Setting WPA/WPA2-Personal (PSK)

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

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

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

3. For "Encryption Technique", select "TKIP", "AES", or "TKIP+AES". This setting will have to be identical on the wireless clients that you set up.

4. Enter your pre-shared key (PSK). This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the wireless clients that you set up. For example, your PSK might be something like: "Smith family network key". Click "Apply Changes" to finish. You must now set all wireless clients to match these settings.

BELKIN | Router Setup

Home | Help | Logout | Internet Status:

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

[Clear Changes] [Apply Changes]

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

Setting WPA Security

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

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

Setting WPA-PSK

1. From the "Security Mode" drop-down menu, select "WPA-PSK".

2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.

3. Enter your pre-shared key. This can be from eight to 36 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.
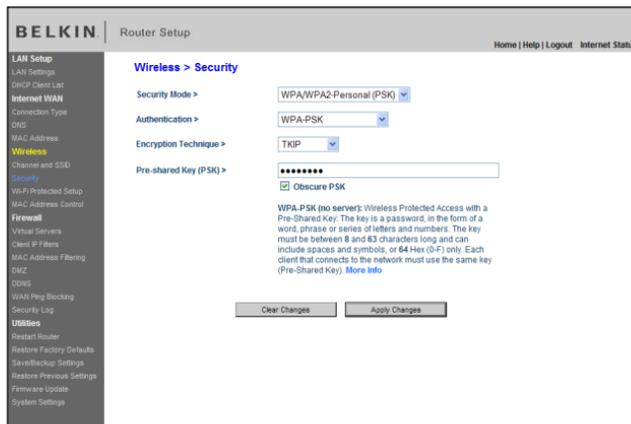
Setting WEP Encryption

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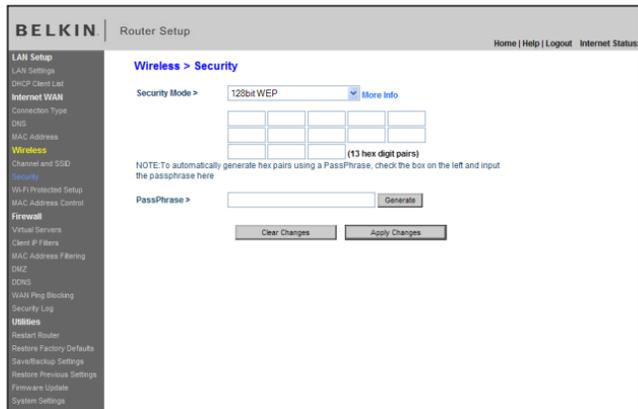
3. Encryption in the Router is now set. Each of your computers on your wireless network will now need to be configured with the same passphrase. Refer to the documentation of your wireless network adapter for information on making this change.

Using a Hexadecimal Key

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

For instance:

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

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

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

Example: AF   IF   4B   C3   D4

64-bit: ☐ ☐ ☐ ☐ ☐

128-bit: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

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

Setting MAC Address Control

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

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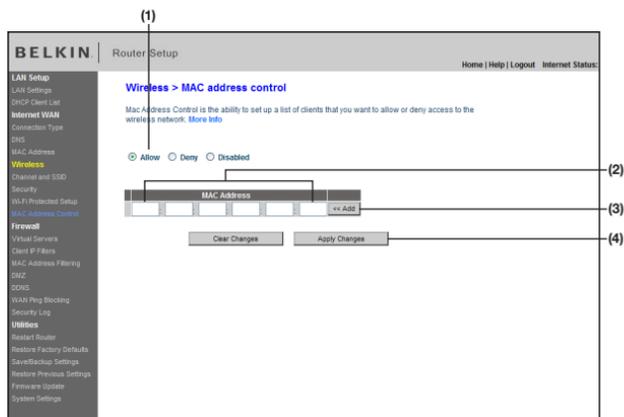
4. Click "Apply Changes" **(4)** to finish.

Setting up a Deny Access List

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

1. Select the "Deny" radio button **(1)** to begin setting up a list of computers to be denied access to the wireless network.

2. Next, in the "MAC Address" field that is blank **(2)**, type in the MAC address of the wireless computer you want to deny access to the wireless network, then click "<<Add" **(3)**.

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

4. Click "Apply Changes" **(4)** to finish.
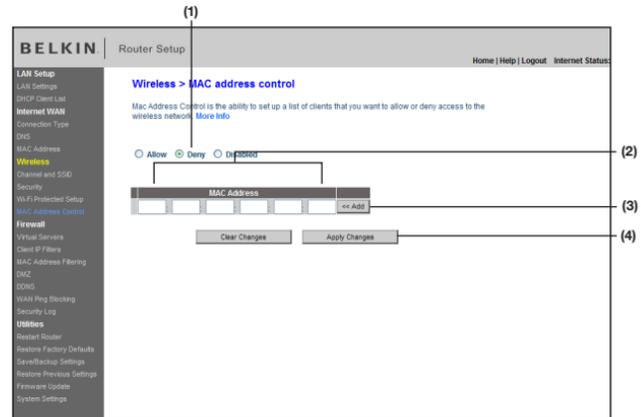
Configuring the Firewall

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

- IP Spoofing

- Land Attack Ping of Death (PoD)

- Denial of Service (DoS)

- IP with zero length

- Smurf Attack

- TCP Null Scan

- SYN flood

- UDP flooding

- Tear Drop Attack

- ICMP defect

- RIP defect

- Fragment flooding

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be "stealth" meaning that for all intents and purposes, they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.
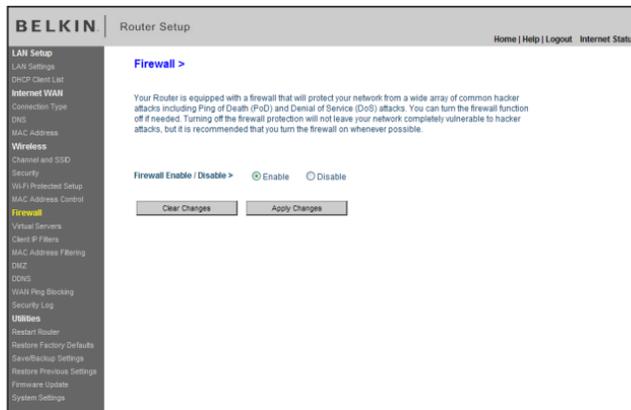
Configuring Internal Forwarding Settings

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.

Choosing an Application

Select your application from the drop-down list. Click "Add". The settings will be transferred to the next available space in the screen. Click "Apply Changes" to save the setting for that application. To remove an application, select the number of the row that you want to remove then click "Clear".

Manually Entering Settings into the Virtual Server

To manually enter settings, enter the IP address in the space provided for the internal (server) machine, the port(s) required to pass (use a comma between multiple ports), select the port type (TCP or UDP), and click "Apply Changes". You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Setting Client IP Filters

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

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

Setting MAC Address Filtering

The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client (computer) on your network to allow network access to each.

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

Note: You will not be able to delete the MAC address of the computer you are using to access the Router's administrative functions (the computer you are using now).
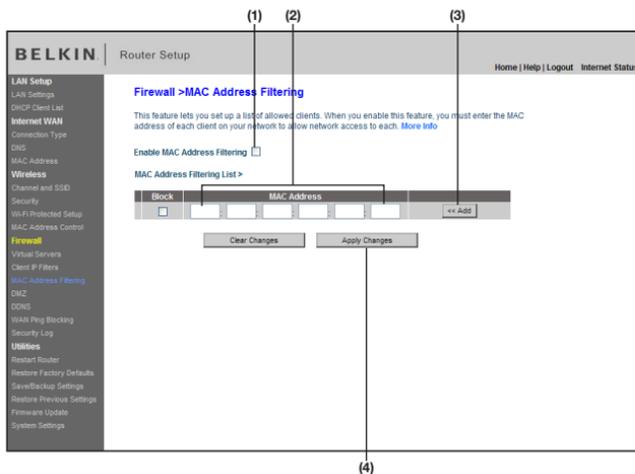
Enabling the Demilitarized Zone (DMZ)

The DMZ feature allows you to specify one computer on your network to be placed outside of the firewall. This may be necessary if the firewall is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is NOT protected from hacker attacks.

To put a computer in the DMZ, enter the last digits of its IP address in the IP field and select "Enable". Click "Apply Changes" for the change to take effect. If you are using multiple static WAN IP addresses, it is possible to select which WAN IP address the DMZ host will be directed to. Type in the WAN IP address you wish the DMZ host to direct to, enter the last two digits of the IP address of the DMZ host computer, select "Enable" and click "Apply Changes".
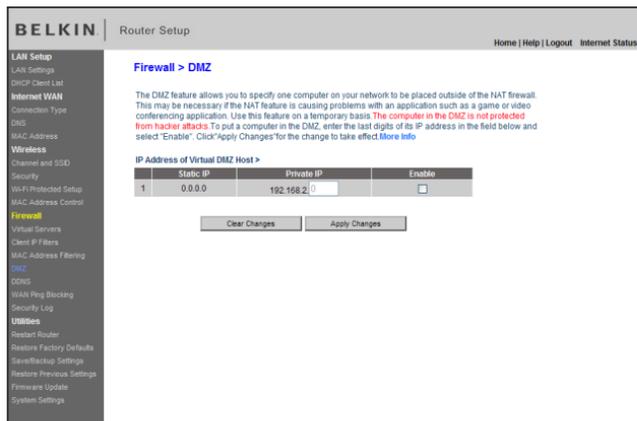
Using Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static host name in any of the many domains DynDNS.org offers, allowing your network computers to be more easily accessed from various locations on the Internet. DynDNS.org provides this service, for up to five host names, free to the Internet community.

The Dynamic DNS^{SM} service is ideal for a home website, file server, or to make it easy to access your home PC and stored files while you're at work. Using the service can ensure that your host name always points to your IP address, no matter how often your ISP changes it. When your IP address changes, your friends and associates can always locate you by visiting yourname.dyndns.org instead!

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

Setting up the Router's Dynamic DNS Update Client

You must register with DynDNS.org's free update service before using this feature. Once you have your registration, follow the directions below.

1. Select DynDNS.org from the "DDNS Service" drop-down box **(1)**.

2. Enter your DynDNS.org user name in the "User Name" field **(2)**.

3. Enter your DynDNS.org password in the "Password" field **(3)**.

4. Enter the DynDNS.org domain name you set up with DynDNS.org in the "Domain Name" field **(4)**.

5. Click "Update Dynamic DNS" to update your IP address **(5)**.

Whenever your IP address assigned by your ISP changes, the Router will automatically update DynDNS.org's servers with your new IP address. You can also do this manually by clicking the "Update Dynamic DNS" button **(5)**.
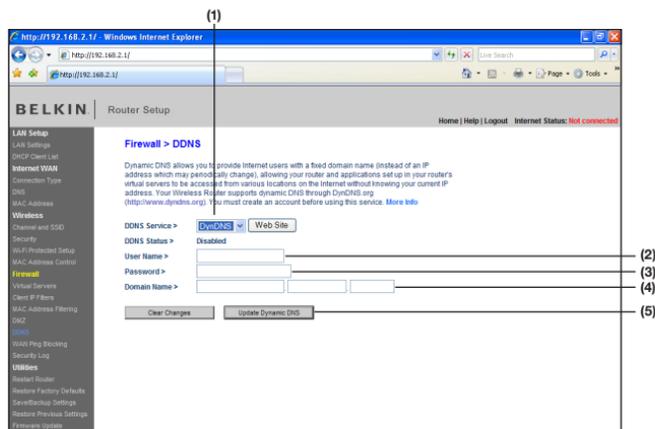
Blocking an ICMP Ping

Computer hackers use what is known as "pinging" to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an ICMP ping from the outside. This heightens your Router's security level.

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

Utilities

The "Utilities" screen lets you manage different parameters of the Router and perform certain administrative functions.

Restarting the Router

Sometimes it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.

Restarting the Router to Restore Normal Operation

1. Click the "Restart Router" button.

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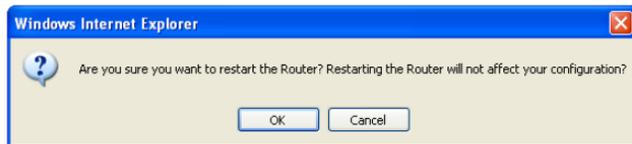
3. The following message will appear. Restarting the Router can take up to 60 seconds. It is important not to turn off the power to the Router during the restart.

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

Saving a Current Configuration

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.
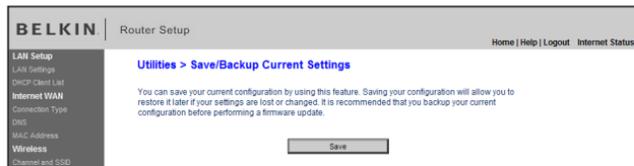
1. Click "Save". A window called "File Download" will open. Click "Save".

2. A window will open that allows you to select the location where you want to save the configuration file. Select a location. You can name the file anything you want, or use the default name "user.conf". Be sure to name the file so you can locate it yourself later. When you have selected the location and name of the file, click "Save".
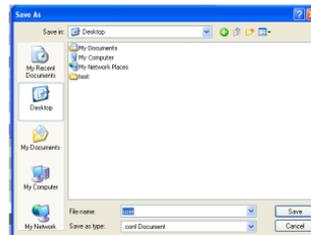
3. When the save is complete, you will see the window below. Click "Close".
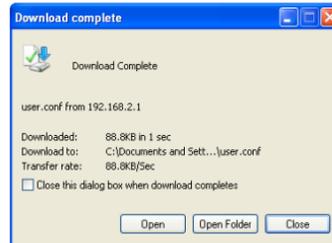
4. The configuration is now saved.

Restoring a Previous Configuration

This option will allow you to restore a previously saved configuration.
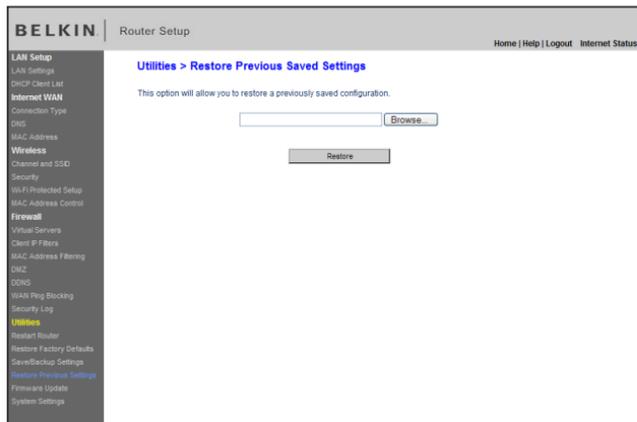
1. Click "Browse". A window will open that allows you to select the location of the configuration file. All configuration files end with a ".conf". Locate the configuration file you want to restore and double-click on it.
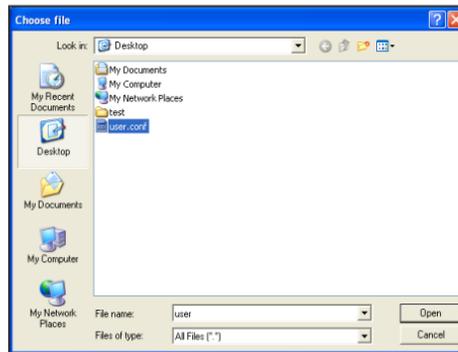
2. You will be asked if you want to continue. Click "OK".

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

Windows Internet Explorer

⚠ After settings are restored, the Router may not respond
to commands for as long as one minute.
This is normal. Do not power down the Router during this time.

OK

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

Updating the Firmware

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may have existed. When Belkin releases new firmware, you can download the firmware from the Belkin update website and update your Router's firmware to the latest version.

Checking for a New Version of Firmware

The "Check Firmware" **(1)** button allows you to instantly check for a new version of firmware. When you click the button, a new browser window will appear informing you that either no new firmware is available or that there is a new version available. If a new version is available, you will have the option to download it.
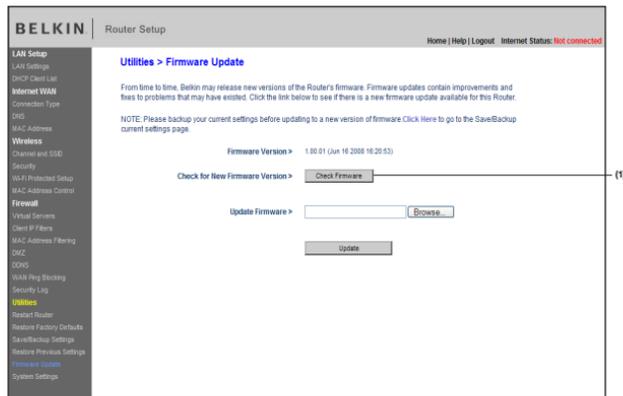
Downloading a New Version of Firmware

If you click the "Check Firmware" button and a new version of firmware is available, you will see a screen similar to the one below:

Update Available
An updated version of firmware is available
for your Router

Model:
F5D8636-4 N Wireless Modem Router

Firmware Version Information:
Belkin Wireless Modem Router Version : 1.00.01
Release Date : 6/17/2008
Image location :
http://networking.belkin.com/update/files/F5D8636-
4/v1/WW/F5D8636-4_WW_1.00.01.bin

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

Click here for full instructions
*NOTE: You will need Adobe Acrobat Reader to
view this document.* Click here to get Adobe
Acrobat Reader

Download Firmware NOW

Download New Manual NOW

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

A window will open that allows you to select the location where you want to save the firmware file. Select a location. You can name the file anything you want, or use the default name. Be sure to locate the file in a place where you can locate it yourself later. When you have selected the location, click "Save".

2. When the save is complete, you will see the following window. Click "Close".
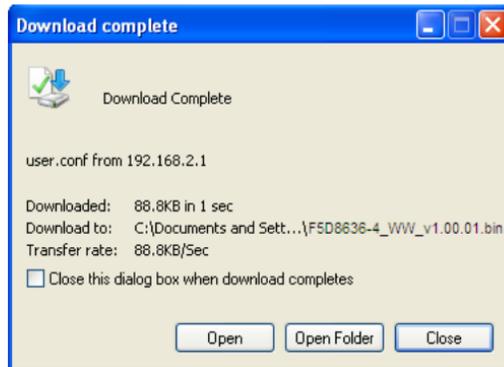
3. The download of the firmware is complete. To update the firmware, follow the next steps in "Updating the Router's Firmware".

Updating the Router's Firmware

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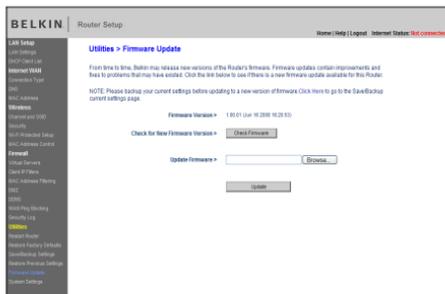
2. Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.

The "Update Firmware" box will now display the location and name of the firmware file you just selected. Click "Update".
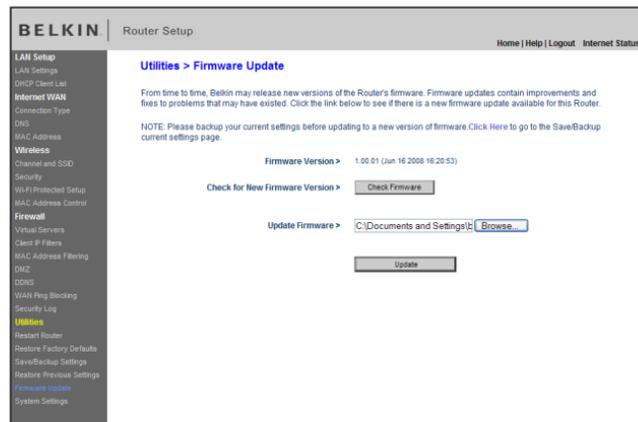
3. You will be asked if you are sure you want to continue. Click "OK".

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

Windows Internet Explorer

⚠ At the end of the upgrade, the Router may not respond to commands for as long as one minute. This is normal. Do not turn off or reboot the Router during this time.

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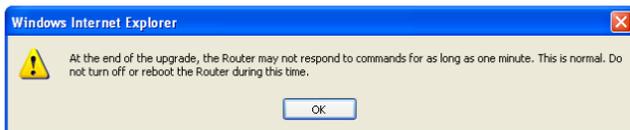
5. A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router firmware update will be complete. The Router home page should appear automatically. If not, type in the Router's address (default = 192.168.2.1) into the navigation bar of your browser.

Changing System Settings

The "System Settings" page is where you can enter a new administrator password, set the time zone, enable remote management, and turn on and off the NAT function of the Router.

Setting or Changing the Administrator Password

The Router ships with NO password entered. If you wish to add a password for greater security, you can set a password here. Write down your password and keep it in a safe place, as you will need it if you need to log into the Router in the future. It is also recommended that you set a password if you plan to use the remote management feature of your Router.

BELKIN | Router Setup

Home | Help | Logout   Internet Status:

LAN Setup
LAN Settings
DHCP Client List

Internet WAN
Connection Type
DNS
MAC Address

Wireless
Channel and SSID
Security
Wi-Fi Protected Setup
MAC Address Control
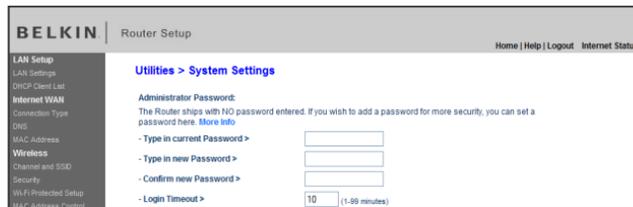
Utilities > System Settings

Administrator Password:

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. More Info

- Type in current Password >

- Type in new Password >

- Confirm new Password >

- Login Timeout >   10   (1-99 minutes)

Changing the Login Time-Out Setting

The login time-out option allows you to set the period of time that you can be logged into the Router's advanced setup interface. The timer starts when there has been no activity. For example, imagine you have made some changes in the advanced setup interface, then left your computer alone without clicking "Logout". Assuming the time-out is set to 10 minutes, 10 minutes after you leave, the login session will expire. You will have to log into the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes. Note: Only one computer can be logged into the Router's advanced setup interface at one time.

Setting the Time and Time Zone

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in. You have the option to select a primary and a backup NTP server to keep your Router's clock synchronized. Select your desired NPT server from the drop-down box, or simply keep it as is.

If you reside in an area that observes daylight saving, then place a check mark in the box next to "Enable Daylight Saving". The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

Time and Time Zone:	June 26, 2008 2:58:56 PM
Please set your time Zone. If you are in an area that observes daylight saving check this box. More Info	
- Time Zone >	(GMT) Greenwich Mean Time: Lisbon, London
- Daylight Savings >	☑ Automatically Adjust Daylight Saving
- Primary NTP Server >	129.132.2.21-Europe
- Backup NTP Server >	130.149.17.8-Europe

Enabling Remote Management

Before you enable this advanced feature of your Belkin Router, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD. Remote management allows you to make changes to your Router's settings from anywhere on the Internet. There are two methods of remotely managing the Router. The first is to allow access to the Router from anywhere on the Internet by selecting "Any IP address can remotely manage the Router". By typing in your WAN IP address from any computer on the Internet, you will be presented with a login screen where you need to type in the password of your Router.

The second method is to allow a specific IP address only to remotely manage the Router. This is more secure, but less convenient. To use this method, enter the IP address you know you will be accessing the Router from in the space provided and select "Only this IP address can remotely manage the Router". Before you enable this function, it is STRONGLY RECOMMENDED that you set your administrator password. Leaving the password empty will potentially open your Router to intrusion.

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

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

☐ Any IP address can remotely manage the router.

- Only this IP address can remotely manage the router >   [   ] . [   ] . [   ] . [   ]

- Remote Access Port >   [8080]

Enabling/Disabling UPnP

UPnP (Universal Plug-and-Play) is yet another advanced feature offered by your Belkin Router. It is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports, and in some instances, setting trigger ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature enabled. If you want to disable this feature, simply select "Disable" in the "UPnP Enabling" section of the "Utilities" page. Click "Apply Changes" to save the change.

UPNP Enabling:
ADVANCED FEATURE! Allows you to turn the UPNP feature of the Router on or off. If you use applications that support UPnP, enabling UPnP will allow these applications to automatically configure the router. **More Info**

- **UPNP Enable / Disable >**   ⊙ Enable ○ Disable

USING THE WEB-BASED ADVANCED USER INTERFACE

Enabling/Disabling Auto Firmware Update

This innovation provides the Router with the built-in capability to automatically check for a new version of firmware and alert you that the new firmware is available. When you log into the Router's advanced interface, the Router will perform a check to see if new firmware is available. If so, you will be notified. You can choose to download the new version or ignore it.

Auto Update Firmware Enabling:

ADVANCED FEATURE! Allows you to automatically check the availability of firmware updates for your router.More Info

- **Auto Update Firmware Enable / Disable >**   ○ Enable ⊙ Disable

| Clear Changes | Apply Changes |

MANUALLY CONFIGURING NETWORK SETTINGS

Set up the computer that is connected to the cable or DSL modem FIRST using these steps. You can also use these steps to add computers to your Router after the Router has been set up to connect to the Internet.

Manually Configuring Network Settings in Mac OS up to 9.x

1. Pull down the Apple menu. Select "Control Panels" and select "TCP/IP".

2. You will see the TCP/IP control panel. Select "Ethernet Built-In" or "Ethernet" in the "Connect via:" drop-down menu **(1)**.

3. Next to "Configure" **(2)**, if "Manually" is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.
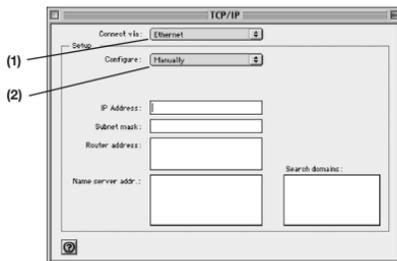
IP address: [ ]

Subnet Mask: [ ]

Router Address: [ ]

Name Server Address: [ ]

4. If not already set, at "Configure:", choose "Using DHCP Server". This will tell the computer to obtain an IP address from the Router.
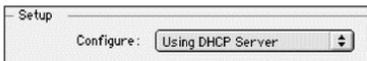
5. Close the window. If you made any changes, the following window will appear. Click "Save".
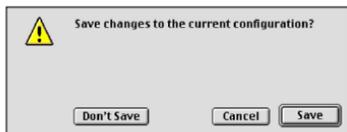
Restart the computer. When the computer restarts, your network settings are now configured for use with the Router.

Manually Configuring Network Settings in Mac OS X

1. Click on the "System Preferences" icon.

Select "Network" **(1)** from the "System Preferences" menu.
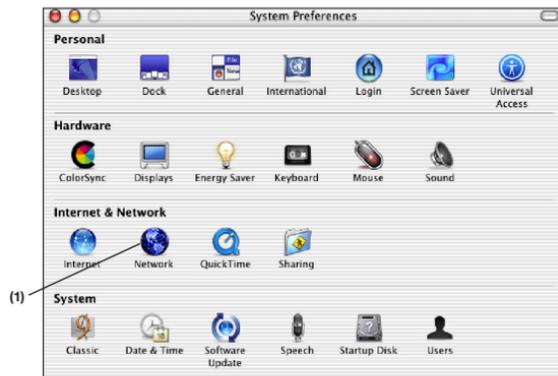
3. Select "Built-in Ethernet" **(2)** next to "Show" in the Network menu.
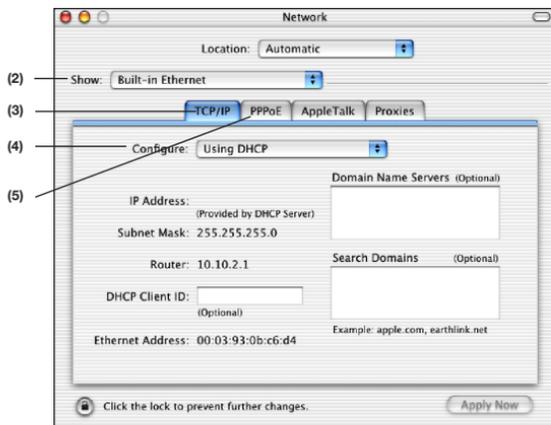
4. Select the "TCP/IP" tab **(3)**. Next to "Configure" **(4)**, you should see "Manually" or "Using DHCP". If you do not, check the PPPoE tab **(5)** to make sure that "Connect using PPPoE" is NOT selected. If it is, you will need to configure your Router for a PPPoE connection type using your user name and password.

5. If "Manually" is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

IP address:	
Subnet Mask:	
Router Address:	
Name Server Address:	

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

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

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

1. Click "Start", "Settings", then "Control Panel".

2. Double-click on the "Network and dial-up connections" icon (Windows 2000) or the "Network" icon (Windows XP).

3. Right-click on the "Local Area Connection" associated with your network adapter and select "Properties" from the drop-down menu.

4. In the "Local Area Connection Properties" window, click "Internet Protocol (TCP/IP)" and click the "Properties" button. The following screen will appear:
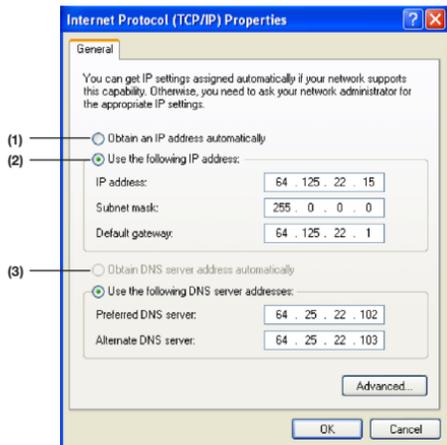
5. If "Use the following IP address" **(2)** is selected, your Router will need to be set up for a static IP connection type. Write the address information the table below. You will need to enter this information into the Router.

IP address:	
Subnet Mask:	
Router Address:	
Name Server Address:	

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

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

Manually Configuring Network Settings in Windows 98 or Me

1. Right-click on "My Network Neighborhood" and select "Properties" from the drop-down menu.

2. Select "TCP/IP -> settings" for your installed network adapter. You will see the following window.
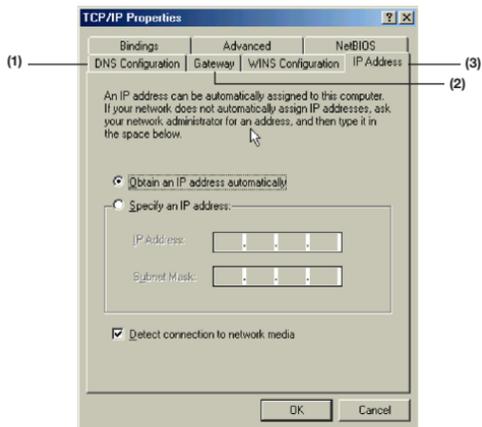
3. If "Specify and IP address" is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

4. Write the IP address and subnet mask from the "IP Address" tab **(3)**.

5. Click the "Gateway" tab **(2)**. Write the gateway address down in the chart.

6. Click the "DNS Configuration" tab **(1)**. Write the DNS address(es) in the chart.

IP address:	
Subnet Mask:	
Router Address:	
Name Server Address:	

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

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

RECOMMENDED WEB BROWSER SETTINGS

In most cases, you will not need to make any changes to your web browser's settings. If you are having trouble accessing the Internet or the Web-Based Advanced User Interface, then change your browser's settings to the recommended settings in this section.

Microsoft® Internet Explorer 4.0 or Higher

1. Start your web browser. Select "Tools" then "Internet Options".
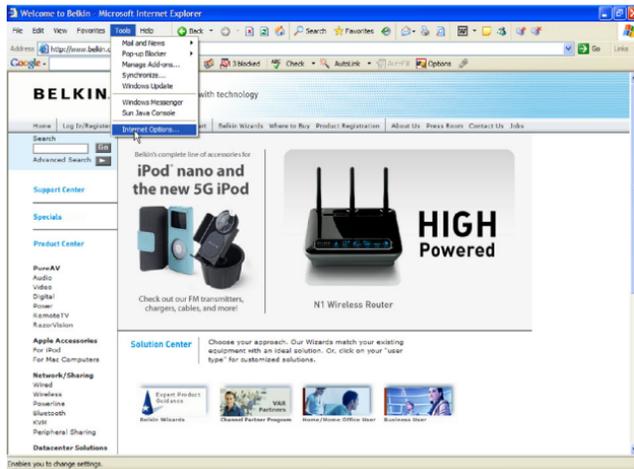
2. In the "Internet Options" screen, there are three selections: "Never dial a connection", "Dial whenever a network connection is not present", and "Always dial my default connection". If you can make a selection, select "Never dial a connection". If you cannot make a selection, go to the next step.

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

4. Make sure there are no check marks next to any of the displayed options: "Automatically detect settings", "Use automatic configuration script", and "Use a proxy server". Click "OK". Then click "OK" again in the "Internet Options" page.
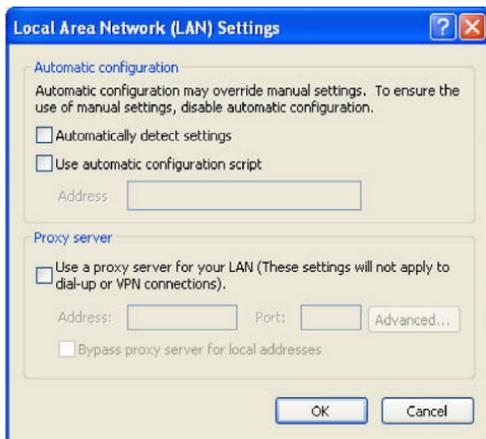
Netscape® Navigator® 4.0 or Higher

1. Start Netscape. Click on "Edit" then "Preferences".

2. In the "Preferences" window, click on "Advanced" then select "Proxies". In the "Proxies" window, select "Direct connection to the Internet".
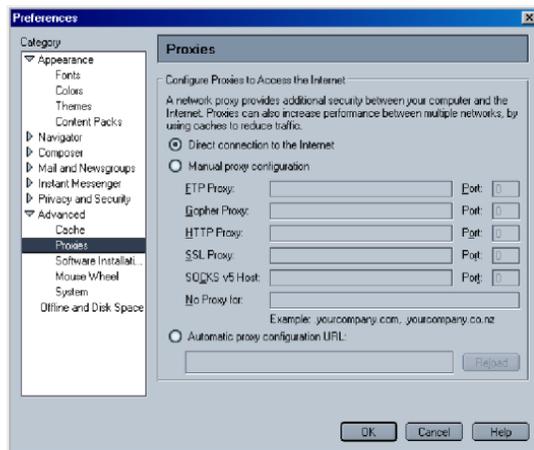
TROUBLESHOOTING

Problem:

Installation CD does not automatically start.

Solution:

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

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

2. Next, double-click on the CD-ROM drive that the Setup Assistant Software CD has been placed in to start the installation.
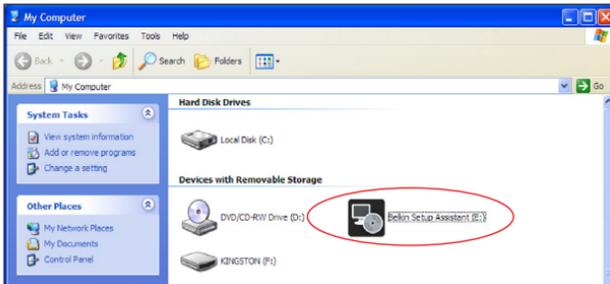
3. The Setup Assistant should start within a few seconds. If, instead, a window appears showing the files on the CD, double-click on the icon labeled "SetupAssistant.exe".
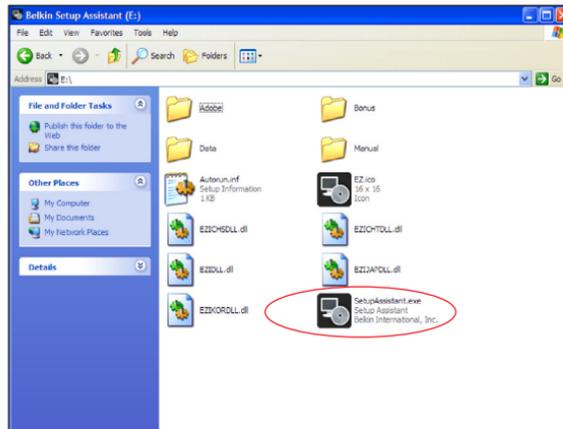
4. If the Setup Assistant still does not start, reference the section titled "Manually Configuring Network Settings" (page 74 of this User Manual) for an alternate setup method.

Problem:

The Setup Assistant cannot find my Router.

Solution:

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

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

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

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

2. Unplug power to the Router for 10 seconds, and then plug the power back into the Router. Ensure that the Router's Power light is on; it should be solid green. If not, check to make sure that the AC adapter is correctly connected to the Router and plugged into a wall outlet.

3. Ensure that you have a cable (use the cable included with the Router) connected between (1) the network (Ethernet) port on the back of the computer and (2) one of the LAN ports, labeled "1" through "4", on the back of the Router.

Note: The computer should NOT be connected to the port labeled "Modem" on the back of the Router.

4. Try shutting down and restarting your computer, then rerunning the Setup Assistant.

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

Problem:

The Setup Assistant cannot connect my Router to the Internet.

Solution:

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

1. Use the troubleshooting suggestions within the Setup Assistant. If the troubleshooting screen does not open automatically, click on the "Troubleshoot" button in the lower, right-hand corner of the Setup Assistant window.

2. If your ISP requires a user name and password, make sure that you have typed in your user name and password correctly. Some user names require that the ISP's domain be at the end of the name. Example: "myname@myisp.com". The "@myisp.com" part of the user name may need to be typed as well as your user name.

If you continue to have no Internet connection, reference the section titled "Manually Configuring Network Settings" (page 74 of this User Manual) for alternate setup method.

Problem:

- The Setup Assistant completed installation, but my web browser doesn't work.

- I am unable to connect to the Internet. The Router's "Internet" light is off and the "Modem" light is blinking.

Solution:

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

1. Make sure the network cable between the modem and the Router is connected. We strongly recommend using the cable that was supplied with your cable or DSL modem for this purpose. The cable should be connected at one end to the Router's "Modem" port, and at the other end to the network port on your modem.

2. Unplug the cable or DSL modem from its power source for three minutes. After three minutes, plug the modem back into its power source. This may force the modem to properly recognize the Router.

3. Unplug the power to your Router, wait 10 seconds, and then reconnect the power. This will cause the Router to reattempt communication with the modem.

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

4. Try shutting down and restarting your computer.

Problem:

• The Setup Assistant completed installation, but my web browser doesn't work.

• I am unable to connect to the Internet. The Router's "Modem" light is on and the "Internet" light is blinking.

Solution:

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

• If you have a "static IP address" connection, your ISP must assign you the IP address, subnet mask, and gateway address. Please refer to the section entitled "Alternate Setup Method" for details on changing this setting.

• If you have a "PPPoE" connection, your ISP will assign you a user name and password and sometimes a service name. Make sure the Router connection type is configured to PPPoE and the settings are entered properly. Please refer to the section entitled "Alternate Setup Method" for details on changing this setting.

• You may need to configure your Router to meet the specific requirements of your ISP. To search our Knowledge Base for ISP-specific issues, go to: http://web.belkin.com/support and type in "ISP"

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

Problem:

• The Setup Assistant completed, but my web browser doesn't work.

• I am unable to connect to the Internet. The "Modem" light on my Router is blinking and the "Internet" light is solid.

Solution:

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

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

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

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

Problem:

I can't connect to the Internet wirelessly.

Solution:

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

1. Look at the lights on your Router. Your Belkin Router's lights should be as follows:

• The "Power" light should be on.

• The "Internet" light should be on and not blinking.

• The "Modem" light should be either on or blinking.

2. Open your wireless utility software by clicking on the icon in the system tray at the bottom, right-hand corner of the screen. If you are also using a Belkin Wireless Card or Adapter with this Router, the tray icon should look like this

3. The exact window that opens will vary depending on the model of wireless card you have; however, any of the utilities should have a list of "Available Networks"—those wireless networks it can connect to.

Does the name of your wireless network appear in the results?

Yes, my network name is listed—go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, but my network name is listed".

No, my network name is not listed—go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, and my network name is not listed".

Problem:

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

Solution:

If the name of your network is listed in the "Available Networks" list, please follow the steps below to connect wirelessly:

1. Click on the correct network name in the "Available Networks" list.

2. If the network has security (encryption) enabled, you will need to enter the network key. For more information regarding security, see the section entitled "Securing your Wi-Fi Network" in this User Manual.

3. Within a few seconds, the tray icon in the lower, left-hand corner of your screen should turn green, indicating a successful connection to the network.

Problem:

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

Solution:

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

1. Temporarily move your computer, if possible, five to 10 feet away from the Router. Close the wireless configuration utility, and reopen it. If the correct network name now appears under "Available Networks", you may have a range or interference problem. Please see the suggestions discussed in the section titled "Placement of your Router for Optimal Performance" in this User Manual.

2. Using a computer that is connected to the Router through a network cable (as opposed to wirelessly), ensure that "Broadcast SSID" is enabled. This setting is found on the Router's wireless "Channel and SSID" configuration page.

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

Problem:

My wireless network performance is inconsistent.

Data transfer is sometimes slow.

Signal strength is poor.

I am having difficulty establishing and/or maintaining a Virtual Private Network (VPN) connection.

Solution:

Wireless technology is radio-based, which means connectivity and the throughput performance between devices decreases when the distance between devices increases. Other factors that will cause signal degradation (metal is generally the worst culprit) are obstructions such as walls and metal appliances. As a result, the typical indoor range of your wireless devices will be between 100 to 200 feet. Note also that connection speed may decrease as you move farther away from the Router or access point.

In order to determine if wireless issues are related to range, we suggest temporarily moving the computer, if possible, five to 10 feet away from the Router.

Changing the Wireless Channel

Depending on local wireless traffic and interference, switching the wireless channel of your network can improve performance and reliability. The default channel the Router is shipped with is channel 11. You may choose from several other channels depending on your region (see the section titled "Changing the Wireless Channel" on page 43 for instructions on how to choose other channels).

Limiting the Wireless Transmit Rate

Limiting the wireless transmit rate can help improve the maximum wireless range, and connection stability. Most wireless cards have the ability to limit the transmission rate. To change this property, go to the Windows Control Panel, open "Network Connections" and double-click on your wireless card's connection. In the "Properties" dialog, select the "Configure" button on the "General" tab (Windows 98 users will have to select the wireless card in the list box and then click "Properties"), then choose the "Advanced" tab and select the rate property. Wireless client cards are usually set to automatically adjust the wireless transmit rate for you, but doing so can cause periodic disconnects when the wireless signal is too weak; as a rule, slower transmission rates are more stable. Experiment with different connection rates until you find the best one for your environment; note that all available transmission rates should be acceptable for browsing the Internet. For more assistance, see your wireless card's user manual.

Problem:

How do I extend the range of my wireless network?

Solution:

Belkin recommends using one of the following products to extend wireless network coverage throughout large homes or offices:

•   Wireless Access Point: A wireless access point can effectively double the coverage area of your wireless network. An access point is typically placed in the area not currently covered by your G Wireless Router, and is connected to the Router using either an Ethernet cable or through your home's power lines using two Powerline Ethernet Adapters.

•   For 802.11g (54g™) wireless networks, Belkin offers a Wireless G Range Extender/Access Point that can be connected wirelessly to a Belkin G Wireless Router, without requiring an Ethernet cable or Powerline Ethernet Adapters.

These Belkin products are available at your local retailer, or can be ordered from Belkin directly.

For network/range extension information, please visit: www.belkin.com/networking to find out more about:

Wireless G Range Extender/Access Point (F5D7130)

Powerline Ethernet Adapter (F5D4070)

Powerline USB Adapter (F5D4050)

TROUBLESHOOTING

Problem:

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

Solution:

1. Log into your Wireless Router or Access Point.

Open your web browser and type in the IP address of the Wireless Router or Access Point. (The Router's default is 192.168.2.1, the Access Point's default is 192.168.2.254.) Log into your Router by clicking on the "Login" button in the top, right-hand corner of the screen. You will be asked to enter your password. If you never set a password, leave the password field blank and click "Submit".

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

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

3. After selecting your WEP encryption mode, you can type in your hex WEP key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a WEP key from the passphrase. Click "Apply Changes" to finish. You must now set all of your clients to match these settings. A hex (hexadecimal) key is a combination of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 hex keys.

For example:

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

4. Click "Apply Changes" to finish. Encryption in the Wireless Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

WARNING: If you are configuring the Wireless Router or Access Point from a computer with a wireless client, you will need to ensure that security is turned on for this wireless client. If this is not done, you will lose your wireless connection.

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

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Belkin client card (Wireless Network Card or Adapter).

Solution:

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

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

2. Once the "Advanced" button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin client card.

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

4. Under "Data Encryption", select "WEP".

5. Ensure the box "The key is provided for me automatically" at the bottom is unchecked. If you are using this computer to connect to a corporate network, please consult your network administrator if this box needs to be checked.

6. Type your WEP key in the "Network key" box.

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

For example: **C3030FAF4BB2C3D44BC3D4E7E4** = 128-bit key

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

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

Problem:

Do Belkin products support WPA?

Solution:

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this publication, a security patch download is available, for free, from Microsoft. This patch works only with the Windows XP operating system.

Download the patch here:

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

You also need to download the latest driver for your Belkin Wireless 802.11g Desktop or Notebook Network Card from the Belkin support site. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as Belkin wireless products.

Download the latest driver at http://web.belkin.com/support

Problem:

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

Solution:

1. From the "Security Mode" drop-down menu, select "WPA-PSK".

2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.

3. Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, symbols, or spaces. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".

4. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Problem:

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

Solution:

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

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

2. Once the "Advanced" button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin client card.

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

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

5. Type your WPA key in the "Network key" box.

> **IMPORTANT:** WPA-PSK is a combination of numbers and letters from A-Z and 0-9. For WPA-PSK, you can enter eight to 63 characters. This network key needs to match the key you assign to your G Wireless Router or access point.

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

Problem:

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

Solution:

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

2. Once the "Advanced" button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin client card.

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

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

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

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

Problem:

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

Solution:

If you are NOT using a Belkin WPA Wireless Desktop or Wireless Notebook Network Card and it is not equipped with WPA-enabled software, a file from Microsoft called "Windows XP Support Patch for Wireless Protected Access" is available for free download:

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

Note: The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time. You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.

Supported Operating Systems:

• Windows XP Professional

• Windows XP Home Edition

Enabling WPA-PSK

1. In systems running Windows XP, click "Start > Control Panel > Network Connections".

2. Right-click on the "Wireless Networks" tab. The "Wireless Network Connection Properties" screen appears. Ensure the "Use Windows to configure my wireless network settings" box is checked.

3. Under the "Wireless Networks" tab, click the "Configure" button, and you will see the client card properties screen.

4. For a home or small business user, select "WPA-PSK" under "Network Administration".

5. Select "TKIP" or "AES" under "Date Encryption". This setting will have to be identical to the G Wireless Router or access point that you set up.

6. Type in your encryption key in the "Network key" box.

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

7. Click "OK" to apply settings.

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

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

Wireless Comparison Chart

Wireless Technology	G (802.11g)	Enhanced (1x1 draft 802.11n)	N MIMO (draft 802.11n with MIMO)	N1 MIMO (draft 802.11n with MIMO)
Speed/Data Rate*	Up to 54Mbps*	Up to 150Mbps*	Up to 300Mbps*	Up to 300Mbps*
Frequency	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz
Compatibility	Compatible with 802.11b/g	Compatible with 802.11b/g, draft 802.11n, and Belkin G+ MIMO	Compatible with draft 802.11n and 802.11b/g	Compatible with draft 802.11n and 802.11b/g
Coverage*	Up to 400 ft.*	Up to 600 ft.*	Up to 1,200 ft.*	Up to 1,400 ft.*
Advantage	Common—widespread use for Internet sharing	Better coverage and consistent speed and range	Enhanced speed and coverage	Leading edge—best coverage and throughput

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

Technical Support

You can find technical support information at http://www.belkin.com/networking or www.belkin.com/support/.

Technical Support

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

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

*Local rates apply.

COUNTRY	NUMBER	INTERNET ADRESS
AUSTRIA	0820 200766	www.belkin.com/uk/networking/
BELGIUM	07 07 00 073	www.belkin.com/nl/networking/
CZECH REPUBLIC	239 000 406	www.belkin.com/uk/networking/
DENMARK	701 22 403	www.belkin.com/uk/networking/
FINLAND	097 25 19 123	www.belkin.com/uk/networking/
FRANCE	08 - 25 54 00 26	www.belkin.com/fr/networking/
GERMANY	0180 - 500 57 09	www.belkin.com/de/networking/
GREECE	00800 - 44 14 23 90	www.belkin.com/uk/networking/
HUNGARY	06 - 17 77 49 06	www.belkin.com/uk/networking/
ICELAND	800 8534	www.belkin.com/uk/networking/
IRELAND	0818 55 50 06	www.belkin.com/uk/networking/
ITALY	02 - 69 43 02 51	www.belkin.com/it/networking/
LUXEMBOURG	34 20 80 85 60	www.belkin.com/uk/networking/
NETHERLANDS	0900 - 040 07 90 €0.10 per minute	www.belkin.com/nl/networking/
NORWAY	81 50 0287	www.belkin.com/uk/networking/
POLAND	00800 - 441 17 37	www.belkin.com/uk/networking/
PORTUGAL	707 200 676	www.belkin.com/uk/networking/
RUSSIA	495 580 9541	www.belkin.com/networking/
SOUTH AFRICA	0800 - 99 15 21	www.belkin.com/uk/networking/
SPAIN	902 - 02 43 66	www.belkin.com/it/networking/
SWEDEN	07 - 71 40 04 53	www.belkin.com/it/networking/
SWITZERLAND	08 - 48 00 02 19	www.belkin.com/uk/networking/
UNITED KINGDOM	0845 - 607 77 87	www.belkin.com/uk/networking/
OTHER COUNTRIES	+44 - 1933 35 20 00	

INFORMATION

EU DECLARATION OF CONFORMITY

Česky [Czech]	*[Belkin Ltd]* tímto prohlašuje, že tento *[F5D8636-4]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *[Belkin Ltd]* erklærer herved, at følgende udstyr *[F5D8636-4]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *[Belkin Ltd]*, dass sich das Gerät *[F5D8636-4]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *[Belkin Ltd]* seadme *[F5D8636-4]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *[Belkin Ltd]*, declares that this *[F5D8636-4]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *[Belkin Ltd]* declara que el *[F5D8636-4]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[Belkin Ltd]* ΔΗΛΩΝΕΙ ΟΤΙ *[F5D8636-4]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *[Belkin Ltd]* déclare que l'appareil *[F5D8636-4]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *[Belkin Ltd]* dichiara che questo *[F5D8636-4]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[Belkin Ltd Belkin Ltd]* deklarē, ka *[F5D8636-4 / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[Belkin Ltd]* deklaruoja, kad šis *[F5D8636-4]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *[Belkin Ltd]* dat het toestel *[F5D8636-4]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *[Belkin Ltd]*, jiddikjara li dan *[F5D8636-4]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *[Belkin Ltd]* nyilatkozom, hogy a *[F5D8636-4]* megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym *[Belkin Ltd]* oświadcza, że *[F5D8636-4]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*[Belkin Ltd]* declara que este *[F5D8636-4]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	*[I Belkin Ltd]* izjavlja, da je ta *[F5D8636-4]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Belkin Ltd]* týmto vyhlasuje, že *[F5D8636-4]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

Suomi [Finnish]	*[Belkin Ltd]* vakuuttaa täten että *[F5D8636-4]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *Belkin Ltd]* att denna *[F5D8636-4]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *[Belkin Ltd]* yfir því að *[F5D8636-4]* er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*[Belkin Ltd]* erklærer herved at utstyret *[F5D8636-4]* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

http://www.belkin.com/doc/

For information on product disposal please refer to
http://environmental.belkin.com

CE Ⓘ

FOR USE IN AT BE CY CZ DK EE FI FR DE GR HU IE
IT LV LT LU MT NL PL PT SK SI ES SE GB IS LI
NO CH BG RO TR **OPERATES ON CHANNELS 1-13**

Restricted Use in Certain Countries................................**Class 2 Equipment**

Belkin International, Inc., Limited Lifetime Product Warranty

What this warranty covers.

Belkin International, Inc. ("Belkin") warrants to the original purchaser of this Belkin product that the product shall be free of defects in design, assembly, material, or workmanship.

What the period of coverage is.

Belkin warrants the Belkin product for the lifetime of the product.

What will we do to correct problems?

Product Warranty.

Belkin will repair or replace, at its option, any defective product free of charge (except for shipping charges for the product). Belkin reserves the right to discontinue any of its products without notice, and disclaims any limited warranty to repair or replace any such discontinued products. In the event that Belkin is unable to repair or replace the product (for example, because it has been discontinued), Belkin will offer either a refund or a credit toward the purchase of another product from Belkin.com in an amount equal to the purchase price of the product as evidenced on the original purchase receipt as discounted by its natural use.

What is not covered by this warranty?

All above warranties are null and void if the Belkin product is not provided to Belkin for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin determines that the Belkin product has been improperly installed, altered in any way, or tampered with. The Belkin Product Warranty does not protect against acts of God such as flood, earthquake, lightning, war, vandalism, theft, normal-use wear and tear, erosion, depletion, obsolescence, abuse, damage due to low voltage disturbances (i.e. brownouts or sags), non-authorized program, or system equipment modification or alteration.

How to get service.

To get service for your Belkin product you must take the following steps:

1.   Contact Belkin Tech Support at the number listed on page 93, within 15 days of the Occurrence. Be prepared to provide the following information:

     a. The part number of the Belkin product.

     b. Where you purchased the product.

     c. When you purchased the product.

     d. Copy of original receipt.

2.   Your Belkin Customer Service Representative will then instruct you on how to forward your receipt and Belkin product and how to proceed with your claim.

Belkin reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin for inspection shall be borne solely by the purchaser. If Belkin determines, in its sole discretion, that it is impractical to ship the damaged equipment to Belkin, Belkin may designate, in its sole discretion, an equipment repair facility to inspect and estimate the cost to repair such equipment. The cost, if any, of shipping the equipment to and from such repair facility and of such estimate shall be borne solely by the purchaser. Damaged equipment must remain available for inspection until the claim is finalized. Whenever claims are settled, Belkin reserves the right to be subrogated under any existing insurance policies the purchaser may have.

How state law relates to the warranty.

THIS WARRANTY CONTAINS THE SOLE WARRANTY OF BELKIN, THERE ARE NO OTHER WARRANTIES, EXPRESSED OR, EXCEPT AS REQUIRED BY LAW, IMPLIED, INCLUDING THE IMPLIED WARRANTY OR CONDITION OF QUALITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND SUCH IMPLIED WARRANTIES, IF ANY, ARE LIMITED IN DURATION TO THE TERM OF THIS WARRANTY.

Some states do not allow limitations on how long an implied warranty lasts, so the above limitations may not apply to you.

IN NO EVENT SHALL BELKIN BE LIABLE FOR INCIDENTAL, SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL OR MULTIPLE DAMAGES SUCH AS, BUT NOT LIMITED TO, LOST BUSINESS OR PROFITS ARISING OUT OF THE SALE OR USE OF ANY BELKIN PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This warranty gives you specific legal rights, and you may also have other rights, which may vary from state to state. Some states do not allow the exclusion or limitation of incidental, consequential, or other damages, so the above limitations may not apply to you.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.   These limits are designed to provide reasonable protection against harmful interference in a residential installation.   This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.   However, there is no guarantee that interference will not occur in a particular installation.   If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

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

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

FCC Part 68 REQUIREMENTS

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: BKCDL01BF5D7634V2. If requested, this number must be provided to the telephone company.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: BKCDL01BF5D7634V2. The digits represented by 01 are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

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

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

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

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

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

COMPANY:
   Belkin International, Inc.
ADDRESS:
   501 West Walnut Street, Compton, CA 90220-5221
TEL NO:
   1 (310) 604-2315

belkin.com

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

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt,
France

Belkin GmbH
Hanebergstrasse 2
80637 Munich
Germany

Belkin Iberia
C/ Anabel Segura, 10 planta baja, Of· 2
28108, Alcobendas, Madrid
Spain

Belkin Italy & Greece
Via Carducci, 7
Milano 20123
Italy

Belkin B·V·
Boeing Avenue 333
1119 PH Schiphol-Rijk,
Netherlands

PM01527ea-C   F5D8636-4 v2