Bountiful WiFi

User Manual

http://www.BountifulWiFi.com

Printed in the United States of America
Published by Bountiful WiFi
707 W. 700 S. Suite 202A
Woods Cross, UT 84087
info@BountifulWiFi.com
Tel: 801-296-5970
Fax: 801-294-9965

Document version 1.2.0.060201

Table of Contents

1 Welcome

1.1 Introduction

Thank you for purchasing the Bountiful WiFi Router. The Router offers WiFi coverage with twice as much range as competing products by providing the strongest signal over the largest area for reliable wireless networking in difficult environments.

1.2 Package contents

- Bountiful WiFi Router
- Power adapter
- Ethernet cable
- Antennas (2)
- Documentation CD
- Quick Start Guide

1.3 Minimum system requirements

- Ethernet network connection
- Computer with 802.11 b or g wireless capability
- Any operating system that supports 802.11 networking (Instructions are provided for Microsoft Windows 2000,Windows XP only)
- TCP/IP network protocol installed on each computer

1.4 Technical support

1.4.1 SELF HELP

To obtain answers to Router configuration questions, visit the Bountiful WiFi support page at this address:

http://www.BountifulWiFi.com

Help items are also available next to each option item in the configuration pages of the Bountiful WiFi Router Web interface. Enter

192.168.0.1 or xxx.xxx.xxx.254 (depending on configuration)

in the browser’s address text box, and click the help button next to any option item when the configuration screen appears.

1.4.2 BASIC SETUP SUPPORT

Contact the Router vendor if experiencing problems with:

- Installing and configuring Router
- Establishing a wireless connection to the Router
- Connecting to the internet

1.4.3 ADVANCED NETWORKING SUPPORT

If a wireless network has been set up and support is needed in one of the following areas:

- LAN support of multiple computers and peripherals
- Microsoft Windows Networking
- Microsoft Internet Connection Sharing (ICS)
- Advanced LAN configuration with multiple computers
- Wireless card installation, configuration, or troubleshooting
- Commercial firewall software configuration

Contact a system administrator, networking professional or manufacturer for the equipment requiring support.

We welcome any suggestions or feedback you may have regarding Bountiful WiFi products or this manual. Please send comments to support@bountifulwifi.com.

1.4.4 CONTACT INFORMATION

Corporate address:	Bountiful WiFi 707 W. 700 S. Suite 202A Woods Cross, UT 84087
Phone:	801-296-5970
Fax:	801-294-9965
Toll-free:	877-247-6378
Support e-mail:	support@BountifulWiFi.com
Sales e-mail:	sales@BountifulWiFi.com
Information e-mail:	info@BountifulWiFi.com
Corporate URL:	http://www.BountifulWiFi.com

1.5 Features

2.4GHz WLAN radio compliance	• IEEE Std 802.11g-2003 • IEEE Std 802.11b-1999
WLAN security options	• WEP 64 or 128-bit key • WEP 802.1x/RADIUS authentication • WPA 802.1x/RADIUS authentication & key management • WPA Pre-Shared Key (PSK) mode
Broadband gateway functions:	• IP/Ethernet (not PPPoE connections) • Port Forwarding • WAN port MAC adjustment • DNS proxy, Dynamic DNS • DHCP server, DHCP/BOOTP client • NAT/NAPT, Virtual server, DMZ hosting • VLAN support • WiFi multimedia
Security mechanisms:	• Layer 2/3/4 access control • Layer 2/3/4 firewall & packet filtering
Ethernet switch:	• 10/100Mbps auto negotiation • Half/Full duplex auto negotiation • MDI/MDI-X cross-over auto detection
Network Address Translation (NAT) protocol support	• FTP • ICMP • VPN pass-through (PPTP/IPSec), • MSN messenger, • Windows messenger, • Netmeeting, • H.323, etc.
Management interfaces	• Easy setup wizard • Browser based configuration pages • Command line telnet interface
Firmware upgrade	• Browser based firmware upload utility

1.6 General Specifications

Standards	• IEEE Std 802.11g-2003 IEEE802.3x • IEEE Std 802.11b-1999 IEEE802.1x • IEEE 802.3 WPA version II • IEEE 802.3u
Number of channels	• 11 Channels (2.412-2.462GHz) US
Interfaces	• 1 – WAN port, 10/100 Mbps RJ45 with auto MDI • 4 – LAN ports, 10/100 Mbps RJ45 with auto MDI • 1 – WLAN port, 802.11b/g
Antenna Ports	• Separate TX and RX antennas minimize interference Note: when using remote antennas; connect separate RX and TX antennas.
Transmission Rate	• Ethernet: 10/100 Mbps • WLAN: 1, 2, 5.5, 6, 11, 12, 18, 24, 36, 48, 54Mbps
Modulation	• OFDM, CCK, DQPSK, DBPSK
Protocols	• TCP/IP • IPX/SPX • NetBEUI
LED Indication	• System: Power/Fault • WAN: Link/Activity • LAN: Link/Activity • WLAN: Link/Activity
TX Power	• OFDM: 28.4 dBm • CCK: 29.14 dBm
Cabling	• Ethernet: Cat5 or better

1.7 Environmental Specifications

Humidity	• 10%-90%, Non-condensing
Dimension	• 8.5 x 6.6 x 1.75 inches (21.6 x 16.8 x 4.4 cm)
Temperature Operating	• 0ºC – 35ºC
Storage	• -20ºC – 70ºC

2 Overview

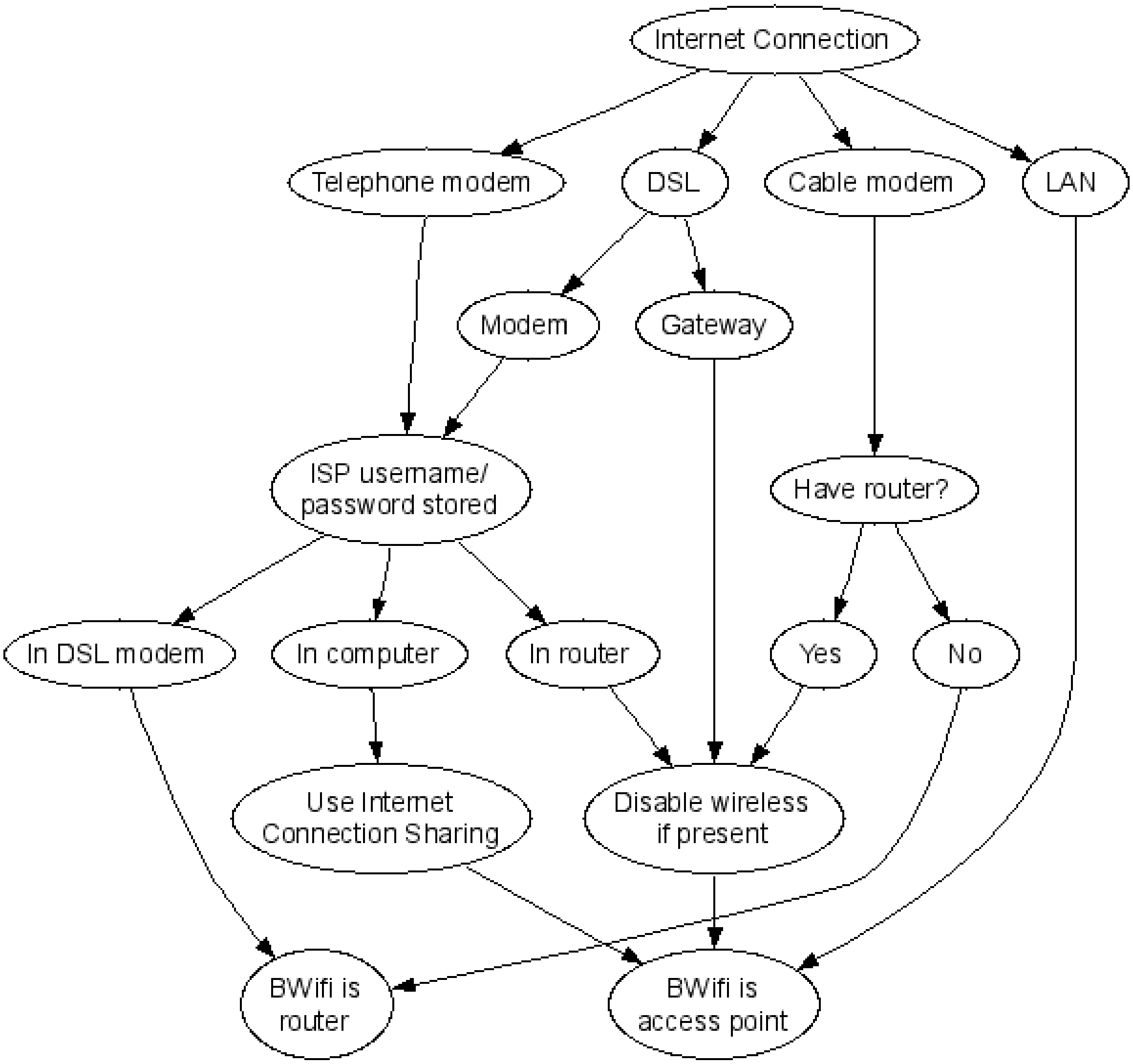
2.1 Network terminology

- **WAN** – Wide Area Network. A computer network that spans a relatively large geographical area. Computers connected to a wide-area network are often connected through public networks, such as the telephone system. The largest WAN in existence is the Internet.
- **LAN** – Local Area Network. A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.
- **WLAN** – Wireless local area network that uses radio waves as its carrier: the last link with the users is wireless, to give a network connection to all users in the surrounding area. Areas may range from a single room to an entire campus. The backbone network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network.
- **IP Address** – Group of numbers that uniquely identifies each device on a network. The IP Addresses used commonly on the Internet use four groups of numbers separated by decimals. Each group can have any value from 0 to 255 but the combination must be unique on the network that it connects with.
- **MAC Address** – Media Access Control address; also called Ethernet Address is a unique 48-bit hexadecimal identifier attached to most forms of networking equipment. This address is usually assigned to a device when it is manufactured.
- **ISP** – Internet Service Provider such as cable company, telephone company or any company that provides Internet access.
- **Modem** – Device that connects to the line that supplies Internet access, i.e. cable, DSL, telephone or T1 line. Some modem connections are manually setup with a static IP and others use auto configuration with dynamic IP.
- **Router** – Device that allows multiple computers to access a single internet connection through wired and/or wireless networks. This device typically connects one WAN to one or more LAN ports. It allows multiple computers on the LAN to share one WAN connection.
- **Access point** – Device that serves as the WiFi base station allowing wireless access to the wired network. Used to extend the wired LAN onto the WLAN.
- **Switch/Hub** – Device that provides a common connection point for network cables.
- **Gateway** – Device that combines the functionality of Modem/Router and sometimes Switch/Hub into one device. This device provides an interface between the LAN computers and the WAN network. LAN computers must be configured to send all packets destined for the WAN to the Gateway device.
- **DNS Server** – Also called Name Server. Server that can help resolve a domain name (eg. www.BountifulWiFi.com) into the IP Address (eg. 64.90.199.115) of the computer that will respond to requests for that domain name. Each computer on an IP network must know the address of two DNS servers (primary and secondary) so they can lookup addresses for domain names.
- **BWiFi** – Bountiful WiFi Router which can be configured to have the functionality of an Access Point, Router and/or Switch/Hub.

2.2 Network configuration

The Bountiful WiFi Router functions as either a router or as an access point. A router connects LAN computers to the WAN. An access point connects WLAN computers to the LAN.

Compare the existing network (without the BWiFi device) to the following diagram to identify which configuration to use for the BWiFi in the network. Start by selecting the type of Internet Connection used in the network:

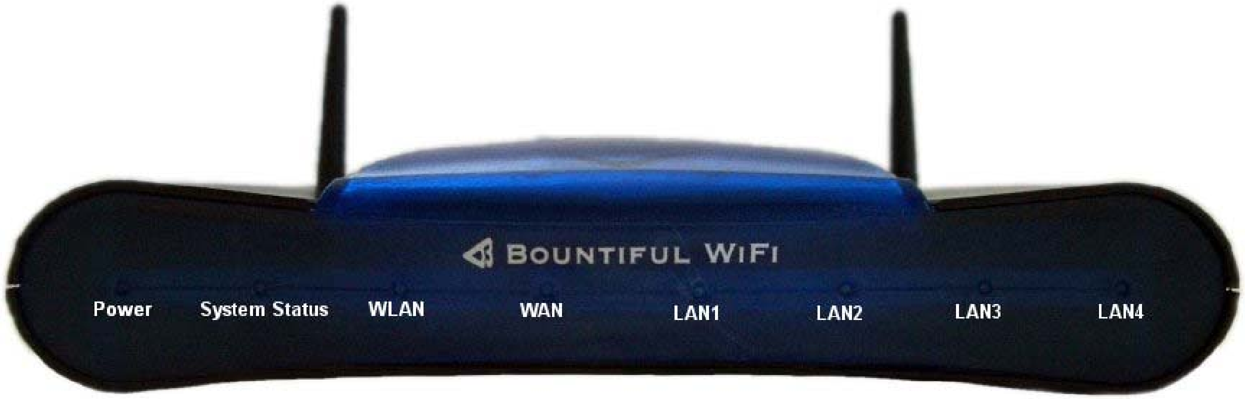


Example: If the existing network uses a DSL Modem for the Internet Connection with the ISP username and password stored in an existing wireless router; the wireless capability should be disabled in the existing router using that routers configuration pages and the BWiFi will be attached to the router and function as a wireless access point. The existing router will continue to provide DHCP and routing services to the network.

Determine whether to use the BWiFi device as an access point or router and reference the Quick Start Guide and/or Configuration Pages sections for network configuration help.

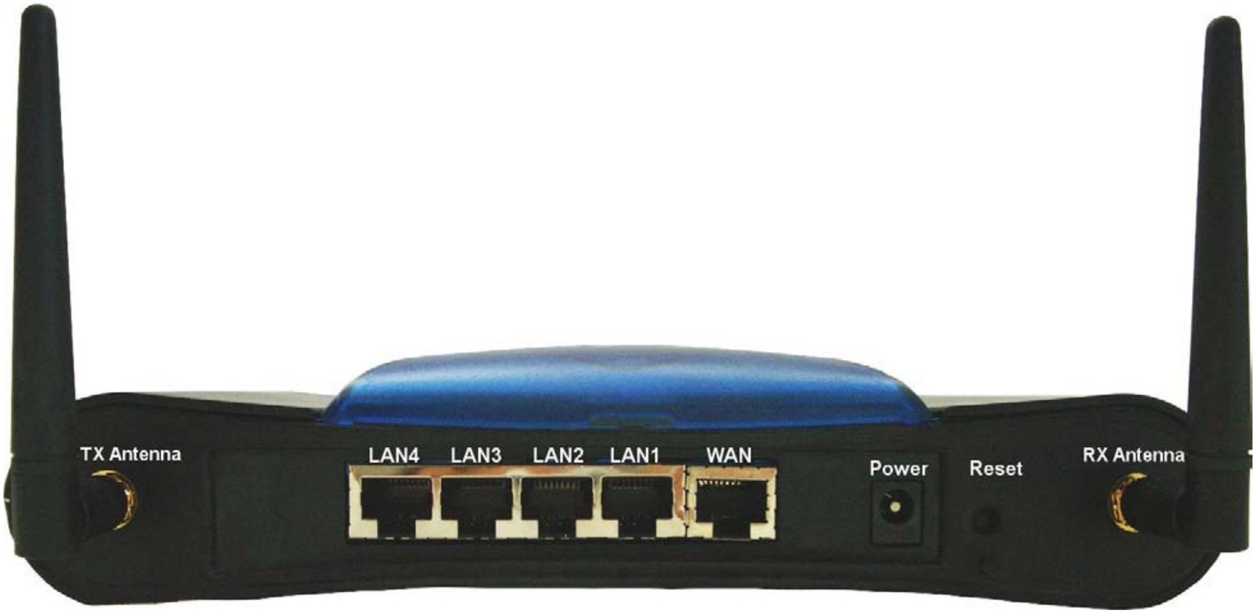
2.3 Router Lights, Switches and Ports

2.3.1 ROUTER LIGHTS AND SWITCHES



- **Power** – The Power light displays the Gateway's current status. If the Power light glows steadily green, the Gateway is receiving power and fully operational.
- **System Status** – The System Status light is solid green when the Router is operating normally and the wireless network is enabled. When the System Status light is flashing, the Gateway is initializing. When the System Status light is off, and the Power light is on, the wireless network has been disabled.
- **WLAN** –The WLAN light blinks steadily when the device is operating normally. The WLAN light flashes rapidly when data is being sent to the wireless network.
- **WAN** – The WAN light is illuminated when there is an active network cable connected to the WAN port. When it flashes, data is being sent via the WAN port.
- **LAN** – The LAN lights are illuminated when there is an active network cable connected to the LAN port. When a LAN light flashes, data is being sent via the corresponding LAN port.

2.3.2 ROUTER PORTS AND SWITCHES



- **TX Antenna** – Wireless network signals are transmitted through the TX Antenna port. Connect the transmit antenna here. Separate antenna ports provide the best performance by isolating the high power transmit signal and the low noise receive wireless signals to minimize interference.

  Warning: Never apply power to the Bountiful WiFi device with the TX Antenna disconnected as the device may be permanently damaged.

- **LAN** – Use any of the four LAN ports to connect to the network when operating as an access point. Also use LAN ports to connect additional computers to the network.
- **WAN** – Use this port to connect to the network connection when using the routing capability (DHCP server enabled) of the Bountiful WiFi device. When using the device as an access point, do NOT connect a network connection to the WAN port, use the LAN port instead. See section 2.2.
- **Power** – 5 volt 4 Amp DC power input
- **RX Antenna** – Wireless network signals are received through the RX Antenna port. Connect the receive antenna here. Separate antenna ports provide the best performance by isolating the high power transmit signal and the low noise receive wireless signals to minimize interference.
- **Reset** – Depressing the reset switch for one or two seconds will power cycle the Router (similar to unplugging and then plugging in the Router's power cord). To restore the Gateway's factory default settings, depress and hold the Reset Switch for approximately 30 seconds (until the System Status light turns off). When the System Status light flashes off, the reset process has started, wait approximately 30 seconds for the BWiFi to re-initialize.

  Warning: Do not unplug the power cord from the Gateway during the reset process. Doing so may result in permanent damage to the Gateway.

  Note: When connecting outdoor / remote antennas it is necessary to connect separate antenna cables and separate antennas to the TX and RX antenna ports. Using a combiner/splitter device to connect both ports to one antenna will result in a significant decrease in performance.

3 Quick Start Guide

3.1 Introduction

This Quick Start Guide will help you set up a simple wireless network. These basic instructions are for setting up a wireless connection with no security enabled; troubleshooting tip 5 explains how to enable security. For advanced help and other options refer to Configuration Pages section of this manual.

Requirements:

- A computer running Windows 2000 or Windows XP that is already connected to the internet.
- The Bountiful WiFi Quick Start Kit:

Router

Power Adapter

Network Cable

Antennas

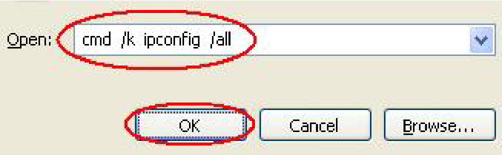
3.2 Gather network information

Using an Internet connected computer, click on the Windows Start Button → Run…

Type

cmd /k ipconfig /all

Into the window and click **OK**



Open: cmd /k ipconfig /all

Write the network information in the spaces provided.

The three letter reference code below the names will be used to indicate where to use these numbers later on.

IP Address: ______ . ______ . ______ . ______
(IP1)

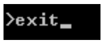
Subnet Mask: ______ . ______ . ______ . ______
(SM1)

Default Gateway: ______ . ______ . ______ . ______
(DG1)

DNS Servers: (1) ______ . ______ . ______ . ______
(NS1)

DNS Servers: (2) ______ . ______ . ______ . ______
(NS2)

Type Exit in the command window and press **Enter** on the keyboard to close the window.



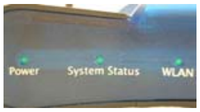
```
>exit_
```

3.3 Connect router for configuration

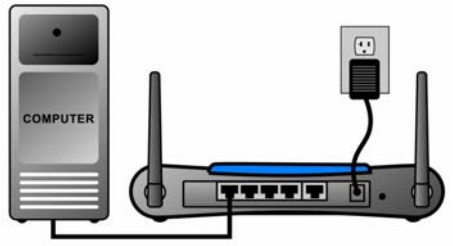
Remove the Router from the Quick Start Kit. Remove two antennas from the slot in the Quick Start Kit packaging. Attach the two antennas to the Router.

Connect the **Router** to a power supply and plug it into a wall outlet.

NOTE: Sound of cooling fans is normal.



Confirm the **Power** and **System Status** lights on the **Router** are solid green and that the **WLAN** light is flashing steadily.



Connect the **LAN4** port of the **Router** using a **Network Cable** to the network port on the computer

Confirm that the **LAN4** light on the Router is green. This may take a few seconds.

Note: If the **LAN4** light does NOT turn green, make sure the **Network Cable** is properly connected on both ends.

3.4 Configure Router

Understand basic network terminology.

- Modem – Device that connects to the line that supplies internet access, i.e. cable, DSL line, telephone line. Some modems are setup manually with a static IP and others have auto configuration with dynamic IP.
- Router – Device that allows multiple computers to access a single internet connection through wired and/or wireless networks.
- Access point – Device that serves as the WiFi base station allowing wireless access to the wired network.
- Switch/Hub – Device that provides a common connection point for network cables.
- Gateway – Device that combines the functionality of Modem/Router and sometimes Switch/Hub into one device.
- BWiFi – Bountiful WiFi Router which can be configured to have the functionality of an Access Point, Router and/or Switch/Hub, see section 2.2.

Identify current network scenario. Which of the following scenarios best matches the way the network is configured before adding the **Bountiful WiFi Router**:

A : Modem → PC

B : Gateway → PC

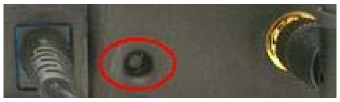
C : Gateway/Switch/Hub → PC(s)

D : Modem → Router(wired or wireless)/Switch/Hub → PC(s)

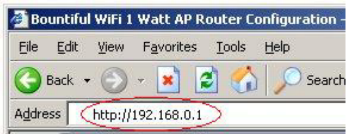
The letter corresponding to the existing network will be used throughout the rest of the guide to reference configuration scenarios **A**, **B**, **C** and **D**.

NOTE: Do not change any cable connections at this time.

Press and hold Reset button for 30 seconds. Wait another 30 seconds for device to reset.

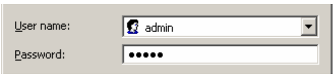


Open a web browser, i.e. FireFox or Internet Explorer. In the address bar type **http://192.168.0.1**; press **Enter** on the keyboard.


Bountiful WiFi 1 Watt AP Router Configuration -

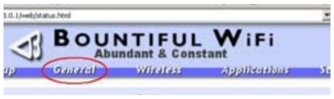
Address http://192.168.0.1

Log in to the Router using User name: **admin** and Password: **admin**.


User name: admin

Password: •••••

The “Status” screen appears; select the “General” tab.



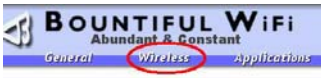
Configure the following parameters on the **General** tab according to the Scenario that matches the network configuration: (help is available by pressing button near each item)

Configuration Scenario	**Router**	**Access Point**
General tab settings		
Internet Connection Type:	Static (Manual)	DHCP (Automatic)
Static IP Address:	IP1* – xxx.xxx.xxx.xxx	
Static IP Netmask:	SM1 – xxx.xxx.xxx.xxx	
Gateway:	DG1 – xxx.xxx.xxx.xxx	
Name Server 1:	NS1 – xxx.xxx.xxx.xxx	
Name Server 2:	NS2 – xxx.xxx.xxx.xxx	
Local IP Address:	192.168.0.1	IP1 – xxx.xxx.xxx.**254**
Local Netmask:	255.255.255.0	SM1 – xxx.xxx.xxx.xxx
DHCP Server:	Enable	Disable

* Use information collected in section 3.2, “Gather Network Information”. If ISP uses dynamic configuration, select “Internet Connection Type: DHCP (Automatic” and leave static configuration fields blank.

Scroll to the bottom of the screen and press Submit.

Choose NOT to reboot the **Router** at this time. Select the “Wireless” tab.



Configure the following parameters on the **Wireless** tab. All configuration scenarios use the same wireless settings:

Network Scenario	**Router or Access Point**
Wireless tab settings	
Wireless SSID	Choose a wireless network ID
Wireless Authentication	Open System

NOTE: After initially testing the system it is recommended that you enable wireless authentication to protect the network and computers from other wireless users in the area. For help with this see Solution 5 at the end of this guide.

Scroll to the bottom of the screen and press Submit.

Reboot **Router**.

that require a reboot. Ple

If the DCHP Server was disabled in this section, the BWiFi device must be connected to the network in order to communicate with the device after the reboot. Also, note any connections must be made to the correct IP address which may be different than the default of “192.168.0.1”,

3.5 Connect Router for operation

Install the **Router** in a location that is central to where the wireless computer(s) will be used.

Use the **Network Cable** to connect the **Router** to the network following the correct Network Scenario:

A : Modem → BWiFi → PC

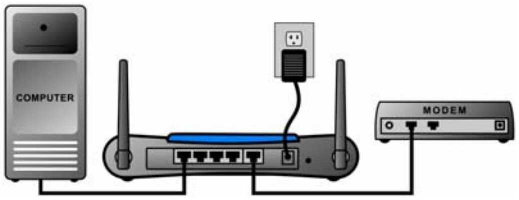
B : Gateway → BWiFi → PC

C : Gateway/Switch/Hub → BWiFi → PC(s)

D : Modem → Router/Switch/Hub → BWiFi → PC(s)

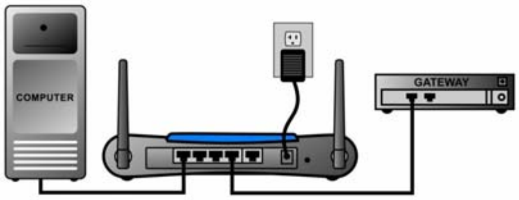
Note: In scenario **A** the Modem should be connected to the **WAN port** of the BWiFi **Router**. In all other scenarios, connect to a **LAN** port on the BWiFi **Router**. Any wired PC’s can be connected to **LAN ports** 1 – 4. In scenario **D** disable any existing wireless network using router configuration pages, do NOT remove from system.

Connection diagram for Scenario **A**.



Connection diagram for Scenario **B**.

Scenarios **C** & **D** also use this diagram and connect a router or gateway to the LAN1 port (WAN port is NOT connected).



Install network adapters in each of the PC's that will be connecting wirelessly. Follow the directions for the particular wireless adapter that you are installing. The Bountiful WiFi Router will communicate with any combination of wireless PCMCIA adapters, USB adapters or PCI adapters in the client PC's.

3.6 Testing Connection

You are now ready to test for an Internet connection. On each computer, open the web browser to access a website (example: www.bountifulwifi.com). If you are able to access the Internet, the installation for that computer is successful.

Note: For any computer that is unable to access the Internet, follow **Step 2** and then test for an Internet connection again.

In you have completed the appropriate steps above and you still do not have an Internet connection, you need to do a power cycle. Do this with the following steps:

1. Turn off the computer
2. Unplug the **Router**
3. Unplug the modem or gateway
4. Wait 30 seconds
5. Plug in the Modem
6. Plug in the **Router**
7. Turn on the computer

Check to see if you have an Internet connection again. If you still do not, go to **Troubleshooting**.

4 Configuration Pages

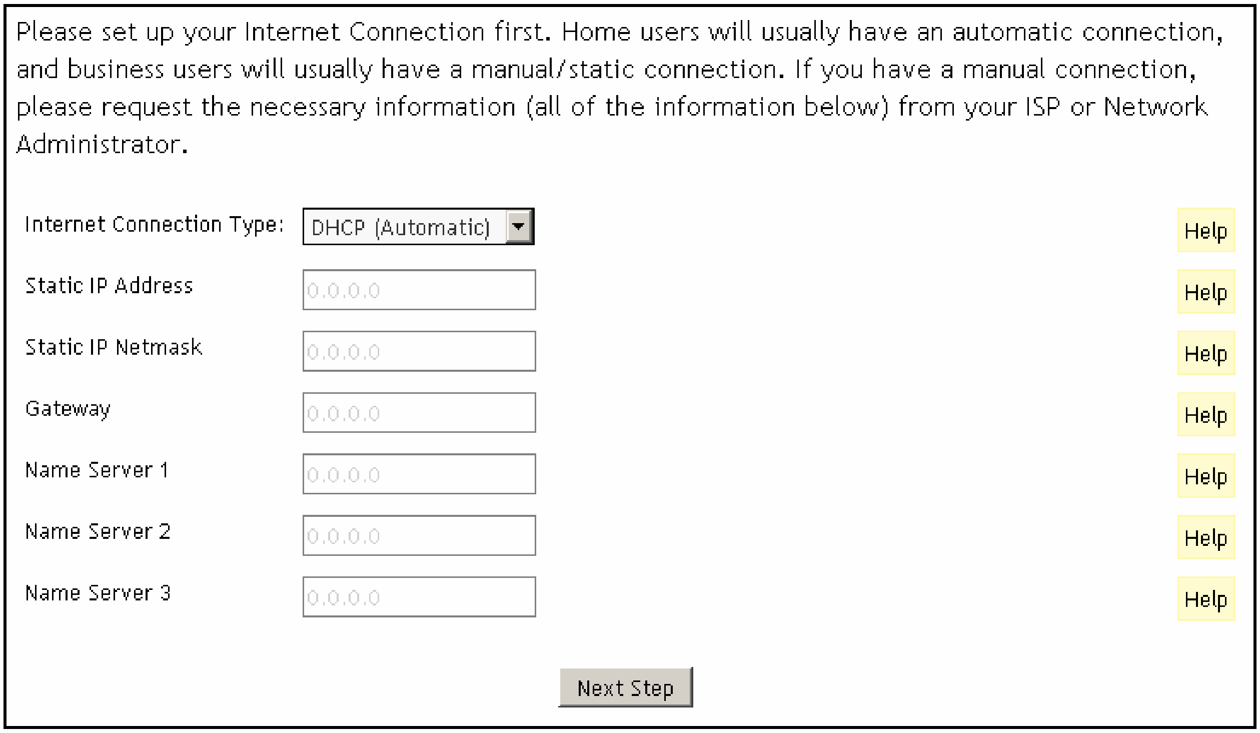
4.1 Quick Setup

The Bountiful WiFi router features a guided setup sequence that can be accessed by pressing the Quick Setup tab.

This section helps the user perform the basic setup tasks; there is a help button next to each option for additional information on any topic. All of the options available during the Quick Setup are also available on the General and Wireless tabs in the advanced configuration pages.

Simply fill in the appropriate information in the fields as you navigate through the Quick Step screens pressing next after each step. We also provide a cross reference for each screen to inform you about how to modify these settings outside of the Quick Setup. More detailed information for each item is available later in this manual under the more advanced section headings.

4.1.1 QUICK SETUP STEP 1

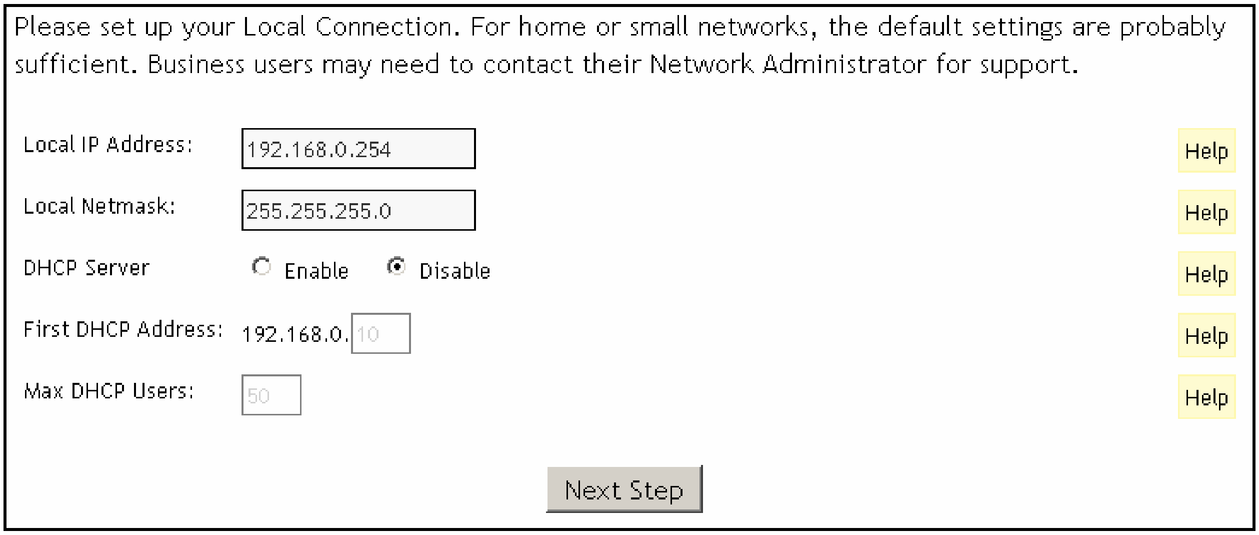


Please set up your Internet Connection first. Home users will usually have an automatic connection, and business users will usually have a manual/static connection. If you have a manual connection, please request the necessary information (all of the information below) from your ISP or Network Administrator.

Internet Connection Type:	DHCP (Automatic)	Help
Static IP Address	0.0.0.0	Help
Static IP Netmask	0.0.0.0	Help
Gateway	0.0.0.0	Help
Name Server 1	0.0.0.0	Help
Name Server 2	0.0.0.0	Help
Name Server 3	0.0.0.0	Help

- General tab – Internet Connection Setup

4.1.2 QUICK SETUP STEP 2

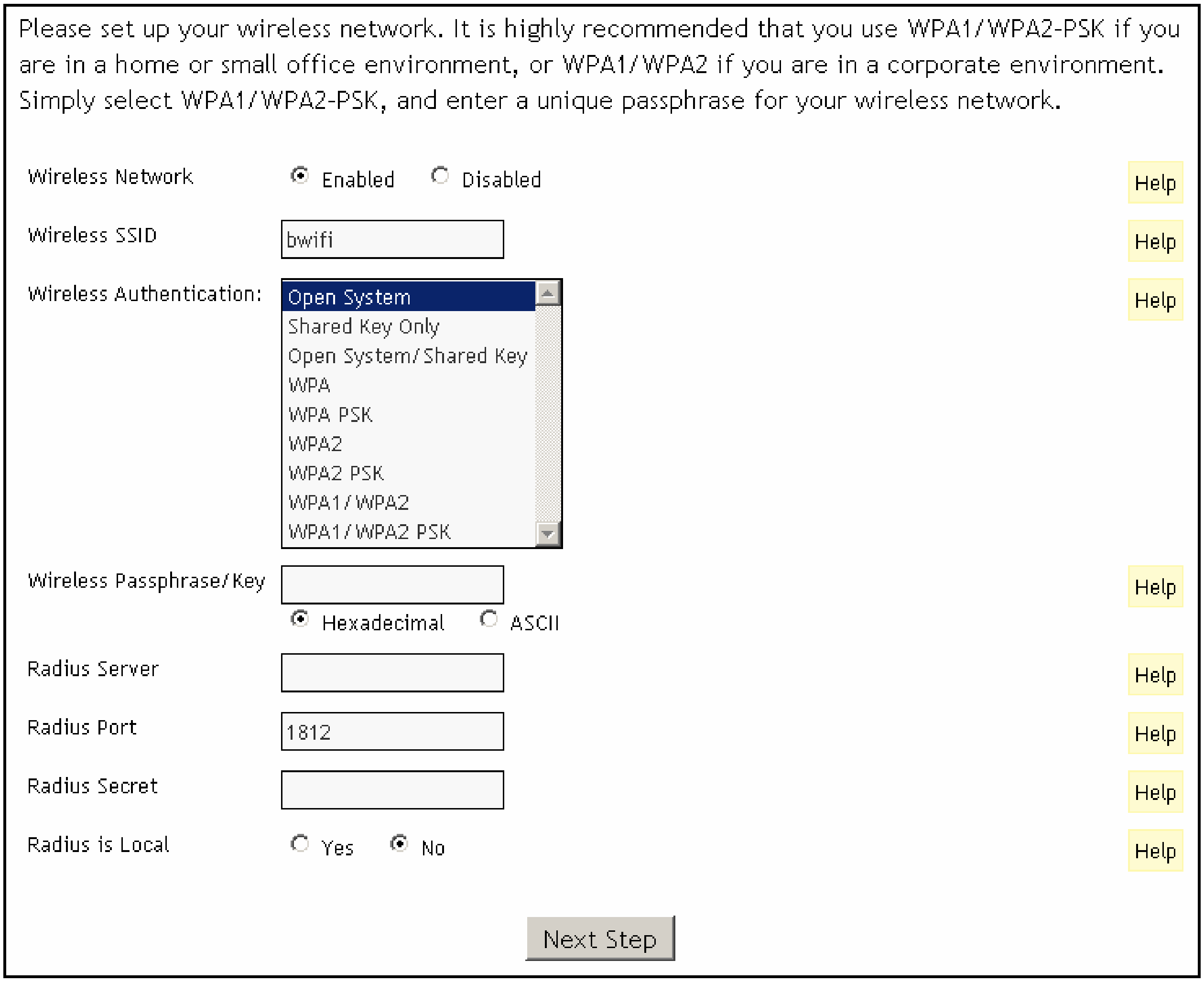


Please set up your Local Connection. For home or small networks, the default settings are probably sufficient. Business users may need to contact their Network Administrator for support.

Local IP Address:	192.168.0.254	Help
Local Netmask:	255.255.255.0	Help
DHCP Server	○ Enable ● Disable	Help
First DHCP Address:	192.168.0.10	Help
Max DHCP Users:	50	Help

- General – Local Connection (LAN)

4.1.3 QUICK SETUP STEP 3

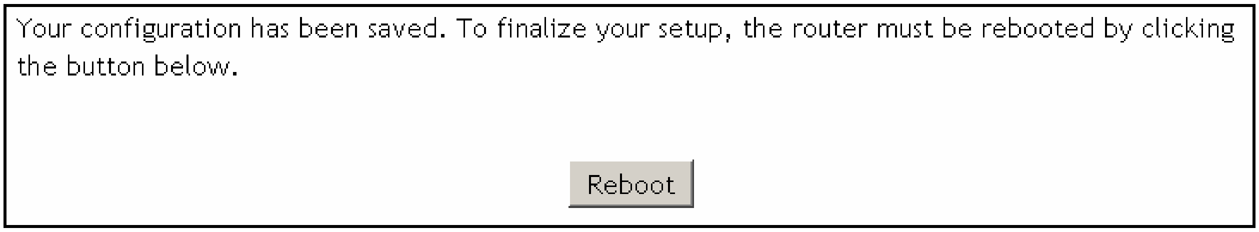


Please set up your wireless network. It is highly recommended that you use WPA1/WPA2-PSK if you are in a home or small office environment, or WPA1/WPA2 if you are in a corporate environment. Simply select WPA1/WPA2-PSK, and enter a unique passphrase for your wireless network.

Wireless Network	● Enabled ○ Disabled
Wireless SSID	bwifi
Wireless Authentication:	Open System Shared Key Only Open System/Shared Key WPA WPA PSK WPA2 WPA2 PSK WPA1/WPA2 WPA1/WPA2 PSK
Wireless Passphrase/Key	● Hexadecimal ○ ASCII
Radius Server	
Radius Port	1812
Radius Secret	
Radius is Local	○ Yes ● No

- Wireless – Wireless settings: Wireless Network, Wireless SSID
- Wireless – Authentication

4.1.4 QUICK SETUP STEP 4

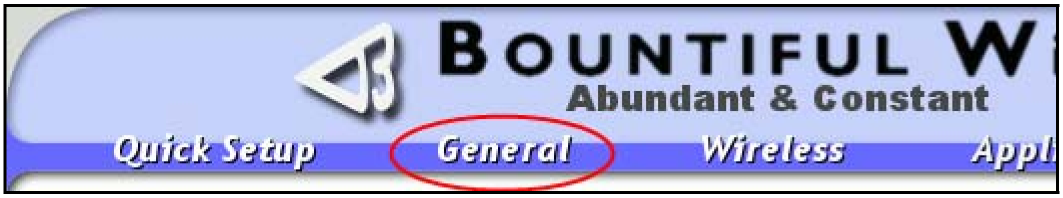


Your configuration has been saved. To finalize your setup, the router must be rebooted by clicking the button below.

- Reboot

4.2 General

None of the changes made on this page take effect until the Submit button at the bottom of this page is clicked and the BWiFi is rebooted.

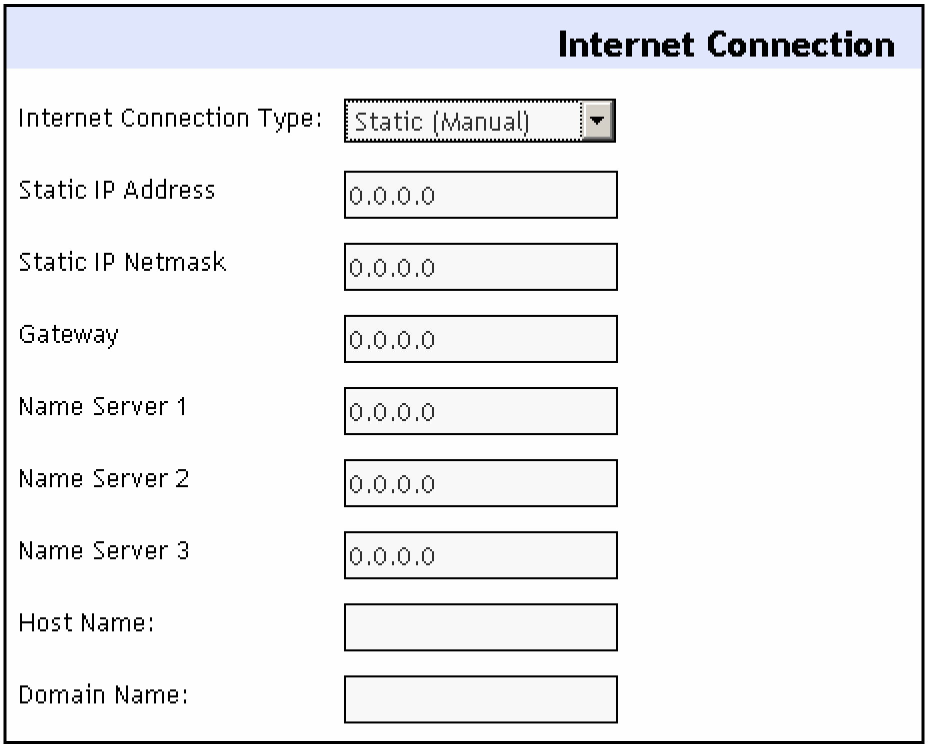


Some of the parameters below are discussed in the context of either access point or router configuration (see chapter 2).

4.3 General – Internet Connection

A router requires two IP addresses, one address for communication with the WAN network and a separate IP address for communication with the LAN network. Connect network cable from Internet modem to BWiFi Router WAN port. Select the behavior required by the Internet Service Provider (ISP). Contact the ISP for assistance if required. Recommended settings:

Configuration	Access point	Router
Internet Connection Section Settings		
Internet Connection Type	DHCP	Depends on ISP
Internet cable connection		
Connection port	LAN	WAN



Internet Connection

Internet Connection Type:	Static (Manual)
Static IP Address	0.0.0.0
Static IP Netmask	0.0.0.0
Gateway	0.0.0.0
Name Server 1	0.0.0.0
Name Server 2	0.0.0.0
Name Server 3	0.0.0.0
Host Name:	
Domain Name:	

4.3.1 DHCP (AUTOMATIC)

Choose this setting when the ISP automatically configures the IP address and other network information. When selected, the manual configuration fields are disabled.

4.3.2 STATIC (MANUAL)

Choose this setting when the ISP requires manual configuration of network information. When selected, the Static IP Address, Static IP Netmask, Gateway, Name Server 1 and Name Server 2 fields are required.

4.3.3 STATIC IP ADDRESS

Manually configure IP Address for WAN connection. This information is typically provided by ISP if required. Required for static configuration.

4.3.4 IP NETMASK

Manually configure IP Netmask for WAN connection, e.g. 255.255.255.0. This information is typically provided by ISP if required. Required for static configuration.

4.3.5 GATEWAY

Manually configure Gateway address. This is the address of the router or gateway the network accesses to connect to the internet. This information is typically provided by ISP if required. Required for static configuration.

4.3.6 NAME SERVER 1

Manually configure Name Server 1 (Primary DNS) address. This is the address of a primary server that can look up the IP address of Internet domain names. This information is typically provided by ISP if required. Required for static configuration.

4.3.7 NAME SERVER 2

Manually configure Name Server 2 (Secondary DNS) address. This is the address of a secondary server that can look up the IP address of Internet domain names. This information is typically provided by ISP if required. Required for static configuration.

4.3.8 NAME SERVER 3

Manually configure Name Server 3 address. This is the address of a server that can look up the IP address of Internet domain names. Optional for static configuration.

4.3.9 HOST NAME

A unique name used to identify the BWiFi on a network, e.g. “bwifi”. Use a host name to access the BWiFi configuration pages without using the IP address from the WAN network. The host name is not available on the LAN network. Optional for all configurations.

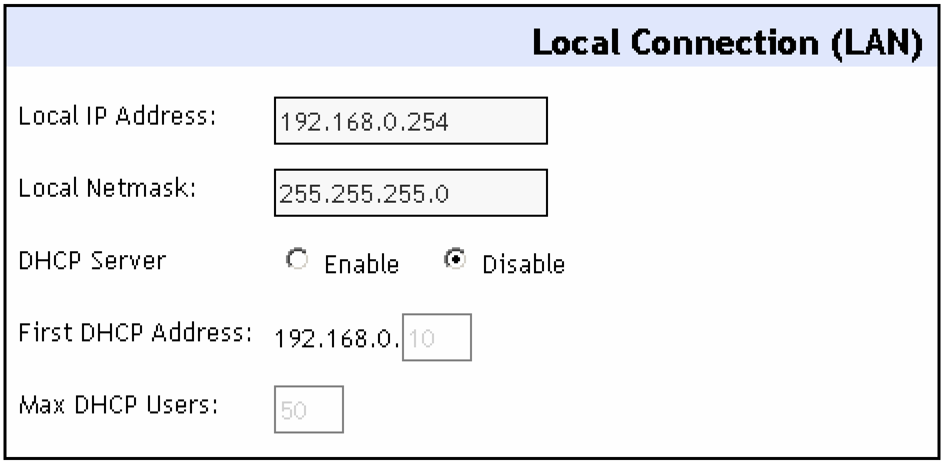
4.3.10 DOMAIN NAME

The unique name used to identify the local network, e.g. “thecompany.com”. Used in conjunction with the Host Name to uniquely identify a device on the network, e.g. bwifi.thecompany.com can be used to access BWiFi configuration pages from the WAN without typing the IP address directly. The domain name is not available on the LAN network. Optional for all configurations.

4.4 General – Local Connection (LAN)

Configure settings for LAN connection. Recommended settings:

Configuration	Access point	Router
Local IP Address	IP1 – xxx.xxx.xxx.254	192.168.0.1
Local Net Mask	SM1 – xxx.xxx.xxx.xxx	255.255.255.0
DHCP Server	Disable	Enable
First DHCP Address	n/a	10
Max DHCP Users	n/a	50



Local Connection (LAN)

Local IP Address:	192.168.0.254
Local Netmask:	255.255.255.0
DHCP Server	○ Enable ● Disable
First DHCP Address:	192.168.0.10
Max DHCP Users:	50

4.4.1 LOCAL IP ADDRESS

Specify the LAN IP Address for the local network. This address will be used to access the BWiFi configuration pages. Verify that this address is: unique (not duplicated on the network), in the same subnet as other machines on the network. Required for all configurations.

4.4.2 LOCAL NETMASK

Subnet mask for the local network i.e. “255.255.255.0”. The netmask specifies which number groups (separated by dots) in the IP address will be unique on the network. Number groups that correspond to a 255 in the netmask must match other network IP addresses exactly. Number groups that correspond to a 0 in the netmask must be unique when appended together. Typically only the fourth number group is 0. Required for all configurations.

4.4.3 DHCP SERVER

A DHCP server assigns IP addresses to other computers on the local network (LAN). Only one device on the network should be configured as DHCP server. Enable this option when a DHCP server does NOT already exist on the network.

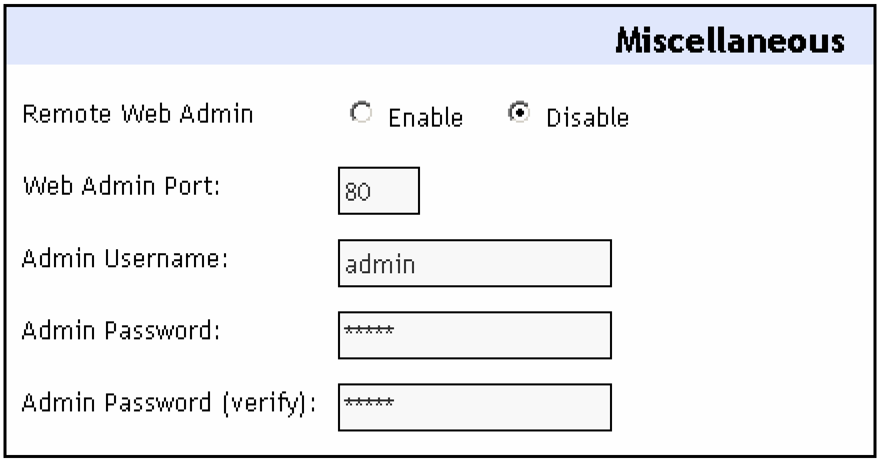
4.4.4 FIRST DHCP ADDRESS

Specify the first IP address to be assigned by the DHCP server. The DHCP server assigns incrementing IP addresses as additional devices join the network, i.e. a value of 10 results in the sequential assignment of xxx.xxx.xxx.10, xxx.xxx.xxx.11, and etc. to devices joining the network. Required when DHCP Server is enabled.

4.4.5 MAX DHCP USERS

Number of IP addresses the DHCP server is authorized to assign to network devices. Required when DHCP Server is enabled.

4.5 General – Miscellaneous



Miscellaneous

Remote Web Admin	○ Enable ● Disable
Web Admin Port:	80
Admin Username:	admin
Admin Password:	*****
Admin Password (verify):	*****

4.5.1 TELNET ADMIN

Enables administration via telnet. Command line interface not documented at this time. Use only when directed by technical support.

4.5.2 REMOTE WEB ADMIN

Enables router administration through the WAN port over the internet. This functionality could open the device and/or the network to malicious intrusion. Disable unless absolutely required.

4.5.3 WEB ADMIN PORT

TCP Port number to be used by the internal web server for Remote Web Administration. Default is port 80. A particular port is identified with an Internet socket address, which is the combination of an Internet host address and a port number. Required when Remote Web Admin is Enabled.

4.5.4 ADMIN PASSWORD

Change the password used to access the BWiFi configuration pages. Default is “admin”.

4.5.5 ADMIN PASSWORD (VERIFY)

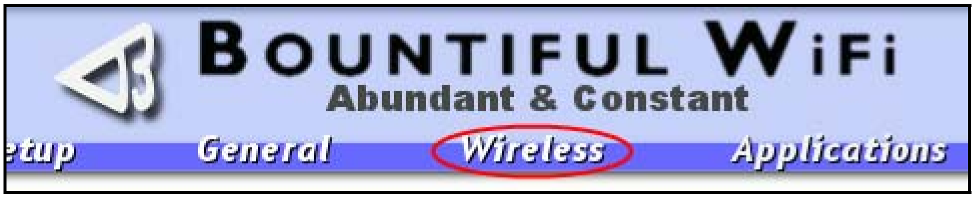
Enter the same password a second time to change the password used to access the BWiFi configuration pages.

4.5.6 SUBMIT BUTTON

None of the changes made on this page take effect until the Submit button is clicked and the BWiFi is rebooted.

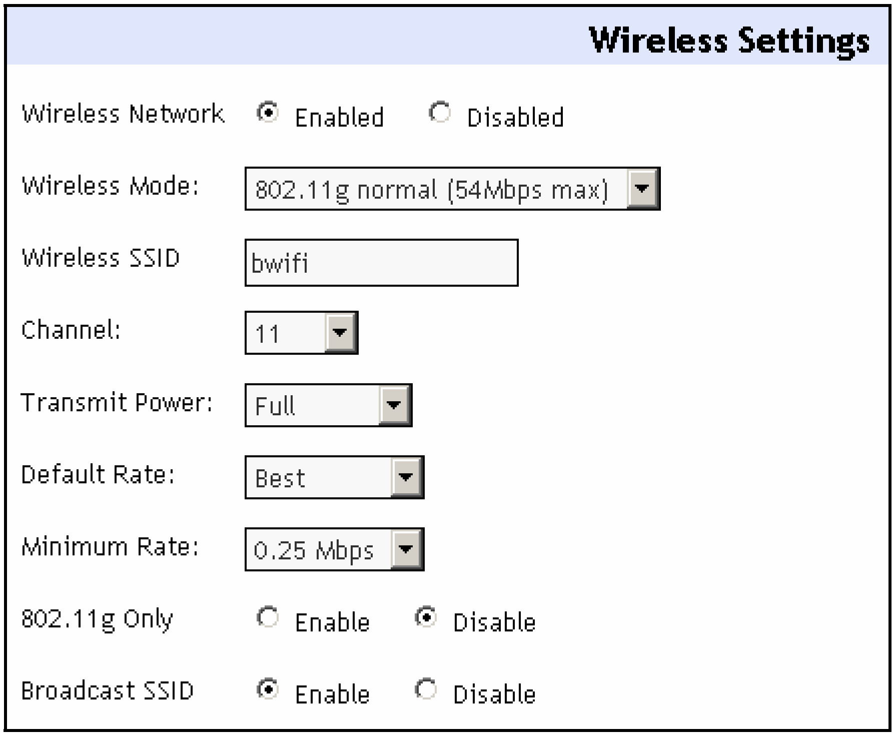
4.6 Wireless

Configure the wireless options of the Router.



4.7 Wireless – Wireless Settings

None of the changes made on this page take effect until the Submit button at the bottom of this page is clicked and the BWiFi is rebooted.



Wireless Settings

Wireless Network	● Enabled	○ Disabled
Wireless Mode:	802.11g normal (54Mbps max)	
Wireless SSID	bwifi	
Channel:	11	
Transmit Power:	Full	
Default Rate:	Best	
Minimum Rate:	0.25 Mbps	
802.11g Only	○ Enable	● Disable
Broadcast SSID	● Enable	○ Disable

4.7.1 WIRELESS NETWORK

Turns on/off your wireless network.

4.7.2 WIRELESS MODE

Sets wireless network mode – “G Mode” enables both 802.11b and g capability.

4.7.3 WIRELESS SSID

Wireless network SSID, or name of the wireless network.

4.7.4 CHANNEL

The channel selects which frequency is at the center of the 802.11 transmission. The center frequencies are spaced 5 Mhz apart, however, each channel is 22 Mhz wide so each channel overlaps several adjacent neighbors. For best results select channels that do not overlap when setting up multiple wireless networks in the same area, i.e. channels to 1 or 6 or 11 are non-overlapping.

Channel	Lower Frequency	Center Frequency	Upper Frequency
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

4.7.5 TRANSMIT POWER

Access Point Transmit Power. Set to full for best wireless network range. Each decrement lowers the output 3 db.

4.7.6 DEFAULT RATE

Wireless network rate. Set to best for fastest operation.

4.7.7 MINIMUM RATE

Minimum wireless network rate. Will only allow computers connecting at this rate or higher to connect to the network.

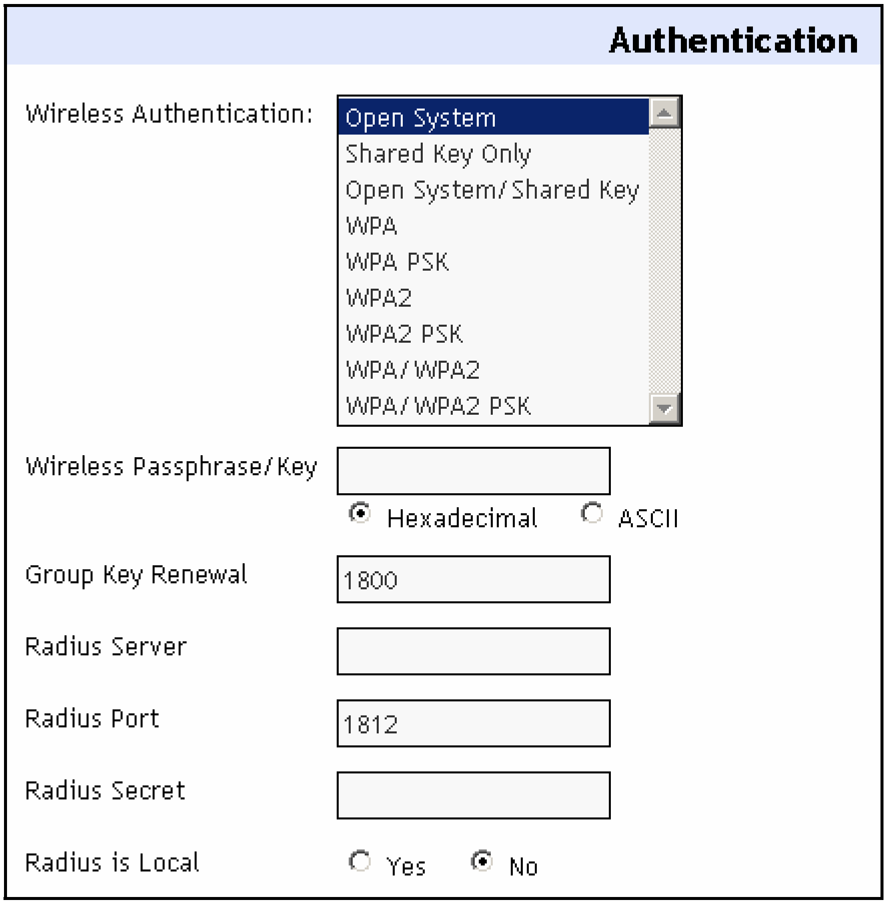
4.7.8 802.11G ONLY

Will only allow computers with 802.11g cards to connect.

4.7.9 BROADCAST SSID

Enable to allow easier access to this network. Disable to “hide” this wireless network from plain view to network scanners.

4.8 Wireless – Authentication



Authentication

Wireless Authentication:
- Open System
- Shared Key Only
- Open System/Shared Key
- WPA
- WPA PSK
- WPA2
- WPA2 PSK
- WPA/WPA2
- WPA/WPA2 PSK

Wireless Passphrase/Key

● Hexadecimal ○ ASCII

Group Key Renewal: 1800

Radius Server:

Radius Port: 1812

Radius Secret:

Radius is Local: ○ Yes ● No

4.8.1 WIRELESS AUTHENTICATION

Wireless Authentication method. Open and shared-key systems allow either WEP (low-grade) or no encryption. For smaller wireless networks without a RADIUS server, select WPA1 or WPA2 with a Private Shared Key (PSK). For corporate networks, select WPA1 or WPA2 without a PSK, and set up the RADIUS server.

WPA PSK and/or WPA2 PSK are used with clients/operating systems that support them to provide more security than WEP. WPA encryption is not supported by Windows 95, Windows 98, Windows ME, Windows 2000 or Windows XP service pack 1.

WPA and/or WPA2 are only used with radius servers.

4.8.2 WIRELESS PASSPHRASE/KEY HEXADECIMAL ASCII

For Open/Shared Key Systems: WEP Key. Key size is automatically determined by the length of your input.

For WPA: Private Shared Key ASCII/Hex entry does not apply to WPA PSKs.

For open system/shared key selection – a 5 character/byte key = 64 bit encryption – a 13 character/byte key = 128 bit encryption.

4.8.3 GROUP KEY RENEWAL

How often to renew wireless network group keys. Default value is 1800 seconds.

4.8.4 RADIUS SERVER

(For WPA non-PSK only) IP Address of the RADIUS Server.

4.8.5 RADIUS PORT

(For WPA non-PSK only) Port number of the RADIUS Server. Default is 1812.

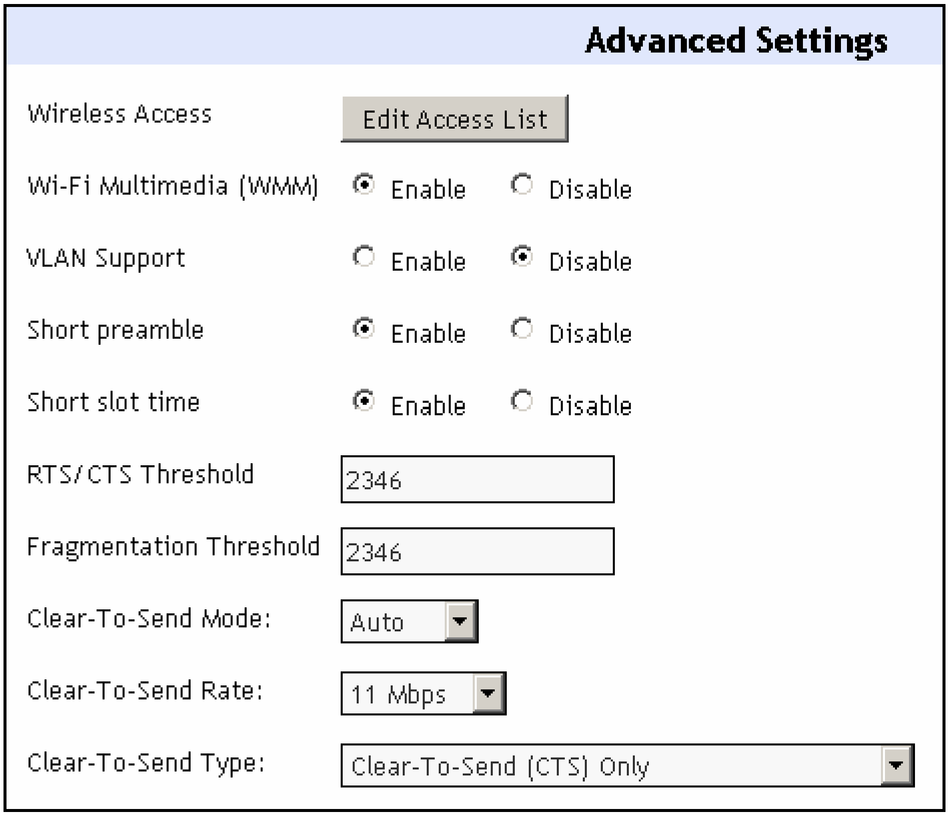
4.8.6 RADIUS SECRET

(For WPA non-PSK only) RADIUS Secret/Password.

4.8.7 RADIUS IS LOCAL YES NO

(For WPA non-PSK only) Enable if RADIUS server is connected via the LAN ports.

4.9 Wireless – Advanced Settings

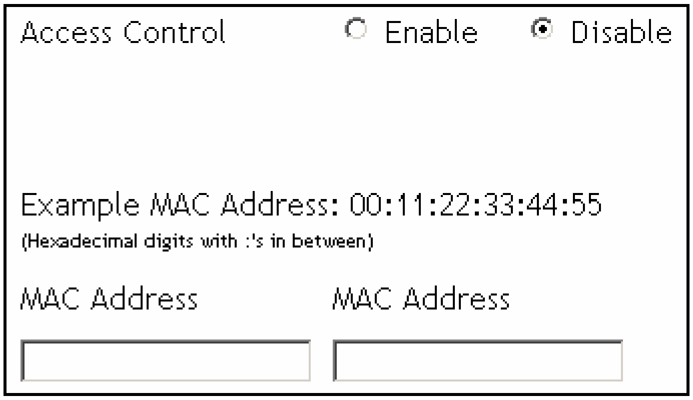


Advanced Settings

Wireless Access	Edit Access List	
Wi-Fi Multimedia (WMM)	● Enable	○ Disable
VLAN Support	○ Enable	● Disable
Short preamble	● Enable	○ Disable
Short slot time	● Enable	○ Disable
RTS/CTS Threshold	2346	
Fragmentation Threshold	2346	
Clear-To-Send Mode:	Auto	
Clear-To-Send Rate:	11 Mbps	
Clear-To-Send Type:	Clear-To-Send (CTS) Only	

4.9.1 WIRELESS ACCESS

Press this button to launch the Access Control dialog box. Scroll to the bottom of the dialog box and press submit to save any changes.



Access Control ○ Enable ● Disable

Example MAC Address: 00:11:22:33:44:55
(Hexadecimal digits with :'s in between)

MAC Address MAC Address

Access Control is disabled by default, allowing any wireless client to attempt to access the network. Wireless client(s) may still be required to supply a password to access the network depending on the wireless authentication settings.

When Access Control is enabled, enter up to 64 specific MAC addresses of devices that are allow to attempt connections to the wireless network. Any devices attempting to connect will be denied access if their MAC address was not previously entered into the BWiFi device. Wireless Authentication settings also apply after the MAC address is found in the table.

4.9.2 WI-FI MULTIMEDIA (WMM)

Enables WMM, which prioritizes some network traffic above other traffic (such as streaming audio/video, etc.). Wi-Fi Multimedia (WMM), also known as Wireless Multimedia Extensions (WME) is a Wi-Fi Alliance interpretability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

4.9.3 VLAN SUPPORT

Enable this option to prevents wireless computers on the network from communicating with each other. It is recommended that this option be enabled for WiFi hot-spots. The router creates a virtual LAN (VLAN) for each wireless user and does not allow users to ‘see’ each other on the network.

4.9.4 SHORT PREAMBLE

Allows packets with a short pre-amble on to the network.

4.9.5 SHORT SLOT TIME ENABLE DISABLE

Enables short slot time.

4.9.6 RTS/CTS THRESHOLD

Maximum time to wait for RTS/CTS. Ranges from 1 to 2346. Default is 2346.

4.9.7 FRAGMENTATION THRESHOLD

Maximum fragmentation value. Ranges from 256 to 2346. Default is 2346.

4.9.8 CTS MODE

Sets the wireless CTS mode. Default is Auto.

4.9.9 CTS RATE

Sets the wireless CTS rate. Default is 11 Mbps.

4.9.10 CTS TYPE

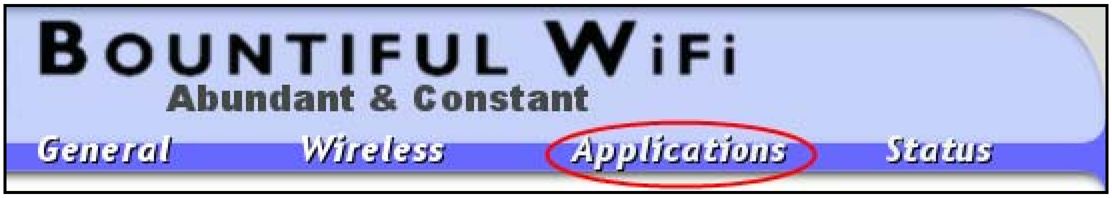
Set the wireless CTS type. Default is CTS-Only.

4.9.11 SUBMIT BUTTON

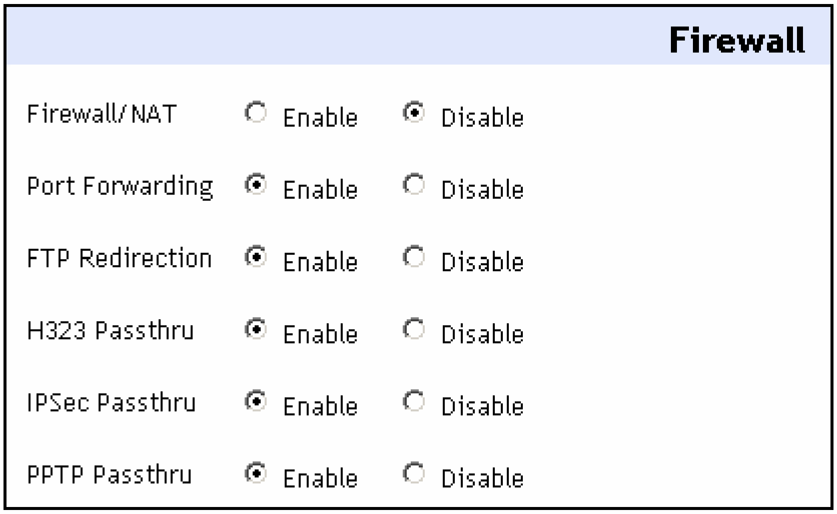
None of the changes made on this page take effect until the Submit button is clicked and the BWiFi is rebooted.

4.10 Applications

None of the changes made on this page take effect until the Submit button at the bottom of this page is clicked and the BWiFi is rebooted.



4.11 Applications – Firewall



Firewall

Firewall/ NAT	○ Enable	● Disable
Port Forwarding	● Enable	○ Disable
FTP Redirection	● Enable	○ Disable
H323 Passthru	● Enable	○ Disable
IPSec Passthru	● Enable	○ Disable
PPTP Passthru	● Enable	○ Disable

4.11.1 FIREWALL / NAT

Enables the Stateful Packet Inspection Firewall.

4.11.2 PORT FORWARDING

Enables port forwarding according to the Port Forwarding table.

4.11.3 FTP REDIRECTION

Allows you to establish File Transfer Protocol (FTP) connections from the inside network to the Internet.

4.11.4 H323 PASS THRU

Automatically configures and routes H323 streaming applications. The H.323 protocol is a standard for real-time voice and/or video conferencing over packet-based networks implemented in conferencing software such as NetMeeting.

4.11.5 IPSEC PASS THRU

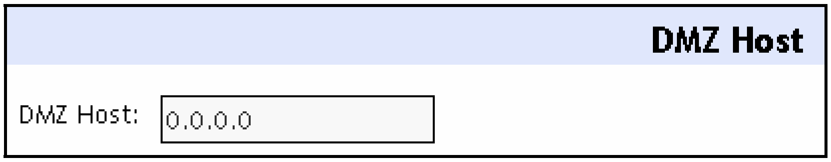
Automatically configures and routes IPSec connections. The IPSec protocol is used to create VPNs.

4.11.6 PPTP PASS THRU

Automatically configures and routes Point-to-Point Tunneling Protocol (PPTP) connections to support Virtual Private Networks (VPN).

4.12 Applications – DMZ Host

Forwards any incoming traffic (except those ports listed below) to a local computer, essentially placing the computer out on the WAN/Internet. Useful for some games, but should generally be avoided. Set to 0.0.0.0 or blank to disable.

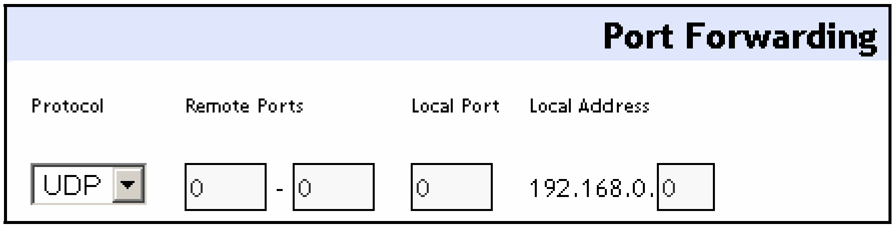


DMZ Host

DMZ Host: 0.0.0.0

4.13 Applications – Port Forwarding

Forwards up to 15 ports of incoming WAN/Internet traffic to a local computer. For example, forwarding remote ports 25-100 to local port 10025, local address 10, would forward traffic from port 25 to local computer 192.168.0.10 port 10025, traffic from port 26 to local port 10026, etc.



Port Forwarding

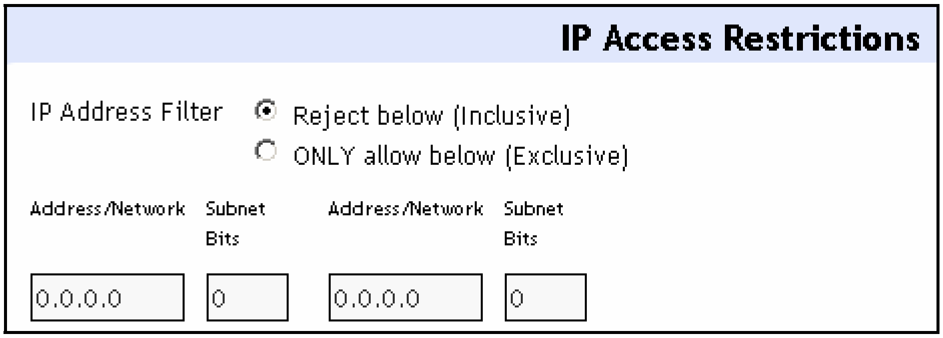
Protocol	Remote Ports	Local Port	Local Address
UDP	0 - 0	0	192.168.0.0

4.14 Applications – IP Access Restrictions

Inclusive filter will allow all traffic, EXCEPT for the IP Addresses listed below. Exclusive filter will ONLY allow traffic on IP Addresses listed below.

4.14.1 IP ACCESS RESTRICTIONS

Allows or rejects access to certain external IP Addresses and Networks. For example, to block Internet traffic to the 110.30.30.0 class C subnet, enter 110.30.30.0 as the address, and 24 for the subnet bits. Subnet bits are the number of 1 bits before 0's in the netmask, for example, 24 = 255.255.255.0, 30 = 255.255.255.252, 32 = 255.255.255.255, etc.



IP Access Restrictions

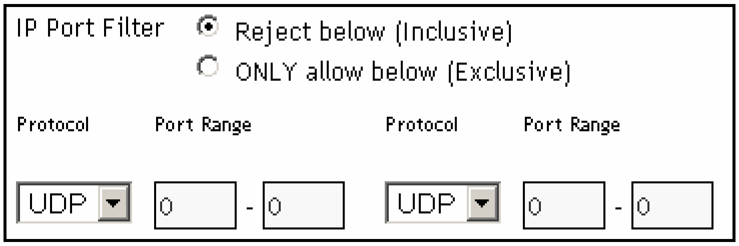
IP Address Filter ● Reject below (Inclusive)
○ ONLY allow below (Exclusive)

Address/Network	Subnet Bits	Address/Network	Subnet Bits
0.0.0.0	0	0.0.0.0	0

4.14.2 IP PORT FILTER

Inclusive filter will allow all traffic, EXCEPT for on the ports listed below. Exclusive filter will ONLY allow traffic on ports listed below. UDP/53 is name server, TCP/80 is web, TCP/21 is FTP.

Allows or rejects access to certain external IP ports. For example, to block certain filesharing ports, create a block of TCP ports from 6969 to 6969, and make sure that the filter is inclusive. To only allow web traffic to the WAN, add TCP ports 80-80, and make sure the filter is exclusive.



IP Port Filter ● Reject below (Inclusive)
○ ONLY allow below (Exclusive)

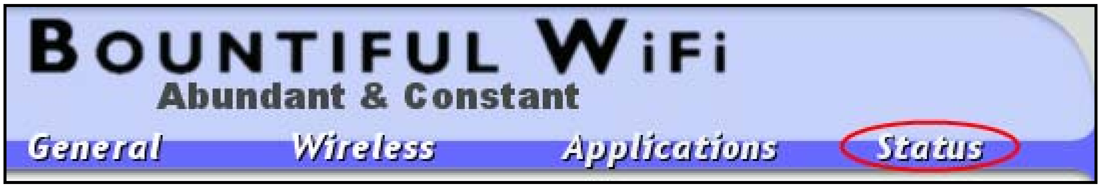
Protocol	Port Range			Protocol	Port Range		
UDP	0	-	0	UDP	0	-	0

4.14.3 SUBMIT BUTTON

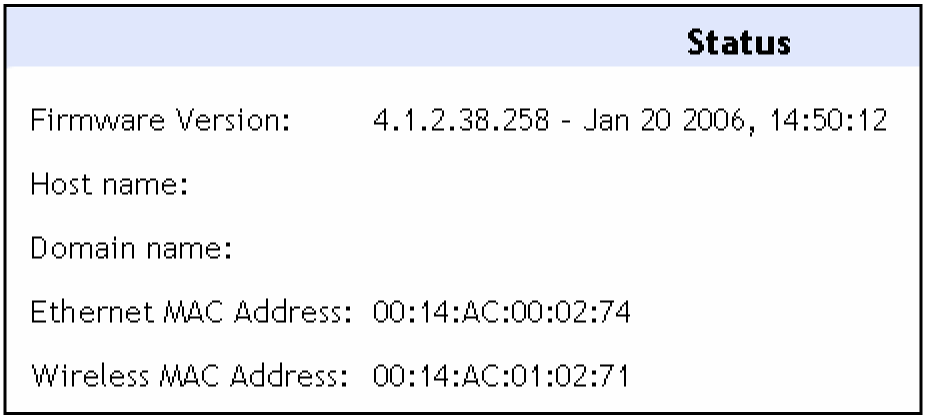
None of the changes made on this page take effect until the Submit button is clicked and the BWiFi is rebooted.

4.15 Status

The Status pages show detailed information about the firmware version and current configuration.



4.16 Status – Status



Status

Firmware Version:	4.1.2.38.258 - Jan 20 2006, 14:50:12
Host name:	
Domain name:	
Ethernet MAC Address:	00:14:AC:00:02:74
Wireless MAC Address:	00:14:AC:01:02:71

4.16.1 FIRMWARE VERSION:

Version of firmware currently loaded into Bountiful WiFi device.

4.16.2 HOST NAME

Value of the host name saved in the current configuration. Configure on General – Internet Connection tab.

4.16.3 DOMAIN NAME

Value of the domain name saved in the current configuration. Configure on General – Internet Connection tab.

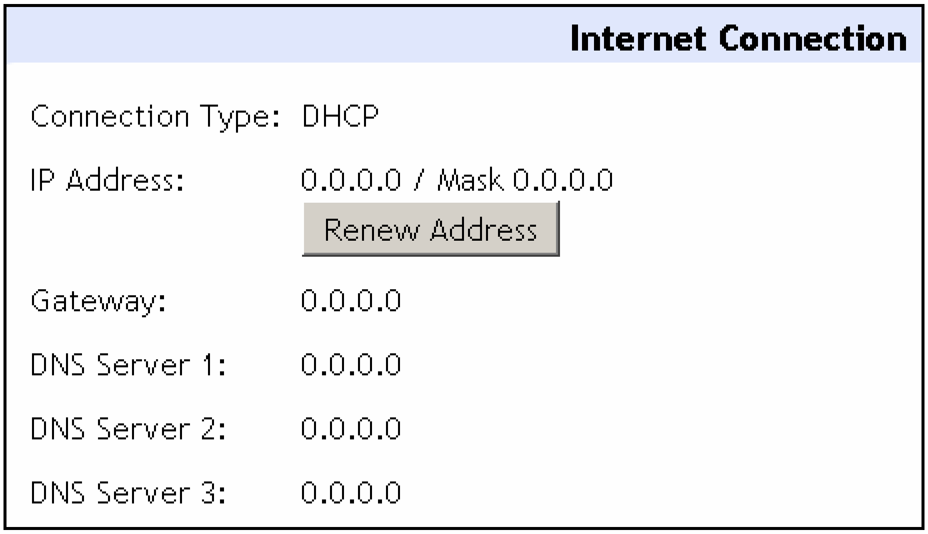
4.16.4 ETHERNET MAC ADDRESS

MAC address of the WAN Ethernet port

4.16.5 WIRELESS MAC ADDRESS

MAC address of the wireless Ethernet port.

4.17 Status – Internet Connection



Internet Connection

Connection Type: DHCP

IP Address: 0.0.0.0 / Mask 0.0.0.0

Gateway: 0.0.0.0

DNS Server 1: 0.0.0.0

DNS Server 2: 0.0.0.0

DNS Server 3: 0.0.0.0

4.17.1 CONNECTION TYPE

WAN connection type setting options: DHCP (automatic configuration) or Static (Manual configuration). When the device is used as an access point with no network cable attached to the WAN port, the Connection Type may display: “DHCP – Renewing” when the port does not have an IP address because there is no cable connected; this is normal.

4.17.2 IP ADDRESS / MASK

The WAN IP address and subnet mask for the BWiFi device obtained either through Static manual configuration or DHCP automatic configuration.

Click **Renew Address** button to release the current automatically assigned network configuration and obtain a new network configuration.

4.17.3 GATEWAY

The address of the gateway device obtained either through Static manual configuration or DHCP automatic configuration.

4.17.4 DNS SERVER 1

The address of the primary DNS server obtained either through Static manual configuration or DHCP automatic configuration.

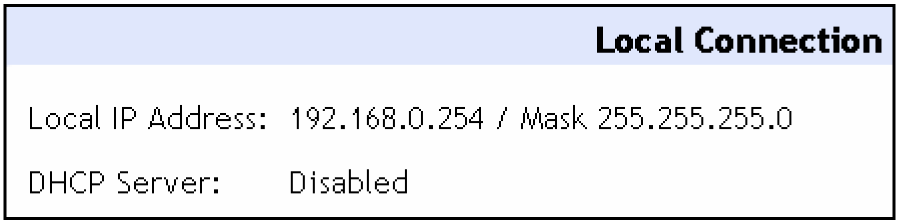
4.17.5 DNS SERVER 2

The address of the secondary DNS server obtained either through static manual configuration or DHCP automatic configuration.

4.17.6 DNS SERVER 3

The address of the tertiary DNS server obtained either through Static manual configuration or DHCP automatic configuration.

4.18 Status – Local Connection



Local Connection

Local IP Address: 192.168.0.254 / Mask 255.255.255.0

DHCP Server: Disabled

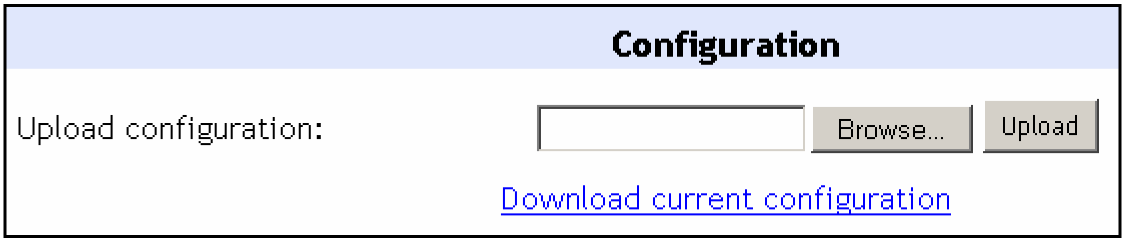
4.18.1 LOCAL IP ADDRESS / MASK

The LAN IP address and subnet mask obtained either through Static manual configuration or DHCP automatic configuration.

4.18.2 DHCP SERVER

Status of the DHCP server in the BWiFi device. When BWiFi is used as an access point, DHCP server is disabled, when used as a router, DHCP server is enabled.

4.19 Status – Configuration

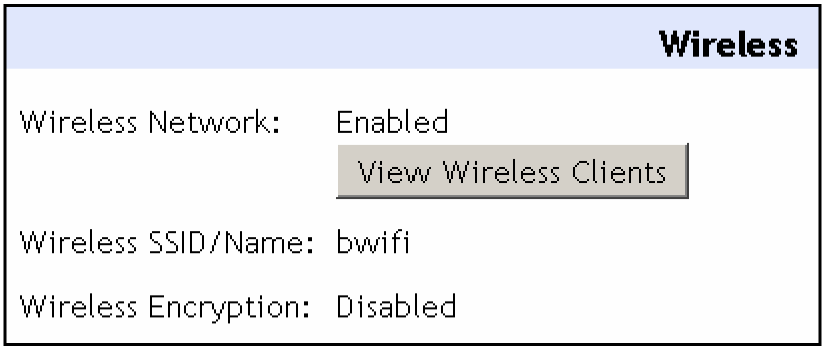


Configuration

Upload configuration:

Save and restore configuration files. To save the current configuration, click on the **Download current configuration** link and save the configuration file on the computer hard drive. The default file name is *ap.cfg*, it is ok to change the file name to make it easer to identify in the future. To restore a saved configuration, click the **Browse** button and select the previously saved configuration file, then press the **Upload** button and reboot.

4.20 Status – Wireless



Wireless Network: Enabled

Wireless SSID/Name: bwifi

Wireless Encryption: Disabled

4.20.1 WIRELESS NETWORK

Click **View Wireless Clients** button to display a list of the network devices that currently have a wireless connection to BWiFi.

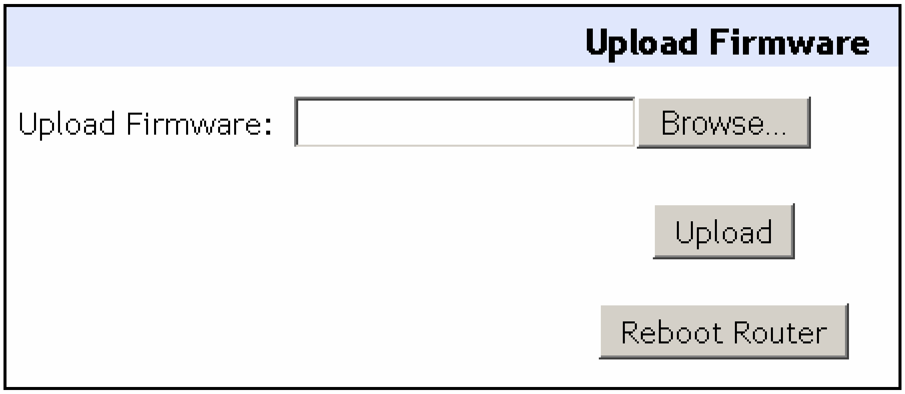
4.20.2 WIRELESS SSID/NAME

The name of the wireless network as assigned during setup. The default is “bwifi”.

4.20.3 WIRELESS ENCRYPTION

Shows which wireless encryption is currently enabled on the BWiFi device.

4.21 Status – Upload Firmware



4.21.1 UPLOAD FIRMWARE

To upload new firmware to the BWiFi device:

1. Visit www.BountifulWiFi.com to download the .romz file with the latest firmware the the computer hard drive.
2. Press the **Browse** button and select the .romz file downloaded.

3. Press the **Upload** button and wait for the BWiFi device to transfer the file, this will take several minutes.
4. Press the **Reboot Router** button when the upload is complete.
5. Hold **Reset button** on back of router for 30 seconds, release and wait an additional 30 seconds for the new firmware to take effect.

Warning: Do not unplug the power cord from the Router during the upload process. Doing so may result in permanent damage to the Router.

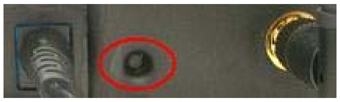
5 Trouble Shooting

5.1 Cable Check

- Verify that the modem or gateway is connected into the proper port of the Bwifi Router and that you are using the network cable that came with the Router. If you are running a firewall software program, temporarily disable it.
- If a computer is wired into the Bwifi router, be sure it is connected to one of the numbered LAN ports on the router (not the WAN port).

5.2 Reset Router

Are you unable to access the Router configuration page? Power on router and connect to computer to a LAN port using Network Cable. Press and hold Reset button for 30 seconds. Wait another 30 seconds for device to reset. Browse to http://192.168.0.1 (User name: **admin** password: **admin**) for configuration.



5.3 SSID Check

The SSID must be the same on all wireless adapters and on the Router. The SSID is “bwifi” by default. If you choose to change the SSID on Router, be sure to change it to the identical word or phrase on the wireless adapters.

To check the SSID on the wireless adapters: double click the Wireless Network Connection icon in the system tray, view the SSIDs of the available networks and select the correct network from the list.

5.4 Maximizing Wireless Range

The Bountiful WiFi Router offers better range than other routers; however, range is still dependent on environment.

To obtain maximum range:

- Place the Router as high as possible and as close to the center of the coverage area as possible.
- Adjust the antennas to a vertical position.
- Keep the Router away from any large, metal objects.
- In cases of possible interference, try changing the channel. Go to the router’s setup page http://192.168.0.1 or http://xxx.xxx.xxx.254 (User name: **admin** password: **admin**) and change the channel (it is on channel 11 by default). Try channels 1, 6 or 11 as they are the furthest apart from each other.

5.5 Wireless security

Setting up Security on the Wireless Network: Enabling encryption to give me more security with the Wireless network.

1. Enabling encryption will encrypt all the data traveling through the air in the Wireless network. To enable this feature, first log into the **Router**’s setup page by typing the following into the web browser: http://192.168.0.1 or http://xxx.xxx.xxx.254 and pressing Enter.

2. Enter User name: **admin** password: **admin**. Once in the router's setup page, select the **Wireless** tab.

- If all the PC's with wireless adapters are using Windows XP Service Pack 2 then choose Wireless Authentication: WPA PSK to enable robust WPA encryption.
- If any wireless PC's use Windows 98, 2000 or XP SP1 choose Wireless Authentication: Open/Shared Key Only to enable WEP encryption.

3. Select ASCII passphrase/key radio button. Enter a 5 digit passphrase for 64 bit encryption and a 13 digit passphrase for 128 bit encryption. Save this word or phrase. See User Manual for additional security options.
4. Scroll down and click the Submit button, then Reboot. You now have encryption set on the router.
5. Click on the Wireless network settings icon in the system tray on one of the computers.
6. When the **Wireless Network Connection** wizard appears, select the network from the list and enter the correct passphrase to establish a connection. Do this for every computer that has a wireless adapter. Some software/hardware versions require different approaches. Refer to the support documention for the operating system and the wireless adapter.

5.6 Contact Technical Support

For additional help or questions, contact Bountiful WiFi technical support:

- Tollfree: 877-247-6378
- Email: support@bountifulwifi.com
- Web: www.BountifulWiFi.com

6 Glossary

6.1 Glossary

AES
An extremely strong encryption standard that's just starting to become available. AES stands for Advanced Encryption System.

DHCP
A protocol by which a server automatically assigns IP addresses to clients so users doesn't have to configure them manually. DHCP stands for Dynamic Host Configuration Protocol.

DMZ
A feature in a NAT gateway that lets you expose a machine on your internal network to the outside Internet. DMZ stands for demilitarized zone.

DNS
An Internet protocol for mapping IP addresses (like 198.65.100.241) to human-readable domain names (like bountifulwifi.com). DNS stands for Domain Name Service

DSL
A common form of broadband Internet connection delivered on a standard phone line. DSL stands for Digital Subscriber Line.

Dynamic DNS
A technique that lets people connect a permanent domain name to an IP address that may change.

Firewall
A network program that blocks malevolent traffic that might endanger the computers on your network.

Firmware
The internal software that runs dedicated hardware devices. Upgrades to firmware are often necessary to fix problems.

Infrastructure mode
The most common way of creating a wireless network in which clients associate with an access point.

IP address
The numeric address (like 192.168.0.1) that identifies each device in a TCP/IP network.

LAN
Local Area Network, The computers at your site, connected via Ethernet or Wi-Fi. Local area network is often abbreviated to LAN.

MAC address
The unique address assigned to every wireless and wired Ethernet network adapter. MAC stands for Media Access Control.

Mbps
Megabits per second, or millions of bits per second, a measure of bandwidth.

NAT
A network service that makes it possible to share a single IP address with a network of many computers.

NAT stands for Network Address Translation. Since a NAT gateway exposes only a single IP address to the outside Internet, it's useful for security.

Port mapping
The act of mapping a port on an Internet-accessible NAT gateway to another port on a machine on your internal network. Port mapping enables you to run a public Internet service on a machine that is otherwise hidden from the Internet by your NAT gateway. Other names for port mapping include "port forwarding," "pass-through," and "punch-through."

Router
An intelligent network device that goes one step beyond bridging by converting address-based protocols that describe how packets move from one place to another. In practice, this generally comes down to translating between IP addresses and MAC addresses for data flowing between your local network and the Internet. Many people use the term interchangeably with "gateway." You must enter the IP address of your router when configuring network settings manually.

SSID
Service Set Identifier, a set of characters that give a unique name to a WLAN.

Subnet mask
A network setting that indicates the size of the network you're on.

Switch
A specific type of hub that isolates the communications between any two computers from the rest of the network, thus increasing throughput. Switches are also called "switching hubs."

TKIP
An encryption key that's part of WPA. TKIP stands for Temporal Key Integrity Protocol. It's nominally weaker than the government-grade AES, but in the real world, TKIP is more than strong enough.

WAN
Wide Area Network, A collection of local area networks connected by a variety of physical means. The Internet is the largest and most well-known wide area network. Wide area network is generally abbreviated to WAN.

WAP
Wireless Application Protocol, a set of standards to enable wireless devices to access Internet services, such as the World Wide Web and email.

WEP
An encryption system for preventing eavesdropping on wireless network traffic. WEP stands for Wired Equivalent Privacy. WEP is easily broken, and is in the process of being replaced by WPA.

WLAN
Wireless Local Access Network, a LAN that can be connected to via a wireless connection.

WPA
A modern encryption system for preventing eavesdropping on wireless network traffic that solves the problems that plagued WEP. WPA stands for Wi-Fi Protected Access.

Voice-over-IP
A way of making telephone calls over a packet-switched network like the Internet. Voice-over-IP requires special telephones and software. Voice-over-IP is commonly abbreviated to VoIP.

VoIP
Short for Voice over IP, which is simply voice data sent using Internet Protocol over the public Internet or an intranet. Its main advantage is that it avoids the usual phone service tolls. A few companies are offering cordless VoIP phones that work on Wi-Fi networks.

VPN
A method of creating an encrypted tunnel through which all traffic passes, preventing anyone from snooping through transmitted and received data. VPN stands for virtual private network.

7 Agency Certifications

7.1 FCC Certification

7.1.1 CLASS B EQUIPMENT

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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. 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 to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into 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.

7.1.2 MODIFICATIONS

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Bountiful WiFi, llc., may void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference;
- This device must accept any interference received, including interference that may cause unwanted operation.

NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

For questions regarding this product or the FCC declaration, contact:

Bountiful WiFi, llc.
707 W. 700 S. Suite 202A
Woods Cross, UT 84087

www.BountifulWiFi.com
info@BountifulWiFi.com

Tel: 801-296-5970
Fax: 801-294-9965