BELKIN®

Wireless G Router

User Manual

F5D7230-4

Table of Contents

Introduction

Thank you for purchasing the Belkin Wireless G Router (the Router). The following two short sections discuss the benefits of home networking and outline best practices for maximizing 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 Router for Optimal Performance" on page 2.

Benefits of a Home Network

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

Advantages of a Wireless Network

Mobility – you 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 – the Belkin Setup Assistant Software makes setup simple

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

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

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

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

Placement of your Router for Optimal Performance

Important Factors for Placement and Setup

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

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

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

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

1. **Wireless Router Placement**
   Place your Router, the central connection point of your network, as close as possible to the center of your wireless network devices.

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

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

2. Avoid Obstacles and Interference

Avoid placing your Router near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

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

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

3. Cordless Phones

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

- Try moving cordless phones away from the Router and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check the manufacturer's information). If this fixes the problem, your phone may be interfering.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Router to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz 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 or card to locate any other wireless networks that are available (see your wireless adapter's or card's user manual), and move your Router and computers to a channel as far away from other networks as possible.

- Experiment with more than one of the available channels in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices.
- For Belkin wireless networking products, use the detailed Site Survey and wireless channel information included with your Wireless Network Card. See your Network Card's user guide for more information.

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

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

US:	**877-736-5771**
	800-223-5546 ext. 2263
	310-898-1100 ext. 2263
UK:	**0845 607 77 87**
Australia:	**1800 235 546**
New Zealand:	**0800 235 546**
Singapore:	**65 64857620**
Europe:	**www.belkin.com/support**

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 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® 9.x, X v10.x, AppleTalk®, Linux®, Windows® 98, Me, NT®, 2000, XP, Vista®, 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 IP addresses to your Internet service account.

SPI Firewall

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

Integrated 10/100 4-Port Switch

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

Universal Plug-and-Play (UPnP) Compatibility

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

Support for VPN Pass-Through

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

Built-In Dynamic Host Configuration Protocol (DHCP)

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

Setup Assistant Software

The Setup Assistant Software 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 Wireless Router will be up and running on the Internet.

NOTE: Setup Assistant Software software is compatible with Windows 98SE, Me, 2000, XP, Vista, and Mac OS 9.X and Mac OS X. If you are using another operating system, the Wireless Router can be set up using the Alternate Setup Method described in this User Manual (see page 24).

Integrated 802.11g Wireless Access Point

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

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.

Package Contents

- Belkin Wireless G Router
- Quick Installation Guide
- Belkin Setup Assistant Software CD with User Manual
- Belkin RJ45 Ethernet Networking Cable
- Power Supply

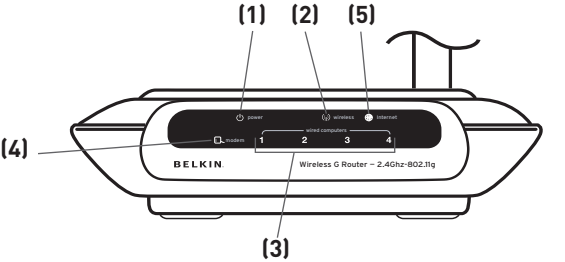
System Requirements

- 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

Setup Assistant Software System Requirements

- A PC running Windows 2000, XP, or Vista, or a Mac computer running Mac OS 9.x or OS X
- Minimum 64MB RAM
- Internet browser

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



1. 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

2. Wireless Network LED

OFF	Wireless Network is OFF
Green	Wireless Network is Ready
Blinking	Indicates Wireless Activity

3. 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. GREEN means a 10/100Base-T device is connected. When information is being sent over the port, the LED blinks rapidly.

OFF	No Device is Linked to the Port
Green	10/100Base-T Device Connected
Blinking (Orange or Green)	Port Activity

4. Modem Status LED

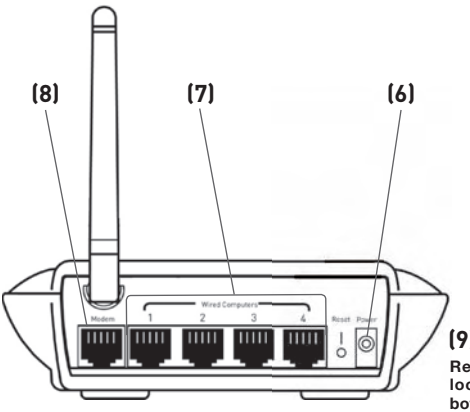
This LED lights in GREEN to indicate that your modem is connected properly to the Router. It blinks rapidly when information is being sent over the port between the Router and the modem.

OFF	No WAN Link
Solid Green	Good WAN Link
Blinking Green	WAN Activity

5. Internet 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



6. **Power Jack**
   Connect the included 5V DC power supply to this jack.

7. **Connections to Computers (Wired Computer Ports)—Gray**
   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.

8. **Connection to Modem (Modem Port)—Yellow**
   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.

9. **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 Router
- Quick Installation Guide
- Belkin Setup Assistant Software CD with User Manual
- RJ45 Ethernet Networking Cable (for connection of the Router to the computer)
- Power Supply

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

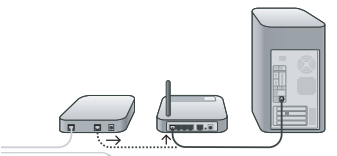
ALWAYS INSTALL YOUR ROUTER FIRST! IF YOU ARE INSTALLING NUMEROUS NETWORK DEVICES FOR THE FIRST TIME, IT IS IMPORTANT THAT YOUR ROUTER IS CONNECTED AND RUNNING BEFORE ATTEMPTING TO INSTALL OTHER NETWORK COMPONENTS SUCH AS NOTEBOOK CARDS AND DESKTOP CARDS.

Setup Assistant

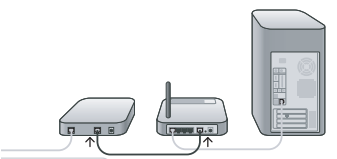
Belkin has provided our Setup Assistant software to make installing your Router a simple and easy task. You can use it to get your Router up and running in minutes. The Setup Assistant requires that your Windows 2000/XP or Vista computer be connected directly to your cable or DSL modem and that the Internet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

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

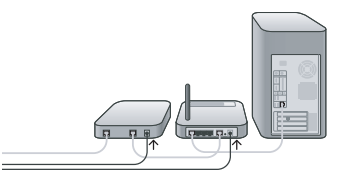
A. Unplug your modem's power cord. Put the Router next to the modem. Raise the Router's antennas.



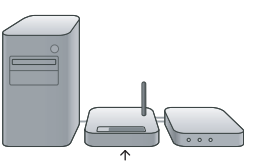
B. Locate the networking cable that connects your modem and computer. Unplug that cable from your modem, and plug it into any gray port on the back of the Router.



C. 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.



D. 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.



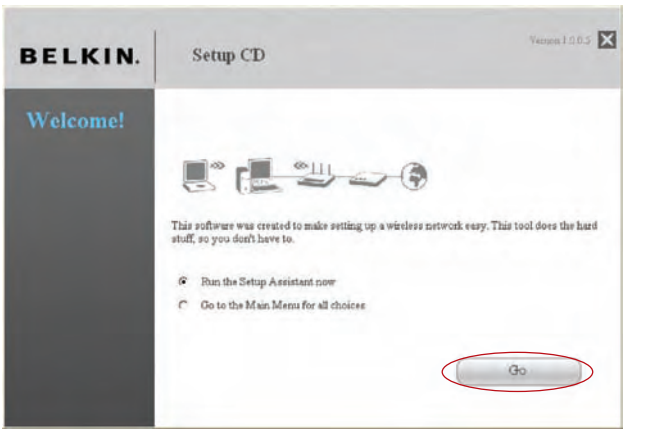
E. Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the "Wired" and "Router" icons are lit up in blue. If they are not, recheck your connections.

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

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

B. Insert the CD into your computer. The Setup Assistant will automatically appear on your computer's screen within 15 seconds. Click on "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 – B.



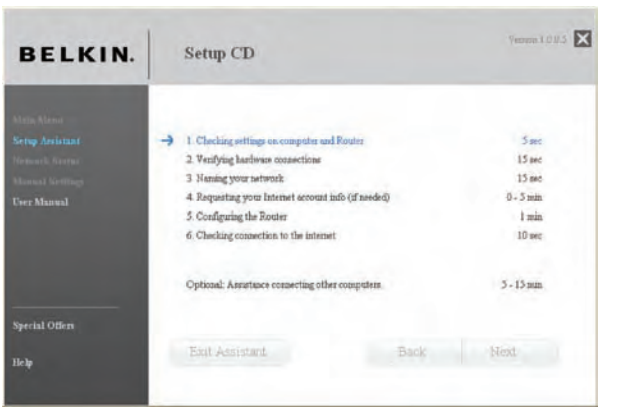
Note for Windows Users: If the Setup Assistant does not start up automatically, select your CD-ROM drive from "My Computer" and double-click on the file named "SetupAssistant" to start the Setup Assistant.

Confirmation Screen

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

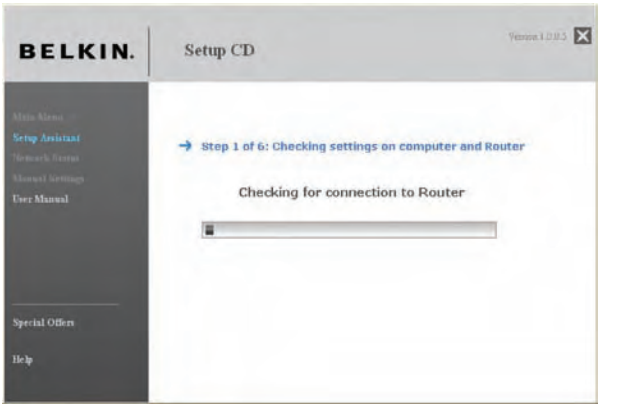
Progress Screen

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



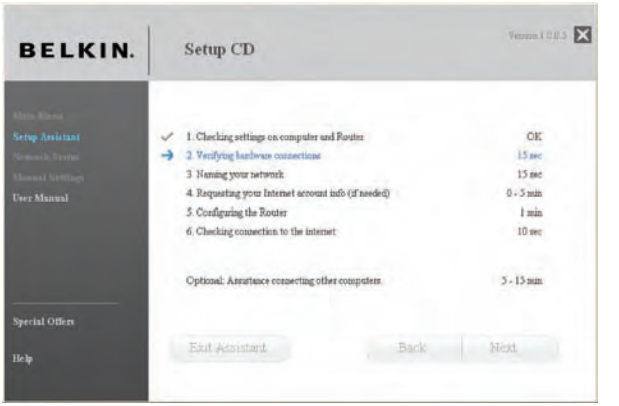
1.1 Checking Settings

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



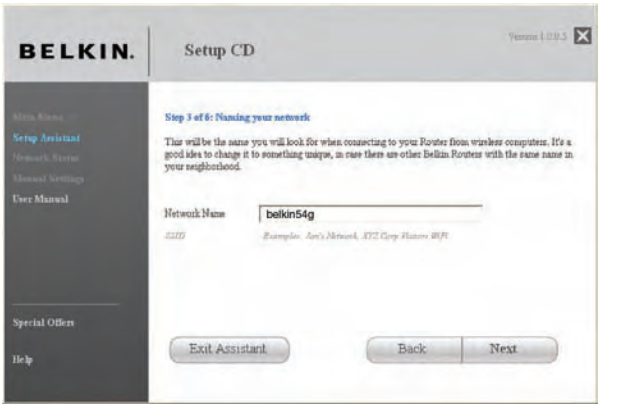
1.2 Verifying Hardware Connections

The Setup Assistant will now verify your hardware connection.



1.3 Naming your Wireless Network

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



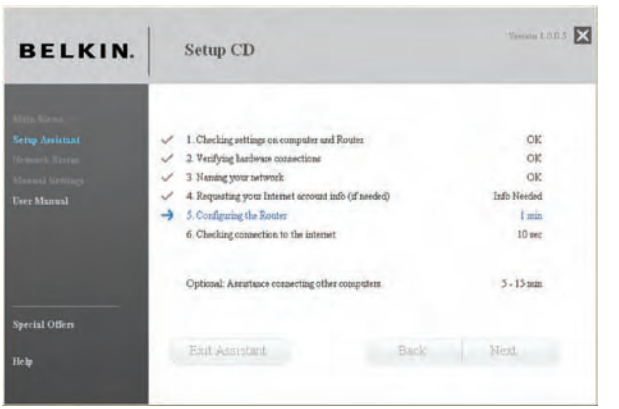
1.4 Requesting Internet Account Info (if needed)

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.

1.5 Configuring the Router

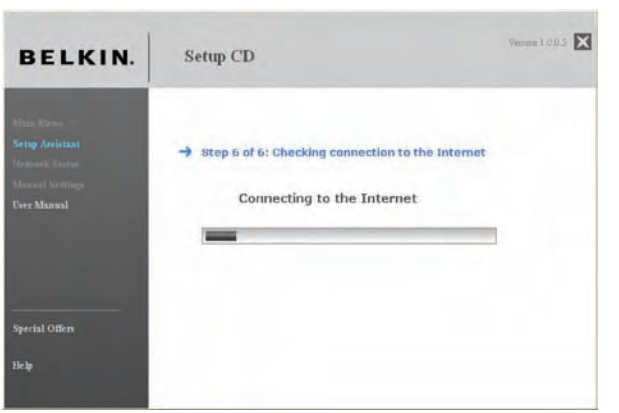
The Setup Assistant will now configure your Router by sending data to the Router and restarting it. Wait for the on-screen instructions.

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



1.6 Checking Internet Connection

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

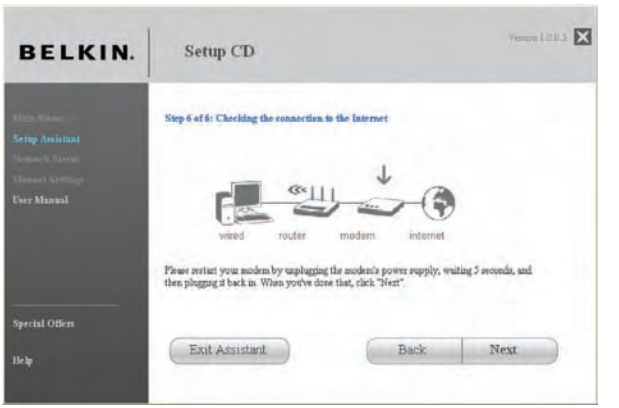


Congratulations
You have finished installing your new Belkin Router. You will see the Congratulations screen when your Router can connect to the Internet. You can begin surfing by opening your browser and going to any website.

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

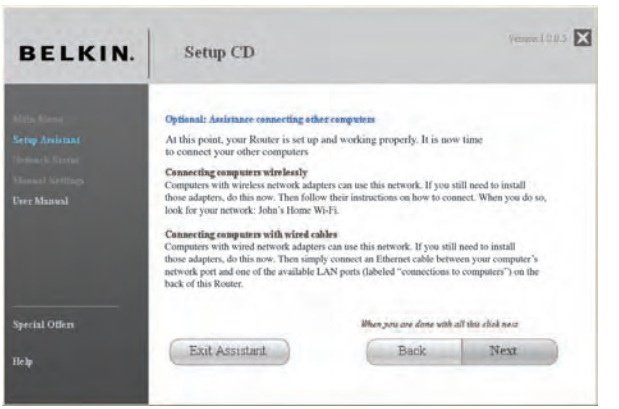
Troubleshooting

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



1.7 Optional: Assistance Connecting Other Computers

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



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.

Alternate Setup Method

The Web-Based Advanced User Interface is a web-based tool that you can use to set up the Router if you don't want to use the Setup Assistant. You can also use it to manage advanced functions of the Router. From the Web-Based Advanced User Interface, you can perform the following tasks:

- View the Router's current settings and status
- Configure the Router to connect to your ISP with the settings that they provided you
- Change the current network settings such as the Internal IP address, the IP address pool, DHCP settings, and more
- Set the Router's firewall to work with specific applications (port forwarding)
- Set up security features such as client restrictions, MAC address filtering, WEP, and WPA
- Enable the DMZ feature for a single computer on your network
- Change the Router's internal password
- Enable/Disable UPnP (Universal Plug-and-Play)
- Reset the Router
- Back up your configuration settings
- Reset the Router's default settings
- Update the Router's firmware

Step 1 | Connect your Router

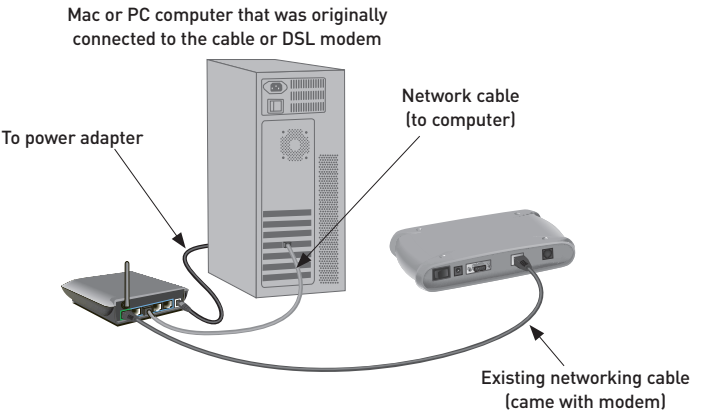
1.1 Turn off the power to your modem by unplugging the power supply from the modem.

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 "Modem".

1.4 Connect a new network cable (not included) from the back of the computer to one of the wired computers 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.



Note: Your Router may have ports in different locations than depicted in the illustration above.

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.

1.7 Verify that your modem is connected to the Router by checking the lights on the front of the Router. The green light labeled "Modem" should be ON if your modem is connected correctly to the Router. If it is not, recheck your connections.

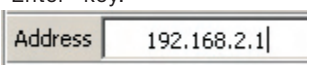
1.8 Verify that your computer is connected properly to the Router by checking the lights labeled "1–4". The light that corresponds to the numbered port connected to your computer should be ON if your computer is connected properly. If it is not, recheck your connections.

Step 2 | Set up 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 | Configure 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" (you do not need to type in anything else such as "http://" or "www"). Then press the "Enter" key.



PLEASE NOTE: If you have difficulty accessing the Router's Web-Based Advanced User Interface, go to the section entitled "Manually Configuring Network Settings".

Logging into the Router

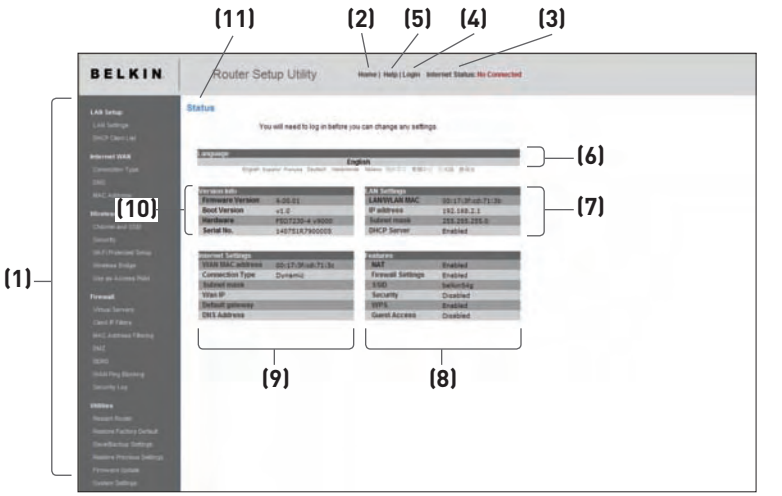
You will see the Router's home page in your browser window. The home page is visible to any user who wants to see it. To make any changes to the Router's settings, you have to log in. Clicking the "Login" button or clicking on any one of the links on the home page will take you to the login screen. The 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 1 to 99 minutes. For more information, see the section in this manual entitled "Changing the Login Time-Out Setting".

Using the Web-Based Advanced User Interface

The home page is the first page you will see when you access the Web-Based 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 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 UI, 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.

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. Language

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

7. 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.

8. 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.

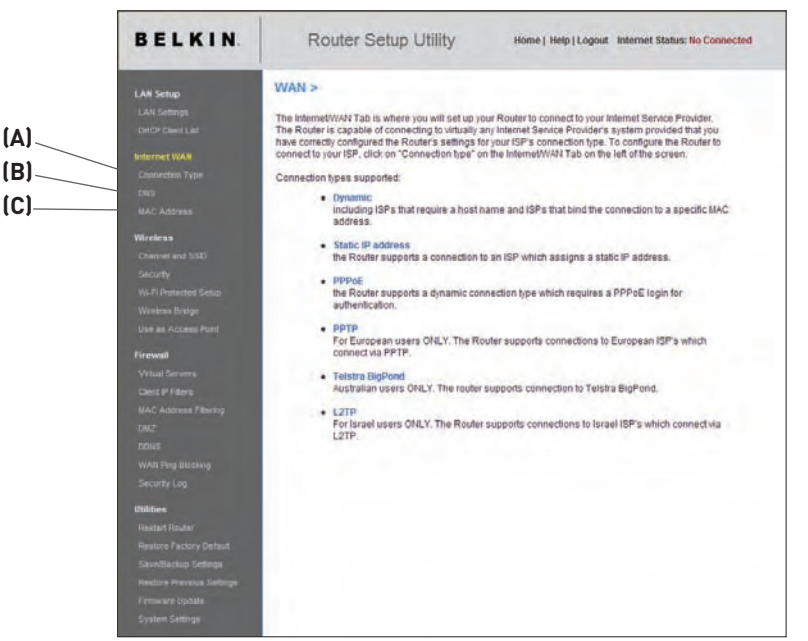
9. Internet Settings
Shows the settings of the Internet/WAN side of the Router that connects to the Internet. Changes to any of these settings can be made by clicking on the links or by clicking on the “Internet/WAN” “Quick Navigation” link on the left side of the screen.

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

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

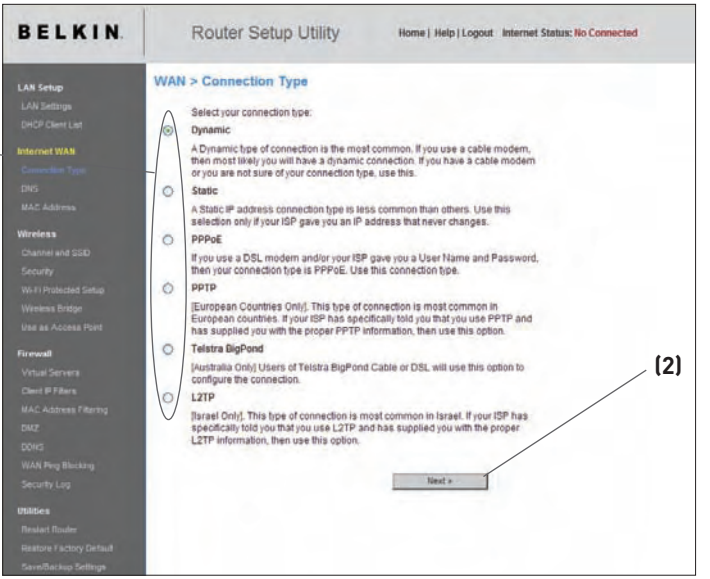
Step 4 | Configure your Router for Connection to your Internet Service Provider (ISP)

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.



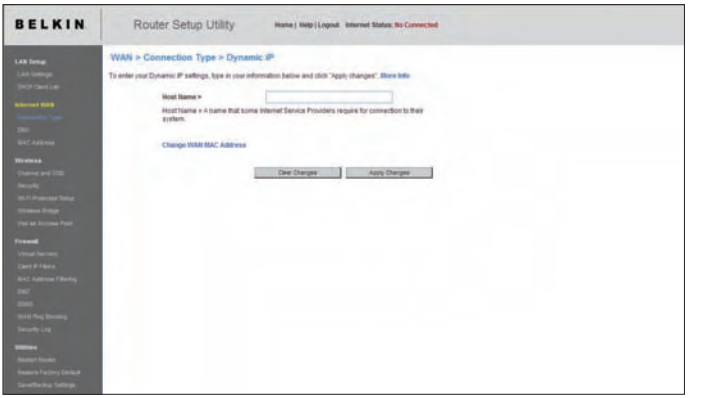
Setting your Connection Type

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)**.



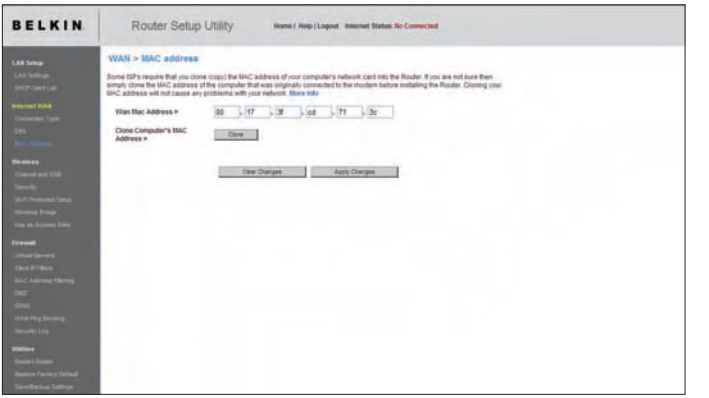
Setting your Internet Service Provider (ISP) Connection Type to Dynamic IP

A dynamic connection type is the most common connection type used 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.



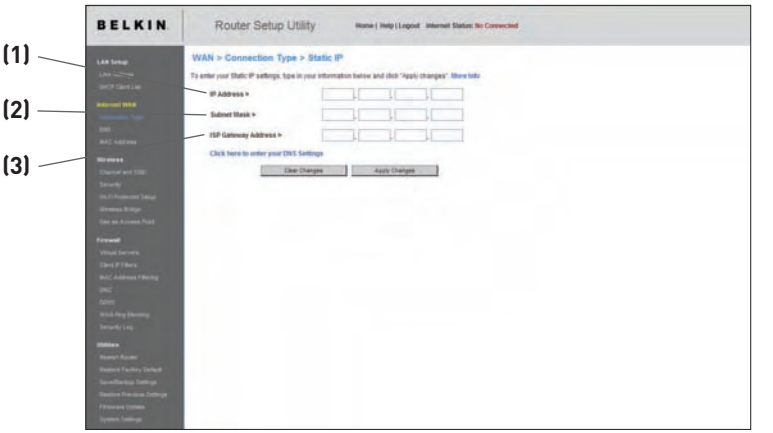
Change WAN MAC Address

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 **(1)**, subnet mask **(2)**, and ISP gateway address **(3)**. 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". 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.

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 Enternet300 that you use to connect to the Internet; or

3) You have to double-click on a desktop icon other than your browser to get on the Internet.

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 re-type it into the “Retype Password” box to confirm it.

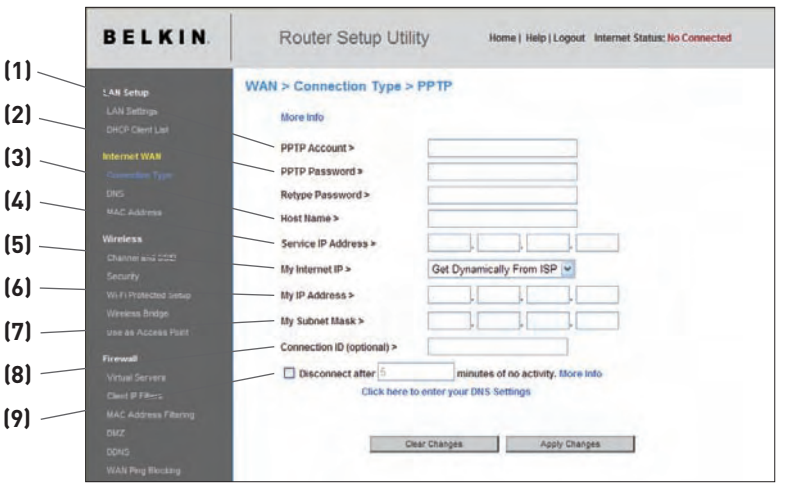
3. **Service Name**
   A service name is rarely required by an ISP. If you are not sure if your ISP requires a service name, leave this blank.

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

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 the information provided by your ISP in the space provided. When you have finished, click "Apply Changes". After you apply the changes, the "Internet Status" indicator will read "connection OK" if your Router is set up properly.



1. **PPTP Account**
   Provided by your ISP. Enter your PPTP User ID 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. **Service IP Address**
   Provided by your ISP. Enter your PPTP gateway/service IP address here.

5. My Internet IP
Select a type of getting your Internet IP address from your ISP server. It depends on your ISP service type. If you are not sure of this, please contact your ISP's technical-support hotline.

6. My IP Address
Provided by your ISP. Enter the IP address here.

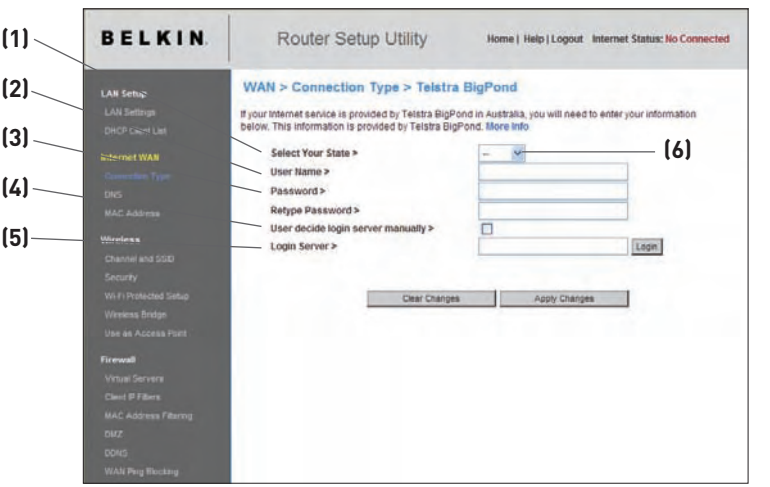
7. My Subnet Mask
Provided by your ISP. Enter the IP address here.

8. Connection ID
Provided by your ISP. Enter the connection ID here.

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

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



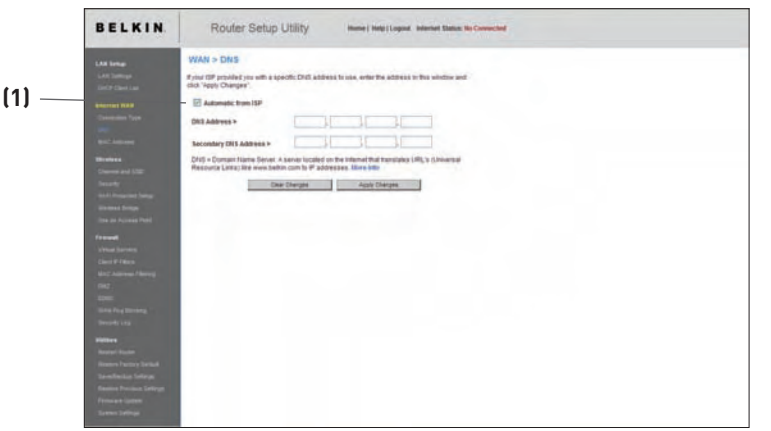
1. **Select your State**
   Select your state from the drop-down menu **(6)**. The "Login Server" box will automatically be filled in with an IP address. If for some reason this address does not match the address that Telstra has given, you can manually enter the login server address. See "User decide 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 typing 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 Locators (URLs) like "www.belkin.com" into 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" to save the settings.



Configuring your WAN Media Access Controller (MAC) Address

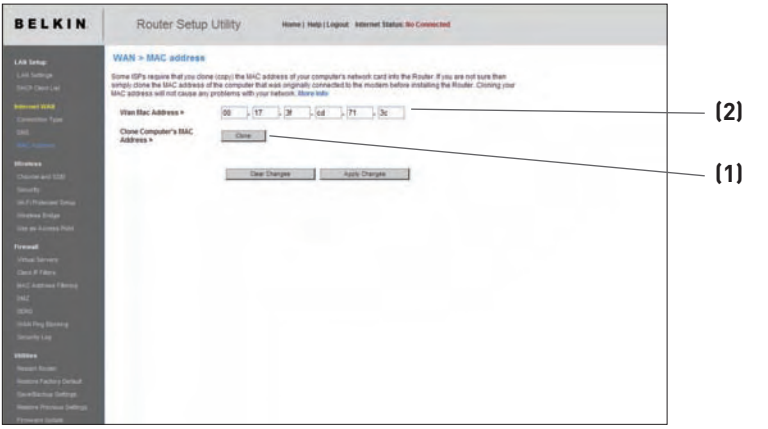
All network components including cards, adapters, and routers, have a unique “serial number” called a MAC address. Your Internet Service Provider may record the MAC address of your computer’s adapter and only let that particular computer connect to the Internet service. When you install the Router, its 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 “Clone” button **(1)**. Click “Apply Changes”. Your MAC address is now cloned to the Router.

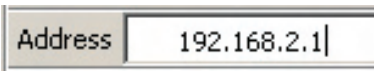
Entering a Specific MAC Address

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



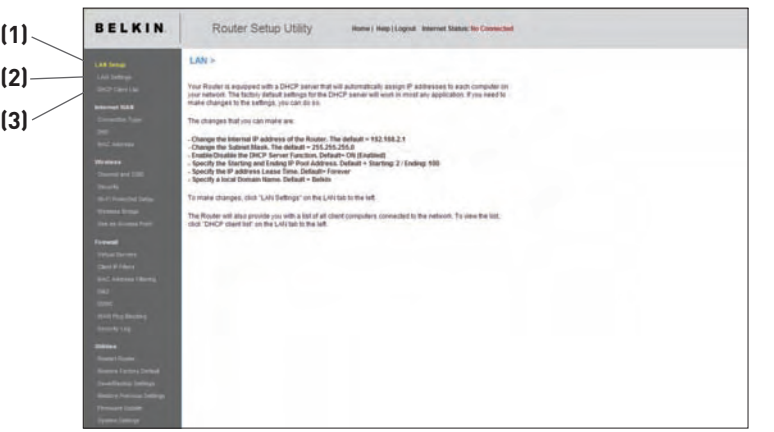
Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (do not type in anything else such as "http://" or "www"), then press the "Enter" key.

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



Viewing the LAN Settings

Clicking on the header of the "LAN Setup" tab **(1)** will take you to its 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)**.



Changing LAN Settings

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

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 Web-Based Advanced User 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), and 10.x.x.x (where x is any number 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

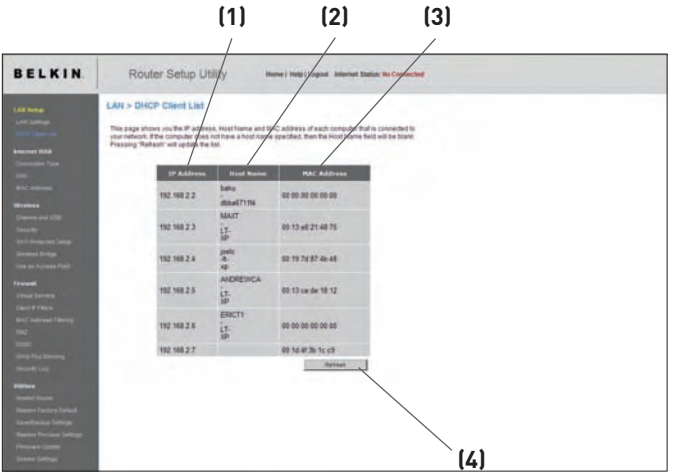
The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to “Forever”. The default setting is “Forever”, meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular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

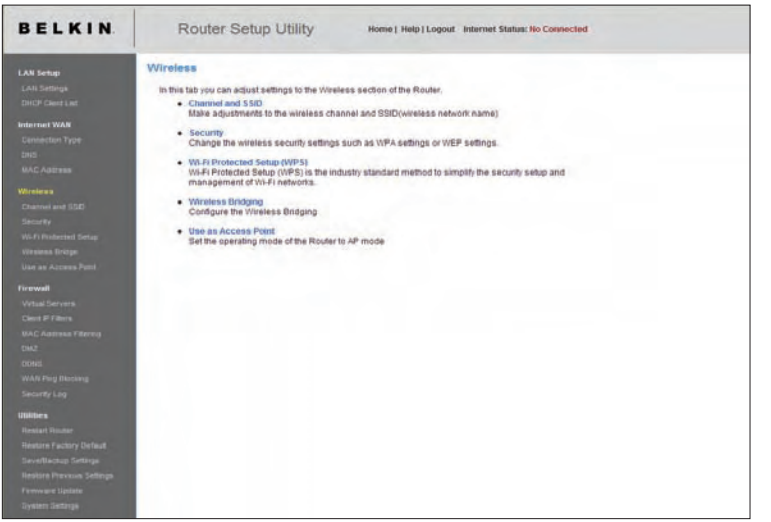
Viewing the DHCP Client List Page

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.



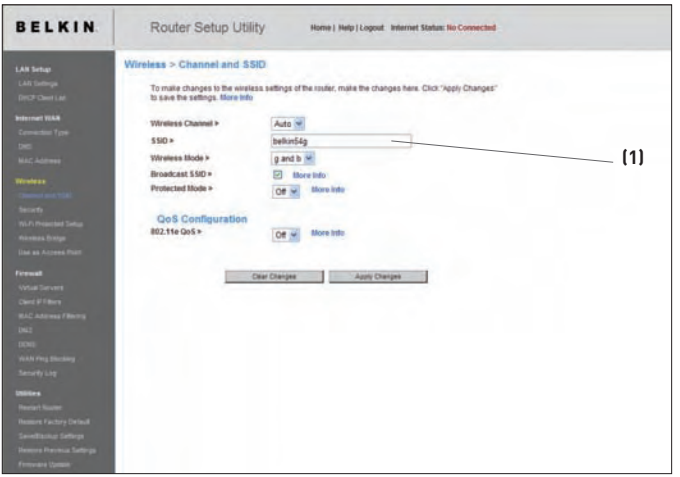
Configuring the Wireless Network Settings

Clicking on the header of the “Wireless” tab will take you to the “Wireless” header page. Under the “Wireless” tab, there are links that allow you to make changes to the wireless network settings.



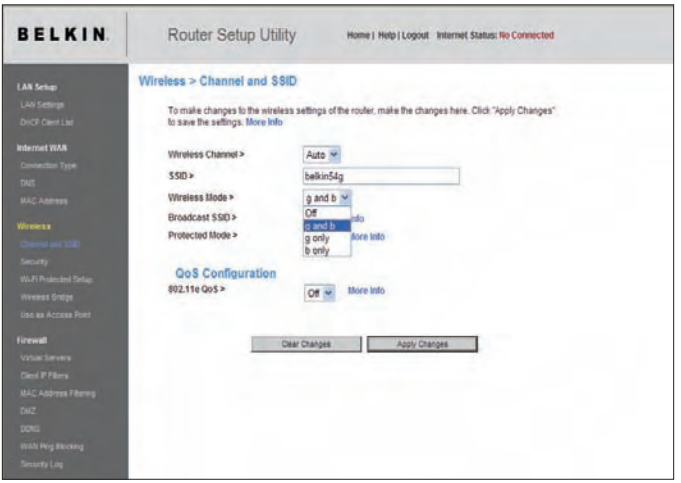
Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. The default SSID of the Router is “belkin54g”. You can change this to anything you want to or you can leave it unchanged. If there are other wireless networks operating in your area, you will want to make sure that your SSID is unique (does not match that of another wireless network in the area). To change the SSID, type the SSID that you want to use in the “SSID” field (**1**) and click “Apply Changes”. The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.



Using the Wireless Mode Switch

Your Router can operate in four different wireless modes: “off”, “g and b”, “g only”, and “b only”. The different modes are explained on the next page.



g and b Mode

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

g only Mode

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

b only Mode

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

When to use b only Mode

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

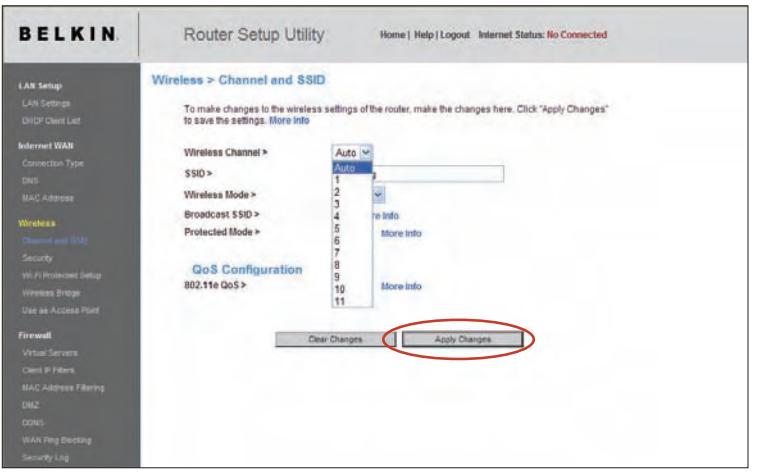
QoS (Quality of Service) Configuration

QoS prioritizes important data on your network such as multimedia content and Voice over IP (VoIP) so it will not be interfered with by other data being sent over the network. Based on 802.11e, you can turn this feature on or off by selecting it from the drop-down menu and choosing the acknowledgement mode you want to use. If you plan to stream multimedia content or use VoIP on your network, we recommend that you enable the QoS feature.

Changing the Wireless Channel

There are a number of operating channels you can choose from. In the United States, there are 11 channels. In Australia, 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 default channel is 11 (unless you are in a country that does not allow channel 11). The channel can be changed if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks. For best performance, use a channel that is at least five channels away

from the other wireless network. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. To change the channel, select the channel from the drop-down list. Click “Apply Changes”. The change is immediate.



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

As part of the 802.11g specification, Protected mode ensures proper operation of 802.11g clients and access points when there is heavy 802.11b traffic in the operating environment. When Protected mode is ON, 802.11g scans for other wireless network traffic before it transmits data. Therefore, using this mode in environments with HEAVY 802.11b traffic or interference achieves best performance results. If you are in an environment with very little—or no—other wireless network traffic, your best performance will be achieved with Protected mode OFF.

Securing your Wi-Fi® Network

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

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

Wired Equivalent Privacy (WEP)

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

64-Bit WEP

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

128-Bit WEP

As a result of 64-bit WEP's potential security weaknesses, a more secure method of 128-bit encryption was developed. 128-bit encryption includes a key length of 104 bits plus 24 additional bits of system-generated data (128 bits total). Some hardware manufacturers refer to 128-bit as 104-bit encryption.

Most of the new wireless equipment in the market today supports both 64-bit and 128-bit WEP encryption, but you might have older equipment that only supports 64-bit WEP. All Belkin wireless products will support both 64-bit and 128-bit WEP.

Encryption Keys

After selecting either the 64-bit or 128-bit WEP encryption mode, it is critical that you generate an encryption key. If the encryption key is not consistent throughout the entire wireless network, your wireless networking devices will be unable to communicate with one another on your network and you will not be able to successfully communicate within your network.

You can enter your key by typing in the hex key manually, or you can type a passphrase in the "Passphrase" field and click "Generate" to create a key. A hex (hexadecimal) key is a combination of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

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

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

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

Wi-Fi Protected Access™ (WPA™)

WPA is a new Wi-Fi standard that was designed to improve upon the security features of WEP. To use WPA security, the drivers and software of your wireless equipment must be upgraded to support WPA. These updates will be found on the wireless vendor's website. There are three types of WPA security: WPA-PSK (no server), and WPA2.

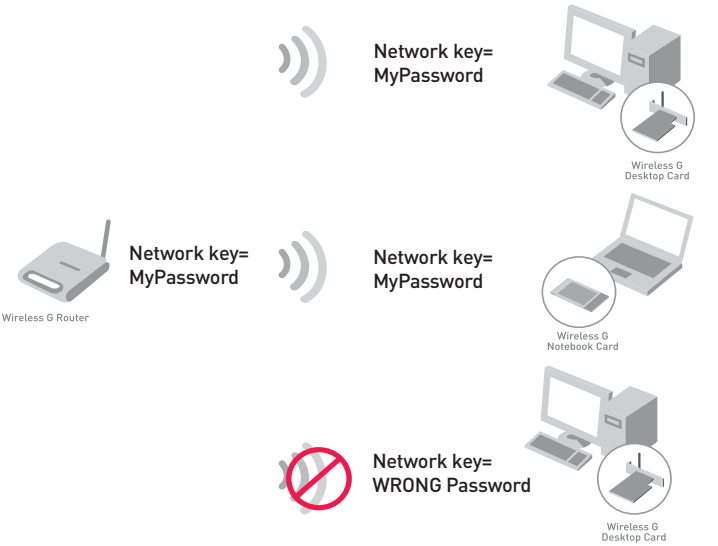
WPA-PSK (no server) uses what is known as a pre-shared key as the network key. A network key is basically a password that is between eight and 63 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same network key to access the network. Typically, this is the mode that will be used in a home environment.

WPA2™ requires Advanced Encryption Standard (AES) for encryption of data, which offers much greater security than WPA. WPA uses both Temporal Key Integrity Protocol (TKIP) and (AES) for encryption.

For a list of Belkin wireless products that support WPA, please visit our website at **www.belkin.com/networking.**

Sharing the Same Network Keys

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



The Wireless G Desktop Card cannot access the network because it is using a different network key than the network key that is configured on the Wireless G Router.

Using a Hexadecimal Key
A hexadecimal key is a combination of numbers and letters from A–F and 0–9. 64-bit keys are five two-digit numbers. 128-bit keys are 13 two-digit numbers.

For instance:

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

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

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

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

WEP Setup

64-Bit WEP Encryption

1. Select “64-bit WEP” from the “Security” menu’s “Security Mode”.

2. After selecting your WEP encryption mode, you can enter your key by typing in the hex key manually, or you can put a check mark in “Passphrase”, then type in your passphrase. Click “Generate” to generate four different hex keys.

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

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

3. Click “Apply Changes” to save the setting.

WARNING: If you are configuring the Wireless G 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, your client will lose its wireless connection.

128-Bit 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.

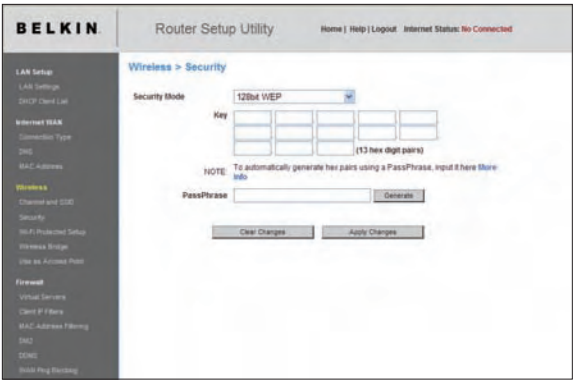
1. Select “128-bit WEP” from the “Security” menu’s “Security Mode”.

2. After selecting your WEP encryption mode, you can enter your key by typing in the hex key manually, or you can put a check mark in “Passphrase”, then type in your passphrase. Click “Generate” to generate the hex keys.

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

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

3. Click “Apply Changes” to save the setting.



WARNING: If you are configuring the Wireless G 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, your client will lose its wireless connection.

Changing the Wireless Security Settings

Your Router is equipped with the latest security standard called Wi-Fi Protected Access 2 (WPA2) and the legacy security standard called Wired Equivalent Privacy (WEP). Your Router also supports the Wi-Fi Protected Setup™ (WPS) specification, which simplifies the setup of a wireless network. WPS uses familiar methodologies, such as typing in a Personal Identification Number (PIN) or pushing a button, to enable users to automatically configure network names and strong WPA/WPA2 data encryption and authentication. 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.

Using Wi-Fi Protected Setup

WPS uses WPA2 (described below) for encryption. It does not provide additional security, but rather, standardizes the method for securing your wireless network. You may use either the Push Button Configuration (PBC) method or PIN method to allow a device access to your wireless network. Conceptually, the two methods work as follows:

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

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

1. Wi-Fi Protected Setup (WPS): Enabled or Disabled.
2. Personal Identification Number (PIN) Method: In this method, a wireless client wishing to access your network must supply a 4- or 8-digit PIN to the Router. After clicking “Enroll”, you must start the WPS handshaking procedure from the client within two minutes.
3. Router PIN: If an external registrar is available, you may enter in the Router’s PIN to the registrar. Click “Generate New PIN” to change the PIN from the default value. Click “Restore Default PIN” to reset the PIN value.
4. Push Button Configuration (PBC) Method: PBC is an alternate method to connect to a WPS network. Push the PBC button located on the back of the Router for three seconds, and then initiate the PBC on the client device. Alternatively, push the “Start PBC” soft button to start this process.
5. Manual Configuration Method: This section lists the default security settings if not using WPS.

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

WPA Setup

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this User Manual's publication, a security patch download is available, for free, from Microsoft®. This patch works only with the Windows XP operating system. You also need to download the latest driver for your Belkin Wireless G Desktop or Notebook 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.

WPA uses a so-called pre-shared key as the security key. A pre-shared key is a password that is between eight and 63 characters long. It can be a combination of letters, numbers, and other characters. Each client uses the same key to access the network. Typically, this mode will be used in a home environment.

WPA2 is the second generation of WPA, offering a more advanced encryption technique over WPA.

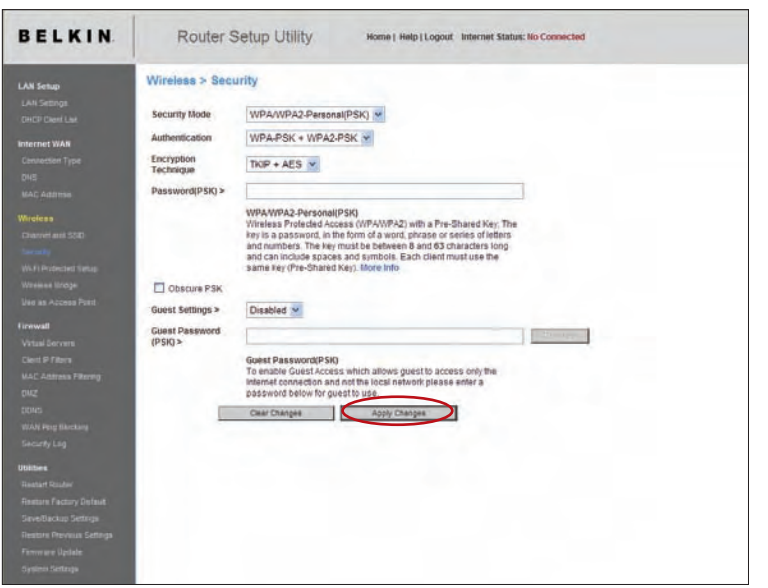
Setting WPA/WPA2

1. Select “WPA/WPA2-Personal (PSK)” from the “Security Mode” drop-down box.

2. Select “WPA-PSK” for just WPA authentication, or “WPA2-PSK” for just WPA2 authentication, or you may select “WPA-PSK + WPA2-PSK” for WPA and WPA2 as the authentication type.

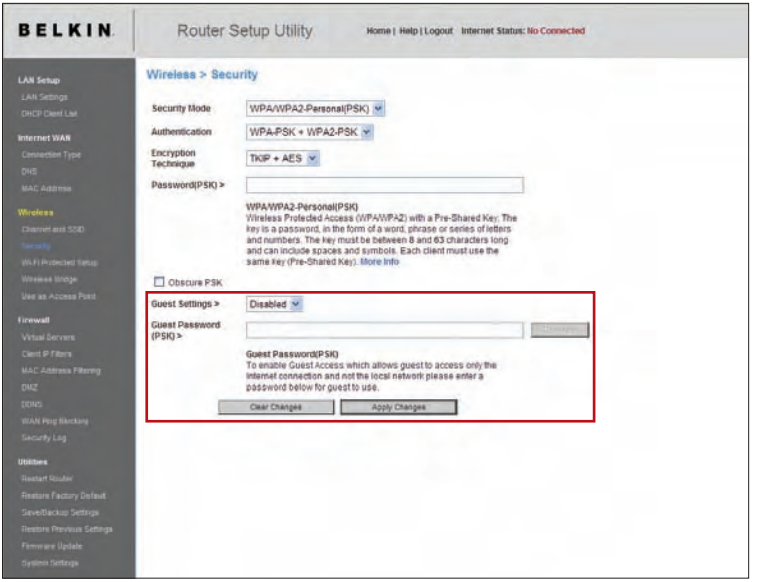
3. Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up. This pre-shared key will allow users full access to your network including shared files and printers.

4. Click “Apply Changes” to finish. You must now set all clients to match these settings depending on the type of access you want them to have.



Guest Access (Optional)

The guest pre-shared key allows guest users an Internet-only access to restrict them from entering your network and having access to files on your PCs. Enter your pre-shared key for guest access. This can be from eight to 63 characters and can be letters, numbers, or symbols. Click "Apply Changes" to finish.



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

If you do NOT have a Belkin WPA Wireless Desktop or Wireless Notebook Card and it is not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available for free download.

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

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

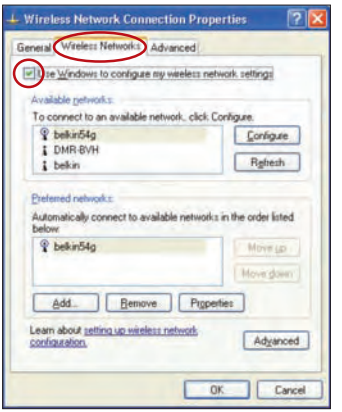
Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

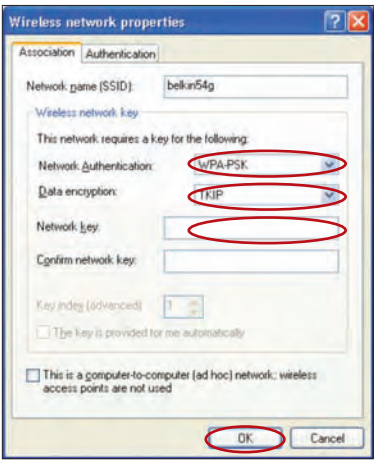
Setting up Windows XP Wireless Network Utility to use WPA-PSK

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

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



4. Under the “Wireless Networks” tab, click the “Configure” button and you will see the following screen.



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

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

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

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

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

8. Click “OK” to apply settings.

Using the Access Point Mode

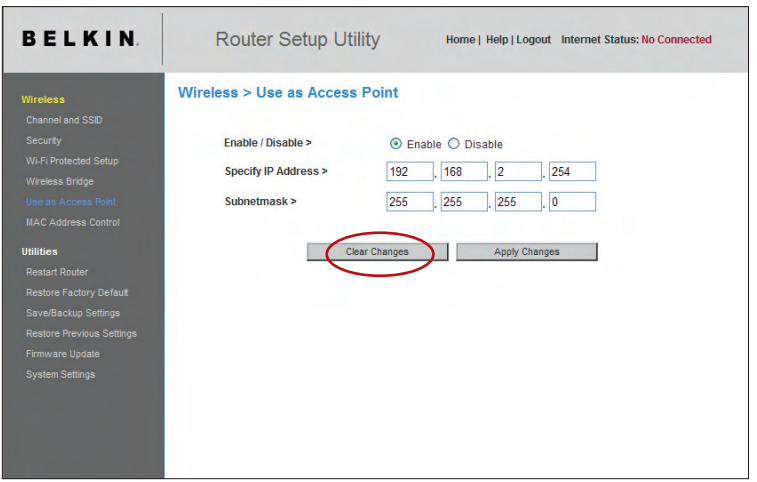
Note: This advanced feature should be employed by advanced users only. The Router can be configured to work as a wireless network access point. Using this mode will defeat the NAT IP sharing feature and DHCP server. In Access Point (AP) mode, the Router will need to be configured with an IP address that 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 “Modem” port on the Router to your existing network.

The Router is now acting as an access point. To access the Router’s Web-Based 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.



Wireless Range Extension and Bridging

Wireless range extension and bridging works with the following models only:

F5D7231-4 Wireless G Plus Router

F5D7230-4 Wireless G Router

F5D7130 Wireless G Range Extender/Access Point

F5D7132 Wireless G Universal Range Extender

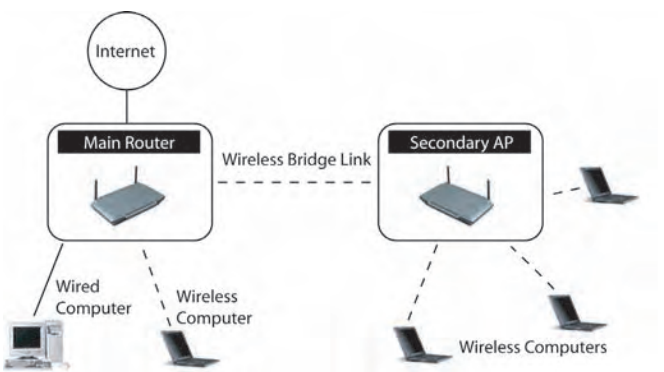
Please make sure to download the latest firmware version for the Router or Access Point for optimal performance: **http://web.belkin.com/support.**

What is a Wireless Bridge?

A wireless bridge is a "mode" in which your Wireless Router can directly connect to a secondary Wireless Access Point. Note that you can only bridge your Belkin Wireless G Router (model F5D7230-4, F5D7231-4) to a Belkin Wireless G Range Extender/Access Point (model F5D7131, F5D7130). We do not support bridging with access points of other manufacturers at this time. 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.

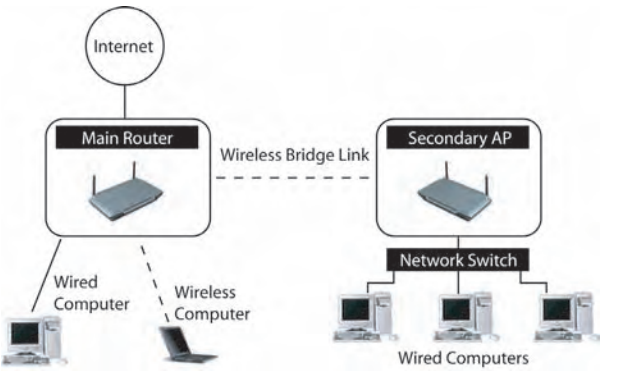
Range Extension

Range extension will extend the wireless coverage area in your home or office. The example on the next page illustrates the 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.



Adding Another Network Segment Wirelessly

Bridging an Access Point to your Router allows you to add a 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 (for more information on changing channels, see page 48 of this User Manual).

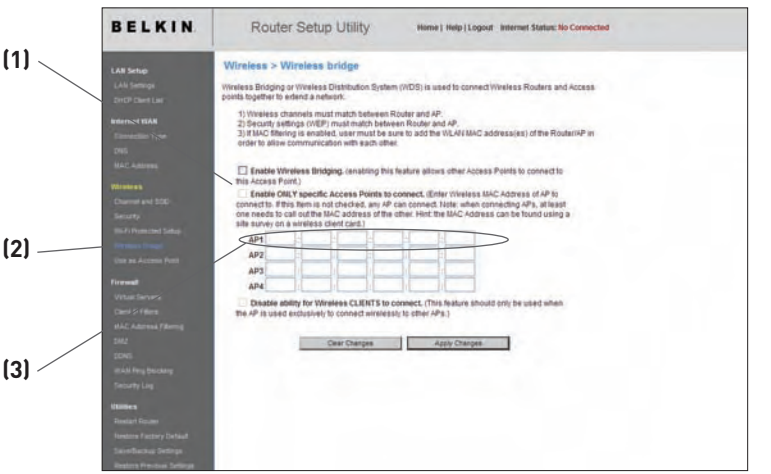
2. Find the Access Point's MAC address on the bottom of the Access Point. There are two MAC addresses on the bottom label. You will need the MAC address named "WLAN MAC Address". The MAC address starts with 0030BD and is followed by six other numbers or letters (i.e. 0030BD-XXXXXX). Write the MAC address below. Go to the next step.

3. Place your secondary Access Point within range of your Wireless Router and near the area where you want to extend the range or add the network segment. Typically, indoor range should be between 100 and 200 feet.

4. Connect power to your Access Point. Make sure the Access Point is on and proceed to the next step.

5. From a computer already connected to your Router, access the Advanced Setup Utility by opening your browser. In the address bar, type in "192.168.2.1". Do not type in "www" or "http://" before the number. **Note:** If you have changed your Router's IP address, use that IP address.

6. You will see the Router's user interface in the browser window. Click "Wireless Bridge" **(2)** on the left-hand side of the screen. You will see the following screen.



7. Check the box that says "Enable ONLY specific Access Points to connect" **(1)**.

8. In the fields named "AP1" **(3)**, type in the MAC address of your secondary Access Point. When you have typed in the address, click "Apply Changes".

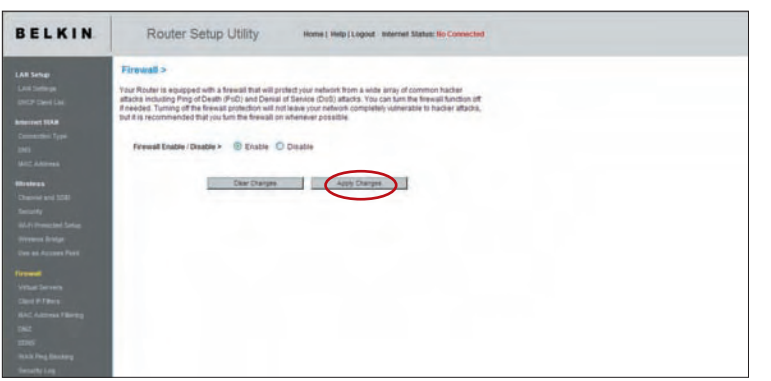
9. Bridging is now set up.

Configuring the Firewall

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

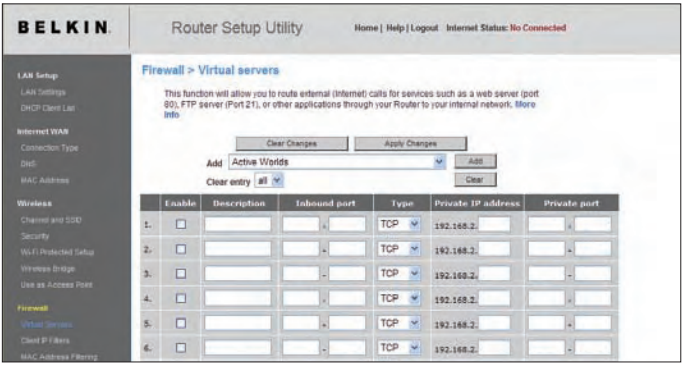
- IP Spoofing
- SYN flood
- Land Attack
- UDP flooding
- Ping of Death (PoD)
- Tear Drop Attack
- Denial of Service (DoS)
- ICMP defect
- IP with zero length
- RIP defect
- Smurf Attack
- Fragment flooding
- TCP Null Scan

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, while disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, it is recommended that you leave the firewall enabled.



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.” You will need to contact the application vendor to find out which port settings you need.



Entering Settings into the Virtual Server

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