Step 1: Hardware Connections – Follow the Quick Installation Guide

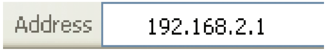
See the QIG or Step 1: Hardware Connections from the previous section.

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

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

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

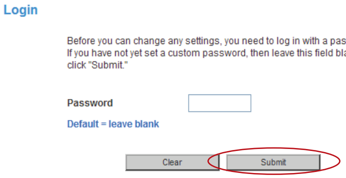
Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (do not type in anything else such as "http://" or "www"). Then press the "Enter" key.



Address 192.168.2.1

Logging into the Router

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



Login

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

Password

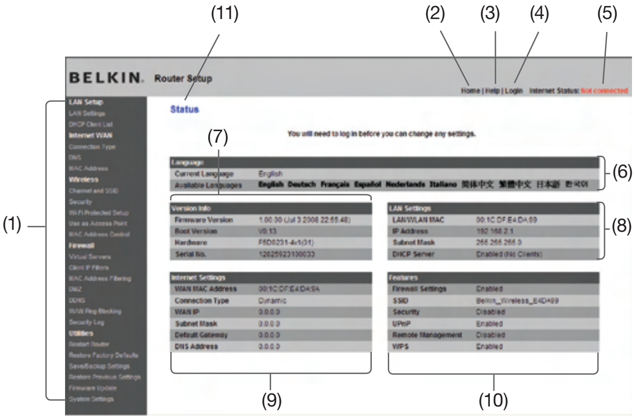
Default = leave blank

Logging out of the Router

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

Understanding the Web-Based Advanced User Interface

The home page is the first page you will see when you access the Advanced User Interface (UI). The home page shows you a quick view of the Router’s status and settings. All advanced setup pages can be reached from this page.



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

Language	
Current Language	English
Available Languages	English Deutsch Français Español Nederlands Italiano 简体中文 繁體中文 日本語 한국어

Version Info	
Firmware Version	1.00.00 (Jul 3 2008 22:55:48)
Boot Version	V0.13
Hardware	F5D8231-4v1(01)
Serial No.	12825923100033

LAN Settings	
LAN/WLAN MAC	00:1C:DF:E4:DA:99
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled (No Clients)

Internet Settings	
WAN MAC Address	00:1C:DF:E4:DA:9A
Connection Type	Dynamic
WAN IP	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS Address	0.0.0.0

Features	
Firewall Settings	Enabled
SSID	Belkin_Wireless_E4DA99
Security	Disabled
UPnP	Enabled
Remote Management	Disabled
WPS	Enabled

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 header of each tab will show you a short description of the tab's function.

2. Home Button

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

3. Help Button

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

4. Login/Logout Button

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

5. Internet-Status Indicators

This indicator is visible in all pages of the Router, indicating the connection status of the Router. When the indicator says "Connected" in blue, the Router is connected to the Internet. When the Router is not connected to the Internet, the indicator will read "Not Connected" in RED. The indicator is automatically updated when you make changes to the settings of the Router.

6. Language

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

7. Version Info

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

8. 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.

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. Features

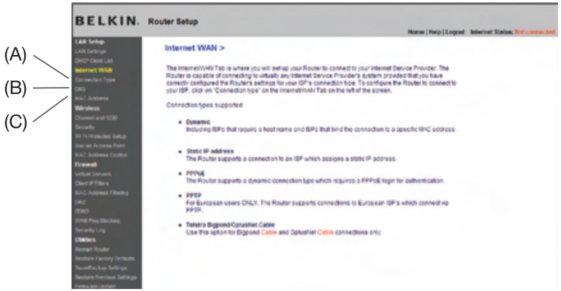
Shows the status of the Router's firewall, and wireless features. Changes can be made to the settings by clicking on any one of the links or by clicking the quick-navigation links on the left side of the screen.

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: 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.



Internet WAN >

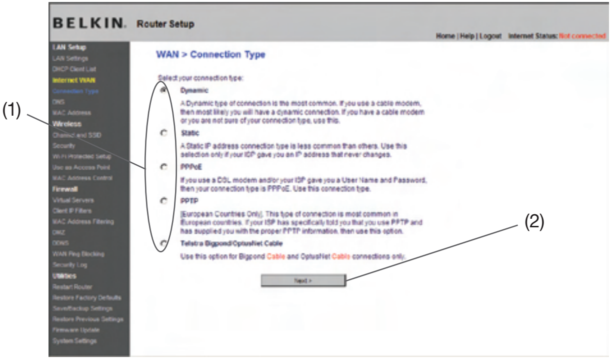
The Internet/WAN Tab is where you will setup your Router to connect to your Internet Service Provider. The Router is capable of connecting to virtually any Internet Service Provider's system provided that you have correctly configured the Router's settings for your ISP's connection type. To configure the Router to connect to your ISP, click on "Connection type" on the Internet/WAN Tab on the left of the screen.

Connection types supported:

- **Dynamic**
  Including ISPs that require a host name and ISPs that bind the connection to a specific MAC address.
- **Static IP address**
  The Router supports a connection to an ISP which assigns a static IP address.
- **PPPoE**
  The Router supports a dynamic connection type which requires a PPPoE login for authentication.
- **PPTP**
  For European users ONLY. The Router supports connections to European ISP's which connect via PPTP.
- **Telstra Bigpond/OptusNet Cable**
  Use this option for Bigpond Cable and OptusNet Cable connections only.

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).



WAN > Connection Type

Select your connection type:

● Dynamic

A Dynamic type of connection is the most common. If you use a cable modem, then most likely you will have a dynamic connection. If you have a cable modem or you are not sure of your connection type, use this.

○ Static

A Static IP address connection type is less common than others. Use this selection only if your ISP gave you an IP address that never changes.

○ PPPoE

If you use a DSL modem and/or your ISP gave you a User Name and Password, then your connection type is PPPoE. Use this connection type.

○ PPTP

[European Countries Only]. This type of connection is most common in European countries. If your ISP has specifically told you that you use PPTP and has supplied you with the proper PPTP information, then use this option.

○ Telstra Bigpond/OptusNet Cable

Use this option for Bigpond Cable and OptusNet Cable connections only.

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

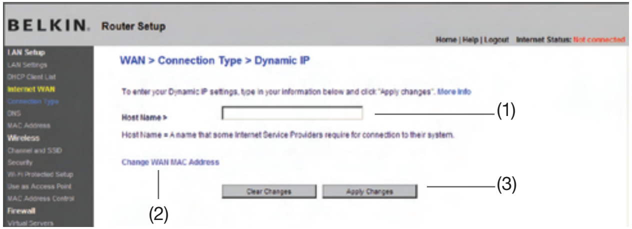
A dynamic connection type is the most common connection type found with cable modems. Setting the connection type to “dynamic” in many cases is enough to complete the connection to your ISP. Some dynamic connection types may require a host name. You can enter your host name in the space provided if you 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 (1)

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 (2)

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.



WAN > Connection Type > Dynamic IP

To enter your Dynamic IP settings, type in your information below and click "Apply changes". More Info

Host Name >

Host Name = A name that some Internet Service Providers require for connection to their system.

Change WAN MAC Address

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” (4). After you apply the changes, the Internet Status indicator will read “Connected” if your Router is set up properly.

1. **IP Address (1)**

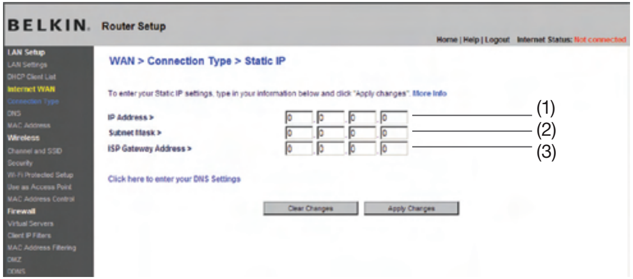
Provided by your ISP. Enter your IP address here.

2. **Subnet Mask (2)**

Provided by your ISP. Enter your subnet mask here.

3. **ISP Gateway Address (3)**

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



WAN > Connection Type > Static IP

To enter your Static IP settings, type in your information below and click "Apply changes". More Info

IP Address > 0 . 0 . 0 . 0

Subnet Mask > 0 . 0 . 0 . 0

ISP Gateway Address > 0 . 0 . 0 . 0

Setting your ISP Connection Type to PPPoE

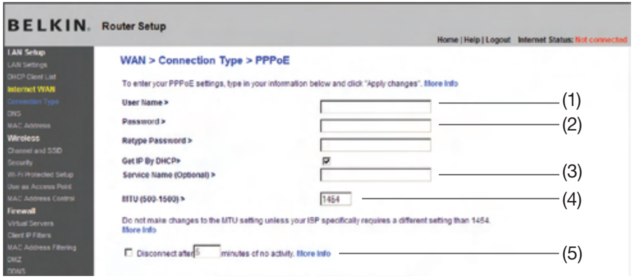
Most DSL providers use PPPoE as the connection type. If you use a DSL modem to connect to the Internet, your ISP may use PPPoE to log you into the service. If you have an Internet connection in your home or small office that doesn’t require a modem, you may also use PPPoE.

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.

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



Internet Status: Not connected

WAN > Connection Type > PPPoE

To enter your PPPoE settings, type in your information below and click "Apply changes". More Info

User Name >

Password >

Retype Password >

Get IP By DHCP> ☑

Service Name (Optional) >

MTU (500-1500) > 1454

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

□ Disconnect after 5 minutes of no activity. More Info

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

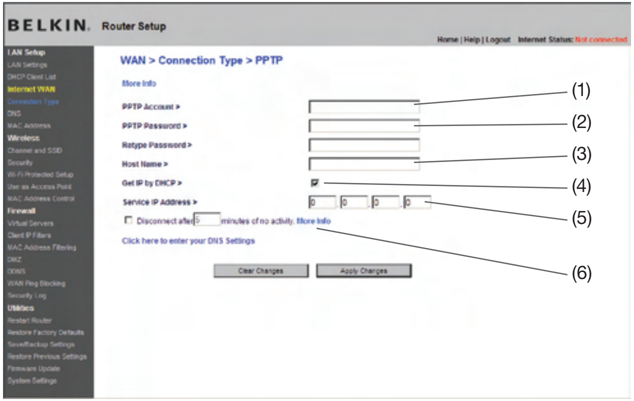
The MTU setting should never be changed unless your ISP gives you a specific MTU setting. Making changes to the MTU setting can cause problems with your Internet connection including disconnection from the Internet, slow Internet access, and problems with Internet applications working properly.

5. Disconnect after X minutes…

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.

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.



Internet Status: Not connected

WAN > Connection Type > PPTP

PPTP Account >

PPTP Password >

Retype Password >

Host Name >

Get IP by DHCP > ☑

Service IP Address > 0 . 0 . 0 . 0

☐ Disconnect after 5 minutes of no activity. More Info

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. Get IP by DHCP

If your ISP provided you with a specific IP address, uncheck this box and enter your IP address, subnet mask, and default gateway in the fields that appear.

5. Service IP Address

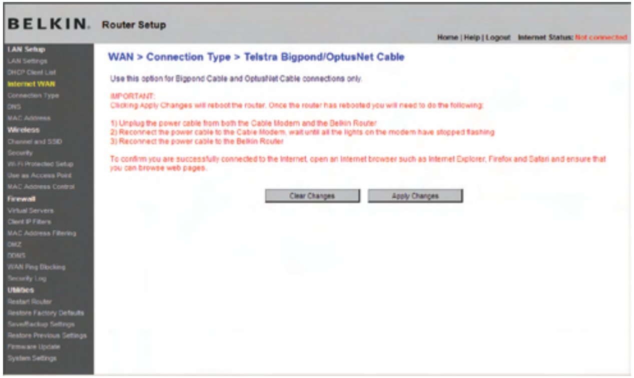
Provided by your ISP. Enter your service IP address here.

6. 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.

Setting your Connection Type if You Are a Telstra® BigPond/OptusNet Cable User

[Australia Only] Follow the on-screen steps and click “Apply Changes” to complete your setup.



WAN > Connection Type > Telstra Bigpond/OptusNet Cable

Use this option for Bigpond Cable and OptusNet Cable connections only.

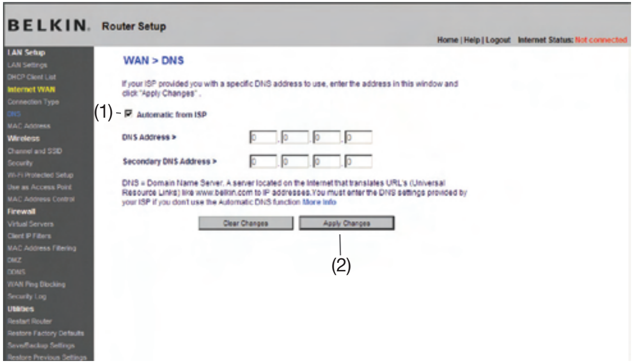
IMPORTANT:
Clicking Apply Changes will reboot the router. Once the router has rebooted you will need to do the following:

1) Unplug the power cable from both the Cable Modem and the Belkin Router
2) Reconnect the power cable to the Cable Modem, wait until all the lights on the modem have stopped flashing
3) Reconnect the power cable to the Belkin Router

To confirm you are successfully connected to the Internet, open an Internet browser such as Internet Explorer, Firefox and Safari and ensure that you can browse web pages.

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.



Internet Status: Not connected

WAN > DNS

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

☑ Automatic from ISP

DNS Address > 0 . 0 . 0 . 0

Secondary DNS Address > 0 . 0 . 0 . 0

DNS = Domain Name Server. A server located on the Internet that translates URL's (Universal Resource Links) like www.belkin.com to IP addresses.You must enter the DNS settings provided by your ISP if you dont use the Automatic DNS function More Info

Configuring your WAN Media Access Controller (MAC) Address

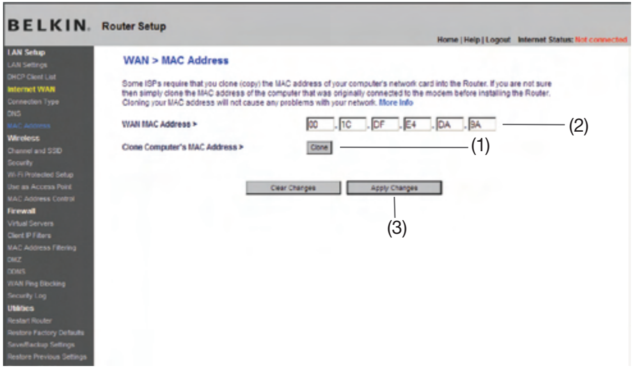
All network components including cards, adapters, and routers, have a unique “serial number” called a MAC address. Your Internet Service Provider (ISP) may record the MAC address of your computer’s adapter and only let that particular computer connect to the Internet service. When you install the Router,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



Some ISPs require that you clone (copy) the MAC address of your computer's network card into the Router. If you are not sure then simply clone the MAC address of the computer that was originally connected to the modem before installing the Router. Cloning your MAC address will not cause any problems with your network. More Info

WAN MAC Address > 00 . 1C . DF . E4 . DA . 9A

Clone Computer's MAC Address >

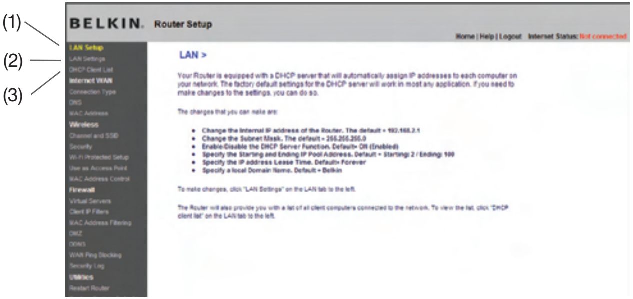
Using your Internet browser, you can access the Router's Web-Based Advanced User Interface. In your browser, type "192.168.2.1" (do not type in anything else such as "http://" or "www") then press the "Enter" key.

Address 192.168.2.1

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).



LAN >

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

The changes that you can make are:

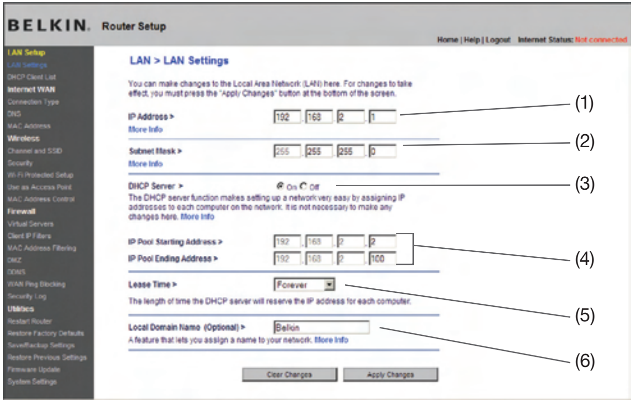
- Change the internal IP address of the Router. The default = 192.168.2.1
- Change the Subnet Mask. The default = 255.255.255.0
- Enable/Disable the DHCP Server Function. Default= ON (Enabled)
- Specify the Starting and Ending IP Pool Address. Default = Starting: 2 / Ending: 100
- Specify the IP address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

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

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

Changing LAN Settings

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



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 > 192 . 168 . 2 . 1
More Info

Subnet Mask > 255 . 255 . 255 . 0
More Info

DHCP Server > ● On ○ Off
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 > 192 . 168 . 2 . 2
IP Pool Ending Address > 192 . 168 . 2 . 100

Lease Time > Forever
The length of time the DHCP server will reserve the IP address for each computer.

Local Domain Name (Optional) > Belkin
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 1 and 254)

10.x.x.x (where x is anything between 1 and 254)

172.y.x.x (where x is anything between 1 and 254 and y is anything between 16 and 31)

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

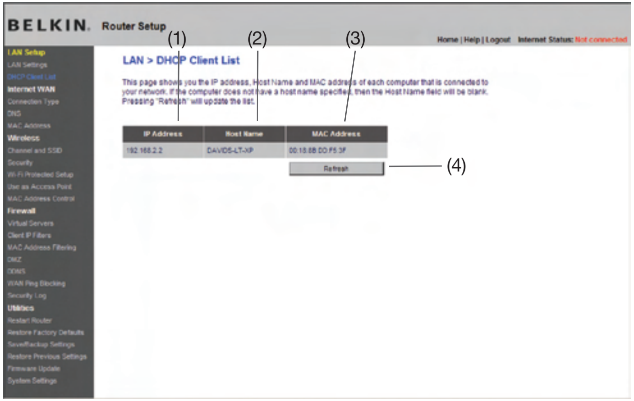
The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to "Forever". The default setting is "Forever", meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular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



LAN > DHCP Client List

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

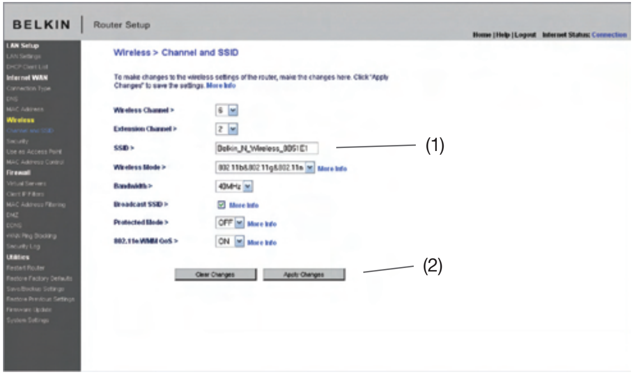
IP Address	Host Name	MAC Address
192.168.2.2	DAVIDS-LT-XP	00:18:8B:DD:F5:3F

Configuring the Wireless Network Settings

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

Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID is used. The SSID is your network name. The default network name of the Router is “Belkin N Wireless” followed by six digits that are unique to your Router. Your network name will look something like “Belkin_N_Wireless_123456”. You can change this to anything you choose, or you can leave it unchanged. Keep in mind, if you decide to change your wireless network name, and there are other wireless networks operating in your area, your network name needs to be different from other wireless networks that may be operating in your area. To change the SSID, type in the SSID that you want to use in the SSID field (1) and click “Apply Changes” (2). The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.



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 > 6

Extension Channel > 2

SSID > Belkin_N_Wireless_0051E1

Wireless Mode > 802.11b&802.11g&802.11n More Info

Bandwidth > 40MHz

Broadcast SSID > ☑ More Info

Protected Mode > OFF More Info

802.11e WMM QoS > ON More Info

Clear Changes | Apply Changes

Note: Please periodically check for new Router firmware updates from the “Utilities > Firmware update” page. Newer firmware can fix problems, add wireless features, and/or improve wireless performance (see page 61).

Changing the Wireless Channel

There are a number of operating channels from which you can choose—in the United States, there are 11 and in the United Kingdom (and most of Europe), there are 13. 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 in which you reside. The channel can be changed if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks.

Extension Channel

The IEEE 802.11n draft specification allows the use of a secondary channel to double the bandwidth (see "Using the Bandwidth Switch" below). An appropriate extension channel will be displayed when operating in 40MHz mode (see "Using the Wireless Mode Switch" below). The channel can be changed if needed.

Using the Wireless Mode Switch

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

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

1) 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.

2) 802.11g only

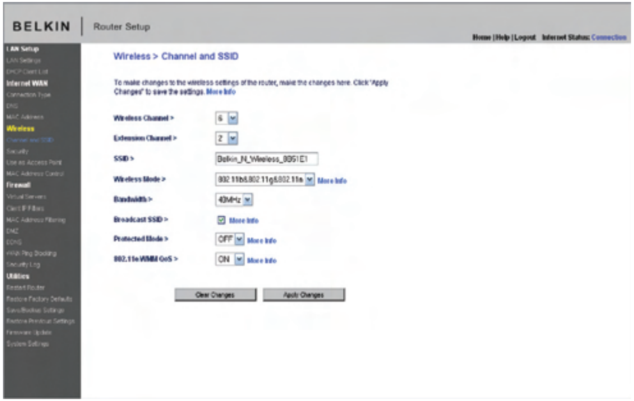
Setting the Router to this mode will allow only 802.11g-compliant devices to join the network, keeping out any slower 802.11b devices.

3) 802.11b+g+n

Setting the Router to this mode will allow 802.11b-, 802.11g-, and 802.11n-compliant devices to join the network.

4) 802.11n only

Setting the Router to this mode will allow only N/draft 802.11n-compliant devices to join the network, keeping out 802.11g and 802.11b devices.



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 > 6

Extension Channel > 2

SSID > Belkin_N_Wireless_8B51E1

Wireless Mode > 802.11b&802.11g&802.11n More Info

Bandwidth > 40MHz

Broadcast SSID > ☑ More Info

Protected Mode > OFF More Info

802.11e WMM QoS > ON More Info

Using the Bandwidth Switch

This switch allows you to set the Router's wireless bandwidth modes. There are several modes available:

1) 20MHz only

Setting the Router to this mode allows only 20MHz operation. This mode is compatible with N, draft 802.11n-, 802.11g-, and 802.11b-compliant devices, but will limit N, draft 802.11n-compliant devices' bandwidth by half. Reducing bandwidth to 20MHz-only operation might solve some wireless problems.

2) 20MHz/40MHz Auto

Setting the Router to this mode allows it to switch automatically between 20MHz and 40MHz operation. This mode enables 40MHz operation, to maximize speed for N, draft 802.11n-compliant devices when conditions permit. When a legacy 802.11g access point is presented and occupies an adjacent secondary channel, the Router automatically reverts to 20MHz operation to maximize compatibility. We recommend using this as the default mode.

Using the Broadcast SSID Feature

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

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

Protected Mode Switch

Protected mode ensures proper operation of N, draft 802.11n-compliant devices on your wireless network when 802.11g or 802.11b devices are present or when there is heavy 802.11g or 802.11b traffic in the operating environment. Use protected mode if your network consists of a mix of Belkin N Wireless Cards and 802.11g or 802.11b cards on your network. If you are in an environment that includes little to no 802.11g or 802.11b wireless network traffic, you will achieve the best N wireless performance with protected mode OFF. Conversely, in an environment with HEAVY 802.11g or 802.11b traffic or interference, you will achieve the best N wireless performance with protected mode ON. This will ensure N wireless performance is not affected.

802.11e/WMM QoS Switch

Allows you to turn ON or OFF wireless QoS.

Changing the Wireless Security Settings

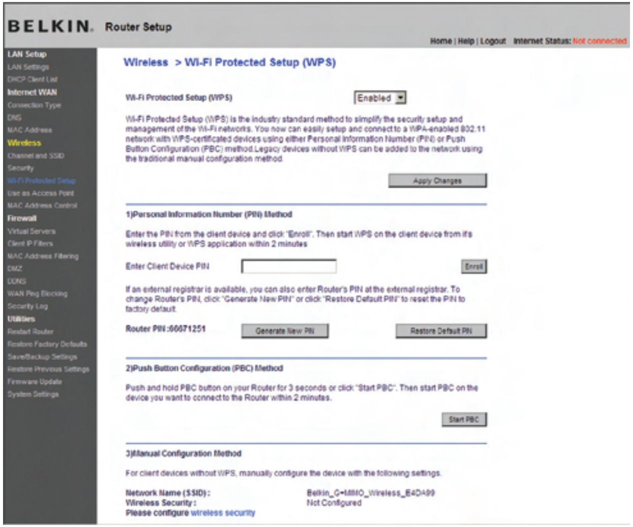
Your N Wireless Router is equipped with the latest security standard called Wi-Fi Protected Access™ 2 (WPA2™) and the legacy security standard called Wired Equivalent Privacy (WEP). Your Router also supports the Wi-Fi Protected Setup™ (WPS) specification, which simplifies the setup of a wireless network. 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 recommends WPA/WPA2 (described on page 45) 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 front 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 screen illustrated below. Enter the client's PIN into the Router's internal registrar (accessed through this screen). The client will be automatically enrolled into your wireless network within two minutes.



Wireless > Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) Enabled

Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of the Wi-Fi networks. You now can easily setup and connect to a WPA-enabled 802.11 network with WPS-certificated devices using either Personal Information Number (PIN) or Push Button Configuration (PBC) method.Legacy devices without WPS can be added to the network using the traditional manual configuration method.

1)Personal Information Number (PIN) Method

Enter the PIN from the client device and click "Enroll". Then start WPS on the client device from it's wireless utility or WPS application within 2 minutes

Enter Client Device PIN

If an external registrar is available, you can also enter Router's PIN at the external registrar. To change Router's PIN, click "Generate New PIN" or click "Restore Default PIN" to reset the PIN to factory default.

Router PIN :00671251

2)Push Button Configuration (PBC) Method

Push and hold PBC button on your Router for 3 seconds or click "Start PBC". Then start PBC on the device you want to connect to the Router within 2 minutes.

3)Manual Configuration Method

For client devices without WPS, manually configure the device with the following settings.

Network Name (SSID) : Belkin_G+MIMO_Wireless_E4DA99
Wireless Security : Not Configured
Please configure wireless security

1. Wi-Fi Protected Setup (WPS): Enabled or Disabled.

2. Personal Identification Number (PIN) Method: In this method, a wireless client wishing to access your network must supply an 8-digit PIN to the Router. After clicking “Enroll”, you must start the WPS handshaking procedure from the client within two minutes.

3. Router PIN: If an external registrar is available, you may enter in the Router’s PIN to the registrar. Click “Generate New PIN” to change the PIN from the default value. Click “Restore Default PIN” to reset the PIN value.

4. Push Button Configuration (PBC) Method: PBC is an alternate method to connect to a WPS network. Push the PBC button located on the back of the Router for three seconds, and then initiate the PBC on the client device. Alternatively, push the “Start PBC” soft button to start this process.

5. Manual Configuration Method: This section lists the default security settings to be set up if not using WPS.

WPA2 Requirements

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

> For Windows XP computers that do not have Service Pack 2 (SP2), a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access (KB 826942)” is available for free download at http://support.microsoft.com/kb/826942
>
> For Windows XP with Service Pack 2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB971021). The update is available from: http://support.microsoft.com/kb/917021

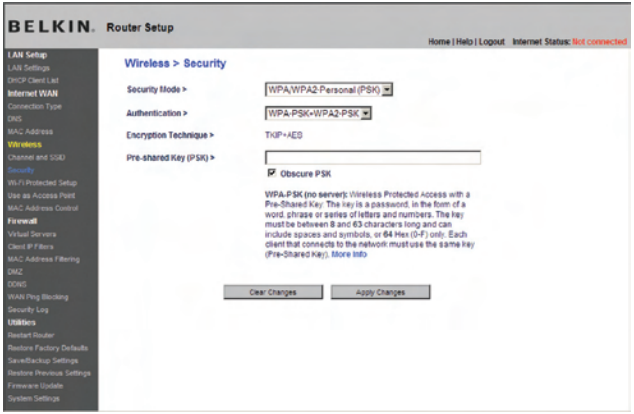
IMPORTANT: You also need to ensure that all your wireless client cards/adapters support WPA2, and that you have downloaded and installed the latest driver. Most of the Belkin wireless cards have driver updates available for download from the Belkin support site: www.belkin.com/networking.

Setting WPA/WPA2-Personal (PSK)

1. After you've set up your Router, go to the "Security" page under "Wireless" and select "WPA/WPA2-Personal (PSK)" from the "Security Mode" drop-down menu.

2. For "Authentication", select "WPA-PSK", "WPA2-PSK", or "WPA-PSK + WPA2-PSK". This setting will have to be identical on the wireless clients that you set up. "WPA-PSK + WPA2-PSK" mode will allow the Router to support clients running either WPA or WPA2 security.

3. 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.



Wireless > Security

Security Mode > WPA/WPA2-Personal (PSK)

Authentication > WPA-PSK+WPA2-PSK

Encryption Technique > TKIP+AES

Pre-shared Key (PSK) >

☑ Obscure 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-F) only. Each client that connects to the network must use the same key (Pre-Shared Key). More Info

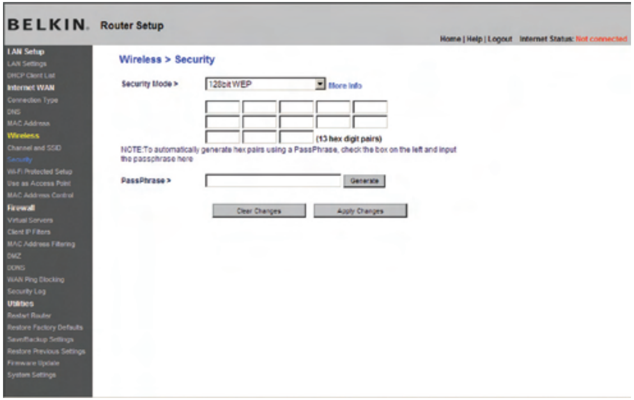
IMPORTANT: Make sure your wireless computers are updated to work with WPA or WPA2, and have the correct settings to get proper connection to the Router.

Setting WEP Encryption

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

1. Select “128-bit WEP” or “64-bit WEP” from the drop-down menu.

2. After selecting your WEP encryption mode, you can enter you WEP key manually by typing in the hex WEP key manually, or you can type a passphrase in the “PassPhrase” field and click “Generate” to create a WEP key from the passphrase. Click “Apply Changes” to finish. You must now set all of your clients to match these settings.



Wireless > Security

Security Mode > 128bit WEP

(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 >

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

Using a Hexadecimal Key

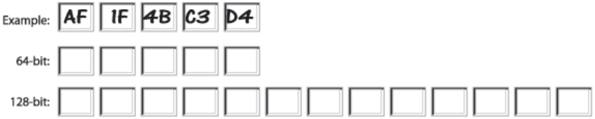
A hexadecimal key is a mixture of numbers and letters from A–F and 0–9. 64-bit keys are 10 digits long and can be divided into five two-digit numbers. 128-bit keys are 26 digits long and can be divided into 13 two-digit numbers.

For instance:

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

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

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



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.

Using the Access Point Mode

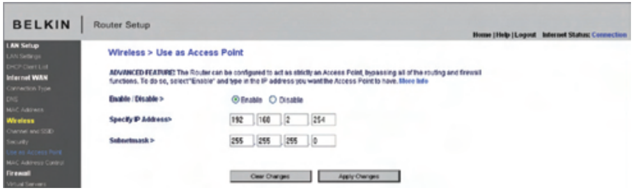
Note: This advanced feature should be employed by advanced users only. The Router can be configured to work as a wireless network access point. Using this mode will defeat the NAT IP sharing feature and DHCP server. In AP mode, the Router will need to be configured with an IP address that is in the same 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 my 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 WAN 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.



Wireless > Use as Access Point

ADVANCED FEATURE! The Router can be configured to act as strictly an Access Point, bypassing all of the routing and firewall functions. To do so, select "Enable" and type in the IP address you want the Access Point to have. More Info

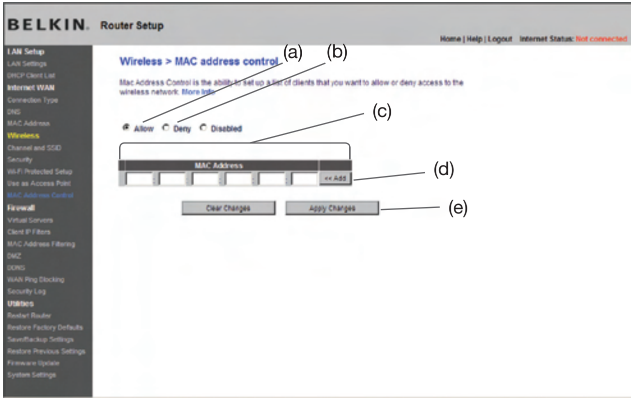
Enable / Disable > ● Enable ○ Disable

Specify IP Address> 192 . 168 . 2 . 254

Subnetmask > 255 . 255 . 255 . 0

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.



Wireless > MAC address control

Mac Address Control is the ability to set up a list of clients that you want to allow or deny access to the wireless network. More Info

● Allow ○ Deny ○ Disabled

Setting up an Allow Access List

1. Select the "Allow" radio button (a) 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 (c), type in the MAC address of the wireless computer you want to be able to access the wireless network, then click "<<Add" (d).

3. Continue to do this until all of the computers you want to add have been entered.

4. Click "Apply Changes" (e) to finish.

Setting up a Deny Access List

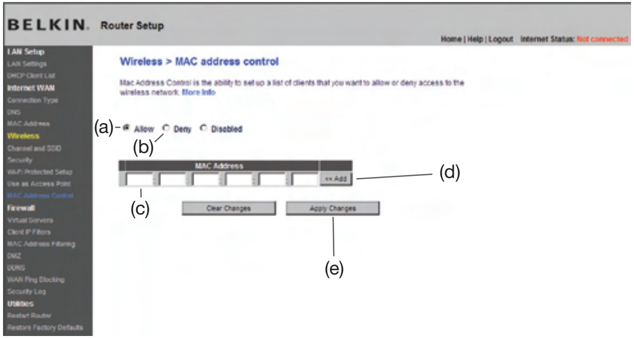
The "Deny Access" list lets you specify computers that you DO NOT want to access the network. Any computer in the list will not be allowed access to the wireless network. All others will.

1. Select the "Deny" radio button (b) 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 (c), type in the MAC address of the wireless computer you want to deny access to the wireless network, then click "<<Add" (d).

3. Continue to do this until all of the computers you want to deny access to have been entered.

4. Click "Apply Changes" (e) to finish.



Wireless > MAC address control

Mac Address Control is the ability to set up a list of clients that you want to allow or deny access to the wireless network. More Info

● Allow ○ Deny ○ Disabled

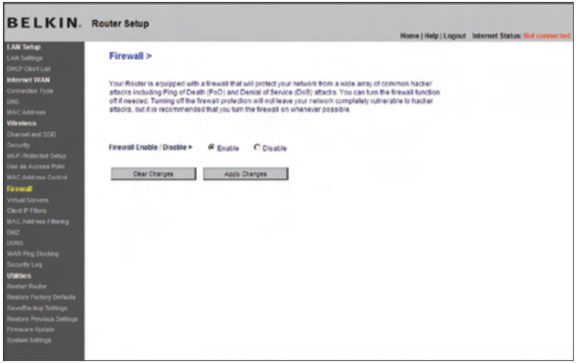
Internet Status: Not connected

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.



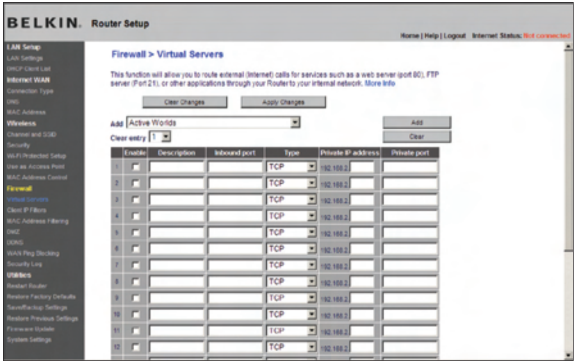
Firewall >

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

Firewall Enable / Disable > ● Enable ○ Disable

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.



Firewall > Virtual Servers

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

Add: Active Worlds

Clear entry: 1

	Enable	Description	Inbound port	Type	Private IP address	Private port
1	□			TCP	192.168.2.	
2	□			TCP	192.168.2.	
3	□			TCP	192.168.2.	
4	□			TCP	192.168.2.	
5	□			TCP	192.168.2.	
6	□			TCP	192.168.2.	
7	□			TCP	192.168.2.	
8	□			TCP	192.168.2.	
9	□			TCP	192.168.2.	
10	□			TCP	192.168.2.	
11	□			TCP	192.168.2.	
12	□			TCP	192.168.2.	