



HW2R1

## HI-GAIN™ WIRELESS-N DUAL RADIO SMART REPEATER

website [www.hawkingtech.com](http://www.hawkingtech.com)  
e-mail [techsupport@hawkingtech.com](mailto:techsupport@hawkingtech.com)

© COPYRIGHT 2009 HAWKING TECHNOLOGIES, INC. ALL RIGHTS RESERVED.

USER'S MANUAL ►►

**Federal Communication Commission**  
**Interference Statement**

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

**FCC Caution**

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

## **Federal Communication Commission (FCC) Radiation Exposure Statement**

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## **R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

## **Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## **EU Countries Intended for Use**

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

## Contents

Chapter I: Product Information.....	1
1-1 Introduction and safety information .....	1
1-2 Safety Information .....	3
1-3 System Requirements .....	5
1-4 Package Contents.....	6
Chapter II: Basic Configuration and Setup.....	10
2-1 Build your network (Initial hardware setup) .....	10
2-2 Accessing the Web Setup Menu .....	12
2-2-1 Windows 95/98/Me IP Address Setup:.....	13
2-2-2 Windows 2000 IP Address Setup: .....	15
2-2-3 Windows XP IP Address Setup: .....	17
2-2-4 Windows Vista/7/8/10 IP Address Setup:.....	19
2-2-5 Mac OS X IP Address Setup .....	21
2-2-6 Smart Repeater IP address lookup.....	22
2-3 Quick Setup .....	23
2-3-1 Network Pass Through (Bridge Mode).....	29
Chapter III: General Setup.....	30
3-1 System .....	30
3-1-1 Time Zone .....	31
3-1-2 Change Management Password .....	32
3-1-3 Remote Management.....	34
3-2 Internet Connection (Setup).....	35
3-2-1 Setup procedure for Wireless Internet Connection: .....	36
3-2-2 Setup procedure for ‘Wired Internet Connections: .....	39
3-2-3 Setup procedure for ‘DNS’: .....	51
3-2-4 Setup procedure for ‘DDNS’: .....	53
3-3 Home Network (LAN: Local Area Network) Configuration .....	55
3-3-1 LAN IP section:.....	56
3-3-2 DHCP Server:.....	59
3-3-3 Static DHCP Leases Table:.....	60
3-4 Wireless Home Network (WLAN) Configuration.....	62
3-4-1 Basic Wireless Settings .....	62
3-4-2 Advanced Wireless Settings .....	66

3-4-3 Wireless Security .....	69
3-4-4 Wireless Access Control .....	78
3-4-5 WPS - Wi-Fi Protected Setup .....	81
3-4-6 Security Tips for Wireless Network .....	84
Chapter IV: Advanced Functions .....	85
4-1 Quality of Service (QoS) .....	85
4-1-1 Basic QoS Settings .....	85
4-1-2 Add a new QoS rule .....	88
4-2 Network Address Translation (NAT) .....	90
4-2-1 Basic NAT Settings (Enable or disable NAT function) .....	90
4-2-2 Port Forwarding .....	92
4-2-3 Virtual Server .....	95
4-2-4 Port Mapping for Special Applications .....	98
4-2-5 UPnP Setting .....	101
4-2-6 ALG Settings .....	103
4-3 Firewall .....	105
4-3-1 Access Control .....	107
4-3-2 URL Blocking .....	113
4-3-3 DoS Attack Prevention .....	116
4-3-4 Demilitarized Zone (DMZ) .....	121
4-4 System Status .....	124
4-4-1 System information and firmware version .....	124
4-4-2 Internet Connection Status .....	125
4-4-3 Home Network .....	126
4-4-4 System Log .....	127
4-4-5 Active DHCP client list .....	129
4-4-6 Statistics .....	130
4-5 Configuration Backup and Restore .....	131
4-6 Firmware Upgrade .....	133
4-7 System Reboot .....	135
4-8 Using the Support Utility .....	136
Chapter V: Appendix .....	141
5-1 Hardware Specification .....	141
5-2 Troubleshooting .....	142
5-3 Glossary .....	144

## Chapter I: Product Information

### *1-1 Introduction and safety information*

Thank you for purchasing the Hi-Gain™ Wireless-300N Smart Repeater! This advanced Smart Repeater is the best choice for your home, office, RV, boat or other range extending applications. The Hi-Gain™ Wireless-300N Smart Repeater is the most intelligent and easy to configure, high performance Wi-Fi range extending solution on the market.

With two radios running concurrently to process an 802.11b/g/n wireless Internet connection as well as redistributing the signal via 802.11n within your local surroundings, the Hi-Gain™ Wireless-300N Smart Repeater is the only repeater capable of recreating an independent network from any 802.11b/g/n Wi-Fi source. The HW2R1 features a full function Wireless-300N router as well as an 802.11b/g modem port.

#### **HW2R1 Features:**

- High-Speed Internet Access throughput via wired or wireless connection
- 1 x Dedicated Amplified Wireless-N WAN (Wide Area Network) antenna port
- 2 x Dedicated Wireless-N LAN (Wireless Local Area Network) antenna ports
- Includes a Hi-Gain 13dBi Antenna for WAN and two 3dBi Omni-Directional Antennas for WLAN.
- Allow multiple users to share a single wired or wireless Internet line
- Supports up to 253 users (access through local network)
- Share a single 802.11b/g/n Wi-Fi, Cable or xDSL internet connection
- Access private LAN servers from the internet
- Four wired LAN ports (10/100M), one WAN port (10/100M) and one Wireless (802.11b/g) WAN port
- Provides IEEE 802.11b/g/n wireless LAN capability
- Support DHCP (Server/Client) for easy IP-address setup
- Advanced network and security features like: Special Applications, QoS, DMZ, Virtual Servers, Access Control, Firewall.

- Allows you to monitor device and network status features: DHCP Client Log, System Log, Security Log and Device/Connection Status
- Easy to use Web-based GUI for network configuration and management purposes
- Remote management function allows configuration and upgrades from a remote computer (over the Internet)
- Auto MDI / MDI-X function for all wired Ethernet ports.

## ***1-2 Safety Information***

In order to maintain the safety of the users and properties, please adhere to the following safety instructions:

1. This Smart Repeater is designed for indoor use only; DO NOT place this Smart Repeater outdoors
2. DO NOT put this Smart Repeater at or near hot or humid places, like kitchens or bathrooms. Also, do not leave this Smart Repeater in the car during warm weather.
3. DO NOT pull any connected cable with force; disconnect them from the Smart Repeater first.
4. If you want to place this Smart Repeater in a high location or hang on the Smart Repeater on a wall, make sure the Smart Repeater is firmly secure. Falling from high places will damage the Smart Repeater and its accessories, and the warranty will be void.
5. Accessories of this Smart Repeater, like antennas and power supply, are a danger to small children under 3 years old. They may put the small parts in their nose or mouth and it may cause serious harm. **KEEP THIS SMART REPEATER OUT OF REACH OF CHILDREN!**
6. The Smart Repeater will become hot when being used for extended periods of time (***This is normal and is not a malfunction***). DO NOT put this Smart Repeater on paper, cloth, or other flammable materials.
7. There are no user-serviceable parts inside the Smart Repeater. If you have found that the Smart Repeater is not working properly, please contact technical support or your dealer of purchase and ask for help. DO NOT disassemble the Smart Repeater, or warranty will be void.
8. If the Smart Repeater falls into water when it's powered on, DO NOT use your hand to pick it up. Switch the electrical power off before you do anything, or contact an experienced technician for help.



9. If you smell something strange, or even see some smoke coming out from the Smart Repeater or power supply, remove the power supply or switch the electrical power off immediately, and call dealer of purchase for help.

### ***1-3 System Requirements***

- A computer
- Internet web browser
- A wired or wireless networking adapter (e.g. AirPort card, built-in Ethernet adapter, etc.)
- Broadband modem (e.g. Cable or DSL) or wireless Internet connection (e.g. Hotspot, 802.11b/g network, etc.)

## ***1-4 Package Contents***



Before you start to use this Smart Repeater, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:




- 1 x Hi-Gain™ Wireless-300N Smart Repeater
- 1 x Quick Installation Guide
- 1 x CD with User's Manual and PC Support Utility
- 1 x A/C power adapter
- 3 x 3dBi Hi-Gain Dipole Omni-Directional Antennas

## 1-5 Product Overview

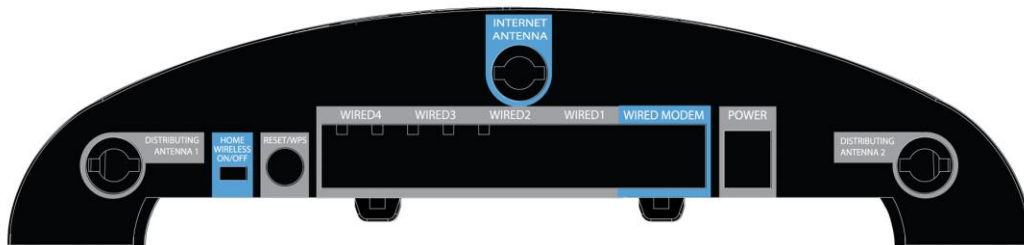
### Top Panel



LED Name (Front Left to Right)	Light Status	Description
<b>PWR</b> 	Stable ON	Smart Repeater is switched on and correctly powered
	Stable OFF	Smart Repeater is off
	Slow Blinking	Factory Default Reset (Reset button is held for longer than 5 seconds)
	Fast Blinking	Standard Reset (Reset button is held for less than 5 seconds)
<b>Wireless (WAN) Internet</b> 	Stable ON	Good Wireless Connection (Signal Strength > 70%)
	Stable OFF	Cannot find wireless network to connect to / not connected
	Slow Blinking	Poor Wireless Connection (Signal Strength < 35%)
	Fast Blinking	Normal Wireless Connection (Signal Strength

		between 36% and 70%)
Local (LAN) Wireless 	Fast Blinking	Connected with Traffic
	Stable ON	Connected without Traffic
	Stable Off	No Connection. Wireless LAN Off
Wired Internet 	Fast Blinking	Connected with Traffic
	Stable On	Connected without Traffic
	Stable Off	No Connection
WIRED Local Network (1~4) 	Fast Blinking	Port is Connected with Traffic
	Off	Port has no Connection

### Back Panel



Item Name	Description
Internet Antenna	Antenna connector used for the connection to a Wireless Internet Connection (Wireless WAN).
Home Wireless On/Off	This switch is used to turn the radio for your “home” local wireless connection on or off. When not in use, it is recommended to keep the Home Wireless connection off to avoid unwanted intrusions.
Distributing Antenna	Antenna connectors used for your local home wireless network (Wireless LAN).
Reset/WPS	Reset the Smart Repeater to factory default settings (clear all

	<p>settings). Press this button and hold for MORE THAN 30 seconds to restore all settings to factory defaults.</p> <p>If pressed for less than 5 seconds, the Smart Repeater will simply reboot.</p>
Wired (1 – 4)	Local Area Network (LAN) ports 1 to 4. Used for wired connections to your computers and network devices.
Wired Modem	Wired Wide Area Network (WAN / Internet) port. The port for connecting your Cable/DSL modem.

## Chapter II: Basic Configuration and Setup

### 2-1 Build your network (Initial hardware setup)

Please follow these instructions to build the network connection between the Hi-Gain™ Wireless-300N Smart Repeater and your computers and other network devices:

1. Connect the included antennas to your Smart Repeater.



2. Connect the power adapter to the Smart Repeater
3. Connect all 'wired' users to the HW2R1 via the Wired Local Area Network (LAN) ports in grey. For wireless users, scan for the SSID of the Smart Repeater (**Smart\_Repeater**) and connect. You must be within range of the Smart Repeater before connecting.
4. Check to see the activity of the LEDs on the front panel. The PWR LED should be on. The LAN LEDs should be on if the computer / network device connected to the respective port of the Smart Repeater is powered on and properly connected. If PWR LED is not on, or any LED you expected is not on, please recheck the power connection, or jump to "**5-2 Troubleshooting**" for possible reasons and solutions.

Traditional Router Setup (Optional):

If you do not plan on using the Wireless Internet Connection and instead plan on using a traditional wired modem connection (such as Cable or DSL) then you will need to attach the Ethernet cable from your modem to the blue 'Modem' port on the Smart Repeater. This will allow the Smart Repeater to function as a traditional wireless router.



## ***2-2 Accessing the Web Setup Menu***

After your Smart Repeater has been connected and powered the next step is to access the Web Menu for initial configuration. To do this, your computer must be able to get an IP address automatically (use dynamic IP address setting).

Try to access: <http://setup.hawkingtech.com>

(or try typing: <http://192.168.5.200> into your Internet browser's address bar)

If the Web Menu appears you can skip the next steps and go to step 2-3. You will need to enter the following default login and password to access the "Quick Setup" menu:

Login: admin

Password: 1234

If it's set to use a static IP address or you are unsure, please follow the following instructions to configure your computer to use a static IP address:

**Note: Please be sure to set your network IP addresses back to default after you have finished configuration.**

*If the operating system of your computer is....*

**Windows 95/98/Me** - please go to section 2-2-1

**Windows 2000** - please go to section 2-2-2

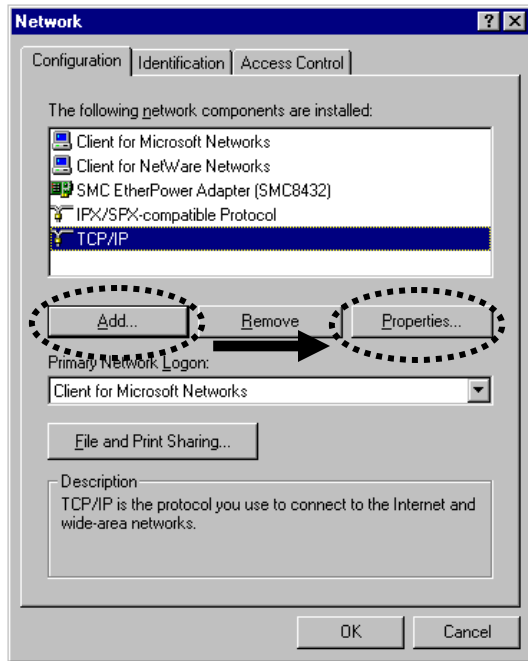
**Windows XP** - please go to section 2-2-3

**Windows Vista/7** - please go to section 2-2-4

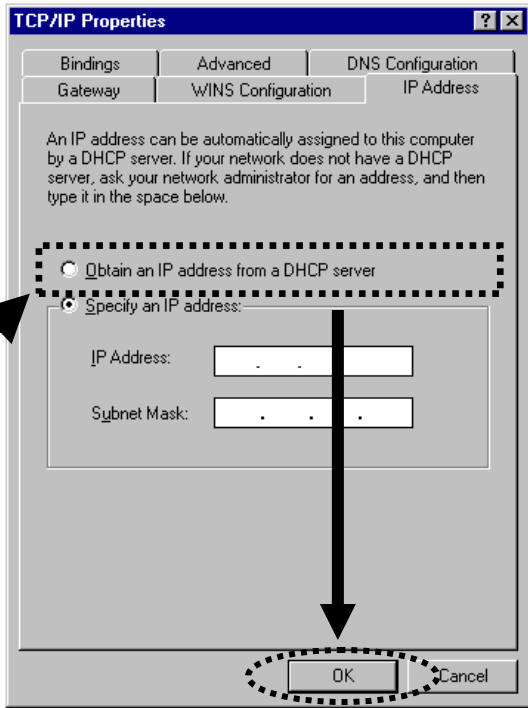
**Mac OS X** - please go to section 2-2-5

## 2-2-1 Windows 95/98/Me IP Address Setup:

1. Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Double-click *Network* icon, and *Network* window will appear. Select “TCP/IP”, then click “Properties”.

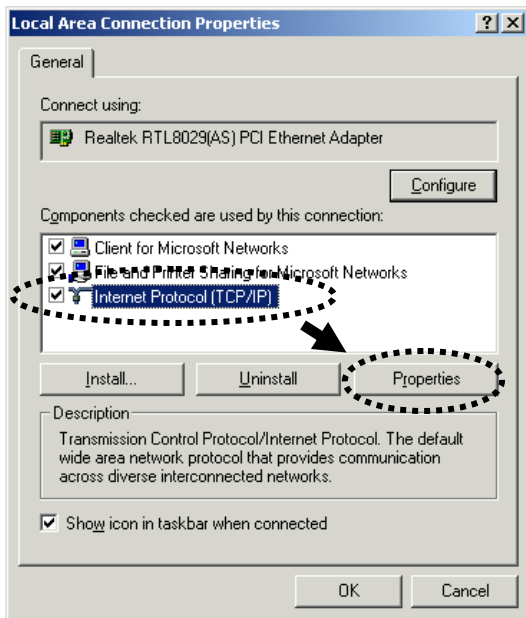


2. Select “Obtain an IP address from a DHCP server” and then click “OK”.

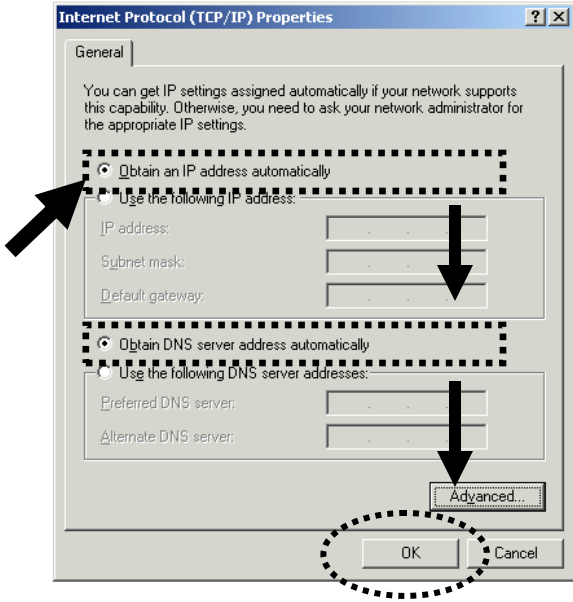


## 2-2-2 Windows 2000 IP Address Setup:

1. Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Double-click *Network and Dial-up Connections* icon; click *Local Area Connection*, and *Local Area Connection Properties* window will appear. Select “Internet Protocol (TCP/IP)” and then click “Properties”

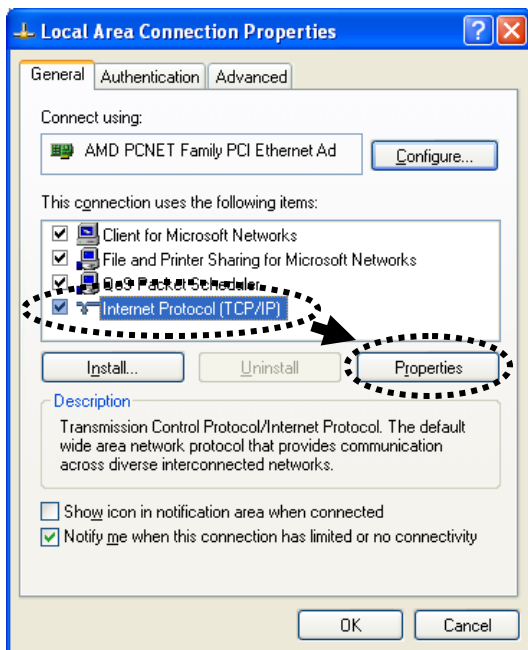


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.

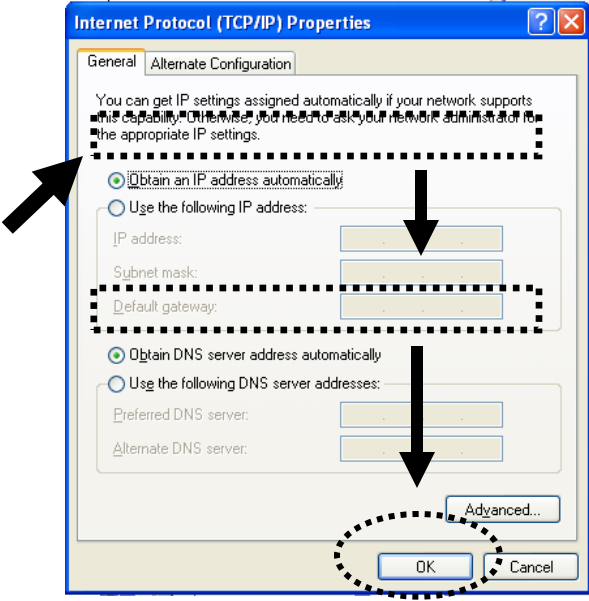


### 2-2-3 Windows XP IP Address Setup:

1. Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Double-click *Network and Internet Connections* icon, click *Network Connections*, and then double-click *Local Area Connection, Local Area Connection Status* window will appear, and then click ‘Properties’

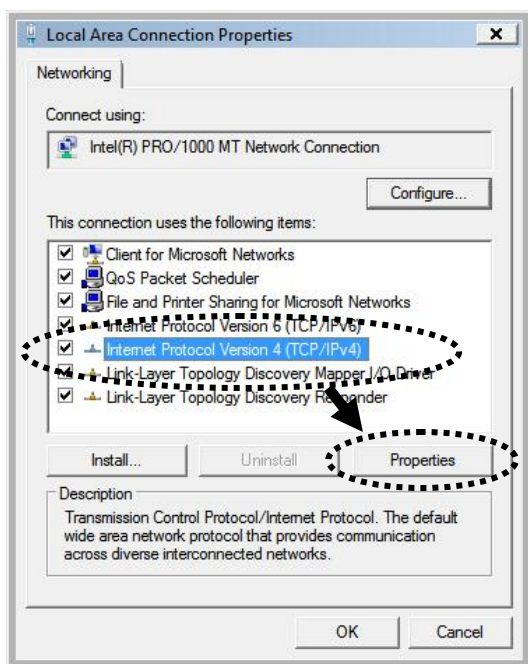


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.



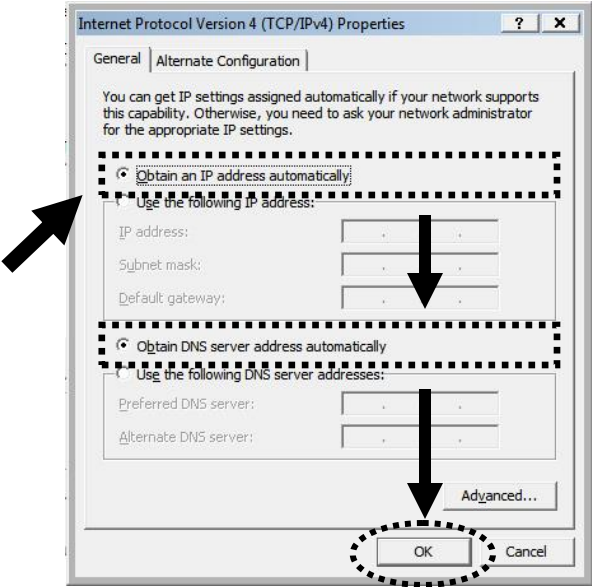
## 2-2-4 Windows Vista/7/8/10 IP Address Setup:

1. Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Under *Network and Internet*, Click *View Network Status and Tasks*, then click *Manage Network Connections/Change Adapter Settings* on the right hand column. Right-click *Local Area Network*, then select “*Properties*”. *Local Area Connection Properties* window will appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”



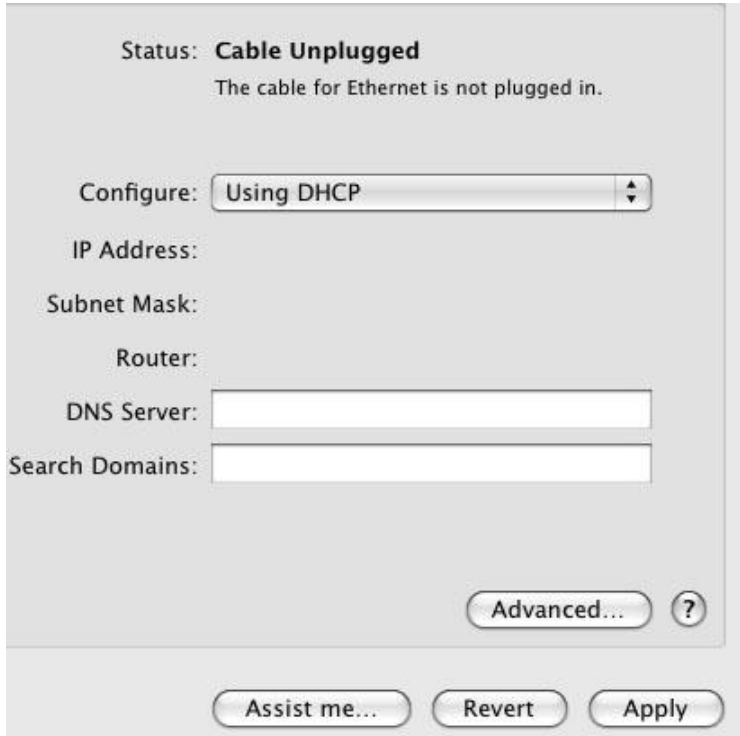
2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.





## 2-2-5 Mac OS X IP Address Setup

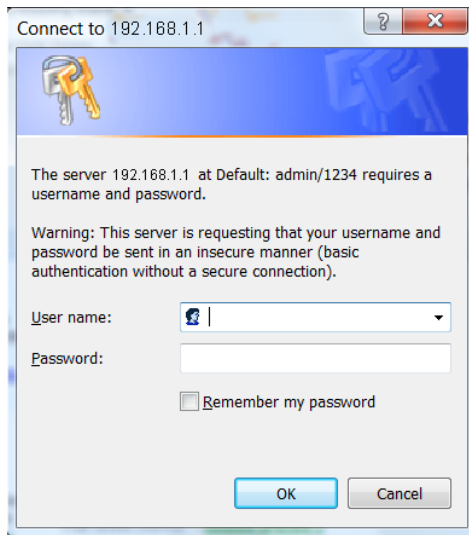
- 1) Go to your system preferences, go to network. Select your network connection. Make sure “Configure” is set to “Using DHCP”.



## 2-2-6 Smart Repeater IP address lookup

After your computer obtained an IP address from Smart Repeater, please start your web browser, and input “192.168.5.200” in address bar. The following message should be shown (or you may type in <http://setup.hawkingtech.com> to access the quick setup menu):

Please input user name and password in the field respectively, default user name is “admin”, and default password is “1234”, then press ‘OK’ button, and you can see the web management interface of this Smart Repeater.



## ***2-3 Quick Setup***

This Smart Repeater provides a “Quick Setup” procedure, which will help you to complete all required settings you need to access the Internet in a very short time. Please follow the following instructions to complete the “Quick Setup”:

- a. The first step of the “Quick Setup” is to locate a position to place your Smart Repeater. The position should be a location where the Repeater can pick up the signal that you wish to repeat (i.e. the neighbor’s wireless connection, local hot spot, etc.).



### Welcome to the Setup Wizard

To set up your Hi-Gain Wireless-300N Smart Repeater Pro you will need to first scan for an available wireless network (Hot Spot) to connect and redistribute within your current "Home Network" location.

Click Scan to begin a search for available networks. If you are using a Hi-Gain Antenna, then make sure your antenna is pointed towards the direction where you wish to scan for wireless network.



1 Scan for a wireless network to extend your WiFi network:

Network	Encryption	Authentication	Strength
1 Hawking Tech	WEP	OPEN	55%
2 SSA	WEP	OPEN	50%
2 SPRE-Wireless	TKIP	WPASK	40%
3 WLAN	TKIP	WPASK	35%
4 Hawking Tech	WEP	OPEN	35%

Pass Through Router Settings  
 (Network Bridging Mode):  Enable

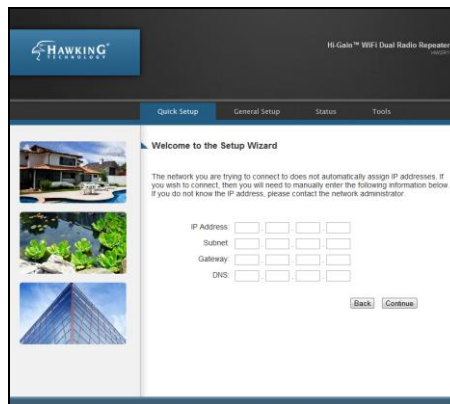
[Read Warning before enabling.](#)

2 Select and click Connect:

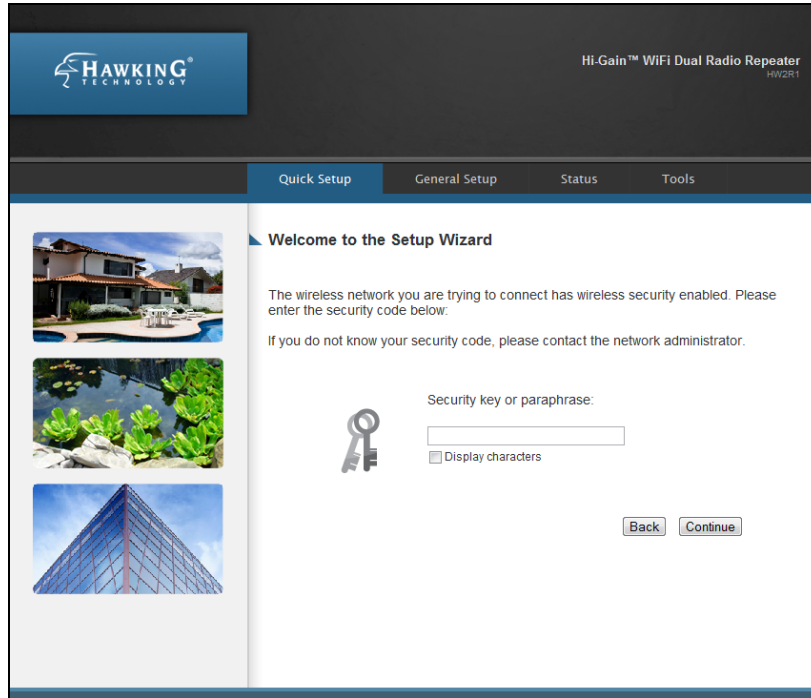
- b. Click “Scan” to locate all the networks within your area. Once you have found the network you wish to repeat, highlight it and click “Connect”. Each wireless network will be listed with their respective signal strengths and whether or not they are using security. For secure networks, you will need to have the correct key to access the network. If you do not you will not be able to repeat this network. It is recommended that the signal strength of the network you are trying to repeat is above 50% to ensure a solid connection to the Internet. Without a stable Internet connection, the rebroadcasted signal will be unstable as well. If you wish to setup a Pass Through mode (Network Bridging Mode), see section 2-3-1
- c. The “Quick Setup” wizard will now attempt to connect to your wireless Internet connection.

Select “Automatic Setup” to have the wizard automatically configure the IP settings of your Internet Connection. Most networks use Dynamic IP settings to automatically assign IP Addresses to incoming connections. Click “Apply”.

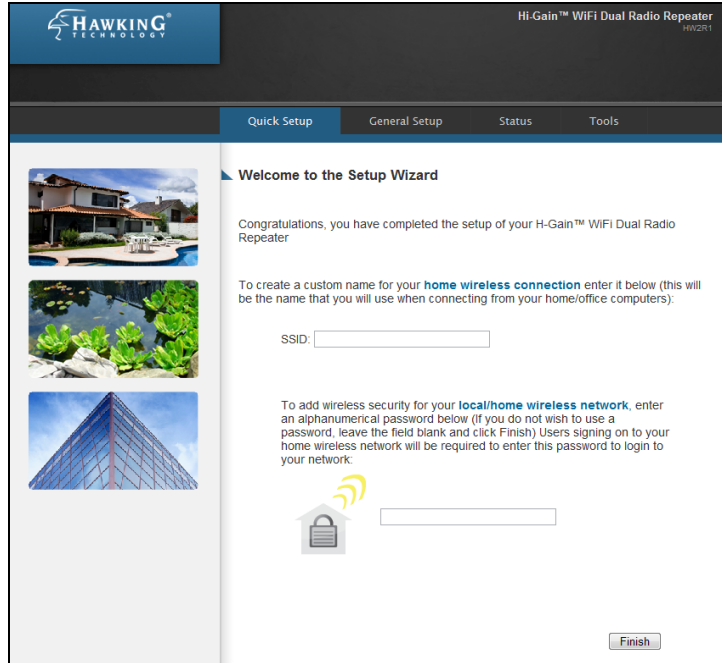
If the network you are connecting does not use Dynamic IP settings or you wish to manually configure your IP, you can choose “Manual Setup”.



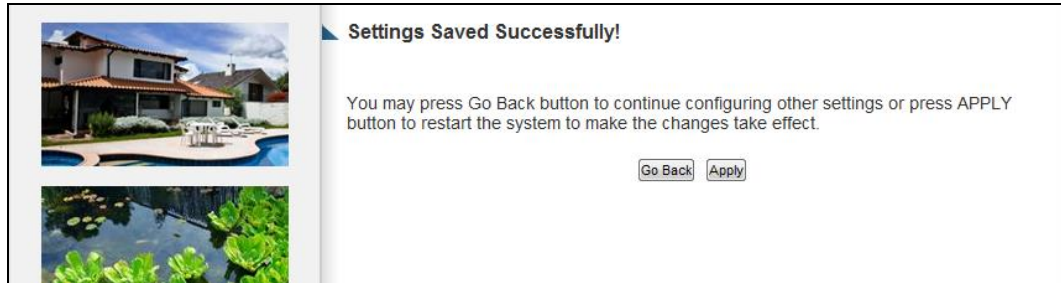
- d. If a wireless security key is necessary, the wizard will prompt you to enter the key. This key pertains to WEP and WPA wireless security keys and passphrases. The Smart Repeater will automatically decipher which type of security you are using. Type in the key or phrase and press “Continue”.



- e. When the connection has been established the wizard will prompt you if you wish to adjust the name of the wireless network used within your home (a.k.a. the SSID of the network that users will be connecting to from within your home – the redistributed wireless network). In addition, if you would like to add wireless security to your home wireless network you may do so here as well (By default, it uses WPA security. If you wish to change the security type, see section 3-4-3 after you have finished the configuration.) Click “Continue”.

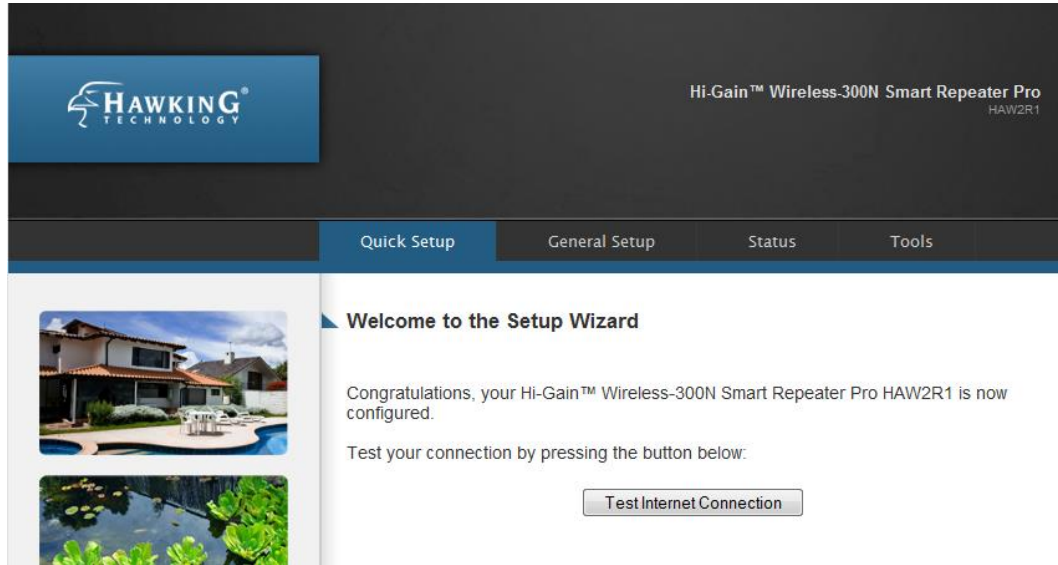


- f. Click “Finish” to complete your setup. Then press “Apply” to initiate the restart of your Smart Repeater.

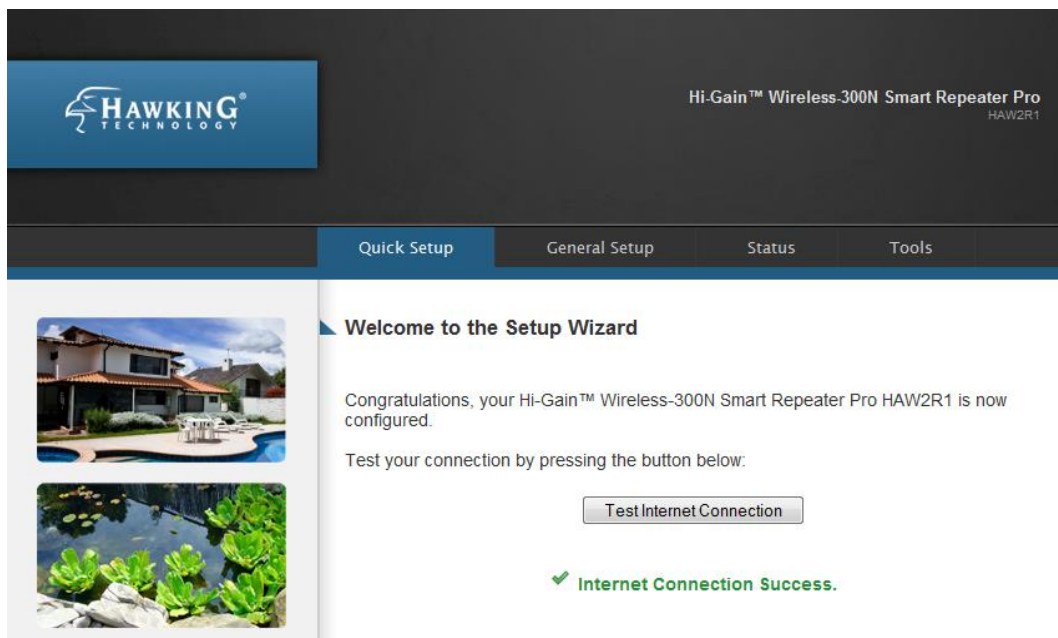


Allow the Smart Repeater to reboot.





After the system restarts, you can test your Internet connection to check that your setup was successful.



Once your Internet connection has tested successfully your setup is officially complete.

### 2-3-1 Network Pass Through (Bridge Mode)

The Smart Repeater by default creates a separate wireless network. When you search for wireless networks, you will see your original as well as the Smart Repeater. Because of these default settings, wireless devices connected to the Smart Repeater will be on a separate IP range. This may cause issues if you wish to share files, printers or just be on one network.

If you wish to have the system on one network, you will have to enable “Pass Through Router Settings” (Network Bridging Mode).

Pass Through Router Settings  Enable  
(Network Bridging Mode): [Read Warning before enabling.](#)

2 Select and click Connect:

After you check enable, just continue on with the rest of the Quick Setup steps. At the end of the setup, after you reboot the system, please be sure to also restart your computer. After your computer comes back up, select the Smart Repeater as your network. You should now be able to see your network files and computers all on one system.

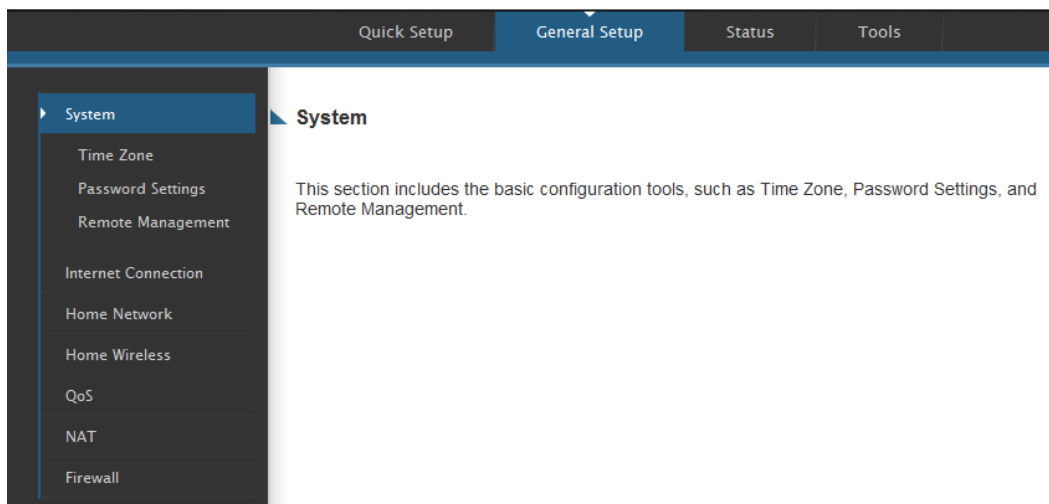
Note, by enabling Pass Through Mode, you will **not** be able to access the web menu unless your IP Settings match. To set your IP, see section 3-3-1.

## Chapter III: General Setup

In this chapter, you'll learn how to change the time zone, password, and remote management settings. Please start your web browser and log onto Smart Repeater web management interface (See Section 2-2), then click on the "General Setup" tab.

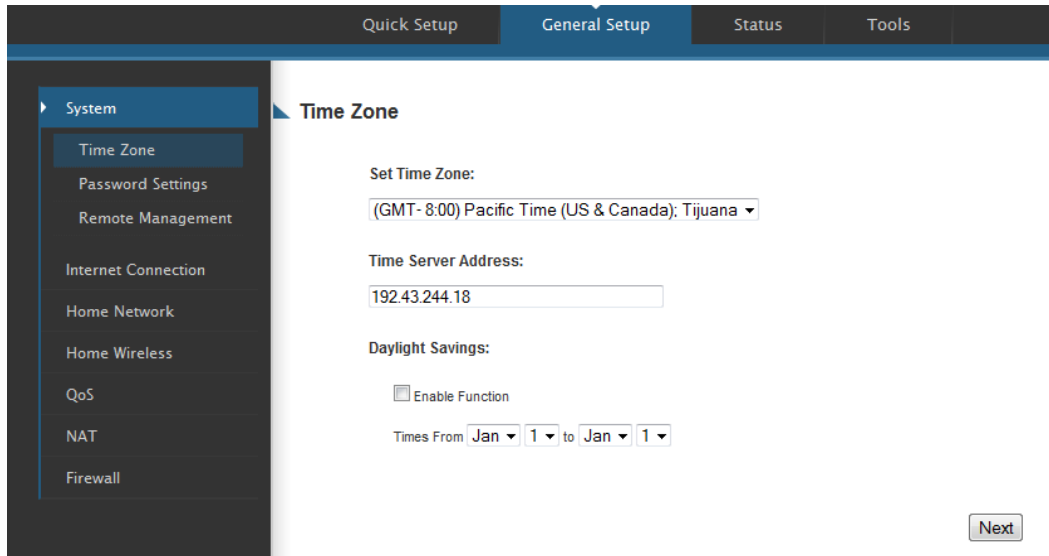
### 3-1 System

The system page allows you to configure the time zone, password settings and remote management

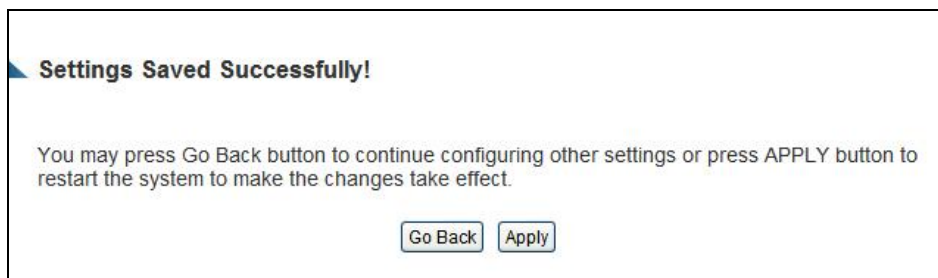


### 3-1-1 Time Zone

Please follow the following instructions to set time zone and time auto-synchronization parameters:



Please click “System” tab in menu on the left of web management interface, then click on “Time Zone”. Please select the correct time zone from the drop-down list, and input the IP address or host name of time server. If you want to enable daylight savings time settings, please check “Enable Function” box, and set the duration of daylight setting. When you finish, click “Apply”. You’ll see the following message displayed on web browser:



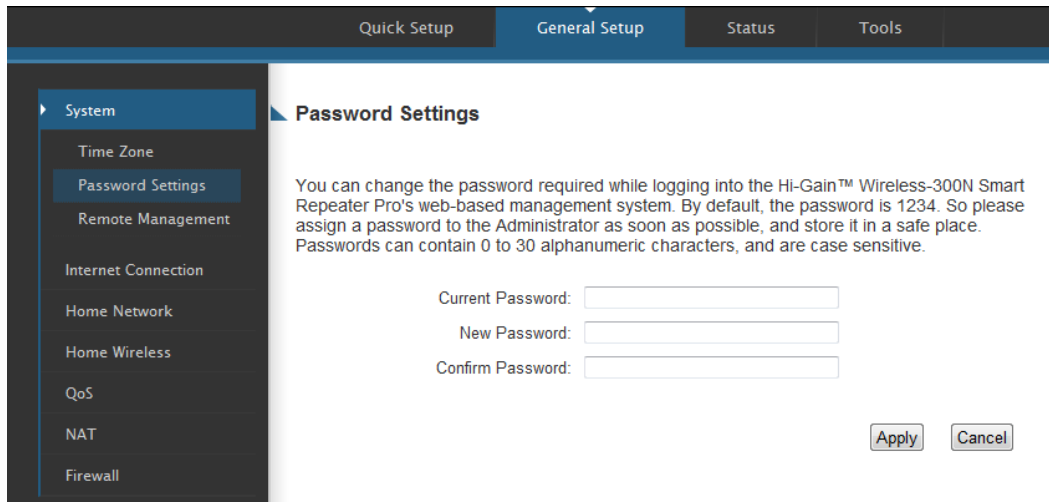
Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-1-2 Change Management Password

The default password of this Smart Repeater is “1234”, and it’s displayed on the login prompt when accessed from web browser. There’s a security risk if you don’t change the default password, since everyone can see it. This is very important when you have wireless function enabled.

To change password, please follow the instructions:

Please click “System” tab on the left hand column of the web management interface, then click “Password Settings”, and the following message will be displayed on your web browser:



---

*Current Password:* *Please input current password here.*

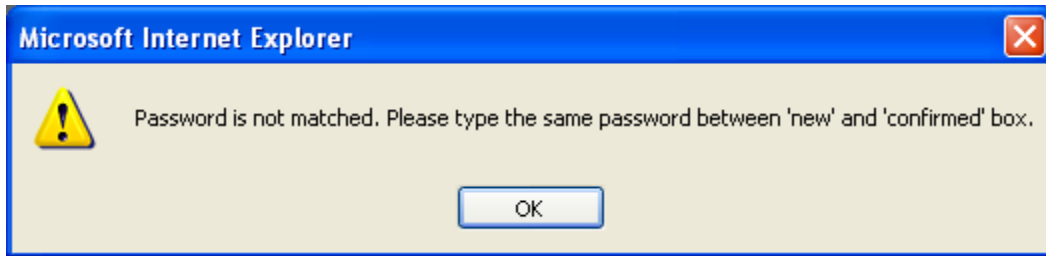
*New Password:* *Please input new password here.*

*Confirmed Password:* *Please input new password here again.*

---

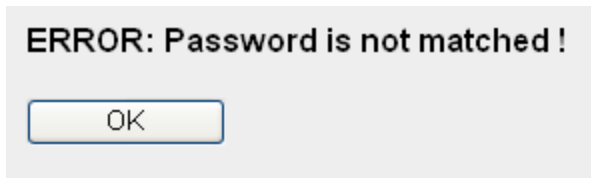
When you finish, click ‘Apply’. If you want to keep original password unchanged, click ‘Cancel’.

If the password you typed in “New Password” and “Confirmed Password” fields are not the same, you’ll see the following message:



Please retype the new password again when you see above message.

If you see the following message:



This error displays when the “Current Password” field is entered incorrectly. Click “OK” to go back to the previous menu and input your current password again.

After entering the correct login information you will be prompted to login again with your new login settings.

### 3-1-3 Remote Management

This Smart Repeater by default does not allow management access from the Internet in order to prevent possible security risks. However, you can still manage this Smart Repeater from a specific IP address by enabling the “Remote Management” Function.

To do so, please follow these instructions:

Click the “General Setup” tab at top of web management interface, then click “Remote Management” from the menu on the left and the following message will be displayed on your web browser:

	Host Address	Port	Enable
1	<input type="text" value="0.0.0.0"/>	2 <input type="text" value="8080"/>	3 <input type="checkbox"/>

---

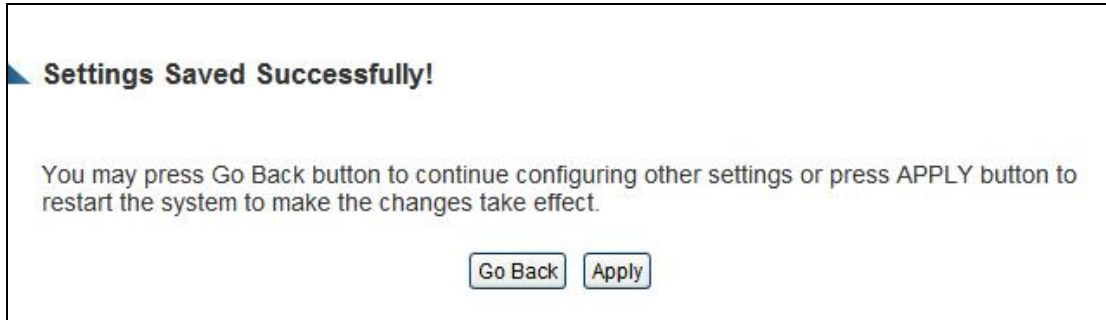
*Host Address (1):*      *Input the IP address of the remote host you wish to initiate a management access.*

*Port (2):*              *Define the port number that the Smart Repeater will receive incoming requests from. If you are providing a web service (default port number is 80), you should try to use other port number. You can use the default port setting '8080', or something like '32245' or '1429'. (Any integer between 1 and 65534)*

*Enabled (3):*              *Select the field to start the configuration.*

---

When you finish with all of your settings, click “Apply” and you’ll see the following message displayed on web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater so the settings will take effect after it reboots.

**NOTE: When you want to manage this Smart Repeater from another computer over the internet, you have to input the IP address and port number of this Smart Repeater. If your Internet service provider assigns you with a static IP address, it will not be a problem; but if the IP address your service provider assigns to you will vary every time you establish an Internet connection, this will be a problem.**

**Please either ask your service provider to give you a static IP address, or use dynamic IP to host name mapping services like DDNS. Please refer to chapter 3-2-4 ‘DDNS client’ for details.**

**NOTE2: Default port number the web browser will use is ‘80’. If the ‘Port’ setting in this page is not ‘80’, you have to assign the port number in the address bar of web browser manually. For example, if the IP address of this Smart Repeater is 1.2.3.4, and the port number you set is 8888, you have to input following address in the address bar of web browser:**

**http://1.2.3.4:8888**



## 3-2 Internet Connection (Setup)

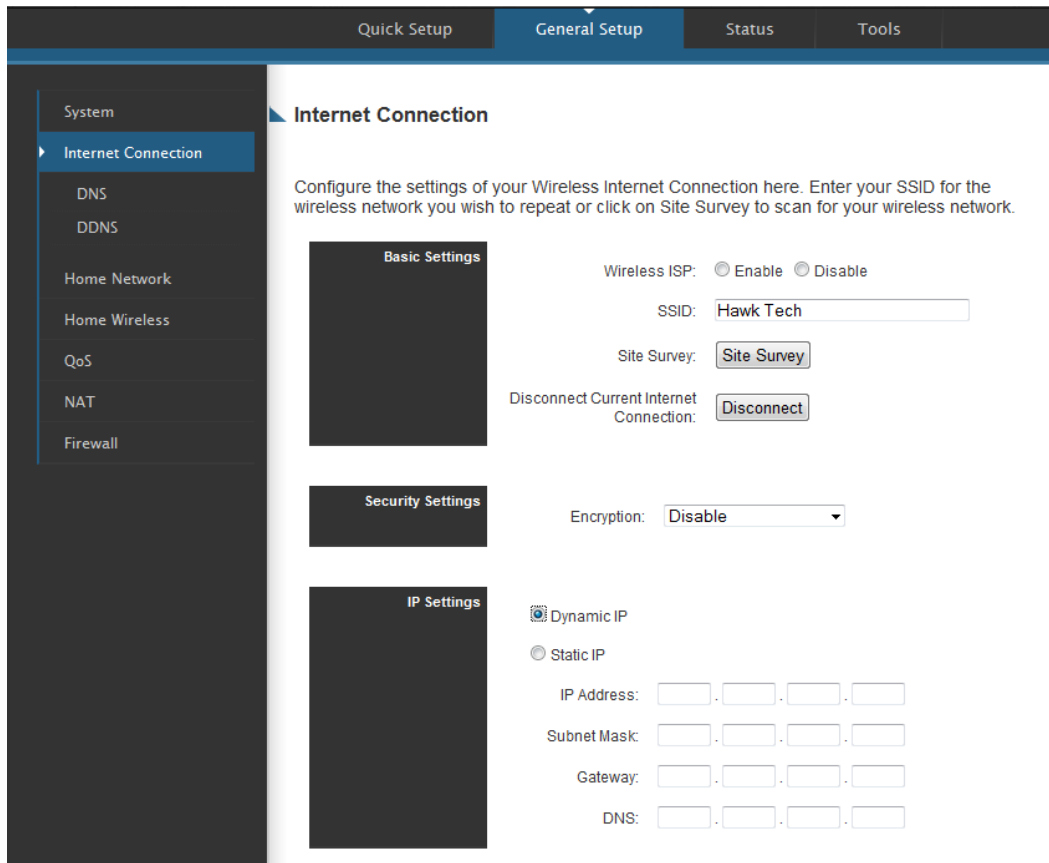
The Wireless Internet connection setup can be configured through the “Quick Setup” menu described in Chapter 2-3. However for a more detailed setup of either a wired setup (via DSL or Cable Modem) or a wireless Internet connection setup click on the “General Setup Tab” and then navigate to the “Internet Connection” tab on the left hand column.

### 3-2-1 Setup procedure for Wireless Internet Connection:

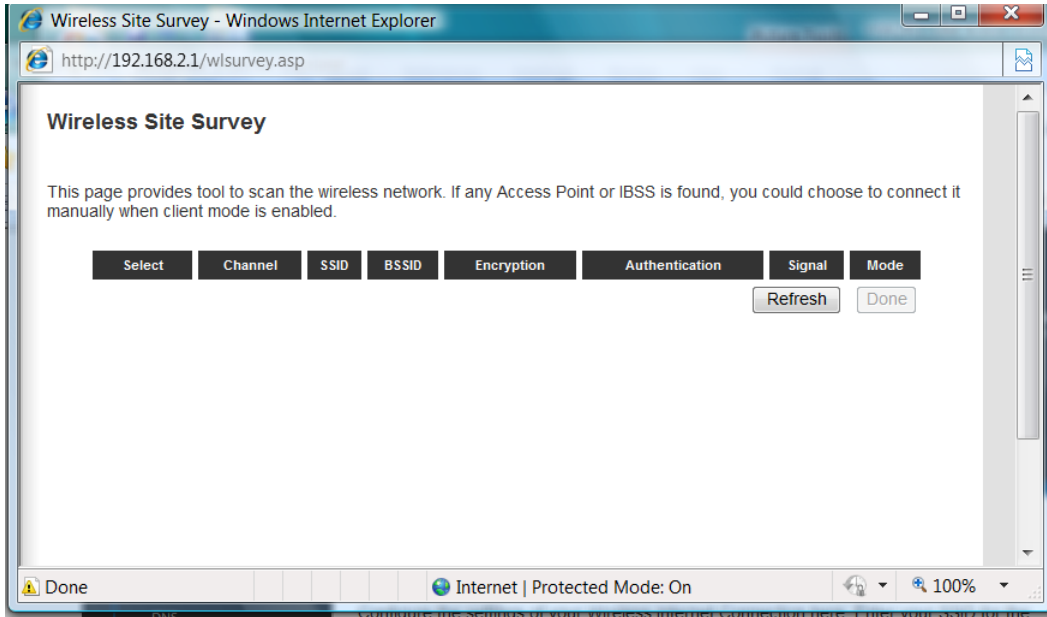
To manually configure a Wireless Internet Connection select “Configure” next to Wireless Internet Connection.

The screenshot displays the Hawking Technology web interface for configuring a Hi-Gain™ Wireless-N Dual Radio Smart Repeater (HW2R1). The interface features a top navigation bar with tabs for 'Quick Setup', 'General Setup', 'Status', and 'Tools'. A left-hand navigation menu is visible, with 'Internet Connection' selected. The main content area shows the 'Wireless Internet Connection' configuration page, which includes a 'Configure' button and a diagram illustrating the setup. The diagram shows an 'Internet' connection (represented by a globe) connected to a 'HotSpot' tower, which is connected to a 'Hi-Gain™ Wireless-N Dual Radio Repeater HW2R1'. The repeater is then connected to a 'Home Network' consisting of a laptop and a desktop computer. Below this, the 'Wired Internet Connection' configuration page is also visible, featuring a 'Configure' button and a diagram illustrating the setup. The diagram shows an 'Internet' connection (represented by a globe) connected to a 'Cable Modem', which is connected to a 'Hi-Gain™ Wireless-N Dual Radio Smart Repeater HW2R1'. The repeater is then connected to a 'Home Network' consisting of a laptop and a desktop computer.

The menu below should appear.



You may manually enter the SSID of the wireless network you plan on connecting to or you can click “Site Survey” to have the web interface scan for local networks in your vicinity. (See Site Survey Menu below)



After you have selected a wireless Internet connection network, you may configure the security settings for that network if required. Select the security type and the encryption method and enter the appropriate key for the network you plan on connecting to.

#### Under IP Settings

Most networks use Dynamic IP settings to automatically assign IP Addresses to incoming connections. Click “Apply”.

If the network you are connecting does not use Dynamic IP settings or you wish to manually configure your IP, you can choose “Manual Setup”.

Click “Apply” when you have completed your setup.

### 3-2-2 Setup procedure for ‘Wired Internet Connections:

To setup a wired Internet connection such as Cable Modem or DSL, click “Configure” next to “Wired Internet Connection”



A menu will appear with a choice of wired Internet connection types. Select the one that fits your connection and scroll to the menu describing your selection below.

## Wired Internet Connection

For wired Internet connections, such as cable or DSL modems, select the configuration settings for your connection below.

- Dynamic IP (Most Cable Modems)**  
Obtains an IP address automatically from your Service Provider.
- Static IP**  
Uses a Static IP Address. Your Service Provider provides a Static IP Address to access Internet services.
- PPPoE**  
PPP over Ethernet is a common connection method used in xDSL connections.
- PPTP xDSL**  
Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.
- L2TP**  
Layer Two Tunneling Protocol is a common connection method used in xDSL connections..

[More Configuration](#)

Dynamic IP	- Please go to section 3-2-2-1
Fixed IP	- Please go to section 3-2-2-2
PPPoE	- Please go to section 3-2-2-3
PPTP	- Please go to section 3-2-2-4
L2TP	- Please go to section 3-2-2-5

### 3-2-2-1 Setup procedure for Dynamic IP:

#### Dynamic IP

Internet Connection > Dynamic IP

The Host Name is optional, but may be required by some Internet Service Providers (ISPs). The default MAC Address is set to the WAN physical interface on the Wireless Router. If required by your ISP, you can use the 'Clone MAC Address' button to copy the MAC Address of the Network Interface Card installed in your PC and replace the WAN MAC Address with this MAC Address.

1 Host Name:

2 MAC Address:

---

*Host Name (1): Please input host name of your computer, this is optional, and only required if your service provider asks you to do so.*

*MAC Address (2): Please input MAC address of your computer, if your service provider only permits computer with certain MAC address to access internet. If you're using the computer which used to connect to Internet via cable modem, you can simply press "Clone Mac address" button to fill the MAC address field with the MAC address of your computer,*

---

After you finish with all settings, click "OK"; if you want to remove a value you entered, click "Back".

After you click "OK", the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater so the settings will take effect after it reboots.

### 3-2-2-2 Setup procedure for ‘Static IP’:

#### Static IP

Internet Connection > Static IP

If your Internet Service Provider has assigned a Fixed IP address; enter the assigned IP Address, Subnet Mask and the Gateway IP Address provided. After you click Apply and before you reboot the HAW2R1, be sure to enter your DNS settings on the left menu.

1 IP Address:

2 Subnet Mask:

3 Default Gateway:

Apply

Cancel

Back

---

*IP address assigned  
by your Service  
Provider (1):*

*Please input IP address assigned  
by your service provider.*

*Subnet Mask (2):*

*Please input subnet mask assigned by your service provider*

*Service Provider*

*Please input the IP address of DNS*

*Gateway Address (3):*

*server provided by your service provider.*

---

After you finish with all settings, please click the “Apply” button and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.



Before you click “Apply” to reboot, be sure to click on the DNS settings on the left and input your ISP’s DNS settings. (See Section 3-2-3). Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-2-2-3 Setup procedure for ‘PPPoE’:

#### Point-to-Point Protocol over Ethernet (PPPoE)

Internet Connection > PPPoE

Enter the Point-to-Point Protocol over Ethernet (PPPoE) User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some Service Providers. Enter a Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then the connection will be dropped. You can enable the Connect on Demand option to automatically re-establish the connection as soon as you attempt to access the Internet again. If your Internet Service Provider requires the use of PPPoE, enter the information below.

1 User Name:

2 Password:

3 Service Name:

4 MTU:  (512<=MTU Value<=1492)

5 Connection Type:

6 Idle Time Out:  (1-1000 minutes)

- 
- User Name (1): Please input user name assigned by your Internet service provider here.*
- Password (2): Please input the password assigned by your Internet service provider here.*
- Service Name (3): Please give a name to this Internet service, this is optional*
- MTU (4): Please input the MTU value of your network connection here. If you don't know, you can use default value.*
- Connection Type (5): Please select the connection type of Internet connection you wish to use.*  
*Continuous – The connection will be kept always on. If the*

*connection is interrupted, the Smart Repeater will re-connect automatically.*

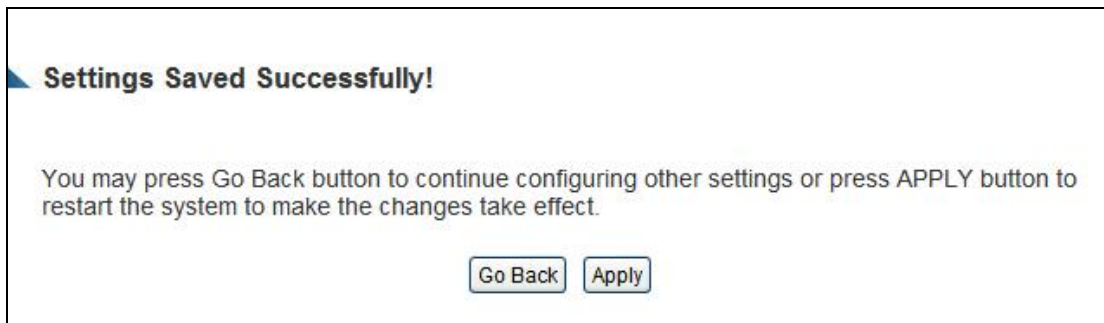
*Connect On-Demand – Only connect when you want to surf the Internet. “Idle Time Out” is set to stop the connection when the network traffic is not sending or receiving after an idle time.*

*Manual – After you have selected this option, you will see the “Connect” button and “Disconnect” button, click “Connect” and the Smart Repeater will connect to the ISP. If you want to stop the connection, please click “Disconnect” button.*

*Idle Time Out (6): If you have selected the connection type to “Connect-On-Demand”, please input the idle time out.*

---

After you finish with all the settings, click the “Apply” button. The following message will be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-2-2-4 Setup procedure for ‘PPTP’:

PPTP requires two kinds of setting: WAN interface setting (setup IP address) and PPTP setting (PPTP user name and password). Here we start from WAN interface setting:

**WAN Interface Settings**  
 **Obtain an IP address automatically**  
Host Name:   
MAC Address:    
 **Use the following IP address**  
IP Address:   
Subnet Mask:   
Default Gateway:

Select the type of how you obtain IP address from your service provider here. You can choose ‘Obtain an IP address automatically’ (equal to DHCP, please refer to ‘Cable Modem’ section above), or ‘Use the following IP address’ (i.e. static IP address)

WAN interface settings must be correctly set, or the Internet connection will fail even if settings of PPTP settings are correct. Please contact your Internet service provider if you don’t know what you should fill in these fields.

PPTP settings section:

**PPTP Settings**

1 User Name:

2 Password:

3 PPTP Gateway:

4 Connection ID:  (Optional)

5 MTU:  (512<=MTU<=1492)

6 BEZEQ-ISRAEL:  Enable (For BEZEQ network in ISRAEL use only)

7 Connection Type:

8 Idle Time Out:  (1-1000 Minute)

---

*User ID (1): Please input user ID (user name) assigned by your Internet service provider here.*

*Password (2): Please input the password assigned by your Internet service provider here.*

*PPTP Gateway (3): Please input the IP address of PPTP gateway assigned by your Internet service provider here.*

*Connection ID (4): Please input the connection ID here, this is optional and you may leave it blank.*

*MTU (5): Please input the MTU value of your network connection here. If you don't know, you can use default value.*

*BEZEQ-ISRAEL (6): If you are connecting to the BEZEQ network in Israel. Please enable this function.*

*Connection Please select the connection type of Internet*

*type (7): connection you wish to use, please refer to section 2-5-3 for detailed descriptions.*

*Idle Time Out (8): Please input the idle time out of Internet connection you wish to use, and refer to section 2-5-3 for detailed descriptions.*

---

Setting item 'BEZEQ-ISRAEL' is only required to check if you're using the service provided by BEZEQ network in Israel.

Press "Go Back" to save the settings and go back to the web management interface; press "Apply" to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-2-2-5 Setup procedure for 'L2TP':

**L2TP Settings**

1 User Name:

2 Password:

3 L2TP Gateway:

4 MTU:  (512<=MTU<=1492)

5 Connection Type:

6 Idle Time Out:  (1-1000 Minute)

---

*User ID (1): Please input user ID (user name) assigned by your Internet service provider here.*

*Password (2): Please input the password assigned by your Internet service provider here.*

*L2TP Gateway (3): Please input the IP address of PPTP gateway assigned by your Internet service provider here.*

*MTU (4): Please input the MTU value of your network connection here. If you don't know, you can use default value.*

*Connection type (5): Please select the connection type of Internet connection you wish to use.*

*Idle Time Out (6): Please input the idle time out of Internet connection you wish to use.*

---

Press "Go Back" to save the settings and go back to the web management interface; press "Apply" to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-2-3 Setup procedure for ‘DNS’:

If you select “*Dynamic IP*” or “*PPPoE*” as Internet connection method, at least one DNS server’s IP address should be assigned automatically. However, if you chose “*Static IP*” have preferred DNS server, or your service provider didn’t assign the IP address of DNS server for any reason, you can input the IP address of DNS server here.

#### DNS

A Domain Name System (DNS) server is similar to an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as `www.broadbandrouter.com`, a DNS server will find that name in its index and find the matching IP address. Most Internet Service Providers (ISPs) provide a DNS server for speed and convenience. Since your ISP may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.

Primary DNS:

Secondary DNS:

---

*Primary DNS*                      *Please input the IP address of DNS server provided by your service provider.*

*Secondary DNS*                      *Please input the secondary DNS provided by your service provider*

---

**NOTE: Only an IP address can be entered here; *DO NOT* use the hostname of DNS server! (i.e. only numeric characters and dots are accepted)**

**10.20.30.40..... Correct**  
**dns.serviceprovider.com..... Incorrect**

After you finish with all of your settings, click “Apply” and the following message will



be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-2-4 Setup procedure for ‘DDNS’:

DDNS (Dynamic DNS) is an IP-to-Hostname mapping service for those Internet users who don’t have a static (fixed) IP address. It will be a problem when such users want to provide services to other users on the Internet, because their IP address will vary every time when connected to the Internet, and other users will not be able to know the IP address they’re using at any certain time.

This Smart Repeater supports DDNS service of several service providers, for example:

DynDNS (<http://www.dyndns.org>)

TZO (<http://www.tzo.com>)

Go to one of the DDNS service provider’s web pages listed above, and get a free DDNS account by the instructions given on their webpage.

**DDNS**

DynamicDNS (DDNS) allows users to map the static domain name to a dynamic IP address. You must get a account, password and your static domain name from the DDNS service providers.

1 Dynamic DNS:  Enable  Disable

2 Provider:

3 Domain Name:

4 Account:

5 Password/Key:

---

*Dynamic DNS (1): If you want to enable DDNS function, please select ‘Enabled’; otherwise please select ‘Disabled’.*

*Provider (2): Select your DDNS service provider here.*

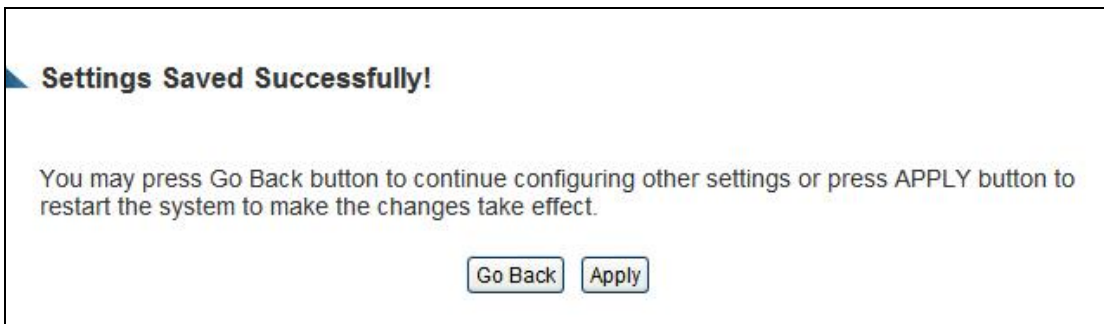
*Domain Name (3):        Input the domain name you've obtained from DDNS service provider.*

*Account /  
E-Mail (4):                Input account or email of DDNS registration.*

*Password / Key (5):      Input DDNS service password or key.*

---

After you finish with all of your settings, click “Apply” and the following message will be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### ***3-3 Home Network (LAN: Local Area Network) Configuration***

A LAN is the network within your home. All computers accessing your Internet connection through the Smart Repeater are considered part of your Home Network. Each of these users will either have their own manually configured IP address or an automatically configured IP address from the Smart Repeater via its DHCP server.

There are two ways to assign IP addresses to computers: static IP address (set the IP address for every computer manually), and dynamic IP address (IP address of computers will be assigned by Smart Repeater automatically). It's recommended for most computers to use dynamic IP address, it will save a lot of time on setting IP addresses for every computer, especially when there are a lot of computers in your network; for servers and network devices which will provide services to other computers and users that come from the Internet, a static IP address should be used.

#### ***Suggestions on IP address numbering plan:***

**If you have no idea on how to define an IP address plan for your network, here are some suggestions.**

- 1. A valid IP address has 4 fields: a.b.c.d, for most of home and company users, it's suggested to use 192.168.c.d, where c is an integer between 0 and 254, and d is an integer between 1 and 254. This Smart Repeater is capable to work with up to 253 clients, so you can set 'd' field of IP address of Smart Repeater as 1 or 254 (or any number between 1 and 254), and pick a number between 0 and 254 for field 'c'.**
- 2. In most cases, you should use '255.255.255.0' as subnet mask, which allows up to 253 clients (this also meets Smart Repeater's capability of working with up to 253 clients).**
- 3. For all servers and network devices which will provide services to other people (like Internet service, print service, and file service), they should use static IP address. Give each of them a unique number between 1 and 253, and maintain a list, so everyone can locate those servers easily.**
- 4. For computers which are not dedicated to provide specific service to others, they should use dynamic IP address.**

Please follow the following instructions to set wired LAN parameters:

Click the “Home Network” tab at the left menu of the web management interface, there are three setup groups here: “LAN IP”, “DHCP Server”, and “Static DHCP Leases Table”.

The screenshot displays the web management interface for the Hi-Gain™ Wireless-300N Smart Repeater Pro (HAW2R1). The interface features a top navigation bar with tabs for "Quick Setup", "General Setup" (selected), "Status", and "Tools". A left sidebar menu includes "System", "Internet Connection", "Home Network" (selected), "Home Wireless", "QoS", "NAT", and "Firewall".

The main content area is titled "Home Network" and contains the following configuration options:

- LAN IP**
  - IP Address:
  - Subnet Mask:
  - 802.1d Spanning Tree:
  - DHCP Server:
- DHCP Server**
  - Lease Time:
  - DHCP Client Start IP:
  - DHCP Client End IP:
  - Domain Name:

At the bottom of the configuration area, there are "Apply" and "Cancel" buttons.

Below the configuration area is a section titled "Static DHCP Lease Table - Up to 16 entries." which contains a table with the following columns: "No.", "MAC Address", "IP Address", and "Select". The table body is currently empty.

### 3-3-1 LAN IP section:

LAN IP

1 IP Address:

2 Subnet Mask:

3 802.1d Spanning Tree:

4 DHCP Server:

---

*IP address (1): Please input the IP address of this Smart Repeater. This is the IP address used to access your Smart Repeater. Make sure to make note of the new IP Address after you change it since the old one will no longer work.*

*Subnet Mask (2): Please input subnet mask for this network.  
802.1d If you wish to activate 802.1d spanning tree*

*Spanning Tree (3): function, select 'Enabled' for setup item '802.1d Spanning Tree', or set it to 'Disabled'*

*DHCP Server (4): If you want to activate the DHCP server function of this Smart Repeater, select 'Enabled', or 'Disabled'. If you select Disable, the IP settings from your source Internet network will be passed through to clients connecting through the Smart Repeater. (For example, a network with a DHCP server IP range of 10.1.1.1 – 10.1.1.100 will disperse IP addresses within that range to computers connecting through your Smart Repeater while the Smart Repeater is connected to that specific network)*

---

**Recommended (Default) Values if you don't know what to fill:**

IP Address: 192.168.1.200  
Subnet Mask: 255.255.255.0  
802.1d Spanning Tree: Disabled  
DHCP Server: Enabled



### 3-3-2 DHCP Server:



DHCP Server

1 Lease Time: Forever

2 DHCP Client Start IP:

3 DHCP Client End IP:

4 Domain Name:

These settings are only available when 'DHCP Server' in 'LAN IP' section is "Enabled".

---

*Lease Time (1): Please choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this Smart Repeater from dropdown menu.*

*Start IP (2): Please input the start IP address of the IP range.*

*End IP (3): Please input the end IP address of the IP range.*

*Domain Name (4): If you wish, you can also optionally input the domain name for your network. This is optional.*

---

#### **Recommended (Default) Value if you don't know what to fill:**

Lease Time: Two Weeks (or 'Forever', if you have less than 20 computers)

Start IP: 192.168.1.1

End IP: 192.168.1.199

Domain Name: (leave it blank)

#### **NOTE:**

1. The number of the last field (mentioned '3' field) of 'End IP' must be greater than 'Start IP', and cannot be the same as Smart Repeater's IP address.
2. The former three fields of IP address of 'Start IP', 'End IP', and 'IP Address of 'LAN IP' section should be the same.
3. These settings will affect wireless clients too.



### 3-3-3 Static DHCP Leases Table:

This function allows you to assign a static IP address to a specific computer forever, so you don't have to set the IP address for a computer, and still enjoy the benefit of using DHCP server. A maximum of 16 static IP addresses can be assigned here.

*(If you set "Lease Time" to "forever" in "DHCP Server" section, you can also assign an IP address to a specific computer permanently, however, you will not be able to assign a certain IP address to a specific computer, since IP addresses will be assigned in random order by this way).*

<input type="checkbox"/> 1 Enable Static DHCP Leases	
MAC Address	IP Address
2 <input type="text"/>	3 <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/>	

---

*Enable Static DHCP Leases (1):* Check this box to enable this function, otherwise uncheck it to disable this function.

*MAC Address (2):* Input the MAC address of the computer or network device (total 12 characters, with characters from 0 to 9, and from a to f, like '001122aabbcc')

*IP address (3):* Input the IP address you want to assign to this computer or network device

---

If you want to remove all characters you just entered, click "Clear".

After you clicked "Add", the MAC address and IP address mapping will be added to "Static DHCP Leases Table" section.

Static DHCP Lease Table - Up to 16 entries.			
No.	MAC Address	IP Address	Select
1	00:11:22:33:44:55	192.168.2.100	1 <input type="checkbox"/>

2  
Delete
3  
Delete All

If you want to delete a specific item, check the “Select” box of a MAC address and IP address mapping (1), then click “Delete” button (2); if you want to delete all mappings, click “Delete All” (3).

After you finish all LAN settings, click “Apply” on the bottom of this page. After you click “Apply”, the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Go Back
Apply

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### ***3-4 Wireless Home Network (WLAN) Configuration***

If your computer, PDA, game console, or other network devices has a wireless network adapter, you can use the wireless function of this Smart Repeater to let them connect to Internet and share resources with other computers on your wired home network. You can also use the built-in security functions to protect your network from intruders with malicious attacks.

Follow these instructions to set your wireless parameters:

Click the “Home Wireless” tab on the left side of the web management interface, and the following message will be displayed on your web browser.

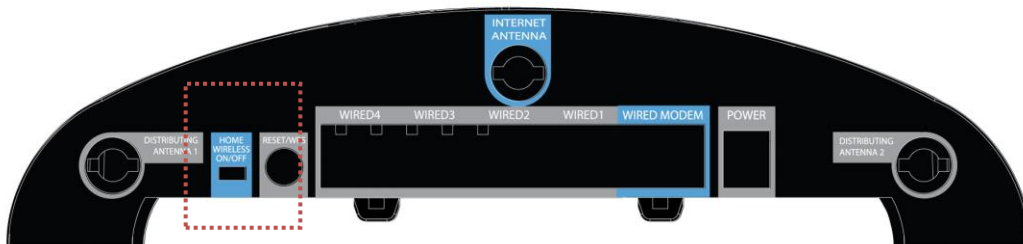
#### **Home Wireless**

Your local wireless network status is displayed below.

To enable or disable wireless access to your Repeater, adjust the switch labeled "Home Wireless On/Off" on the back of the Repeater.

Local Wireless Network: ● Enabled

If you wish to enable wireless, make sure the switch on the back of the Smart Repeater is switched to “On”. If you wish to disable the wireless, make sure the switch on the Smart Repeater is switch to “Off”.



### 3-4-1 Basic Wireless Settings

Click “Basic Setup” menu at the top of web management interface, then click “Basic Settings”, and the following message will be displayed on your web browser:

#### Home Wireless

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode: Access Point

1 Band:

2 SSID:

3 Channel Number:

4 Associated Clients:

---

*Band (1): Please select the radio band from one of following options:*

2.4 GHz (B)	2.4GHz band, only allows 802.11b wireless network clients to connect to this Smart Repeater (maximum transfer rate 11Mbps).
2.4 GHz (N)	2.4GHz band, only allows 802.11n wireless network clients to connect to this Smart Repeater(maximum transfer rate 300Mbps).
2.4 GHz (B+G)	2.4GHz band, only allows 802.11b and 802.11g wireless network clients to connect to this Smart Repeater (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients).
2.4 GHz (G)	2.4GHz band, only allows 802.11g wireless network clients to connect to this Smart Repeater (maximum transfer rate 54Mbps).
2.4 GHz (B+G+N)	2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network clients to connect to this Smart Repeater (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 300Mbps for 802.11n clients).

**NOTE: For 802.11b and 802.11g mode, the signals can be transmitted only by antenna 1 (The antenna on the right side of the rear panel).**

**For 802.11n mode: The Smart Repeater is operating in a 2T2R Spatial Multiplexing MIMO configuration. 2 antennas are for signal transmitting and 2 antennas are for signal receiving.**

*ESSID (2): This is the name of wireless Smart Repeater. You can type any alphanumerical characters here, maximum 32 characters. ESSID is used to identify your own wireless Smart Repeater from others when in the same area. Default SSID is "Smart\_Repeater". It's recommended to change default ESSID value to the one which is meaningful to you, like myhome, office\_room1, etc.*

*Channel Number (3): Please select a channel from the dropdown list of 'Channel*

*Number', 1 to 11 for USA. (This product is only for use in the USA and is restricted to usage of the channels 1-11 only) You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, as some wireless clients support manual channel number selecting, and this would help in certain scenarios when there is some radio communication problems.*

*Associated Clients (4): Click 'Show Active Clients' button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.*

---

**NOTE: If you don't have special reason to limit the type of allowed wireless clients, it's recommended to choose '2.4 GHz (B+G+N) to maximize wireless client compatibility.**

**TIPS: You can try to change channel number to another one if you think the data transfer rate is too slow. There could be some other wireless devices using the same channel, which will disturb the radio communication between wireless client and the wireless Smart Repeater.**

### 3-4-2 Advanced Wireless Settings

This Smart Repeater provides some advanced controls of the wireless parameters. If you want to configure these settings, click the “Advanced Settings” selection from the left side menu under “Wireless Home”, and the following message will be displayed:

**Advanced Settings**

Advanced wireless settings for your home network.

1 Fragment Threshold:  (256 - 2346)

2 RTS Threshold:  (0-2347)

3 Beacon Interval:  (20-1024 ms)

4 DTIM Period:  (1-10)

5 Data Rate:  ▾

6 N Data Rate:  ▾

7 Channel Width:  Auto 20/40 MHz  20 MHz

8 Preamble Type:  Short Preamble  Long Preamble

9 Broadcast Essid:  Enable  Disable

10 CTS Protect:  Auto  Always  None

11 Tx Power:  ▾

12 WMM:  Enable  Disable

- 
- Fragment Threshold (1):* Set the Fragment threshold of wireless radio. **Do not modify default value if you don't know what it is, default value is 2346.**
- RTS Threshold (2):* Set the RTS threshold of wireless radio. **Do not modify default value if you don't know what it is, default value is 2347.**
- Beacon Interval (3):* Set the beacon interval of wireless radio. **Do not modify default**

*value if you don't know what it is, default value is 100.*

*DTIM Period (4): Set the DTIM period of wireless radio. **Do not modify default value if you don't know what it is, default value is 3.***

*Data Rate (5): Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, **it's not necessary to change this value unless you know what will happen after modification.***

*N Data Rate (6): Same as above, but only for 802.11n clients.*

*Channel Width (7): Set channel width of wireless radio. **Do not modify default value if you don't know what it is, default setting is "Auto 20/40 MHz".***

*Preamble Type (8): Set the type of preamble, **do not modify default value if you don't know what it is, default setting is "Short Preamble".***

*Broadcast ESSID (9): Decide if the wireless Smart Repeater will broadcast its own ESSID or not. You can hide the ESSID of your wireless Smart Repeater (set the option to "Disable"), so only those people who know the ESSID of your wireless can get connected.*

*CTS Protect (10): Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g/n wireless access points. It's recommended to set this option to "Auto" or "Always". However, if you set to "None", your wireless Smart Repeater should be able to work fine, too.*

*Tx Power (11): You can set the output power of wireless radio. Unless you're using this wireless Smart Repeater in a really big space, you may not have to set output power to 100%. **This will enhance security (malicious / unknown users in distance will not be able to reach your wireless Smart Repeater).***



WMM(12):

*Short for Wi-Fi Multimedia, it will enhance the data transfer performance of multimedia contents when they're being transferred over a wireless network. **If you don't know what it is / not sure if you need it, it's safe to set this option to "Enable", however, default value is "Disable".***

---

After you finish these wireless settings, click "Apply" and the following message will be displayed on your web browser:



Press "Go Back" to save the settings made and go back to the web management interface; press "Apply" to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### **3-4-3 Wireless Security**

*It's very important to set wireless security settings properly!* Consequences of wireless networks without security include intrusion from hackers and malicious users that can steal valuable data from your network. It is highly recommended to setup security settings for your wireless network.

To set wireless security settings, click “Wireless” menu at the top of web management interface, then click “Security Settings”. Follow the instructions to set wireless security settings:

Select an encryption method from the “Encryption” dropdown menu, there are four options: Disable, WEP, WPA and WPA Radius.

### **3-4-3-1 Disable Wireless Security**

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless Smart Repeater if no other security measure is enabled (like MAC address access control - see section 3-4-4, or disable ESSID broadcast).

*Only use this option when you want to allow everyone to use your wireless Smart Repeater, and you don't care if there's someone that reads the data you transfer over the network.*

### 3-4-3-2 WEP - Wired Equivalent Privacy

When you select this mode, the wireless Smart Repeater will use WEP encryption, and the following setup menu will be shown on your web browser:

The screenshot shows a web browser window titled "Security Settings". Below the title is a blue arrow icon and the text "Secure your home wireless network below. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your home wireless network." The settings are as follows:

- 1 Encryption: WEP (dropdown menu)
- 2 Key Length: 64-bit (dropdown menu)
- 3 Key Format: Hex (10 Characters) (dropdown menu)
- 4 Default Tx Key: Key 1 (dropdown menu)
- Encryption Key 1: [Redacted]
- 5 Encryption Key 2: [Redacted]
- Encryption Key 3: [Redacted]
- Encryption Key 4: [Redacted]
- 6  Enable 802.1x Authentication

At the bottom right, there are "Apply" and "Cancel" buttons.

Here are descriptions of every setup item:

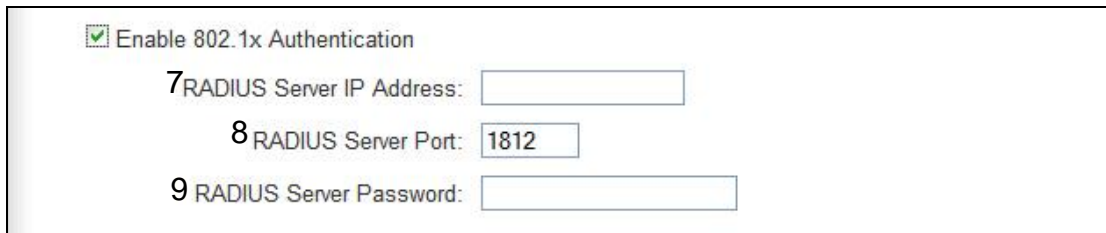
*Key Length (2): There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.*

*Key Format (3): There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select '64-bit' as key length, and 'Hex' as key format, you'll see the message at the right of 'Key Format' is 'Hex (10 characters)', which means the length of WEP key is 10 characters.*

*Default Tx Key (4): You can set up to four sets of WEP key, and you can decide which key is being used by default here. **If you don't know which one you should use, select "Key 1".***

*Encryption Key 1 to 4 (5): Input WEP key characters here, the number of characters must be the same as the number displayed at "Key Format" field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select "ASCII" key format, and if you select "Hex" as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be same with each other.*

*Enable 802.1x Authentication (6): IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless Smart Repeater before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. If there is a RADIUS server in you environment, please enable this function. Check this box and another sub-menu will appear:*



Enable 802.1x Authentication

7 RADIUS Server IP Address:

8 RADIUS Server Port:

9 RADIUS Server Password:

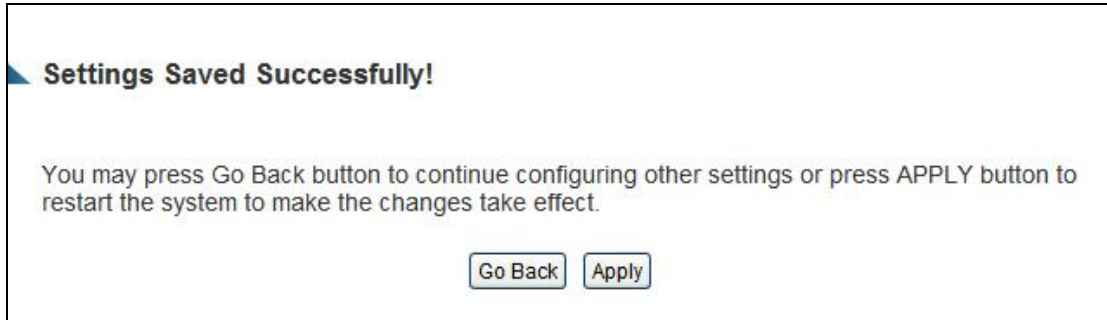
*RADIUS Server IP address (7): Please input the IP address of radius server here*

*RADIUS Server Port (8): Please input the port number of radius server here.*

*RADIUS Server Password (9): Please input the port number of radius password here.*

---

After you finish with the WEP settings, click “Apply” and the following message will be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-4-3-3 WPA - Wi-Fi Protected Access:

When you select this mode, the wireless Smart Repeater will use WPA encryption, and the following setup menu will be shown on your web browser:

The screenshot shows a web browser window titled "Security Settings". Below the title is a paragraph: "Secure your home wireless network below. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your home wireless network." Below this are four numbered configuration items: 1. "Encryption:" with a dropdown menu set to "WPA pre-shared key"; 2. "WPA Unicast Cipher Suite:" with three radio buttons: "WPA(TKIP)" (selected), "WPA2(AES)", and "WPA2 Mixed"; 3. "Pre-shared Key Format:" with a dropdown menu set to "Passphrase"; 4. "Pre-shared Key:" with an empty text input field. At the bottom right are "Apply" and "Cancel" buttons.

---

<i>WPA Unicast Cipher Suite (2):</i>	<i>Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.</i>
<i>Pre-shared Key Format (3):</i>	<i>Select the type of pre-shared key, you can select Passphrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).</i>
<i>Pre-shared Key (4):</i>	<i>Please input the WPA passphrase here. It's not recommended to use a word that can be found in a dictionary due to security reason.</i>

---

After you finish WPA Pre-shared key settings, click “Apply” and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

**NOTE: Some wireless clients (especially those manufactured before year 2003) only support WEP or WPA (TKIP) cipher. A driver upgrade would be needed for those clients to use WPA and WPA2 encryption.**



### 3-4-3-4 WPA RADIUS:

If you have a RADIUS server, this Smart Repeater can work with it and provide safer wireless authentication.

The screenshot shows a web interface titled "Security Settings". Below the title is a paragraph: "Secure your home wireless network below. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your home wireless network." The configuration area includes:  
1. Encryption: A dropdown menu set to "WPA RADIUS".  
2. WPA Unicast Cipher Suite: Three radio buttons for "WPA(TKIP)", "WPA2(AES)", and "WPA2 Mixed".  
3. RADIUS Server IP Address: An empty text input field.  
4. RADIUS Server Port: A text input field containing "1812".  
5. RADIUS Server Password: An empty text input field.  
At the bottom right are "Apply" and "Cancel" buttons.

---

<i>WPA Unicast Cipher Suite:</i>	<i>Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.</i>
<i>RADIUS Server IP address (3):</i>	<i>Please input the IP address of your Radius authentication server here.</i>
<i>RADIUS Server Port (4):</i>	<i>Please input the port number of your Radius authentication server here. <b>Default setting is 1812.</b></i>
<i>RADIUS Server Password (5):</i>	<i>Please input the password of your Radius authentication server here.</i>

---

After you finish with all of your settings, click “Apply” and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 3-4-4 Wireless Access Control

This function will help you to prevent unauthorized users from connecting to your wireless Smart Repeater; only those wireless devices who have the MAC address you assigned here can gain access to your wireless Smart Repeater. You can use this function with other security measures described in previous section, to create a safer wireless environment.

Up to 20 MAC addresses can be assigned by using this function. Click the 'Wireless' tab at the top of web management interface, then click 'Access Control', and the following message will be displayed on your web browser:

MAC Address Filtering Table - It allows 20 entries only.

NO.	MAC Address	Comment	Select
1			2 3 Delete Delete All

4  Enable Access Control

MAC Address	Comment
5 <input type="text"/>	6 <input type="text"/>

7 Add 8 Clear

Apply Cancel

All allowed MAC addresses will be displayed in 'MAC Address Filtering Table' (1).

*Delete Selected (2): If you want to delete a specific MAC address entry, check the 'select' box of the MAC address you want to delete, then click 'Delete Selected' button. (You can select more than one MAC addresses).*

*Delete All (3): If you want to delete all MAC addresses listed here, please click 'Delete All' button.*

*Enable Wireless Access Control (4):* To enforce MAC address filtering, you have to check 'Enable Wireless Access Control'. When this item is unchecked, wireless Smart Repeater will not enforce MAC address filtering of wireless clients.

*MAC Address (5):* Input the MAC address of your wireless devices here, dash ( - ) or colon ( : ) are not required. (i.e. If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or 'aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff'.

*Comment (6):* You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory aid.

*Add (7):* Click 'Add' button to add the MAC address and associated comment to the MAC address filtering table.

*Clear (8):* Click 'Clear' to remove the value you inputted in MAC address and comment field.

---

After you finish with all of your settings, click "Apply" and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### **3-4-5 WPS - Wi-Fi Protected Setup**

Wi-Fi Protected Setup (WPS) is the simplest way to build a secure connection between wireless users and the Smart Repeater. You do not have to select the specific wireless security encryption mode and input a long encryption passphrase each time a wireless user connects to your network. Instead you only have to press a button on wireless user's device (assuming WPS is supported by that device) and push the "WPS" button on the back of the Smart Repeater and WPS will automatically configure your wireless security settings and wireless connection.

This Smart Repeater supports two types of WPS modes: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the device of the wireless user (usually titled WPS) to start the WPS mode. In addition the Smart Repeater must be activated for WPS mode for the connection to work. You can push Reset/WPS button of the Smart Repeater, or click "Start PBC" button in the web configuration interface to do this; if you want to use a PIN code, you have to know the PIN code of the wireless device and switch it to WPS mode, then provide the PIN code of the wireless device you wish to connect to the Smart Repeater. The detailed instructions are below:

Click "Wireless Home" from the left side menu, then click "WPS", and the following message will be displayed:

## Wi-Fi Protected Setup (WPS)

This section allows you to change the setting for Wi-Fi Protected Setup (WPS). Wi-Fi Protected Setup can help your wireless client automatically connect to the Hi-Gain™ Wireless-N Dual Radio Smart Repeater.

1  Enable WPS

2 **WPS Information**

WPS Status: Unconfigured  
 PinCode Self:   
 SSID: default  
 Authentication Mode: Disable  
 Passphrase Key:

**Device Configure**

3 Config Mode: Registrar   
 4 Configure by Push Button:   
 5 Configure by Client PinCode:

*Enable WPS (1)*

*Check this box to enable WPS function, uncheck it to disable WPS.*

*Wi-Fi Protected Setup Information (2)*

*WPS-related system information will be displayed here*

*WPS Status: If the wireless security (encryption) function of this wireless Smart Repeater is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'Not configured'.*

*Self PIN code: This is the WPS PIN code of this wireless Smart Repeater. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices.*

*SSID: The SSID of the Smart Repeater will be displayed here.*

*Authentication Mode: The wireless security authentication mode of the Smart Repeater will be displayed here. If you do not enable the security function of the Smart Repeater before WPS is activated, the Smart Repeater will automatically set the security to WPA (AES) and generate a set passphrase key for a WPS connection.*

*Passphrase Key: The wireless security key of the Smart Repeater will be displayed here.*

*Config Mode (3)*

*There are “Registrar” and “Enrollee” modes for the WPS connection. When “Registrar” is enabled, the wireless clients will follow the Smart Repeater’s wireless settings for WPS connection. When “Enrollee” mode is enabled, the Smart Repeater will follow the wireless settings of wireless client for WPS connection.*

*Configure  
via Push Button (4)*

*Click “Start PBC” to start Push-Button style WPS setup procedure. The Smart Repeater will wait for WPS requests from wireless clients for 2 minutes. The “Wireless” LED on the Smart Repeater will be on steadily for 2 minutes while the Smart Repeater waits for incoming WPS requests.*

*Configure  
via client  
PinCode (5)*

*Please input the PIN code of the wireless client you wish to connect, and click “Start PIN” button.  
The “WLAN” LED on the wireless Smart Repeater will be steady on when this wireless Smart Repeater is waiting for incoming WPS request.*

---



### **3-4-6 Security Tips for Wireless Network**

Here are some quick tips to help you improve the security level of your wireless network:

1. Never use simple words (like school, apple and computer) as WEP encryption or WPA passphrase security keys.
2. A complicated (combination of numbers, alphabets, and even symbols) WEP key and WPA passphrase is much safer than short and simple ones. Remember that the wireless client is capable of keeping the key or passphrase for you, so you only have to input the complicated key or passphrase once.
3. You can hide the ESSID of this Smart Repeater by setting the “Broadcast ESSID” option to “Disable”. Your wireless Smart Repeater will not be found by other people in proximity if they’re just using the AP scanning function of their wireless client, and this can reduce the chance of being intruded.
4. Use “Access Control” function described in section 3-4-4, so those people who are not in your list will not be able to connect to your network.

## **Chapter IV: Advanced Functions**

### ***4-1 Quality of Service (QoS)***

Quality of service provides an efficient way for computers on the network to share the internet bandwidth with a preset connection quality of internet service. Without QoS, all computers and devices on the network will compete with each other to get internet bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephone) will be affected, therefore an undesirable result will occur, like the interruption of video / audio transfer.

With this function, you can limit the maximum bandwidth or give a guaranteed bandwidth to a specific user. This tool is very useful for bandwidth management for the network administrator.

#### **4-1-1 Basic QoS Settings**

Please follow the following instructions to set QoS parameters:

Please click ‘Applications and Gaming’ and click the ‘QoS’ tab at the top of web management interface and the following message will be displayed on your web browser:

1  Enable QoS

2 Total Download Bandwidth : --Select-- >> 0 kbits

3 Total Upload Bandwidth: --Select-- >> 0 kbits

4

Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select
5				
6				
7				
8				
9				
10				

Buttons: Add, Edit, Delete, Delete All, Move Up, Move Down, Apply, Cancel

*Enable QoS (1): Check this box to enable QoS function, unselect this box if you don't want to enforce QoS bandwidth limitations.*

*Total Download Bandwidth (2): You can set the limit of total download bandwidth in kbits. To disable download bandwidth limitation, input '0' here.*

*Total Upload Bandwidth (3): You can set the limit of total upload bandwidth in kbits. To disable upload bandwidth limitation, input "0" here.*

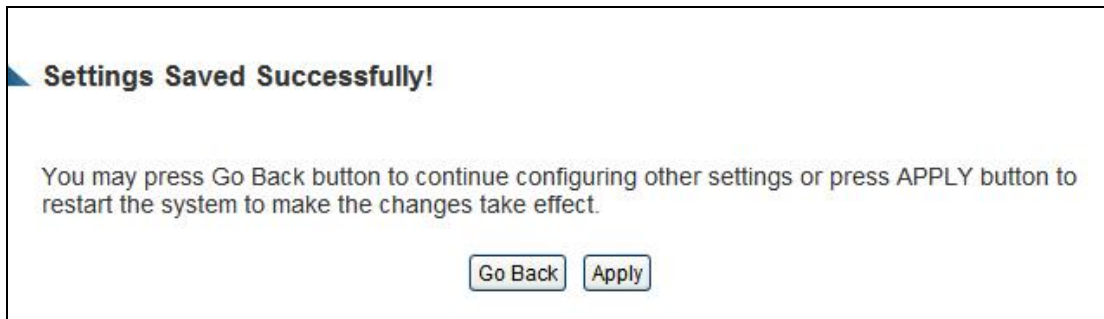
*Current QoS Table (4): All existing QoS rules will be displayed here.*

*Add (5): Click "add" button to add a new QoS rule, see section 4-1-2 "Add a new QoS rule" below.*

*Edit (6): If you want to modify the content of a specific rule, please check the "select" box of the rule you want to edit, then click "Edit" button. **Only one rule should be selected a time.** If you didn't select a rule before clicking 'Edit' button, you'll be prompted to add a new rule.*

- Delete Selected (7):* You can delete selected rules by clicking this button. You can select one or more rules to delete by check the “select” the box of the rule(s) you want to delete a time. **If the QoS table is empty, this button will be grayed out and cannot be clicked.**
- Delete All (8):* By clicking this button, you can delete all rules currently in the QoS table. **If the QoS table is empty, this button will be grayed out and cannot be clicked.**
- Move Up (9):* You can pull up the priority of the QoS rule you selected by clicking this button.
- Move Down (10):* You can lower the priority of the QoS rule you selected by clicking this button.
- 

After you finish with all of your settings, click “Apply” and the following message will be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

## 4-1-2 Add a new QoS rule

After you click “Add” button in QoS menu, the following message will appear:

**QoS**

This page allows users to add/modify the QoS rule's settings.

1 Rule Name :

2 Bandwidth :   Kbps

3 Local IP Address :  -

4 Local Port Range :

5 Remote IP Address :  -

6 Remote Port Range :

7 Traffic Type :

8 Protocol :

---

*Rule Name (1): Please give a name to this QoS rule (up to 15 alphanumerical characters)*

*Bandwidth (2): Set the bandwidth limitation of this QoS rule. You have to select the data direction of this rule (Upload of Download), and the speed of bandwidth limitation in Kbps, then select the type of QoS: “guarantee” (guaranteed usable bandwidth for this rule) or “max” (set the maximum bandwidth for the application allowed by this rule).*

*Local IP Address (3): Specify the local (source) IP address that will be affected by this rule. Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.*

<i>Local Port Range (4):</i>	<i>Please input the range of local (source) port number that will be affected by this rule. If you want to apply this rule on port 80 to 90, please input “80-90”; if you want to apply this rule on a single port, just input the port number, like “80”.</i>
<i>Remote IP Address: (5):</i>	<i>Specify the remote (destination) IP address that will be affected by this rule. Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.</i>
<i>Remote Port Range (6):</i>	<i>Please input the range of remote (destination) port number that will be affected by this rule. If you want to apply this rule on port 80 to 90, please input “80-90”; if you want to apply this rule on a single port, just input the port number, like “80”. If the remote (destination) IP address and /or port number is universal, just leave it blank.</i>
<i>Traffic Type (7):</i>	<i>Please select the traffic type of this rule, available options are None, SMTP, HTTP, POP3, and FTP. You can select a specific traffic type for this rule, if you want to make this rule as a IP address based rule (apply the limitation on all traffics from / to the specified IP address / port number), select “None”.</i>
<i>Protocol (8):</i>	<i>Please select the protocol type of this rule, available options are TCP and UDP. If you don't know what protocol your application uses, please try 'TCP' first, and switch to “UDP” if this rule doesn't seems to work.</i>

---

After you finish with all settings, click “Save” (9). You will be brought back to previous menu, and the rule you just set will appear in current QoS table; if you did anything wrong, you'll get an error message when you click “Save”, correct your input by the instructions given by the error message.

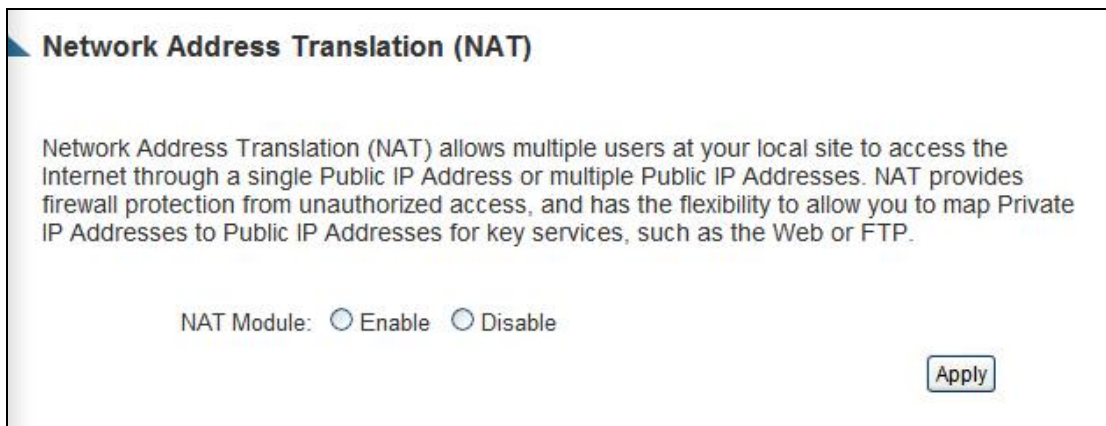
## ***4-2 Network Address Translation (NAT)***

Network address translations solve the problem of sharing a single IP address with multiple computers. Without NAT, all computers must be assigned with a valid Internet IP address to get connected to Internet, but Internet service providers only provide very few IP addresses to every user. Therefore it's necessary to use NAT technology to share a single Internet IP address to multiple computers on local network, so everyone can connect to the Internet.

Please follow these instructions to set NAT parameters:

### **4-2-1 Basic NAT Settings (Enable or disable NAT function)**

Click the 'NAT' tab at the top of web management interface, and the following message will be displayed on your web browser:



**Network Address Translation (NAT)**

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides firewall protection from unauthorized access, and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services, such as the Web or FTP.

NAT Module:  Enable  Disable

Apply

To enable NAT function, select “Enable” for “Enable NAT module function”; to disable, please select “Disable”.

After you have made the selection, click “Apply” and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings made and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.



## 4-2-2 Port Forwarding

This function allows you to redirect a single port or consecutive ports of Internet IP address to the same port of the IP address on local network. The port number(s) of Internet IP address and private IP address (the IP address on local network) must be the same. If the port number of Internet IP address and private IP address is different, please use ‘Virtual Server’ function, described in next section.

Click the “Apps and Gaming” tab at the top of web management interface, then click “Port Forwarding”. The following message will be displayed on your web browser:

1  Enable Port Forwarding

Private IP	Computer Name	Type	Port Range	Select
<input type="text"/>	<< -----Select-----	Both	<input type="text"/> - <input type="text"/>	<input type="text"/>

2 3 4 5 6 Add 7 Reset 8

9 Current Port Forwarding Table

No.	Computer Name	Private IP	Type	Port Range	Comment	Select
-----	---------------	------------	------	------------	---------	--------

10 Delete 11 Delete All 12 Reset

Apply Cancel

*Enable Port Forwarding (1):* Check this box to enable port mapping, and uncheck this box to disable port mapping.

*Private IP (2):* Input the IP address of the computer on local network which provides internet service.

*Computer Name (3):* Pull down the menu and all the computers connected to the Smart Repeater will be listed here. You can easily to select the computer name without checking the IP address of the computer.

<i>Type (4):</i>	<i>Select the type of connection, TCP or UDP. If you're not sure, please select 'Both'.</i>
<i>Port Range (5):</i>	<i>Input the starting port number in the left field, and input the ending port number in the right field. If you only want to redirect a single port number, just fill the port number in the left field.</i>
<i>Comment (6):</i>	<i>Please input any text to describe this mapping, up to 16 alphanumerical characters.</i>
<i>Add (7):</i>	<i>Add the mapping to port forwarding table.</i>
<i>Reset (8):</i>	<i>Remove all inputted values.</i>
<i>Port Forwarding Table (9):</i>	<i>All existing port forwarding mappings will be displayed here.</i>
<i>Delete Selected (10):</i>	<i>Please select a port forwarding mapping by clicking the "Select" box of the mapping, then click "Delete Selected" button to remove the mapping. If there's no existing mapping, this button will be grayed out.</i>
<i>Delete All (11):</i>	<i>Delete all mappings existed in virtual server table.</i>
<i>Reset (12):</i>	<i>Unselect all mappings.</i>

---

After you finish with all of your settings, click "Apply" and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 4-2-3 Virtual Server

This function allows you to redirect a port on Internet IP address (on WAN port) to a specified port of an IP address on the local network. This allows you to setup an Internet service on the computer on the local network, without exposing it on the Internet directly. You can also build many sets of port redirections to provide many different Internet services on different local computers via a single Internet IP address.

Click “Apps and Gaming” on top of web management interface, then click “Virtual Server”, and the following message will be displayed on your web browser:

1  Enable Virtual Server

Private IP	Computer Name	Private Port	Type	Public Port	Comment
<input type="text"/>	<< -----Select----- >>	<input type="text"/>	Both	<input type="text"/>	<input type="text"/>

2 3 4 5 6 7

8 Add 9 Reset

10 Current Virtual Server Table

No.	Computer Name	Private IP	Private Port	Type	Public Port	Comment	Select

11 Delete 12 Delete All 13 Reset

Apply Cancel

Here are descriptions of every setup items:

---

*Enable Virtual Server (1):* Check this box to enable virtual server, and uncheck this box to disable virtual server.

*Private IP (2):* Input the IP address of the computer which provides Internet service.

*Computer Name (3): Pull down the menu and all the computers connected to the Smart Repeater will be listed here. You can easily to select the computer name without checking the IP address of the computer.*

*Private Port (4): Input the port number of the IP address which provides Internet service.*

*Type (5): Select the type of connection, TCP or UDP. If you're not sure, please select 'Both'.*

*Public Port (6): Please select the port number of Internet IP address which will be redirected to the port number of local IP address defined above.*

*Comment (7): Please input any text to describe this mapping, up to 16 alphanumerical characters.*

*Add (8): Add the mapping to virtual server table.*

*Reset (9): Remove all inputted values.*

*Virtual Server Table (10): All existing virtual server mappings will be displayed here.*

*Delete Selected (11): Please select a virtual server mapping by clicking the "Select" box of the mapping, then click "Delete Selected" button to remove the mapping. If there's no existing mapping, this button will be grayed out.*

*Delete All (12): Delete all mappings existed in virtual server table.*

*Reset (13): Unselect all mappings.*

---

After you finish with all of your settings, click "Apply" and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

## 4-2-4 Port Mapping for Special Applications

Some applications require more than one connection at a time; these applications won't work with simple NAT rules. In order to make these applications work, you can use this function to let these applications work. Go to "Apps and Gaming" and click "Special Applications".

1  Enable Special Applications

IP Address	Computer Name	TCP Port to Open	UDP Port to Open	Comment
0.0.0.0	<< -----Select-----			

Popular Applications: -----Select----- Add

7

Add 8 Reset 9

10: Current Trigger-Port Table

No.	Computer Name	IP Address	TCP Port to Open	UDP Port to Open	Comment	Select
-----	---------------	------------	------------------	------------------	---------	--------

Delete 11 Delete All 12 Reset 13

Apply Cancel

**Enable (1):** Check this box to enable special applications and uncheck this box to disable virtual server.

**IP Address (2):** Input the IP address of the computer which you want to open the ports.

**Computer Name (3):** Pull down the menu and all the computers connected to the Smart Repeater will be listed here. You can easily to select the computer name without checking the IP address of the computer.

**TCP Port to Open (4):** This is the out going (Outbound) range of TCP port numbers for this particular application.

*UDP Port to Open (5): This is the out going (Outbound) range of UDP port numbers for this particular application.*

*Comment (6): The description of this setting.*

*Pop. Applications This section lists the more popular applications that (7): require multiple connections. Select an application from the Popular Applications selection and click 'Add' to save the setting to "Current Trigger-Port Table".*

*Add (8): Add the setting to the "Current Trigger-Port Table".*

*Reset (9): Click "Reset" will clear all above setting and you can set up again.*

*Current Trigger-Port (10): All the settings for the special applications will be listed here. If you want to remove some Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Application settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.*

*Delete Selected (11): Please select a special application by clicking the 'Select' box of the mapping, then click 'Delete Selected' button to remove the setting. If there's no setting here, this button will be grayed out.*

*Delete All (12): Delete all settings existed in trigger port table.*

---

Note: Only one LAN client can use a particular special application at a time.



After you finish with all of your settings, click “Apply” and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

## 4-2-5 UPnP Setting

This function enables network auto-configuration for peer-to-peer communications, with this function, network devices will be able to communicate with other devices directly, and learn information about other devices. Many network devices and applications rely on UPnP functions nowadays.

Click “Apps and Gaming” at top of web management interface, then click “UPnP”, and the following message will be displayed on your web browser:

### UPnP Settings

UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices—all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.

Note: This service may not function properly if your Repeater is behind another firewall.

UPnP Module:  Enable  Disable

There is only one option in this page, select “Enable” or “Disable” to enable or disable UPnP function. Click “Apply”, and the following message will be displayed on your web browser:

### Settings Saved Successfully!

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take

effect after it reboots.

## 4-2-6 ALG Settings

Application Layer Gateway (ALG) is a special function of this Smart Repeater. It includes many preset routing rules for numerous applications which require special support. With these supports, those applications which required special support will be able to work with NAT architecture.

Click the “Apps and Gaming” tab at the top of web management interface, then click “ALG Settings”, and the following message will be displayed on your web browser:

### Application Layer Gateway (ALG) Settings

Below are applications that need Hi-Gain™ Wireless-N Dual Radio Smart Repeater's special support to function properly under the NAT. Select the applications below.

Enable	Name	Comment
<input checked="" type="checkbox"/>	Amanda	Support for Amanda backup tool protocol.
<input checked="" type="checkbox"/>	Egg	Support for eggdrop bot networks.
<input checked="" type="checkbox"/>	FTP	Support for FTP.
<input checked="" type="checkbox"/>	H323	Support for H323/netmeeting.
<input checked="" type="checkbox"/>	IRC	Allows DCC to work though NAT and connection tracking.
<input checked="" type="checkbox"/>	MMS	Support for Microsoft Streaming Media Services protocol.
<input checked="" type="checkbox"/>	Quake3	Support for Quake III Arena connection tracking and nat.
<input checked="" type="checkbox"/>	Talk	Allows netfilter to track talk connections.
<input checked="" type="checkbox"/>	TFTP	Support for TFTP.
<input checked="" type="checkbox"/>	IPsec	Support for IPsec passthrough
<input type="checkbox"/>	Starcraft	Support for Starcraft/Battle.net game protocol.
<input type="checkbox"/>	MSN	Support for MSN file tranfer.
<input type="checkbox"/>	PPTP Pass Through	Support for PPTP passthrough.

There are many applications listed here. Check the box for the special support for applications you need, and then click “Apply” and the following message will be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 4-3 Firewall

Besides NAT, this Smart Repeater also provides firewall function to block malicious intruders from accessing your computers on local network. These functions include inbound attack prevention and blocking outbound traffic, like URLs which have pre-defined keywords.

Please follow these instructions to enable or disable firewall function:

Click “Security” tab at top of web management interface, and the following message will be displayed on your web browser:

#### Firewall

The Hi-Gain™ Wireless-300N Smart Repeater Pro provides extensive firewall protection by restricting connection parameters, thus limiting the risk of unauthorized access, and defending against a wide array of common attacks. Most wireless Internet connections will have a pre-existing firewall enabled. If you wish to configure your own firewall settings, click enable below.

Firewall Module:  Enable  Disable

Apply

Please select “Enable” or “Disable” to enable or disable firewall function of this Smart Repeater, then click “Apply”, and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Go Back Apply

Press “Go Back” to save the settings made and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 4-3-1 Access Control

This function allows or denies computers with specific MAC address from connecting to the network; it can also allow or deny computers with specific IP address, protocol, or port.

Click “Security” tab at the top of web management interface, then click “Access Control”, and the following message will be displayed on your web browser:

1  Enable MAC Filtering

Client PC MAC Address	Computer Name	Comment
2 <input type="text"/>	3 << -----Select----- >>	4 <input type="text"/>
		5 <input type="button" value="Add"/> <input type="button" value="Reset"/>

---

7 Current MAC Filtering Table

No.	Computer Name	Client PC MAC Address	Comment	Select
				8 <input type="button" value="Delete"/> 9 <input type="button" value="Delete All"/> 10 <input type="button" value="Reset"/>

---

11  Enable IP Filtering  Deny  Allow

No.	Client PC Description	Client PC IP Address	Client Service	Protocol	Port Range	Select
		12				<input type="button" value="Add PC"/> <input type="button" value="Delete"/> <input type="button" value="Delete All"/>
					13 14 15	

*Enable MAC Filtering (1):*

*Check this box to enable MAC address based filtering, and please select “Deny” or “Allow” to decide the behavior of MAC filtering table. If you select deny, all MAC addresses listed in filtering table will be denied from connecting to the network; if you select allow, only MAC addresses listed in filtering table will be able to connect to the network, and rejecting all*



*other network devices.*

- Client PC  
MAC address (2):* Please input the MAC address of computer or network device here, dash ( - ) or colon ( : ) are not required. (i.e. If the MAC address label of your wireless device indicates “aa-bb-cc-dd-ee-ff” or “aa:bb:cc:dd:ee:ff”, just input “aabbccddeeff”
- Computer Name (3):* Pull down the menu and all the computers connected to the Smart Repeater will be listed here. You can easily to select the computer name without checking the IP address of the computer.
- Comment (4):* You can input any text here as the comment of this MAC address, like “ROOM 2A Computer” or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it’s recommended to use this field to write a comment for every MAC addresses as a memory aid.
- Add (5):* Click “Add” button to add the MAC address and associated comment to the MAC address filtering table.
- Reset (6):* Remove all inputted values.
- MAC Filtering Table (7):* All existing MAC addresses in filtering table will be listed here.
- Delete Selected (8):* If you want to delete a specific MAC address entry, check the “select” box of the MAC address you want to delete, then click “Delete Selected” button. (You can select more than one MAC addresses).
- Delete All (9):* If you want to delete all MAC addresses listed here, please click “Delete All” button.
- Reset (10):* You can also click “Reset” button to unselect all MAC addresses.

*Enable IP Filtering Table (11):*      *Check this box to enable IP address based filtering, and please select “Deny” or “Allow” to decide the behavior of IP filtering table. If you select deny, all IP addresses listed in filtering table will be denied from connecting to the network; if you select allow, only IP addresses listed in filtering table will be able to connect to the network, and rejecting all other network devices.*

*IP Filtering Table (12):*      *All existing IP addresses in filtering table will be listed here.*

*Add PC (13):*      *Click this button to add a new IP address to IP filtering table, up to 20 IP addresses can be added. Please refer to section 4-3-1-1 “Add PC” below.*

*Delete Selected (14):*      *If you want to delete a specific IP address entry, check the “select” box of the IP address you want to delete, then click “Delete Selected” button. (You can select more than one IP addresses).*

*Delete All (15):*      *If you want to delete all IP addresses listed here, please click “Delete All” button.*

---

After you finish with all of your settings, click “Apply” and the following message will be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take

effect after it reboots.

### 4-3-1-1 Add PC

After button is clicked, the following message will be displayed on your web browser:

1 Client PC Description :

2 Client PC IP address :  -

**Client PC Service :**

Service Name	Detail Description	Select
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 389,522,1503,1720,1731	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

3

**User Define Service :**

4 Protocol :

5 Port Range :

6

*Client PC  
Description (1):*

*Please input any text to describe this IP  
address, up to 16 alphanumerical characters.*

*Client PC IP address (2):* Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.

*Client PC Service (3):* Please check all services you want to allow or deny this IP address to use, you can check multiple services.

*Protocol (4):* If the service you need is not listed above, you can create a new service on your own. Please select TCP or UDP, if you're not sure, please select "Both".

*Port Range (5):* Please input the port range of new service here. If you want to specify port 80 to 90, please input "80-90"; if you want to apply this rule on a single port, just input the port number, like "80".

*Add (6):* When you finish with all settings, please click "Add" to save settings, you'll be brought back to previous menu, and the rule you just set will appear in current IP filtering table.

---

If you want to remove all settings on this page, click the "Reset" button.

### 4-3-2 URL Blocking

If you want to prevent computers in a local network from accessing certain websites (like pornography, violence, or anything you wish to block), you can use this function to stop computers in a local network from accessing the site you define here.

This function is useful for parents and company managers.

Follow these instructions to set URL blocking parameters:

Please click “Security” tab at top of web management interface, then click “URL Blocking”, and the following message will be displayed on your web browser:

The screenshot shows a web management interface titled "URL Blocking". It contains the following elements:

- 1**: A checkbox labeled "Enable URL Blocking".
- 2**: A text input field for "URL/Keyword" with "http://" pre-filled.
- 3**: An "Add" button.
- 4**: A "Reset" button.
- 5**: A section header "Current URL Blocking Table".
- 6**: A "Delete" button.
- 7**: A "Delete All" button.
- 8**: A "Reset" button.
- 9**: "Apply" and "Cancel" buttons.

No.	URL/Keyword	Select
-----	-------------	--------

Here are descriptions of every setup items:

*Enable URL*

*Check this box to enforce URL Blocking,*

- Blocking (1): uncheck it to disable URL Blocking.*
- URL/Keyword (2): Input the URL (host name or IP address of website, like <http://www.blocked-site.com> or <http://11.22.33.44>), or the keyword which is contained in URL (like pornography, cartoon, stock, or anything).*
- Add (3): Click 'Add' button to add the URL / keyword to the URL / Keyword filtering table.*
- Reset (4): Click 'Reset' to remove the value you inputted in URL/Keyword field.*
- Current URL Blocking Table (5): All existing URL/Keywords in filtering table will be listed here.*
- Delete Selected (6): If you want to delete a specific URL/Keyword entry, check the "select" box of the MAC address you want to delete, then click "Delete Selected" button. (You can select more than one MAC addresses).*
- Delete All (7): If you want to delete all URL/Keyword listed here, please click "Delete All" button.*
- Reset (8): You can also click "Reset" button to unselect all URL/Keywords.*
- 

After you finish with all of your settings, click "Apply", and the following message will be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.



### 4-3-3 DoS Attack Prevention

Denial of Service (DoS) is a common attack measure, by transmitting a great amount of data or request to your Internet IP address and server, the Internet connection will become very slow, and server may stop responding because it is not capable of handling too much traffic.

This Smart Repeater has a built-in DoS attack prevention mechanism; when you activate it, the Smart Repeater will stop the DoS attack for you.

Please follow these instructions to set DoS prevention parameters:

Click the “Security” tab at the top of web management interface, then click “DoS”, and the following message will be displayed on your web browser:

The screenshot shows a web management interface for the Denial of Service (DoS) configuration. At the top, there is a header "Denial of Service (DoS)". Below the header, a paragraph states: "The Hi-Gain™ Wireless-N Dual Radio Smart Repeater's firewall can block common unauthorized access or intrusions, including DoS, Discard Ping from WAN and Port Scan." Below this text is a "DoS Module" section with four checkboxes: "1 Ping of Death: ", "2 Discard Ping from WAN: ", "3 Port Scan: ", and "4 Sync Flood: ". Below these checkboxes is an "Advanced Settings" button, which is labeled with the number "5". At the bottom right of the form are "Apply" and "Cancel" buttons.

---

*Ping of Death (1): Ping of Death is a special packet, and it will cause certain computer to stop responding. Check this box and the Smart*

*Repeater will filter this kind of packet out.*

*Discard Ping  
From WAN (2):*

*Ping is a common and useful tool to know the connection status of a specified remote network device, but some malicious intruder will try to fill your network bandwidth with a lot of PING request data packet, to make your internet connection become very slow, even unusable. Check this box and the Smart Repeater will ignore all inbound PING request, but when you activate this function, you will not be able to ping your own Smart Repeater from internet, too.*

*Port Scan (3):*

*Some malicious intruder will try to use a 'port scanner' to know how many ports of your Internet IP address are open, and they can collect a lot of valuable information by doing so. Check this box and the Smart Repeater will block all traffics which are trying to scan your Internet IP address.*

*Sync Flood (4):*

*This is another kind of attack, which uses a lot of fake connection request to consume the memory of your server, and try to make your server become unusable. Check this box and the Smart Repeater will filter this kind of traffic out.*

*Advanced  
Settings (5):*

*Click this button and you can set advanced settings of the DoS prevention method listed above, please see section 4-3-3-1 'DoS – Advanced Settings' below.*

---

After you finish with all of your settings, click “Apply” and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 4-3-3-1 DoS - Advanced Settings

When you click “Advanced” in DoS menu, the following message will be displayed on your web browser:

The screenshot shows a configuration window titled "DoS Module" with the following settings:

- 1  Ping of Death: 5 Packet(s) per Second Burst 5
- 2  Discard Ping from WAN
- 3  Port Scan
  - NMAP FIN / URG / PSH
  - Xmas tree
  - Another Xmas tree
  - Null scan
  - SYN / RST
  - SYN / FIN
  - SYN (only unreachable port)
- 4  Sync Flood: 30 Packet(s) per Second Burst 30

Buttons: Apply, Cancel

---

*Ping of Death (1): Set the threshold of when this DoS prevention mechanism will be activated. Please check the box of Ping of Death, and input the frequency of threshold (how many packets per second, minute, or hour), you can also input the “Burst” value, which means when this number of “Ping of Death” packet is received in very short time, this DoS prevention mechanism will be activated.*

*Discard Ping From WAN (2): Check the box to activate this DoS prevention mechanism.*

*Port Scan (3): Many kind of port scan methods are listed here, please check one or more DoS attack methods you want to prevent.*

*Sync Flood (4): Like Ping of Death, you can set the threshold of when this DoS prevention mechanism will be activated.*

---

After you finish with all of your settings, click “Apply” and the following message will

be displayed on your web browser:



Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.

### 4-3-4 Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ) refers to a special area in your local network. This area resides in the local network, and all computers in this area use private IP addresses, too. But these private IP addresses are mapped to a certain Internet IP address, so other people on the Internet can fully access those computers in the DMZ.

Please follow the instructions to set DMZ parameters:

Click the “Security” tab at the top of web management interface, then click “DMZ”, and the following message will be displayed on your web browser:

1  Enable DMZ

URL/Keyword	Client IP Address	Computer Name
<input type="radio"/> Dynamic IP 2	Session 1	Local Host
<input type="radio"/> Static IP	3	4

5 Add 6 Reset

7 Current DMZ Table

No.	Computer Name	Public IP	Client IP Address	Select
-----	---------------	-----------	-------------------	--------

8 Delete 9 Delete All 10 Reset

Apply Cancel

*Enable DMZ (1): Check this box to enable DMZ function, uncheck this box to disable DMZ function.*

- Public IP address (2):* You can select 'Dynamic IP' or 'Static IP' here. If you select 'Dynamic IP', you have to select an Internet connection session from dropdown menu; if you select 'Static IP', please input the IP address that you want to map to a specific private IP address.
- Client PC IP address (3):* Please input the private IP address that the Internet IP address will be mapped to.
- Computer Name (4):* Pull down the menu and all the computers connected to the Smart Repeater will be listed here. You can easily to select the computer name without checking the IP address of the computer.
- Add (5):* Click 'Add' button to add the public IP address and associated private IP address to the DMZ table.
- Reset (6):* Click 'Clear' to remove the value you inputted in Public IP address and Client PC IP address field.
- Current DMZ table (7):* All existing public IP address and private IP address mapping will be displayed here.
- Delete Selected (8):* If you want to delete a specific DMZ entry, check the 'select' box of the DMZ entry you want to delete, then click 'Delete Selected' button. (You can select more than one DMZ entries).
- Delete All (9):* If you want to delete all DMZ entries listed here, please click 'Delete All' button.
- Reset (10):* You can also click 'Reset' button to unselect all DMZ entries.

After you finish with all of your settings, click "Apply" and the following message will be displayed on your web browser:

**Settings Saved Successfully!**

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

Press “Go Back” to save the settings and go back to the web management interface; press “Apply” to save the settings made and restart the Smart Repeater. The settings will take effect after it reboots.



## 4-4 System Status

The functions described here will provide you with system related information. To enter system status menu, either click “Status” link located at the upper-right corner of web management interface, or click “Status” button in main menu.

### 4-4-1 System information and firmware version

You can use this function to know the system information and firmware version of this Smart Repeater.

Click the “Status” link located at the upper-right corner of web management interface, and the following message will be displayed on your web browser

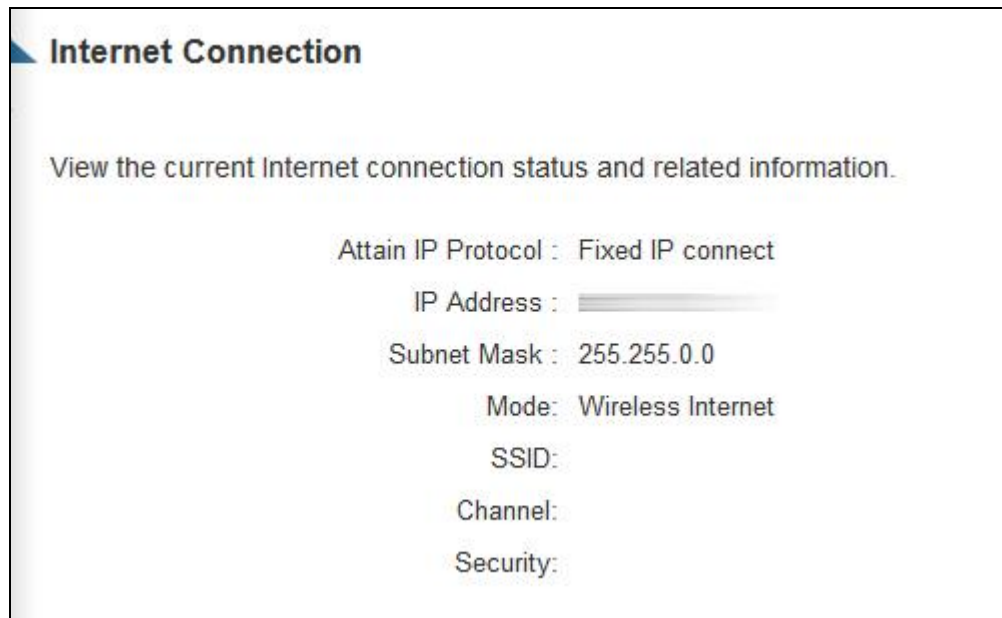


**NOTE: Information displayed here may vary.**

## 4-4-2 Internet Connection Status

You can use this function to view the status of your current Internet connection.

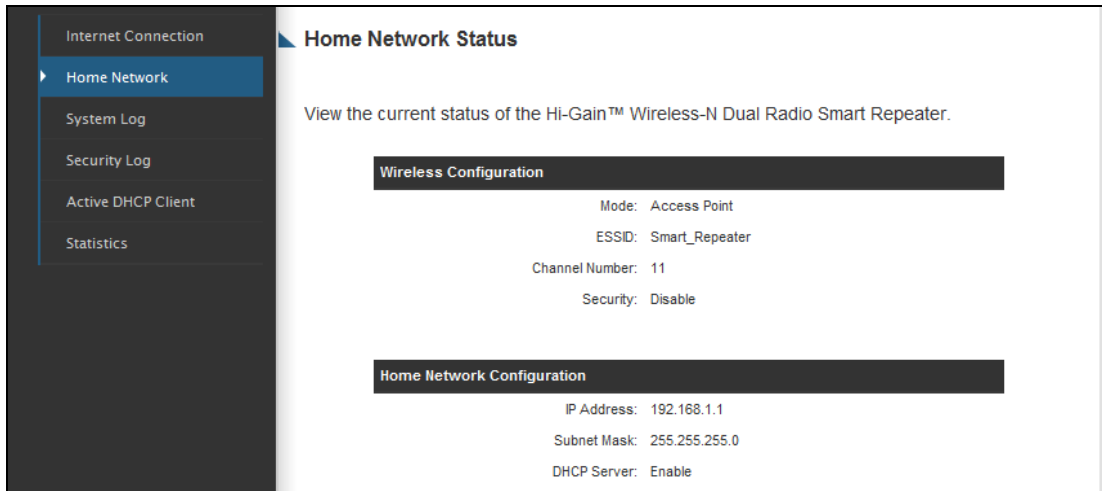
Click 'Status' menu at the top of web management interface, then select 'Internet Connection' from the left hand menu and the following message will be displayed:



This information will vary depending on the connection status and the type of internet connection that you are using. It will provide IP information, the Internet connection mode (i.e. wired or wireless) as well as the details of a wireless connection.

### 4-4-3 Home Network

The Home Network status page displays information regarding your local wireless home network and your wired home network. It will display the SSID of your home wireless network as well as the LAN IP settings of your home wired network.



The screenshot shows a web interface with a dark sidebar on the left containing navigation links: Internet Connection, Home Network (selected), System Log, Security Log, Active DHCP Client, and Statistics. The main content area is titled "Home Network Status" and includes a sub-header "View the current status of the Hi-Gain™ Wireless-N Dual Radio Smart Repeater." Below this, there are two configuration sections:

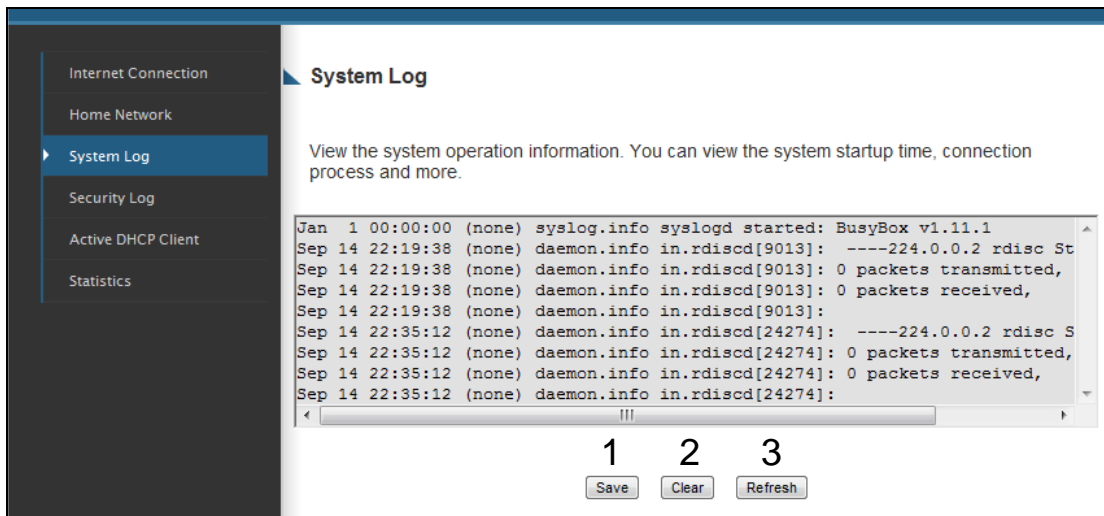
- Wireless Configuration**
  - Mode: Access Point
  - ESSID: Smart\_Repeater
  - Channel Number: 11
  - Security: Disable
- Home Network Configuration**
  - IP Address: 192.168.1.1
  - Subnet Mask: 255.255.255.0
  - DHCP Server: Enable

This information will vary depending on the device status.

## 4-4-4 System Log

Important system events are logged here. You can use this function to check the event log of your Smart Repeater.

Click the “System Log” tab at the top of web management interface, and the following will be displayed on your web browser:



The system events will be displayed in this page, and here are descriptions of every buttons:

---

*Save (1):*                      *Save current event log to a text file.*

*Clear (2):*                    *Delete all event logs displayed here.*

---

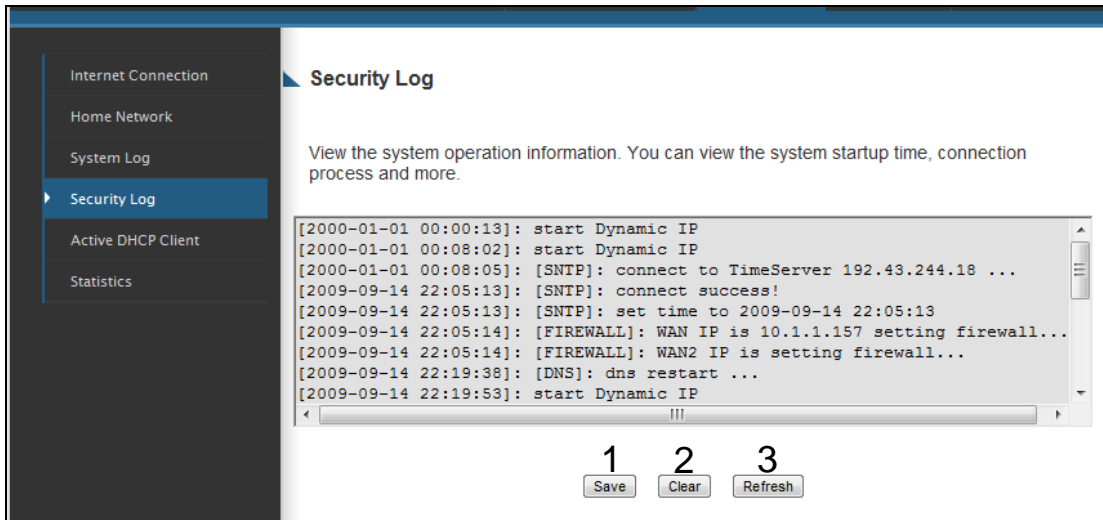
*Refresh (3):*                 *Refresh the event log display.*

---

#### 4-4-5 Security Log

Information regarding your network and system security is kept here. You may use this function to check the security event log of your Smart Repeater.

Click the “Security Log” tab at the top of web management interface, and the following message will be displayed on your web browser:



The system events will be displayed in this page:

---

*Save (1):*                      *Save current event log to a text file.*

*Clear (2):*                    *Delete all event logs displayed here.*

*Refresh (3):*                 *Refresh the event log display.*

---

#### 4-4-5 Active DHCP client list

If you're using the DHCP server function of this Smart Repeater, you can use this function to check all active DHCP leases issued by this Smart Repeater.

Click the "Active DHCP client" tab at the top of web management interface, and the following message will be displayed on your web browser:

### Active DHCP Client

This section shows the assigned IP address, MAC address and time expired for each DHCP leased client.

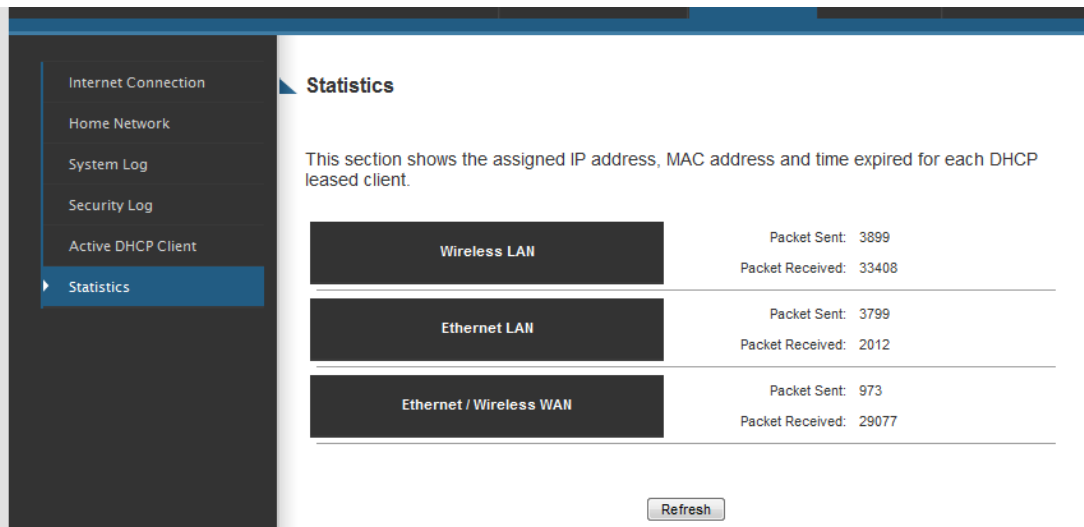
Wireless Configuration	MAC Address	Time Expired (Second)
192.168.2.103		forever

All information about active DHCP leases issued by this Smart Repeater will be displayed here. You can click "Refresh" button to display latest information.

## 4-4-6 Statistics

You can use this function to check the statistics of wireless, LAN, and WAN interface of this Smart Repeater.

Click the “Statistics” tab at the top of web management interface, and the following message will be displayed on your web browser:



The screenshot shows a web management interface with a dark sidebar on the left containing navigation options: Internet Connection, Home Network, System Log, Security Log, Active DHCP Client, and Statistics (highlighted). The main content area is titled "Statistics" and includes a descriptive text: "This section shows the assigned IP address, MAC address and time expired for each DHCP leased client." Below this text is a table of statistics for three network interfaces. A "Refresh" button is positioned at the bottom right of the table area.

Interface	Packet Sent	Packet Received
Wireless LAN	3899	33408
Ethernet LAN	3799	2012
Ethernet / Wireless WAN	973	29077

You can click “Refresh” button to display latest information.

## 4-5 Configuration Backup and Restore

You can backup all configurations of this Smart Repeater to a file, so you can make several copies of Smart Repeater configuration for security reasons.

To backup or restore a Smart Repeater configuration, follow these instructions:

Click the “Admin” tab located at the upper-right of web management interface, then click “Configuration Tools”. The following message will be displayed on your web browser:

**Configuration Tools**

Use the "Backup" tool to save the Hi-Gain™ Wireless-N Dual Radio Smart Repeater's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Repeater. Alternatively, you can use the "Restore to Factory Default" tool to force the Repeater to perform System Reset and restore the original factory settings.

1 Backup Settings

---

2 Restore Settings

3 Restore to Factory Default

---

*Backup Settings (1):* Press “Save”, and you will be prompted to download the configuration as a file, default filename is “default.bin”, you can please save it as another filename for different versions, and keep it in a safe place.

*Restore Settings (2):* Press “Browse” to pick a previously-saved configuration file from your computer, and then click “Upload” to transfer the configuration file to Smart Repeater. After the configuration is uploaded, the Smart Repeater’s configuration will be replaced by the file you just uploaded.



*Restore to*                      *Press “Reset” to remove all settings*  
*Factory Default (3):*      *you made, and restore the configuration of this*  
   *Smart Repeater back to factory default settings.*

---

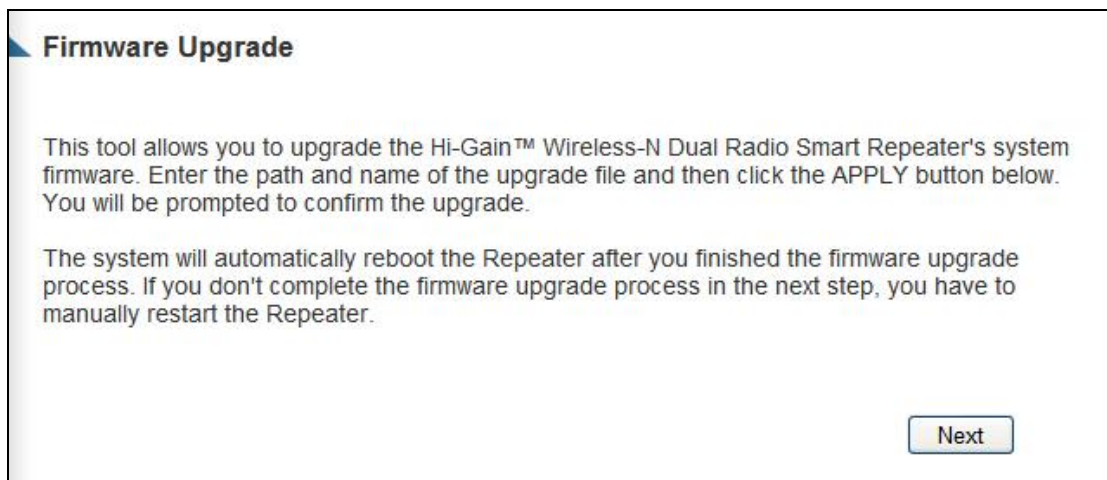
## ***4-6 Firmware Upgrade***

The system software used by this Smart Repeater is known as ‘firmware’, just like any applications on your computer, when you replace the old application with a new one; your hardware will be equipped with new functions. You can also use this firmware upgrade to add new functions to your Smart Repeater, even fix the bugs on this Smart Repeater.

To upgrade firmware, follow these instructions:

Check what version of the firmware you have. Refer to Section 4-4. It will be the “Runtime Code Version”. Go to [www.hawkingtech.com](http://www.hawkingtech.com) to check what the latest firmware version is. If your current version is older than the one on our website, download the firmware file, save it to your computer and proceed with the following steps.

Please click “Admin” tab located at the upper-right corner of web management interface, then click “Firmware Upgrade”. The following message will be displayed on your web browser:



### Firmware Upgrade

This tool allows you to upgrade the Hi-Gain™ Wireless-N Dual Radio Smart Repeater's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

Click “Browse” first, you’ll be prompted to provide the filename of the firmware upgrade file. Choose the file you downloaded earlier.

After a firmware upgrade file is selected, click “Apply”, and the Smart Repeater will start firmware upgrade procedure automatically. The procedure may take several minutes, please be patient.

**NOTE: Never interrupt the upgrade procedure by closing the web browser or physically disconnecting your computer from Smart Repeater. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may have to return this Smart Repeater to the dealer of purchase to ask for help. (Warranty is void if you interrupt the upgrade procedure).**

## ***4-7 System Reboot***

If you think your network performance is bad, or you find the behavior of the Smart Repeater is strange, you can perform a Smart Repeater reboot. It may solve the problem.

To do so, click the “Tools” tab located at the upper-right corner of web management interface, then click “Reboot:” The following message will be displayed on your web browser:

**Reboot**

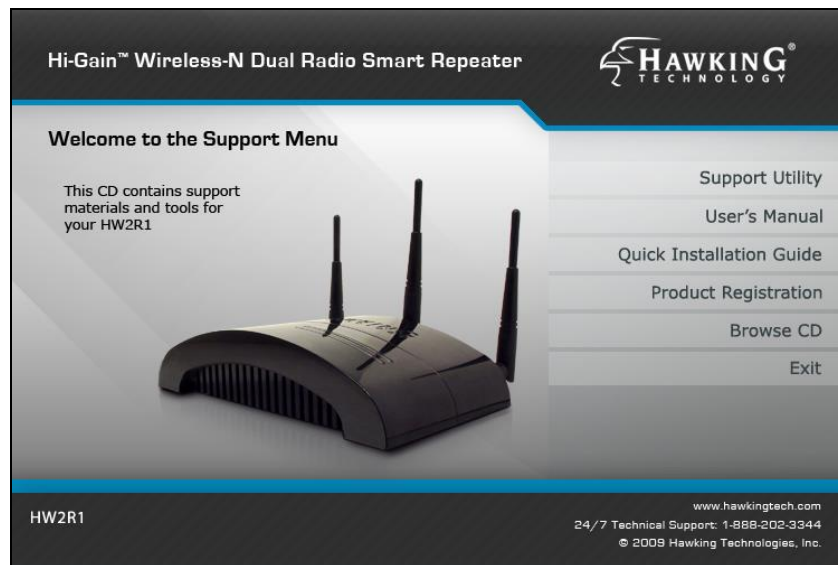
In the event that the system stops responding correctly or stops functioning, you can perform a Reboot. Your settings will not be changed. To perform the reboot, click on the Apply button below. You will be asked to confirm your decision. The reboot will be complete when the LED Power light stops blinking.

Click “Apply” to reboot your Smart Repeater, and it will be available again after a few minutes, please be patient.

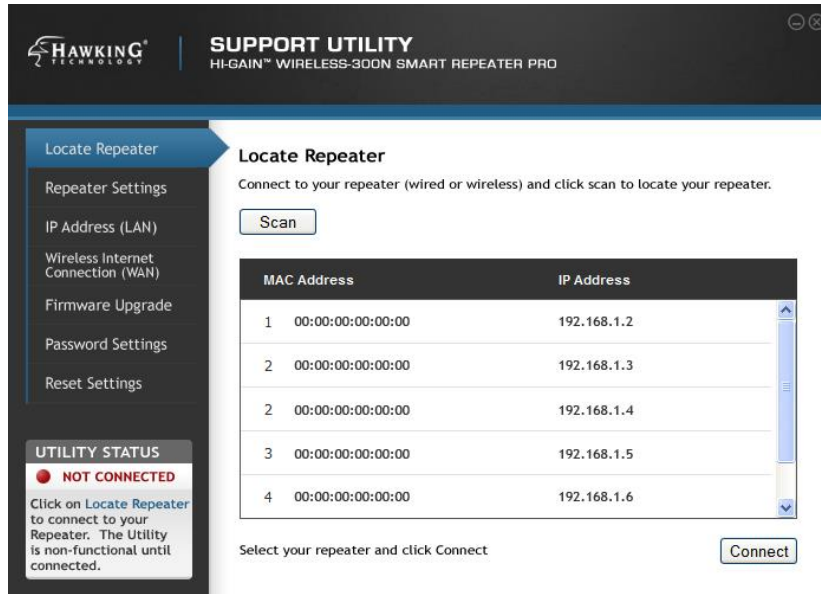
## ***4-8 Using the Support Utility***

The Smart Repeater Support Utility is used to help troubleshoot a connection or easily access the basic configuration settings of the Smart Repeater without having to log into the web interface. This Utility may often be used in conjunction with support calls from our support department or by the user when on site or for quick configuration purposes.

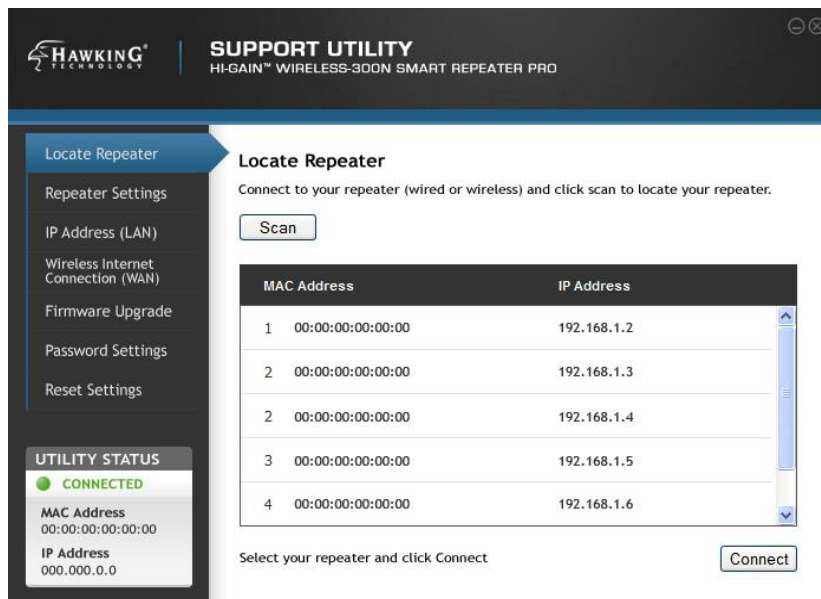
To run the support utility, insert the CD into your computer's CD rom and click on "Software Utility". Note: this utility only supports Windows operating systems. If your computer prompts you, please allow the program through your firewall.



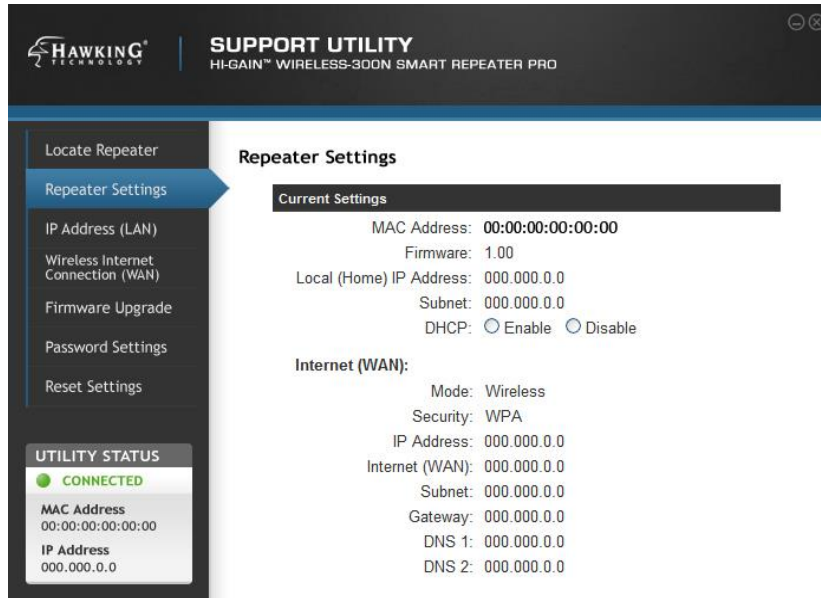
Click on SCAN to locate the Smart Repeater you wish to configure. Once selected click 'CONNECT' to connect to the Repeater.



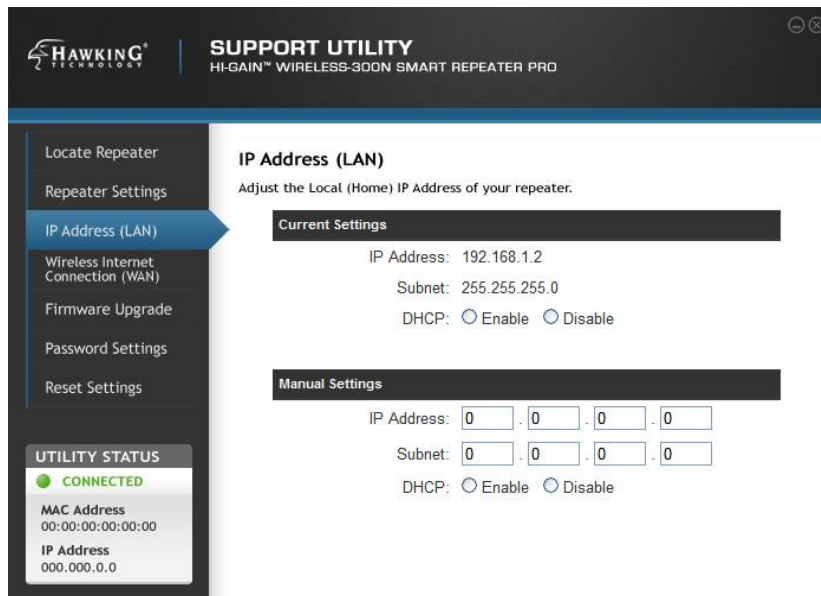
Note: before making any configurations on the Utility, you **MUST** be connected to a Repeater. The status of the Utility and Repeater connection is displayed on the bottom left corner.



The Repeater Settings tab provides information on all current settings for the local network (LAN) as well as the Internet network (WAN). The firmware version and MAC Address are listed as well.

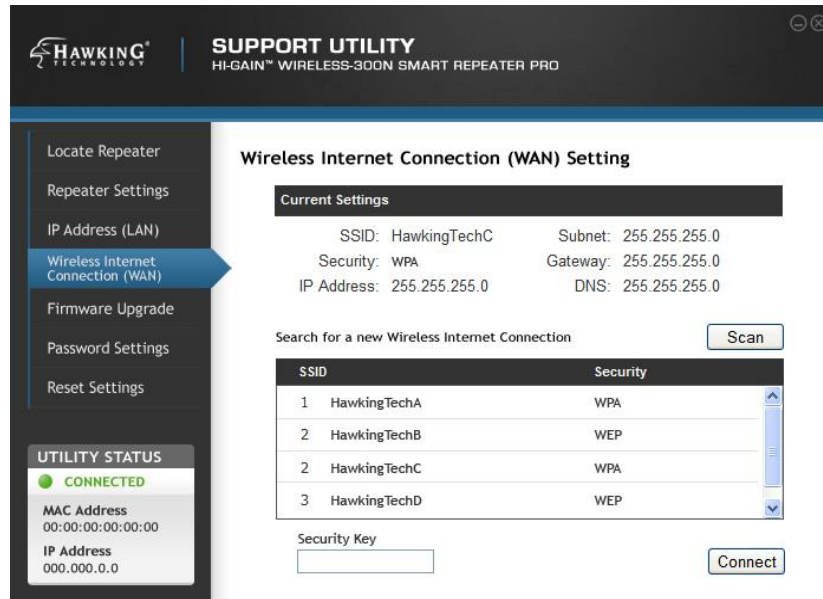


The IP Address (LAN) tab allows you to enable or disable DHCP (automatic IP assignment to clients connecting to the Smart Repeater) as well as make adjustments to the local IP Address of the Repeater.

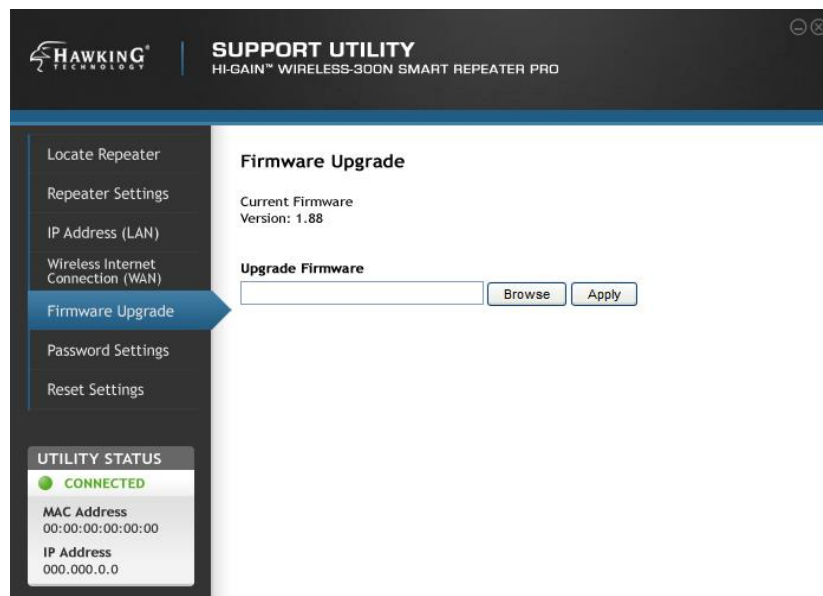


The Wireless Internet Connection tab allows you to see the current Internet (WAN) settings for the Repeater. From here you can also scan for other wireless networks detected by the Repeater and highlight them to change your Internet Connection source to begin repeating from a new wireless network. If the network you are trying to connect

to uses encryption it will be required that you enter the Security Key in the field below.

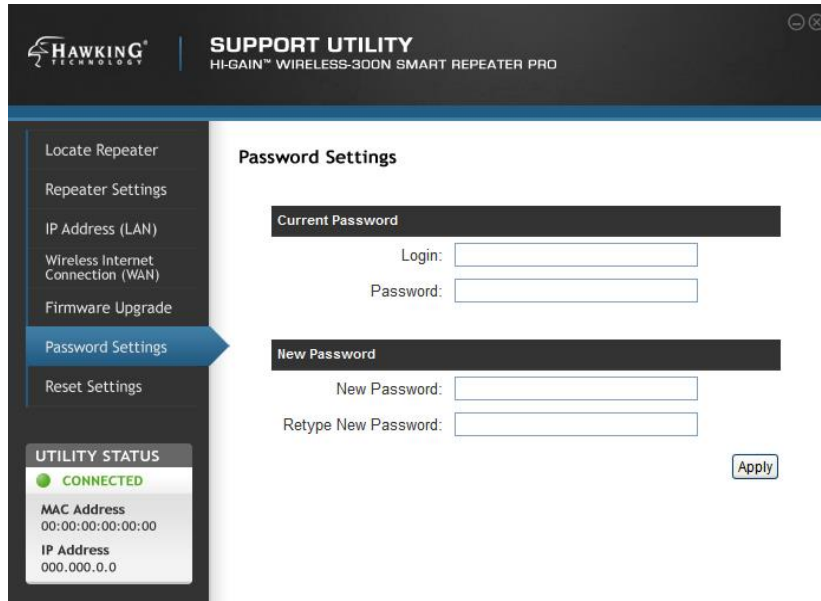


Firmware Upgrade: Simply browse for the latest firmware file and click Apply to upload the firmware of your Repeater.

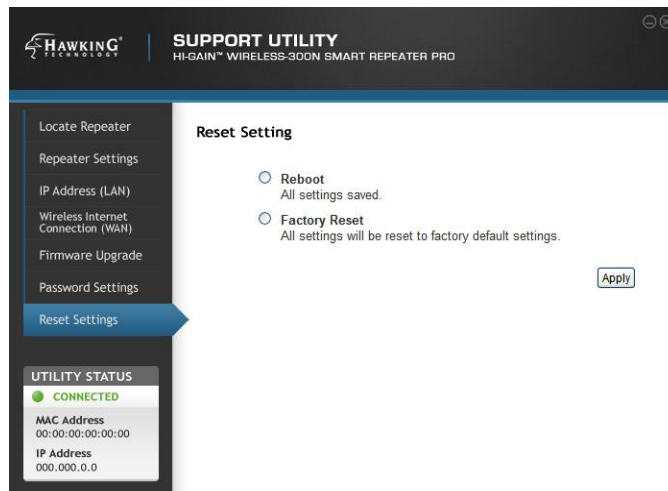


The Password Settings tab gives you access to change your current password for logging into the web interface. You will need to first enter your current login and password before you are able to change your login password.





The Reset Settings tab allows you to reboot your Repeater in the event of a lock up or refresh while still saving all of your current settings. To reset the Smart Repeater to factory default settings select Factory Reset and click ‘Apply.’



## **Chapter V: Appendix**

### ***5-1 Hardware Specification***

Flash: 4MB

SDRAM: 16MB

WAN Port: 10/100M UTP Port x 1

WAN Port: 802.11g Client

LAN Ports: 10/100M UTP Port x 4

Outer Antennas: 3dBi Dipole Antenna x 2 (Reverse SMA)

For WLAN (2T2R Spatial Multiplexing MIMO configuration)

Center Antenna : 3dBi Dipole Antenna x 2 (Reverse SMA)

For WAN (Dedicated Internet Antenna)

Power: 12VDC, 1A Switching Power Adapter

Dimension: 30(H) x 187(W) x 100(D) mm

Product Weight : 1.40 lbs (antennas included)

Transmit Power: 17dBm  $\pm$  1dBm

Temperature: 32~104°F (0 ~ 40°C)

Humidity: 10-90% (NonCondensing)

Certification: FCC

## 5-2 Troubleshooting

If you found the Smart Repeater is working improperly or stops responding, don't panic! Before you contact your dealer of purchase for help, please read this troubleshooting first. Some problems can be solved by you in a very short time!

Scenario	Solution
<p>Internet Connection Test says success but I still cannot get into the internet.</p>	<p>a. On the web interface, go to the status, and click on Internet Connection. Make sure your wireless settings are correct, ie. Security, channel and SSID.</p> <p>b. If everything is correct, try the following. Go to 'General Setup', under Internet Connection, click on DNS. Manually specify a DNS entry and click save/apply. You can use your ISP's DNS settings or a common DNS such as Google's, "8.8.8.8".</p>
<p>I am getting drastically reduced speeds when compared to my original WiFi signal. How do I fix this?</p>	<p>Log into the Smart Repeater, go to General Settings, go to Home Wireless, basic settings. Try adjusting channels until you get close to your original speed. The reason for this is related to wireless interference.</p> <p>Another issue that might cause the problem might be the security. Log into the Smart Repeater, go to General Settings, go to Home Wireless, Security Settings. Change the security to WPA-Pre-shared key and select WPA2-AES. Type in a passphrase. Save and apply.</p>
<p>How come I don't see my network files when I'm connected to the HW2R1?</p>	<p>The HW2R1 by default creates an isolated network. You will see two networks after it is configured, your original wireless network and the HW2R1. This is by default for security reasons, especially if you are connecting to an open/public network.</p> <p>If you wish the two wireless signals to be on one network, during the quick setup, there is a check box for bridging/passthrough mode. Please check this box and go through the setup process. Then restart your system.</p>

	When you connect to the HW2R1 after this, you should be on the same network as your original network. Refer to section 2-3-1
During the setup, I notice that the HW2R1 has its own wireless name. Can I make it the same as my original network?	No, the HW2R1 requires that its own wireless name (SSID) be different from the wireless name it is repeating.
File download is very slow or breaks frequently	<ul style="list-style-type: none"> <li>a. Are you using QoS function? Try disabling it and try again.</li> <li>b. Source Internet connection is poor</li> <li>c. Try to reset the Smart Repeater</li> <li>d. Multiple users may be accessing the Internet simultaneously. Attempt to download the file at another time.</li> <li>e. Contact Hawking Techsupport</li> </ul>
I can't log onto web management interface: password is wrong	<ul style="list-style-type: none"> <li>a. Make sure you're connecting to the correct IP address of the Smart Repeater.</li> <li>b. Password is case-sensitive. Make sure the "Caps Lock" light is not illuminated.</li> <li>c. If you forgot the password, do a hard reset. Press the reset button on the back for 30 seconds, power off/on.</li> </ul>
Smart Repeater becomes hot	<ul style="list-style-type: none"> <li>a. This is not a malfunction, as long as it is not so hot that you cannot touch it for a prolonged period of time</li> <li>b. If you smell something wrong or see smoke coming out from Smart Repeater or A/C power adapter, please disconnect the Smart Repeater and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.</li> </ul>
The date and time of all event logs are wrong	<ul style="list-style-type: none"> <li>a. Adjust the internal clock of Smart Repeater.</li> </ul>

### ***5-3 Glossary***

**Default Gateway (Smart Repeater):** Every non-Smart Repeater IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

**DHCP:** Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

**DNS Server IP Address:** DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as `www.BroadbandSmart Repeater.com`) and one or more IP addresses (such as `192.34.45.8`). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "`Broadbandrouter.com`" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

**DSL Modem:** DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

**Ethernet:** A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

**Idle Timeout:** Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

**IP Address and Network (Subnet) Mask:** IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, which identifies a single, unique Internet computer host in an IP network. Example: `192.168.1.2`. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": `aaa.aaa.aaa.aaa`, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": `bbbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb`, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.

When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000

It means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for Smart Repeaters to route IP packets to their destination.

**ISP Gateway Address:** (see ISP for definition). The ISP Gateway Address is an IP address for the Internet Smart Repeater located at the ISP's office.

**ISP:** Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

**LAN:** Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

**WLAN:** Wireless Local Area Network. A WLAN is a group of computers and devices connected together in a relatively small area (such as a house or an office) wirelessly. Your wireless home network is considered a WLAN.

**MAC Address:** MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

**NAT:** Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband Smart Repeater's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

**Port:** Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

**PPPoE:** Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

**Protocol:** A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

**Smart Repeater:** A Smart Repeater is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses. It provides modem access with any wireless 802.11b/g/n network and redistributes the signal via Ethernet or wireless Ethernet with full router capabilities.

**Subnet Mask:** A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

**TCP/IP, UDP:** Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

**WAN:** Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

**Source Wireless Network:** A wireless network that is used to connect to the Internet. This network can be from another connection with a wireless router and a broadband modem. The Smart Repeater uses the Source Wireless Network to establish a connection to share the Internet connection locally. The Source Wireless Network may be a local coffee shop Wi-Fi hot spot or another home or office with a WLAN (with Internet access).

**Web-based management Graphical User Interface (GUI):** Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Firefox or Microsoft Internet Explorer to Control/configure or monitor the device being managed.