BELKIN®

G Wireless Modem Router

User Manual

PM01218ea-B F5D7634-4v2

ENGLISH

FRANÇAIS

DEUTSCH

NEDERLANDS

ESPAÑOL

ITALIANO

TABLE OF CONTENTS

Thank you for purchasing the Belkin G Wireless Modem Router (the Router). In minutes you will be able to share your Internet connection and network your computers with your new Router. The following is a list of features that make your Router an ideal solution for your home or small office network. Please be sure to read through this User Manual completely, and pay special attention to Appendix B entitled “Important Factors for Placement and Setup”.

Product Features

Compatibility with both PCs and Mac® Computers

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

Front-Panel LED Display

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

Web-Based Advanced User Interface

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

Integrated 10/100 4-Port Switch

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

Integrated 802.11g Wireless Access Point

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

Built-In Dynamic Host Configuration Protocol (DHCP)

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

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.

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.

MAC Address Filtering

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

Universal Plug-and-Play (UPnP) Compatibility

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

Support for VPN Pass-Through

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

Benefits of a Home Network

By following our simple setup instructions, you will be able to use your Belkin home network to:

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

Advantages of a Wireless Network

Mobility – you'll no longer need a dedicated "computer room"—now you can work on a networked laptop or desktop computer anywhere within your wireless range

Easy installation – Belkin's Setup Wizard makes setup simple

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

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

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

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

Package Contents

- G Wireless Modem Router
- Quick Installation Guide
- RJ11 Telephone Cord – Gray
- RJ45 Ethernet Networking Cable – Yellow
- ADSL Micro Filter*
- Power Adapter
- User Manual and Belkin Setup Assistant Software on CD-ROM

*ADSL micro filter varies by country. If it's not included, you will need to purchase one.

System Requirements

- An active ADSL service with a telephone wall jack for connecting the Router
- At least one computer with a Network Interface Card (NIC) and Internet browser installed and correctly configured
- TCP/IP networking protocol installed on each computer connected to the Router
- No other DHCP server on your local network assigning IP addresses to computers and devices

Setup Assistant Software System Requirements

- A PC running Windows® 2000, XP, or Vista®; or Mac OS® X v10.4, v10.5
- Minimum 500MHz processor and 128MB RAM
- Internet browser

Internet Connection Settings

The Setup Assistant contains a database of Internet Service Providers (ISPs) in each country to help you set up your Router quickly. If your ISP is not on the list, please collect the following information from your ISP before setting up the Router:

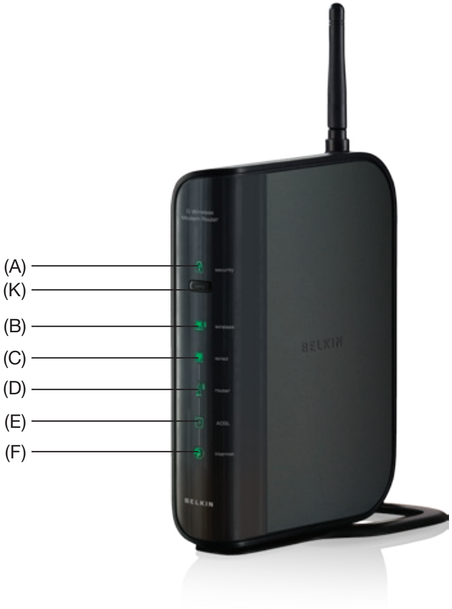
- Internet connection protocol: (PPPoE, PPPoA, Dynamic IP, Static IP)
- Multiplexing method or Encapsulation: (LLC or VC MUX)
- Virtual circuit: VPI (Virtual Path Identifier) __________ (a number between 0 and 255)
- VCI (Virtual Channel Identifier) __________ (a number between 1 and 65535)
- For PPPoE and PPPoA users: ADSL account user name and password _______________
- For static IP users: IP Address ___ . ___ . ___ . ___

  Subnet Mask ___ . ___ . ___ . ___

  Default Gateway Server ___ . ___ . ___ .
- IP address for Domain Name Server ___ . ___ . ___ . ___ (If given by your ISP)

Knowing your Router

The Router has been designed to be placed on a desktop. All of the cables exit from the rear of the Router for better organization and utility. The Network Status Display is easily visible on the FRONT of the Router to provide you with information about network activity and status. See the Network Status Display Guide for more detailed information.



A. Security

OFF	Wireless security is OFF
Solid Green	Wireless security is ON
Flashing Green	WPS sync is in progress

B. Wireless-Computer Status

OFF	Wireless computer is not present
Solid Green	Wireless computer is connected to the Router
Blinking Amber	Problem with wireless computer connecting properly to the Router

C. Wired-Computer Status

OFF	Wired computer is not present
Solid Green	Wired computer is connected to the Router
Blinking Amber	Problem with wired computer connecting to the Router

D. Router/Power Status

When you apply power to the Router or restart it, a short period of time elapses while the Router boots up. During this time, the “router” icon blinks. When the Router has completely booted up, the “router” icon becomes a solid light, indicating the Router is ready for use.

OFF	Router is off
Blinking Green	Router is booting up
Solid Green	Router is on and ready

E. ADSL Line Status

This icon lights in green to indicate that your modem is connected properly to the Router. It turns amber when problem is detected.

OFF	Router is NOT connected to a functioning ADSL line
Blinking Green	Router is attempting to connect to the ADSL line
Solid Green	Router is connected to an ADSL service and is functioning properly
Blinking Amber	Problem with ADSL line

F. Internet Status

This unique icon shows you when the Router is connected to the Internet. When the light is off, the Router is NOT connected to the Internet. When the light is blinking amber, the Router is attempting to connect to the Internet. When the light is solid green, the Router is connected to the Internet. When using the “Disconnect after x minutes” feature, this icon becomes extremely useful in monitoring the status of your Router’s connection.

OFF	Router is NOT connected to the Internet
Blinking Green	Router is attempting to connect to the Internet
Solid Green	Router is connected to the Internet

G. Connection to ADSL – Gray

This port is for connection to your ADSL. Connect your ADSL to this port. An RJ11 telephone cord is provided in the package.

H. Connections to Wired Computers – Yellow

Connect your wired (non-wireless) computers to these ports. These ports are RJ45, 10/100 auto-negotiation, auto-uplinking ports for standard UTP category 5 or 6 Ethernet cable. The ports are labeled 1 through 4, with onboard LEDs on the connectors.

I. Reset Button

The “Reset” button is used in rare cases when the Router may function improperly. Resetting the Router will restore the Router’s normal operation while maintaining the programmed settings. You can also restore the factory default settings by using the “Reset” button. Use the restore option in instances where you may have forgotten your custom password.

i. Resetting the Router

Push and release the “Reset” button. The lights on the Router will momentarily flash. The “Router” light will begin to blink. When the “Router” light becomes solid again, the reset is complete.

ii. Restoring the Factory Defaults

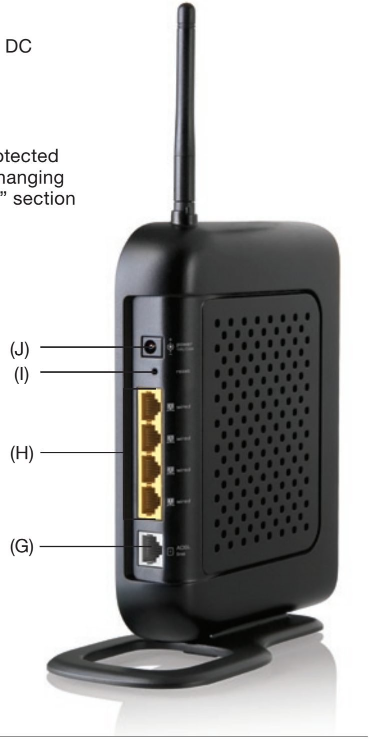
Press and hold the “Reset” button for at least 10 seconds, then release it. The lights on the Router will momentarily flash. The “Router” light will begin to blink. When the “Router” light becomes solid again, the restore is complete.

J. Power Jack – Black

Connect the included 12V/. 1A DC power supply to this jack.

K. WPS Push Button WPS

This button is for the Wi-Fi Protected Setup feature. Refer to the “Changing the Wireless Security Settings” section for more details.



Setup Assistant

Belkin has provided Setup Assistant software to make installing your Router a simple and easy task. You can use it to get your Router up and running in minutes. The Setup Assistant requires that your Windows 2000, XP, or Vista computer be connected directly to your ADSL and that the Internet connection is **active and working** at the time of installation. If it is not, you must use the "Alternate Setup Method" section of this User Manual to configure your Router. Additionally, if you are using an operating system other than Windows 2000, XP, or Vista, or Mac OS X, you must use the "Alternate Setup Method" section of this User Manual.

Step 1: Hardware Connections

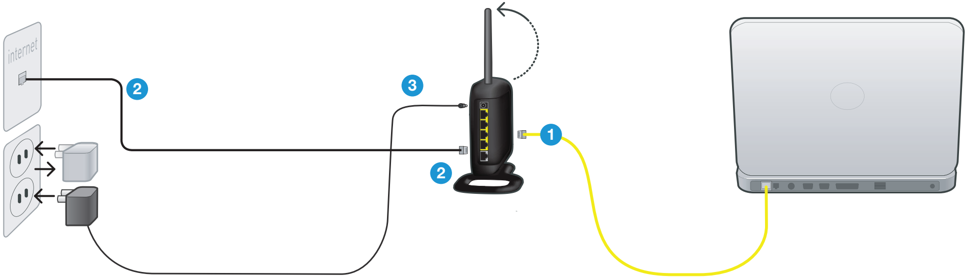
New Router Setup

Follow these steps if you are NOT replacing an existing modem. If you are replacing an existing modem, skip to the next section, "Replacing an Existing Modem or Modem Router".

Unpack your new Router from the box and place it next to your computer. Raise the Router's antenna.

1.1 Brand-New Setup

Follow these steps if you are not replacing an existing modem.
If you are replacing an existing modem, skip to the next section, “Replacing an Existing Modem or Modem Router”.



1. Retrieve the yellow RJ45 cable that was included with your Router. First, connect one end to any yellow port labeled “to Wired Computers” on the back of your Router. Then, connect the other end to the networking port on the back of your computer.

2. Retrieve the included gray RJ11 phone cord. Connect one end to the gray port labeled “to ADSL” on the back of your Router. Then, connect the other end to your ADSL connection (either a wall jack or an ADSL splitter).

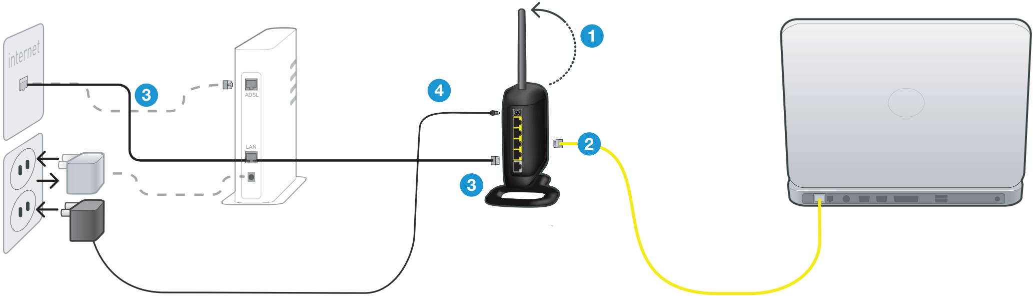
Note: Some ADSL connections require a micro filter. Your ADSL provider can tell you if you need one. Belkin includes a micro filter in regions known to use them. You may or may not have received one in your box.

3. Plug your Router’s power supply into the black port labeled “Power” on the back of your Router.

4. Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the “Power” and “LAN (1-4)” LEDs are lit up in green.

1.2 Replacing an Existing Modem or Modem Router

Follow these steps if you currently have a modem or a modem router that you will be replacing with your new Router.



1. Unpack your new Router from the box and place it next to your computer. Raise the Router’s antennas.

2. Locate the cable that connects your old modem to your computer. Unplug that cable from your old modem and plug it into any yellow port labeled “to Wired Computers” on the back of your new Router.

3. Locate the cable that connects your old modem to the ADSL wall jack. Unplug it from your old modem and then connect it to the gray port labeled “to ADSL” on the back of your Router.

4. Plug your Router’s power supply into the black port labeled “Power” on the back of your Router.

5. Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the “Power” and “LAN (1-4)” LEDs are lit up in green.

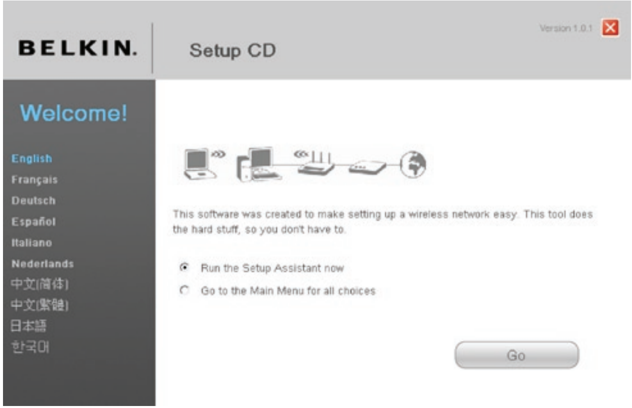
Step 2: Set Up the Router – Run the Setup Assistant Software

1. Shut down any programs that are running on your computer at this time.

Turn off any firewall or Internet-connection-sharing software on your computer.

3. Insert the CD into your computer. The Setup Assistant will automatically appear on your computer's screen within 15 seconds. Click on "Go" to run the Setup Assistant. Follow the instructions there.

IMPORTANT: Run the Setup Assistant from the computer that is directly connected to the Router from 1.1 Step 1.



This software was created to make setting up a wireless network easy. This tool does the hard stuff, so you don't have to.

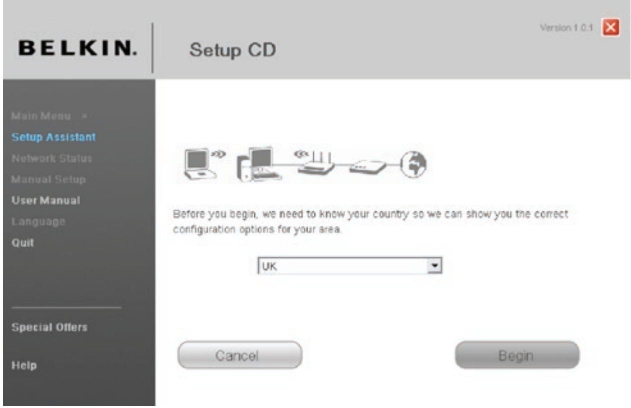
● Run the Setup Assistant now

○ Go to the Main Menu for all choices

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

2.1 Select Country

Select your country from the drop-down box. Click “Begin” to continue.



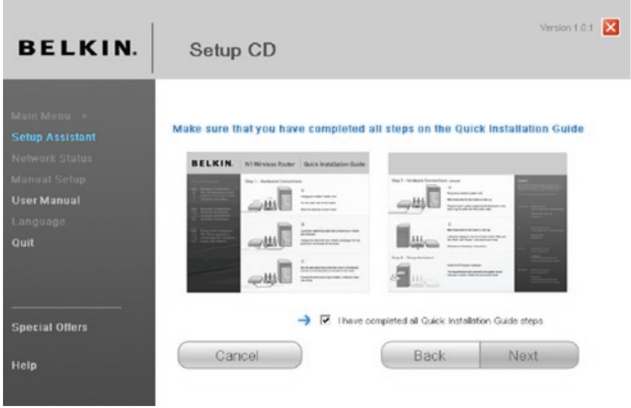
Before you begin, we need to know your country so we can show you the correct configuration options for your area.

UK

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

2.2 Confirmation Screen

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

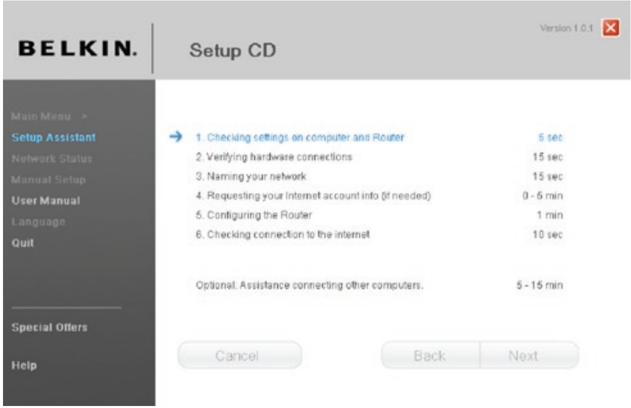


Make sure that you have completed all steps on the Quick Installation Guide

→ ☑ I have completed all Quick Installation Guide steps

2.3 Progress Screen

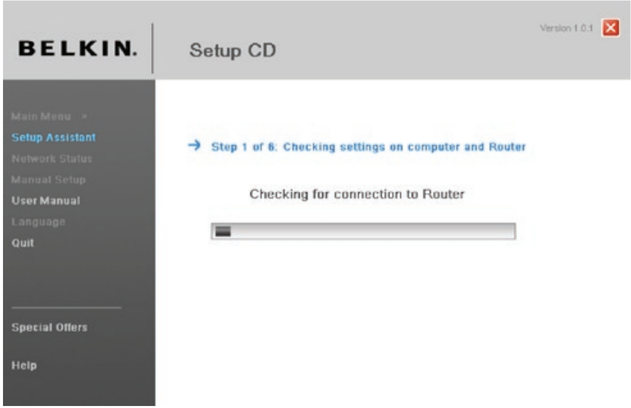
Setup Assistant will show you a progress screen each time a step in the setup has been completed.



1. Checking settings on computer and Router	5 sec
2. Verifying hardware connections	15 sec
3. Naming your network	15 sec
4. Requesting your Internet account info (if needed)	0 - 5 min
5. Configuring the Router	1 min
6. Checking connection to the internet	10 sec
Optional: Assistance connecting other computers.	5 - 15 min

2.4 Checking Settings

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

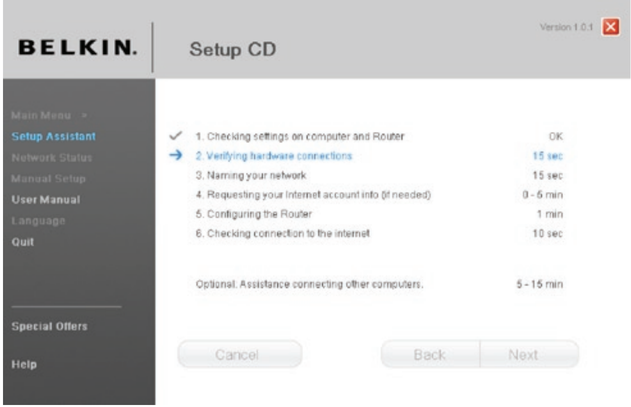


Step 1 of 6: Checking settings on computer and Router

Checking for connection to Router

2.5 Verifying Hardware Connections

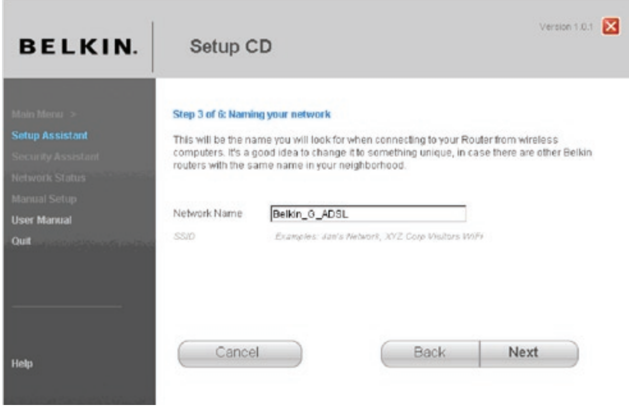
The Setup Assistant will now verify your hardware connection.



✓ 1. Checking settings on computer and Router	OK
→ 2. Verifying hardware connections	15 sec
3. Naming your network	15 sec
4. Requesting your Internet account info (if needed)	0 - 6 min
5. Configuring the Router	1 min
6. Checking connection to the internet	10 sec
Optional: Assistance connecting other computers.	5 - 15 min

2.6 Naming your Wireless Network

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



Step 3 of 6: Naming your network

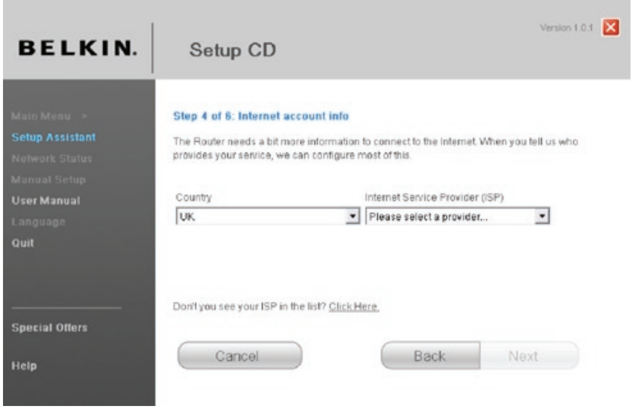
This will be the name you will look for when connecting to your Router from wireless computers. It's a good idea to change it to something unique, in case there are other Belkin routers with the same name in your neighborhood.

Network Name: Belkin_G_ADSL

SSID — Examples: Jan's Network, XYZ Corp Visitors WiFi

2.7 Requesting Internet Account Info (if needed)

If your Internet account requires a login and password, you will be prompted with a screen similar to the illustration below. Select your country or ISP from the drop-down boxes.



Step 4 of 6: Internet account info

The Router needs a bit more information to connect to the Internet. When you tell us who provides your service, we can configure most of this.

Country: UK

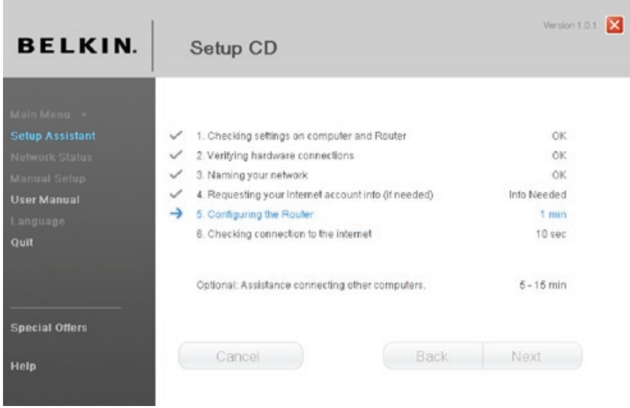
Internet Service Provider (ISP): Please select a provider...

Don't you see your ISP in the list? Click Here.

2.8 Configuring the Router

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

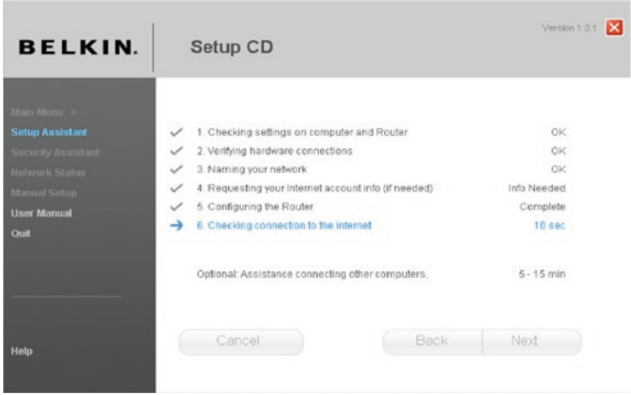
Note: Do not disconnect any cable or power off the Router while the Router is rebooting. Doing so will render your Router inoperable.



✓	1. Checking settings on computer and Router	OK
✓	2. Verifying hardware connections	OK
✓	3. Naming your network	OK
✓	4. Requesting your Internet account info (if needed)	Info Needed
→	5. Configuring the Router	1 min
	6. Checking connection to the internet	10 sec
	Optional: Assistance connecting other computers.	5 - 15 min

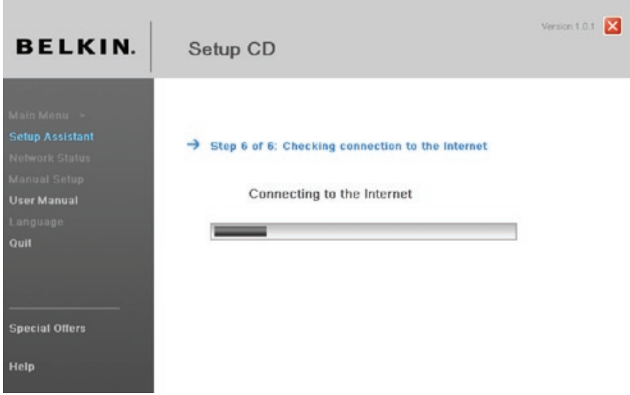
2.9 Checking Internet Connection

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



✓ 1. Checking settings on computer and Router OK
✓ 2. Verifying hardware connections OK
✓ 3. Naming your network OK
✓ 4. Requesting your Internet account info (if needed) Info Needed
✓ 5. Configuring the Router Complete
→ 6. Checking connection to the internet 10 sec

Optional: Assistance connecting other computers. 5 - 15 min



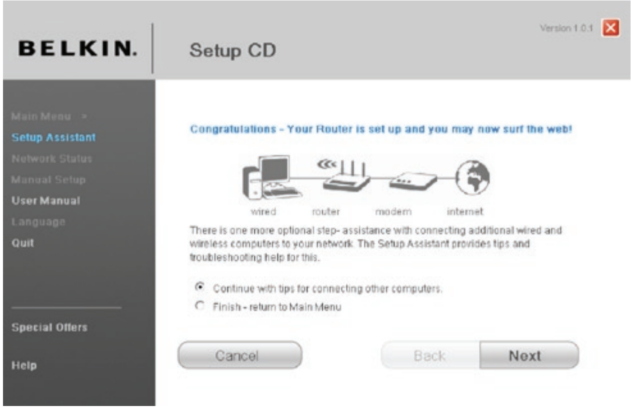
→ Step 6 of 6: Checking connection to the Internet

Connecting to the Internet

Congratulations

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

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



Congratulations - Your Router is set up and you may now surf the web!

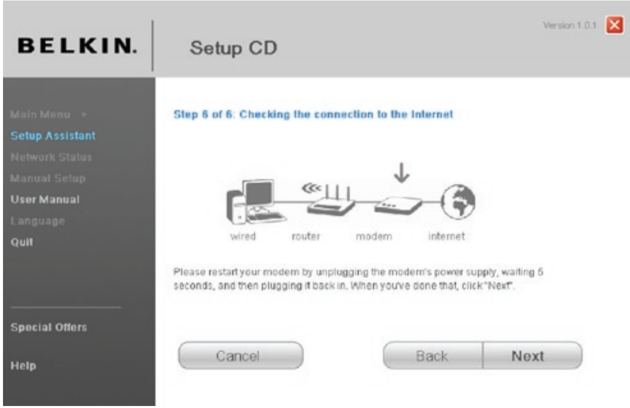
There is one more optional step- assistance with connecting additional wired and wireless computers to your network. The Setup Assistant provides tips and troubleshooting help for this.

● Continue with tips for connecting other computers.

○ Finish - return to Main Menu

Troubleshooting

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

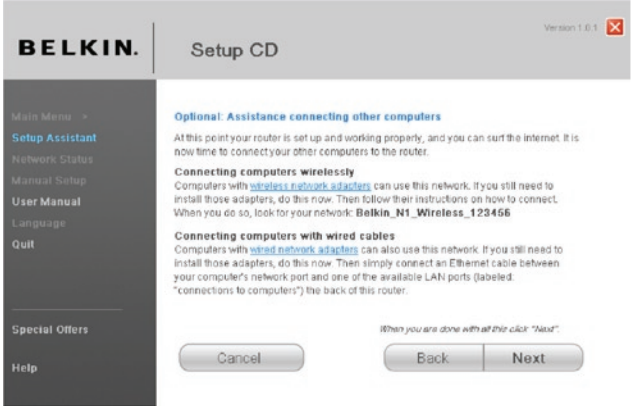


Step 6 of 6: Checking the connection to the Internet

Please restart your modem by unplugging the modem's power supply, waiting 5 seconds, and then plugging it back in. When you've done that, click "Next".

2.10 Optional: Assistance Connecting Other Computers

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



Optional: Assistance connecting other computers

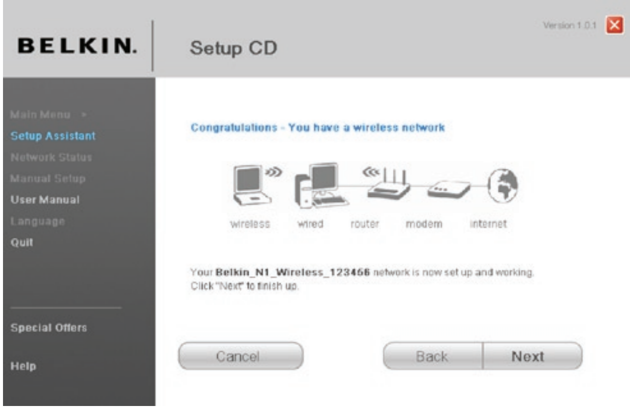
At this point your router is set up and working properly, and you can surf the internet. It is now time to connect your other computers to the router.

Connecting computers wirelessly
Computers with wireless network adapters can use this network. If you still need to install those adapters, do this now. Then follow their instructions on how to connect. When you do so, look for your network: **Belkin_N1_Wireless_123456**

Connecting computers with wired cables
Computers with wired network adapters can also use this network. If you still need to install those adapters, do this now. Then simply connect an Ethernet cable between your computer's network port and one of the available LAN ports (labeled: "connections to computers") the back of this router.

When you are done with all this click "Next".

Once you have verified that your other wired and wireless computers are properly connected, your network is set up and working. You can now surf the Internet. Click "Next" to take you back to the main menu.



Congratulations - You have a wireless network

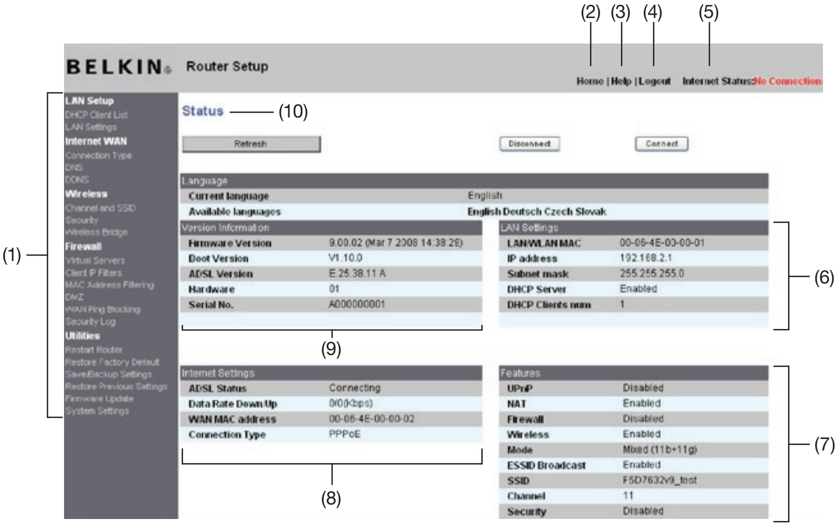
Your **Belkin_N1_Wireless_123456** network is now set up and working.
Click "Next" to finish up.

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.

Using Web-Based Manager

Once your host PC is properly configured, start your web browser and type the private IP address of the Router into the URL field: "192.168.2.1" and then click "Enter".



Language	
Current language	English
Available languages	English Deutsch Czech Slovak

Version Information	
Firmware Version	9.00.02 (Mar 7 2008 14:38:29)
Boot Version	V1.10.0
ADSL Version	E.25.38.11 A
Hardware	01
Serial No.	A000000001

LAN Settings	
LAN/WLAN MAC	00-06-4E-00-00-01
IP address	192.168.2.1
Subnet mask	255.255.255.0
DHCP Server	Enabled
DHCP Clients num	1

Internet Settings	
ADSL Status	Connecting
Data Rate Down/Up	0/0(Kbps)
WAN MAC address	00-06-4E-00-00-02
Connection Type	PPPoE

Features	
UPnP	Disabled
NAT	Enabled
Firewall	Disabled
Wireless	Enabled
Mode	Mixed (11b+11g)
ESSID Broadcast	Enabled
SSID	F5D7632v9_test
Channel	11
Security	Disabled

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. Help Button

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

4. Login/Logout Button

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

5. Internet Status Indicator

This indicator is visible in all pages of the Router, showing 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.

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

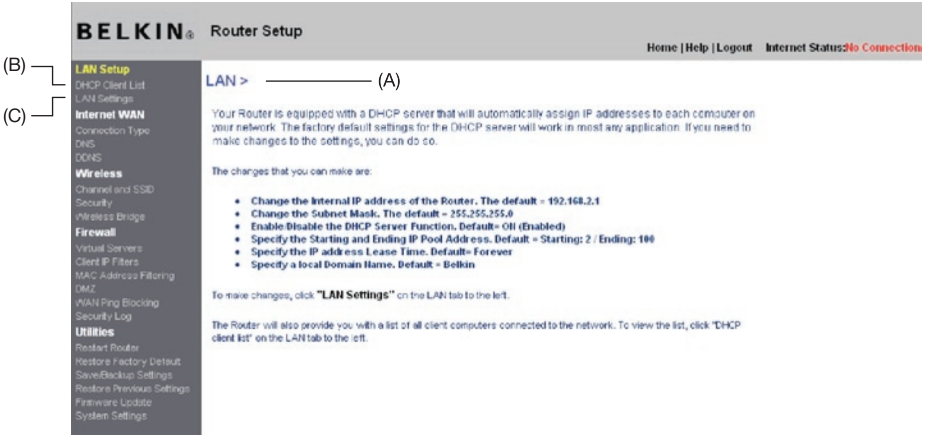
The page you are on can be identified by this name. This manual will sometimes refer to pages by name. For instance, “LAN > LAN Settings” refers to the “LAN Settings” page.

Changing LAN Settings

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

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)**.



LAN >

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

The changes that you can make are:

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

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

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

IP Address

The "IP address" is the internal IP address of the Router. The default IP address is "192.168.2.1". To access the advanced setup interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type in the new IP address and click "Apply Changes". The IP address you choose should be a non-routable IP. Examples of a non-routable IP are:

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

Subnet Mask

There is no need to change the subnet mask. This is a unique, advanced feature of your Belkin Router.

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".

IP Pool

The range of IP addresses set aside for dynamic assignment to the computers on your network. 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 starting IP address must be lower in number than the ending IP address.

Lease Time

The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to "Forever". The default setting is "Forever", meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular computer. Setting lease times for shorter intervals such as one day or one hour frees IP addresses after the specified period of time. This also means that a particular computer's IP address may change over time. If you have set any of the other advanced features of the Router such as DMZ or client IP filters, these are dependent on the IP address. For this reason, you will not want the IP address to change.

Local Domain Name

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, which are connected to your network. You are able to view the IP address of the computer, the host name (name of the computer in your network), and the MAC address of the computer's network interface card (NIC). Pressing the "Refresh" button will update the list. If there have been any changes, the list will be updated.

Internet WAN

The "Internet WAN" tab is where you will set up your Router to connect to your Internet Service Provider (ISP). The Router is capable of connecting to virtually any 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" (1) on the left side of the screen. Select the connection type you use. If your ISP gave you DNS settings, clicking "DNS" (2) 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 "Connected" if your Router is set up properly.

Connection Type

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

PPPoE

PPPoA

Dynamic IP (1483 Bridged)

Static IP (IPoA)

Modem Only (Disable Internet Sharing)

Note: If you are not sure which connection type to select, please contact your ISP.

Select the type of connection you use by clicking the radio button next to your connection type and then clicking "Next".

Setting your ISP Connection Type to PPPoE or PPPoA

PPPoE (Point-to-Point Protocol over Ethernet) is the standard method of connecting networked devices. It requires a user name and password to access the network of your ISP for connecting to the Internet. PPPoA (PPP over A™) is similar to PPPoE, but is mostly implemented in the UK. Select PPPoE or PPPoA and click “Next”. Then, enter the information provided by your ISP, and click “Apply Changes” to activate your settings.

1. **User Name –** Enter the user name. (Assigned by your ISP).

2. **Password –** Enter your password. (Assigned by your ISP).

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

4. **IP Assigned by ISP –** Leave “Yes” if your ISP automatically assigns an IP address. If your ISP assigned a fixed IP address, select “No” and enter assigned values.

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

6. **Encapsulation –** Select your encapsulation type (supplied by your ISP) to specify how to handle multiple protocols at the A™ transport layer. VC-MUX: PPPoA Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with fewer overheads. LLC: PPPoA Logical Link Control allows multiple protocols running over one virtual circuit (more overhead).

7. **Dial on Demand –** By selecting “Dial on Demand”, your Router will automatically connect to the Internet when a user opens up a web browser.

8. **Idle Time (Minutes) –** Enter the maximum idle time for the Internet connection. After this time has been exceeded, the connection will be terminated.

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

Setting your Connection Type to Dynamic IP (1483 Bridged)

This connection method bridges your network and ISP's network together. The Router will obtain an IP address automatically from your ISP's DHCP server.

1. **IP Assigned by ISP –** Leave "Yes" if your ISP automatically assigns an IP address. If your ISP assigned a fixed IP address, select "No" and enter assigned values.
2. **VPI/VCI –** Enter your VPI and VCI parameter here. These identifiers are assigned by your ISP.
3. **Encapsulation –** Select LLC or VC MUX your ISP uses.

Setting your ISP Connection Type to Static IP (IPoA)

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

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

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

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

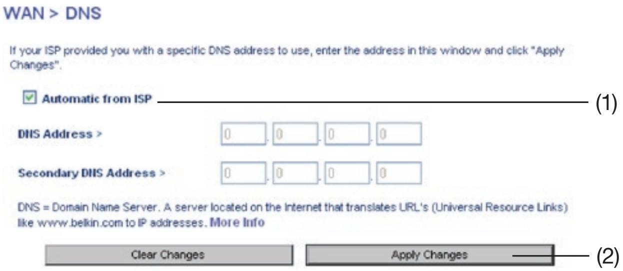
1. **VPI/VCI –** Enter your VPI and VCI parameter here. (Assigned by your ISP).

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

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 > 0 . 0 . 0 . 0

Secondary DNS Address > 0 . 0 . 0 . 0

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

Using DDNS (Dynamic DNS)

The DDNS service allows you to alias a dynamic IP address to a static host name in any of the many domains DynDNS.org offers, allowing your network computers to be more easily accessed from various locations on the Internet. DynDNS.org provides this service, for up to five host names, free to the Internet community. TZO.com is another alternative to DynDNS.org. DDNS service is ideal for a home website, file server, or to make it easy to access your home PC and stored files while you're at work. Using the service can ensure that your host name always points to your IP address, no matter how often your ISP changes it. When your IP address changes, your friends and associates can always locate you by visiting yourname.dyndns.org instead! To register free for your Dynamic DNS host name, please visit http://www.dyndns.org.

Setting up the Router's Dynamic DNS Update Client

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

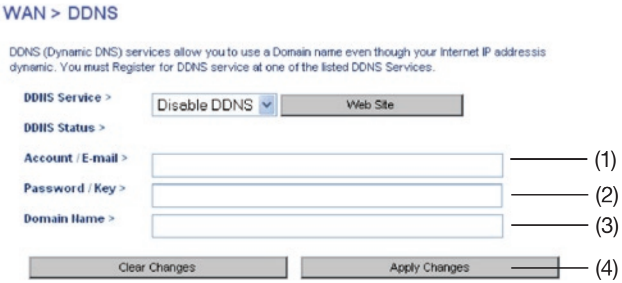
1. Enter your DynDNS.org user name in the "Account / E-mail" field **(1)**.

2. Enter your DynDNS.org password in the "Password / Key" field **(2)**.

3. Enter the DynDNS.org domain name you set up with DynDNS.org in the "Domain Name" field **(3)**.

4. Click "Apply Changes" to update your IP address.

Whenever your IP address assigned by your ISP changes, the Router will automatically update DynDNS.org's servers with your new IP address. You can also do this manually by clicking the "Apply Changes" button **(4)**.



WAN > DDNS

DDNS (Dynamic DNS) services allow you to use a Domain name even though your Internet IP addressis dynamic. You must Register for DDNS service at one of the listed DDNS Services.

DDNS Service > Disable DDNS

DDNS Status >

Account / E-mail >

Password / Key >

Domain Name >

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

1. Changing the Wireless Network Name (SSID)

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. 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 and click “Apply Changes”. The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.

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.

3. Using the Wireless Mode Switch

Your Router can operate in three different wireless modes: “Mixed (11b+11g)”, “11g Only”, and “11b Only”. The different modes are explained below.

Mixed (11b+11g) Mode

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

11g-Only Mode

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

11b-Only Mode

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

4. Changing the Wireless Channel

There are a number of operating channels from which to choose. 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 requirements. Your Router is configured to operate on the proper channels in which the country you reside. The default is “Auto”. 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.

Encryption/Security

Securing your Wi-Fi Network

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

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

Wired Equivalent Privacy (WEP)

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

64-Bit WEP

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

128-Bit WEP

As a result of 64-bit WEP's potential security weaknesses, a more secure method of 128-bit encryption was developed. 128-bit encryption includes a key length of 104 bits plus 24 additional bits of system-generated data (128 bits total). Some hardware manufacturers refer to 128-bit as 104-bit encryption. Most of the new wireless equipment in the market today supports both 64-bit and 128-bit WEP encryption, but you might have older equipment that only supports 64-bit WEP. All Belkin wireless products will support both 64-bit and 128-bit WEP.

Encryption Keys

After selecting either the "64-bit" or "128-bit WEP" encryption mode, it is critical that you generate an encryption key. If the encryption key is not consistent throughout the entire wireless network, your wireless networking devices will be unable to communicate with one another on your network and you will not be able to successfully communicate within your network. You can enter your key by typing in the hex key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a key. A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit WEP key
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key

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

Wi-Fi Protected Access (WPA)

WPA is a new Wi-Fi standard that was designed to improve upon the security features of WEP. To use WPA security, the drivers and software of your wireless equipment must be upgraded to support WPA. These updates will be found on the wireless vendors' websites. There are two types of WPA security: WPA-PSK (no server) and WPA (with 802.1x radius server).

WPA-PSK (no server)

This method uses what is known as a "pre-shared key" as the network key. A network key is basically a password that is between eight and 63 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same network key to access the network. Typically, this is the mode that will be used in a home environment.

WPA (with 802.1x radius server)

With this system, a radius server distributes the network key to the clients automatically. This is typically found in a business environment.

WPA2

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

WPA2 Requirements

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

For a Windows XP computer that does not have Service Pack 2 (SP2), a file from Microsoft called "Windows XP Support Patch for Wireless Protected Access (KB 826942)" is available for free download at http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=009D8425-CE2B-47A4-ABEC-274845DC9E91.

For Windows XP computers with SP2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB893357). The update can be downloaded from: http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en.

IMPORTANT: You also need to ensure that all your wireless client cards and adapters support WPA2, and that you have downloaded and installed the latest driver. Most of the Belkin wireless cards have updated drivers available for download from the Belkin support site: www.belkin.com/networking. For a list of Belkin wireless products that support WPA/WPA2, please visit our website at www.belkin.com/networking.

Sharing the Same Network Keys

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

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 2-digit numbers. 128-bit keys are 13 2-digit numbers.

For instance:

AF 0F 4B C3 D4 = 64-bit key
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit key

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

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

WEP Setup

1. Select “WEP” from the drop-down menu.

2. Select “WEP Mode” of 64-bit or 128-bit.

3. After selecting your WEP mode, you can enter your key by typing in the hex key manually.

A hex (hexadecimal) key is a mixture of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

AF 0F 4B C3 D4 = 64-bit key
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit key

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

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

Changing the Wireless Security Settings

Your Router is equipped with WPA/WPA2, the latest wireless security standard. It also supports the legacy security standard, WEP. By default, wireless security is disabled. To enable security, you must first determine which standard you want to use. To access the security settings, click “Security” on the “Wireless” tab.

WPA Setup

Note: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this User Manual's publication, a security patch download is available free from Microsoft. This patch works only with the Windows XP operating system. You also need to download the latest driver for your Belkin Wireless G Desktop or Notebook Card from the Belkin support site. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as Belkin 802.11g products.

There are two types of WPA security: WPA-PSK (no server) and WPA (with radius server). WPA-PSK (no server) uses a so-called pre-shared key (PSK) as the security key. A pre-shared key is a password that is between eight and 63 characters long. It can be a combination of letters, numbers, and other characters. Each client uses the same key to access the network. Typically, this mode will be used in a home environment. WPA (with radius server) is a configuration wherein a radius server distributes the keys to the clients automatically. This is typically used in a business environment. WPA2 is the second generation of WPA, offering a more advanced encryption technique over WPA.

Setting WPA/WPA2-PSK (no server)

1. From the “Allowed Client Type” drop-down menu, select “WPA/WPA2”.

2. For “Authentication”, select “Pre-shared Key” for typical home/SOHO use. This setting will have to be identical on the clients that you set up.

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

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

Wireless Range Extension and Bridging

What is a Wireless Bridge?

A wireless bridge is actually an operation "mode" you can use to extend the range of your wireless network, or add an extension of your network in another area of your office or home without running cables.

Note: We can make no guarantees that this feature will interoperate with hardware from other wireless manufacturers.

Note: Please make sure to download the latest firmware version for the Router for optimal performance at: http://web.belkin.com/support.

Adding Another Network Segment Wirelessly

Connecting a network switch or hub to the Router's RJ45 jack will allow a number of computers connected to the switch access to the rest of the network.

Setting up a Bridge Between your Router and a Secondary Access Point

Bridging your Belkin Router to a secondary access point requires that you access the Router's Advanced Setup Utility and enter the MAC address of the access point in the appropriate area. There are also a few other requirements.

PLEASE BE SURE TO FOLLOW THE STEPS BELOW CAREFULLY.

1. Set your access point to the same channel as the Router. For more information on changing channels, see the "Wireless - Channel and SSID" section of this User Manual.

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

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

4. Connect power to your access point. Make sure the access point is on and proceed to the next step.

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

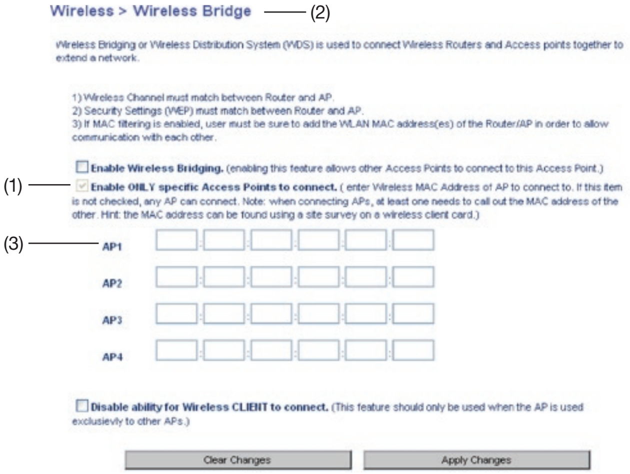
6. You will see the Router's user interface in the browser window. Click "Wireless Bridge" **(2)** on the left-hand side of the screen. You will see the following screen.

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

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

9. Bridging is now set up.

Note: It may take up to a minute for the bridged connection to properly establish itself. In some cases, it may be necessary to restart the access point and the Router to initiate the bridge.



Wireless > Wireless Bridge

Wireless Bridging or Wireless Distribution System (WDS) is used to connect Wireless Routers and Access points together to extend a network.

1) Wireless Channel must match between Router and AP.
2) Security Settings (WEP) must match between Router and AP.
3) If MAC filtering is enabled, user must be sure to add the WLAN MAC address(es) of the Router/AP in order to allow communication with each other.

□ **Enable Wireless Bridging.** (enabling this feature allows other Access Points to connect to this Access Point.)

☑ **Enable ONLY specific Access Points to connect.** (enter Wireless MAC Address of AP to connect to. If this item is not checked, any AP can connect. Note: when connecting APs, at least one needs to call out the MAC address of the other. Hint: the MAC address can be found using a site survey on a wireless client card.)

AP1 __ : __ : __ : __ : __ : __

AP2 __ : __ : __ : __ : __ : __

AP3 __ : __ : __ : __ : __ : __

AP4 __ : __ : __ : __ : __ : __

□ **Disable ability for Wireless CLIENT to connect.** (This feature should only be used when the AP is used exclusievly to other APs.)

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

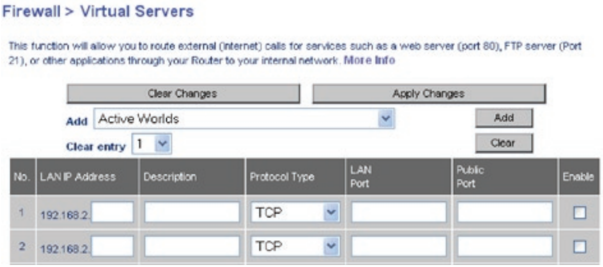
The firewall also masks common ports that are frequently used to attack networks. These ports appear to be “Stealth”, meaning that essentially they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.

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. You can manually input this port information into the Router.

Choosing an Application

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



Firewall > Virtual Servers

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

Add: Active Worlds

Clear entry: 1

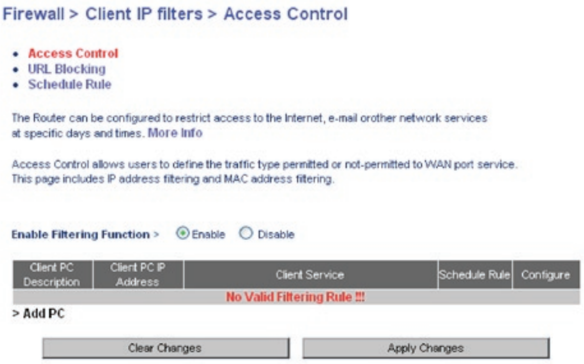
No.	LAN IP Address	Description	Protocol Type	LAN Port	Public Port	Enable
1	192.168.2.		TCP			□
2	192.168.2.		TCP			□

Manually Entering Settings into the Virtual Server

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

Client IP Filters

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



Firewall > Client IP filters > Access Control

The Router can be configured to restrict access to the Internet, e-mail orother 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.

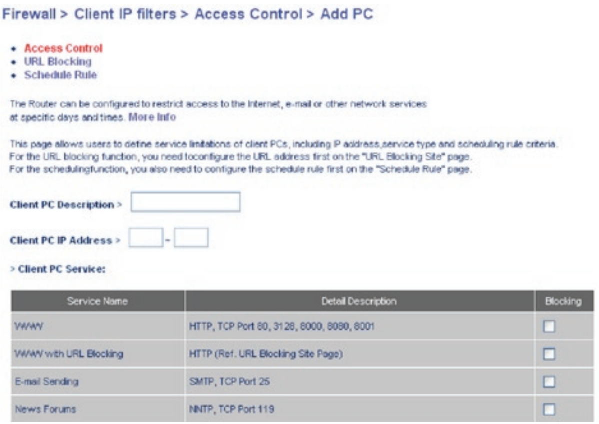
Enable Filtering Function > ● Enable ○ Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

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).
3. Click "OK" and then click "Apply Changes" to save your settings.



Firewall > Client IP filters > Access Control > Add PC

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 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 toconfigure the URL address first on the "URL Blocking Site" page.
For the schedulingfunction, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address > -

> Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	□
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	□
E-mail Sending	SMTP, TCP Port 25	□
News Forums	NNTP, TCP Port 119	□

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

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.

Follow these steps to add a schedule:

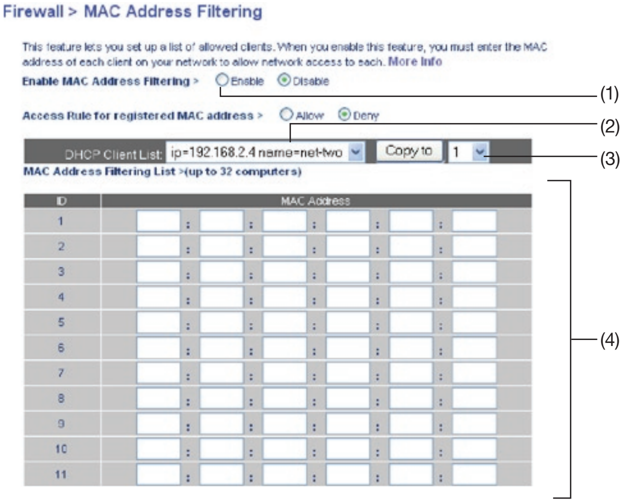
1. Click "Add Schedule Rule".
2. You will see the following screen.
3. To configure the schedule rule, specify the name, comment, start time, and end time that you want to filter on your network.
4. Click "OK" and then "Apply Changes" to save your settings.
5. To complete this configuration, you will 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.

Setting MAC-Address Filtering

The MAC-address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client (computer) on your network to allow network access to each. The “Block” feature lets you turn on and off access to the network easily for any computer without having to add and remove the computer’s MAC address from the list. To enable this feature, select “Enable MAC Address Filtering” **(1)**. Next, select the access rule as “Allow” or “Deny”.

Then, enter the MAC address of each computer on your network by selecting from the “DHCP Client List” drop-down box **(2)** and the ID to copy to **(3)** before clicking “Copy to”. As an alternative method, click in the space provided **(4)** and enter the MAC address of the computer you want to add to the list. Click “Apply Changes” to save the settings.

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



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

Access Rule for registered MAC address > ○ Allow ● Deny

DHCP Client List: ip=192.168.2.4 name=net-two Copy to 1

MAC Address Filtering List >(up to 32 computers)

ID	MAC Address
1	: : : : :
2	: : : : :
3	: : : : :
4	: : : : :
5	: : : : :
6	: : : : :
7	: : : : :
8	: : : : :
9	: : : : :
10	: : : : :
11	: : : : :

DMZ (Demilitarized Zone)

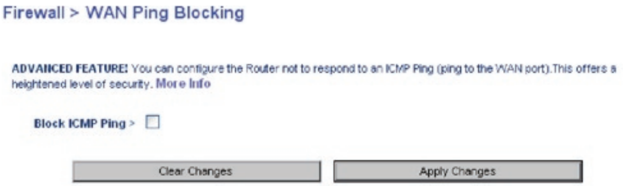
If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted 2-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video-conferencing application. Use this 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 IP address in the IP field and select “Enable”. Click “Apply Changes” for the change to take effect. If you are using multiple static WAN IP addresses, it is possible to select to which WAN IP address the DMZ host will be directed. Type in the WAN IP address to which you wish the DMZ host to direct, enter the last two digits of the IP address of the DMZ host computer, select “Enable”, and click “Apply Changes”.

Blocking an ICMP Ping

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

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



Firewall > WAN Ping Blocking

ADVANCED FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to the WAN port).This offers a heightened level of security. More Info

Block ICMP Ping > □

Utilities

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

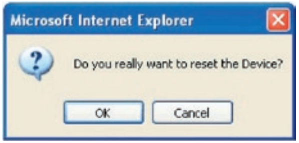
Restart Router

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

Restarting the Router to Restore Normal Operation

1. Click the “Restart Router” button.

2. The following message will appear. Click “OK” to restart your Router.



Microsoft Internet Explorer

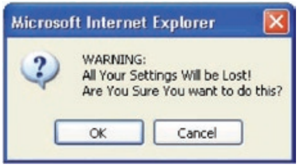
Do you really want to reset the Device?

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.



Microsoft Internet Explorer

WARNING:
All Your Settings Will be Lost!
Are You Sure You want to do this?