, MAC Address, Wireless, Channel and SSID, Security, QoS, Host Address Control, MAC Address Control, Firewall, Virtual Servers, Client IP Filter, URL Blocking, DMZ, DMZ, Web Ping Blocking, Security Log, Utilities, Parental Control, Restore Router, Restore Factory Defaults, Restore Previous Settings, Deviceless Current Settings, Restore Previous Settings, External Media, and System Settings. The main content area is titled 'Firewall > Virtual Servers'. It includes a description: '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. Please Note'. Below the description are buttons for 'Clear Changes' and 'Apply Changes'. There is an 'Add' button with a dropdown menu for 'Active Worlds' and an 'Add' button. Below these is a 'Clear' button. A table with 6 columns (Enable, Description, Inbound Port, Type, Private IP address, Private Port) displays a list of virtual servers. The table has 14 rows, with the first row (index 1) showing 'Active Worlds' enabled, inbound port 80, TCP type, and private IP address 192.168.2.1. The last row (index 14) shows 'Active Worlds' disabled, inbound port 80, TCP type, and private IP address 192.168.2.1. A 'GO BACK TO LIST' button is at the bottom right.

| Enable | Description | Inbound Port | Type | Private IP address | Private Port |
|-----------------------------|---------------|--------------|------|--------------------|--------------|
| 1 <input type="checkbox"/> | Active Worlds | 80 | TCP | 192.168.2.1 | 80 |
| 2 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 3 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 4 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 5 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 6 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 7 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 8 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 9 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 10 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 11 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 12 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 13 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |
| 14 <input type="checkbox"/> | | | TCP | 192.168.2.1 | |

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: Connected

LAN Setup
[Link Settings](#)
[DHCP Client List](#)
[Internet WAN](#)
[Connection Type](#)
[DNS](#)
[MAC Address](#)
[Dynamic and Static](#)
[Security](#)
[QoS](#)
[Use as Access Point](#)
[NAT Address Control](#)
Firewall
[Virtual Servers](#)
[Client IP Filters](#)
[URL Blocking](#)
[Anti-DDoS](#)
[NAT Ping Blocking](#)
[Security Log](#)
Utilities
[Parental Control](#)
[Router Filter](#)
[Restore Factory Defaults](#)
[Save/Backup Current 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. *Note: Idle*

| IP | Port | Type | Block Time | Day | Time | Enable |
|--------------|------|--------------------|-----------------|------------|--------------------------|--------------------------|
| 192.168.2.22 | 80 | TCP UDP Both | Always Block | SUN SUN | 12:00 A.M. 12:00 A.M. | <input type="checkbox"/> |
| 192.168.2.22 | 80 | TCP UDP Both | Always Block | SUN SUN | 12:00 A.M. 12:00 A.M. | <input type="checkbox"/> |
| 192.168.2.22 | 80 | TCP UDP Both | Always Block | SUN SUN | 12:00 A.M. 12:00 A.M. | <input type="checkbox"/> |
| 192.168.2.22 | 80 | TCP UDP Both | Always Block | SUN SUN | 12:00 A.M. 12:00 A.M. | <input type="checkbox"/> |
| 192.168.2.22 | 80 | TCP UDP Both | Always Block | SUN SUN | 12:00 A.M. 12:00 A.M. | <input type="checkbox"/> |
| 192.168.2.22 | 80 | TCP UDP Both | Always Block | SUN SUN | 12:00 A.M. 12:00 A.M. | <input type="checkbox"/> |

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

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”.

| (1) IP | (2) Port | Type | Block Time | (5) Day | (6) Time | (9) Enable |
|--------------|----------|------|------------|---------|------------|-------------------------------------|
| 192.168.2.22 | 80 | Both | Block | SUN | 12:00 A.M. | <input checked="" type="checkbox"/> |
| | | | | SUN | 12:00 A.M. | |

(3) (4) (7) (8)

Using the Web-Based Advanced User Interface

URL Blocking

You can configure the Router to restrict access to predefined websites. URL-blocking will block LAN computers from connecting to these websites. Restriction can be set for a single website or multiple websites.

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

LAN Setup
LAN Settings
Router Client List
Internet WAN
Connection Type
DHCP
MAC Address
Wireless
Channel and ESSID
Security
QoS
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filter
URL Blocking
DMZ
DDoS
Web Ping Blocking
Security Log
Utilities
Firmware Control
Firmware Update
Restore Factory Defaults
Save/Backup Current Settings
Restore Previous Settings
Firmware Updates
System Settings

Firewall > URL Blocking
URL Blocking will block LAN computers to connect to predefined Websites.

(1) URL Blocking > ☐ Enable (2) (3)

| ID | URL | Enable |
|----|-----|--------------------------|
| 1 | | <input type="checkbox"/> |
| 2 | | <input type="checkbox"/> |
| 3 | | <input type="checkbox"/> |
| 4 | | <input type="checkbox"/> |
| 5 | | <input type="checkbox"/> |
| 6 | | <input type="checkbox"/> |
| 7 | | <input type="checkbox"/> |
| 8 | | <input type="checkbox"/> |
| 9 | | <input type="checkbox"/> |
| 10 | | <input type="checkbox"/> |
| 11 | | <input type="checkbox"/> |
| 12 | | <input type="checkbox"/> |
| 13 | | <input type="checkbox"/> |
| 14 | | <input type="checkbox"/> |
| 15 | | <input type="checkbox"/> |

You can also enable or disable the URL-blocking feature for the Router by checking or unchecking the “Enable” check box (1) on top of the page.

To restrict Internet access to a single website for example, click on the “Enable” check box (1) on top of the “URL Blocking” page. Then, enter the URL or IP address of the website to which you wish to restrict access in the URL field(s) (2) and check the “Enable” box (3) next to it. You can enable or disable specific URL-access rules by clicking on the “Enable” box (3), to activate or deactivate blocking for an indicated website.

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.

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

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
QoS
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
URL Blocking
DMZ
WAN
Web Page Blocking
Security Log
Utilities
Firewall Control
Reset Router
Restore Factory Defaults
Save/Backup Current 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 "Submit" for the change to take effect. [More Info](#)

IP Address of Virtual DMZ Host >

| Static IP | Private IP | Enable |
|--------------|-------------|-------------------------------------|
| 192.168.1.20 | 192.168.2.0 | <input checked="" type="checkbox"/> |

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

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

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

BELKIN Router Setup Home | Help | Logout Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address

Wireless
Channel and SSID
Security
WEP
Wireless Access Point
MAC Address Control

Firewall
Virtual Servers
Client IP Filter
URL Blocking
DMZ
DNS
Web Ping Blocking
Bandwidth
Utilities
Firmware Control
Restart Router
Restore Factory Defaults
Advanced Setup Current Settings
Restore Previous Settings
Firmware Updates
System Settings

Firewall > DDNS

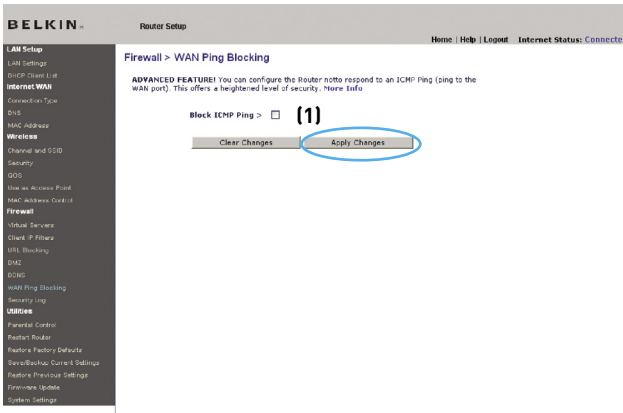
Dynamic DNS allows you to provide Internet users with a fixed domain name (instead of an IP address which may periodically change), allowing your router and applications set up in your router's virtual servers to be accessed from various locations on the Internet without knowing your current IP address. Your Wireless Router supports dynamic DNS through DynDNS.org (<http://www.dyndns.org>). You must create an account before using this service. [More Info](#)

User Name > **(1)**
Password > **(2)**
Domain Name > **(3)** **(4)**

Using the Web-Based Advanced User Interface

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.



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

Using the Web-Based Advanced User Interface

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 left sidebar contains a navigation menu with categories: LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area is titled 'Utilities >' and contains a description of the Utilities screen and a list of functions: Parental Control, Restart Router, Restore Factory Defaults, Save/Backup Current Settings, Restore Previous Saved Settings, and Firmware Update. The top navigation bar includes links for Home, Help, Logout, and Internet Status (Connected).

BELKIN Router Setup Home | Help | Logout Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
WAN
MAC Address
Wireless
Channel and SSID
Security
QoS
Web Set Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filter
URL Blocking
NAT
DMZ
ICNS
Web Ping Blocking
Security Log
Utilities
Parental Control
Restart Router
Restore Factory Defaults
Restore Current Settings
Restore Previous Settings
Firmware Update
System Settings

Utilities >

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

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

Parental Control

See the included Parental Control User Manual for more information on the Parental Control feature.

The screenshot shows the Belkin Router Setup interface, specifically the 'Utilities > Parental Control' section. The left sidebar is the same as the previous screenshot. The main content area is titled 'Utilities > Parental Control' and contains a description of the Parental Control feature and a 'Parental Control Sign-up' section with a 'Subscribe Now' button. The top navigation bar is the same as the previous screenshot.

BELKIN Router Setup Home | Help | Logout Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
WAN
MAC Address
Wireless
Channel and SSID
Security
QoS
Web Set Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filter
URL Blocking
DMZ
ICNS
Web Ping Blocking
Security Log
Utilities
Parental Control
Restart Router
Restore Factory Defaults
Restore Current Settings
Restore Previous Settings
Firmware Update
System Settings

Utilities > Parental Control

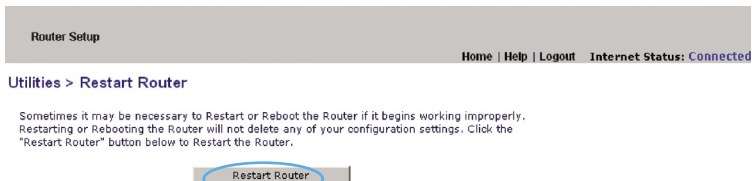
Belkin's Parental Control protects you and your children/employees from objectionable content on the web. Parental Control comes pre-configured to block many types of web content, but is custom configurable to be more or less restrictive. Any web site can easily be set to be either, always blocked, or always allowed.

Parental Control Sign-up
If you wish to sign up for Belkin's Parental Control feature, please click the button below

[Subscribe Now](#)

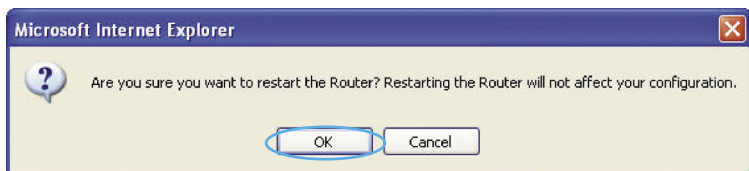
Restarting the Router

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.



Restarting the Router to Restore Normal Operation

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

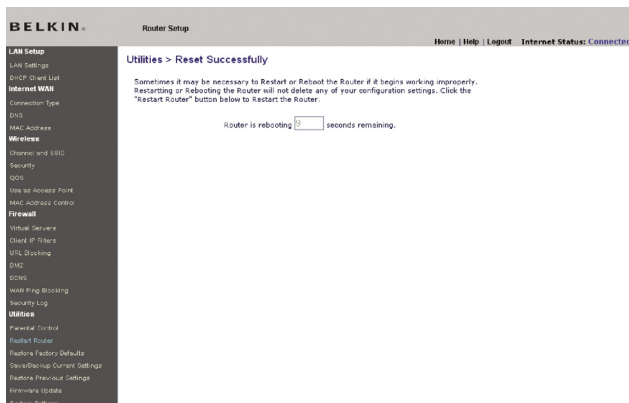


3. The following message will appear. Restarting the Router can take up to 60 seconds. It is important not to turn off the power to the Router during the restart. Click “OK”.



Using the Web-Based Advanced User Interface

4. A 12-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.



1

2

3

4

5

6

7

8

9

10

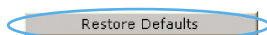
section

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.

Utilities > Restore Factory Defaults

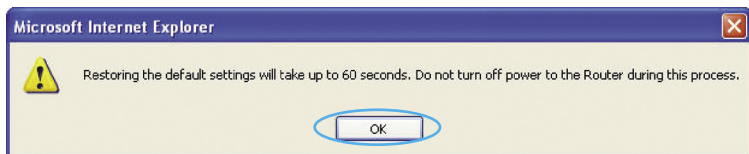
Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.



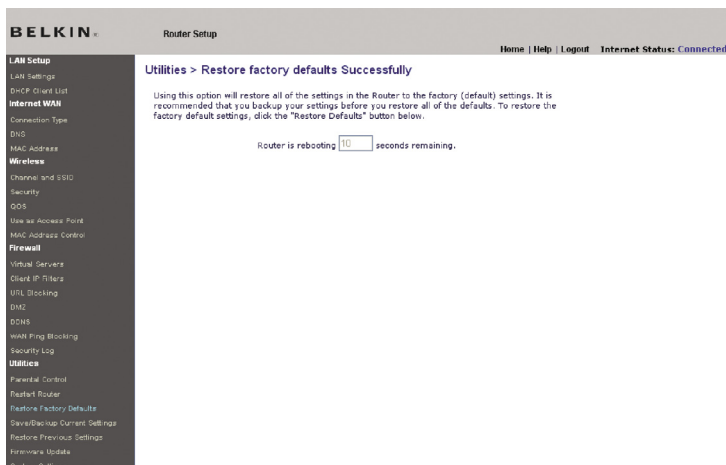
1. Click the "Restore Defaults" button.
2. The following message will appear. Click "OK".



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. Click "OK".



4. A 12-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.

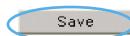


Saving a Current Configuration

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.

Utilities > Save/Backup Current Settings

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



1

2

3

4

5

6

7

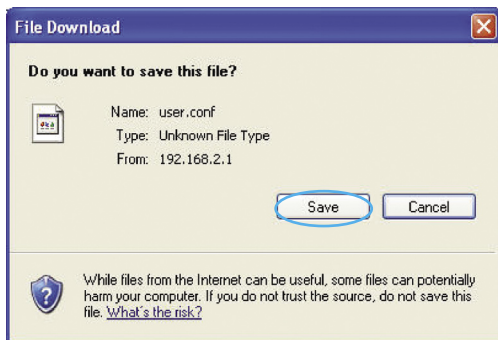
8

9

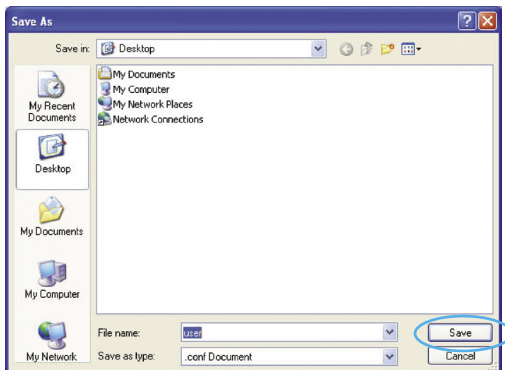
10

Using the Web-Based Advanced User Interface

1. Click “Save”. A window called “File Download” will open. Click “Save”.

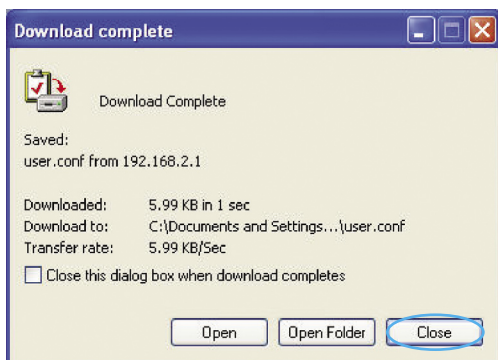


2. A window will open that allows you to select the location where you want to save the configuration file. Select a location. You can name the file anything you want, or use the default name “Config”. Be sure to name the file so you can locate it yourself later. When you have selected the location and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



Using the Web-Based Advanced User Interface

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



The configuration is now saved.

1

2

3

4

5

6

7

8

9

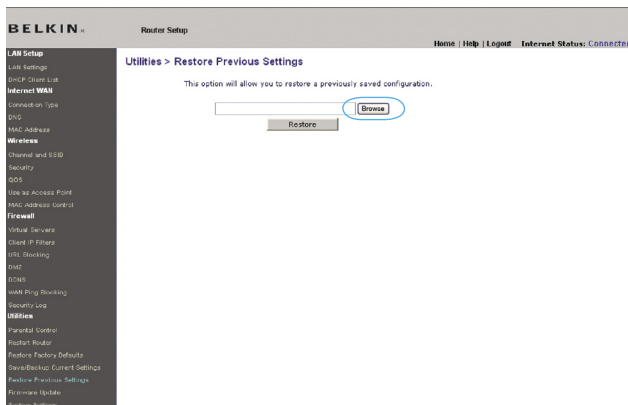
10

section

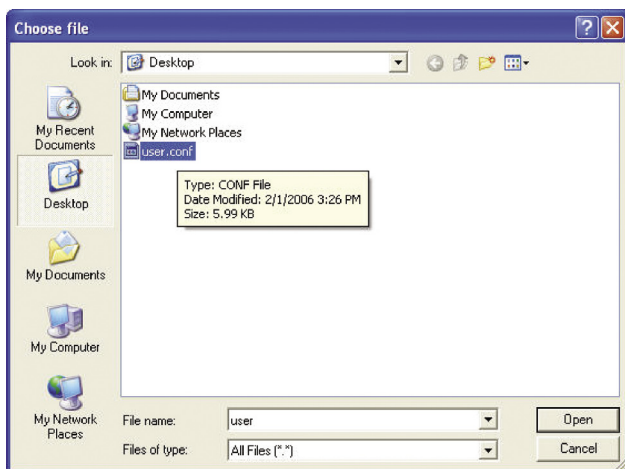
Using the Web-Based Advanced User Interface

Restoring a Previous Configuration

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



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



Using the Web-Based Advanced User Interface

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



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



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.

1

2

3

4

5

6

7

8

9

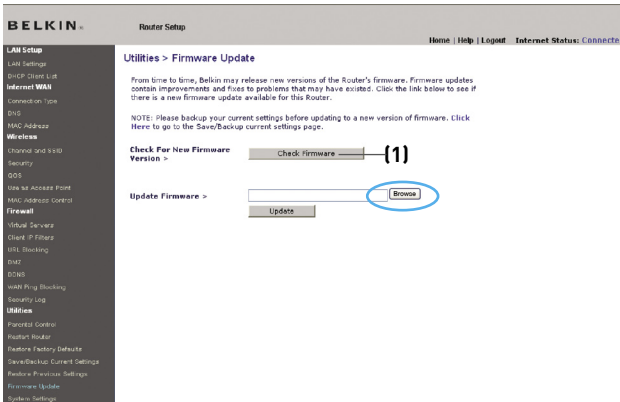
10

section

Using the Web-Based Advanced User Interface

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.

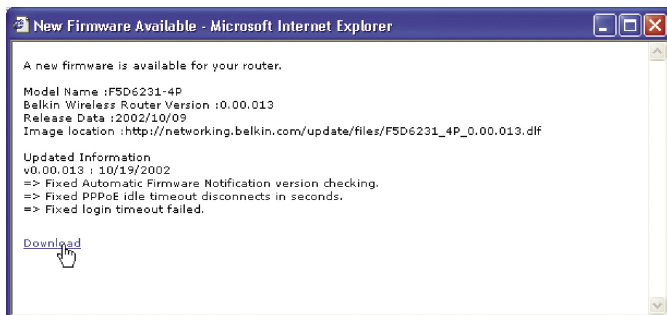


Checking for a New Version of Firmware

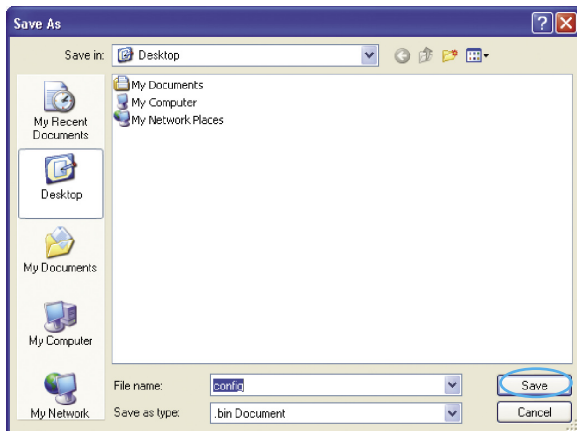
The “Check Firmware” (1) button allows you to instantly check for a new version of firmware. When you click the button, a new browser window will appear informing you that either no new firmware is available or that there is a new version available. If a new version is available, you will have the option 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:

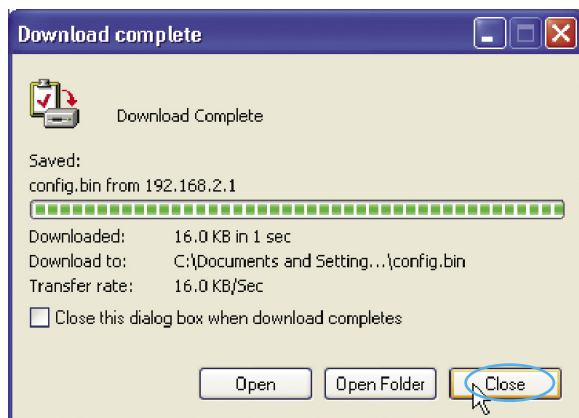


1. To download the new version of firmware, click “Download”.
2. A window will open that allows you to select the location where you want to save the firmware file. Select a location. You can name the file anything you want, or use the default name. Be sure to locate the file in a place where you can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



Using the Web-Based Advanced User Interface

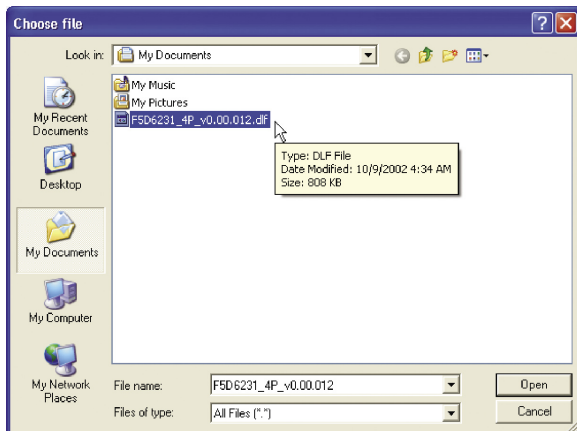
3. When the save is complete, you will see the following window. Click “Close”.



The download of the firmware is complete. To update the firmware, follow the next steps in “Updating the Router’s Firmware”.

Updating the Router's Firmware

1. In the “Firmware Update” page, click “Browse”. A window will open that allows you to select the location of the firmware update file.
2. Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.



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

Utilities > Firmware update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed. Click the link below to see if there is a new firmware update available for this Router.

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

Check For New
Firmware Version >

Check Firmware

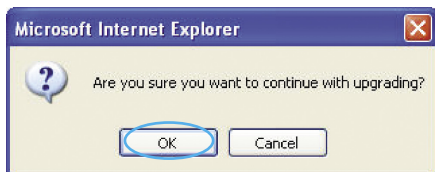
Update Firmware >

C:\Documents and Settings\h\ Browse...

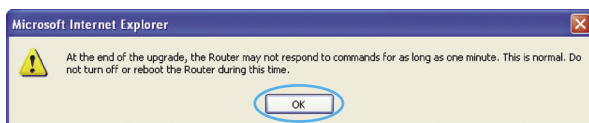
Update

Using the Web-Based Advanced User Interface

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



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



6. 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. If you wish to add a password for more security, you can set a password here. [More Info](#)

-Type in current Password >

-Type in new Password >

-confirm new Password >

-Login Timeout >

(1-9999 seconds)

Clear Changes

Apply Changes

Using the Web-Based Advanced User Interface

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.

The screenshot displays the 'Time and Time Zone' configuration page in a web browser. On the left is a dark sidebar with a menu containing: 'File Sharing', 'DMZ', 'QoS', 'WAN Ping Blocking', 'Security Log', 'Utilities', 'Parental Control', 'Product Router', 'Restore Factory Defaults', 'Save/Backup Current Settings', 'Restore Previous Settings', 'Firmware Update', and 'System Settings'. The main content area has a header showing the current time: 'Time and Time Zone: 2006年10月12日 上午 01:39:28'. Below this, it says 'Please set your time zone. If you are in an area that observes daylight saving check this box. More Info'. The 'Time Zone' is set to '(GMT-08:00) Pacific Time (US & Canada)' with a dropdown arrow. The 'Daylight Savings' section has a checked box for 'Automatically adjust Daylight Saving'. The 'Primary NTP Server' dropdown is open, showing a list of servers: '192.43.244.18-North America', '192.43.244.18-North America', '132.163.4.102-North America', '192.5.41.41-North America', '192.5.41.208-North America', '207.200.61.113-North America', '208.184.49.9-North America', '129.132.2.21-Europe', '130.149.17.8-Europe', and '137.189.6.174-Asia Pacific'. An 'Apply Changes' button is to the right of the list. Below the NTP servers is the 'Remote Management' section, which includes the text 'ADVANCED FEATURE! If you want to allow anyone on the Internet to manage your Router, please change the Administrator Password. MAKE SURE YOU HAVE SEEN THE MESSAGE!'. There are checkboxes for 'Any IP address can remotely manage the router.' and 'Only this IP address can remotely manage the router.' with an input field containing '80'. The 'Remote Access Port' is also set to '80'. There are 'Clear Changes' and 'Apply Changes' buttons at the bottom of this section. At the very bottom, there is a 'NAT Enabling' section with the text 'ADVANCED FEATURE! Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. More Info'.

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 80.

The screenshot displays the 'Remote Management' section of a Belkin Router's web-based Advanced User Interface. On the left, a sidebar contains links for 'Factory Defaults', 'Firmware Updates', 'System Settings', and 'Advanced Settings'. The main content area is titled 'Remote Management' and includes an 'ADVANCED FEATURE' warning: 'Remote management allows you to change 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'. Below this, there are two radio button options: 'Any IP address can remotely manage the router.' (which is selected) and 'Only this IP address can remotely manage the router >'. The second option is followed by four empty input fields for an IP address. A 'Remote Access Port >' label is followed by an input field containing the number '80'. At the bottom of this section are 'Clear Changes' and 'Apply Changes' buttons. The next section is 'NAT Enabling', with an 'ADVANCED FEATURE' warning: 'Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. More Info'. It includes a 'NAT Enable/Disable >' label and two radio buttons: 'Enable' (selected) and 'Disable'. It also has 'Clear Changes' and 'Apply Changes' buttons. The final section is 'UPNP Enabling', with an 'ADVANCED FEATURE' warning: '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'. It includes a 'UPNP Enable/Disable >' label and two radio buttons: 'Enable' (selected) and 'Disable'. It also has 'Clear Changes' and 'Apply Changes' buttons. At the very bottom, there is a link for 'Auto Update Firmware Enabling'.

Using the Web-Based Advanced User Interface

Enabling/Disabling NAT (Network Address Translation)

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

NAT Enabling:

ADVANCED FEATURE! Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. [More Info](#)

-NAT Enable/Disable >

☒ Enable ☐ Disable

Clear Changes

Apply Changes

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

Clear Changes

Apply Changes

Enabling/Disabling Auto Firmware Update

This innovation provides the Router with the built-in capability to automatically check for a new version of firmware and alert you that the new firmware is available. When you log into the Router's 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

1

2

3

4

5

6

7

8

9

10

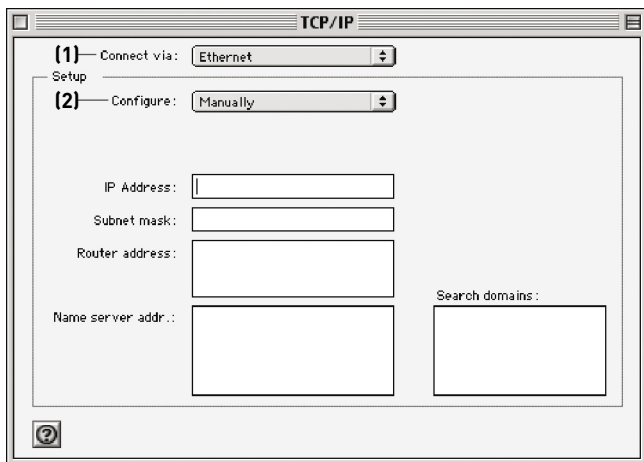
section

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).



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.

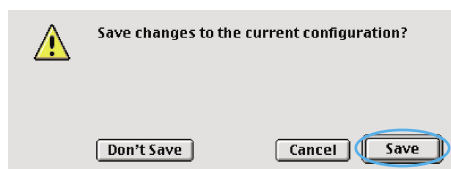
| | |
|----------------------|----------------------|
| IP address: | <input type="text"/> |
| Subnet Mask: | <input type="text"/> |
| Router Address: | <input type="text"/> |
| Name Server Address: | <input type="text"/> |

Manually Configuring Network Settings

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



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



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

1

2

3

4

5

6

7

8

9

10

section

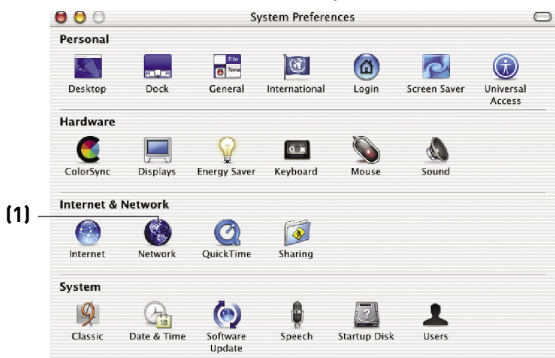
Manually Configuring Network Settings

Manually Configuring Network Settings in Mac OS X

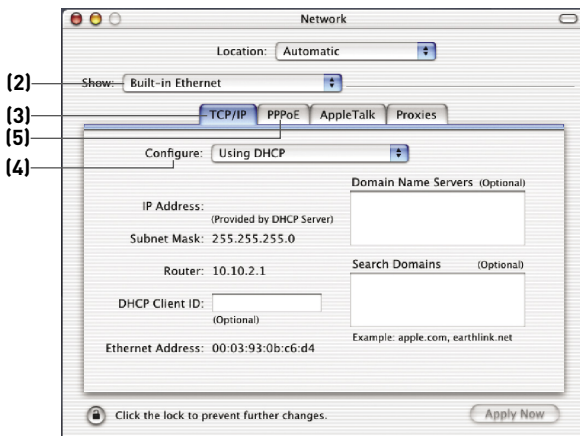
1. Click on the “System Preferences” icon.



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



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



Manually Configuring Network Settings

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"/> |

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.

1

2

3

4

5

6

7

8

9

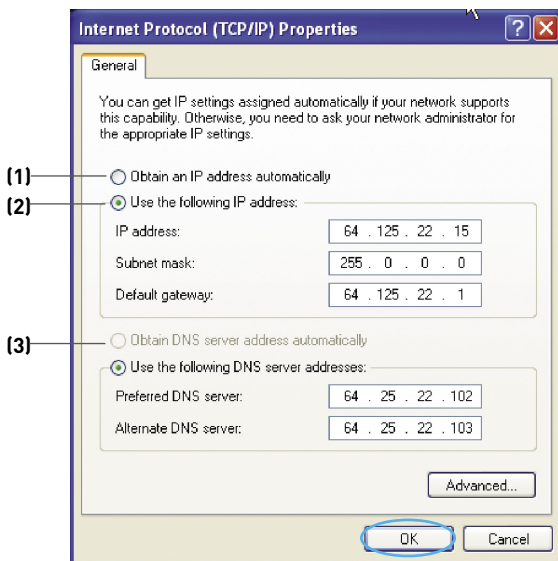
10

section

Manually Configuring Network Settings

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:



Manually Configuring Network Settings

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"/> |

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.

1

2

3

4

5

6

7

8

9

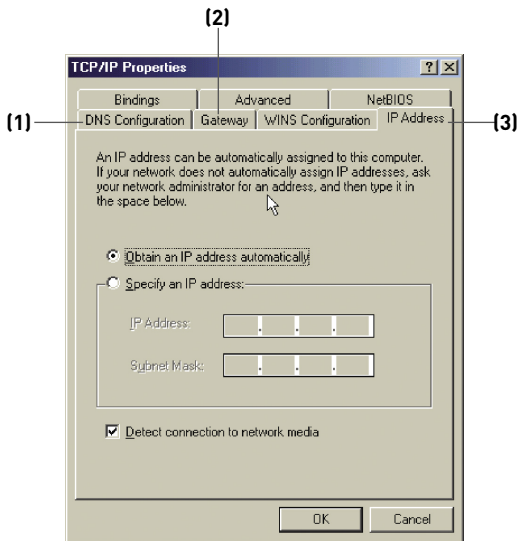
10

section

Manually Configuring Network Settings

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.



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.

Manually Configuring Network Settings

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"/> |

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.

1

2

3

4

5

6

7

8

9

10

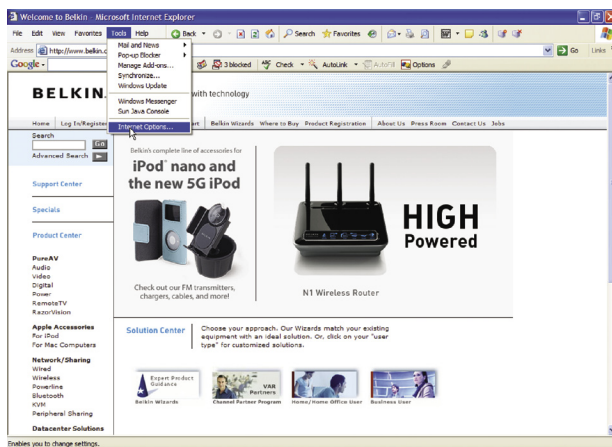
section

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.

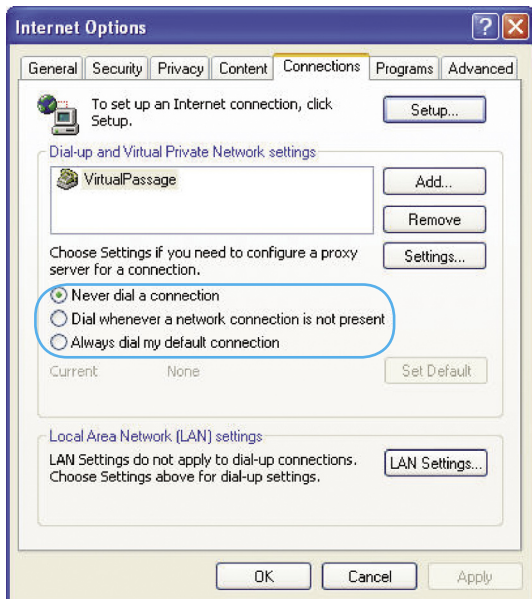
Microsoft® Internet Explorer 4.0 or Higher

1. Start your web browser. Select “Tools” then “Internet Options”.



Recommended Web Browser Settings

2. In the “Internet Options” screen, there are three selections: “Never dial a connection”, “Dial whenever a network connection is not present”, and “Always dial my default connection”. If you can make a selection, select “Never dial a connection”. If you cannot make a selection, go to the next step.



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

1

2

3

4

5

6

7

8

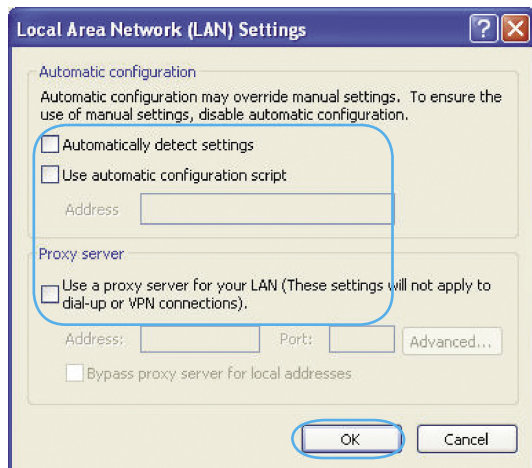
9

10

section

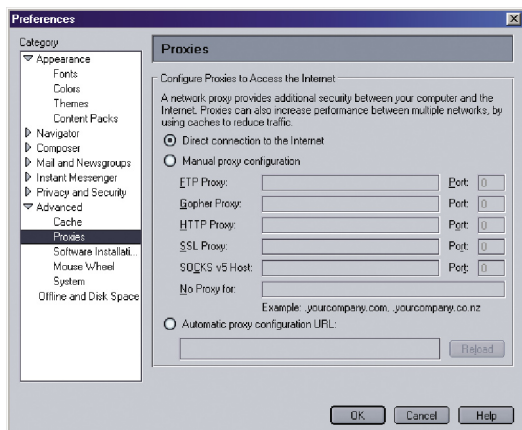
Recommended Web Browser Settings

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.



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”.



Problem:

Easy Install Wizard cannot find my Router.

Solution:

If the Easy Install Wizard is not able to find the Router during the installation process, please check the following items:

1. If the Easy Install Wizard 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 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 "Internet/WAN" on the back of the Router.

4. Try shutting down and restarting your computer, then rerunning the Easy Install Wizard.

If the Easy Install Wizard is still unable to find the Router, reference the section titled "Manually Configuring Network Settings" (page 98 of this User Manual) for installation steps.

Problem:

Easy Install cannot connect my Router to the Internet.

Solution:

If the Easy Install Wizard is not able to connect the Router to the Internet, please check the following items:

1. Use the troubleshooting suggestions within the Easy Install Wizard. If the troubleshooting screen does not open automatically, click on the “Troubleshoot” button in the lower, right-hand corner of the Easy Install Wizard 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 may 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 98 of this User Manual) for an alternative setup method.

Problem:

- **The Easy Install Wizard completed installation, but my web browser doesn’t work.**
- **I am unable to connect to the Internet. The “WAN” light on my Router is off, and the “Connected” light is blinking.**

Solution:

If you cannot connect to the Internet, and the “WAN” light is off, and the “Connected” 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 “Internet/WAN” 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 “WAN” 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 Easy Install Wizard completed installation, but my web browser doesn’t work.**
- **I am unable to connect to the Internet. The “WAN” light on my Router is on, and the “Connected” light is blinking.**

Solution:

1. If you cannot connect to the Internet, the “WAN” light is on, and the “Connected” light is blinking, the problem may be that your connection type may not match the ISP’s connection.
2. 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.
3. 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’s 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.
4. 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 Easy Install Wizard completed, but my web browser doesn’t work.**
- **I am unable to connect to the Internet. The “WAN” light on my Router is blinking, and the “Connected” light is solid.**

Solution:

1. If the “WAN” light is blinking, and the “Connected” 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.
2. 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.
3. 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 check the following items:

1. Look at the lights on your Router. If you're using a Belkin Router, the lights should be as follows:
 - The "Power" light should be on.
 - The "Connected" light should be on, and not blinking.
 - The "WAN Internet" light should be either on or blinking.
 - The "Wireless" light should be 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.



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 "Setting WEP Encryption" (page 60).
3. Within a few seconds, the tray icon in the lower, left-hand corner of your screen should turn green, indication of a successful connection to the network.

Problem:

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

Solution:

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

1. Temporarily move computer, if possible, five to 10 feet from the Router. Close the wireless utility, and 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 Wireless G Plus MIMO Router" of this User Manual.
2. Using a computer that is connected to the Router via a network cable (as opposed to wirelessly), ensure that "Broadcast SSID" is enabled. This setting is found on the Router's wireless "Channel and SSID" configuration page.

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

Problem:

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

Solution:

Wireless technology is radio-based, which means connectivity and the throughput performance between devices decreases when the distance between devices increases. Other factors that will cause signal degradation (metal is generally the worst culprit) are obstructions such as walls and metal appliances. 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 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 on page 54 entitled “Changing the Wireless Channel” 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:

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

Solution:

1. Log into your Wireless Router or (Access Point). 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 802.11g Access Point is 192.168.2.254.) Log into your Router by clicking on the "Login" button in the top right-hand corner of the screen. You will be asked to enter your password. If you never set a password, leave the "Password" field blank and click "Submit".

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 mixture of numbers and letters from A-F and 0-9. For 128-bit WEP, you need to enter 26 hex keys.

For example:

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

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.

Solution:

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

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

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

For example:

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

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

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

Problem:

Do Belkin products support WPA?

Solution:

You need to download the latest driver for your Belkin 802.11g Wireless 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> for the following products:

F5D7000, F5D7001, F5D7010, F5D7230-4, F5D7231-4, F5D7130, F5D9010, F5D9050, F5D9230-4

Problem:

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

Solution:

1. From the "Security Mode" drop-down menu, select "WPA-PSK (no server)".
2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key. 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 Wireless Protected Access (WPA) security on a Belkin wireless client card for a home network.

Solution:

Clients must use the same key that the Wireless Router (or access point) uses. For instance, if the key is "Smith Family Network Key" in the Wireless Router (or access point), the clients must also use that same key.

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

1

2

3

4

5

6

7

8

9

10

section

2. Once the “Advanced” button is clicked, the Belkin Wireless Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless 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 (no server).”
5. Type your WPA key in the “Network key” box.
Important: WPA-PSK is a mixture of numbers and letters from A-Z and 0-9. For WPA-PSK you can enter eight to 63 characters. This network key needs to match the key you assign to your Wireless Router (or access point).
6. Click “OK”, then “Apply” to save the settings.

Problem:

I am NOT using a Belkin client card for a home network and I am having difficulty setting up Wireless Protected Access (WPA) security.

Solution:

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

Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time. You also need to ensure that the wireless card’s 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

1. Under Windows XP, click “Start > Control Panel > Network Connections”.
2. Right-click on the “Wireless Networks” tab. Ensure the “Use Windows to configure my wireless network settings” check box is checked.
3. Under the “Wireless Networks” tab, click the “Configure” button.
4. For a home or small business user, select “WPA-PSK” under “Network Administration”.

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

5. Select “TKIP” or “AES” under “Data Encryption”. This setting will have to be identical to the Wireless Router (or access point) that you set up.

6. Type in your encryption key in the “Network key” box.

Important: Enter your 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.

Problem:

What is the difference between 802.11b, 802.11g, G Plus MIMO, and Pre-N?

Solution:

Currently there are four levels of wireless networking standards, which transmit data at very different maximum speeds. Each is based on the designation 802.11(x), so named by the IEEE, the board that is responsible for certifying networking standards. The most common wireless networking standard, 802.11b, transmits information at 11Mbps; 802.11a and 802.11g work at 54Mbps; G Plus MIMO works at 54Mbps; and Pre-N works at 108Mbps.

Wireless Comparison Chart

| Wireless Technology | 802.11b | G (802.11g) | G Plus (802.11g with HSM) | G Plus MIMO (802.11g with MIMO MRC) | N1 MIMO (draft 802.11n with MIMO) |
|----------------------|--|--|--|--|--|
| Speed* | 11Mbps link rate/baseline | 5x faster than 802.11b* | 10x faster than 802.11b* | 10x faster than 802.11b* | Wired speed over the air* |
| 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 | Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz |
| Compatibility | Compatible with 802.11g | Compatible with 802.11b/g | Compatible with 802.11b/g | Compatible with 802.11b/g | Compatible with draft 802.11n** and 802.11b/g |
| Coverage* | Typically 100–200 ft.* indoors | Up to 400 ft.* | Up to 700 ft.* | Up to 1,000 ft.* | Up to 1,400 ft.* |
| Advantage | Mature—legacy technology | Common—widespread use for Internet sharing | Enhanced speed and coverage | Better coverage and consistent speed and range | Leading edge—best coverage and throughput |

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

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

1

2

3

4

5

6

7

8

9

10

Technical Support

You can find technical support information at <http://www.belkin.com/networking> or www.belkin.com through the tech support area. If you want to contact technical support by phone, please call:

US: 877-736-5771 or 310-898-1100 ext. 2263

UK: 0845 607 77 87

Australia: 1800 235 546

New Zealand: 0800 235 546

Singapore: 800 616 1790

Europe: www.belkin.com/support

FCC Statement

DECLARATION OF CONFORMITY WITH FCC RULES FOR ELECTROMAGNETIC COMPATIBILITY

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

F5D9230-4

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

Caution: Exposure to Radio Frequency Radiation.

The radiated output power of this device is far below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such a manner that the potential for human contact during normal operation is minimized. When connecting an external antenna to the device, the antenna shall be placed in such a manner to minimize the potential for human contact during normal operation. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Federal Communications Commission Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

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

Modifications

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

1

2

3

4

5

6

7

8

9

10

Canada-Industry Canada (IC)

The wireless radio of this device complies with RSS 139 & RSS 210 Industry Canada. This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme à la norme NMB-003 du Canada.

Europe-European Union Notice

Radio products with the CE 0682 or CE alert marking comply with the R&TTE Directive (1995/5/EC) issued by the Commission of the European Community.

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

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

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

Products with the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage Directive (72/23/EEC) issued by the Commission of the European Community. Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards).

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

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

Belkin Corporation Limited Lifetime Product Warranty

What this warranty covers.

Belkin Corporation 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 Corporation 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 Corporation for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin Corporation 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 (other than lightning) such as flood, 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 Corporation at 501 W. Walnut St., Compton CA 90220, Attn: Customer Service, or call (800)-223-5546, within 15 days of the Occurrence. Be prepared to provide the following information:
 - a. The part number of the Belkin product.
 - b. Where you purchased the product.
 - c. When you purchased the product.
 - d. Copy of original receipt.
2. Your Belkin Customer Service Representative will then instruct you on how to forward your receipt and Belkin product and how to proceed with your claim.

Belkin Corporation reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin Corporation 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 Corporation, 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 Corporation 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 CORPORATION, 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 CORPORATION 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®

Wireless G Plus MIMO Router

BELKIN®

www.belkin.com

Belkin Tech Support

US: 877-736-5771

310-898-1100 ext. 2263

UK: 0845 607 77 87

Australia: 1800 235 546

New Zealand: 0800 235 546

Singapore: 800 616 1790

Europe: www.belkin.com/support

Belkin Corporation

501 West Walnut Street

Los Angeles, CA 90220-5221, USA

310-898-1100

310-898-1111 fax

Belkin Ltd.

Express Business Park, Shipton Way

Rushden, NN10 6GL, United Kingdom

+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

© 2006 Belkin Corporation. 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, NT, and Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.