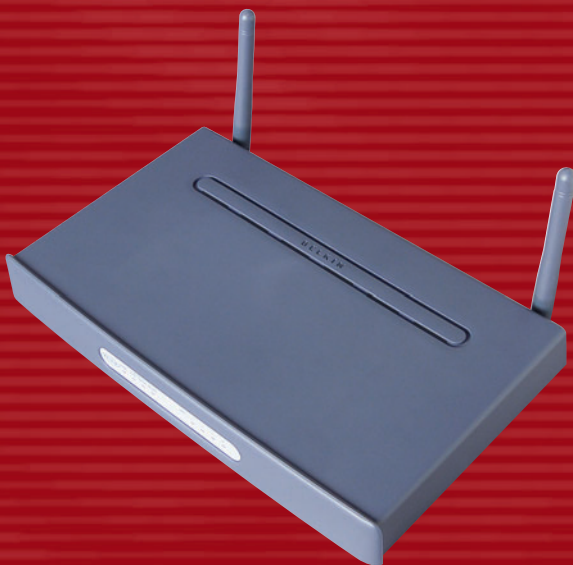


**BELKIN**

# ADSL Modem with Built-In 802.11g Wireless Router

*Network your computers with this one-box  
solution that connects and shares your ADSL  
Internet access*



**User Manual**

F5D7630-4A

F5D7630-4B

## TABLE OF CONTENTS

Introduction .....	1
Overview .....	1
Key Features .....	1
Package Contents .....	3
System Requirements .....	3
Knowing your Router .....	4
Placement of your Router .....	7
Connecting and Configuring your Router .....	8
Navigating the Web Browser Interface .....	14
Understanding the Web-Based User Interface .....	17
Manually Configuring Network Settings .....	48
Glossary .....	55
Troubleshooting .....	61
Information .....	63

# INTRODUCTION

Thank you for purchasing the ADSL Modem with Built-In 802.11g Wireless Router (the Router). In minutes, you will be able to share your Internet connection and network your computers. The following is a list of features that make your new Router an ideal solution for your home or small office network.

## OVERVIEW

### Key Features

#### **Integrated 802.11g Wireless Access Point**

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

#### **Works with Both PCs and Mac® Computers**

The Wireless ADSL Modem Router supports a variety of networking environments including Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98, Me, NT®, 2000, and XP, and others. All that is needed is an Internet browser and a network adapter that supports TCP/IP (the standard language of the Internet).

#### **Front-Panel LED Display**

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

#### **Web-Based User Interface**

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

#### **NAT IP Address Sharing**

Your Router employs Network Address Translation (NAT) to share the single IP address assigned to you by your Internet Service Provider while saving the cost of adding additional IP addresses to your Internet service account.

# INTRODUCTION

## **SPI Firewall**

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

## **Integrated 10/100 4-Port Switch**

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

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

## **MAC Address Filtering**

For added security, you can set up a list of MAC addresses (unique client identifiers) that are allowed access to your network. Every network interface card has its own unique MAC address. Simply enter these MAC addresses into a list using the web-based user interface and you can control access to your network.

## **Applications and Advantages**

- Economically connect multiple computers to a single Internet connection
- SOHO (Small Office/Home Office) networking needs  
Provides the easy and quick small network installation SOHO users need

# INTRODUCTION

## Package Contents

- ADSL Modem with Built-In 802.11g Wireless Router
- RJ45 Ethernet Networking Cable (for connecting the Router to the computer)
- RJ11 Phone Line Cord (for connecting the Router to the ADSL line)\*
- ADSL In-Line Filter\*
- Power Supply
- Quick Installation Guide
- User Manual CD-ROM
- Registration Card

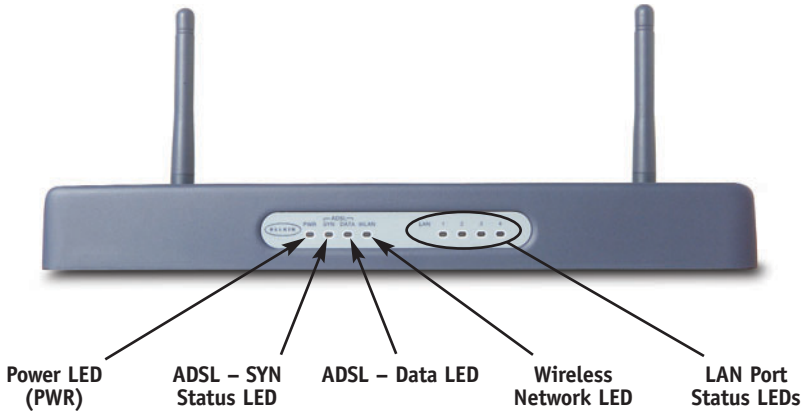
## System Requirements

- ADSL connection
- At least one computer with an installed network interface adapter
- TCP/IP networking protocol installed on each computer
- CAT5 networking cable (or better)
- Microsoft® Internet Explorer 4.0 or later, or Netscape® 4.0 or later

\* *Germany excluded (Provided by local ISP)*

# KNOWING YOUR ROUTER

## Front Panel



<b>Power LED (PWR)</b>	
OFF	Router is OFF
Green	Router is ready

<b>ADSL – SYN Status LED</b>	
OFF	No ADSL connection
Solid Green	ADSL connection is ready
Blinking Green	Negotiating connection

This LED lights in GREEN to indicate that your Modem Router is connected properly to the ADSL line.

<b>ADSL – Data LED</b>	
OFF	No WAN connection
Green	WAN connection is ready
Blinking	Indicates WAN activity

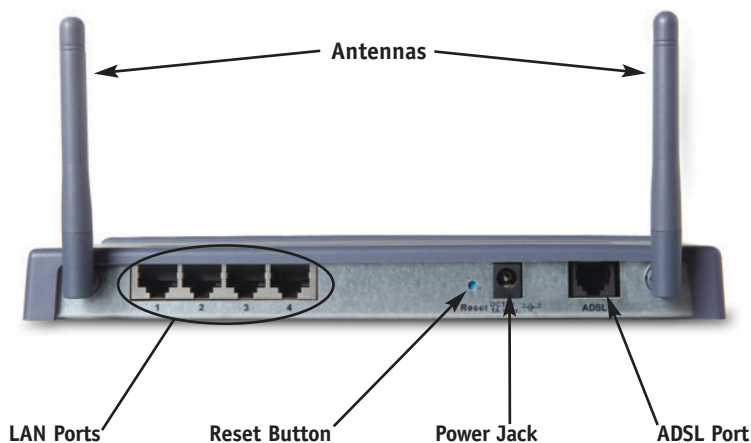
<b>Wireless Network LED</b>	
OFF	Wireless network is OFF
Green	Wireless network is ready
Blinking	Indicates wireless activity

## KNOWING YOUR ROUTER

LAN Port-Status LEDs	
OFF	No device is linked to the port
Solid Orange	10/100Base-Tx device connected
Blinking Orange	Port activity

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

### Rear Panel



### LAN Ports

The LAN ports are RJ45, 10/100 auto-negotiation. The ports are labeled 1 through 4. These ports correspond to the numbered LEDs on the front of the Router. Connect your LAN computers or any networking devices to one of these ports.

### Reset Button

The “Reset” button is used in rare cases when the Router may function improperly. Resetting the Router will restore the Router’s normal operation while

## KNOWING YOUR ROUTER

maintaining the programmed settings. You can also restore the factory default settings by using the Reset button. Use the restore option in instances where you may have forgotten your custom password.

### **a. Resetting the Router**

Push and release the Reset button. When the Power/Ready light becomes solid again, the reset is complete.

### **b. Restoring the Factory Defaults**

Press and hold the Reset button for 10 seconds then release it. When the Power/Ready light becomes solid again, the restore is complete.

### **Power Jack**

Connect the included 12V DC power supply to this inlet. Using the wrong type of power adapter may cause damage to your Router.

### **ADSL Port**

This port is for connection to your ADSL line. Connect your ADSL line to this port.



## PLACEMENT OF YOUR ROUTER

Proper placement of your Router is important to ensure the best performance of your wireless network. Typically, indoors your Wireless Router can provide a circular coverage area of 250 feet or more. However, different types of construction materials and other obstructions in a building can greatly affect the wireless signal and decrease the range. Whenever possible, your Router should be placed as close as possible to the center of the area that you want to cover. In multi-story homes, place the Router on a floor that is as close to the center of the home as possible; this may mean placing the Router on an upper floor.

Use care when choosing the location of your Router.

- Be aware of appliances or large objects such as a refrigerator or washer/dryer unit that may be on the opposite side of a wall from where you decide to place your Router.
- Place the Router on top of a desk and away from metal cabinets and computer cases.
- Do not place objects or components on top of the Router.
- Make sure that both antennas are pointing UP at all times.
- Metallic-based UV window tint can affect wireless performance. Do not place the Router next to a tinted window.

We realize that in the real world, it may not be possible to place your Router in the center of your coverage area. In cases where you may experience difficulty covering the entire area you want, try placing the Router as high as possible. Wireless devices work best in a line-of-sight situation where there are no obstacles between the wireless computer and the Router. The Router may also be mounted to a wall with the antennas facing UP. There are other options for expanding your wireless coverage area. Visit [www.belkin.com/networking](http://www.belkin.com/networking) for solutions.

The wireless signal can be affected by many things including neighboring wireless networks, microwave ovens in operation, and 2.4GHz cordless phones. While these things can affect the network performance, your wireless network typically will work fine under most conditions where these devices exist.

## ISP Settings

Please collect the following information from your ISP before setting up the Wireless ADSL Modem Router.

For PPPoE and PPPoA users

- VCI and VPI number
- An ISP account user name and password

For fixed IP users

- IP address and subnet mask
- IP address for your ISP's Gateway Server and Domain Name Server

## Connect the System

### Connect the ADSL Line

Run standard telephone cable from the wall jack providing ADSL service to the ADSL port on your Wireless ADSL Modem Router. When inserting an ADSL RJ11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. If you are using splitterless ADSL service, add low-pass filters between the ADSL wall jack and your telephones. (These filters pass voice signals through but filter data signals out.)

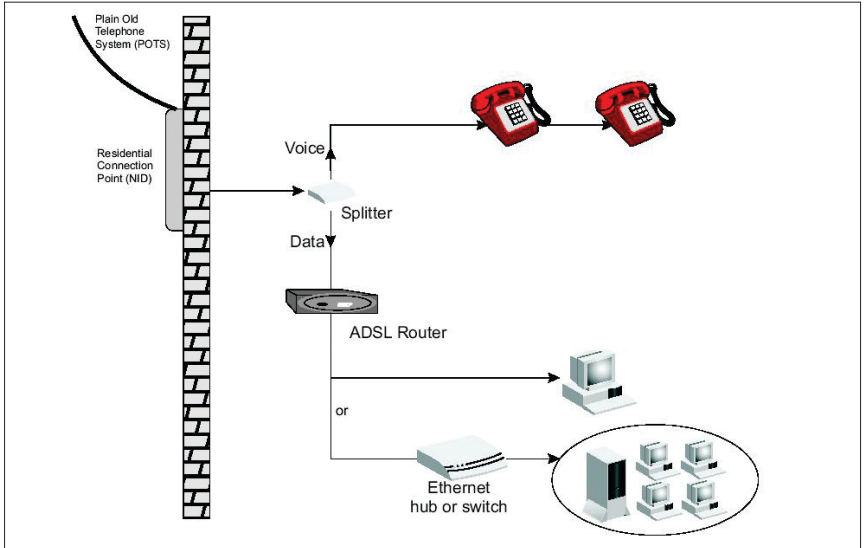
## Phone Line Configuration

### Installing a Full-Rate Connection

If you are using a full-rate (G.dmt) connection, your service provider will attach the ADSL line to a data/voice splitter. In this case, you can connect your phones and computer directly to the splitter as shown on the next page.

# CONNECTING AND CONFIGURING YOUR ROUTER

## Installing with a Splitter

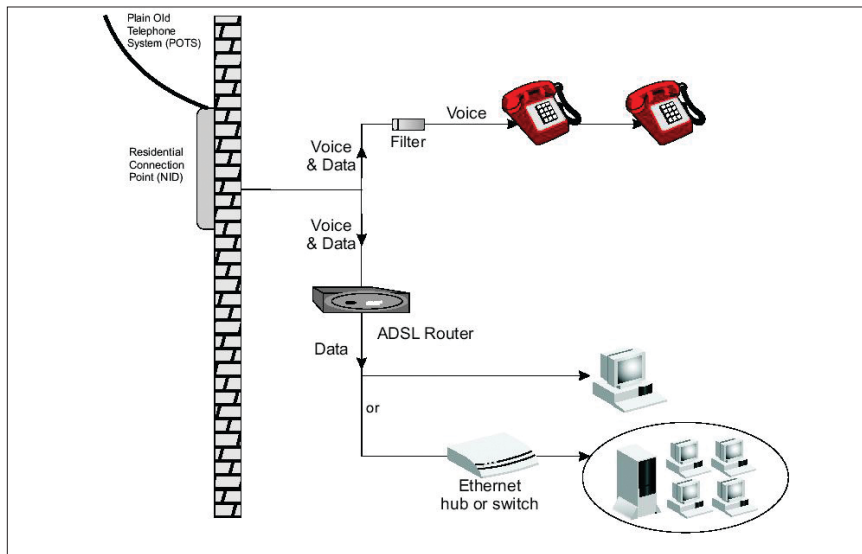


## Installing a Splitterless Connection

If you are using a splitterless (G.lite) connection, then your service provider will attach the outside ADSL line directly to your phone system. In this case, you can connect your phones and computer directly to the incoming ADSL line, but you will have to add low-pass filters to your phones as shown on the next page.

# CONNECTING AND CONFIGURING YOUR ROUTER

## Installing without a Splitter



### Attach to your Network Using Ethernet Cabling

The four LAN ports on the ADSL Modem Router auto-negotiate the connection speed to 10Mbps Ethernet or 100Mbps Fast Ethernet, as well as the transmission mode to half duplex or full duplex.

### Configuring the Router

The Belkin Wireless ADSL Modem Router is equipped with a Web-Based Interface that you can use to set up the Router. From the Web-Based Interface, you can perform the following tasks:

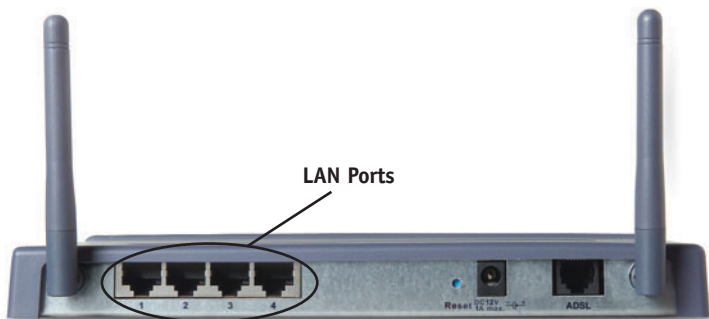
- View the Router's current settings and status.
- Configure the Router to connect to your ISP with the settings that they provided you.
- Change the current network settings such as the internal IP address, the IP address pool, DHCP settings, and more.

## CONNECTING AND CONFIGURING YOUR ROUTER

- Set the Router's firewall to work with specific applications (port forwarding).
- Set up security features such as client restrictions and MAC address filtering.
- Enable the DMZ feature for a single computer on your network.
- Change the Router's internal password.
- Reset the Router.
- Reset the Router's default settings.
- Update the Router's firmware.

### Step 1: Installing the Hardware

1. Power down your equipment.
2. Connect each PC to one of the ports on the rear of the Router labeled LAN by using a RJ45 networking cable.



3. Connect the telephone cable from the wall jack providing ADSL service to the ADSL port on your Router.

*Note: When inserting an ADSL RJ11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.*

4. Connect the power adapter to the Router.
5. After the Router is turned on, the Router's Power light should be on.

## CONNECTING AND CONFIGURING YOUR ROUTER

- Turn on the rest of your computers. After your computers boot up, a LAN link light (on the front of the Router) will be on for each port to which a wired computer is connected. These lights are your means to verify that your computers are connected.

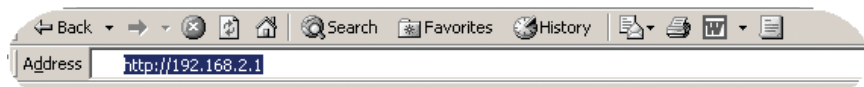


### Step 2: Set your Computer's Network Settings to Work with a DHCP Server

Configure the TCP/IP settings on your computers to obtain an IP address automatically. The Router will assign each computer an IP address in the range of 192.168.2.x. In most cases, your computer is programmed to automatically obtain your IP address when you turn it on. If your computer is not set to work with a DHCP server, then see the section in this manual called “Manually Configuring Network Settings” for directions.

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

Using your Internet browser, you can access the Router's Web-Based 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.



## CONNECTING AND CONFIGURING YOUR ROUTER

### Logging into the Router

To configure the Router's settings, you have to log in. The Router is supplied with no password entered. In the login screen, leave the password blank and click the "Submit" button to log in.

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

**Password >**

Default = leave blank

### Logging out of the Router

One computer at a time can log into the Router for the purposes of making changes to the settings of the Router. Once a user has logged in to make changes, there are two ways that the computer can be logged out. Clicking the "Logout" button will log the computer out. The second method is automatic. The login will time-out after a specified period of time. The default login time-out is 10 minutes. This can be changed from 1 to 99 minutes. For more information, see the section in this manual titled "Changing the Login Time-out Setting".

## Setup Wizard

### 1. Internet Sharing

Select the connection type you are using. This information is provided by your ISP.

**Wizard > 1.Connection Type**

The following information are provided by your ISP.

Please select the Internet sharing protocol

PPPoE(Routing Mode, for multiple PCs)

PPPoA(Routing Mode, for multiple PCs)

Disable Internet Sharing(Bridge Mode, for single PC)

Multiple protocol over ATM(Routing Mode, for multiple PCs)

**Next**

### 2. Setting your ISP Connection Type to PPPoE or PPPoA

Enter the PPPoE (Point-to-Point Protocol over Ethernet) or PPPoA information in the provided spaces, and click "Next". Click "Apply" to activate your settings. This information is provided by your ISP.

**Wizard > 2. Parameter Setting**

The following information are usually provided by your ISP.

> **Username:**

> **Password:**

> **Retype Password:**

> **VPI/VCI:**  /

**User Name** - Enter the ISP assigned user name. (Assigned by your ISP).

**Password** - Enter your password. (Assigned by your ISP).

**Retype Password** - Confirm the password. (Assigned by your ISP).

**VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).



## NAVIGATING THE WEB BROWSER INTERFACE

### 3. Setting your Connection Type to Disable Internet Sharing

Enter VPI/VCI value in the provided spaces, and then click “Next”. Click “Apply” to activate your settings.

**Wizard > 2. Parameter Setting**

The following information are usually provided by your ISP.

VPI/VCI  /

**VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).

### 4. Setting your Connection Type to Multiple Protocol over ATM Mode

Enter ATM (Asynchronous Transfer Mode) information in the provided spaces, and click “Next”. Click “Apply” to activate your settings.

**Wizard > 2. Parameter Setting**

The following information are usually provided by your ISP.

> **WAN IP:**  .  .  .

> **Subnet Mask:**  .  .  .

> **VPI/VCI:**  /

> **Default Gateway:**  .  .  .

**WAN IP** - Enter an IP address for the Wireless ADSL Modem Router WAN interface. (Assigned by your ISP).

**Subnet Mask** - Enter a subnet mask. (Assigned by your ISP).

## NAVIGATING THE WEB BROWSER INTERFACE

**VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).

**Default Gateway** - Enter a default gateway IP address. If the Wireless ADSL Modem Router cannot find the destination address within its local network, it will forward the packets to the Default Gateway. (Assigned by your ISP).

5. Click apply to activate your settings.

**Wizard > You have filled in the following Configuration Parameters**

ADSL Parameters:

Protocol	PPP over Ethernet
VPI / VCI	0 / 33
AAL5 Encapsulation	LLC
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Domain Name Server	

ISP Parameters:

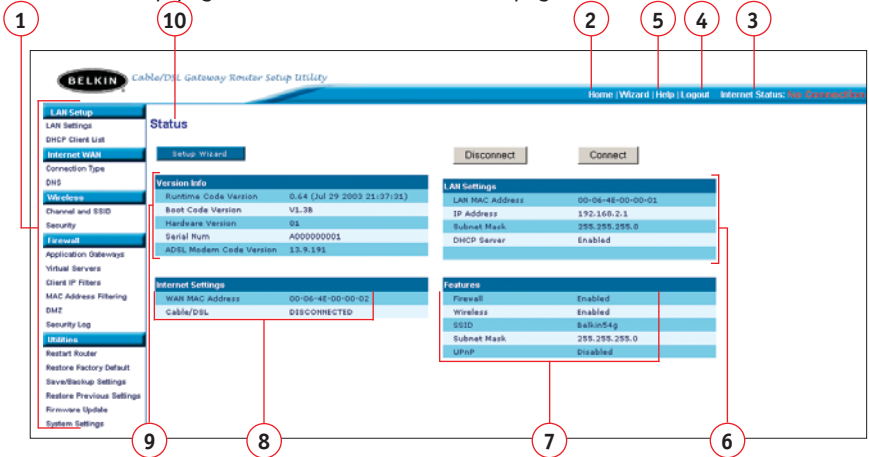
User Name	belkinc@sbculldogglobal.net
Password	*****

Back Apply

You have finished installing your new Belkin Router. You should have Internet access at this point. To test your Internet connection, open your browser and visit a website such as [www.belkin.com](http://www.belkin.com).

# UNDERSTANDING THE WEB-BASED USER INTERFACE

The home page shows you a quick view of the Router's status and settings. All advanced setup pages can be reached from this page.



## 1. Quick-Navigation Links

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

## 2. Home Button

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

## 3. Internet Status Indicator

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

## 4. Login/Logout Button

This button enables you to log in and out of the Router with the press of one button. When you are logged into the Router, this button will change to read "Logout". Logging into the Router will take you to a separate login

page where you will need to enter a password. When you are logged into the Router, you can make changes to the settings. When you are finished making changes, you can log out of the Router by clicking the “Logout” button. For more information about logging into the Router, see the section called “Logging into the Router”.

### **5. Help Button**

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

### **6. LAN Settings**

Shows you the settings of the Local Area Network (LAN) side of the Router. Changes can be made to the settings by clicking the “LAN” Quick Navigation link on the left side of the screen.

### **7. Features**

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

### **8. Internet Settings**

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

### **9. Version Info**

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

### **10. Page Name**

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

# UNDERSTANDING THE WEB-BASED USER INTERFACE

## Changing LAN Settings

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

### 1. LAN Settings

Clicking on the header of the LAN tab (A) 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" (B) or to view the list of connected computers, click on "DHCP client list" (C).

The screenshot shows the Belkin web-based user interface. On the left is a navigation menu with the following items: LAN Settings, LAN Settings, DHCP Client List, Internet WAN, Connection Type, DNS, Wireless, Channel and SSID, Security, Firewall, Application Discovery, Virtual Servers, Client IP Filters, MAC Address Filtering, DMZ, Security Log, Utilities, Restore Router, Restore Factory Default, Restore Backup Settings, Restore Previous 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, it lists 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 = NONE". It also states: "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."

The screenshot shows the "LAN > LAN Settings" page. It contains the following fields and options: "IP Address >" with input fields for 192, 168, 2, and 1; "Subnet Mask >" with input fields for 255, 255, 255, and 0; "DHCP server >" with radio buttons for On (selected) and Off; "IP Pool Starting Address >" with input fields for 192, 168, 2, and 2; "IP Pool Ending Address >" with input fields for 192, 168, 2, and 100; "Lease Time >" with a dropdown menu set to Forever; and "Local Domain Name > (Optional)" with an input field containing Belkin. At the bottom are "Clear Changes" and "Apply Changes" buttons. Red circles with numbers 1 through 6 are placed to the left of the page, with lines pointing to the IP Address, Subnet Mask, DHCP server, IP Pool Starting Address, IP Pool Ending Address, and Local Domain Name fields respectively.

## 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 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.

## 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 IP Pool is 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

Lease time is 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

## UNDERSTANDING THE WEB-BASED USER INTERFACE

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".

### DHCP Client List

You can view a list of the computers (known as clients), which are connected to your network. You are able to view the IP address (1) of the computer, the host name (2) (if the computer has been assigned one), and the MAC address (3) of the computer's network interface card (NIC). Pressing the "Refresh" (4) button will update the list. If there have been any changes, the list will be updated.

**LAN > DHCP Client List**

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

IP Address	Host Name	MAC Address
192.168.2.11	Ericd-XP	00-30-BD-3D-AB-09

Refresh

The screenshot shows a web interface for viewing DHCP clients. It includes a title, a descriptive paragraph, a table with three columns (IP Address, Host Name, MAC Address), and a Refresh button. Red callout boxes with numbers 1 through 4 are placed above the interface: 1 points to the IP address '192.168.2.11', 2 points to the Host Name 'Ericd-XP', 3 points to the MAC Address '00-30-BD-3D-AB-09', and 4 points to the Refresh button.

## 2. 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 ADSL Service Provider’s system provided you have correctly configured the Router’s settings for your ISP’s connection type. Your 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. When you have finished making settings, the “Internet Status” indicator will read “Connection OK” if your Router is set up properly.

<b>LAN Setup</b>	<a href="#">LAN Settings</a> <a href="#">DHCP Client List</a>
<b>Internet WAN</b>	
A	<a href="#">Connection Type</a>
B	<a href="#">DNS</a>
<b>Wireless</b>	
<b>Firewall</b>	
<b>Utilities</b>	

### Internet WAN >

In this page you can configure WAN parameters.

- **PPPoE:** To configure PPPoE parameters.
- **ATM:** To configure ATM VC parameters.
- **ISP:** To configure parameters for ISP.
- **DNS:** To configure DNS parameters.



## UNDERSTANDING THE WEB-BASED USER INTERFACE

### Connection Type

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

**WAN > Connection type**  
Select your connection type :

- PPPoE(Routing Mode, for multiple PCs)
- PPPoA(Routing Mode, for multiple PCs)
- Disable Internet Sharing(Bridge Mode, for single PC)
- Multiple protocol over ATM(Routing Mode, for multiple PCs)

### Setting your ISP Connection Type to PPPoE or PPPoA

Enter the PPPoE (Point-to-Point Protocol over Ethernet) or PPPoA information in the provided spaces, and click “Next”. Click “Apply” to activate your settings. This information is provided by your ISP.

**WAN > Connection Type > PPPoE Interface**  
PPPoE Interface

- 
- 
- 
- 
- 
- 
- 
- Dial on Demand
-

## UNDERSTANDING THE WEB-BASED USER INTERFACE

- a. **Username** - Enter the ISP assigned user name. (Assigned by your ISP).
- b. **Password** - Enter your password. (Assigned by your ISP).
- c. **Retype Password** - Confirm the password. (Assigned by your ISP).
- d. **IP assigned by ISP** - Select "Yes" for automatic IP assignment from your ISP. Select "No" only if your ISP assigns you a fixed IP address.
- e. **IP address** - If you are using a fixed IP address, enter the fixed IP address supplied by your ISP.
- f. **Subnet Mask** - If you are using a fixed IP address, enter the subnet mask supplied by your ISP.
- g. **VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).
- h. **Encapsulation** - Select your encapsulation type (supplied by your ISP) to specify how to handle multiple protocols at the ATM transport layer.
  - VC-MUX:** Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with fewer overheads.
  - LLC:** Point-to-Point Protocol over ATM Logical Link Control allows multiple protocols running over one virtual circuit (more overhead).
- i. **Dial on Demand** - By selecting "Dial on Demand" your Router will automatically connect to the Internet when a user opens up a web browser.
- j. **Idle Time (Minutes)** - Enter the maximum idle time for the Internet connection. After this time has been exceeded, the connection will be terminated.

## UNDERSTANDING THE WEB-BASED USER INTERFACE

### Setting your ISP Connection Type to Disable Internet Sharing

**VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).

**Encapsulation** - Select LLC or VC MUX. (Assigned by your ISP).

WAN > Connection Type > Disable Internet Sharing(Bridge Mode, for single PC)

ATM Interface

VPI/VCI >

Encapsulation >

### Setting your ISP Connection Type to Multiple Protocol over ATM

ATM Interface

a **IP Address** >

b **Subnet Mask** >

c **Default Route** >

d **VPI/VCI** >

e **Encapsulation** >

- WAN IP** - Enter an IP address for the Wireless ADSL Modem Router WAN interface. (Assigned by your ISP).
- Subnet Mask** - Enter a subnet mask. (Assigned by your ISP).
- Default Route** - Enter a default gateway IP address. If the Wireless ADSL Modem Router cannot find the destination address within its local network, it will forward the packets to the Default Gateway. (Assigned by your ISP).
- VPI/VCI** - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).
- Encapsulation** - Select LLC or VC MUX. (Assigned by your ISP).

## UNDERSTANDING THE WEB-BASED USER INTERFACE

### DNS (Domain Name Server) Settings

A “Domain Name Server” is a server located on the Internet that translates Universal Resource Links (URLs) like “www.belkin.com” to IP addresses. Many 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.

WAN > DNS

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

Automatic from ISP

DNS Address >

Secondary DNS Address >

DNS = Domain Name Server. A server located on the Internet that translates URL's (Universal Resource Links) like www.belkin.com to IP addresses. [More Info](#)

### 3. Wireless

The Wireless tab lets you make changes to the wireless network settings. From this tab, you can make changes to the wireless network name (SSID), operating channel, and encryption security settings.

### Channel and SSID

#### Changing the Wireless Channel

There are a number of operating channels you can choose from. In the United States, there are 11 channels. In the United Kingdom and most of Europe, there are 13 channels. In a small number of other countries, there are other channel

## UNDERSTANDING THE WEB-BASED USER INTERFACE

requirements. Your Router is configured to operate on the proper channels for the country you reside in. The default channel is 11 (unless you are in a country that does not allow channel 11). The channel can be changed if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks. For best performance, use a channel that is at least five channels away from the other wireless network. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. To change the channel, select the channel from the drop-down list. Click "Apply Changes". The change is immediate.

The screenshot shows a web-based user interface for configuring wireless settings. The title is "Wireless > Channel and SSID". Below the title is a note: "To make changes to the wireless settings of the router, make the changes here. Click 'Apply Changes' to save the settings. [More Info](#)".

The settings are as follows:

- Wireless Channel >**: A drop-down menu with a scrollable list of channels from 3 to 13. Channel 6 is selected.
- SSID >**: A text input field containing "54g".
- ESSID Broadcast >**: Radio buttons for "ENABLE" and "DISABLE". "DISABLE" is selected.
- Wireless Mode >**: A drop-down menu with "(11b+11g)" selected.
- Transmission Rate >**: A drop-down menu with "Automatic" selected.
- g Nitro >**: Radio buttons for "ENABLE" and "DISABLE". "DISABLE" is selected.

At the bottom of the form are two buttons: "Clear Changes" and "Apply Changes".

### Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. The default SSID of the Router is "belkin54g". You can change this to anything you want to or you can leave it unchanged. If there are other wireless networks operating in your area, you will want to make sure that your SSID is unique (does not match that of another wireless network in the area). To change the SSID, type 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.

## UNDERSTANDING THE WEB-BASED USER INTERFACE

**Wireless > Channel and SSID**

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

Wireless Channel > 11

1 SSID > belkin54g

ESSID Broadcast >  ENABLE  DISABLE

Wireless Mode > Mixed (11b+11g)

Transmission Rate > Fully Automatic

g Nitro >  ENABLE  DISABLE

Clear Changes Apply Changes

2

### Using the ESSID Broadcast Feature

For security purposes, 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, select "DISABLE" 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.

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

### Using the Wireless Mode Switch

Your Router can operate in three different wireless modes: "Mixed", "11g Only", and "11b Only". The different modes are explained next.

- **Mixed** - In this mode, the Router is compatible with 802.11b and 802.11g wireless clients simultaneously. This mode is the factory default and ensures full compatibility with Wi-Fi-compatible devices. Set the Router to Mixed mode if you have a mix of 802.11b and 802.11g clients in your network. This is the recommended setting for your router and should only be changed if you have a specific reason to do so.

## UNDERSTANDING THE WEB-BASED USER INTERFACE

- **11g Only Mode** - 11g Only mode is compatible with 802.11g clients only. This mode can be useful only if you do not have any 802.11b clients that need access to the network. To switch modes, select the desired mode from the drop-down box next to “Wireless Mode” then click “Apply Changes”.
- **11b Only Mode** - It is not recommended you use this mode unless you have a very specific reason to do so. This mode exists only to solve unique problems that may occur with some 802.11b client adapters and is NOT necessary for interoperability of 802.11g and 802.11b standards.

*Note: Switching to 11b Only mode will decrease 802.11g performance to 11Mbps.*

### **g Nitro**

Enabling “g Nitro” allows the Router to use Frame Bursting to get the maximum throughput from the Router to 802.11g clients. g Nitro throughput is up to 50% faster than any standard 802.11g equipment. g Nitro will work with 802.11g clients that support g Nitro.

## **Encryption/Security**

### **Changing the Wireless Security Settings**

Your Router is equipped with the latest security standard called WPA (Wireless Protected Access). It also supports the legacy security standard called WEP (Wired Equivalent Privacy). 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.

### **Setting WPA Security**

***Note:** To use WPA security, your clients must be upgraded to drivers and software that support WPA. At the time this manual was published, a security patch from Microsoft is available for free download. This patch works only with Windows XP. You also need to download the latest driver for your Belkin 802.11g Wireless Notebook Network Card from the Belkin support site. Other operating systems are not supported at this time. Only Belkin 802.11g clients support WPA at this time.*

## UNDERSTANDING THE WEB-BASED USER INTERFACE

There are two types of WPA security, WPA-PSK (no server) and WPA (with 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 8 and 40 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.

WPA (with server) is a system where a radius server distributes the keys to the clients automatically. This is typically found in a business environment.

### Setting WPA-PSK (no server)

1. From the Security Mode drop-down menu, select “WPA-PSK (no server)”.
2. Enter your pre-shared key. This can be from 8 to 40 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.
3. Click “Apply Changes” to finish. You must now set all clients to match these settings.

**Wireless > Security > WPA**

**WPA >**

**Encryption technique** TKIP

**Pre-shared Key (PSK)**

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. Each client that connects to the network must use the same key (Pre-Shared Key).

obscure PSK

### Setting WPA (with server) Settings

If your network uses a radius server to distribute keys to the clients, use this setting.



## UNDERSTANDING THE WEB-BASED USER INTERFACE

1. From the Security Mode drop-down menu, select “WPA (with server)”.
2. Enter the IP address of the radius server into the “Radius Server” fields.
3. Enter the radius key into the Radius Key field.
4. Enter the key interval. Key interval is how often the keys are distributed (in packets).
5. Click “Apply Changes” to finish. You must now set all clients to match these settings.

Wireless > Security > WPA

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

Security Mode : WPA (with Radius Server) ▼

Encryption technique TKIP

RADIUS Server > 192 . 168 . 1 . 1

Radius Port > 1812

Radius Key >

Re-Key Interval 3600 Seconds

Clear Changes 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.

Wireless > Security > WPA

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

Security Mode : WPA (with Radius Server) ▼

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

RADIUS Server >

Radius Port >

Radius Key >

Re-Key Interval 3600 Seconds

Clear Changes Apply Changes

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

## UNDERSTANDING THE WEB-BASED USER INTERFACE

- 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 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.

Wireless > Security> WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your device g and wireless client devices to use WEP.

Security Mode: 128-bit WEP

01	01	01	01	01
01	01	01	01	01
01	01	01	(13 hex digit pairs)	

Note : To automatically generate hex pairs using a PassPhrase, input it here.

Passphrase :

- 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 five two-digit numbers. 128-bit keys are 13 two-digit numbers.

For instance:

**AF OF 4B C3 D4** = 64-bit key

**C3 03 0F AF OF 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:

## UNDERSTANDING THE WEB-BASED USER INTERFACE

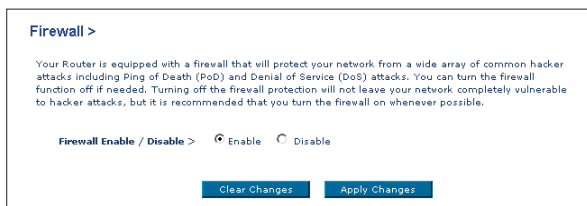
**Note to Mac users:** Original Apple AirPort products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Please check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

### 4. 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 essentially 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.



# UNDERSTANDING THE WEB-BASED USER INTERFACE

## Application Gateways Settings

Application gateways let you select ports to be open for certain applications to work properly with the Network Address Translation (NAT) feature of the Router. A list of popular applications has been included to choose from. Select your application from the drop-down list from the bottom of the screen. If your application is not here, you will need to check with the application vendor to determine which ports need to be configured. You can manually input this port information into the Router.

**Firewall > Application Gateways**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen. Note: 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. [More Info](#)

Popular applications:

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

## Choosing an Application

Select the row that you want to copy the settings to from the drop-down list, select the row you want to copy to, and then click "Copy To". The settings will be transferred to the row you specified. Click "Apply Changes" to save the setting for that application.

**Firewall > Application Gateways**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen. Note: 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. [More Info](#)

Popular applications:

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text" value="6112"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text" value="6112"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input checked="" type="checkbox"/>
2.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

## UNDERSTANDING THE WEB-BASED USER INTERFACE

### Virtual Servers

Virtual Servers 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, machines from the Internet cannot get to them because they cannot be “seen”. If you need to configure the Virtual Server function for a specific application, you will need to contact the application vendor to find out which port settings you need.

**Firewall > Virtual Servers**

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

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<a href="#">Set</a> <a href="#">Clean</a>
2	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<a href="#">Set</a> <a href="#">Clean</a>
3	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<a href="#">Set</a> <a href="#">Clean</a>
4	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<a href="#">Set</a> <a href="#">Clean</a>
5	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<a href="#">Set</a> <a href="#">Clean</a>
6	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<a href="#">Set</a> <a href="#">Clean</a>

### Entering Settings into the Virtual Server

To enter settings, enter the last digit of your LAN IP address in the space provided for the internal machine, input the Protocol Type (TCP or UDP), and the LAN Port & Public Port number required to pass, select “Enable” and click “Set”. 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.

### Client IP Filters

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

# UNDERSTANDING THE WEB-BASED USER INTERFACE

**Firewall > Client IP filters**

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function >  Enable  Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				
<a href="#">Add PC</a>				
<a href="#">Apply Changes</a>				

## Access Control

Access Control allows users to define the outgoing traffic permitted or denied access through the WAN interface. The default is to permit all outgoing traffic. To configure restrictive access to your computers, do the following:

1. Click “Add PC” on the Access Control screen.
2. Define the appropriate settings for client PC services (as shown on the following screen).

**Firewall > Client IP filters**

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL Blocking function, you need to configure the URL address first on the “URL Blocking Site” page. For the scheduling function, you also need to configure the schedule rule first on the “Schedule Rule” page.

Client PC Description >

Client PC IP Address >  ~

> Client PC Services:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 6080, 8001	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>

3. Click “OK” and then click “Apply Changes” to save your settings.

# UNDERSTANDING THE WEB-BASED USER INTERFACE

## URL Blocking

To configure the URL Blocking feature, specify the websites (www.anywebsite.com) and or keywords you want to filter on your network. Click “Apply Changes” to activate the change. To complete this configuration, you will need to create or modify an access rule in the “Client IP filters” section. To modify an existing rule, click the “Edit” option next to the rule you want to modify. To create a new rule, click on the “Add PC” option. From the “Access Control > Add PC” section, check the option for “WWW with URL Blocking” in the Client PC Service table to filter out the websites and keywords specified.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

To configure the URL Blocking feature, use the table below to specify the websites (www.somewebsite.com) and or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the “Access Control” section. To modify an existing rule, click the “Edit” option next to the rule you want to modify. To create a new rule, click on the “Add PC” option.

From the “Access Control Add PC” section check the option for “WWW with URL Blocking” in the Client PC Service table to filter out the websites and keywords specified below.

Rule Number	URL / Keyword
Site 1	
Site 2	
Site 3	
Site 4	
Site 5	
Site 6	
Site 7	
Site 8	
Site 9	
Site 10	
Site 11	
Site 12	

## Schedule Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the “Schedule Rule”, and apply the rule on the “Access Control” page.

Firewall > Client IP filters

>> Access Control >> URL Blocking >> Schedule Rule

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

This page defines schedule rule names and activates the schedule for use in the “Access Control” page.

Rule Name	Rule Comment	Configure
No Valid Schedule Rule !!!		

> Add Schedule Rule

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

## UNDERSTANDING THE WEB-BASED USER INTERFACE

Follow these steps to add a schedule:

1. Click “Add Schedule Rule”.
2. You will see the following screen.

**Firewall > Client IP filters**

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. [More Info](#)

>> Access Control >> URL Blocking >> Schedule Rule

> Edit Schedule Rule

Name >

Comment >

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<input type="text"/>	<input type="text"/>
Sunday	<input type="text"/>	<input type="text"/>
Monday	<input type="text"/>	<input type="text"/>
Tuesday	<input type="text"/>	<input type="text"/>
Wednesday	<input type="text"/>	<input type="text"/>
Thursday	<input type="text"/>	<input type="text"/>
Friday	<input type="text"/>	<input type="text"/>
Saturday	<input type="text"/>	<input type="text"/>

3. To configure the Schedule Rule, specify the Name, Comment, Start Time, and End Time that you want to filter on your network.
4. Click “OK” and then “Apply Changes” to save your settings.
5. To complete this configuration, you will need to create or modify an access rule in the Client IP filters section. This activates the schedule for use in the “Access Control” page.

### 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 on your network to allow network access to each, or copy the MAC address by selecting the name of the computer from the “DHCP Client List”. To enable this feature, select “Enable”. Next, click “Apply Changes” to save the settings.



## UNDERSTANDING THE WEB-BASED USER INTERFACE

Firewall > MAC Address Filtering

This feature lets you set up a list of allowed clients. When you enable this feature, you must enter the MAC address of each client on your network to allow network access to each. [More Info](#)

Enable MAC Address Filtering >  Enable  Disable

DHCP Client List: ip=192.168.2.2 name=Test\_Wireless Copy to 1

MAC Address Filtering List > (up to 32 computers)

ID	MAC Address							
1								
2								
3								
4								
5								
6								
7								

### DMZ (Demilitarized Zone)

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.**

Firewall > DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** [More Info](#)

DMZ >  ENABLE  DISABLE

> IP Address of Virtual DMZ Host

	Public IP	Static IP
1.	0.0.0.0	192.168.2.0
2.	0 0 0 0	192.168.2.0
3.	0 0 0 0	192.168.2.0
4.	0 0 0 0	192.168.2.0
5.	0 0 0 0	192.168.2.0
6.	0 0 0 0	192.168.2.0
7.	0 0 0 0	192.168.2.0
8.	0 0 0 0	192.168.2.0

Clear Changes Apply Changes

## UNDERSTANDING THE WEB-BASED USER INTERFACE

To put a computer in the DMZ, enter the last digits of its LAN IP address in the Static IP field and click “Apply Changes” for the change to take effect.

If you are using multiple Public (WAN) IP addresses, it is possible to select which Public (WAN) IP address the DMZ host will be directed to. Type in the Public (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, and click “Apply Changes”.

### Utilities

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

**Utilities >**

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

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

### Restart 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.

#### Utilities > Restart Router

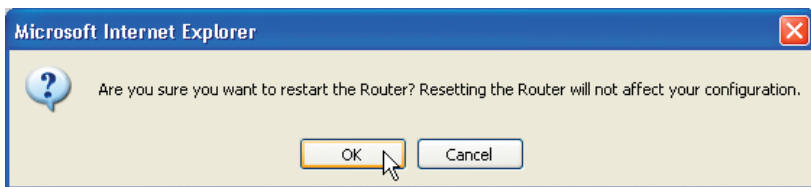
Sometimes it may be necessary to Restart or Reboot the router if it begins working improperly. Restarting or Rebooting the Router will not delete any of your configuration settings. Click the “Restart Router” button below to Restart the Router.

Restart Router

## UNDERSTANDING THE WEB-BASED USER INTERFACE

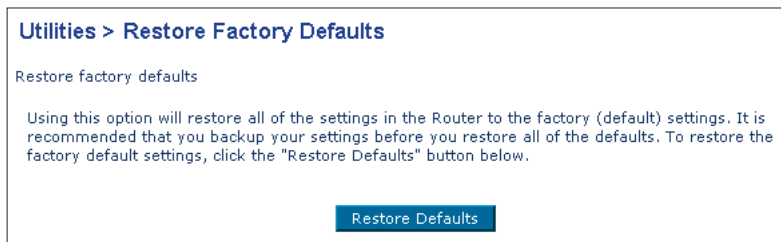
### Restarting the Router to Restore Normal Operation

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

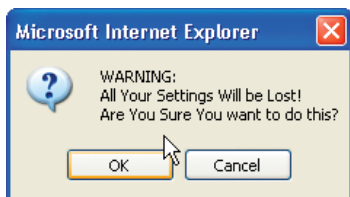


### Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.



1. Click the “Restore Defaults” button.
2. The following message will appear. Click “OK” to restore factory defaults.



# UNDERSTANDING THE WEB-BASED USER INTERFACE

## Saving/Backup Current Settings

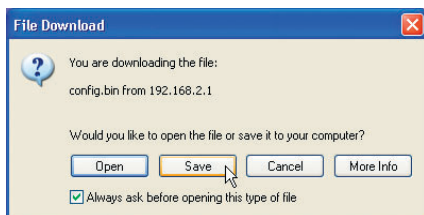
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.

### Utilities > Save/Backup current settings

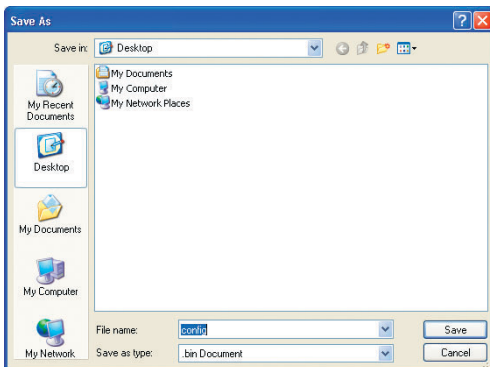
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

Save

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

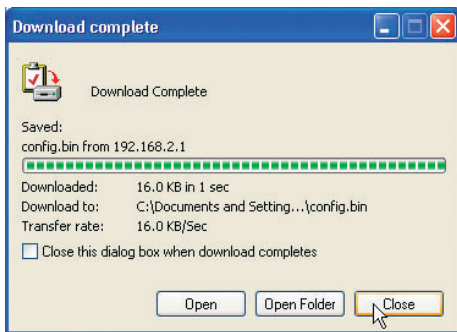


2. A window will open that allows you to select the location in which to save the configuration file. Select a location. There are no restrictions on the file name, however, be sure to name the file so you can locate it yourself later. When you have selected the location and entered the file name, click “Save”.



## UNDERSTANDING THE WEB-BASED USER INTERFACE

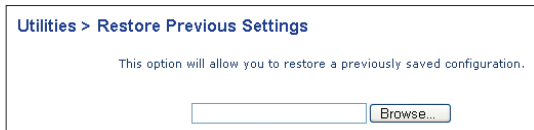
- When the save is complete, you will see the window below. Click “Close”.



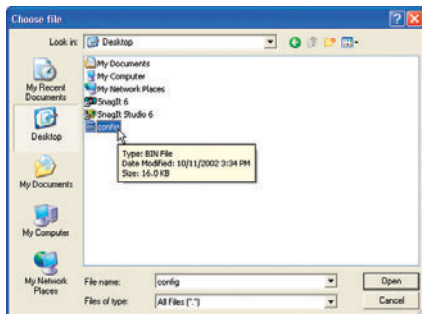
The configuration is now saved.

### Restore Previous Settings

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



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

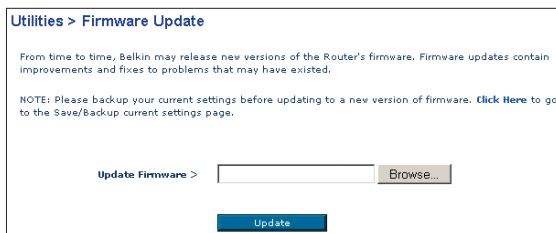


- Then, click “Restore”.

## UNDERSTANDING THE WEB-BASED USER INTERFACE

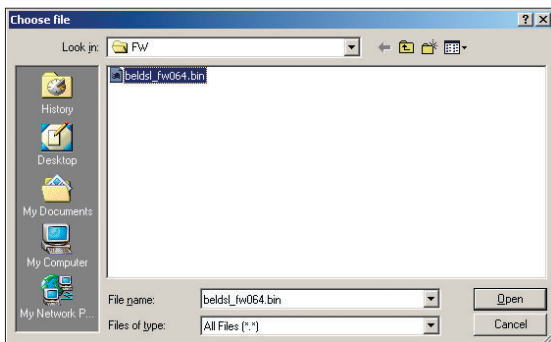
### Firmware Update

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.



### Updating the Router's Firmware

1. In the "Firmware Update" page, click "Browse". A window will open that allows you to select the location of the firmware update file.



2. Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.
3. Click "Update" to upgrade to the latest firmware version.

### 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 UPnP 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.

The screenshot shows a web page titled "Utilities > System Settings". Under the heading "Administrator Password:", there is a paragraph of text: "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". Below this text are four input fields: "Type in current Password >" (empty), "Type in new Password >" (empty), "Confirm new Password >" (empty), and "Login Timeout >" (containing the number "10" with a "(1-99 minutes)" label to its right). At the bottom of the form is a blue button labeled "Apply Changes".

## 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, 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, then 10 minutes after you leave, the login session will expire. You will have to login to 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. The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the timeservers on the Internet and get a response. You cannot set the clock yourself.

## UNDERSTANDING THE WEB-BASED USER INTERFACE

**Time and Time Zone:** January 1, 2002 0:59:15 AM  
Please set your time Zone. If you are in an area that observes daylight saving check this box. [More Info](#)

**Set Time Zone >** (GMT-08:00)Pacific Time (US & Canada): Tijuana ▾

**Configure Time Server (NTP) >**  Enable Automatic Time Server Maintenance

**Primary Server >** 132.163.4.102 - North America ▾

**Secondary Server >** 192.5.41.41 - North America ▾

[Apply Changes](#)

### 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.

#### 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>

.  .  .



## UNDERSTANDING THE WEB-BASED USER INTERFACE

### Enabling/Disabling UPnP

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

UPnP(Universal Plug and Play) Setting:

**ADVANCED FEATURE!** Allows you to turn UPnP on or off. [More Info](#)

UPnP >  ON  OFF

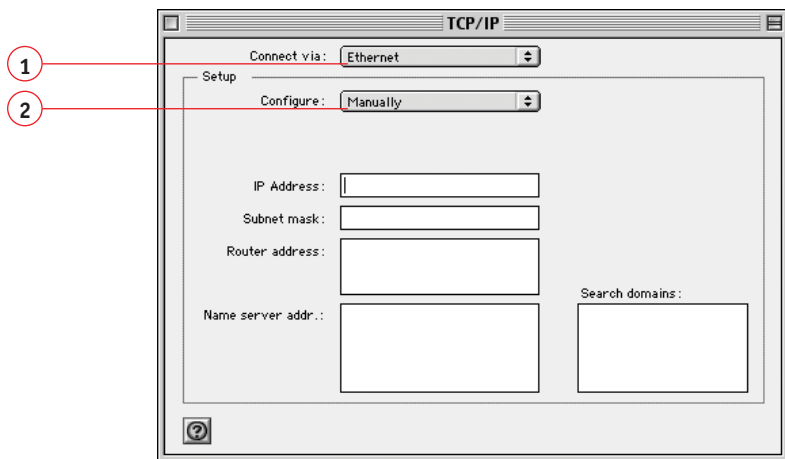
[Apply Changes](#)

## MANUALLY CONFIGURING NETWORK SETTINGS

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

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

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

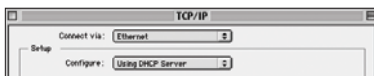


3. Next to "Configure" (2), if "Manually" is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.

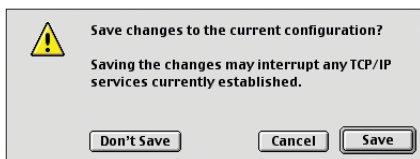
IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Router Address:	<input type="text"/>
Name Server Address:	<input type="text"/>

## MANUALLY CONFIGURING NETWORK SETTINGS

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



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



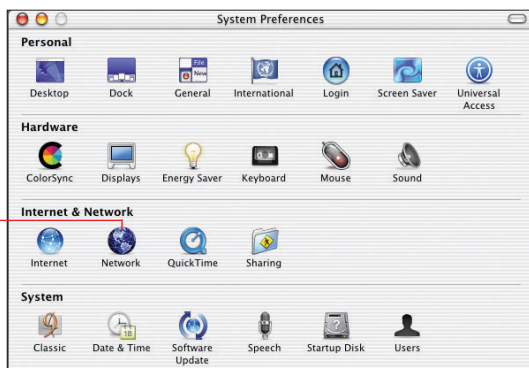
Restart the computer. When the computer restarts, your network settings are now configured for use with the Router.

### Manually Configuring Network Settings in Mac OS X

1. Click on the “System Preferences” icon.

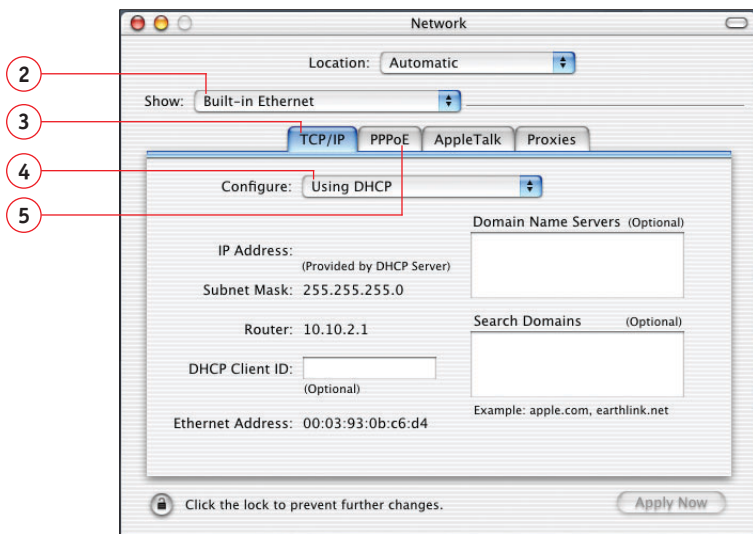


2. Select “Network” (1) from the “System Preferences” menu.



## MANUALLY CONFIGURING NETWORK SETTINGS

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:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Router Address:	<input type="text"/>
Name Server Address:	<input type="text"/>

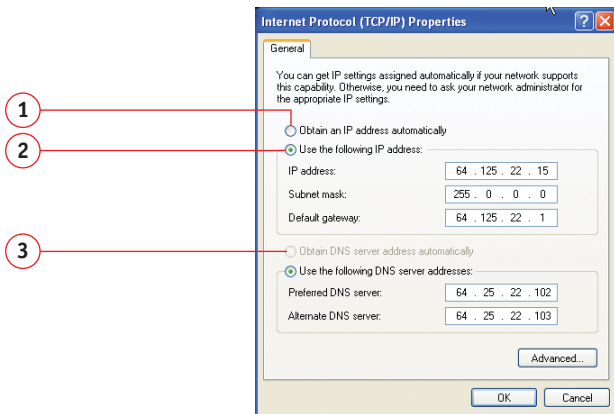
6. If not already selected, select “Using DHCP” next to “Configure” (4), then click “Apply Now”.

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

# MANUALLY CONFIGURING NETWORK SETTINGS

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

1. Click "Start", "Settings", then "Control Panel".
2. Double-click on the "Network and dial-up connections" icon (Windows 2000) or the "Network" icon (Windows XP).
3. Right-click on the "Local Area Connection" associated with your network adapter and select "Properties" from the drop-down menu.
4. In the "Local Area Connection Properties" window, click "Internet Protocol (TCP/IP)" and click the "Properties" button. The following screen will appear:



5. If "Use the following IP address" (2) is selected, your Router will need to be set up for a static IP connection type. Write the address information the table below. You will need to enter this information into the Router.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

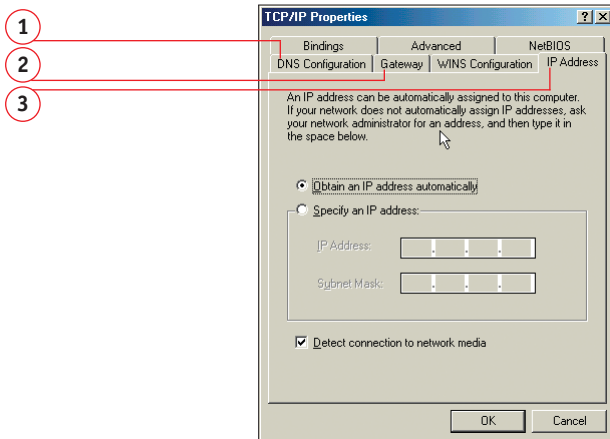
6. If not already selected, select "Obtain an IP address automatically" (1) and "Obtain DNS server address automatically" (3). Click "OK".

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

# MANUALLY CONFIGURING NETWORK SETTINGS

## Manually Configuring Network Settings in Windows 98 or Me

1. Right-click on “My Network Neighborhood” and select “Properties” from the drop-down menu.
2. Select “TCP/IP > Settings” for your installed network adapter. You will see the following window.



3. If “Specify and IP address” is selected, your Router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into the Router.
4. Write the IP address and subnet mask from the “IP Address” tab (3).
5. Click the “Gateway” tab (2). Write the gateway address down in the chart.
6. Click the “DNS Configuration” tab (1). Write the DNS address(es) in the chart.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

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

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

# MANUALLY CONFIGURING NETWORK SETTINGS

## Recommended Web Browser Settings

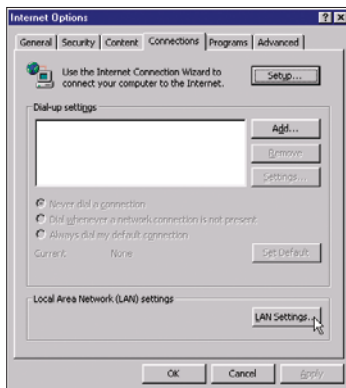
In most cases, you will not need to make any changes to your web browser's settings. If you are having trouble accessing the Internet or the Web-Based Advanced User Interface, then change your browser's settings to the recommended settings in this section.

### Microsoft Internet Explorer 4.0 or Higher

1. Start your web browser. Select "Tools" then "Internet Options".



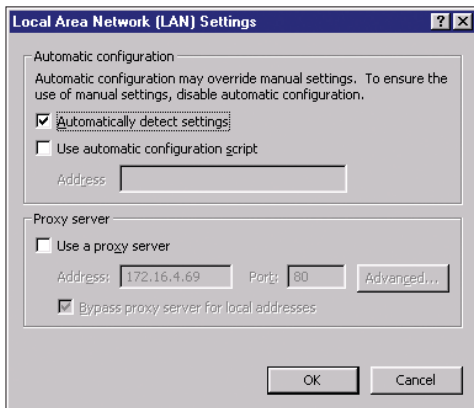
2. In the "Internet Options" screen, there are three selections: "Never dial a connection", "Dial whenever a network connection is not present", and "Always dial my default connection". If you can make a selection, select "Never dial a connection". If you cannot make a selection, go to the next step.



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

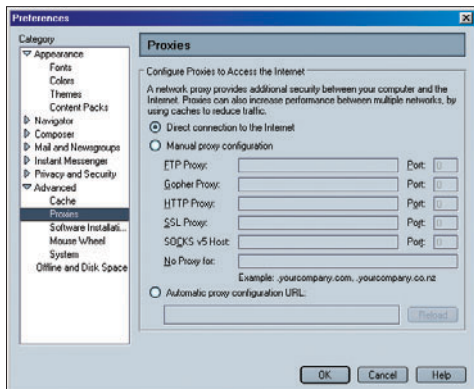
## MANUALLY CONFIGURING NETWORK SETTINGS

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”.





### **IP address**

The “IP address” is the Internal IP address of the Router. 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.)

### **Subnet Mask**

Some networks are far too large to allow all traffic to flood all its parts. These networks must be broken down into smaller, more manageable sections, called subnets. The subnet mask is the network address plus the information reserved for identifying the “subnetwork”.

### **DNS**

DNS is an acronym for Domain Name Server. A Domain Name Server is a server located on the Internet that translates URLs (Universal Resource Links) like www.belkin.com to IP addresses. Many ISPs do not require you to enter this information into the Router. 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.

### **PPPoE (Routing Mode, for multiple PCs)**

Most ADSL providers use PPPoE as the connection type. If you use an ADSL modem to connect to the Internet, your ISP may use PPPoE to log you into the service.

Your connection type is PPPoE if:

1. Your ISP gave you a user name and password which is required to connect to the Internet
2. Your ISP gave you software such as WinPoET, Enternet300 that you use to connect to the Internet

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

To set the Router to use PPPoE, type in your user name and password in the spaces provided. After you have typed in your information, click “Apply Changes”. After you apply the changes, the Internet Status indicator will read “connection OK” if your Router is set up properly.

### **PPPoA (Routing Mode, for multiple PCs)**

Enter the PPPoA information in the provided spaces, and click “Next”. Click “Apply” to activate your settings.

- a. User name - Enter the ISP assigned user name. (Assigned by your ISP).
- b. Password - Enter your password. (Assigned by your ISP).
- c. Retype Password - Confirm the password. (Assigned by your ISP).
- d. VPI/VCI - Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here. (Assigned by your ISP).

### **Disconnect after X...**

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

### **Channel and SSID**

To change the channel of operation of the Router, select the desired channel from the drop-down menu and select your channel. Click “Apply Changes” to save the setting. You can also change the SSID. The SSID is the equivalent to the wireless network’s name. You can make the SSID anything you want to. If there are other wireless networks in your area, you should give your wireless network a unique name. Click inside of the SSID box and type in a new name. Click “Apply Changes” to make the change.

### **ESSID Broadcast**

Many wireless network adapters currently on the market possess a feature known as site survey. It scans the air for any available network and allows each computer to automatically select a network from the survey. This occurs if the computer's SSID is set to "ANY". Your Belkin Router can block this random search for a network. If you disable the "ESSID Broadcast" feature, the only way a computer can join your network is by its SSID being set to the specific name of the network (like WLAN). Be sure that you know your SSID (network name) before enabling this feature. It is possible to make your wireless network nearly invisible. By turning off the broadcast of the SSID, your network will not appear in a site survey. Obviously, turning off the broadcast feature of the SSID helps increase security.

### **Encryption**

Setting encryption can help keep your network secure. The Router uses Wired Equivalent Privacy (WEP) encryption to protect your data and features two rates of encryption: 64-bit and 128-bit. Encryption works on a system of keys. The key on the computer must match the key on the Router, and there are two ways to make a key. The easiest is to let the Router's software convert a passphrase you've created into a key. The advanced method is to enter the keys manually.

### **Application Gateways**

Application Gateways let you specify specific ports to be open for specific applications to work properly with the Network Address Translation (NAT) feature of the Router. A list of popular applications has been included. You can select an application from the popular choices included in the drop-down list. Your selections will be programmed into the Router. From the drop-down list, select the row that you want to copy the settings from, and the row you want to copy to, and then click "Copy To". The settings will be transferred to the row you specified. Click "Apply Changes" to save the setting for that application. If your application is not here, you will need to check with the application vendor to determine which ports need to be configured. You can manually input this port information into the Router.

## Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be “seen”. If you need to configure the Virtual Server function for a specific application, you will need to contact the application vendor to find out which port settings you need. To manually enter settings, enter the IP address in the space provided for the internal machine, the port type (TCP or UDP), and the LAN & Public port(s) required to pass, select “Enable” and click “Set”. 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.

## Client IP filters

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

## URL Blocking

To configure the URL Blocking feature, specify the websites (www.somesite.com) and or keywords you want to filter on your network. Click “Apply Changes” to activate the change. To complete this configuration, you will need to create or modify an access rule in the Client IP filters section. To modify an existing rule, click the “Edit” option next to the rule you want to modify. To create a new rule, click on the “Add PC” option. From the “Access Control Add PC” section, check the option for “WWW with URL Blocking” in the Client PC Service table to filter out the websites and keywords specified.

## Schedule Rule

To configure the Schedule Rule, specify the Name, Comment, Start Time, and End Time that you want to filter on your network. This page defines schedule rule names and activates the schedule for use in the “Access Control” page.

### 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 on your network to allow network access to each or copy the MAC address by selecting the name of the computer from the “DHCP Client List”. To enable this feature, select “Enable”. Next, click “Apply Changes” to save the settings.

### DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.** To put a computer in the DMZ, enter the last digits of its LAN IP address in the Static IP field and click “Apply Changes” for the change to take effect.

If you have only one Public (WAN) IP address, then you can leave the Public IP to 0.0.0.0. If you are using multiple Public (WAN) IP addresses, it is possible to select which Public (WAN) IP address the DMZ host will be directed to. Type in the Public (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, and click “Apply Changes”.

### Administrator Password

The Router ships with NO password entered. If you wish to add a password for more security, you can set a password from your Router’s web-based user interface. Keep your password in a safe place as you will need this password if you need to log into the Router in the future. It is **STRONGLY RECOMMENDED** that you set a password if you plan to use the remote management feature.

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, 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, then 10 minutes after you leave, the login session will expire. You will have to login to 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 a time.

### 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. If you reside in an area that observes daylight saving time, 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 timeservers on the Internet and get a response. You cannot set the clock yourself.

### Remote Management

Before you enable this function, **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.

### UPnP

UPnP (Universal Plug-and-Play) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports and in some instances setting trigger ports. An application that is UPnP-compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The Router ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish to take advantage of the UPnP features, you can enable the UPnP feature. Simply select "Enable" in the "UPnP Enabling" section of the Utilities page. Click "Apply Changes" to save the change.

## TROUBLESHOOTING

You can find technical support information at [www.belkin.com/networking](http://www.belkin.com/networking) or [www.belkin.com](http://www.belkin.com) through the tech support area. If you want to contact technical support by phone, please call 877-736-5771. Technical support is available 24-hours-a-day, 7-days-a-week.

### Problem

### Possible Cause/Solution

#### The ADSL SYN LED is not on.

1. Check the connection between the Modem Router and ADSL line. Make sure the cable from the ADSL line is connected to the port on the Router labeled "ADSL".
2. Make sure the Router has power. The "PWR" LED of the front panel should be illuminated.

#### The ADSL Data LED is not on.

1. Make sure the cable from the ADSL line is connected to the port on the Router labeled "ADSL" and the "SYN" LED is on.
2. Make sure you have the correct VPI/VCI, user name, and password from your ISP provider.

#### My connection type is static IP address. I cannot connect to the Internet.

Since your connection type is static IP address, your ISP must assign you the IP address, subnet mask, and gateway address. Instead of using the Wizard, go to "Connection Type", and then select your connection type. Click "Next", select "Static IP", and enter your IP address, subnet mask, and default gateway information.

## TROUBLESHOOTING

**I've forgotten or lost my password.**

Press the Reset button on the rear panel (holding it down for at least five seconds) to restore the factory defaults.

**My wireless PC cannot connect to the Router.**

1. Make sure the wireless PC has the same SSID settings as the Router, and you have the same security settings on the clients such as WPA or WEP encryption.
2. Make sure the distance between the Router and wireless PC are not too far away.

**The wireless network is often interrupted.**

1. Move your wireless PC closer to the Router to find a better signal.
2. There may also be interference, possibly caused by a microwave oven or 2.4GHz cordless phones. Change the location of the Router or use a different wireless channel.



## FCC Statement

### DECLARATION OF CONFORMITY WITH FCC RULES FOR ELECTROMAGNETIC COMPATIBILITY

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

F5D7630-4

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

## Caution: Exposure to Radio Frequency Radiation.

The radiated output power of this device is far below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such manner that the potential for human contact normal operation is minimized.

When connecting an external antenna to the device, the antenna shall be placed in such a manner to minimize the potential for human contact during normal operation. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

## Federal Communications Commission Notice

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

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

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

## Modifications

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

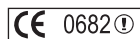
## Canada-Industry Canada (IC)

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

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

## Europe-European Union Notice

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



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

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



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

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

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



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

## **Belkin Corporation Limited Lifetime Product Warranty**

Belkin Corporation warrants this product against defects in materials and workmanship for its lifetime. If a defect is discovered, Belkin will, at its option, repair or replace the product at no charge provided it is returned during the warranty period, with transportation charges prepaid, to the authorized Belkin dealer from whom you purchased the product. Proof of purchase may be required.

This warranty does not apply if the product has been damaged by accident, abuse, misuse, or misapplication; if the product has been modified without the written permission of Belkin; or if any Belkin serial number has been removed or defaced.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE IN LIEU OF ALL OTHERS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. BELKIN SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

No Belkin dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

BELKIN IS NOT RESPONSIBLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO, LOST PROFITS, DOWNTIME, GOODWILL, DAMAGE TO OR REPROGRAMMING OR REPRODUCING ANY PROGRAM OR DATA STORED IN, OR USED WITH, BELKIN PRODUCTS.

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



belkin.com

**Belkin Corporation**

5501 West Walnut Street  
Compton • CA • 90220-5221 • USA  
Tel: +1 310 898 1100  
Fax: +1 310 898 1111

**Belkin Components, Ltd.**

Express Business Park • Shipton Way  
Rushden • NN10 6GL • United Kingdom  
Tel: +44 (0) 1933 35 2000  
Fax: +44 (0) 1933 31 2000

**Belkin Components B.V.**

Starparc Building • Boeing Avenue 333  
1119 PH Schiphol-Rijk • The Netherlands  
Tel: +31 (0) 20 654 7300  
Fax: +31 (0) 20 654 7349

**Belkin, Ltd.**

Hanebergstrasse 2  
80637 München • Germany  
Tel: +49 (0) 89 143405 0  
Fax: +49 (0) 89 143405 100

**Belkin Tech Support**

Europe: 00 800 223 55 460  
US: 877.736.5771  
310.898.1100 ext. 2263

**P74426uk**

© 2003 Belkin Corporation. All rights reserved. All trade names are registered trademarks of respective manufacturers listed. Mac, Mac OS, AppleTalk, Apple, and AirPort are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.