



3.4 Verifying the Connection

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



Congratulations

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

1

2

3

4

5

6

7

8

9

10

section

Alternate Setup Method

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

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

Alternate Setup Method

1

2

3

4

5

section

6

7

8

9

10

Logging into the Router

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

Login

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

Password

Default - leave blank

Clear Submit

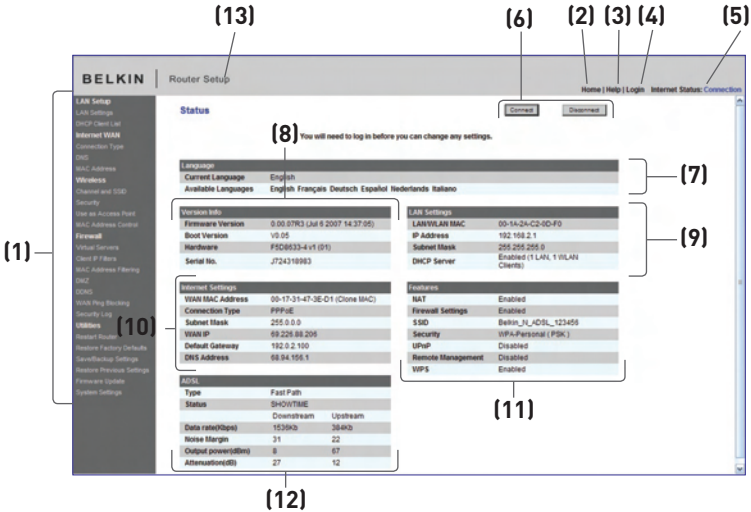
Logging out of the Router

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 (shown on the next 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.

Alternate Setup Method



1. Quick-Navigation Links

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

2. Home Button

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

3. Help Button

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

4. Login/Logout Button

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

5. Internet-Status Indicator

This indicator is visible in all pages of the Router, indicating the connection status of the Router. When the indicator says “Connected” in blue, the Router is connected to the Internet. When the Router is not connected to the Internet, the indicator will read “No Connection” in RED. The indicator is automatically updated when you make changes to the settings of the Router.

6. Connect/Disconnect Buttons

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

7. Language

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

8. Version Info

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

9. LAN Settings

Shows you the settings of the Local Area Network (LAN) side of the Router. Changes can be made to the settings by clicking on any one of the links (IP Address, Subnet Mask, DHCP Server) or by clicking the “LAN” quick-navigation link on the left side of the screen.

10. Internet Settings

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

11. Features

Shows the status of the Router’s 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.

12. ADSL Info

Shows the ADSL status and transmission rates.

13. Page Name

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

Alternate Setup Method

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

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

(A) → Connection Type
(B) → DNS
(C) → MAC Address

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

Internet WAN >

The Internet/WAN Tab is where you will set up 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.

- PPPoE
- PPPoE
- Dynamic/Fixed IP (443 Bridge)
- Static IP (PNA)
- Modem only (Disable Internet Sharing)

Alternate Setup Method

1

Connection Type

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

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

2

3

4

5

section

Select the type of connection you use by clicking the radio button **(1)** next to your connection type and then clicking “Next” **(2)**.

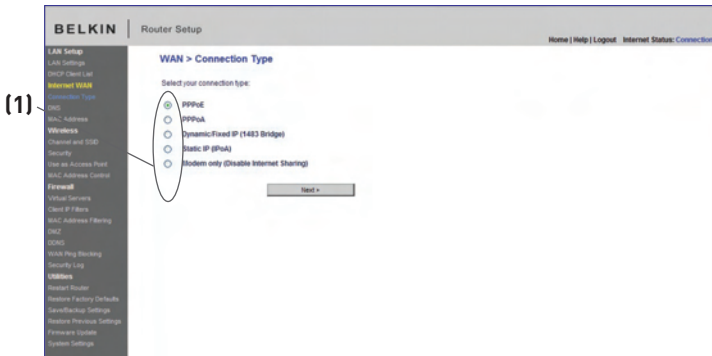
6

7

8

9

10



Alternate Setup Method

Setting your ISP Connection Type to PPPoE or PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) is the standard method of connecting networked devices. It requires a user name and password to access the network of your ISP for connecting to the Internet.

PPPoA (PPP over ATM) is similar to PPPoE, but is mostly implemented in the UK. Select PPPoE or PPPoA and click “Next”. Then enter the information provided by your ISP, and click “Apply Changes” to activate your settings.

The screenshot shows the 'WAN > Connection Type > PPPoE' configuration page in the Belkin Router Setup utility. The page has a sidebar on the left with navigation options like LAN Setup, WAN Setup, Internet WAN, Wireless, Firewall, and Tools. The main content area is titled 'WAN > Connection Type > PPPoE' and contains the following fields and options:

- Username**: A text input field with a blue arrow pointing to it labeled (1).
- Password**: A text input field with a blue arrow pointing to it labeled (2).
- Retype Password**: A text input field with a blue arrow pointing to it labeled (3).
- Service Name (Optional)**: A text input field with a blue arrow pointing to it labeled (4).
- VPI/VCI**: A dropdown menu showing '0' and '35' with a blue arrow pointing to it labeled (4).
- Encapsulation**: A dropdown menu showing 'LLC' and 'mux' with a blue arrow pointing to it labeled (5).
- MTU (500-1500)**: A text input field showing '1492' with a blue arrow pointing to it labeled (6).
- Disconnect after**: A checkbox and a text input field showing '0' minutes of no activity with a blue arrow pointing to it labeled (7).

At the bottom of the form are two buttons: 'Clear Changes' and 'Apply Changes'. The 'Apply Changes' button is circled in blue.

1. **User Name** - Enter the user name. (Assigned by your ISP).
2. **Password** - Enter your password. (Assigned by your ISP).
3. **Retype Password** - Confirm the password. (Assigned by your ISP).
4. **VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).
5. **Encapsulation** - Select your encapsulation type (supplied by your ISP) to specify how to handle multiple protocols at the ATM transport layer.

VC-MUX: PPPoA Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with fewer overheads.

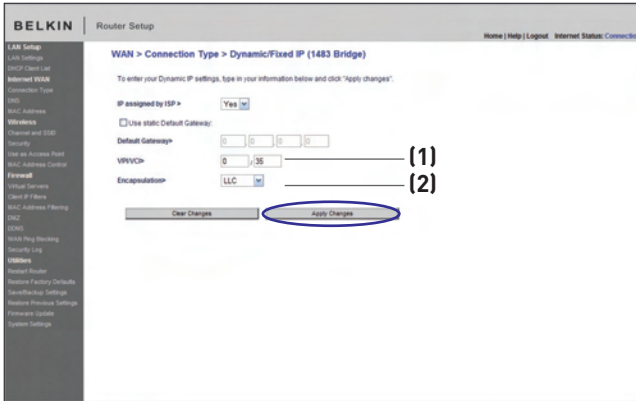
LLC: PPPoA Logical Link Control allows multiple protocols running over one virtual circuit (more overhead).

6. **MTU** - Enter the MTU value for your ISP.
7. **Disconnect after of x minutes of no activity** - Checking the box and enter the number of minute that you want the modem router to auto disconnect after no activity. After this time has been exceeded, the connection will be terminated.

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

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

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



For Dynamic IP connection:

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

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

Alternate Setup Method

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

LAN Setup
LAN Settings
DHCP Client List

Internet WAN
Connection Type
WAN Address
WAN Mask
WAN IP
WAN Gateway
WAN DNS
WAN Security
WAN Firewall
WAN Filter

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

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

IP assigned by ISP > (1)

IP Address (2)

Subnet Mask (3)

Default Gateway (4)

VPI/VCI (5)

Encapsulation > (6)

Click here to enter your DNS Settings

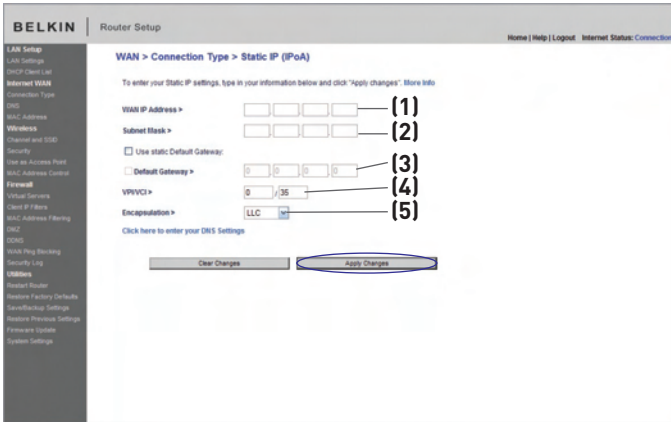
For Dynamic IP connection:

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

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

Setting your ISP Connection Type to Static IP (IPoA)

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



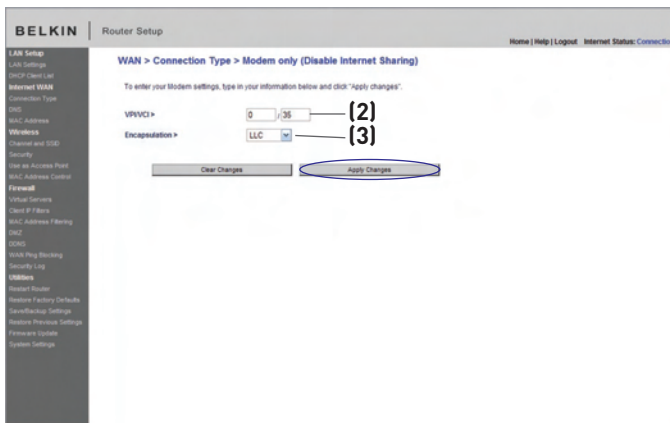
1. **WAN IP Address** - Enter an IP address assigned by your ISP for the Router WAN interface.
2. **Subnet Mask** - Enter a subnet mask assigned by your ISP.
3. **Use Static Default Gateway** - Enter a default gateway IP address. If the Router cannot find the destination address within its local network, it will forward the packets to the default gateway assigned by your ISP.
4. **VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. These identifiers are assigned by your ISP.
5. **Encapsulation** - Select LLC or VC MUX your ISP uses.

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

Alternate Setup Method

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

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

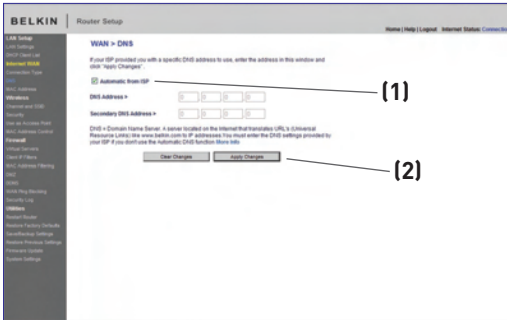


1. **Enable Bridge Service** - Check this box to enable bridge service
2. **VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameters here. (Assigned by your ISP).
3. **Encapsulation** - Select the LLC or VC MUX your ISP uses.

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

Setting Custom Domain Name Server (DNS) Settings

A “Domain Name Server” is a server located on the Internet that translates Universal Resource Locaters (URLs) like “www.belkin.com” to IP addresses. Many Internet Service Providers (ISPs) do not require you to enter this information into the Router. The “Automatic from ISP” box **(1)** should be checked if your ISP did not give you a specific DNS address. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is dynamic or PPPoE, it is likely that you do not have to enter a DNS address. Leave the “Automatic from ISP” box checked. To enter the DNS address settings, uncheck the “Automatic from ISP” box and enter your DNS entries in the spaces provided. Click “Apply Changes” **(2)** to save the settings.



Using the Web-Based Advanced User Interface

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

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)**.

The screenshot shows the Belkin Router Setup web interface. On the left is a navigation menu with the following items: LAN Setup, WAN Setup, Internet WAP, Connection Type, LAN, LAN Address, Wireless, Wireless SSID, Security, Service Access Point, LAN Address Conflict, Firewall, Virus Scans, Guest IP Block, LAN Address Filtering, DMZ, DHCP, Link Up Monitoring, Security Log, Wireless, Guest Router, Restore Factory Defaults, Configuration Settings, System Process Settings, Firmware Update, and System Settings. The main content area is titled "LAN >" and contains the following text: "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." Below this is a list of changes that can be made: "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", and "Specify a local Domain Name. Default = Belkin". At the bottom, it says "To make changes, click 'LAN Settings' on the LAN tab to the left." and "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."

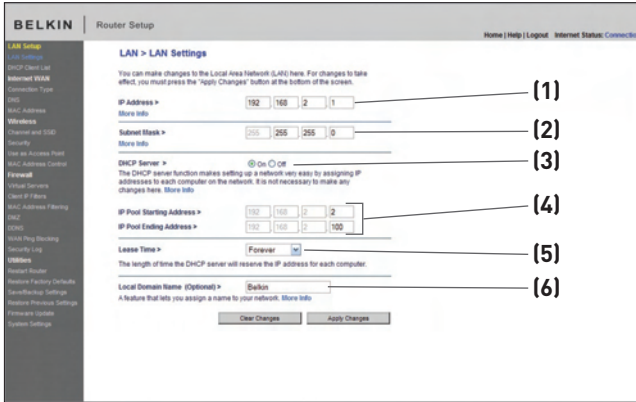
(1) LAN Setup

(2) LAN Settings

(3) DHCP client list

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

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

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

2. Subnet Mask

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

1

2

3

4

5

6

section

7

8

9

10

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

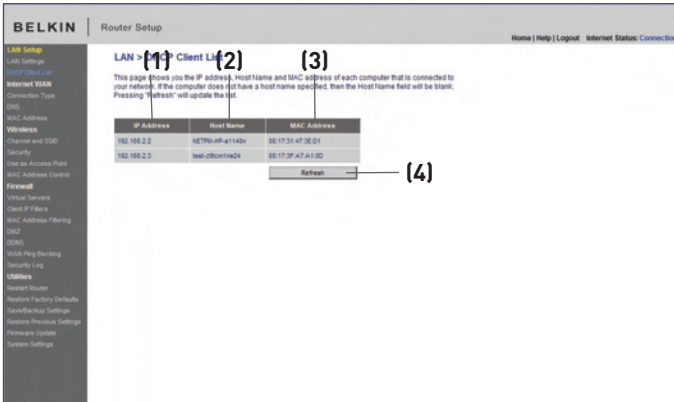
The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to “Forever”. The default setting is “Forever”, meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular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

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.

1

2

3

4

5

6

7

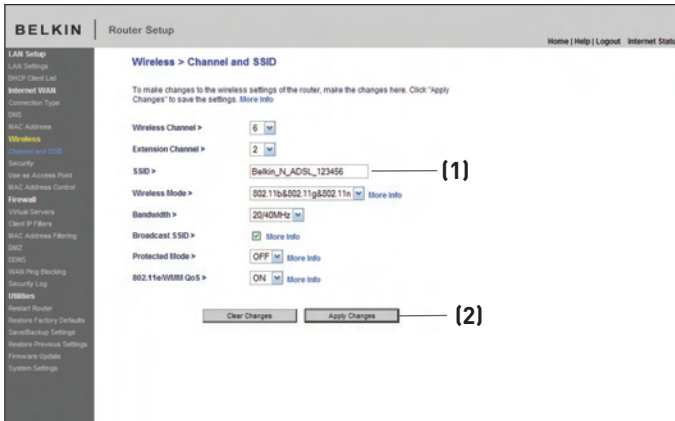
8

9

10

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 N1 Wireless” followed by six digits that are unique to your Router. Your network name will look something like “Belkin_N1_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.



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

Changing the Wireless Channel

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

Extension Channel

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

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

Setting the Router to this mode will allow only 802.11g- and 802.11b-compliant devices to join the network. N1/draft 802.11n devices will operate at the 802.11g speed only.

3) 802.11b & 802.11g & 802.11n

Setting the Router to this mode will allow N1/draft 802.11n-, 802.11g-, and 802.11b-compliant devices to join the network.

4) 802.11n

Setting the Router to this mode will allow only N1/draft 802.11n-compliant devices to join the network, keeping out 802.11g and 802.11b devices.

Using the Bandwidth Switch

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

1) 20MHz/40MHz

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 N1 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. Set the Router to this mode for higher performance.

2) 20MHz

Setting the Router to this mode allows only 20MHz operation. This mode is compatible with N1, draft 802.11n-, 802.11g-, and 802.11b-compliant devices, but will limit N1, draft 802.11n-compliant devices' bandwidth by half. Reducing bandwidth to 20MHz-only operation might solve some wireless problems. This is the default mode for the Router.

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 N1, 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 N1 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 N1 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 N1 wireless performance with protected mode ON. This will ensure N1 wireless performance is not affected.

802.11e/WMM (Wi-Fi® Multimedia) QoS

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

Changing the Wireless Security Settings

Your Router is equipped with the latest security standard called Wi-Fi Protected Access 2 (WPA2). It also supports the legacy security standard called Wired Equivalent Privacy (WEP). By default, wireless security is disabled. To enable security, you will need to determine which standard you want to use. To access the security settings, click “Security” on the “Wireless” tab.

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

WPA2 Requirements

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

For Windows XP computers that do not have Service Pack 2 (SP2), a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access (KB 826942)” is available for free download at <http://support.microsoft.com/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.

1

2

3

4

5

6

7

8

9

10

section

Setting WPA/WPA2-Personal (PSK)

Like WPA security, WPA2 is available in both WPA2-Personal (PSK) mode and WPA2-Enterprise (RADIUS) mode. Typically, WPA2-Personal (PSK) is the mode that will be used in a home environment, while WPA2-Enterprise (RADIUS) is implemented in a business environment where an external radius server distributes the network key to the clients automatically. This guide will focus on WPA2-Personal (PSK) usage. Please refer to the User Manual for more information about wireless security and different types of wireless security.

1. After you've set up your Router, go to the "Security" page under "Wireless" and select "WPA/WPA2-Personal (PSK)" from the "Security Mode" drop-down menu.
2. For "Authentication", select "WPA-PSK", "WPA2-PSK", or "WPA-PSK + WPA2-PSK". This setting will have to be identical on the wireless clients that you set up. "WPA-PSK + WPA2-PSK" mode will allow the Router to support clients running either WPA or WPA2 security.
3. "Encryption Technique", select "TKIP", "AES", or "TKIP+AES". This setting will have to be identical on the wireless clients that you set up.
4. Enter your pre-shared key (PSK). This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the wireless clients that you set up. For example, your PSK might be something like: "Smith family network key". Click "Apply Changes" to finish. You must now set all wireless clients to match these settings.



1

2

3

4

5

6

7

8

9

10

section

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

Setting WPA Security

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

Your Router supports WPA-PSK (no server). WPA-PSK uses what is known as a pre-shared key as the security key. A pre-shared key is basically a password that is between eight and 39 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same key to access the network. Typically this is the mode that will be used in a home environment.

Setting WPA-PSK

1. From the “Security Mode” drop-down menu, select “WPA-PSK (no server)”.
2. For “Encryption Technique”, select “TKIP” or “AES”. This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key. This can be from eight to 39 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.
4. Click “Apply Changes” to finish. You must now set all clients to match these settings.

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

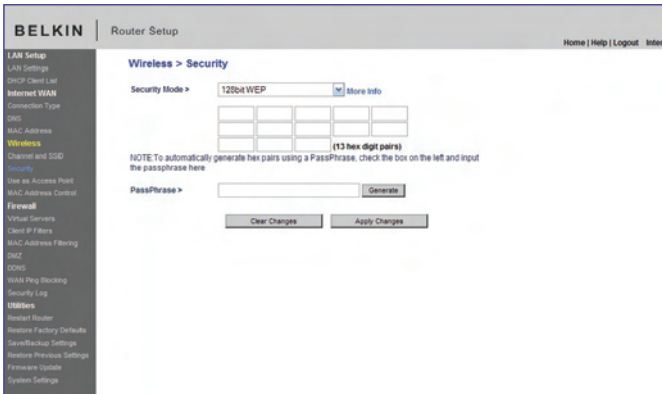
- Security Mode >**: WPA/WPA2 Personal (PSK) (dropdown menu)
- Authentication >**: WPA-PSK (dropdown menu)
- Encryption Technique >**: TKIP (dropdown menu)
- Pre-shared Key (PSK) >**: GoBelkin123 (text input field)
- Obscure PSK (checkbox)

Below the input fields is a paragraph of text: "WPA-PSK (no server): Wireless Protected Access with a Pre-Shared Key. The key is a password, in the form of a word, phrase or series of letters and numbers. The key must be between 8 and 63 characters long and can include spaces and symbols, or 64 Hex (0-F) only. Each client that connects to the network must use the same key (Pre-Shared Key). More info". At the bottom of the configuration area are two buttons: "Clear Changes" and "Apply Changes".

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 your WEP key manually by typing in the hex values in the space provided, 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.



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.

1

2

3

4

5

6

7

8

9

10

Using the Web-Based Advanced User Interface

Using a Hexadecimal Key

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

For instance:

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

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

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

Example:

64-bit:

128-bit:

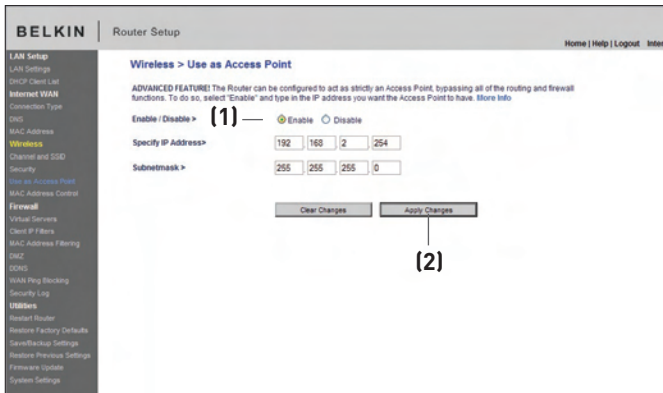
Note to Mac users: Original Apple AirPort products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

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” **(1)** 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” **(2)**.
3. Connect a cable from the “Modem” port on the Router to your existing network.

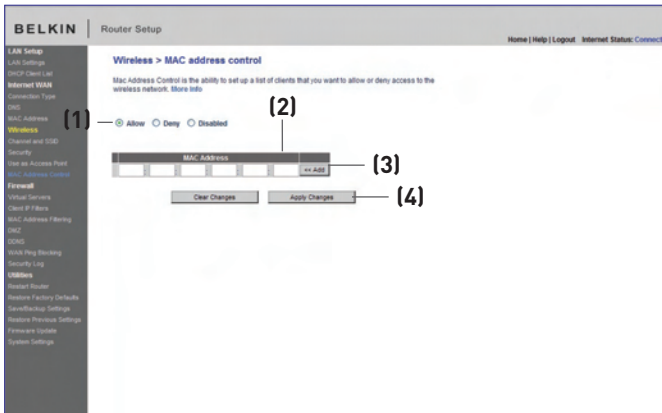
The Router is now acting as an access point. To access the Router’s Web-Based Advanced User Interface again, type the IP address you specified into your browser’s navigation bar. You can set the encryption settings, MAC address filtering, SSID, and channel normally.



Setting MAC Address Control

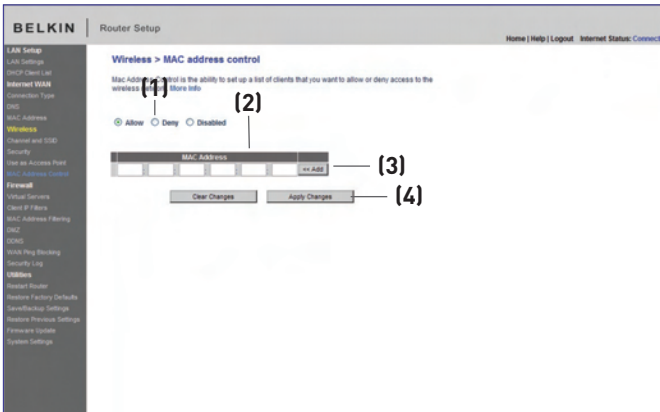
The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the wireless network.

Note: This list applies only to wireless computers. This list can be configured so any computer attempting to access the wireless network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client (computer) to which you want to allow network access. The “Block” feature lets you turn on and off access to the network easily for any computer without having to add and remove the computer’s MAC address from the list.



Setting up an Allow Access List

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



1

2

3

4

5

6

section

7

8

9

10

Setting up a Deny Access List

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

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

Configuring the Firewall

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

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

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be “stealth” meaning that for all intents and purposes, they do not exist to a would-be hacker. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.

