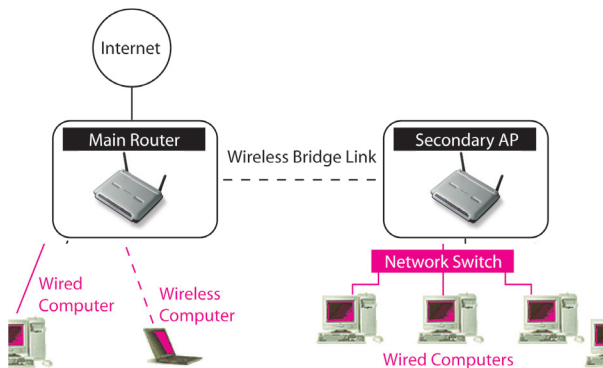


Using the Web-Based Advanced User Interface

Adding Another Network Segment Wirelessly

Bridging an Access Point to your Wireless Router allows you to add another network segment in another area in the home or office without running wires. Connecting a network switch or hub to the Access Point's RJ45 jack will allow a number of computers connected to the switch access to the rest of the network.



Setting Up a Bridge Between your Wireless Router and a Secondary Access Point

Bridging your Belkin Router to a secondary Access Point requires that you access the Router's Advanced Setup Utility and enter the MAC address of the Access Point in the appropriate area. There are also a few other requirements. **PLEASE BE SURE TO FOLLOW THE STEPS BELOW, CAREFULLY.**

1. Set your Access Point to the same channel as the Router. By default, the Router and Access Point channels are set to channel 11 at the factory. If you have never changed the channel, you don't need to do anything (for more information on changing channels, see page 47 of this manual).
2. Find the Access Point's MAC address on the bottom of the Access Point. There are two MAC addresses on the bottom label. You will need the MAC address named "WLAN MAC Address". The MAC address starts with 0030BD and is followed by six other numbers or letters (i.e. 0030BD-XXXXXX). Write the MAC address below. Go to the next step.



3. Place your secondary Access Point within range of your Wireless Router and near the area where you want to extend the range or add the network segment. Typically, indoor range should be between 100 and 200 feet.
4. Connect power to your Access Point. Make sure the Access Point is on and proceed to the next step.

Using the Web-Based Advanced User Interface

- From a computer already connected to your Router, access the Advanced Setup Utility by opening your browser. In the address bar, type in “192.168.2.1”. Do not type in “www” or “http://” before the number. **Note:** If you have changed your Router’s IP address, use that IP address.
- You will see the Router’s user interface in the browser window. Click “Wireless Bridge” (2) on the left-hand side of the screen. You will see the following screen.

BELKIN Cable/DSL Gateway Router Setup Utility

Home | Help | Logout | Internet Status: connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Encryption
Use as Access Point
Wireless Bridge
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
WAN Ping Blocking
Security Log
Utilities
Parental Control
Reset Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings

Wireless > Wireless bridge

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

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

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

AP1	:	:	:	:	:	:
AP2	:	:	:	:	:	:
AP3	:	:	:	:	:	:
AP4	:	:	:	:	:	:

Disable ability for Wireless CLIENTS to connect. (This feature should only be used when the AP is used exclusively to connect wirelessly to other APs.)

- Check the box that says “Enable ONLY specific Access Points to connect” (1).
- In the field named AP1 (3), type in the MAC address of your secondary Access Point. When you have typed in the address, click “Apply Changes”.
- Bridging is now set up.

Configuring the Firewall

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

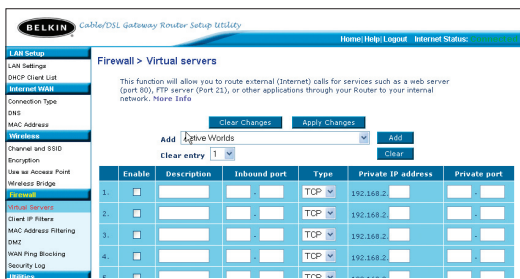
- IP Spoofing
- SYN flood
- Land Attack
- UDP flooding
- Ping of Death (PoD)
- Tear Drop Attack
- Denial of Service (DoS)
- ICMP defect
- IP with zero length
- RIP defect
- Smurf Attack
- Fragment flooding
- TCP Null Scan

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.

The screenshot shows the Belkin Cable/DSL Gateway Router Setup Utility web interface. The page title is "Firewall >". The left sidebar contains a navigation menu with the following items: LAN Setup, LAN Settings, DHCP Client List, Internet WAN, Connection Type, DNS, MAC Address, Firewall (highlighted), Virtual Servers, Client IP Filters, MAC Address Filtering, DMZ, WAN Ping Blocking, Security Log, Utilities, and Parental Control. The main content area contains the following text: "Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible." Below this text, there are two radio buttons: "Firewall Enable / Disable > Disable Enable". At the bottom of the main content area, there are two buttons: "Clear Changes" and "Apply Changes".

Configuring Internal Forwarding Settings

The Virtual Servers function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, computers outside your network (over the Internet) cannot get to them because they cannot be “seen.” A list of common applications has been provided in case you need to configure the Virtual Server function for a specific application. If your application is not listed, you will need to contact the application vendor to find out which port settings you need.



Choosing an Application

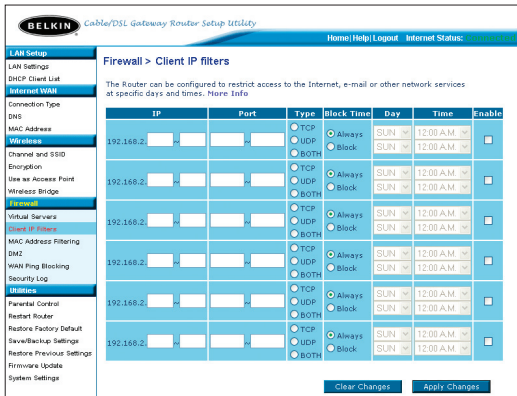
Select your application from the drop-down list. Click “Add”. The settings will be transferred to the next available space in the screen. Click “Apply Changes” to save the setting for that application. To remove an application, select the number of the row that you want to remove then click “Clear”.

Manually Entering Settings into the Virtual Server

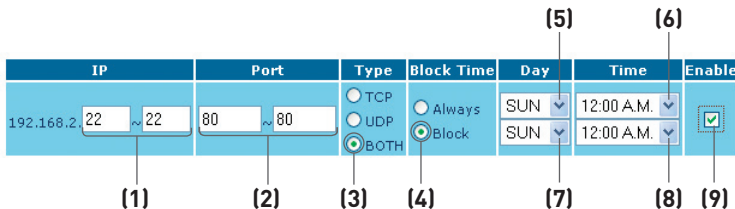
To manually enter settings, enter the IP address in the space provided for the internal (server) machine, the port(s) required to pass, select the port type (TCP or UDP), and click “Apply Changes”. Each inbound port entry has two fields with 5 characters maximum per field that allows a start and end port range, e.g. [xxxxx]-[xxxxx]. For each entry, you can enter a single port value by filling in the two fields with the same value (e.g. [7500]-[7500]) or a wide range of ports (e.g. [7500]-[9000]). If you need multiple single port value or mixture of ranges and a single value, you must use multiple entries up to the maximum of 20 entries (e.g. 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Setting Client IP Filters

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



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



Using the Web-Based Advanced User Interface

Setting MAC Address Filtering

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

The screenshot shows the Belkin Cable/DSL Gateway Router Setup Utility interface. The left sidebar contains a navigation menu with the following items: LAN Setup, LAN Settings, DHCP Client List, Internet WAN, Connection Type, DNS, MAC Address, Wireless, Channel and SSID, Encryption, Use as Access Point, Wireless Bridge, Firewall, Virtual Servers, Client IP Filters, MAC Address Filtering, DMZ, WAN Ping Blocking, Security Log, Utilities, Parental Control, Restart Router, Restore Factory Default, Save/Backup Settings, Restore Previous Settings, Firmware Update, and System Settings. The main content area is titled 'Firewall > MAC Address Filtering'. Below the title, there is a paragraph explaining the feature. A checkbox labeled 'Enable MAC Address Filtering >' is present, with a callout line (1) pointing to it. Below this is a table titled 'MAC Address Filtering List >' with three columns: 'Block', 'Host', and 'MAC Address'. The 'Block' column has a checkbox, the 'Host' column is empty, and the 'MAC Address' column has a callout line (2) pointing to the input space. To the right of the table is an '<< Add' button with a callout line (3) pointing to it. At the bottom of the table area are two buttons: 'Clear Changes' and 'Apply Changes'.

To enable this feature, select “Enable MAC Address Filtering” (1). Next, enter the MAC address of each computer on your network by clicking in the space provided (2) and entering the MAC address of the computer you want to add to the list. Click “Add” (3), then “Apply Changes” to save the settings. To delete a MAC address from the list, simply click “Delete” next to the MAC address you wish to delete. Click “Apply Changes” to save the settings.

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

Enabling the Demilitarized Zone (DMZ)

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

The screenshot shows the Belkin Cable/DSL Gateway Router Setup Utility web interface. The left sidebar contains a navigation menu with the following items: LAN Setup, LAN Settings, DHCP Client List, Internet WAN (highlighted), Connection Type, DNS, MAC Address, Wireless, Channel and SSID, Encryption, Use as Access Point, Wireless Bridge, Firewall (highlighted), Virtual Servers, Client IP Filters, MAC Address Filtering, DMZ (highlighted), WAN Ping Blocking, and Security Log. The main content area is titled "Firewall > DMZ". Below the title, there is a "DMZ" section with a descriptive paragraph: "The DMZ feature allows you to specify one computer on your network to be placed outside of the NAT firewall. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks. To put a computer in the DMZ, enter the last digits of its IP address in the field below and select 'Enable'. Click 'Submit' for the change to take effect. More Info". Below this text is a table titled "IP Address of Virtual DMZ Host >". The table has three columns: "Static IP", "Private IP", and "Enable". There is one row with the index "1.". The "Static IP" column contains the value "67.113.196.172". The "Private IP" column contains the value "192.168.2." followed by a text input field. The "Enable" column contains a checkbox. Below the table are two buttons: "Clear Changes" and "Apply Changes".

	Static IP	Private IP	Enable
1.	67.113.196.172	192.168.2. <input type="text"/>	<input type="checkbox"/>

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

Using the Web-Based Advanced User Interface

Blocking an ICMP Ping

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



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

Using the Web-Based Advanced User Interface

1

2

3

4

5

6

7

8

9

10

11

section

Utilities Tab

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

BELKIN Cable/DSL Gateway Router Setup Utility

Home | Help | Logout Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List

Internet WAN
Connection Type
DNS
MAC Address

Wireless
Channel and SSID
Encryption
Use as Access Point
Wireless Bridge

Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
WAN Ping Blocking
Security Log

Utilities
Parental Control
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings

Utilities > Restart Router

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

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

Parental Control

See separate Parental Control User Manual from Belkin.