Brickcom

Wireless Dual-Band N Router

DWRT-600N

User Manual

Quality Service Group

Brickcom

Product name:	Dual-Band N Router (DWRT-600N)
Release Date:	2010/9
Manual Revision:	V1.0
Web site:	www.brickcom.com
Email:	support@brickcom.com
	info@brickcom.com

Table of Contents

Introduction

Package Contents

- Brickcom Dual-Band Wireless N Router
- Ethernet cable
- Power Adapter
- Quick Setup Guide

Wireless Dual-Band N Router Overview

The Brickcom DWRT-600N is a dual-band wireless router which is designed specifically for use with IP surveillance systems. The DWRT-600N works with wired and simultaneous dual-band wireless (802.11a/b/g/n) network surveillance devices such as IP cameras, network video recorders, and related BrickOne Solution® networking accessories. Up to four wired Internet devices can be connected to the router's integrated 4-port 10/100 switch.

Equipped with simultaneous dual-band wireless, this router is able to prioritize the transmission of network cameras' streaming over regular data files to deliver smooth video and audio surveillance without delay. Users can quickly surf the Internet using the 2.4 GHz band while the Brickcom wireless cameras are streaming high quality video surveillance using the 5 GHz band.

This wireless router is designed to simplify the setup between Brickcom network cameras and the local area network. Upon powering on the router and Brickcom network camera, the connection will be made automatically, requiring no configuration.

Device Description

Front LEDs


Power, Wireless

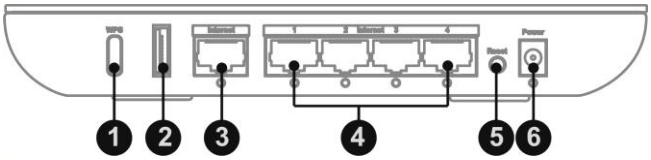

Camera, WPS (Wi-Fi Protected Setup)


WAN

Function	***LED Behavior***	***Description***
 *Power, Wireless*	*Lit*	*Router is powered on and wireless is enabled.*
 *Power, Wireless*	*Flashing*	*Router is sending or receiving data over the network.*
 *Camera, WPS (Wi-Fi Protected Setup)*	*Lit*	*Router is connected with a network camera(s)*
 *Camera, WPS (Wi-Fi Protected Setup)*	*Flashing*	*Router is setting up the WPS connection. The router supports one WPS session at a time so wait until the LED stops flashing before connecting another WPS device.*
 *Camera, WPS (Wi-Fi Protected Setup)*	*Unlit*	*An error occurred during the WPS setup process. Make sure the device(s) supports WPS and try again.*
 *WAN*	*Lit*	*There is a working Internet connection*

WAN	*Flashing*	*Indicates network activity over the Internet port.*

Rear Panel Connections



1. ***WPS (Wi-Fi Protected Setup) Button—*** *WPS allows users to automatically configure wireless security for their wireless network if they are connecting devices that support WI-FI Protected Setup.*
2. ***USB—*** For external USB hard drive or USB sticker.
3. ***Internet—*** *Connect a high-speed cable or DSL Internet service to this port.*
4. ***Ethernet 1, 2, 3, 4—*** *Use these ports to connect Ethernet devices to the router or use an Ethernet cable to connect the router to computers on the wired network. The LED under the port will light up when the router is connected to an Ethernet device. The LED will flash when there is network activity over that port.*
5. ***Reset—*** *Press and hold for approximately ten seconds to reset the router to factory default settings. If any custom settings have been applied to the router, including a login name and password, they will be erased and replaced with the factory default settings.*
6. ***Power—*** *Connect the power adapter to this port. The LED under the port will light up when the router is on. The LED will flash when the router goes through a self-diagnostic test during boot-up.]*

System Requirements

- Broadband Internet connection, such as a cable or DSL modem with an Ethernet (RJ45) connection
- At least one computer with a network adapter
- TCP/IP networking protocol installed on each computer
- Extra Ethernet (RJ-45) cable
- Internet browser (such as Internet Explorer, Firefox, or Safari)

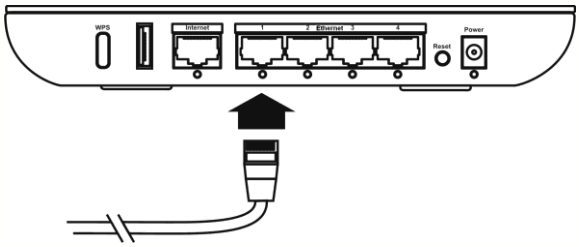
Setting Up the Brickcom Router

Equipment needed:

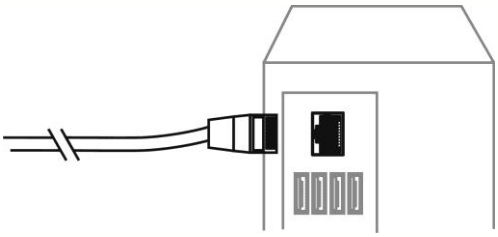
- Brickcom Router, Power Adapter, and Ethernet cable (included)
- High-speed Internet connection and access to Internet modem (Users should contact their local provider assistance if needed)
- Additional Ethernet cable (usually provided with the Internet modem)
- A computer Internet browser (such as Internet Explorer, Firefox, or Safari)

Step by Step Setup

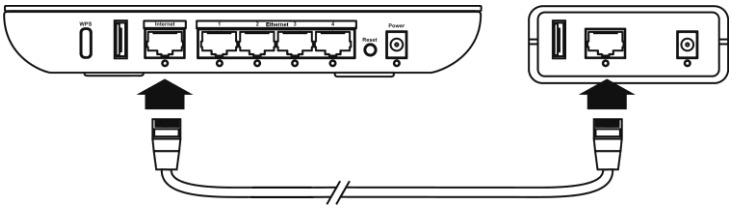
1. Unplug the power cable from the high-speed Internet modem.
2. Connect one end of one of the Ethernet cables to the router's number 1 port.



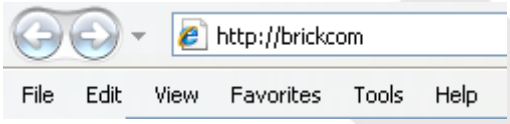
3. Connect the other end to the Ethernet port to a computer.



4. Connect the other Ethernet cable from the high-speed Internet modem into the Internet port on the router.



5. Plug the power back into the high-speed Internet modem. Wait 30 seconds and plug the power adapter into the router. The router will automatically turn on.
6. Wait 30 seconds for the router to fully connect and open an Internet browser window (such as Internet Explorer, Firefox, or Safari). Enter **http://Brickcom** (or 192.168.1.1) in the browser window and press Enter. The router's web GUI will be displayed.



7. From here, click an icon (**INTERNET**, **ROUTER**, or **WIRELESS**) to open its menu and adjust settings.

Finding a Location for the Router

Here are some things to consider when deciding on a proper location for the router:

- Place the router as close as possible to the center of the wireless network devices. The connection will be stronger the closer the devices are to the router. Typical indoor operating range is up to 200 feet.
- Avoid placing the router near devices that may emit "noise", including microwave ovens, refrigerators, and metal cabinets. If the wireless signal seems weak, make sure that objects are not blocking the signal's path between the device and the router.
- For proper ventilation, allow at least 4 inches (10 cm) on all sides of the router.
- Avoid installing the router in places with high humidity, dust, or smoke because these things can shorten the service life of the electronic components.
- Read this user manual carefully before setting up the router.

Wall-Mounting Placement

The router has two wall-mount slots on the bottom panel.

Note: Brickcom is not responsible for damages incurred by unsecure wall-mounting hardware.

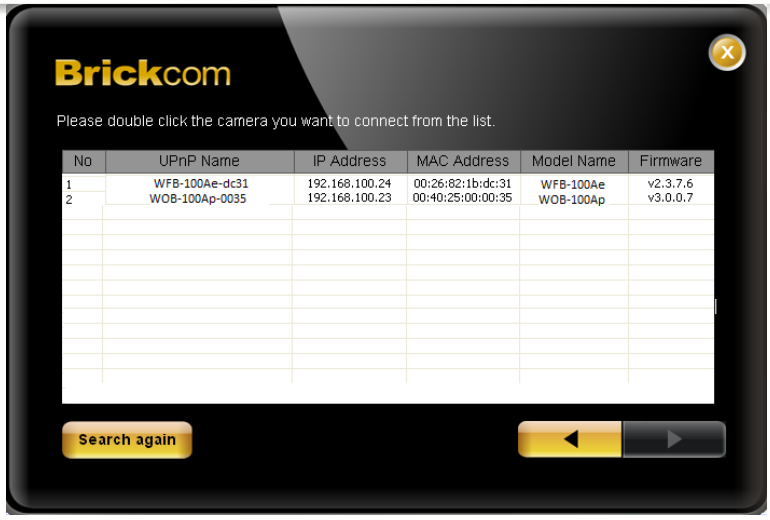
1. Choose a wall that is within reach of an electrical outlet and is smooth and sturdy.
2. Drill two holes 6 inches (152 mm) apart into the wall.
3. Insert a screw into each hole leaving 0.12 inches (3 mm) of the screw head exposed.
4. Line up the wall-mount slots on the bottom of the router with the screws and slide the router down until the screws fit snugly into the wall-mount slots.

Connecting with Brickcom Network Camrea

Follow these steps to quickly launch the camera's web-based live view page via the router.

Setup Steps

1. Complete the installation of the Camera(s) and Access Point.
2. Launch EasyConfig and the Camera(s) on the network will appear on the survey list. Double click on the desired camera to connect.



Note: Install EasyConfig from the Camera's supplied CD.

3. Enter the username and password of the camera. The default username and password are "admin/admin."
4. Follow the EasyConfig software to configure the camera's IP address settings and EasyLinkTM function.
5. When the Camera IP address settings have been configured, the screen will either display a successful or failed connection message. If the connection failed, either try again or quit the installation. Click <Live View> to view the live video from the connected camera.

Note: If the Brickcom Camrea is equipped dual band WiFi connectivity, the 5GHz would be higher priority than 2.4GHz.

Setting up USB Storage

This section details how to connect a USB storage device to the router and use it as a storage device for a network camera. By setting up the router as a samba server for the network camera, the camera can send video clips and snapshots to the storage device via samba protocol.

Note: This user manual uses a Brickcom network camera as an example for setting up the USB storage device. Samba settings for other network cameras may vary.

Step by Step Setup

1. Attach the storage device to the router's USB port.
2. Access the router's GUI and the name of the USB storage device will be displayed in the USB Network Media field.

3. Click on the name of the device to access it and check the root folder name. Normally the root folder name is "*Default0*".

4. Access the network camera's Samba Settings page and enter the following information.

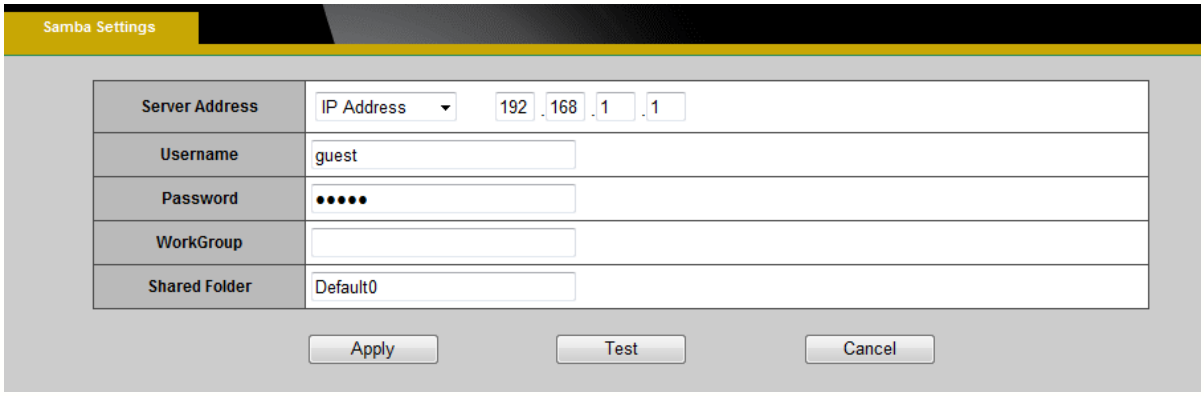
   Server Address- Enter the IP address of the Brickcom Router.

   *Username- *guest*

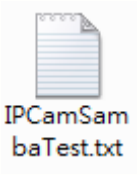
   *Password- *guest*

   *Workgroup- Leave blank

   *Share folder- Enter the root folder name of the USB storage device. Normally this name is *Default0*.

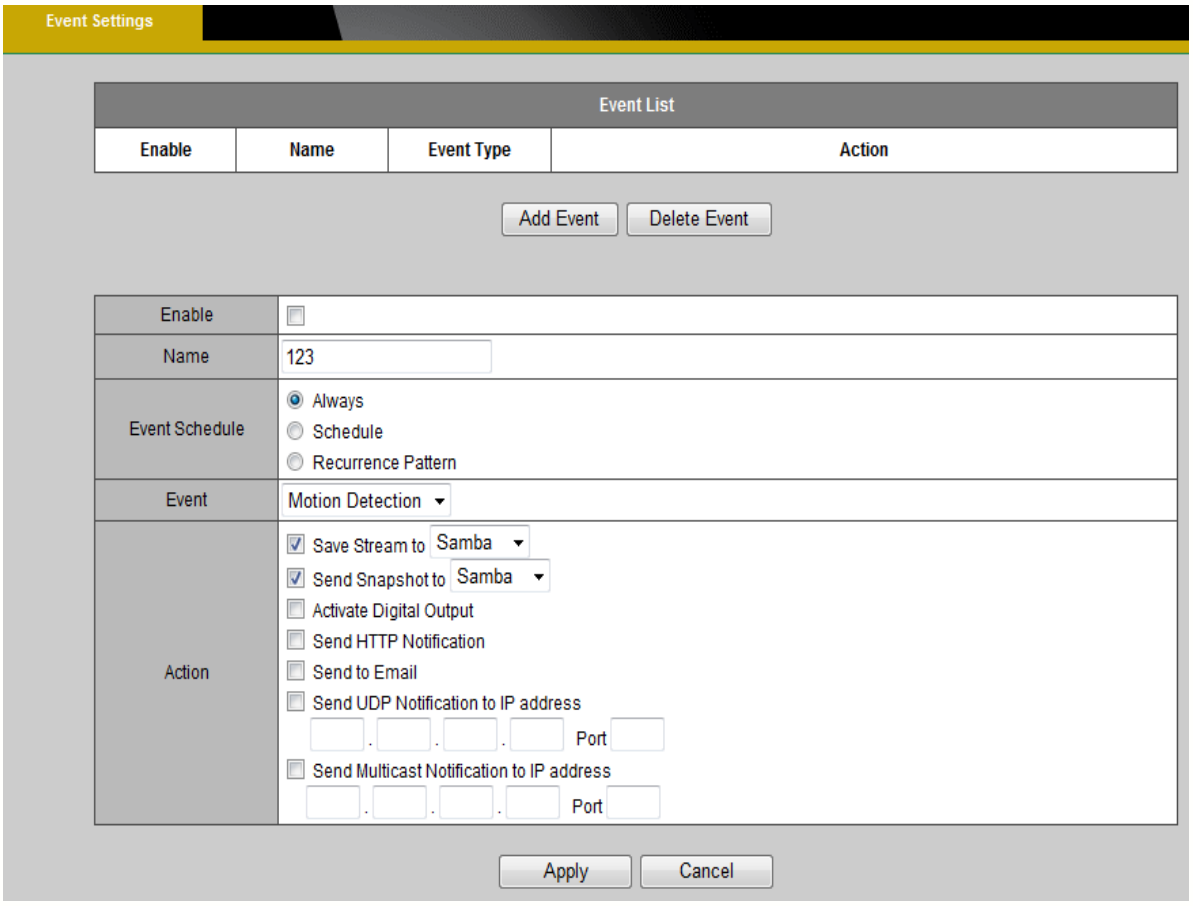


5. Click on **Test** to verify that the samba settings are correct. If the settings are correct., a txt file named "*IPCamSambaTest*" will appear.



6. Click **Apply** to save the settings.

7. The USB storage device can now be used to store video clips and snapshots from the network camera. To use the samba server, access the camera's Event Settings. Enter the event information and select <Save Stream to Samba> or <Save Snapshot to Samba> to save a video clip or snapshot to the USB storage device when event occurs.



Accessing USB Storage

When a USB storage device is connected to the router's USB port, the files on the storage device can be shared with all of the computers on the network.

The router is a DLNA server, which means that music, photo, and video files stored on the connected USB storage device can be automatically accessed through a DLNA-compliant device.

NOTE: The USB storage device must be formatted for NTFS or FAT.

There are three ways to access the files on the USB storage device: from the Router GUI, by browsing the computer's network, or through a DLNA-compatible device (media files only).

Via the Router GUI

1. Ensure that the computer has a working wired or wireless connection to the router.
2. Connect an external USB hard drive or USB flash drive to the USB port on the back of the router.
3. Enter **http://Brickcom** (or 192.168.1.1) in the browser window and press **Enter**. The Router GUI will automatically start and the name of the USB device will be displayed in the USB Network Media field.
4. Click the name of the device to begin browsing the files stored on it.

Via the Computer Network

1. Ensure that the computer has a working wired or wireless connection to the router.
2. Connect an external USB hard drive or USB flash drive to the USB port on the back of the router.
3. On the computer (Windows or Mac), browse the network for the name of the USB storage device.

Via a DLNA-compatible device

1. Ensure that the computer has a working wired or wireless connection to the router.
2. Connect an external USB hard drive or USB flash drive to the USB port on the back of the router.
3. On the DLNA-compatible device, refresh the network list and look for the Brickcom Digital Media Server.
4. Browse the server to locate and play the media files.

Changing Advanced Router Settings

After setting up the router, use a web browser to login to the router's home page and make any desired changes to the router's settings. Use the router home page to:

- View settings and router status
- Set up a firewall to work with specific applications (port forwarding)
- Set up and modify security features
- Set up a user name and password
- Reset the router
- Update the router's firmware

Caution: These are advanced settings that should only be modified by those experienced in setting up and modifying wired and/or wireless networks.

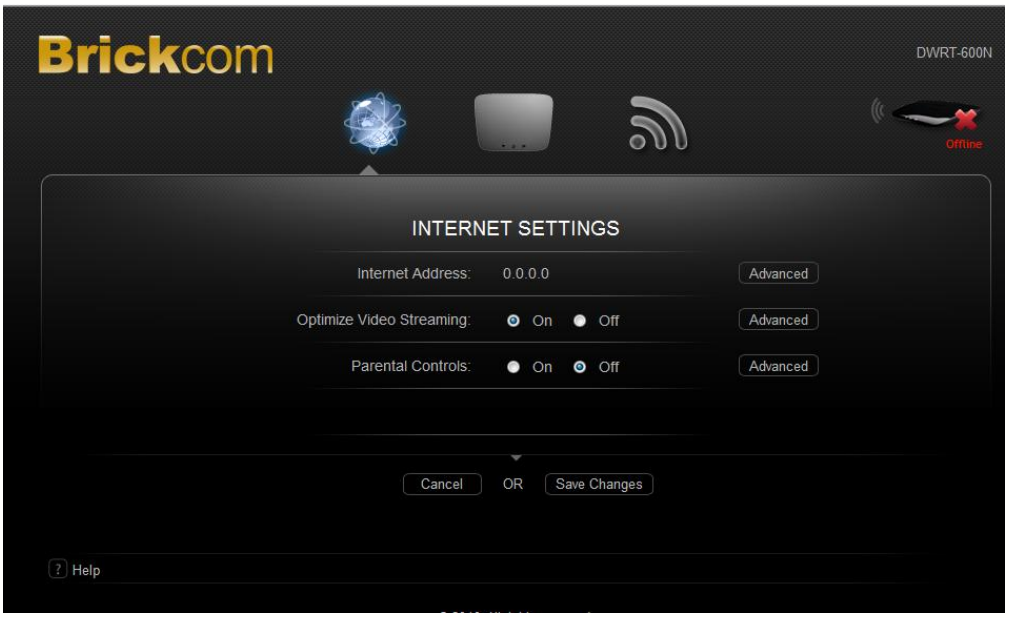
1. **Brickcom—**Click to go back to the Home page.
2. **Internet Status—** A green check indicates a working Internet connection. A red X will appear when there is no working Internet connection.
3. **Settings—**Click an icon to open its menu and adjust settings.
4. **Help—**Click to open the User Manual.

To access the Router GUI:

1. On a computer that is connected to the router, open an Internet browser window (such as Internet Explorer, Firefox, or Safari).
2. Enter **http://Brickcom** (or 192.168.1.1) in the browser window. Press Enter and the GUI will open.
3. Click INTERNET, ROUTER, or WIRELESS to open its menu.

Internet Menu

The Internet menu can be used to customize the Internet settings.



Internet Address

The router's IP address, as seen from the Internet, will be displayed here. To makes changes, click Advanced. A new menu will be displayed showing the advanced options available for the Internet Address. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel the changes.

Advanced Options

Configuration

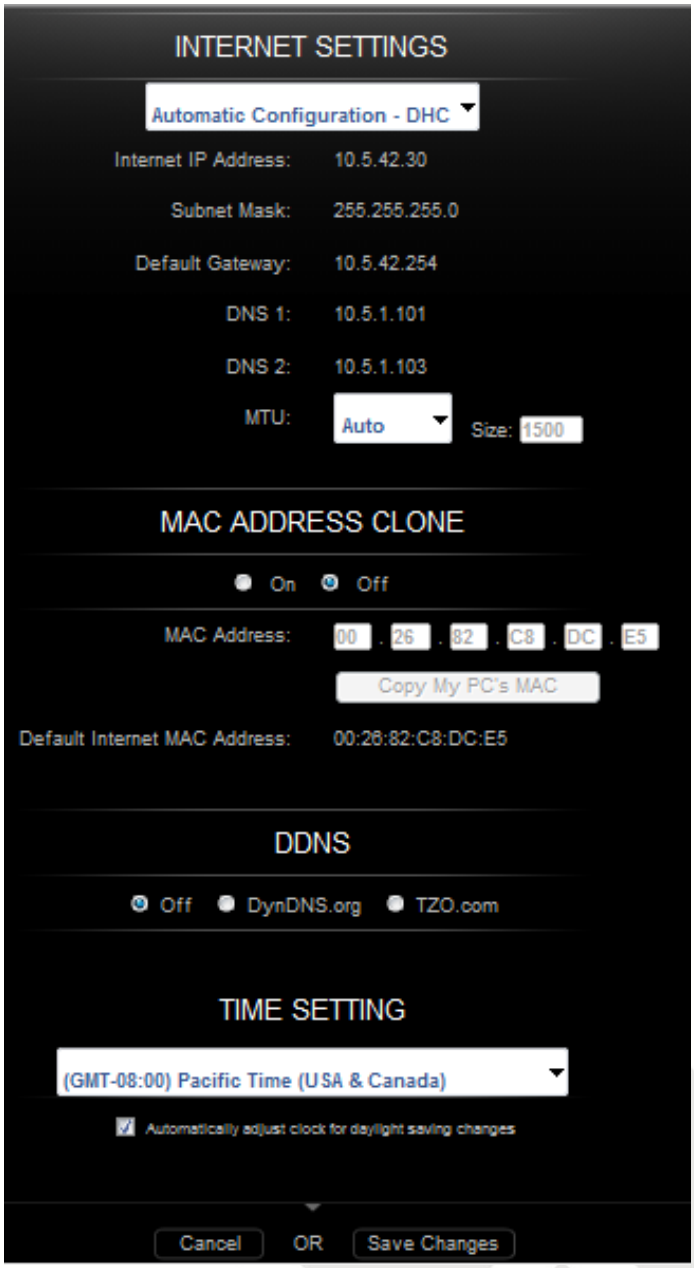
- Select **Automatic Configuration** – DHCP to have the router set the Internet settings automatically (recommended).
- Select **Static IP** to manually assign a permanent public IP address to the router.
- Select **PPPoE** if the router is connected using a DSL line that requires PPPoE (For more details, contact the ISP). Enter the PPPoE user name and password.

Internet IP Address: This is the router's public IP address. Contact the ISP to get the IP Address to enter in the spaces provided.

Subnet Mask: This is the router's Subnet Mask, as seen by other users on the Internet (including the ISP). Do not change the Subnet Mask unless there is a specific reason to do so. Contact the ISP to get the Subnet Mask to enter in the spaces provided.

Default Gateway: This is the ISP server's IP address. Contact the ISP to get the Gateway Address to enter in the spaces provided.

DNS 1 - 2: A Domain Name Server (DNS) is a server on the Internet that translates URLs into IP addresses. If Static IP is selected from the Configuration drop-down box, then the ISP needs to be contacted to get at least one DNS (Domain Name System) Server IP Address to enter in the spaces provided.



MTU: MTU is the Maximum Transmission Unit and specifies the largest packet size permitted for Internet transmission. Select **Manual** to manually enter the largest packet size that is transmitted or select Auto to have the router select the best MTU for the Internet connection.

MAC ADDRESS CLONE: Every computer hardware device, including the network adapter of the computer, has a unique number called a MAC address. Some ISPs require this MAC address to be registered with them in order to access the Internet. In order to avoid re-registering the MAC address with the ISP, assign the MAC address currently registered with the ISP to the router with the MAC Address Clone feature.

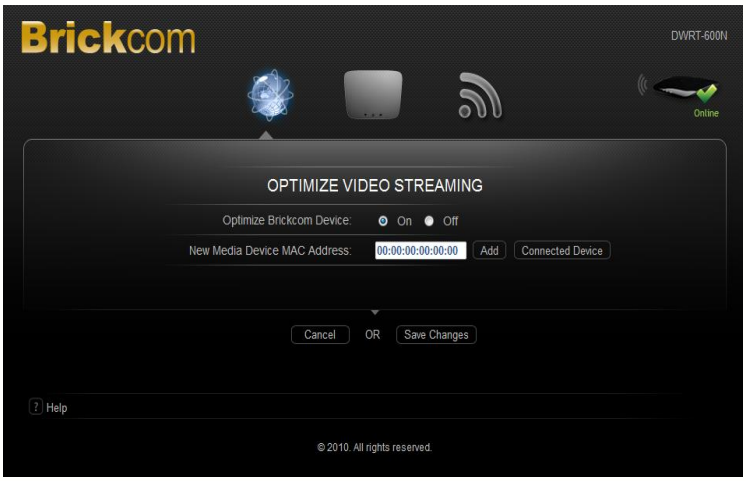
- **On/Off:** Select **On** to enable MAC Address cloning or **Off** to disable MAC Address cloning.
- **MAC Address:** Enter the MAC Address registered with the ISP.
- **Clone My PC's MAC:** Click this button to clone the MAC address of the computer being used.

DDNS: DDNS lets users assign a fixed host and domain name to a dynamic Internet IP address. It is useful when hosting a unique website, FTP server, or other server behind the router. First sign up for DDNS service with a DDNS service provider (for example www.dyndns.org or www.TZO.com) and then select the corresponding option. Select **Off to disable this** feature.

TIME SETTING: Select the desired time zone from this drop-down menu. Select the checkbox to automatically adjust for daylight saving time.

Optimize Video Streaming

Select **On** to enable automatic optimized video streaming of Brickcom IP cameras. To add other non-Brickcom devices to the list:

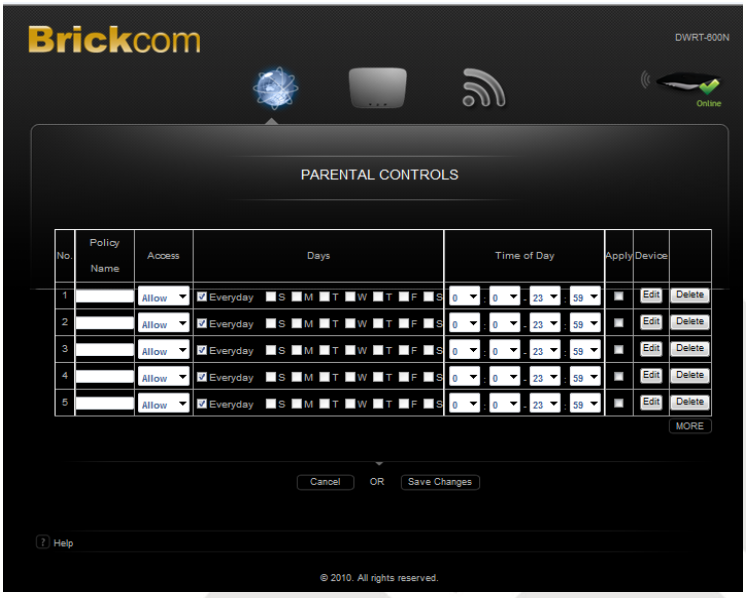


1. Enter their MAC address in the New Media Device MAC Address field and then click **Add**.
2. Click **Connected Device** and selecting the device from the list.

Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.

Parental Controls

The router allows users to control when the computer or device can access the Internet. Select **On** to enable parental control settings or **Off** to disable parental settings. To set policy and access time:



1. Click **Advanced**. A new menu will be displayed showing the advanced options available for the Parental Controls.
2. Enter a unique policy name.
3. Choose whether to **Deny** or **Allow** Internet for this policy.
4. Check Everyday or individual days to deny or allow Internet access.
5. Select the start time and end time using the drop down box. The hour is in 24 hour format (e.g. 13:00 equals 1:00pm).
6. Check the **Apply** checkbox to enable the Parental Control policy.
7. Click **Edit** and select from a list of computers to block or allow access.

8. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.

Other options:

- Click **Delete** to remove that policy.
- Click **More** to add more policies.

Internet Speed Test

Click **Begin Test** to test the speed of the Internet connection. Here is approximately what the results mean:

- 1Mb– 3Mb: Ideal for Standard Definition streaming
- 3Mb – 10Mb: Ideal for High Definition streaming
- 10Mb +: Ideal for Multiple High Definition streaming

Router Menu

The Router menu will display the router's current settings. The user can customize the router settings such as changing the LAN settings, updating the firmware, and accessing a connected USB device.

Router IP

The router's IP address, as seen from the local network, is displayed here. To makes changes, click **Advanced**. A new menu will be displayed showing the advanced options available for the Router IP. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.

Advanced Options

Router IP: This is the router's IP address as it appears on the local network.
Subnet Mask: This is the router's Subnet Mask.
URL Address: This is the URL of the GUI.
DHCP Server: If there is already a DHCP server on the network or to disable the router's DHCP server, select **Off** (it is **On** by default). The remaining DHCP features will be unavailable.
DHCP Reservation: Select to assign a fixed local IP address to a MAC address. A new window will open.

- To automatically add a client, select **Select Clients from DHCP Tables**, click **Select** next to the desired client, and then click **Add Clients**.
- To manually add a client and assign it an IP address, select **Manually Add Client** from the drop-down box and then enter the Client Name, IP address, and MAC address.

Click **Add** to add the IP address.

- To remove a client from the list, click **Remove** next to the client to remove it.

Start IP Address: Enter a value for the DHCP server to start with when issuing IP addresses. Because the router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253.

Maximum Number of Users: Enter the maximum number of computers that can be assigned an IP address by the DHCP server. The default is 50 and cannot exceed 155.

IP Address Range: This displays the range based on the Start IP address and the Maximum Number of Users selected.

Client Lease Time: This is the amount of time a network user will be allowed to be connected to (or "lease") the router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be connected to this dynamic IP address. The default is 0 minutes, which means one day. When time expires, the user will be automatically assigned a new dynamic IP address.

Static DNS 1-3: The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Contact the ISP to get at least one DNS Server IP Address to enter in the spaces provided. Up to two DNS Server IP Addresses can be entered. The router will use these for quicker access to functioning DNS servers.

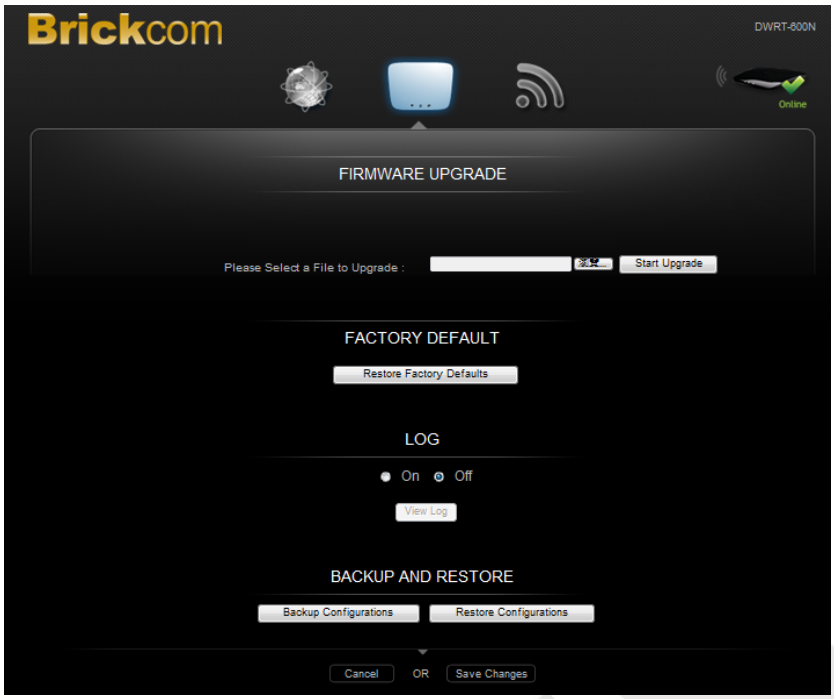
WINS: The Windows Internet Naming Service (WINS) manages each computer's interaction with the Internet. If using a WINS server, enter that server's IP Address here. Otherwise, leave these spaces blank.

Firmware Version

The router's current firmware version is displayed here. To makes changes, click **Advanced**. A new menu will be displayed showing the advanced options available for the Firmware Version. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.

Firmware Upgrade

1. Click **Check Latest Firmware**. If new firmware is available, a link will be displayed above the button.
2. Click the link to download the firmware to the computer.
3. Click **Browse** and locate the firmware file downloaded to the computer.
4. Click **Start Upgrade**.



Caution: Do not upgrade the router's firmware unless you are experiencing problems with your router or the new firmware has a feature you want to use.

Factory Default

Select this option to return the router to factory default settings. All settings that have been changed, including the login username and password, will be replaced by the factory default settings.

Log

The router keeps track of all traffic for the Internet connection. Select **On** to start monitoring traffic between the Internet and the network, otherwise leave it set to **Off**. Select **View Log** to view the log data.

Backup and Restore

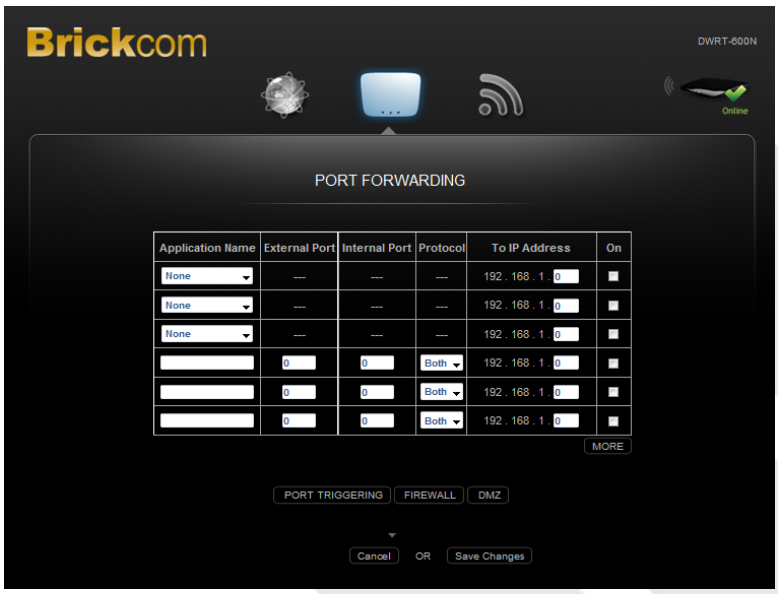
Select **Backup Configurations** to save the router's current configuration, allowing the user to restore it later if the settings are lost or changed. Follow the onscreen instructions to back up the configuration.
Select **Restore Configurations** to restore the router to a saved configuration. Follow the onscreen instructions to restore the configuration.

Firewall

A firewall can filter out various types of unwanted traffic on the local network. The firewall is set to **On** by default. Select **Off** to disable firewall protection. To makes changes, click Advanced. A new menu will be displayed showing the advanced options available for the Firewall setting.

Port Forwarding

Port Forwarding allows the user to customize port services for common applications. When users send these types of requests to the network via the Internet, the router will forward those requests to the appropriate servers (computers). Before using forwarding, the user should assign static IP addresses to the designated servers. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.



Application Name: Select a pre-configured application, or enter a unique name (up to 12 characters).

External Port: Enter the external port numbers.

Internal Port: Enter the internal port numbers.

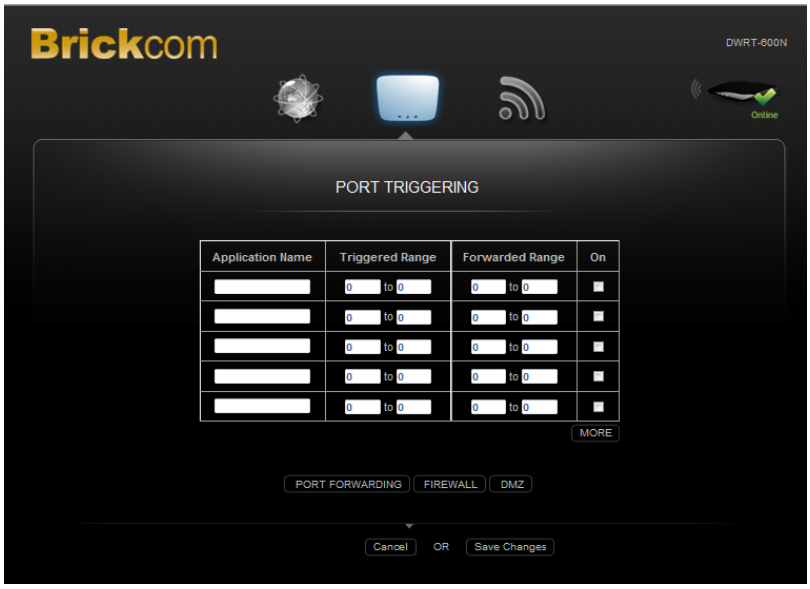
Protocol: Select the protocol used for this application, either **TCP** or **UDP**.

To IP Address: For each application, enter the IP address of the computer that should receive the requests.

On: For each application, select **On** to enable port forwarding.

Click **MORE** to add more applications.

Port Triggering



Port Triggering allows users to watch outgoing data for specific port numbers. The router remembers the IP address of the computer that sends the matching data, so when the requested data returns through the router, the data is pulled back to the correct computer. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.

Application Name: Enter a unique name for the trigger (up to 12 characters).

Triggered Range: Enter the **Start** and **End** port numbers of the Triggered Range. Check with the Internet application documentation for the port number(s) needed.

Forward Range: Enter the **Start** and **End** port numbers of the Forwarded Range. Check with the Internet application documentation for the port number(s) needed.

On: For each application, select **On** to enable port triggering.

Click **MORE** to add more applications.

Firewall

Configure a firewall that can filter out various types of unwanted traffic on the router's local network.

SPI Firewall Protection: Select **Enable** to use firewall protection or **Disable** to turn off firewall protection.

Internet Filter:

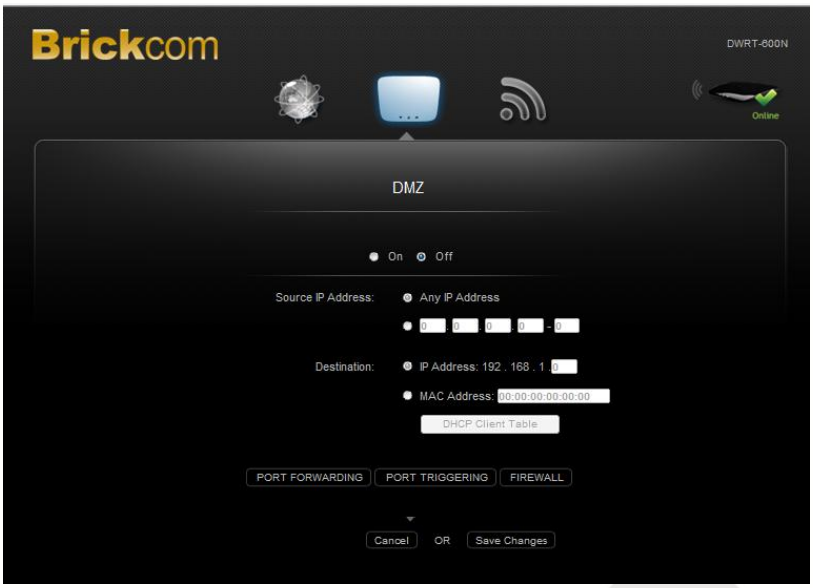
- **Filter Anonymous Internet Requests:** Select to make it more difficult for outside users to access the network.

- **Filter Multicast Multicasting:** Select to allow multiple transmissions to specific recipients at the same time. The router will allow IP multicast packets to be forwarded to the appropriate computers.
- **Filter Internet NAT Redirection:** Select to prevent a local computer from using a URL or Internet address to access the local server.
- **Filter IDENT (Port 113):** Select to keep port 113 from being scanned by devices outside of the local network.

Web Filter: Select **Proxy**, **Java**, **ActiveX**, and **Cookies** to filter those web protocols. The user can select as many options as desired to be filtered.

DMZ

DMZ allows one network computer to be exposed to the Internet for activities such as Internet gaming and videoconferencing. DMZ hosting forwards all the ports at the same time to one computer. Port Forwarding is more secure because the user selects specific ports to open, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet. Disable the DHCP client function of the computer whose port is being forwarded and assign it a new static IP address assigned because its IP address may change when using the DHCP function. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.



On/Off: Select **On** to allow computers on the Internet to access a local computer.

Source IP Address: Select **Any IP Address** or manually enter a specific source IP address of the computer to allow it to access from the Internet.

Destination: Select **IP Address** or **MAC Address** and enter the IP address of MAC address of the local computer to expose it.

DHCP Client Table: Select **DHCP Client Table** to view computers and other devices that have been assigned IP addresses by the router. To copy the MAC address of a computer to the DMZ screen, click **Select**.

Router Auto Login

The router is set to automatically login to the GUI. Select **Off** to prevent the router from automatically logging in and then click **Advanced** to set a user name and password. A new menu will be displayed showing the advanced options available for the Router Auto Login setting. Click **Save Changes** to keep any changes made to the router settings or click **Cancel** to cancel changes.

WEB ACCESS

Username and Router Password: Create a user name and password that must be entered before the GUI will open. Re-enter the password for confirmation. Select the **Show Password** checkbox to see the password instead. The user will now be prompted to enter the username and password each time the GUI opens. If the user forgets the username or password, press and *hold the reset button on the back of the router for 10 seconds to restore the router to default settings.

Access via: HTTP is the standard communications protocol used on the Internet and is the default option. Select **HTTPS** to encrypt data for increased security.

Access via Wireless: Select **On** to allow access to the GUI via a wireless connection. Select **Off** to disable access, especially if using the router in a public domain and guests have access to the wireless connection.

REMOTE ACCESS

Remote Management: To access the router remotely from the Internet, select **On**. This is set to **Off** by default.

Access Via: Select HTTP or HTTPS communications protocols for remote access from the Internet.

Remote Upgrade: Select **On** to be able to upgrade the firmware remotely from the Internet.

This is set to **Off** by default.

Allowed Remote IP Address: Select **Any IP Address** or manually enter an Internet IP address to allow remote access to the web-based utility from the Internet.

Remote Management Port: Enter the port number that will provide outside access to the router's web-based utility.

USB Network Media

The router's USB port connects to a USB storage device, so the user can access the files from any computer on the network. All of the files on the storage device are shared with all of the computers on the network. See Accessing USB Storage for more information on accessing the USB storage device.

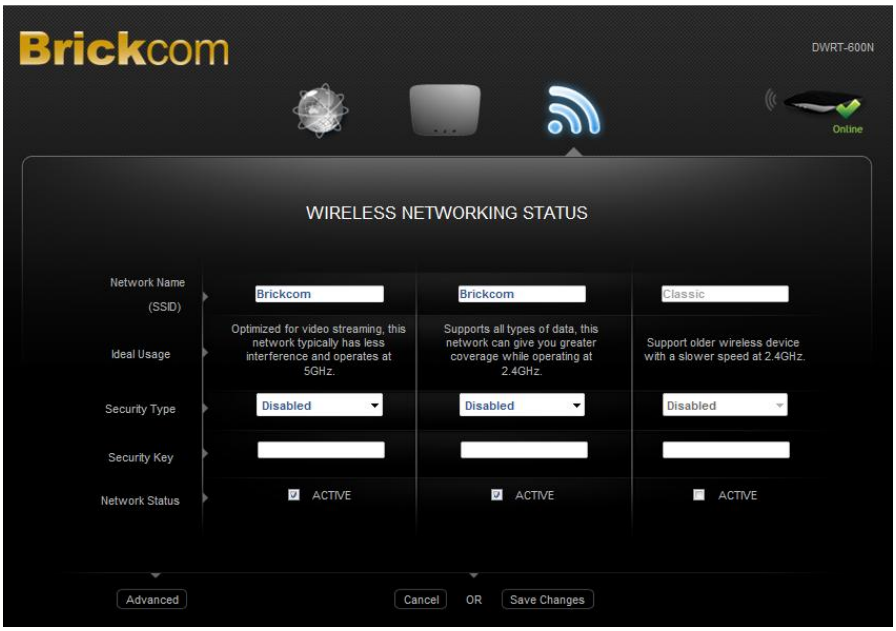
Brickcom Network Camera Site Survey List

The router is able to automatically detect Brickcom network cameras which are in range of the network. Click **Camera Scan** to survey to surrounding network for available Brickcom cameras. When the survey list is displayed, click **View** to automatically open the camera's web GUI.

Note: This function is only able to detect Brickcom network cameras. Other models are not supported.

Restart Router

Click **Restart Route**r to do a software restart of the router.



Wireless Menu

The current wireless settings will be displayed. Select **Advanced** to make changes to the wireless network settings. Select **EDIT SETTINGS** to change the Network Name (SSID), Security Type, Security Key, or Network Status. Select **WPS** to set up the wireless devices using WI-FI Protected Setup.

Edit Settings

Network Name(SSID)

Each wireless network has a unique name or SSID. The three wireless networks have default names which can be customized. If the user changes the name, consider using something unique to make sure it is not the same as other wireless networks that the router may detect in the area. Do not use personal information that can be visible to other users in the area searching for wireless networks.

Security Type

Select from **WPA2 Personal, WPA Personal, WEP 128bit**, or **WEP 64bit**. See the Security Mode Chart above for more information.

Security Key

Enter a new security key that users must enter to gain access to the wireless network. The key must be between 8 and 63 characters.

Network Status

Check the box to keep the network available in the list of available wireless networks or

uncheck it to disable it and remove it from the list of wireless networks.

WPS (Wi-Fi Protected Setup)

Using WPS, there are three ways to connect devices which support WPS to the router. Use the method that applies to the device being configured.

Push Button Method

Use this method if the device being configured has a WPS button.

1. Press the WPS button on the device being configured.
2. Click the **WPS** button on the GUI. A Success message will be displayed after the connection is successfully made.
3. Click Back to return to the main menu.

Device Pin Method

Use this method if device being configured has a WPS Setup PIN number.

1. Enter the PIN number from the device being configured in the field on this screen.
2. Click the **Sync** button. A Success message will be displayed after the connection is successfully made.
3. Click Back to return to the main menu.

Router Pin Method

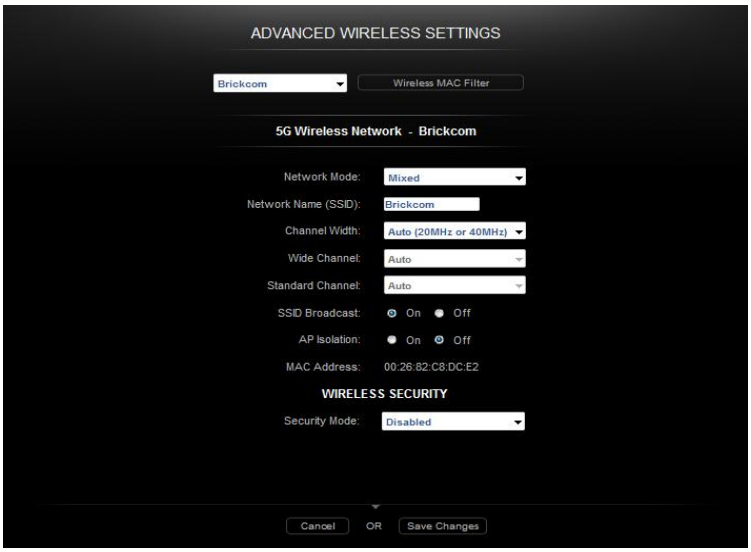
Use this method if the client device asks for the router's PIN number.
Enter the PIN number listed on this screen and on the product label. The wireless device will connect to the router using that PIN.

Advanced

A new menu will be displayed showing the advanced options available for the Advanced Wireless Settings. Choose a Network Name from the drop down list to change the settings for that network.

Wireless MAC Filter

Enter MAC addresses in the spaces provided to prevent or permit wireless devices with those addresses from accessing the wireless network. Click **Wireless Client List** to add MAC addresses by choosing them from a list of clients detected by the router. Click **MORE** to add more addresses.



Network Settings

Network Mode

- **5 GHz:** Select the wireless mode used by the network. Choose from **Disabled, Mixed, Wireless-A Only**, or **Wireless-N Only**.
- **2.4 GHz:** Select the wireless mode used by the network. Choose from **Disabled, Mixed, Wireless-G Only, Wireless-B Only**, or **Wireless-BGN**.

Network Name (SSID): Each wireless network has a unique name or SSID. The three wireless networks have default names which can customize. When changing the network's name, consider using something unique to make sure it is not the same as other wireless networks that the router may detect in the area. Do not use personal information that can be visible to other users in the area searching for wireless networks.

Channel Width

- **5 GHz:** Select **Auto** (20MHz or 40MHz) for best performance in a network using Wireless-A and Wireless-N (5 GHz) devices. Select **40MHz** only for a channel width of 40 MHz and select **20MHz** only for a channel width of 20 MHz.

- **2.4 GHz:** Select **Auto** (20MHz or 40MHz) for best performance in a network using Wireless-B, Wireless-G and Wireless-N (2.4 GHz) devices. Select **40MHz** only for a channel width of 40 MHz and select **20MHz** only for a channel width of 20 MHz.

Wide Channel

- **5 GHz:** Select **40MHz** only or **Auto** (20MHz or 40MHz) to have this setting be available for the primary Wireless-N (5GHz) channel. Select **Auto** if unsure about which channel to select.
- **2.4 GHz:** Select **40MHz** only or **Auto** (20MHz or 40MHz) to have this setting be available for the primary Wireless-N (2.4GHz) channel. Select **Auto** if unsure about which channel to select.

Standard Channel

- **5 GHz:** Select the channel for Wireless-A and Wireless-N (5GHz) networking. If **40MHz** only or **Auto** (20MHz or 40MHz) for Channel Width is selected, then the Standard Channel will be a secondary channel for Wireless-N (5GHz). Select **Auto** if unsure about which channel to select.
- **2.4 GHz:** Select the channel for Wireless-B, Wireless-G, and Wireless-N (2.4GHz) networking. If **40MHz** only or **Auto** (20MHz or 40MHz) is selected for Channel Width, then the Standard Channel will be a secondary channel for Wireless-N (2.4GHz). Select **Auto** if unsure about which channel to select.

SSID Broadcast: Hide the network name (SSID) so people who are not on the network cannot see it in their list of available networks.

AP Isolation: This isolates all wireless clients and wireless devices on the network from each other. Wireless devices will be able to communicate with the router but not with each other.

Wireless Security

Security Mode: Choose from **WEP, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS**, and **Disabled**.

Use the highest level of encryption supported by the network equipment.

Security Type	Description	Level of Security
WPA	**W**i-Fi **P**rotected **A**ccess	WPA/WPA2 is more secure than WEP, because WPA/WPA2 uses dynamic key encryption.
WEP	**W**ired **E**quivalent **P**rivacy	WEP may be the only option available on some older devices that do not support WPA.
RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice	Only use when a RADIUS server is connected to the router.

Encryption: Choose from **TKIP** and **AES** to select an encryption method.

Passphrase: Enter a new passphrase that is between 8 and 63 characters.

Key Renewal: Enter a Key Renewal period that tells the router how often it should change the encryption keys. The default Key

Renewal period is 3,600 seconds.

Wireless Security Information

Wireless networking, like any radio signal that travels through the air, can be intercepted by other devices. Here is how to protect the information that travels over the wireless network:

1. **Change the default wireless network name (SSID)**

   The name of the wireless network is called a Service Set Identifier (SSID) and was set by the factory. The router has three SSIDs (see Features for information about the SSIDs). Consider changing the network name to something unique to make sure it is not the same as other wireless networks that the router may detect in the area. Do not use personal information because others with will be able to see that when searching for a wireless network.

2. **Set a username and password**

   When setting up the router for the first time, no username or password is assigned to the router. To keep the router safe from hackers, set a username and password. See Router Auto Login for information on setting a username and password.

3. **Hide the Router's Network Name (SSID)**

   Hide the network name (SSID) so people who are not on the network cannot see it in their list of available networks. To hide the SSID:

   a. Select the **Wireless** menu option.
   b. Click **Advanced**.
   c. Select the **Off** button next to SSID Broadcast.
   d. Click **Save Changes**.

General Network Security Guidelines

- Password-protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without the user's consent and/or knowledge.

Additional Security Tips

- Keep the router away from exterior walls and windows.
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.