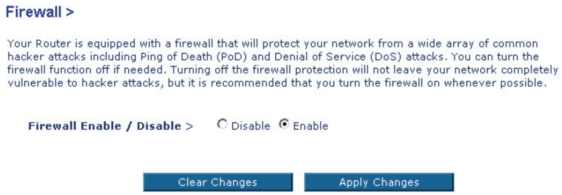
Configuring the Firewall

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.



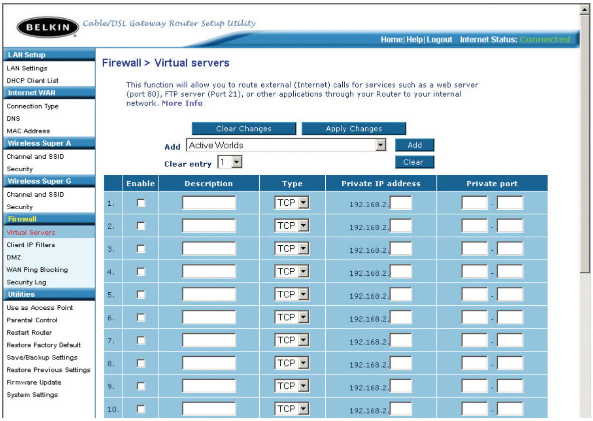
Firewall >

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.

Firewall Enable / Disable > ○ Disable ● Enable

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.



Firewall > Virtual servers

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

Add: Active Worlds

Clear entry: 1

	Enable	Description	Type	Private IP address	Private port
1.	☐		TCP	192.168.2.	-
2.	☐		TCP	192.168.2.	-
3.	☐		TCP	192.168.2.	-
4.	☐		TCP	192.168.2.	-
5.	☐		TCP	192.168.2.	-
6.	☐		TCP	192.168.2.	-
7.	☐		TCP	192.168.2.	-
8.	☐		TCP	192.168.2.	-
9.	☐		TCP	192.168.2.	-
10.	☐		TCP	192.168.2.	-

Choosing an Application

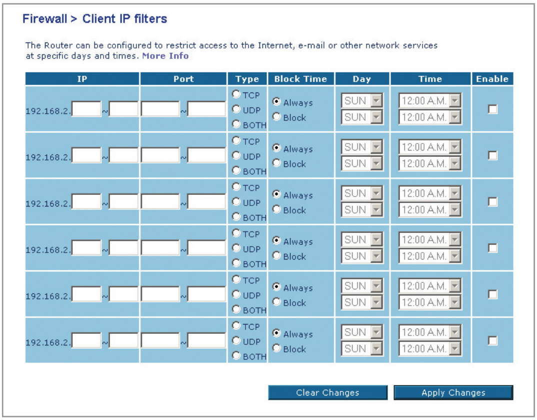
Select your application from the drop-down list. Click "Add". The settings will be transferred to the next available space in the screen. Click "Apply Changes" to save the setting for that application. To remove an application, select the number of the row that you want to remove then click "Clear".

Manually Entering Settings into the Virtual Server

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

Setting Client IP Filters

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



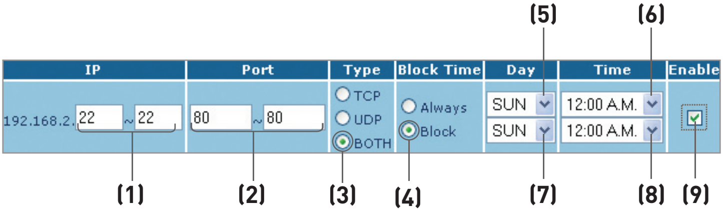
Firewall > Client IP filters

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

IP	Port	Type	Block Time	Day	Time	Enable
192.168.2. ~	~	○ TCP ○ UDP ○ BOTH	● Always ○ Block	SUN SUN	12:00 A.M. 12:00 A.M.	□
192.168.2. ~	~	○ TCP ○ UDP ○ BOTH	● Always ○ Block	SUN SUN	12:00 A.M. 12:00 A.M.	□
192.168.2. ~	~	○ TCP ○ UDP ○ BOTH	● Always ○ Block	SUN SUN	12:00 A.M. 12:00 A.M.	□
192.168.2. ~	~	○ TCP ○ UDP ○ BOTH	● Always ○ Block	SUN SUN	12:00 A.M. 12:00 A.M.	□
192.168.2. ~	~	○ TCP ○ UDP ○ BOTH	● Always ○ Block	SUN SUN	12:00 A.M. 12:00 A.M.	□
192.168.2. ~	~	○ TCP ○ UDP ○ BOTH	● Always ○ Block	SUN SUN	12:00 A.M. 12:00 A.M.	□

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.

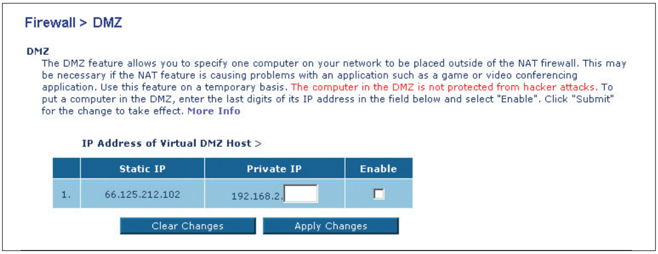
Note: Be sure you have selected the correct time zone under "Utilities> System Settings> Time Zone".



IP	Port	Type	Block Time	Day	Time	Enable
192.168.2. 22 ~ 22	80 ~ 80	○ TCP ○ UDP ● BOTH	○ Always ● Block	SUN SUN	12:00 A.M. 12:00 A.M.	☑

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.



Firewall > DMZ

DMZ

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

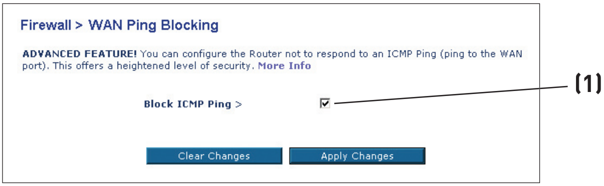
IP Address of Virtual DMZ Host >

	Static IP	Private IP	Enable
1.	66.125.212.102	192.168.2.	☐

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”.

Blocking an ICMP Ping

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



Firewall > WAN Ping Blocking

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

Block ICMP Ping > ☑

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

Utilities

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

Parental Control

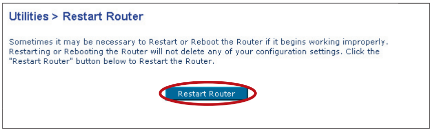
See the included Parental Control User Manual for more information on the Parental Control feature.

Restarting the Router

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

Restarting the Router to Restore Normal Operation

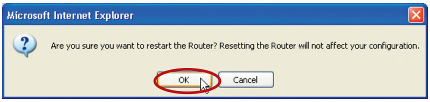
1. Click the "Restart Router" button.



Utilities > Restart Router

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

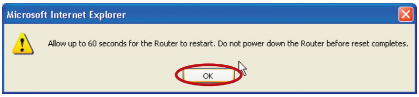
2. The following message will appear. Click "OK".



Microsoft Internet Explorer

Are you sure you want to restart the Router? Resetting the Router will not affect your configuration.

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



Microsoft Internet Explorer

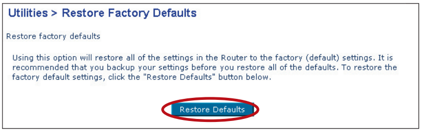
Allow up to 60 seconds for the Router to restart. Do not power down the Router before reset completes.

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

Restoring Factory Default Settings

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

1. Click the "Restore Defaults" button.

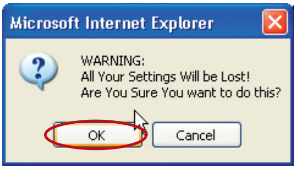


Utilities > Restore Factory Defaults

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.

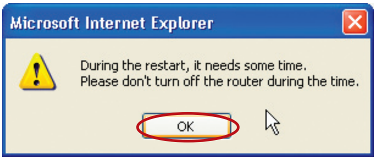
2. The following message will appear. Click "OK".



Microsoft Internet Explorer

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

3. The following message will appear. Restoring the defaults includes restarting the Router. It can take up to 60 seconds. It is important not to turn the power to the Router off during the restart.



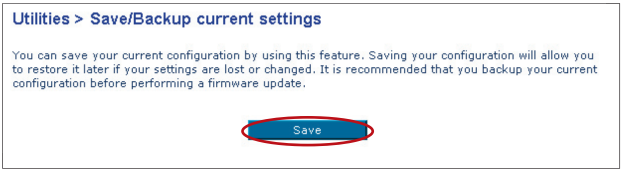
Microsoft Internet Explorer

During the restart, it needs some time.
Please don't turn off the router during the time.

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

Saving a Current Configuration

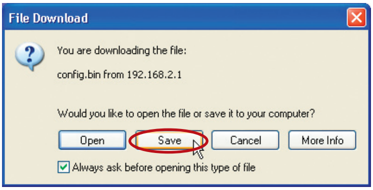
You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.



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



File Download

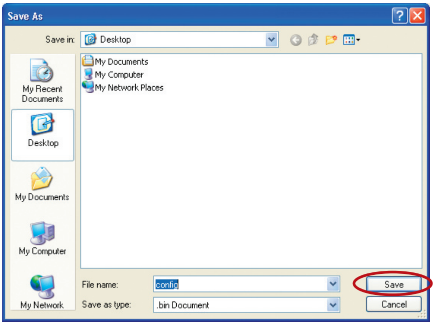
You are downloading the file:

config.bin from 192.168.2.1

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

2. A window will open that allows you to select the location where you want to save the configuration file. Select a location. You can name the file anything you want, or use the default name “Config”. Be sure to name the file so you can locate it yourself later. When you have selected the location and name of the file, click “Save”.



Save As

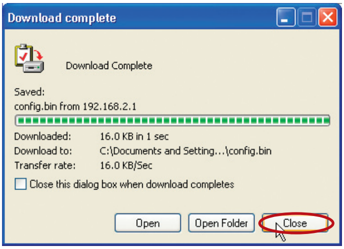
Save in: Desktop

File name: config

Save as type: .bin Document

3. When the save is complete, you will see the following window. Click “Close”.

The configuration is now saved.



Download complete

Download Complete

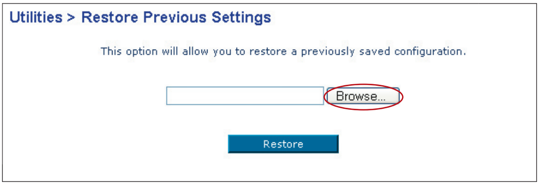
Saved:
config.bin from 192.168.2.1

Downloaded: 16.0 KB in 1 sec
Download to: C:\Documents and Setting...\config.bin
Transfer rate: 16.0 KB/Sec

☐ Close this dialog box when download completes

Restoring a Previous Configuration

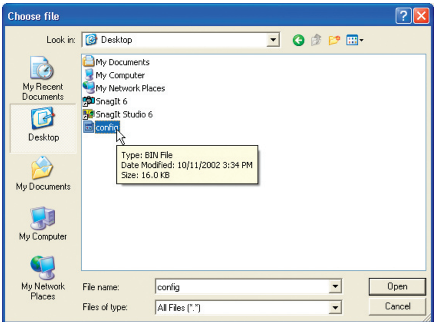
This option will allow you to restore a previously saved configuration.



Utilities > Restore Previous Settings

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

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



Choose file

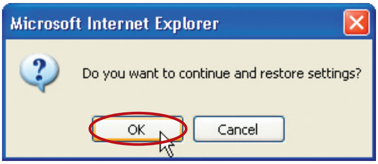
Look in: Desktop

My Documents
My Computer
My Network Places
SnagIt 6
SnagIt Studio 6
config

Type: BIN File
Date Modified: 10/11/2002 3:34 PM
Size: 16.0 KB

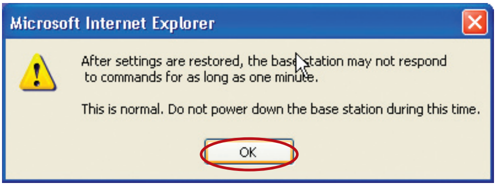
File name: config
Files of type: All Files (*.*)

2. You will be asked if you want to continue. Click “OK”.


Microsoft Internet Explorer

Do you want to continue and restore settings?

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


Microsoft Internet Explorer

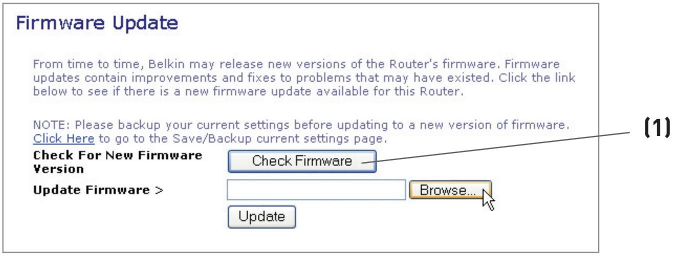
After settings are restored, the base station may not respond to commands for as long as one minute.

This is normal. Do not power down the base station during this time.

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

Updating the Firmware

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may exist. 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.



Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed. Click the link below to see if there is a new firmware update available for this Router.

NOTE: Please backup your current settings before updating to a new version of firmware. Click Here to go to the Save/Backup current settings page.

Check For New Firmware Version

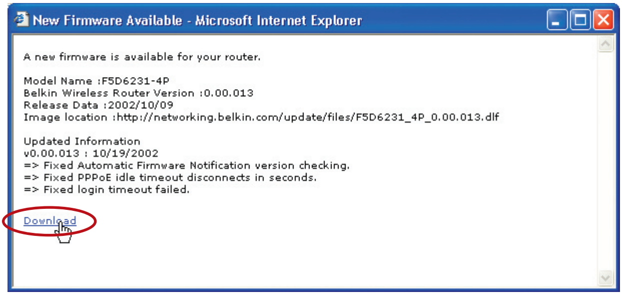
Update Firmware >

Checking for a New Version of Firmware

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

Downloading a New Version of Firmware

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



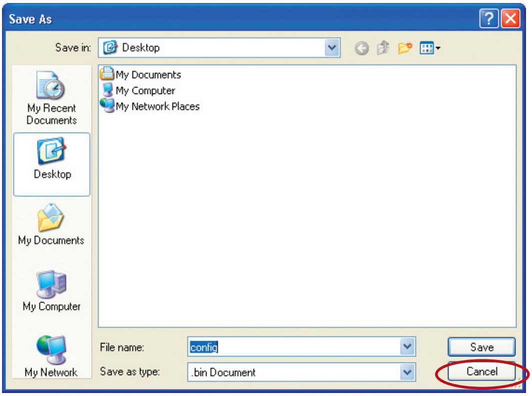
```
A new firmware is available for your router.

Model Name :F5D6231-4P
Belkin Wireless Router Version :0.00.013
Release Data :2002/10/09
Image location :http://networking.belkin.com/update/files/F5D6231_4P_0.00.013.dlf

Updated Information
v0.00.013 : 10/19/2002
=> Fixed Automatic Firmware Notification version checking.
=> Fixed PPPoE idle timeout disconnects in seconds.
=> Fixed login timeout failed.

Download
```

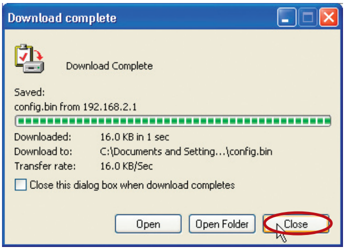
1. To download the new version of firmware, click “Download”.
2. A window will open that allows you to select the location where you want to save the firmware file. Select a location. You can name the file anything you want, or use the default name. Be sure to save the file in a place where you can locate it yourself later. **Note:** We suggest saving this to your desktop to locate the file easily. When you have selected the location, click “Save”.



File name: config

Save as type: .bin Document

3. When the save is complete, you will see the following window. Click “Close”.



Download complete

Download Complete

Saved:
config.bin from 192.168.2.1

Downloaded: 16.0 KB in 1 sec
Download to: C:\Documents and Setting...\config.bin
Transfer rate: 16.0 KB/Sec

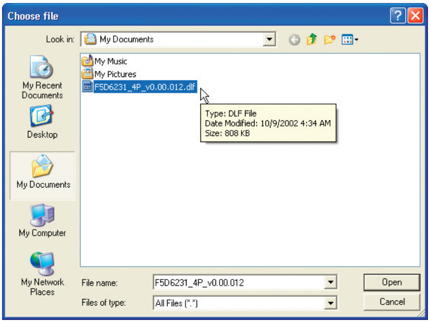
□ Close this dialog box when download completes

The download of the firmware is complete. To update the firmware, follow the next steps in “Updating the Router’s Firmware”.

Updating the Router’s Firmware

1. In the “Firmware Update” page, click “Browse” **(2)**. 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.



Choose file

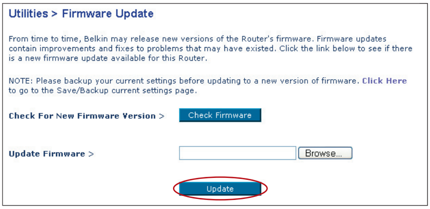
Look in: My Documents

My Music
My Pictures
F5D6231_4P_v0.00.012.dlf

Type: DLF File
Date Modified: 10/9/2002 4:34 AM
Size: 808 KB

File name: F5D6231_4P_v0.00.012
Files of type: All Files (*.*)

3. The “Update Firmware” box will now display the location and name of the firmware file you just selected. Click “Update”.

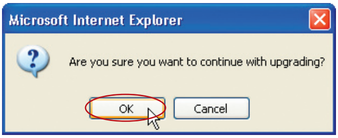


Utilities > Firmware Update

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain improvements and fixes to problems that may have existed. Click the link below to see if there is a new firmware update available for this Router.

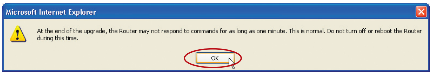
NOTE: Please backup your current settings before updating to a new version of firmware. Click Here to go to the Save/Backup current settings page.

4. You will be asked if you are sure you want to continue. Click “OK”.



Are you sure you want to continue with upgrading?

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



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

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