BELKIN®

ADSL Modem with Wireless G Router

Share

Network your computers and share your ADSL Internet access

User Manual

((G)) 802.11g 54 Mbps 2.4GHz • Wireless

F5D7632uk4

Table of Contents

Thank you for purchasing the Belkin ADSL Modem with Wireless G 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, and XP, 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 Belkin 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 Easy Installation 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

Make Sure You Have the Following

Package Contents

- ADSL Modem with Wireless G Router
- RJ11 Telephone Cord - Gray
- RJ45 Ethernet Networking Cable — Yellow
- USB 1.0 Cable — Blue
- ADSL Microfilter*
- Power Adapter
- User Manual CD

*ADSL microfilter 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

Internet Connection Settings

Please collect the following information from your Internet Service Provider (ISP) before setting up the ADSL Modem Wireless G Router.

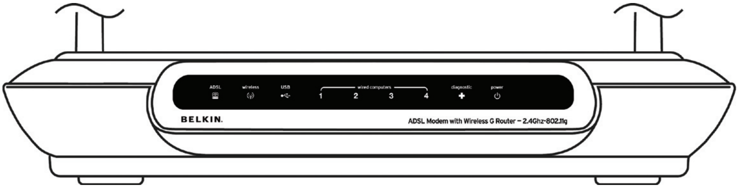
- Internet connection protocol: ________ (PPPoE, PPPoA, Dynamic IP, Static IP)
- Multiplexing method or Encapsulation: _________ (LLC or VC MUX)
- Virtual circuit: VPI (Virtual Path Identifier) _________
  (a number between 0 and 255)
- VCI (Virtual Channel Identifier) _________
  (a number between 1 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)

Note: See Appendix C in this User Manual for some common DSL Internet setting parameters. If you are not sure, please contact your ISP.

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 LED indicators are easily visible on the front of the Router to provide you with information about network activity and status.

Front Panel

The following illustration shows the front panel of the Router:



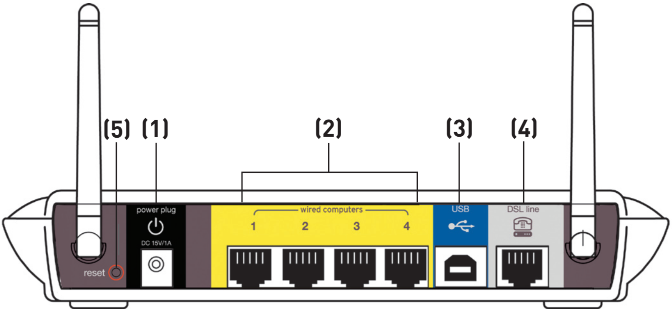
LED Indicators

The Router is equipped with nine LEDs on the front panel as described in the table below (from left to right):

LED	Color	Status	Description
ADSL ☎	Green	Off	Power off or ADSL line connection is physically disconnected
		Blinking	Handshaking or training is in progress
		Solid	ADSL line connection is OK
Wireless ((ı))	Green	Off	Power off or no radio signal (WLAN card is not present or fails to function)
		Blinking	Traffic is going through wireless LAN interface
		Solid	Wireless LAN interface ready to work
USB •⭠	Green	Off	Power off or wait for USB connection going up
		Blinking	User data is going through USB port
		Solid	USB connection is OK
LAN 1–4	Green	Off	Power off or no Ethernet carrier is present
		Blinking	Ethernet carrier is present and user data is going through Ethernet port
		Solid	Ethernet carrier is present
Diagnostic ✚	Green	Off	Power off or initial self-test of the unit is OK
		Blinking	Software downloading or updating operation parameters located in flash memory is in progress
		Solid	Initial self-test failure or programming flash memory failure
Power ⏻	Green	Off	Power off
		Solid	Power on

Rear Panel

The following figure illustrates the rear panel of your Router.



1. **PWR**
   Connect the included power supply to this inlet. Using the wrong type of power adapter may cause damage to your Router.

2. **LAN**
   The Ethernet 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 network-enabled computers or any networking devices to one of these ports.

3. **USB**
   The USB client port connects your network-enabled computers or any networking devices to the Router.

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

5. **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.

   a. **Resetting the Router**

      Push and hold the "Reset" button for one second then release it. When the "Power/Ready" light becomes solid again, the reset is complete.

   b. **Restoring the Factory Defaults**

      Press and hold the "Reset" button for 20 seconds then release it. When the "Power/Ready" light becomes solid again, the restore is complete.

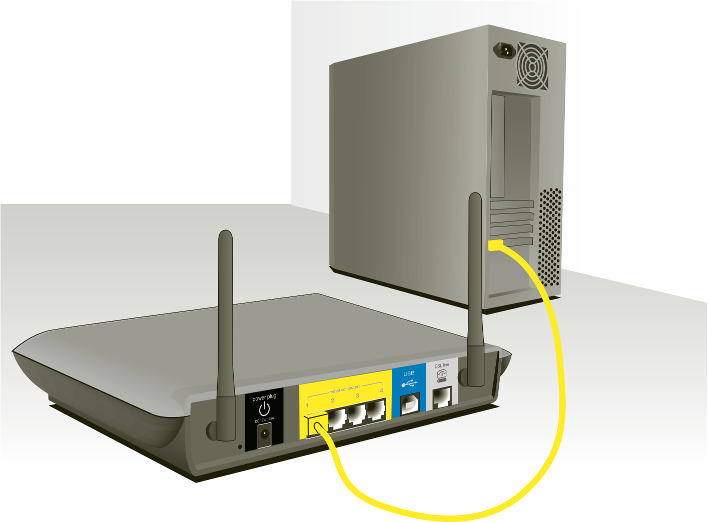
Positioning your Router

Your wireless connection will be stronger the closer your computer is to your Router. Typical indoor operating range for your wireless devices is between 100 and 200 feet. In the same way, your wireless connection and performance will degrade somewhat as the distance between your Router connected devices increases. This may or may not be noticeable to you. As you move farther from your Router, connection speed may decrease. Factors that can weaken signals simply by getting in the way of your network's radio waves are metal appliances, or obstructions, and walls. Please see "Appendix B: Important Factors for Placement and Setup" in this User Manual for more guidelines.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between five and 10 feet from the Router, in order to see if distance is the problem. If difficulties persist even at close range, please see the Troubleshooting section for solutions.

Connecting your Computers

1. Power off your computers and networking equipment.
2. Connect your computer to one of the yellow RJ45 ports on the rear of the Router labeled "connections to your computers" by using an Ethernet networking cable (one Ethernet network cable is supplied).

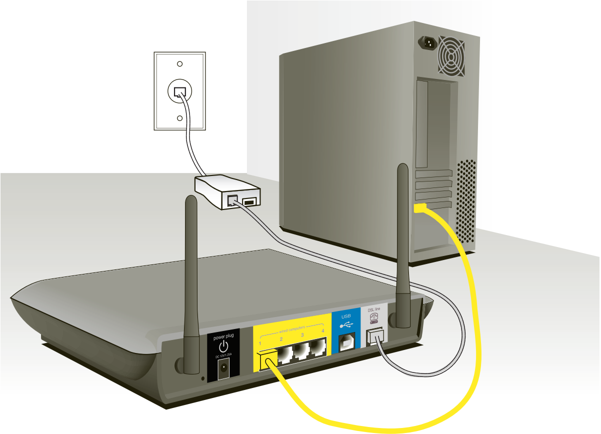


Connecting your ADSL Line

Connection for the Router to the ADSL line varies by country and region. Typically it involves a microfilter or a microfilter with built-in splitter to allow simultaneous use of ADSL service and telephone service on the same telephone line. Please read the following steps carefully and select appropriate method.

1. If your telephone service and ADSL service are on the same telephone line, ADSL microfilters are needed for each telephone and device, such as answering machine, fax machine, and caller ID display. Additional splitters may be used to separate telephone lines for telephone and the Router.

2. If your telephone service and ADSL service are on the same telephone line and you are using an ADSL microfilter with built-in splitter, connect the splitter to the telephone wall jack providing ADSL service. Then, connect the telephone cord from the ADSL microfilter RJ11 port generally labeled “DSL” to the gray RJ11 port labeled “DSL line” on the back of your Router. Connect telephony device to the other port on the ADSL splitter commonly labeled “Phone”. An additional ADSL microfilter is needed for another telephone and device on the same line.



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

3. If you have a dedicated ADSL service telephone line with an RJ11 wall jack, simply connect a telephone cord from the wall jack to the gray RJ11 port labeled "DSL line" on the back of your Router.

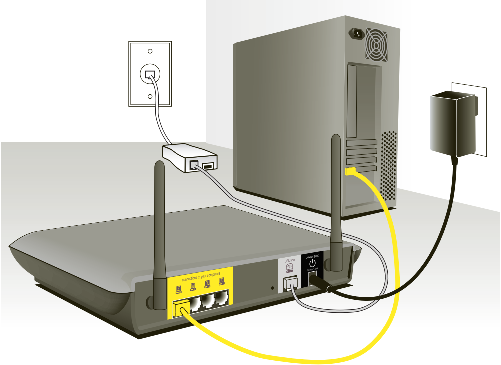
4. If you have an RJ45 wall jack for your ADSL service, connect an RJ45-to-RJ11 converter to the wall jack. Then connect one end of a telephone cord to the converter and the other end to the gray RJ11 port labeled "DSL line" on the back of your Router.

   Note: ADSL microfilter may or may not be provided depending on your country.

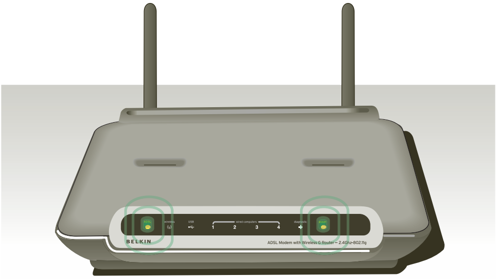
Powering up your Router

1. Connect the supplied power adapter to the Router power-input plug labeled “Power”.

   Note: For safety and performance reasons, only use the supplied power adapter to prevent damage to the Router.



2. After connecting the power adapter and the power source is turned on, the Router’s power icon ⏻ on the front panel should be on. It might take a few minutes for the Router to fully start up.

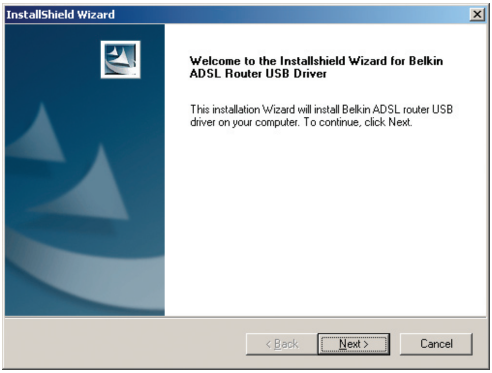


3. Turn on your computers. After your computers boot up, the LAN status LED 💻 on the front of the Router will be on for each port to which a wired computer is connected. These lights show you the connection and activity status. Now you are ready to configure the Router for ADSL connection.

USB Driver Installation

Important: If the Router is connected to a computer through an Ethernet port, you can skip this chapter.

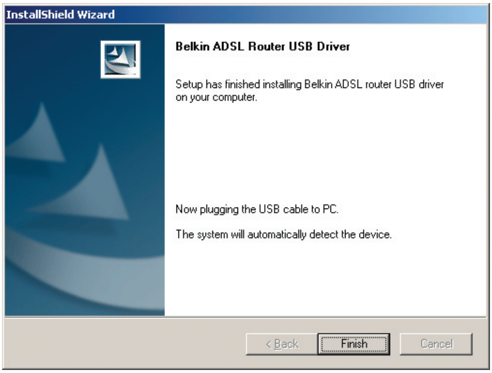
1. Insert the CD into your CD-ROM drive.
2. Open up your CD-ROM drive by going into "My Computer". Double-click on the folder named "Files". Double-click on the folder named "USB". Next double-click on the icon named "setup.exe".
3. When the following screen appears, click "Next".



Welcome to the Installshield Wizard for Belkin ADSL Router USB Driver

This installation Wizard will install Belkin ADSL router USB driver on your computer. To continue, click Next.

4. When the following screen appears, click "Finish".



Belkin ADSL Router USB Driver

Setup has finished installing Belkin ADSL router USB driver on your computer.

Now plugging the USB cable to PC.

The system will automatically detect the device.

5. Connect the USB cable to your Router and PC.

   Note: If the USB device is not detected, check the USB cable between the PC and the device. Also verify that the device is powered on.

6. The system will detect the USB driver automatically. When the system detects it, the following dialog box will appear. Click “Yes”.

7. Now, the system will copy the proper files for this Router.

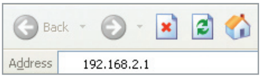
8. When the file copying is finished, the dialog above will close. Now the USB driver is installed properly. You can now use the Router.

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

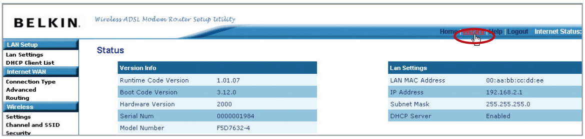
Once your host PC is properly configured, start your web browser and type the private IP address of the Router into the URL field: "192.168.2.1" and then click "Enter".



Address 192.168.2.1

Setup Wizard

Click on the "Wizard" link from the status page.

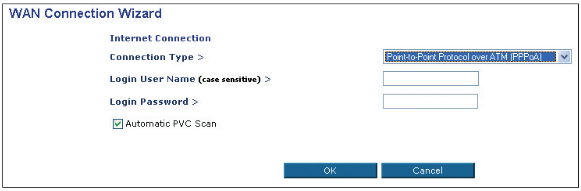


Status

Version Info	
Runtime Code Version	1.01.07
Boot Code Version	3.12.0
Hardware Version	2000
Serial Num	0000001984
Model Number	F5D7632-4

Lan Settings	
LAN MAC Address	00:aa:bb:cc:dd:ee
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

From the "Connection Type" pull-down list, select "Point-to Point Protocol over ATM (PPPoA)". Enter the PPPoA (Point-to-Point Protocol over ATM) information in the provided spaces, and click "OK" to activate your settings. This information is provided by your ISP.



WAN Connection Wizard

Internet Connection

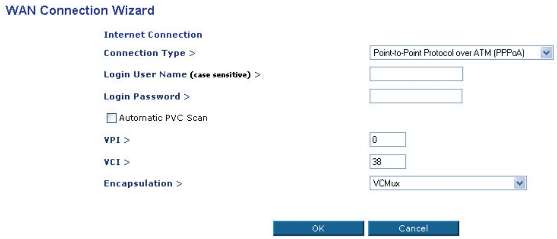
Connection Type > Point-to-Point Protocol over ATM (PPPoA)

Login User Name (case sensitive) >

Login Password >

☑ Automatic PVC Scan

To manually setup your VPI/VCI settings or Encapsulation type, uncheck the "Automatic PVC Scan" checkbox and the following screen will appears. Enter all information in the provided spaces, and click "OK" to activate your settings. This information is provided by your ISP.



WAN Connection Wizard

Internet Connection

Connection Type > Point-to-Point Protocol over ATM (PPPoA)

Login User Name (case sensitive) >

Login Password >

☐ Automatic PVC Scan

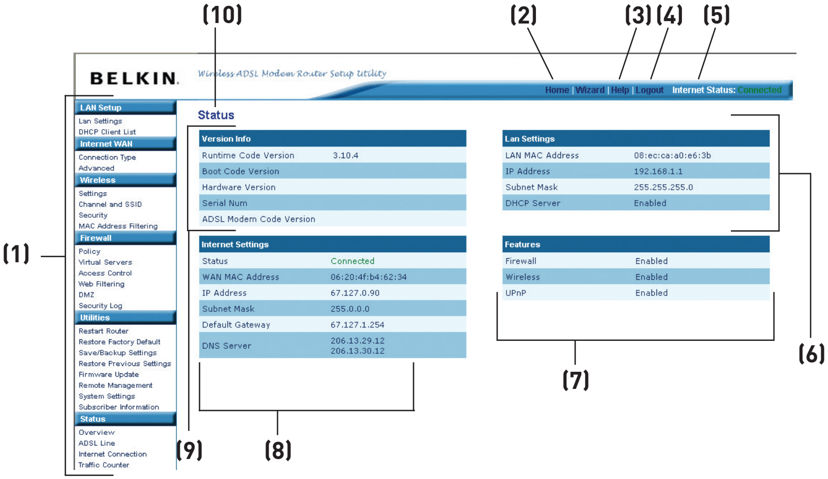
VPI > 0

VCI > 38

Encapsulation > VCMux

Navigating the Web Browser 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.



Status

Version Info	
Runtime Code Version	3.10.4
Boot Code Version	
Hardware Version	
Serial Num	
ADSL Modem Code Version	

Lan Settings	
LAN MAC Address	08:ec:ca:a0:e6:3b
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

Internet Settings	
Status	Connected
WAN MAC Address	06:20:4f:b4:62:34
IP Address	67.127.0.90
Subnet Mask	255.0.0.0
Default Gateway	67.127.1.254
DNS Server	206.13.29.12 206.13.30.12

Features	
Firewall	Enabled
Wireless	Enabled
UPnP	Enabled

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 UPnP, NAT, and firewall 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.

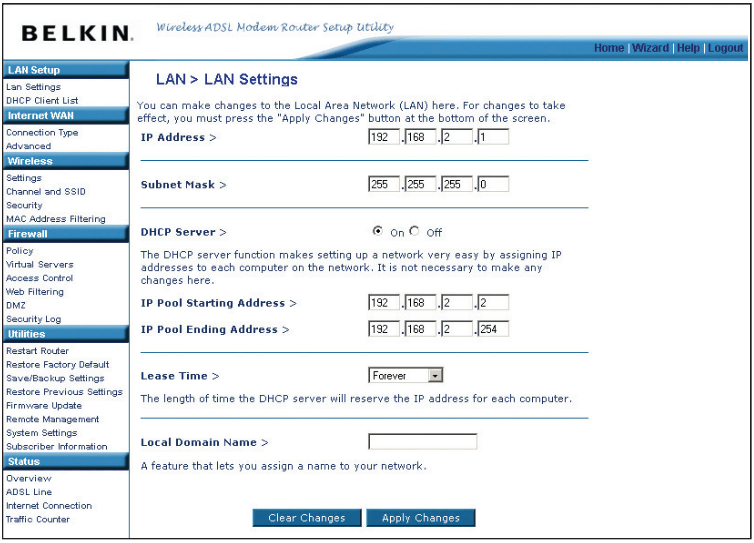
10. **Page Name**

    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



LAN > LAN Settings

You can make changes to the Local Area Network (LAN) here. For changes to take effect, you must press the "Apply Changes" button at the bottom of the screen.

IP Address > 192 .168 .2 .1

Subnet Mask > 255 .255 .255 .0

DHCP Server > ● On ○ Off

The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network. It is not necessary to make any changes here.

IP Pool Starting Address > 192 .168 .2 .2

IP Pool Ending Address > 192 .168 .2 .254

Lease Time > Forever

The length of time the DHCP server will reserve the IP address for each computer.

Local Domain Name >

A feature that lets you assign a name to your network.

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.

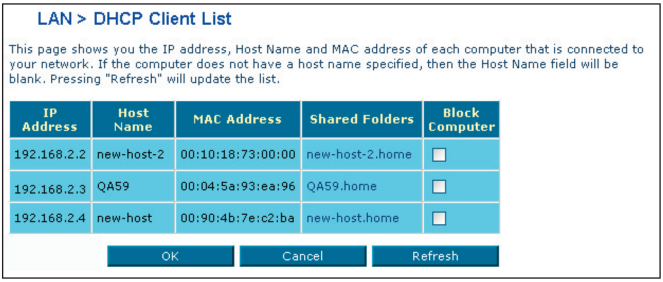
Lease Time

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



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	Shared Folders	Block Computer
192.168.2.2	new-host-2	00:10:18:73:00:00	new-host-2.home	□
192.168.2.3	QA59	00:04:5a:93:ea:96	QA59.home	□
192.168.2.4	new-host	00:90:4b:7e:c2:ba	new-host.home	□

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.

Shared Folders

You can view the shared files and printers by clicking on the host name (name of the computer in your network) below "Shared folders."

Block Computer

You can enable blocking of locally shared files and printers by selecting the "check box" next to the host name (name of the computer in your network) below "Block Computer."

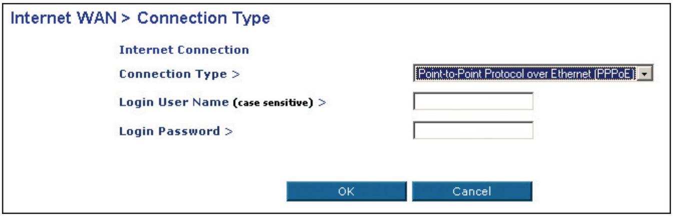
Internet WAN

Connection Type

From the "Connection Type" page, you can select the type of connection you want to use by selecting the "Connection Type" from the pull-down list.

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 "OK" to activate your settings. This information is provided by your ISP.



Internet WAN > Connection Type

Internet Connection

Connection Type > Point-to-Point Protocol over Ethernet (PPPoE)

Login User Name (case sensitive) >

Login Password >

User Name – Enter the ISP assigned user name.

Password – Enter your password (assigned by your ISP).

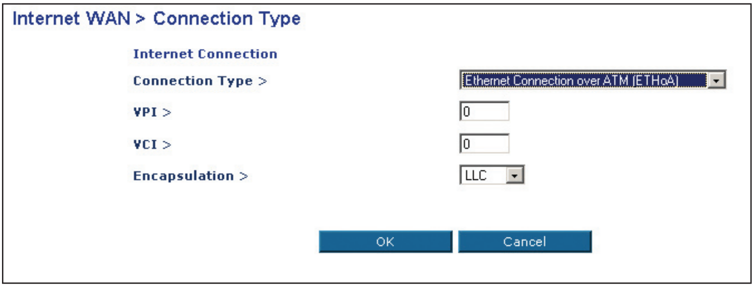
VPI/VCI – Enter your Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) parameter here (assigned by your ISP).

Encapsulation – Select your encapsulation type (supplied by your ISP) to specify how to handle multiple protocols at the ATM transport layer.

LLC – Point-to-Point Protocol over ATM Logical Link Control allows multiple protocols running over one virtual circuit (more overhead).

VC-MUX – Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with fewer overheads.

Setting your ISP Connection Type to Ethernet Connection over ATM (ETHoA)



Internet WAN > Connection Type

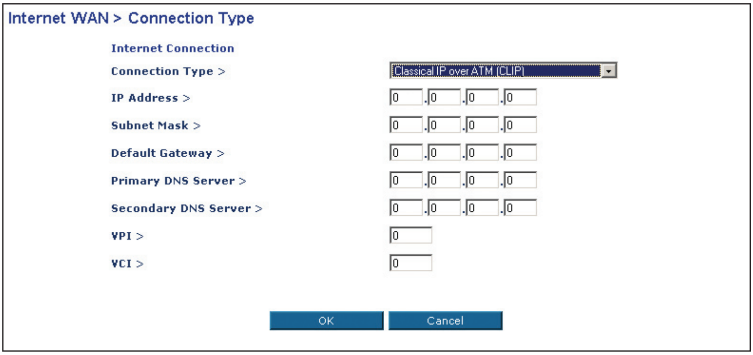
Internet Connection

Connection Type >	Ethernet Connection over ATM (ETHoA)
VPI >	0
VCI >	0
Encapsulation >	LLC

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).

Setting your ISP Connection Type to Classical IP over ATM (CLIP)



Internet WAN > Connection Type

Internet Connection

Connection Type > Classical IP over ATM (CLIP)

IP Address > 0 . 0 . 0 . 0

Subnet Mask > 0 . 0 . 0 . 0

Default Gateway > 0 . 0 . 0 . 0

Primary DNS Server > 0 . 0 . 0 . 0

Secondary DNS Server > 0 . 0 . 0 . 0

VPI > 0

VCI > 0

IP Address – Enter the WAN IP address provided by your ISP.

Subnet Mask – Enter a subnet mask provided by your ISP.

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).

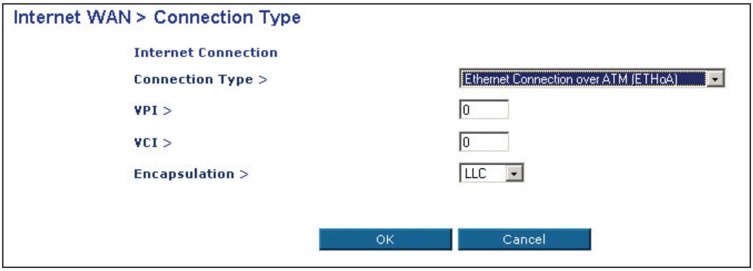
Primary DNS Server – Enter the primary DNS server's IP address provided by your ISP.

Secondary DNS Server – Enter the secondary DNS server's IP address provided by your ISP.

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

Setting your ISP Connection Type to Network Bridging

Enter the VPI/VCI value in the provided spaces. Click "OK" to activate your settings.



Internet WAN > Connection Type

Internet Connection

Connection Type > Ethernet Connection over ATM (ETHoA)

VPI > 0

VCI > 0

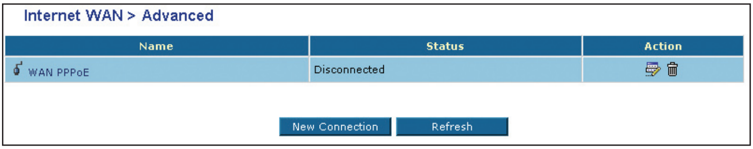
Encapsulation > LLC

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).

Advanced

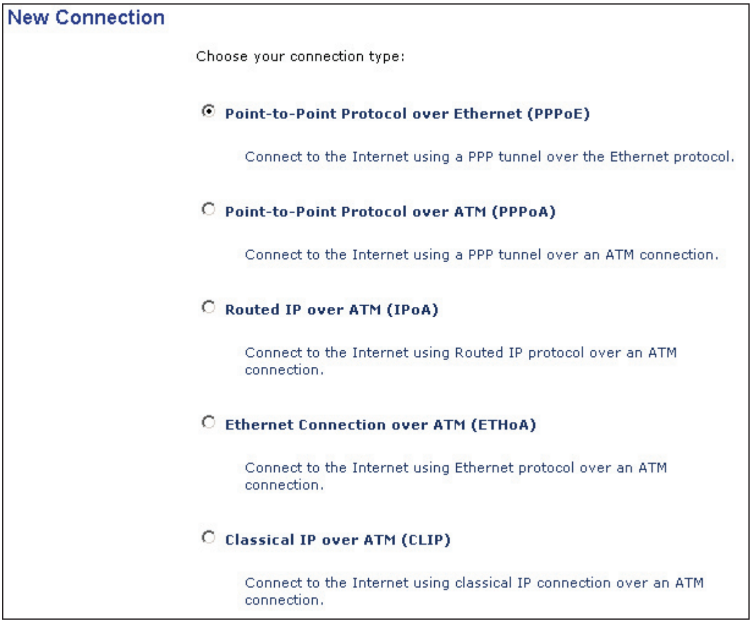
From the “Advanced” page, you can create multiple profiles for your WAN connection. You can create a new connection by clicking the “New Connection” button.



Internet WAN > Advanced

Name	Status	Action
WAN PPPoE	Disconnected	

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



New Connection

Choose your connection type:

● **Point-to-Point Protocol over Ethernet (PPPoE)**

Connect to the Internet using a PPP tunnel over the Ethernet protocol.

○ **Point-to-Point Protocol over ATM (PPPoA)**

Connect to the Internet using a PPP tunnel over an ATM connection.

○ **Routed IP over ATM (IPoA)**

Connect to the Internet using Routed IP protocol over an ATM connection.

○ **Ethernet Connection over ATM (ETHoA)**

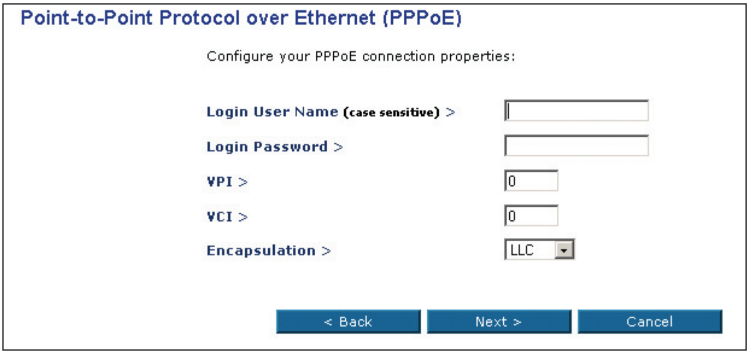
Connect to the Internet using Ethernet protocol over an ATM connection.

○ **Classical IP over ATM (CLIP)**

Connect to the Internet using classical IP connection over an ATM connection.

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”. This information is provided by your ISP.



Point-to-Point Protocol over Ethernet (PPPoE)

Configure your PPPoE connection properties:

Login User Name (case sensitive) >	
Login Password >	
VPI >	0
VCI >	0
Encapsulation >	LLC

Click “Finish” to activate your settings.

User name – Enter the ISP assigned user name.

Password – Enter your password (assigned by your ISP).

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

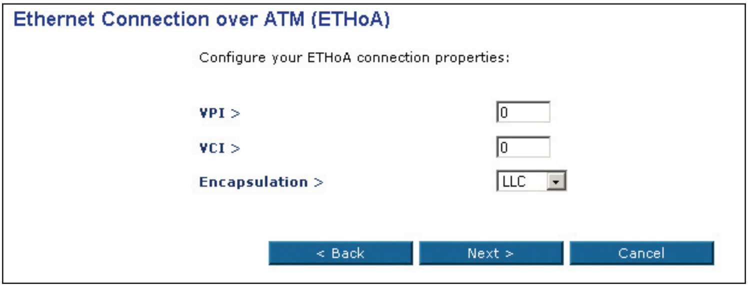
Encapsulation – Select your encapsulation type (supplied by your ISP) to specify how to handle multiple protocols at the ATM transport layer.

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).

Setting your ISP Connection Type to Ethernet Connection over ATM (ETHoA)

Enter (ETHoA) information in the provided spaces, and click “Next”. This information is provided by your ISP.



Ethernet Connection over ATM (ETHoA)

Configure your ETHoA connection properties:

VPI > 0

VCI > 0

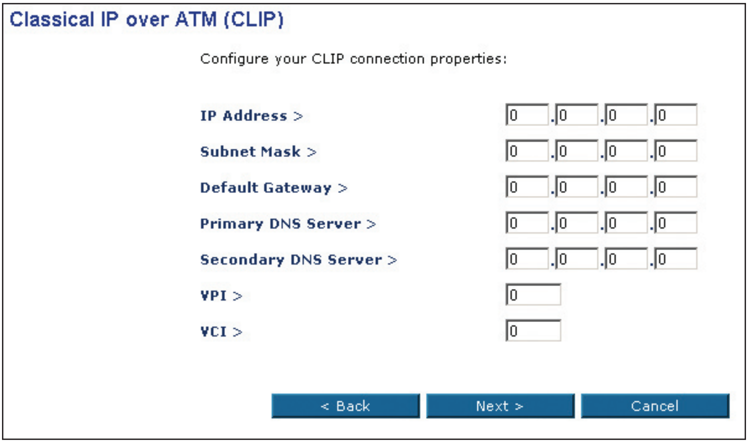
Encapsulation > LLC

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).

Setting your ISP Connection Type to Classical IP over ATM (CLIP)

Enter (CLIP) information in the provided spaces, and click “Next”. This information is provided by your ISP.



Classical IP over ATM (CLIP)

Configure your CLIP connection properties:

IP Address > 0 . 0 . 0 . 0

Subnet Mask > 0 . 0 . 0 . 0

Default Gateway > 0 . 0 . 0 . 0

Primary DNS Server > 0 . 0 . 0 . 0

Secondary DNS Server > 0 . 0 . 0 . 0

VPI > 0

VCI > 0

IP Address – Enter the WAN IP address provided by your ISP.

Subnet Mask – Enter a subnet mask provided by your ISP.

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).

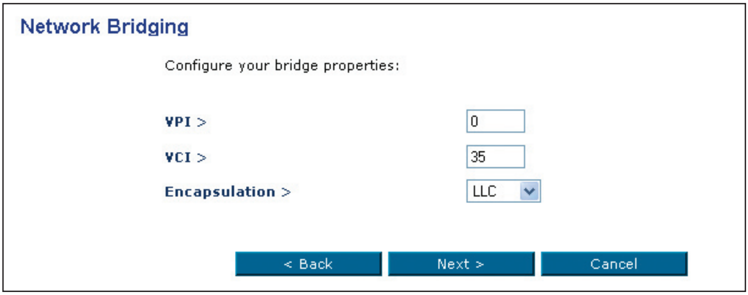
Primary DNS Server – Enter the primary DNS server's IP address provided by your ISP.

Secondary DNS Server – Enter the secondary DNS server's IP address provided by your ISP.

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

Setting your ISP Connection Type to Network Bridging

Enter the VPI/VCI value in the provided spaces, and then click "Next". This information is provided by your ISP.



Network Bridging

Configure your bridge properties:

VPI > 0

VCI > 35

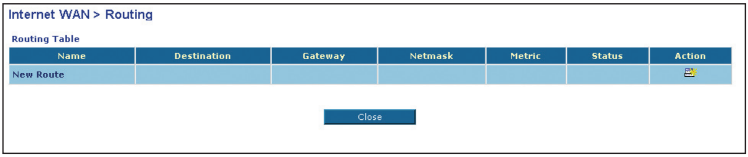
Encapsulation > LLC

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).

Routing

From the "Routing" page, you can add, edit, and delete routing rules from the routing table. You can create a new route by clicking the "New Route" button.

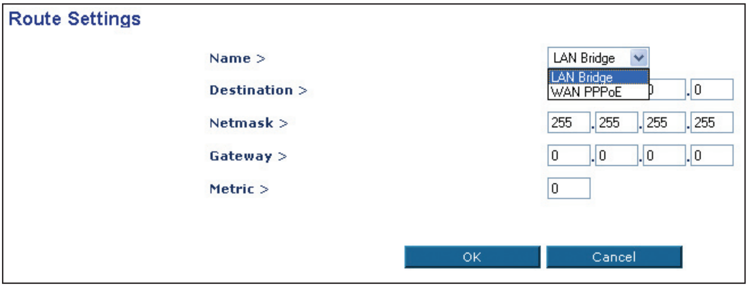


Internet WAN > Routing

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

Enter all the necessary information and click "OK" to add this new route.



Route Settings

Name > LAN Bridge (LAN Bridge / WAN PPPoE)

Destination > 0 . 0 . 0 . 0

Netmask > 255 . 255 . 255 . 255

Gateway > 0 . 0 . 0 . 0

Metric > 0

Name – Select the network device.

Destination – The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.

Netmask – The network mask is used in conjunction with the destination to determine when a route is used.

Gateway – Enter the gateway's IP address.

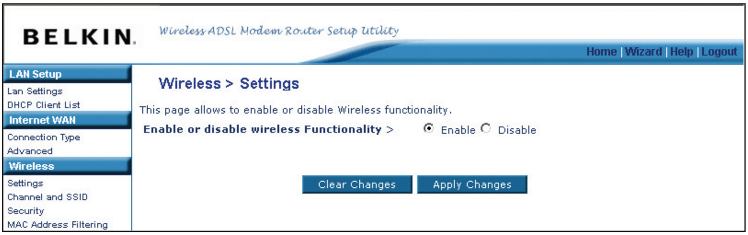
Metric – A measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.

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.

Settings

The "Settings" page allows you to enable and disable your wireless functionality.



Wireless > Settings

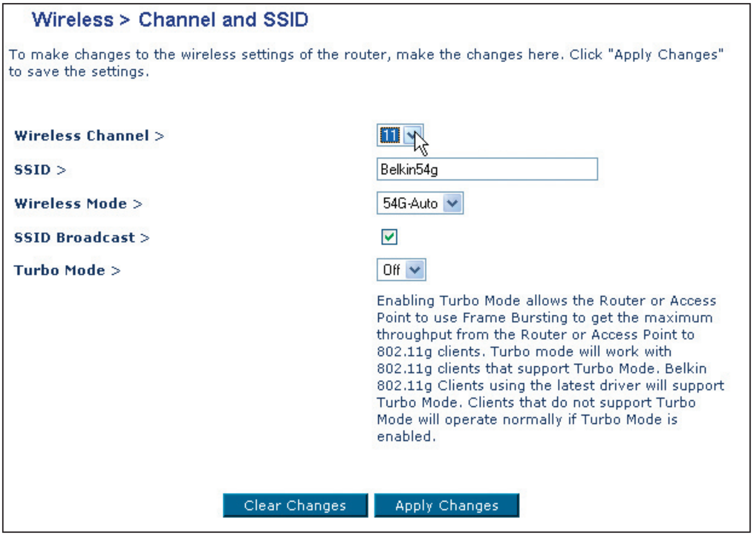
This page allows to enable or disable Wireless functionality.

Enable or disable wireless Functionality > ● Enable ○ Disable

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 requirements. Your Router is configured to operate on the proper channels for the country you reside in. 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.



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.

Wireless Channel > 11

SSID > Belkin54g

Wireless Mode > 54G-Auto

SSID Broadcast > ☑

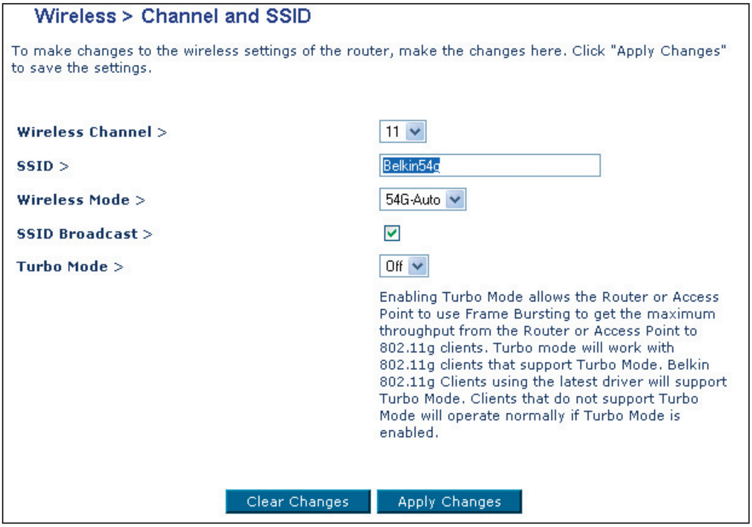
Turbo Mode > Off

Enabling Turbo Mode allows the Router or Access Point to use Frame Bursting to get the maximum throughput from the Router or Access Point to 802.11g clients. Turbo mode will work with 802.11g clients that support Turbo Mode. Belkin 802.11g Clients using the latest driver will support Turbo Mode. Clients that do not support Turbo Mode will operate normally if Turbo Mode is enabled.

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.



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.

Wireless Channel > 11

SSID > Belkin54g

Wireless Mode > 54G-Auto

SSID Broadcast > ☑

Turbo Mode > Off

Enabling Turbo Mode allows the Router or Access Point to use Frame Bursting to get the maximum throughput from the Router or Access Point to 802.11g clients. Turbo mode will work with 802.11g clients that support Turbo Mode. Belkin 802.11g Clients using the latest driver will support Turbo Mode. Clients that do not support Turbo Mode will operate normally if Turbo Mode is enabled.

Refer to the documentation of your wireless network adapter for information on making this change.

Using the Wireless Mode Switch

Your Router can operate in three different wireless modes: “54G-Auto”, “54G-Only”, and “54G-LRS”. The different modes are explained below.

- **54G-Auto –** 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.
- **54G-Only –** 54g 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”.

- **54G-LRS –** 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 54G-LRS only mode will decrease 802.11g performance to 11Mbps.

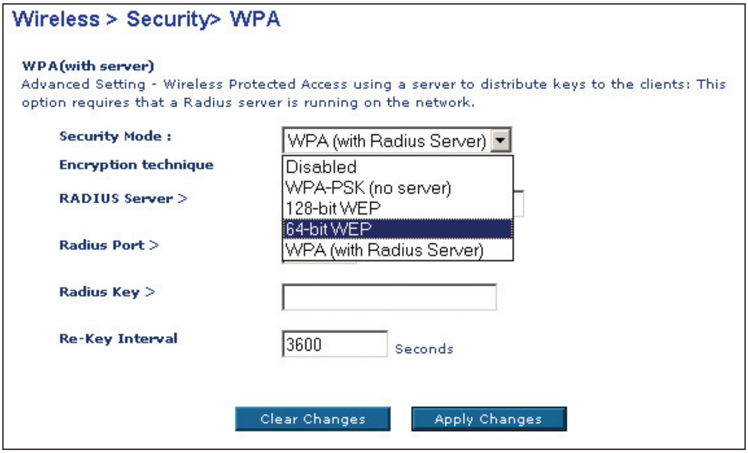
Security

Changing the Wireless Security Settings

Your Router is equipped with the latest security standard called WPA (Wi-Fi Protected Access). It also supports the legacy security standard called WEP (Wired Equivalent Privacy). By default, 64-bit WEP wireless security is enabled. To access the security settings, click “Security” on the “Wireless” tab.

Setting WEP Encryption

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



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

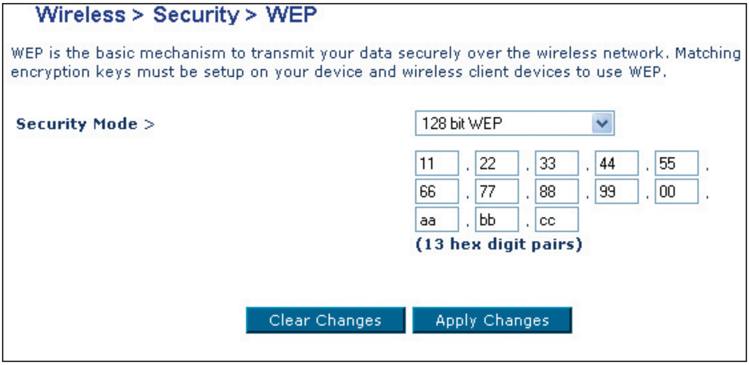
RADIUS Server >

Radius Port >

Radius Key >

Re-Key Interval 3600 Seconds

2. After selecting your WEP encryption mode, you can enter your WEP key manually by typing in the HEX WEP key. Click “Apply Changes” to finish.



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 and wireless client devices to use WEP.

Security Mode > 128 bit WEP

11 . 22 . 33 . 44 . 55 .
66 . 77 . 88 . 99 . 00 .
aa . bb . cc

(13 hex digit pairs)

Hex (Hexadecimal) Key

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

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

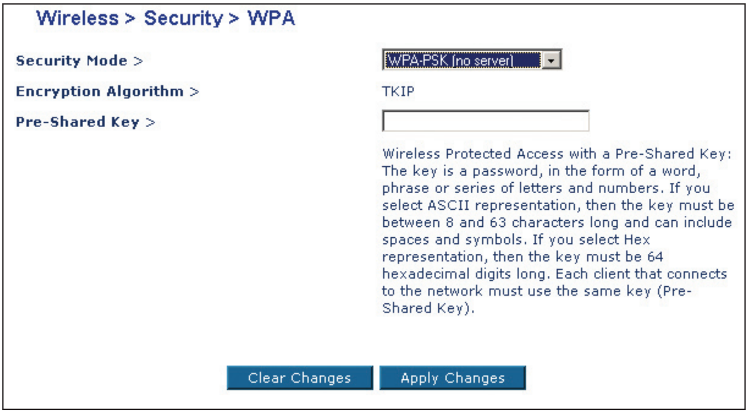
Setting WPA Security

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 was available for free download. This patch works only with Windows XP. You also need to download the latest driver for your Belkin 802.11g CardBus Card from Belkin’s support site. Other operating systems are not supported at this time. Only Belkin 802.11g clients support WPA at this time.

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 eight 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)

From the “Security Mode” drop-down menu, select “WPA-PSK (no server)”. Enter your pre-shared key. This can be from eight 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. Click “Apply Changes” to finish. You must now set up all clients to match these settings.



Wireless > Security > WPA

Security Mode > WPA-PSK (no server)

Encryption Algorithm > TKIP

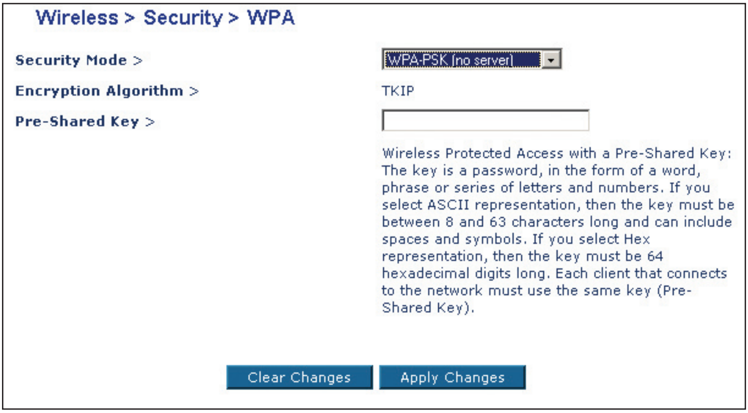
Pre-Shared Key >

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. If you select ASCII representation, then the key must be between 8 and 63 characters long and can include spaces and symbols. If you select Hex representation, then the key must be 64 hexadecimal digits long. Each client that connects to the network must use the same key (Pre-Shared Key).

Setting WPA (with server) Settings

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

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



Wireless > Security > WPA

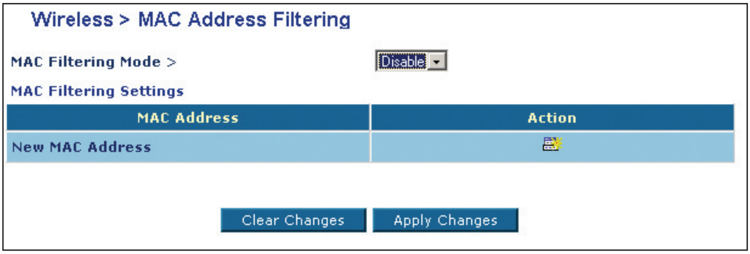
Security Mode >	WPA-PSK (no server)
Encryption Algorithm >	TKIP
Pre-Shared Key >	

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. If you select ASCII representation, then the key must be between 8 and 63 characters long and can include spaces and symbols. If you select Hex representation, then the key must be 64 hexadecimal digits long. Each client that connects to the network must use the same key (Pre-Shared Key).

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.

1. From the "MAC Address Filtering" screen, click "New MAC Address".



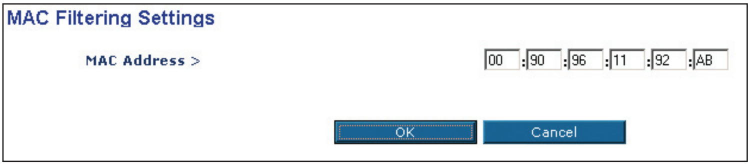
Wireless > MAC Address Filtering

MAC Filtering Mode > Disable

MAC Filtering Settings

MAC Address	Action
New MAC Address	

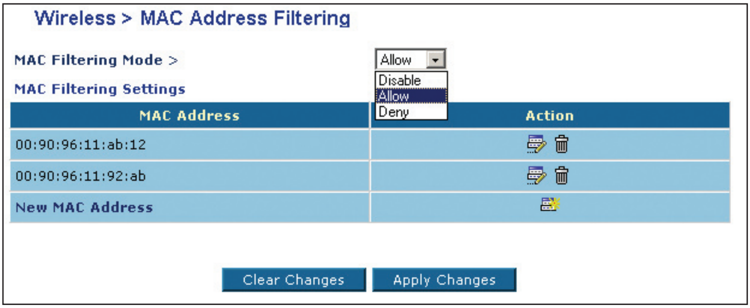
2. Enter the MAC address of your computer and click "OK".



MAC Filtering Settings

MAC Address > 00 :90 :96 :11 :92 :AB

3. From the pull-down menu, select "Allow" to allow access to only the computers with the MAC addresses in the list or select "Deny" to deny access to only the computers with the MAC addresses in the list.



Wireless > MAC Address Filtering

MAC Filtering Mode > Allow

MAC Filtering Settings

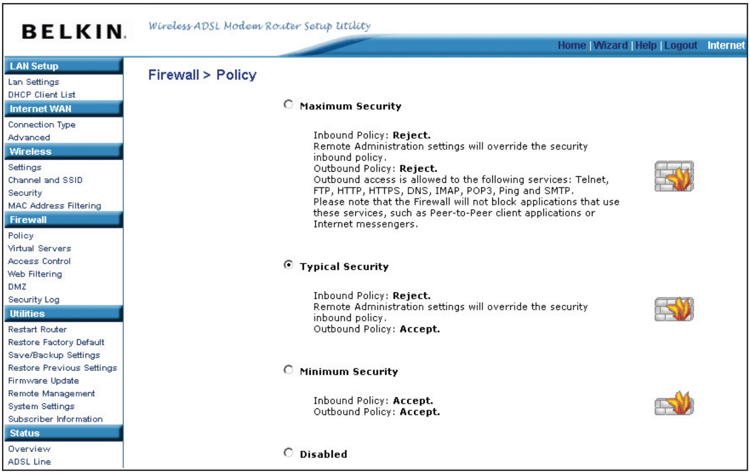
MAC Address	Action
00:90:96:11:ab:12	
00:90:96:11:92:ab	
New MAC Address	

Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks. The firewall also masks common ports that are frequently used to attack networks. These ports appear to be "Stealth", meaning that for all intents and purposes they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.

Policy

This page lets the user set the firewall security level. You may choose from four pre-defined security levels: Maximum, Typical (default setting), Minimum, and Disabled.



Firewall > Policy

○ **Maximum Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, Ping and SMTP.
Please note that the Firewall will not block applications that use these services, such as Peer-to-Peer client applications or Internet messengers.

● **Typical Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

○ **Minimum Security**

Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

○ **Disabled**

Maximum Security – This option will provide the user with maximum security, but it might also block uncommon applications such as online gaming. By selecting this option, the Router will reject all inbound traffic from the Internet except remote administration connections. It will also reject most outbound traffic to the Internet except common applications such as Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, Ping, and SMTP.

Typical Security – By selecting this option, the Router will reject all inbound traffic from the Internet except remote administration connections but it will allow all outbound traffic to the Internet, except as configured in the "Access Control" screen.

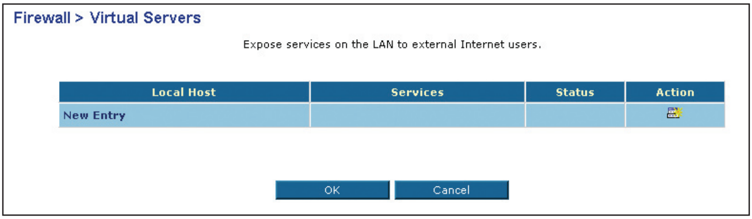
Minimum Security – By selecting this option, the Router will permit all inbound traffic from the Internet. It will also allow all outbound traffic to the Internet, except as configured in the "Access Control" screen.

Disable – By selecting this option, the firewall will be disabled.

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.

1. Click "New Entry" to add an internal computer to the "Virtual Server" list.

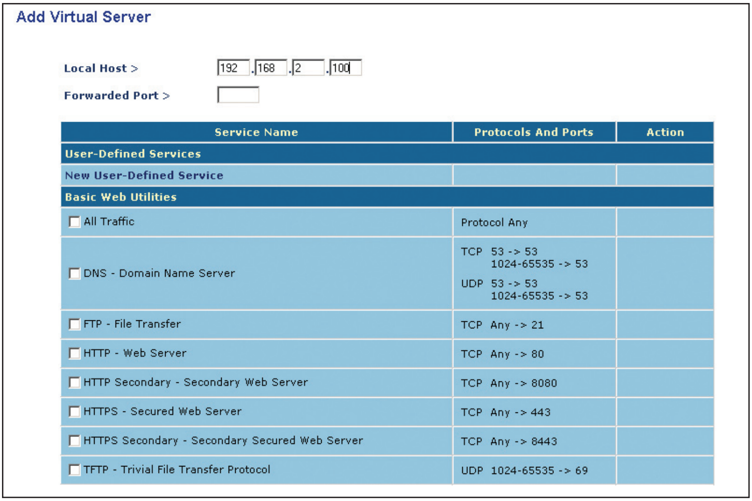


Firewall > Virtual Servers

Expose services on the LAN to external Internet users.

Local Host	Services	Status	Action
New Entry			

2. Enter the LAN IP address in the space provided for the “Local Host”. Select the service that you want in the check box and click “OK” to save your settings.



Add Virtual Server

Local Host > 192 . 168 . 2 . 100

Forwarded Port >

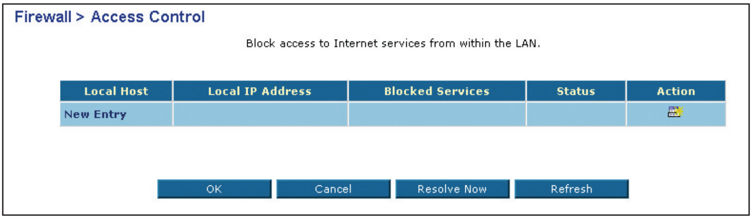
Service Name	Protocols And Ports	Action
User-Defined Services		
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	Protocol Any	
□ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
□ FTP - File Transfer	TCP Any -> 21	
□ HTTP - Web Server	TCP Any -> 80	
□ HTTP Secondary - Secondary Web Server	TCP Any -> 8080	
□ HTTPS - Secured Web Server	TCP Any -> 443	
□ HTTPS Secondary - Secondary Secured Web Server	TCP Any -> 8443	
□ TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	

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.

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 “New Entry” on the “Access Control” screen.

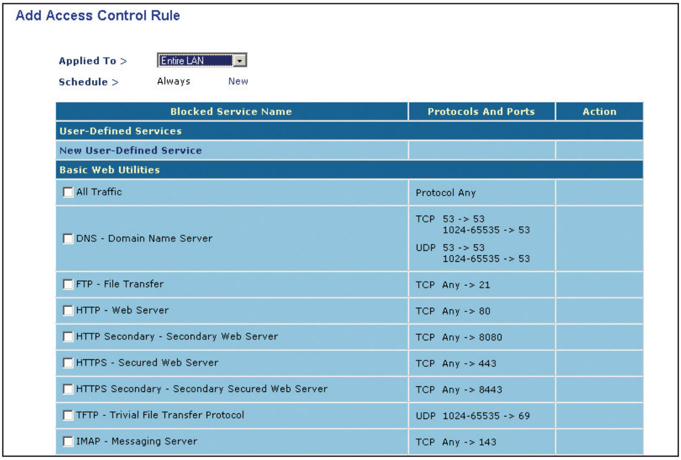


Firewall > Access Control

Block access to Internet services from within the LAN.

Local Host	Local IP Address	Blocked Services	Status	Action
New Entry				✎

2. Select the name of the internal computer from the “Applied To” pull-down list. Select the service that you want in the check box and click “OK” to save your settings.



Add Access Control Rule

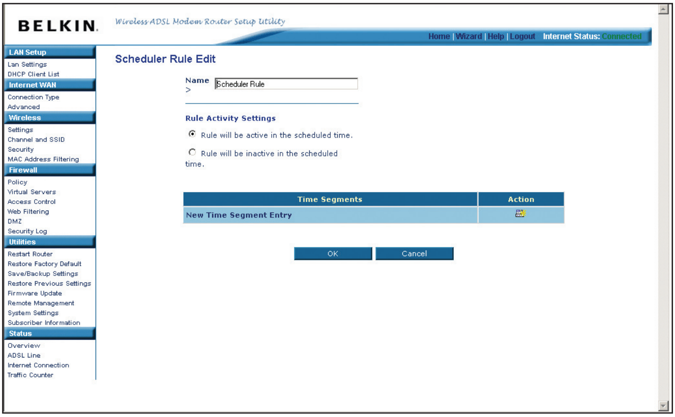
Applied To > Entire LAN ▾

Schedule > Always New

Blocked Service Name	Protocols And Ports	Action
User-Defined Services		
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	Protocol Any	
□ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
□ FTP - File Transfer	TCP Any -> 21	
□ HTTP - Web Server	TCP Any -> 80	
□ HTTP Secondary - Secondary Web Server	TCP Any -> 8080	
□ HTTPS - Secured Web Server	TCP Any -> 443	
□ HTTPS Secondary - Secondary Secured Web Server	TCP Any -> 8443	
□ TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	
□ IMAP - Messaging Server	TCP Any -> 143	

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. To configure the access control for a specific time, do the following:

1. From the previous screen, click "New" and you will see the following screen. Enter a name for this schedule and click "New Time Segment Entry".



Scheduler Rule Edit

Name > Scheduler Rule

Rule Activity Settings

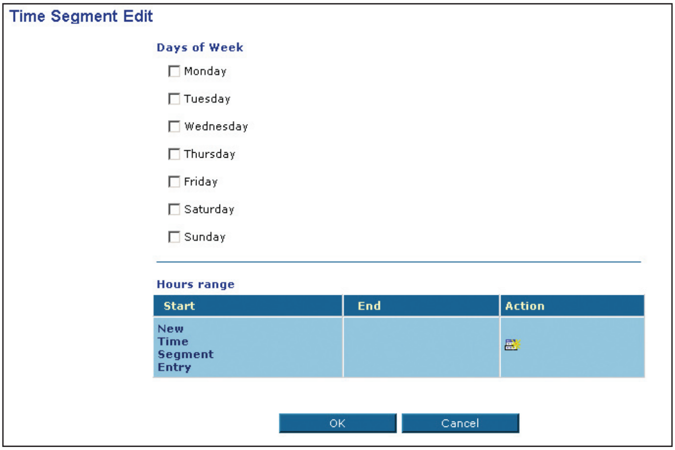
● Rule will be active in the scheduled time.

○ Rule will be inactive in the scheduled time.

Time Segments	Action
New Time Segment Entry	

OK Cancel

2. Select the days of the week that you want to apply the setting and click "New Time Segment Entry".



Time Segment Edit

Days of Week

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

□ Saturday

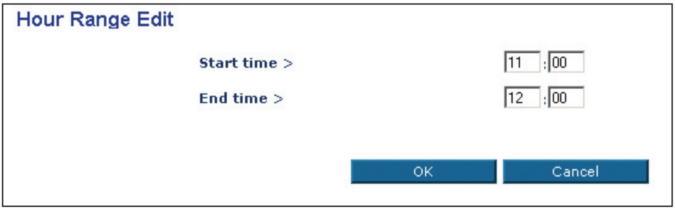
□ Sunday

Hours range

Start	End	Action
New Time Segment Entry		

OK Cancel

3. Enter the start time and end time you want to apply the setting and click “OK”.



Hour Range Edit

Start time > 11 : 00

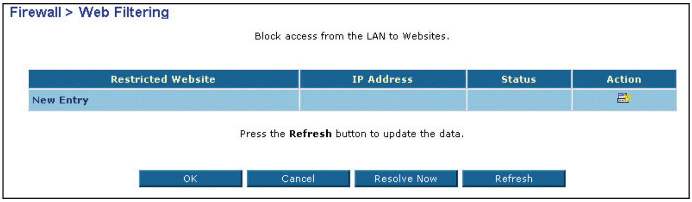
End time > 12 : 00

4. Click “OK” and then click “OK” to save your settings.

Web Filtering

The web-filtering feature will allow you to specify which websites are not allowed to be viewed from the local computer. Any computer attempting to access the website that’s restricted will be denied.

1. Click “New Entry”.



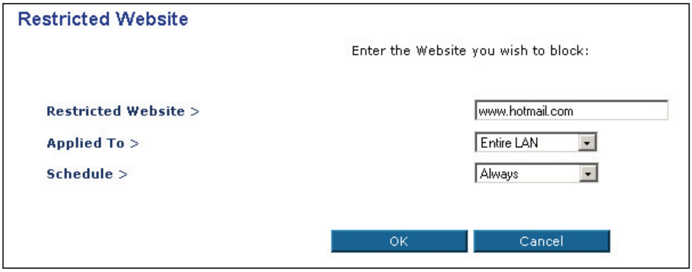
Firewall > Web Filtering

Block access from the LAN to Websites.

Restricted Website	IP Address	Status	Action
New Entry			

Press the **Refresh** button to update the data.

2. To configure the web-filtering feature, specify the websites (www.websitename.com) you want to filter on your network. Enter the “Restricted Website” address and select the computer name you want to block from the “Applied To” list. Click “OK” to save your settings.



Restricted Website

Enter the Website you wish to block:

Restricted Website > www.hotmail.com

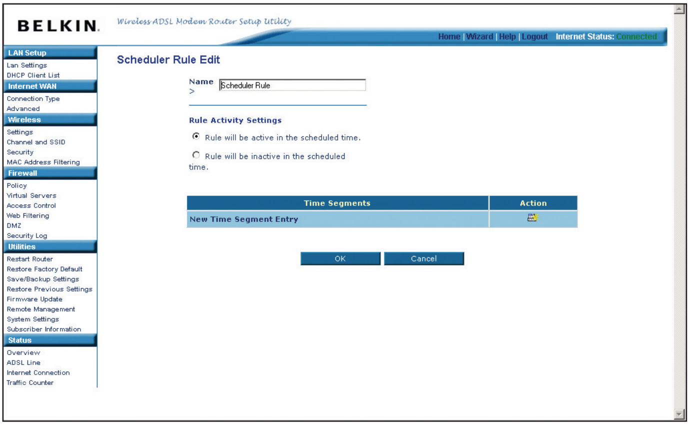
Applied To > Entire LAN

Schedule > Always

Schedule Rule

You may filter website access for local clients based on rules. Each web filter rule may be activated at a scheduled time. To configure the access control for a specific time, do the following:

1. From the previous screen, click "New" and you will see the following screen. Enter a name for this schedule and click "New Time Segment Entry".



Scheduler Rule Edit

Name > Scheduler Rule

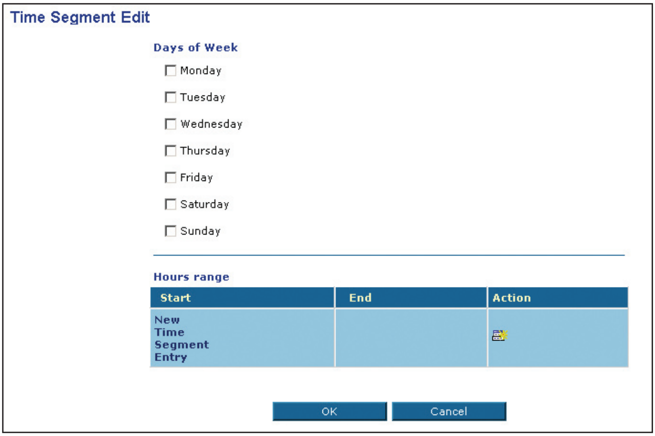
Rule Activity Settings

● Rule will be active in the scheduled time.

○ Rule will be inactive in the scheduled time.

Time Segments	Action
New Time Segment Entry	

2. Select the days of the week that you want to apply the setting and click "New Time Segment Entry".



Time Segment Edit

Days of Week

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

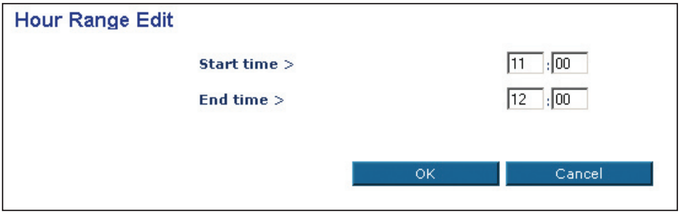
□ Saturday

□ Sunday

Hours range

Start	End	Action
New Time Segment Entry		

3. Enter the start time and end time you want to apply the setting and click "OK".



Hour Range Edit

Start time > 11 : 00

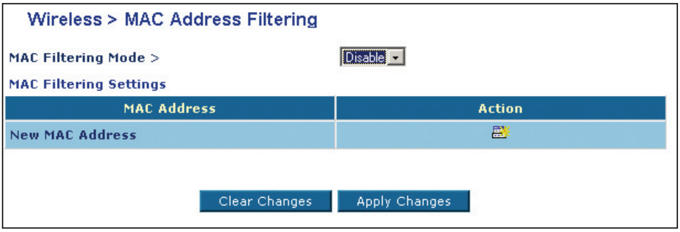
End time > 12 : 00

4. Click "OK" and then click "OK" to save your settings.

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.

1. Click "New MAC Address".



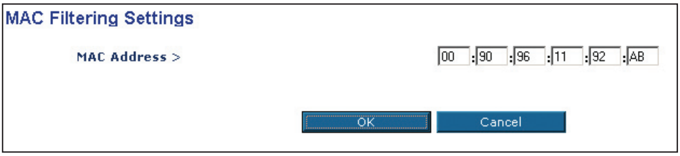
Wireless > MAC Address Filtering

MAC Filtering Mode > Disable

MAC Filtering Settings

MAC Address	Action
New MAC Address	

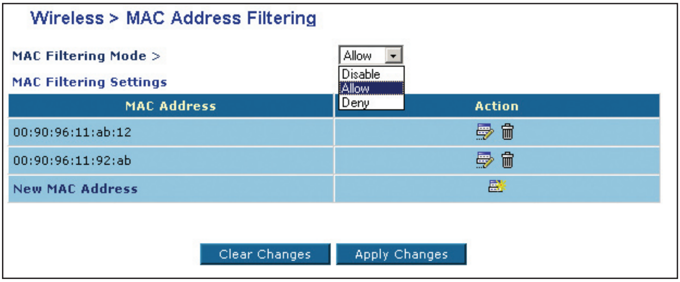
2. Enter the MAC address of the computer that will be allowed access to the network and click "OK".



MAC Filtering Settings

MAC Address > 00 : 90 : 96 : 11 : 92 : AB

3. From the “MAC Filtering Mode” pull-down list, select “Allow” and “Apply Changes” to save your settings.



Wireless > MAC Address Filtering

MAC Filtering Mode > Allow

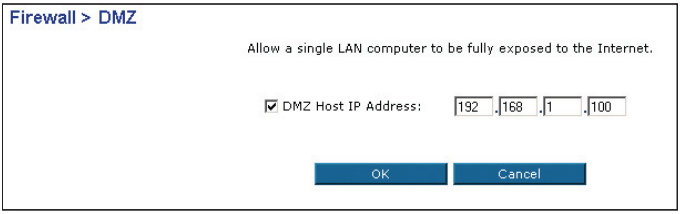
MAC Filtering Settings

MAC Address	Action
00:90:96:11:ab:12	
00:90:96:11:92:ab	
New MAC Address	

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.**

To put a computer in the DMZ, select the “DMZ Host IP Address” check box. Enter the LAN IP address in the “DMZ Host IP Address” field and click “OK” for the change to take effect.



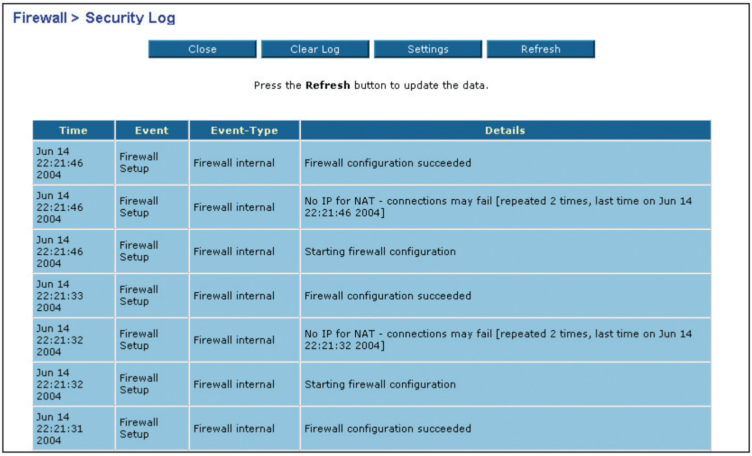
Firewall > DMZ

Allow a single LAN computer to be fully exposed to the Internet.

☑ DMZ Host IP Address: 192 . 168 . 1 . 100

Security Log

As shown in the web page, you can view the system log and configure the system log settings if needed.



Press the **Refresh** button to update the data.

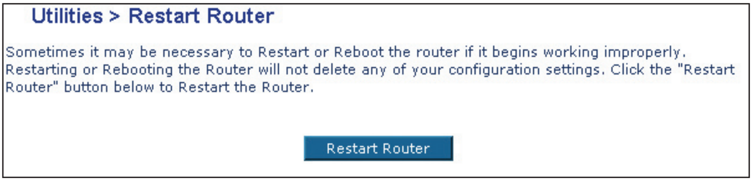
Time	Event	Event-Type	Details
Jun 14 22:21:46 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 22:21:46 2004	Firewall Setup	Firewall internal	No IP for NAT - connections may fail [repeated 2 times, last time on Jun 14 22:21:46 2004]
Jun 14 22:21:46 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 14 22:21:33 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 22:21:32 2004	Firewall Setup	Firewall internal	No IP for NAT - connections may fail [repeated 2 times, last time on Jun 14 22:21:32 2004]
Jun 14 22:21:32 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 14 22:21:31 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded

Utilities

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

Restart Router

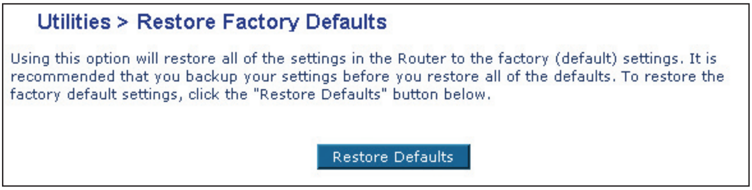
Clicking the "Restart Router" button will restart the Router immediately.



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.

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.



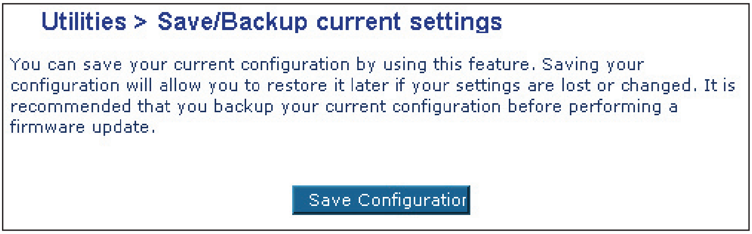
Utilities > Restore Factory Defaults

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Restore Defaults" button below.

Clicking the “Restore Defaults” button will restore all of the settings in the Router to the factory (default) settings immediately.

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.



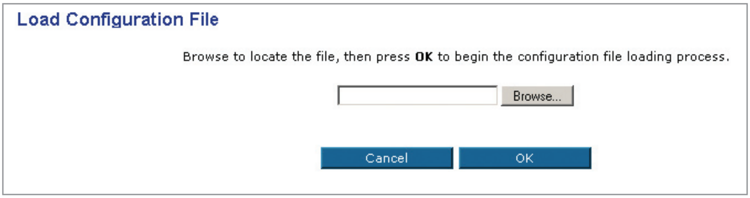
Utilities > Save/Backup current settings

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.

1. Click “Save Configuration”. A window called “File Download” will open.
2. Click “Save”. 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”.
3. When the save is complete, click “Close”. The configuration is now saved.

Restore Previous Settings

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



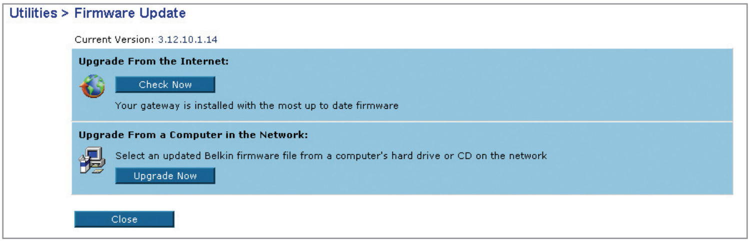
Load Configuration File

Browse to locate the file, then press **OK** to begin the configuration file loading process.

1. Click "Browse". A window will open that allows you to select the location of the configuration file. All configuration files end with a ".conf". Locate the configuration file you want to restore and double-click on it.
2. Click "OK" then "OK" again to restore.

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.



Utilities > Firmware Update

Current Version: 3.12.10.1.14

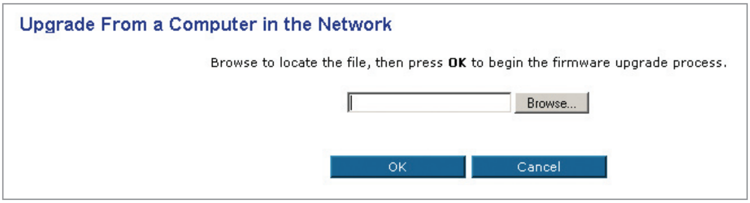
Upgrade From the Internet:

Your gateway is installed with the most up to date firmware

Upgrade From a Computer in the Network:

Select an updated Belkin firmware file from a computer's hard drive or CD on the network

To manually upgrade the firmware from a file on your hardware or CD, click "Upgrade Now".



Upgrade From a Computer in the Network

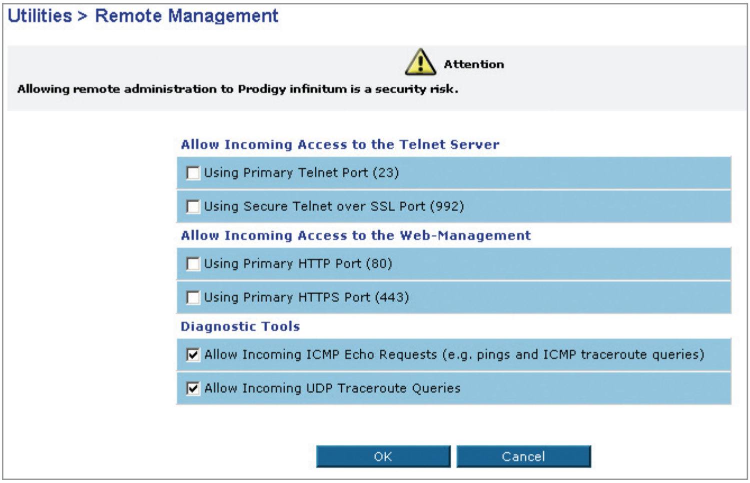
Browse to locate the file, then press **OK** to begin the firmware upgrade process.

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 "OK" to upgrade to the latest firmware version.

Remote Management

Remote management allows you to make changes to your Router's settings from anywhere on the Internet. 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.



Utilities > Remote Management

Attention

Allowing remote administration to Prodigy infinitum is a security risk.

Allow Incoming Access to the Telnet Server

□ Using Primary Telnet Port (23)

□ Using Secure Telnet over SSL Port (992)

Allow Incoming Access to the Web-Management

□ Using Primary HTTP Port (80)

□ Using Primary HTTPS Port (443)

Diagnostic Tools

☑ Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)

☑ Allow Incoming UDP Traceroute Queries

Using Primary Telnet Port (23): Choose this box if you want to have remote management through telnet.

Using Secure Telnet over SSL Port (992): Choose this box if you want to have remote management through secure telnet.

Using Primary HTTP Port (80): Choose this box if you want to have remote access through a web browser.

Using Primary HTTPS Port (443): Choose this box if you want to have remote access through a secure web browser.

Allow Incoming ICMP Echo Requests: Choose this box if you want to allow ping or traceroute commands under DOS prompt.

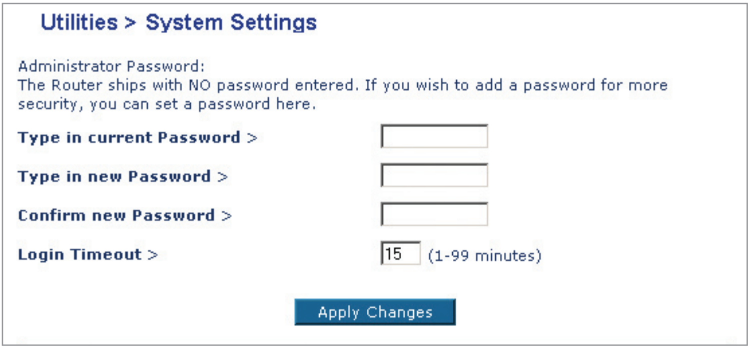
Allow Incoming UDP Traceroute Queries: Choose this box if you want to allow UDP traceroute requests.

System Settings

The "System Settings" page is where you can enter a new administrator password, set the time zone, 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.



Utilities > System Settings

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

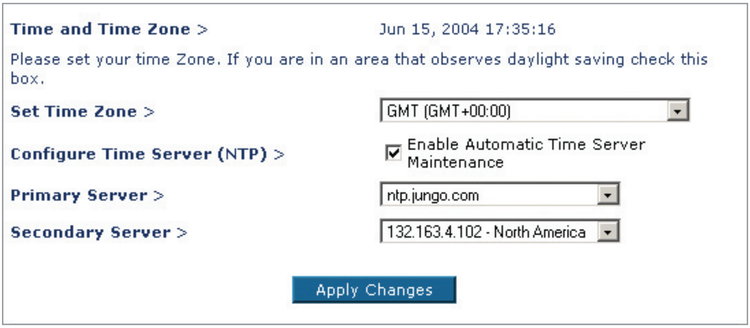
Type in current Password >	
Type in new Password >	
Confirm new Password >	
Login Timeout >	15 (1-99 minutes)

Changing the Login Time-Out Setting

The login time-out option allows you to set the period of time that you can be logged into the Router's advanced setup interface. The timer starts when there has been no activity. For example, 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 three minutes, then three minutes after you leave, the login session will expire. You will have to log into the Router again to make any more changes.

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 time servers on the Internet and get a response. You cannot set the clock yourself.



Time and Time Zone > Jun 15, 2004 17:35:16

Please set your time Zone. If you are in an area that observes daylight saving check this box.

Set Time Zone > GMT (GMT+00:00)

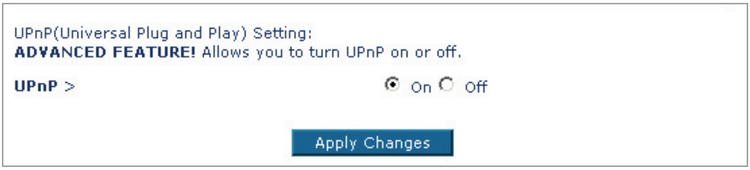
Configure Time Server (NTP) > ☑ Enable Automatic Time Server Maintenance

Primary Server > ntp.jungo.com

Secondary Server > 132.163.4.102 - North America

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. 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.



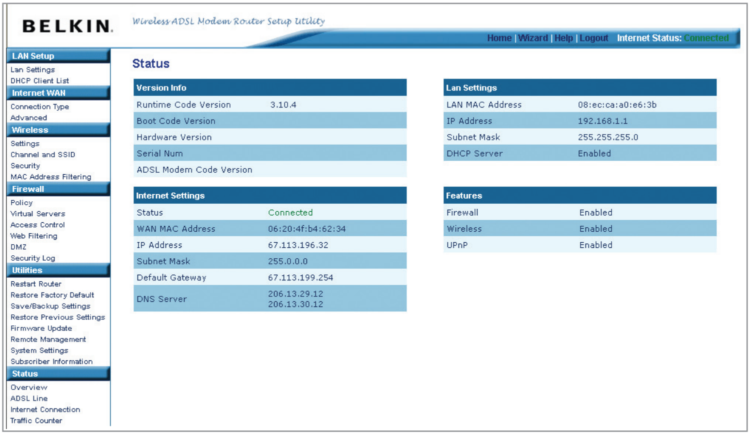
UPnP(Universal Plug and Play) Setting:
ADVANCED FEATURE! Allows you to turn UPnP on or off.

UPnP > ● On ○ Off

Status

Overview

This page shows the current status for the ADSL connection.



Status

Version Info	
Runtime Code Version	3.10.4
Boot Code Version	
Hardware Version	
Serial Num	
ADSL Modem Code Version	

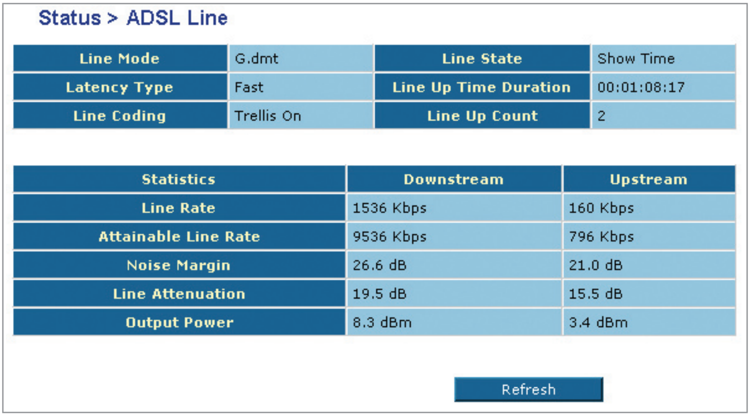
Lan Settings	
LAN MAC Address	08:ec:ca:a0:e6:3b
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

Internet Settings	
Status	Connected
WAN MAC Address	06:20:4f:b4:62:34
IP Address	67.113.196.32
Subnet Mask	255.0.0.0
Default Gateway	67.113.199.254
DNS Server	206.13.29.12 206.13.30.12

Features	
Firewall	Enabled
Wireless	Enabled
UPnP	Enabled

ADSL Line

This page shows all information for the ADSL line.

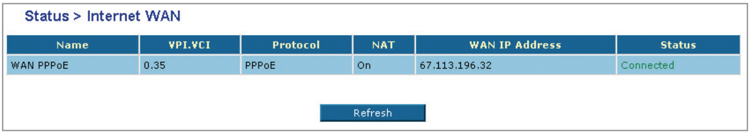

Status > ADSL Line

Line Mode	G.dmt	Line State	Show Time
Latency Type	Fast	Line Up Time Duration	00:01:08:17
Line Coding	Trellis On	Line Up Count	2

Statistics	Downstream	Upstream
Line Rate	1536 Kbps	160 Kbps
Attainable Line Rate	9536 Kbps	796 Kbps
Noise Margin	26.6 dB	21.0 dB
Line Attenuation	19.5 dB	15.5 dB
Output Power	8.3 dBm	3.4 dBm

Internet Connection

This page displays the connection information for your Router, such as name, VPI/VCI settings, protocol, NAT, WAN IP address, and connection status.

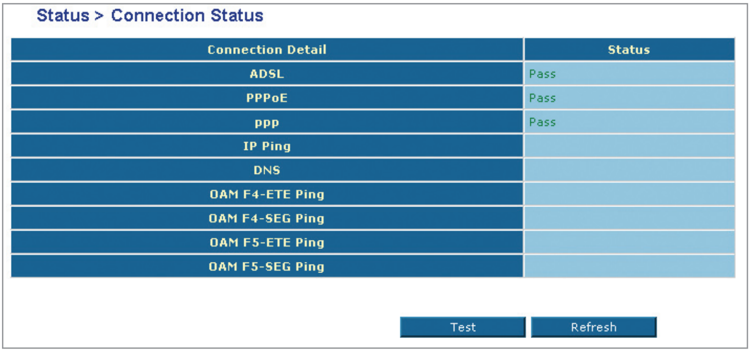


Status > Internet WAN

Name	VPI.VCI	Protocol	NAT	WAN IP Address	Status
WAN PPPoE	0.35	PPPoE	On	67.113.196.32	Connected

Connection Status

This page can test the Internet connection from your Router. To begin the test, click "Test".

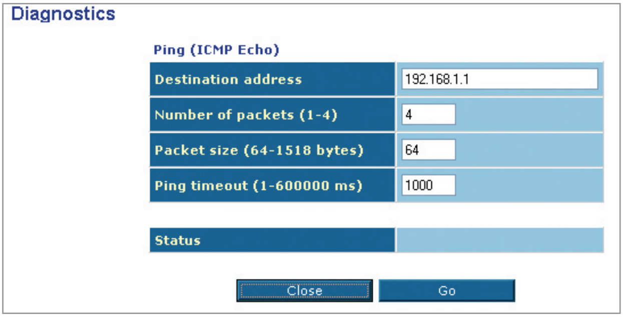


Status > Connection Status

Connection Detail	Status
ADSL	Pass
PPPoE	Pass
PPP	Pass
IP Ping	
DNS	
OAM F4-ETE Ping	
OAM F4-SEG Ping	
OAM F5-ETE Ping	
OAM F5-SEG Ping	

Ping Test

Ping test can provide a basic test of whether a particular host is operating properly and is reachable on the network from the testing host. Enter all the necessary information and click "Go" to begin the test.



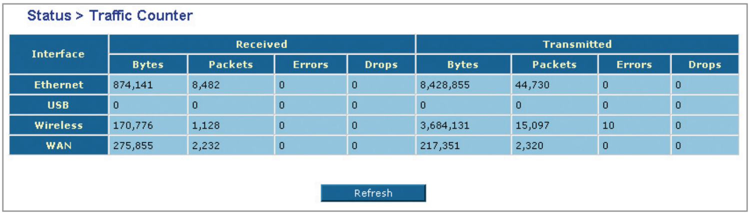
Diagnostics

Ping (ICMP Echo)

Destination address	192.168.1.1
Number of packets (1-4)	4
Packet size (64-1518 bytes)	64
Ping timeout (1-600000 ms)	1000
Status	

Traffic Counter

This table shows the records of data going through the LAN and WAN interface. For each interface, cumulative totals are displayed for "Sent/ Received Packets" and "Sent/Received Bytes".



Status > Traffic Counter

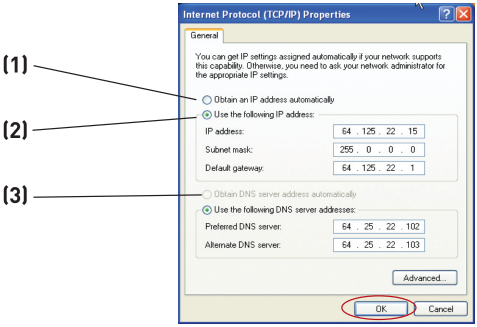
Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
Ethernet	874,141	8,482	0	0	8,428,855	44,730	0	0
USB	0	0	0	0	0	0	0	0
Wireless	170,776	1,128	0	0	3,684,131	15,097	10	0
WAN	275,855	2,232	0	0	217,351	2,320	0	0

In order for your computer to properly communicate with your Router, you will need to change your computer's "TCP/IP Ethernet" settings to "Obtain an IP address automatically/Using DHCP". This is normally the default setting in most home computers.

You can 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 Adapters in Windows XP, 2000, or NT

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:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

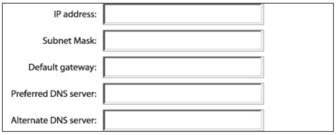
○ Obtain an IP address automatically
● Use the following IP address:

IP address: 64 . 125 . 22 . 15
Subnet mask: 255 . 0 . 0 . 0
Default gateway: 64 . 125 . 22 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 64 . 25 . 22 . 102
Alternate DNS server: 64 . 25 . 22 . 103

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



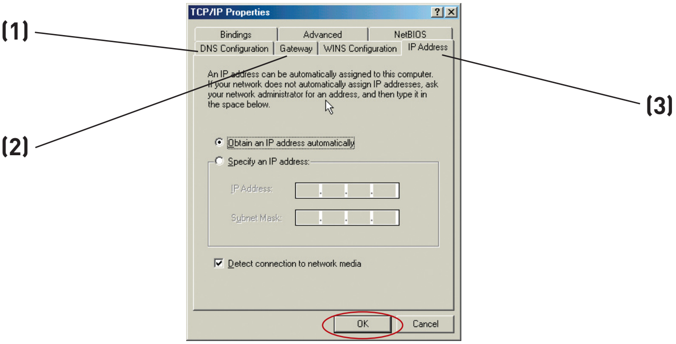
IP address: ____________
Subnet Mask: ____________
Default gateway: ____________
Preferred DNS server: ____________
Alternate DNS server: ____________

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

Your network adapter(s) are now configured for use with the Router.

Manually Configuring Network Adapters in Windows 98SE 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.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

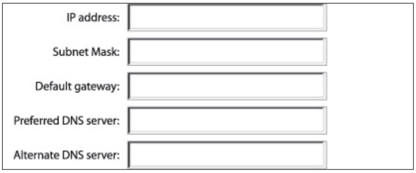
○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

☑ Detect connection to network media

3. If “Specify an 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.



IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

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

Restart the computer. When the computer restarts, your network adapter(s) are now configured for use with the Router.

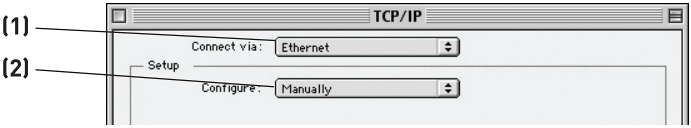
Set up the computer that is connected to the cable or DSL modem by FIRST using these steps. You can also use these steps to add computers to your Router after the Router has been set up to connect to the Internet.

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

In order for your computer to properly communicate with your Router, you will need to change your Mac computer's TCP/IP settings to DHCP.

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)**.



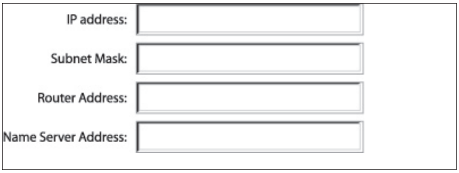
TCP/IP

Connect via: Ethernet

Setup

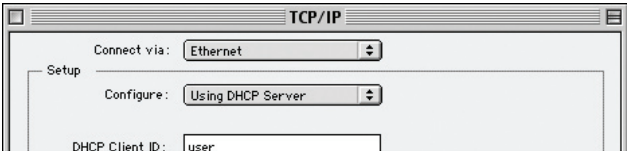
Configure: Manually

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



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

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



TCP/IP

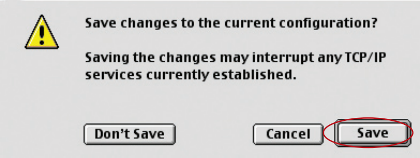
Setup

Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID: user

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



Save changes to the current configuration?

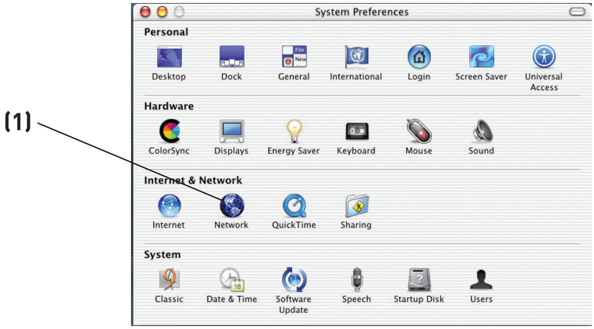
Saving the changes may interrupt any TCP/IP services currently established.

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

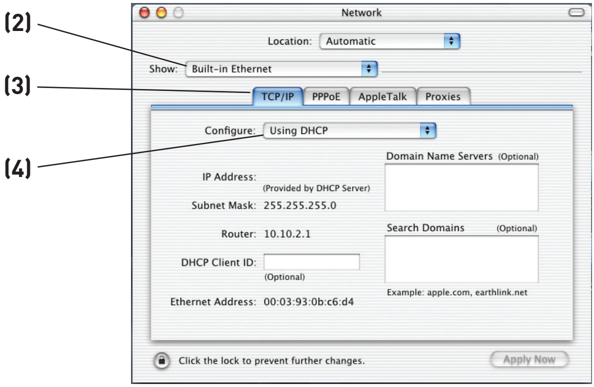
Manually Configuring Network Adapters in Mac OS X

1. Click on the “System Preferences” icon.

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



3. Select “Built-in Ethernet” **(2)** next to “Show” in the Network menu.



Location: Automatic

Show: Built-in Ethernet

TCP/IP | PPPoE | AppleTalk | Proxies

Configure: Using DHCP

Domain Name Servers (Optional)

IP Address: (Provided by DHCP Server)

Subnet Mask: 255.255.255.0

Router: 10.10.2.1

Search Domains (Optional)

DHCP Client ID: (Optional)

Example: apple.com, earthlink.net

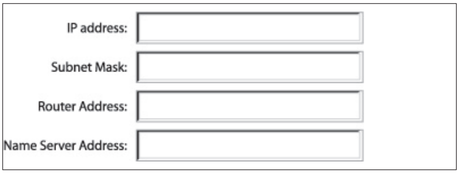
Ethernet Address: 00:03:93:0b:c6:d4

Click the lock to prevent further changes.

Apply Now

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

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



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

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

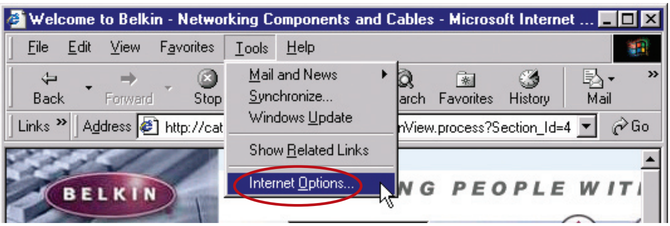
Your network adapter(s) are now configured for use with the Router.

section
1
2
3
4
5
6
7
8
9
10

Recommended Web Browser Settings

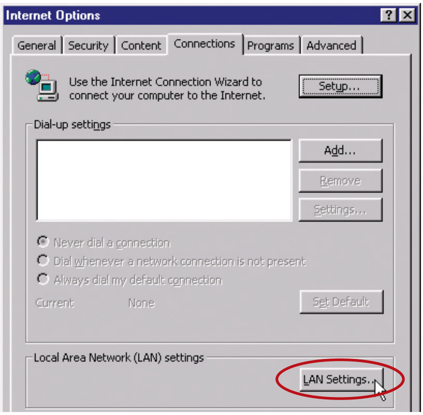
In most cases, you will not need to make any changes to your web browser's settings. If you are having trouble accessing the Internet or the advanced web-based user interface, then change your browser's settings to the recommended settings in this section.

Internet Explorer 4.0 or Higher



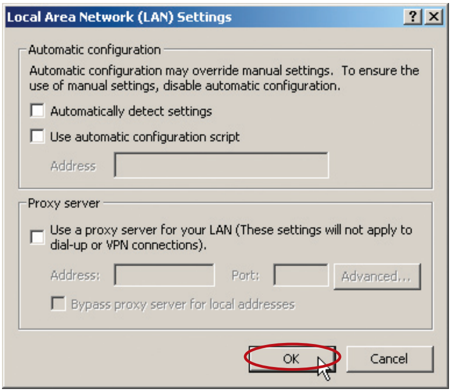
1. Start your web browser. Select "Tools" then "Internet Options".

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.


Internet Options
General
Security
Content
Connections
Programs
Advanced
Use the Internet Connection Wizard to connect your computer to the Internet.
Setup...
Dial-up settings
Add...
Remove
Settings...
○ Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection
Current
None
Set Default
Local Area Network (LAN) settings
LAN Settings...

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

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



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: Advanced...

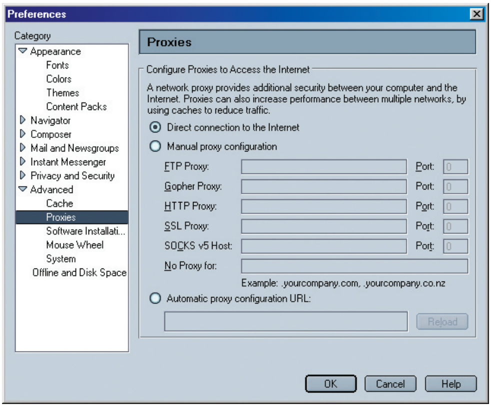
□ Bypass proxy server for local addresses

OK Cancel

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”.



Preferences

Category
- Appearance
  - Fonts
  - Colors
  - Themes
  - Content Packs
- Navigator
- Composer
- Mail and Newsgroups
- Instant Messenger
- Privacy and Security
- Advanced
  - Cache
  - Proxies
  - Software Installati...
  - Mouse Wheel
  - System
  - Offline and Disk Space

Proxies

Configure Proxies to Access the Internet

A network proxy provides additional security between your computer and the Internet. Proxies can also increase performance between multiple networks, by using caches to reduce traffic.

● Direct connection to the Internet

○ Manual proxy configuration

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

HTTP Proxy: Port: 0

SSL Proxy: Port: 0

SOCKS v5 Host: Port: 0

No Proxy for:

Example: .yourcompany.com, .yourcompany.co.nz

○ Automatic proxy configuration URL:

Reload

OK Cancel Help

Problem:

The ADSL LED is not on.

Solution:

1. Check the connection between the Router and ADSL line. Make sure the cable from the ADSL line is connected to the port on the Router labeled “DSL Line”.
2. Make sure the Router has power. The Power LED ⏻ on the front panel should be illuminated.

Problem:

The Internet LED is not on.

Solution:

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

Problem:

My connection type is static IP address. I can’t connect to the Internet.

Solution:

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.

Problem:

I’ve forgotten or lost my password.

Solution:

Press and hold the “Reset” button on the rear panel for at least six seconds to restore the factory defaults.

Problem:

My wireless PC cannot connect to the Router.

Solution:

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.

Problem:

The wireless network is often interrupted.

Solution:

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.

Problem:

I can’t connect to the Internet wirelessly.

Solution:

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

1. Look at the lights on your Router. If you are using a Belkin Router,
   - The “Power” light should be on.
2. Open your wireless utility software by clicking on the icon in the system tray at the bottom right-hand corner of the screen. If you’re using a Belkin Wireless Card, the tray icon should look like this: . The icon may be red or green.
3. The exact window that opens will vary depending on the model of wireless card you have; however, any of the utilities should have a list of “Available Networks”—those wireless networks it can connect to.

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

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

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

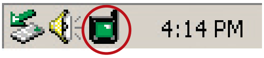
Problem:

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

Solution:

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

1. Click on the correct network name in the "Available Networks" list.
2. If the network has security (encryption) enabled, you will need to enter the network key. For more information regarding security, see the page entitled: "Changing the Wireless Security Settings".
3. Within a few seconds, the tray icon in the lower left-hand corner of your screen should turn green, indicating a successful connection to the network.



Problem:

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

Solution:

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

1. Temporarily move computer, if possible, five to 10 feet from the Router. Close the wireless utility, and re-open it. If the

correct network name now appears under “Available Networks”, you may have a range or interference problem. Please see the suggestions discussed in Appendix B entitled “Important Factors for Placement and Setup”.

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

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

Problem:

My wireless network performance is inconsistent.

Data transfer is sometimes slow.

Signal strength is poor.

Difficulty establishing and/or maintaining a Virtual Private Network (VPN) connection.

Solution:

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

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

Changing the wireless channel - Depending on local wireless traffic and interference, switching the wireless channel of your network can improve performance and reliability. The default channel the Router is shipped with is channel 11, you may choose from several other channels depending on your region; see the section entitled “Changing the Wireless Channel” on page 36 for instructions on how to choose other channels.

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

Problem:

How do I extend the range of my wireless network?

Solution:

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

- Wireless Access Point: A wireless access point can effectively double the coverage area of your wireless network. An access point is typically placed in the area not currently covered by your wireless router, and connected to the router using either an Ethernet cable, or through your home's power lines using two powerline Ethernet adapters.
- For 802.11g (54g) wireless networks, Belkin offers a Wireless Range Extender/Access Point that can be connected wirelessly to a Belkin 802.11g Wireless Router, without requiring an Ethernet cable or powerline Ethernet adapters.

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

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

Wireless G Range Extender/Access Point (F5D7130)

Powerline Ethernet Adapter (F5D4070)

Powerline USB Adapter (F5D4050)

Problem:

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

Solution:

1. Log into your Wireless Router or Access Point.
2. Open your web browser and type in IP address of the Wireless Router or Access Point. (The Router default is 192.168.2.1, the 802.11g Access Point is 192.168.2.254.) Log into your Router by clicking on the "Login" button in the top right-hand corner of the screen. You will be asked to enter your password. If you never set a password, leave the password field blank and click "Submit".
3. Click the "Wireless" tab on the left of your screen. Select the "Encryption" or "Security" tab to get to the security settings page.
4. Select "128-bit WEP" from the drop-down menu.
5. After selecting your WEP encryption mode, you can type in your hex WEP key manually, or you can type in a passphrase in the "Passphrase" field and click "Generate" to create a WEP key from the passphrase. Click "Apply Changes" to finish. You must now set all of your clients to match these settings. A hex (hexadecimal) key is a mixture of numbers and letters from A-F and 0-9. For 128-bit WEP, you need to enter 26 hex keys.

   For example:

   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key
6. Click "Apply Changes" to finish. Encryption in the Wireless Router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

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

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

Problem:

I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Belkin Wireless Card.

Solution:

The Wireless Card must use the same key as the Wireless Router or Access Point. For instance, if your Wireless Router or Access Point uses the key 00112233445566778899AABBCC, then the Wireless Card must be set to the exact same key.

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the Card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Data Encryption” select “WEP”.
6. Ensure the check box “The key is provided for me automatically” at the bottom is unchecked. If you are using this computer to connect to a corporate network, please consult your network administrator if this box needs to be checked.
7. Type your WEP key in the “Network key” box.

   Important: A WEP key is a mixture of numbers and letters from A–F and 0–9. For 128-bit WEP, you need to enter 26 keys. This network key needs to match the key you assign to your Wireless Router or Access Point.

   For example:
   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key
8. Click “OK”, and then “Apply” to save the settings.

If you are **NOT** using a Belkin Wireless Card, please consult the manufacturer for that card’s user manual.

Problem:

Do Belkin products support WPA?

Solution:

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

Download the patch here:

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

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

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

Problem:

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

Solution:

1. From the "Security Mode" drop-down menu, select "WPA-PSK (no server)".
2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.
3. Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols or spaces. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".
4. Click "Apply Changes" to finish. You must now set all clients to match these settings.

Problem:

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

Solution:

If your network uses a radius server to distribute keys to the clients, use this setting. This is typically used in a business environment.

1. From the "Security Mode" drop-down menu, select "WPA (with server)".
2. For "Encryption Technique", select "TKIP" or "AES". This setting will have to be identical on the clients that you set up.
3. Enter the IP address of the radius server into the "Radius Server" fields.
4. Enter the radius key into the "Radius Key" field.

5. Enter the key interval. Key interval is how often the keys are distributed (in packets).
6. Click “Apply Changes” to finish. You must now set all clients to match these settings.

Problem:

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

Solution:

Clients must use the same key that the wireless router or access point uses. For instance if the key is “Smith Family Network Key” in the wireless router or access point, the clients must also use that same key.

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the Card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Network Authentication” select “WPA-PSK (no server)”.
6. Type your WPA key in the “Network key” box.

   Important: WPA-PSK is a mixture of numbers and letters from A–Z and 0–9. For WPA-PSK you can enter eight to 63 characters. This network key needs to match the key you assign to your wireless router or access point.
7. Click “OK, then “Apply” to save the settings.

Problem:

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

Solution:

1. Double-click the “Signal Indicator” icon to bring up the “Wireless Network” screen.
2. The “Advanced” button will allow you to view and configure more options of the Card.
3. Once the “Advanced” button is clicked, the Belkin Wireless LAN Utility will appear. This Utility will allow you to manage all the advanced features of the Belkin Wireless Card.
4. Under the “Wireless Network Properties” tab, select a network name from the “Available networks” list and click the “Properties” button.
5. Under “Network Authentication” select “WPA”.
6. In the “Authentication” tab, select the settings that are indicated by your network administrator.
7. Click “OK, then “Apply” to save the settings.

Problem:

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

Solution:

If you are **NOT** using a Belkin Wireless Desktop or Wireless Notebook Network Card and it is not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available for free download. Download the patch from Microsoft by searching the knowledge base for Windows XP WPA.

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

Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

Enabling WPA-PSK (no server)

1. Under Windows XP, click “Start > Control Panel > Network Connections”.
2. Right-clicking on the “Wireless Networks” tab will display the following screen. Ensure the “Use Windows to configure my wireless network settings” check box is checked.
3. Under the “Wireless Networks” tab, click the “Configure” button.
4. For a home or small business user, select “WPA-PSK” under “Network Administration”.

   Note: Select WPA (with radius server) if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server. Please consult your network administrator for further information.
5. Select “TKIP” or “AES” under “Date Encryption”. This setting will have to be identical to the wireless router or access point that you set up.
6. Type in your encryption key in the “Network Key” box.

   Important: Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.
7. Click “OK” to apply settings.

What is the difference between 802.11b, 802.11g, 802.11a, and Pre-N?

Currently there are four levels of wireless networking standards, which transmit data at very different maximum speeds. Each is based on the designation 802.11(x), so named by the IEEE, the board that is responsible for certifying networking standards. The most common wireless networking standard, 802.11b, transmits information at 11Mbps; 802.11a and 802.11g work at 54Mbps; and Pre-N works at 108Mbps. Pre-N, the precursor to the upcoming 802.11n release, promises speeds that exceed 802.11g, and up to twice the wireless coverage area. See the following chart for more detailed information.

Wireless Comparison Chart

Wireless Technology	802.11b	802.11g	802.11a	Belkin Pre-N
Speed	11Mbps	54Mbps	54Mbps	600% faster than standard 802.11g*
Frequency	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	5GHz—uncrowded band	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz
Compatibility	Compatible with 802.11g	Compatible with 802.11b	Incompatible with 802.11b or 802.11g	Compatible with 802.11g or 802.11b
Coverage*	Depends on interference—typically 100–200 ft. indoors	Depends on interference—typically 100–200 ft. indoors	Interference range is typically 50–100 ft.	Up to 800% wider coverage than standard 802.11g*
Advantage	Mature—legacy technology	Common—widespread use for Internet sharing	Less interference—great for multimedia application	Leading edge—best coverage and throughput

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

Technical Support Information

Technical Support

For latest software updates or if you have any further questions regarding installation of this product, please visit **www.belkin.com/networking** or contact:

Europe:	**00 800 223 55 460**

Appendix A: Glossary

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

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 or Enternet300 that you use to connect to the Internet.

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

   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

Enter the PPPoA information in the provided spaces, and click “Next”. Click “Apply” 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. 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 and public port(s) required to pass. Then 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, 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.

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 log into the Router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes. Note, only one computer can be logged into the Router's advanced setup interface at 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 time servers 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.

Appendix B: Important Factors for Placement and Setup

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

1. **Wireless Router (or Access Point) Placement**

   Place your wireless router (or access point), the central connection point of your network, as close as possible to the center of your wireless network devices.

   To achieve the best wireless network coverage for your "wireless clients" (i.e., computers enabled by Belkin Wireless Notebook Network Cards, Wireless Desktop Network Cards, and Wireless USB Adapters):

   - Ensure that your wireless router's (or access point's) networking antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your wireless router (or access point) itself is positioned vertically, point the antennas a much as possible in an upward direction.
   - In multistory homes, place the wireless router (or access point) on a floor that is as close to the center of the home as possible. This may mean placing the wireless router (or access point) on an upper floor.
   - Try not to place the wireless router (or access point) near a cordless 2.4GHz phone.

2. **Avoid Obstacles and Interference**

   Avoid placing your wireless router (or access point) near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

   - Refrigerators
   - Washers and/or dryers
   - Metal cabinets
   - Large aquariums
   - Metallic-based UV tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal's path (between your computers and wireless router or access point).

3. Cordless Phones

If the performance of your wireless network is impaired after attending to the above issues, and you have a cordless phone:

- Try moving cordless phones away from wireless routers (or access points) and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your wireless router (or access point) to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

4. Choose the "Quietest" Channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with yours.

Use the Site Survey capabilities found in the Wireless LAN Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's manual), and move your wireless router (or access point) and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices.

For Belkin wireless networking products, use the detailed Site Survey and wireless channel information included in your User Manual.

These guidelines should allow you to cover the maximum possible area with your wireless router (or access point). Should you need to cover an even wider area, we suggest the Belkin Wireless Range Extender/Access Point.

5. Secure Connections, VPNs, and AOL

Secure connections typically require a user name and password, and are used where security is important. Secure connections include:

- Virtual Private Network (VPN) connections, often used to connect remotely to an office network
- The “Bring Your Own Access” program from America Online (AOL), which lets you use AOL through broadband provided by another cable or DSL service
- Most online banking websites
- Many commercial websites that require a user name and password to access your account

Secure connections can be interrupted by a computer’s power management setting, which causes it to “go to sleep.” The simplest solution to avoid this is to simply reconnect by rerunning the VPN or AOL software, or by re-logging into the secure website.

A second alternative is to change your computer’s power management settings so it does not go to sleep; however, this may not be appropriate for portable computers. To change your power management setting under Windows, see the “Power Options” item in the Control Panel.

If you continue to have difficulty with Secure Connections, VPNs, and AOL, please review the steps in the previous pages to be sure you have addressed these issues.

Appendix C: Internet Connection Setting Table

This table provides references to select and configure Internet connection in setting up your ADSL connection. Many ISPs use different settings depending on the region and equipment they use. You may try the setting for the ISPs in your region. If it does not work, please contact your ISP for your specific setting.

Country	Connection Protocol	VPI/VCI	Encapsulation	ISPs
Europe				
France	PPPoE	8/35	LLC	Various
Germany	PPPoE	1/32	LLC	T-Online, various
Holland	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Various
Belgium	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italy	PPPoE or PPPoA	8/35	VC MUX	TIN
Spain	PPPoE or 1483 Bridged	8/32	LLC	Telefonica
Sweden	1483 Bridged	3/35	LLC	Telia
UK	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Asia				
Australia	PPPoE or PPPoA	8/35	LLC	Various
New Zealand	PPPoE or PPPoA	0/100	VC MUX	Various
Singapore	PPPoE	0/100	LLC	SingNet, Pacific Internet

*AOL users also need to enter 1400 for MTU.

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,

F5D7632-4

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 a manner that the potential for human contact during 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 this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try 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 user's 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 apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme á 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.

CE 0682 (!)

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.

CE (!)

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 (IEC610000-3-2) – Power Line Harmonics
- EN 61000-3-3 (IEC610000) – Power Line Flicker
- EN 60950 (IEC60950) – Product Safety

CE

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 or 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®

ADSL Modem with Wireless G Router

BELKIN®

www.belkin.com

Belkin Tech Support
Europe: 00 800 223 55 460
US: 877-736-5771
310-898-1100 ext. 2263
Australia: 1800 235 546
New Zealand: 0800 235 546
Singapore: 800 616 1790

Belkin Corporation
501 West Walnut Street
Compton, CA 90220-5221, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, United Kingdom
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin Ltd.
7 Bowen Crescent, West Gosford
NSW 2250, Australia
+61 (0) 2 4372 8600
+61 (0) 2 4372 8603 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, The Netherlands
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax