Sapido

One for all

Mobile Router

WiFi Adapter with Built-in Mini Router

BRD70n

Networking

User Manual v1.0.0

Table of Contents

FCC Caution

FCC Part 15.19 Caution:

1. 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
2. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Statement in User's Manual (for calss B)

FCC Section 15.105

"Federal Communications Commission (FCC) Statement"

This equipment has been tested and found to comply with the limits for a lass B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

CE Statement of Conformity

Our product has been tested in typical configuration by Ecom Sertech Corp and was found to comply with the essential requirement of "Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility" (89/336/EEC; 92/31/EEC; 93/68/EEC)

Chapter 1 Introduction

1.1 Hardware Features

Item	Specification
Key Components	
Main Processor	Realtek RTL8196EU 400MHz Network Processor
Flash	8Mbytes Serial Flash
RAM	32Mbytes SDRAM
Wireless Chip	Realtek RTL8188ER 1T1R single chip
Communication Interfaces	
LAN Port	1 x 10/100Mbps RJ45 with auto MDI/MDIX
USB Port	1 x USB 2.0 OTG USB To Ethernet 10/100Mbps Ethernet
Wireless	IEEE 802.11b/g/n 2.4GHz 1T1R
Others	
Wireless Antenna	Internal x1
Transmission Power	802.11b: 19±2dBm @ normal temp. range 802.11g: 16±2dBm @ normal temp. range 802.11n (20MHz/40MHz): 14±2dBm @ normal temp. range
Receive Sensitivity	11Mbps : TYP. -83dBm @ 8% PER 54Mbps: TYP. -70dBm @ 10% PER 11n (20MHz): TYP. -64dBm @ 10% PER 11n (40MHz): TYP. -61dBm @ 10% PER
Button	**Reboot/Reset button:** push 1 second for restart: push 10 seconds for resetting to system default. **WPS button:** push for starting WPS process
Operation Requirement	Operating Temp.: 0 to 40℃(32 to 104℉) Storage Temp.: -20 to 70℃(-4 to 158℉) Operating Humidity: 10% to 85% Non-Condensing Storage Humidity: 5% to 90% Non-Condensing
Power Supply	Power Adapter DC5V/0.5A
Dimensions	69 (L) x 26 (W) x 19.6 (H) mm

1.2 Product Appearance

LED Indicator Status Description:

LED	Function	Color	Status	Description
⏻	Power indicator	**Green**	On	Power is being applied to this product
(•)/))	Wireless / WPS activity	**Green**	On	Wireless is connected
			Blinking 30ms	Wireless Tx/Rx activity
		Reddish Orange	Blinking 30ms	WPS function in progress
💻	LAN port activity	**Green**	On	100Mbps Ethernet is connected
			Blinking 30ms	100Mbps Ethernet Tx/Rx activity
		Green	On	10Mbps Ethernet is connected
			Blinking 120ms	10Mbps Ethernet Tx/Rx activity

Chapter 2 Utility

BRD70n support driver and utility auto install

	Auto install
Router mode	Install a new usb Ethernet NIC on PC，user can manage BRD70n by this usb Ethernet NIC
USB to Ethernet	Install a new usb Ethernet NIC on PC，user can access internet by it
USB to Wireless	Install a new usb wireless utility and driver on PC，user can connect to AP by this utility

Chapter 3 System and Network Setup

The BRD70N is an easy to setup and wireless device for various application and environment, especially for large installs such as hotels, offices space, warehouses, hot-spots and more. To begin with BRD70N , you must have the following minimum system requirements. If your system can't correspond to the following requirements, you might get some unknown troubles on your system.

- ↙ Internet Account for XDSL/Cable Modem
- ↙ One Ethernet (10/100mbps) network interface card.
- ↙ TCP/IP and at least one web browser software installed (E.g.: Internet Explorer, Firefox, Safari、Chrome latest version).
- ↙ 802.11b、g、n wireless adapter for wireless mobile clients.
- ↙ Recommended OS: WinXP, Visata or Win7 / Linux.

3.1 Build Network Connection

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, Firewall, etc.
Please confirm the network environment or the purpose before setting this product.

3.2 Connecting BRD70N

Prepare the followings before the connection:

- ↙ PC or Notebook for setup
- ↙ Ethernet cable

1. Make sure you are under "Router Mode".
2. Connect BRD70N to xDSL/ Cable modem with the Ethernet cable.
3. Turn on your Computer.

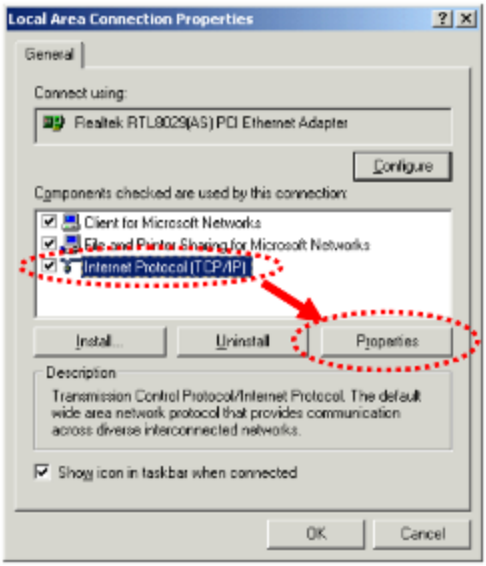
3.3 Network setup

After the network connection is built, the next step is setup the router with proper network parameters, so it can work properly in your network environment. Before you connect to the wireless router and start configuration procedures, your computer must be able to get an IP address from the wireless router automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the below instructions to configure your computer with dynamic IP address:

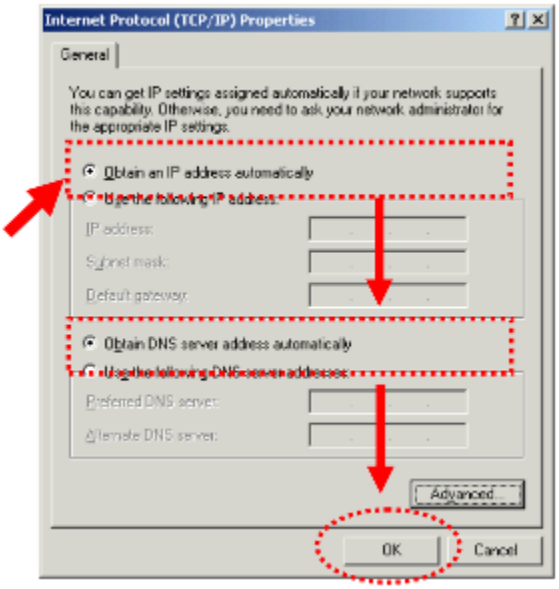
Insert BRD70n into PC USB port and install utility/driver，after the utility and driver done，you can get an IP address from BRD70n（router mode）

3.3.1 Windows 2000

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, double click Local Area Connection, and Local Area Connection Properties window will appear. Select "Internet Protocol (TCP/IP)", then click "Properties".

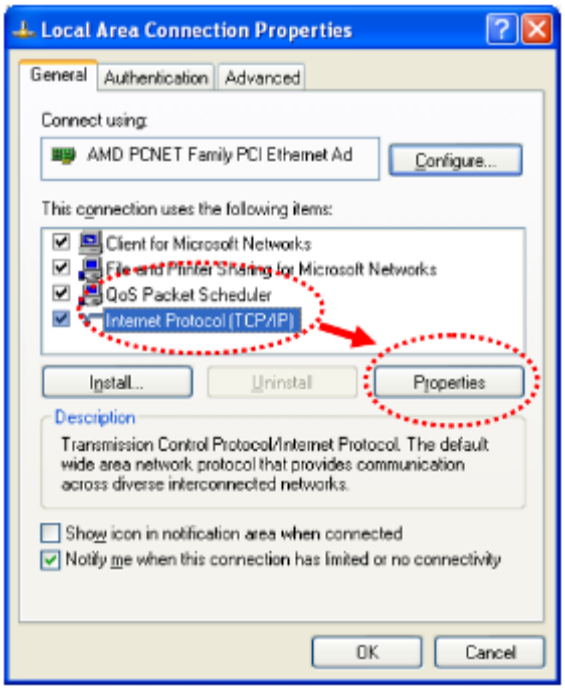


1. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.

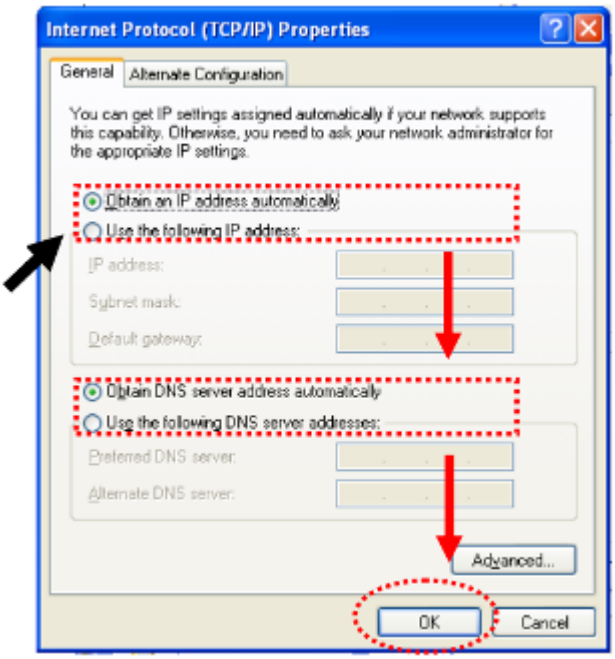


3.3.2 Windows XP

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, then double-click Local Area Connection, Local Area Connection Status window will appear, and then click “Properties”.

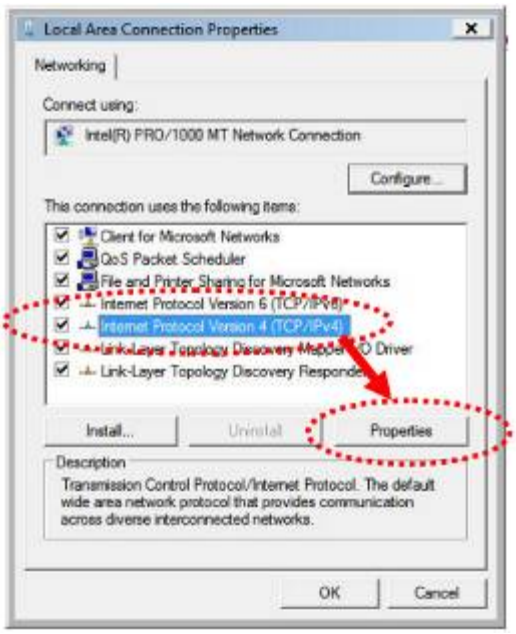


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.

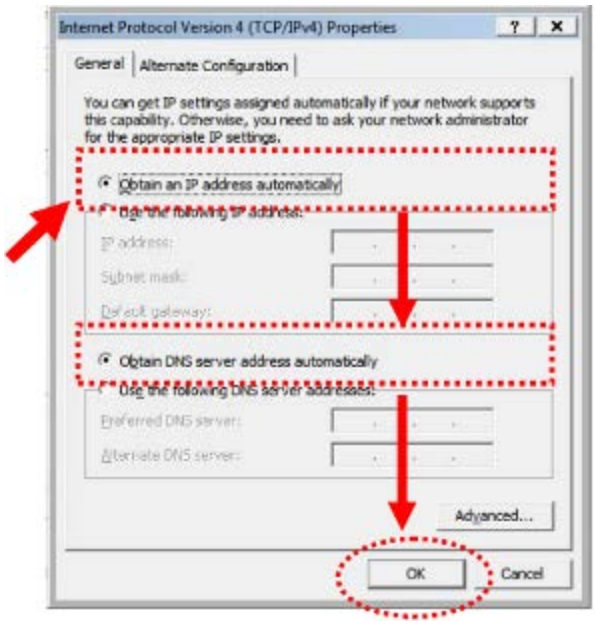


3.3.3 Windows Vista / Windows 7

1. Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Click View Network Status and Tasks, and then click Manage Network Connections. 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”.

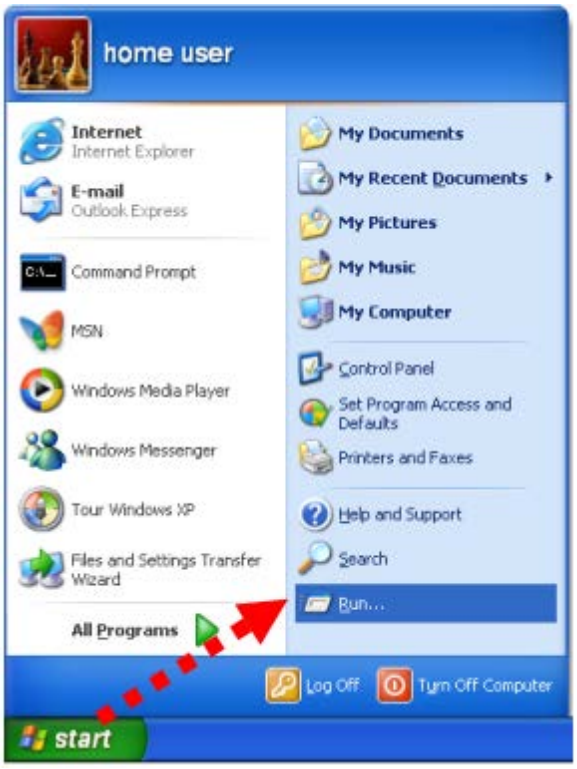


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.

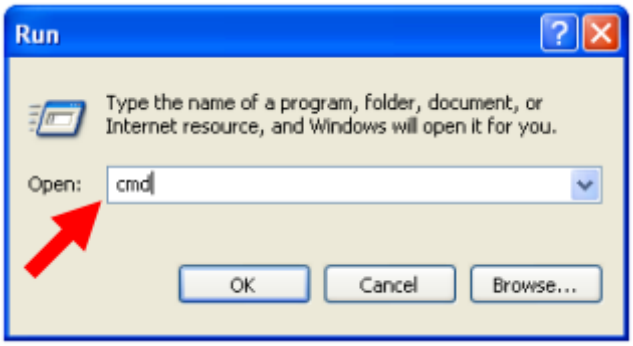


3.4 Router IP Address Lookup

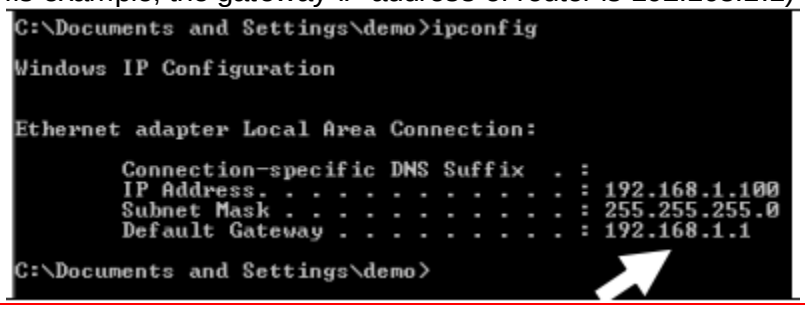
After the IP address setup was completed, please clicks “start” → “run” at the bottom-lower corner of your desktop:



Input “cmd”, and then click “OK”.



Input “ipconfig”, then press “Enter” key. Please check the IP address followed by “Default Gateway” (In this example, the gateway IP address of router is 192.168.1.1)

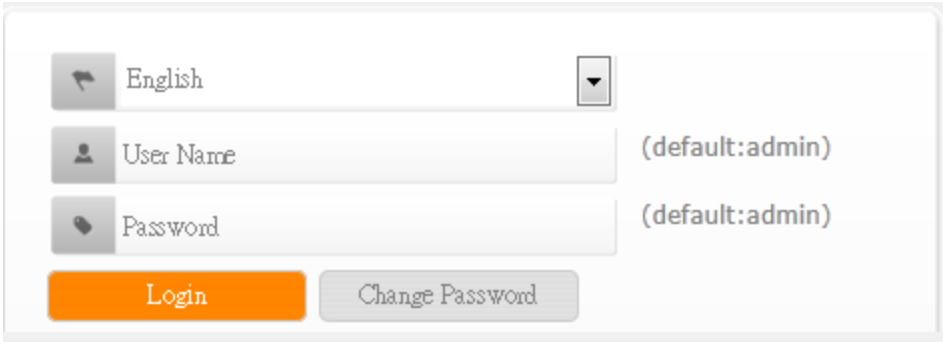


NOTE: If the IP address of Gateway is not displayed, or the address followed by ‘IP Address’ begins with “169.x.x.x”, please recheck network connection between your computer and router, and / or go to the beginning of this chapter, to recheck every step of network setup procedure.

3.4.1 Log into Web GUI（Router mode）

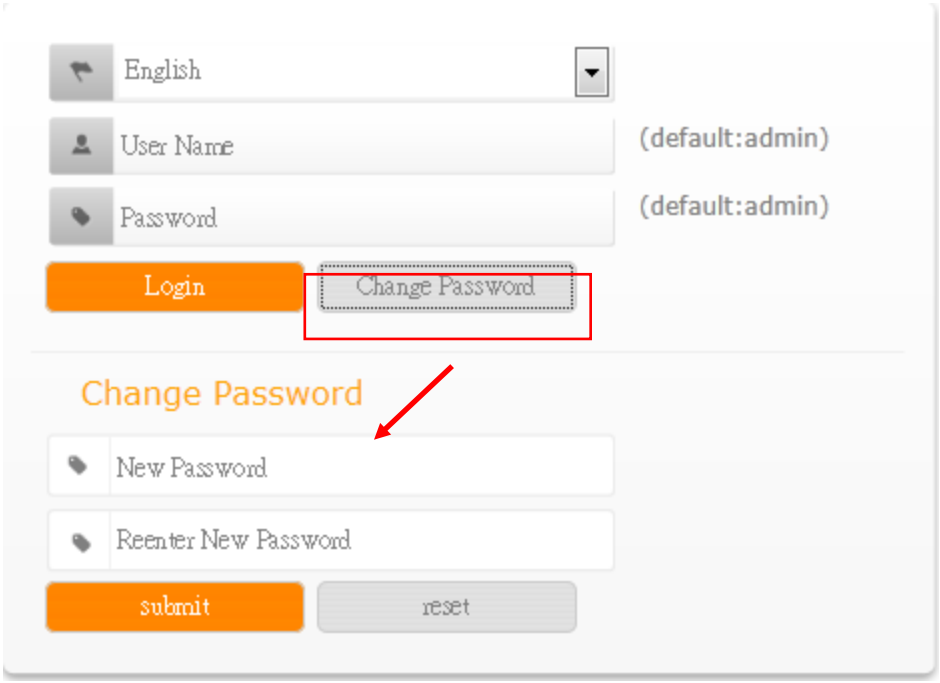
After your computer obtained an IP address from wireless router, please start your web browser, and input the IP address of the wireless router in address bar, and the following message should be shown. Please click “admin” to login the BRD70N .

Enter the User name and Password in to the blank and then Click **Login**. The default values for User Name and Password are **admin** (all in lowercase letters).



Users can set or change user name and password used for accessing the web management interface in this section.

Input User Name and New Password, then input Confirm Password again.



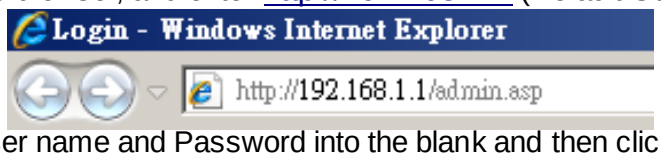
Chapter 4 Internet Connection

This Chapter describes how to setup BRD70N to the internet. The BRD70N is delivered with the following factory default parameters.

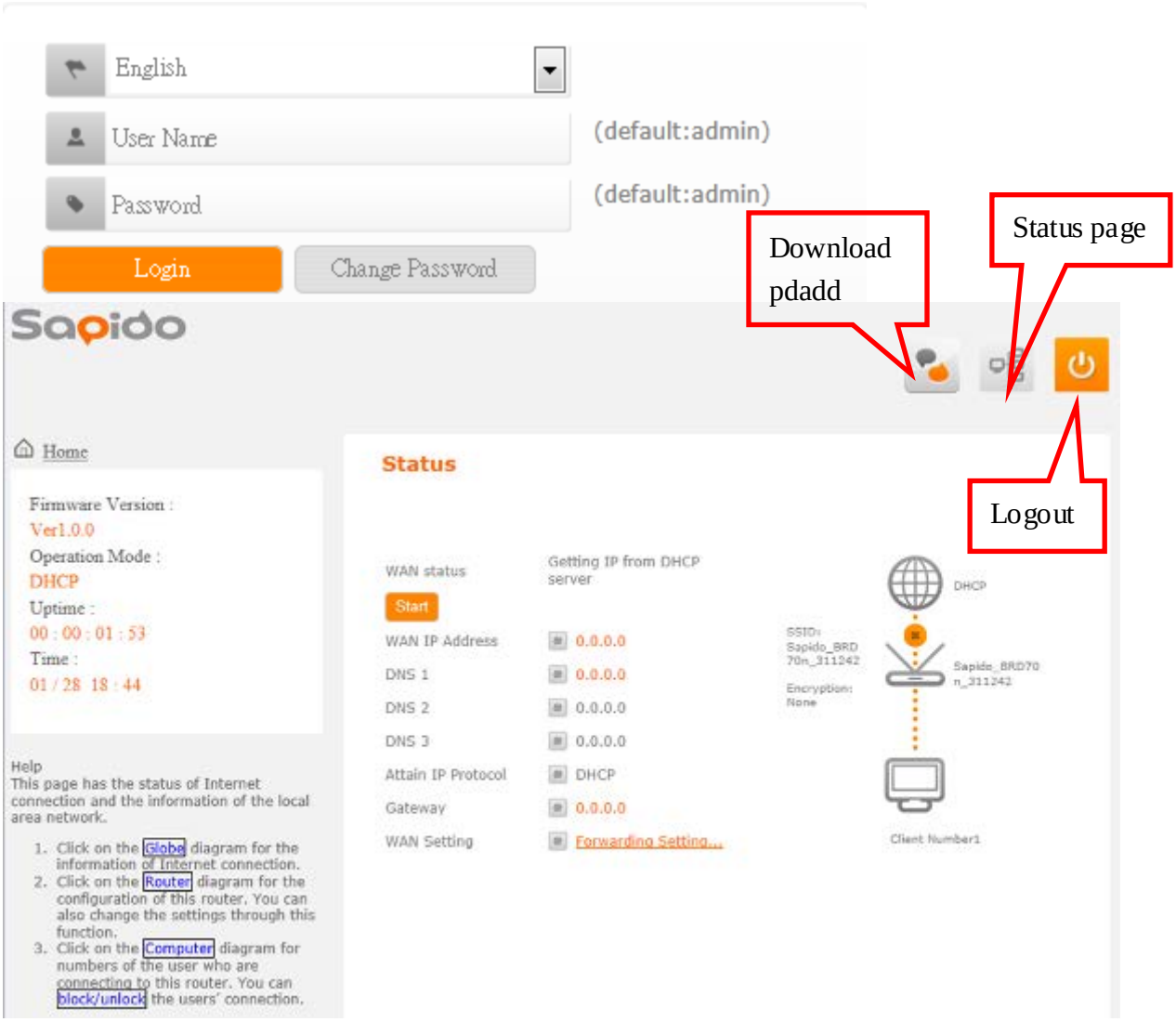
Default IP address: 192.168.1.1
Default IP subnet mask: 255.255.255.0
Web login user name: admin
Web login password: admin

4.1 Using as a broadband router

↔↘ Open a Web browser, and enter http://192.168.1.1 (Default Gateway) into the blank.



↕↘ Enter the User name and Password into the blank and then click **Login**. The default values for User Name and Password are **admin** (all in lowercase letters).



4.2 Home button menu

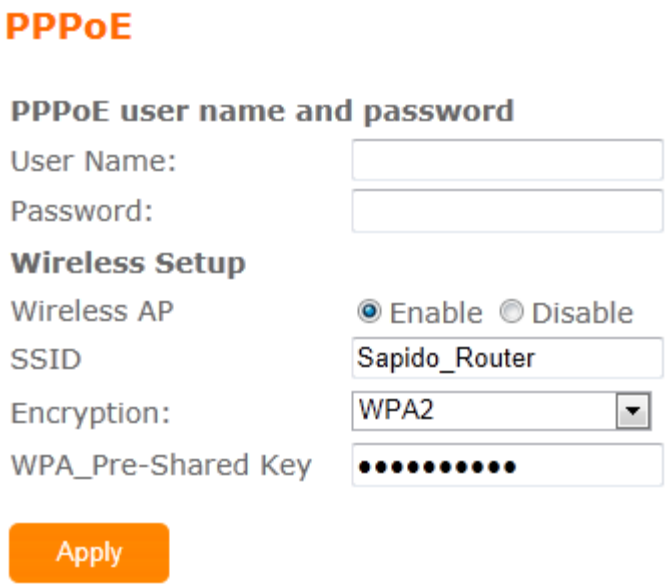
Home **Click Home button icon to enter MENU as below.**

Item	Description
Internet Setup	There are several different method to access Internet，PPPoE、DHCP、Static IP、PPTP、L2TP、WiFi ISP
Wireless Basic Settings	Do wireless basic configuration：SSID、encryption
DDNS	You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider.
Firmware Upgrade	This function allows you upgrade the BRC70X firmware to new version. Please note do not power off the device during the upload because it may crash the system.
Time Zone	You can maintain the system time by synchronizing with a public time server over the Internet.
DoS	Denial of Service
Remote management	This page allows you to access the GUI on WAN.
Advance Setup	Advance setting menu
Status	You could check WAN, LAN, Client network in status.
Factory Default	You could reset the current configuration to factory default.
Reboot	This function is used to reboot
Logout	This page is used to logout.

4.3 Internet Setup

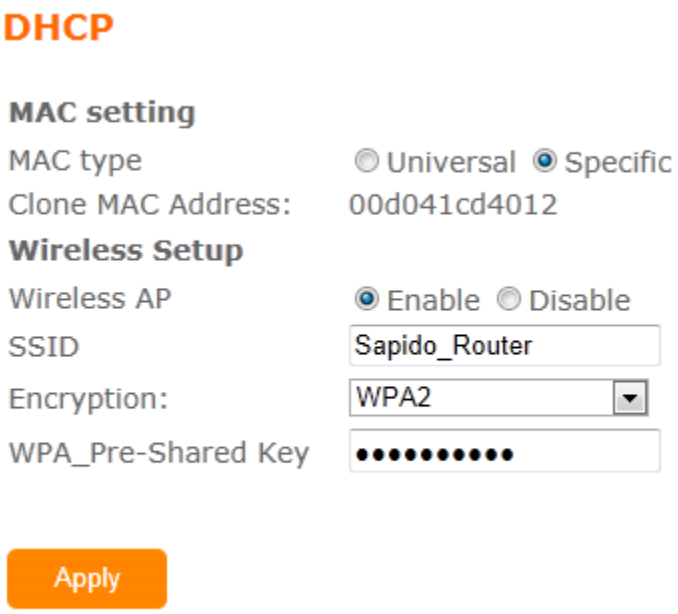
Click **Internet Setup** icon to enter WAN setup as below**.** The Internet Setup is depended on the service that you contract with the provider. The BRD70N provides five selections for the Internet Mode type, **PPPoE, DHCP, Static IP , PPTP and L2TP and HotSpot**. Check with your ISP if you don't know the WAN type.

4.3.1 PPPoE



Item	Description
User Name	Input your user name provided by your ISP. If you don't know, please check with your ISP.
Password	Input the password provided by your ISP.
Wireless AP	Turn on/off wireless
SSID	Service Set identifier, users can define to any or keep as default.
Encryption	Select wireless encryption type form the drop-down list.

4.3.2 DHCP

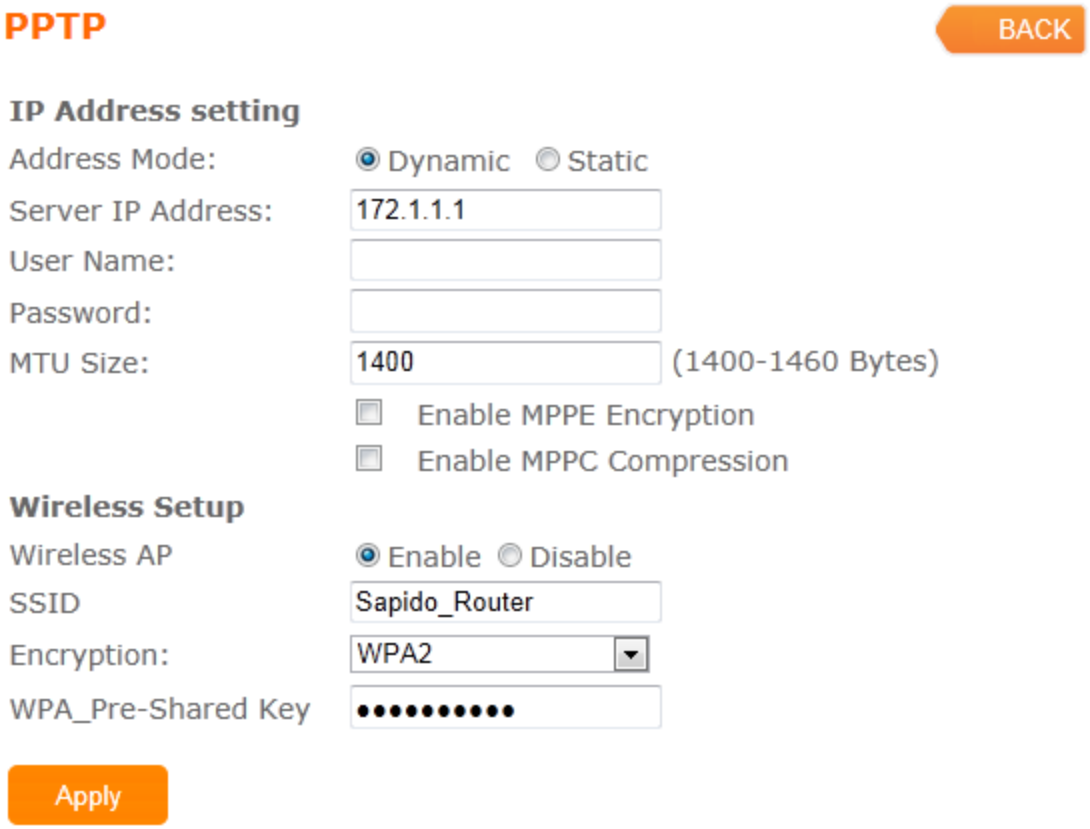


Item	Description
MAC type	Select **"Universal" or "Specific"**
Wireless AP	Turn on/off wireless
SSID	Service Set identifier, users can define to any or keep as default.
Encryption	Select wireless encryption type form the drop-down list.

4.3.3 Static IP

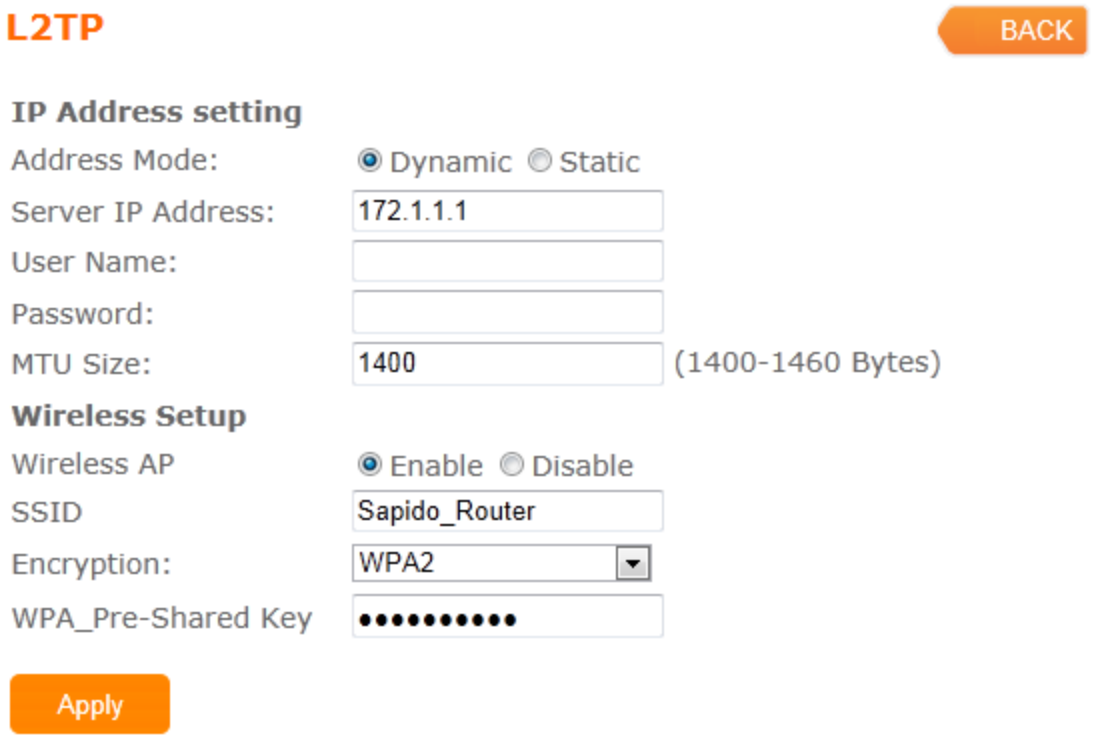
Item	Description
IP Address	Enter the IP address which is provided by your ISP.
Subnet Mask	Please enter the Subnet Mask address
Gateway	Input ISP Default Gateway Address.
DNS	Input DNS information which is provided by your ISP
Wireless AP	Turn on/off wireless
SSID	Service Set identifier, users can define to any or keep as default.
Encryption	Select wireless encryption type form the drop-down list.

4.3.4 PPTP



Item	Description
Address Mode	Select **"Dynamic"** or **"Static"**
IP Address	Input your IP address or domain name
Gateway	Input ISP Default Gateway Address.
Server IP Address	Input your server IP address provided by your ISP. If you don't know, please check with your ISP.
User Name	Input PPTP account provided by your ISP.
Password	Input the password provided by your ISP.
MTU Size	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
Enable MPPE Encryption	Microsoft Point-to-Point Encryption (MPPE) provides data security for the PPTP connection that is between the VPN client and VPN server.
Enable MPPC Compression	Microsoft Point-to-Point Compression (MPPC) is a scheme used to compress Point-to-Point Protocol (PPP) packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ) based algorithm with a continuous history buffer, called a dictionar
Wireless AP	Turn on/off wireless
SSID	Service Set identifier, users can define to any or keep as default.
Encryption	Select wireless encryption type form the drop-down list.

4.3.5 L2TP

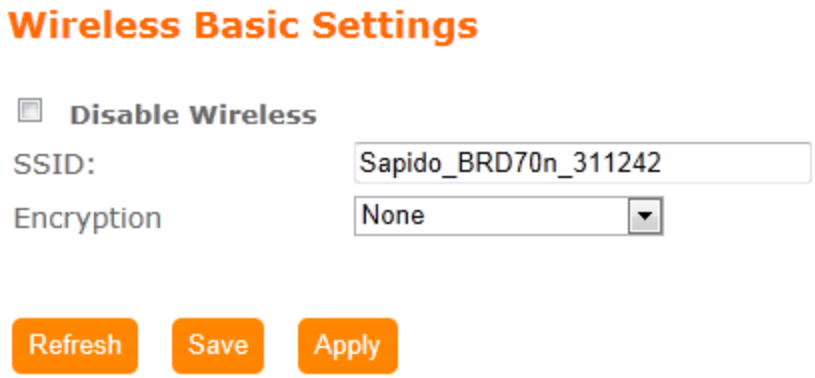


Item	Description
Address Mode	Select **"Dynamic"** or **"Static"**
IP Address	Input your IP address or domain name
Gateway	Input ISP Default Gateway Address.
Server IP Address	Input your server IP address provided by your ISP. If you don't know, please check with your ISP.
User Name	Input PPTP account provided by your ISP.
Password	Input the password provided by your ISP.
MTU Size	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
Wireless AP	Turn on/off wireless
SSID	Service Set identifier, users can define to any or keep as default.
Encryption	Select wireless encryption type form the drop-down list.

Chapter 5 GUI Function Setup

5.1 Wireless basic setting AP

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters

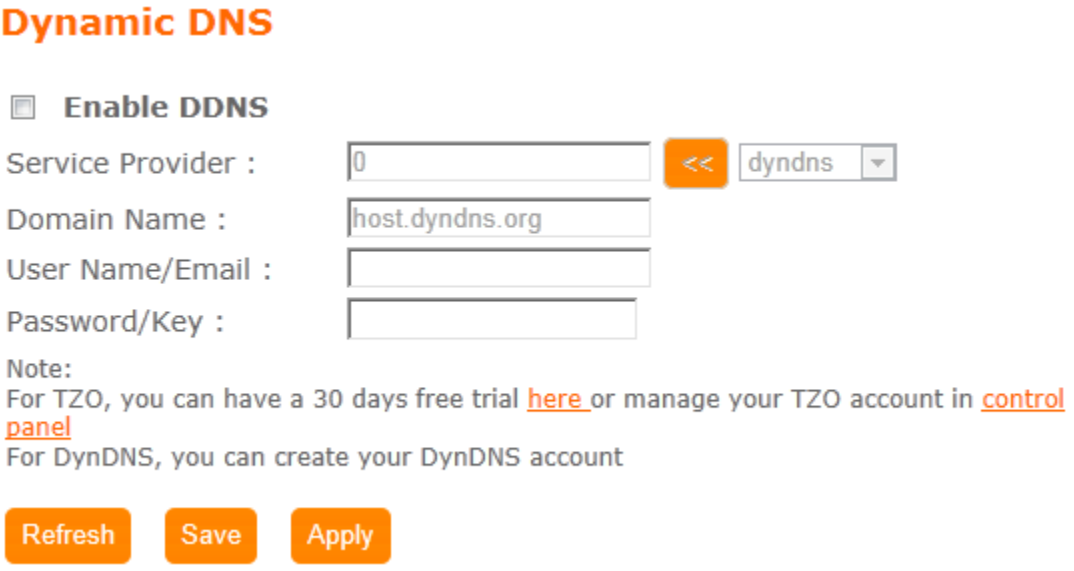


Item	Description
Disable Wireless	Turn on/off wireless
SSID	Service Set identifier, users can define to any or keep as default.
Encryption	Select wireless encryption type form the drop-down list.

5.2 DDNS

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

Note: make sure that you have registered with a DDNS service provider before enabling this feature.



Please enter Domain Name, User Name/Email, and Password/Key. After entering, click on Apply Changes to save the setting, or you may click on Reset to clear all the input data.

Item	Description
Enable/Disable DDNS	Select enable to use DDNS function. Each time your IP address to WAN is changed, and the information will be updated to DDNS service provider automatically.
Service Provider	Choose correct Service Provider from drop-down list, here including DynDNS, TZO, ChangeIP, Eurodns, OVH, NO-IP, ODS, Regfish

	embedded in BRD70n.
User Name/Email	User name is used as an identity to login Dynamic-DNS service.
Password/Key	Password is applied to login Dynamic-DNS service.

5.3 Firmware Upgrade

This function can upgrade the firmware of the router. There are two methods for user upgrade firmware: Auto upgrade and Manual upgrade.

Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

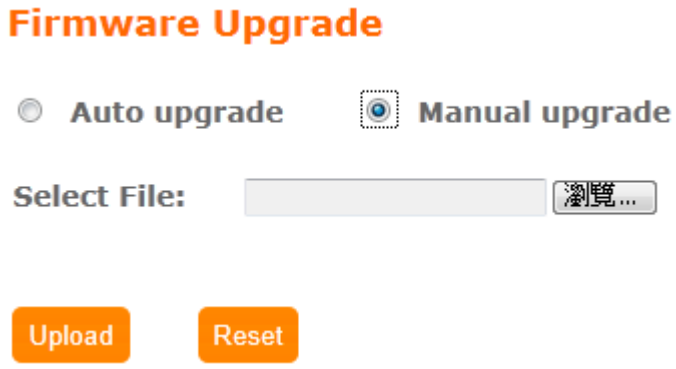
Note: The firmware upgrade will not remove your previous settings.

5.3.1 Auto upgrade

It provide auto detect new firmware from Internet, and user can select to upgrade new version or not.

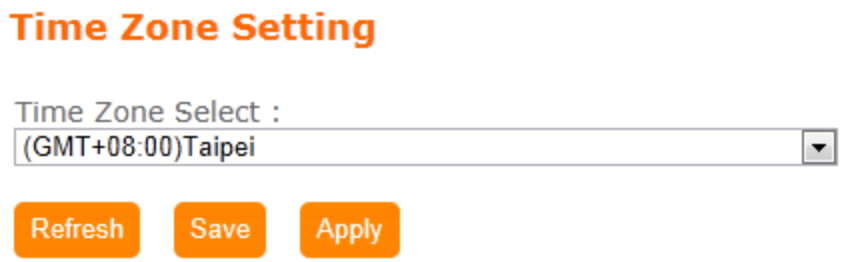
5.3.2 Manual upgrade

If you download firmware from website, you can upgrade firmware manual as below.



5.4 Time Zone

Users can select time zone and synchronize the local clock on the router.

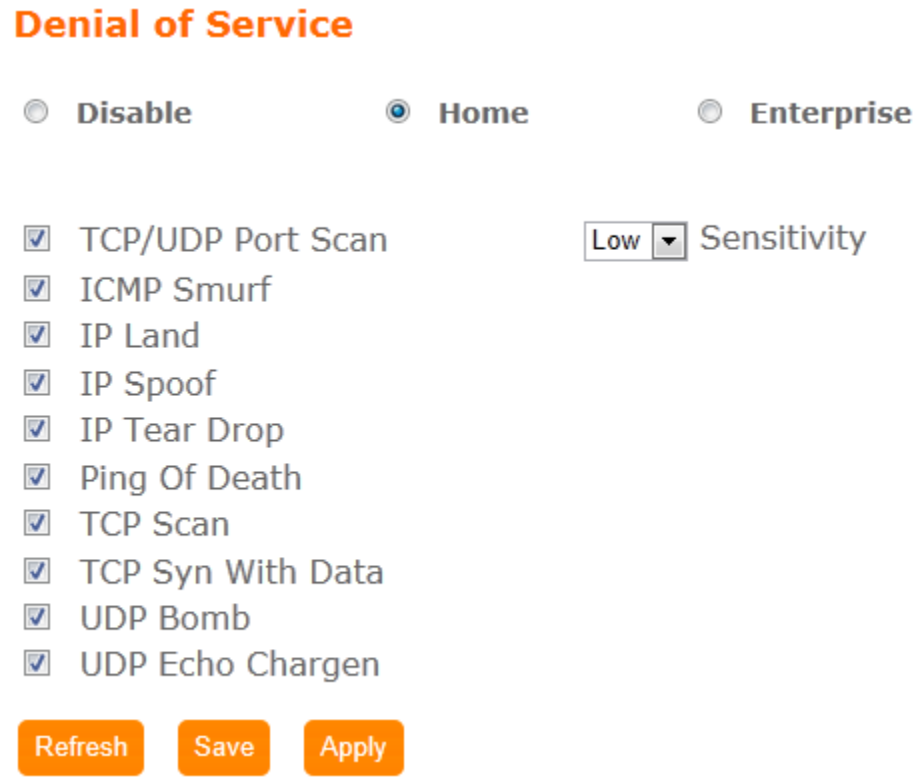


Item	Description
Time Zone Select	Please select the time zone.

5.5 DoS

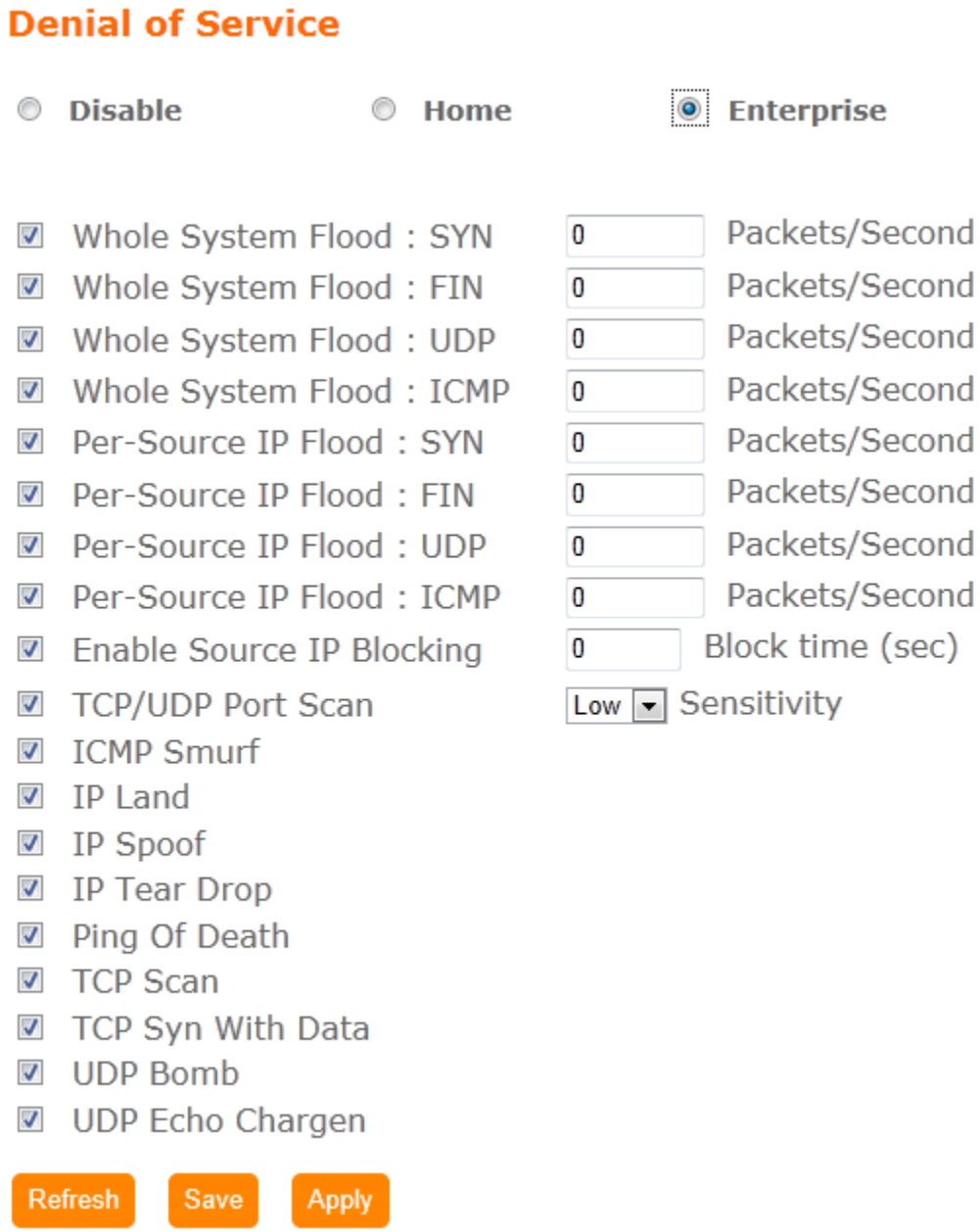
It provide 2 kind of Denial of Service: Home and Enterprise

↙ **Home:**



Item	Description
Home	Check "Home" to enable DoS function for prevention. You also can check "No Prevention" to disable DoS function.

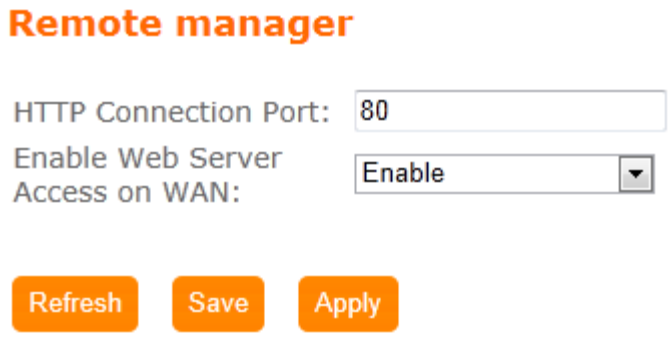
↙ **Enterprise:**



Item	Description
Enterprise	Check "Enterprise" to enable DoS function for prevention. You also can check "No Prevention" to disable DoS function.

5.6 Remote Management

This page allows you to access the GUI on WAN.



Item	Description
HTTP Connection Port	Users can access GUI by this port，default is 80
Enable Web Server Access on WAN	Allow user access GUI from WAN side

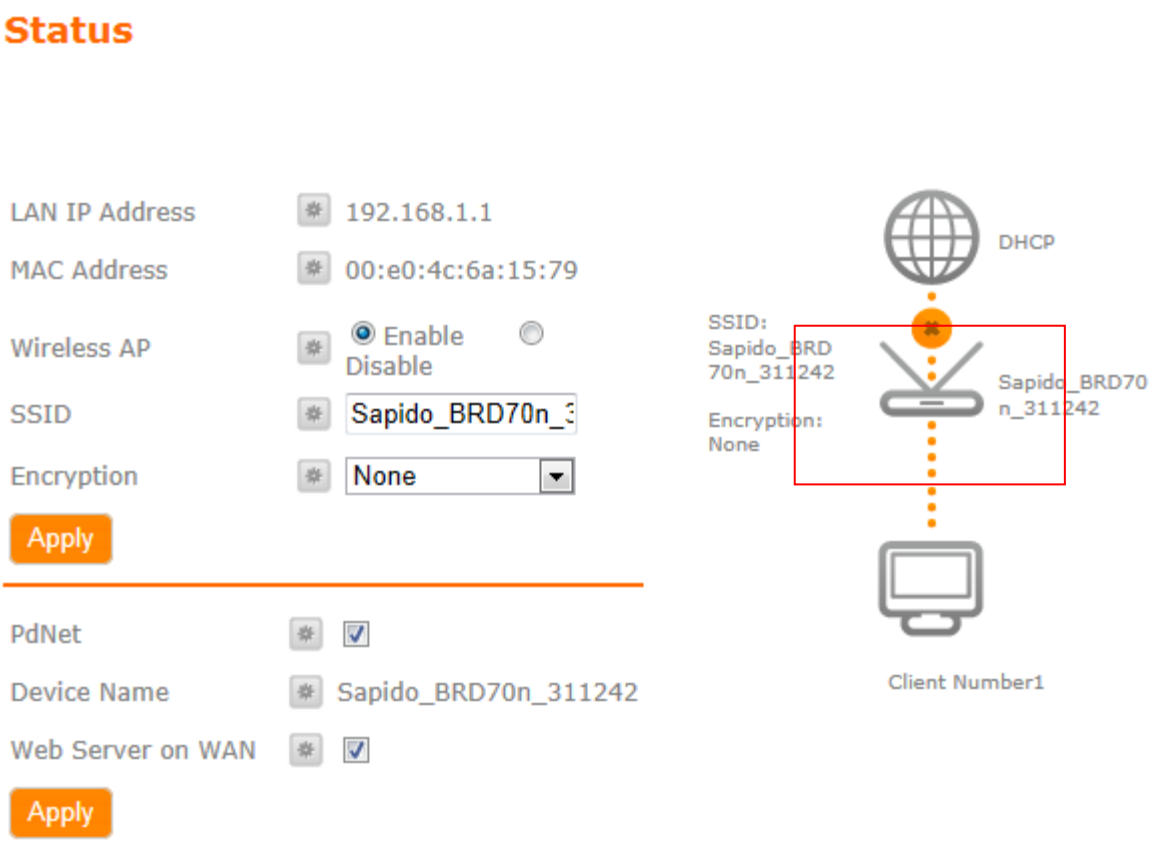
5.7 Status

You could check WAN, LAN, Client network in status.

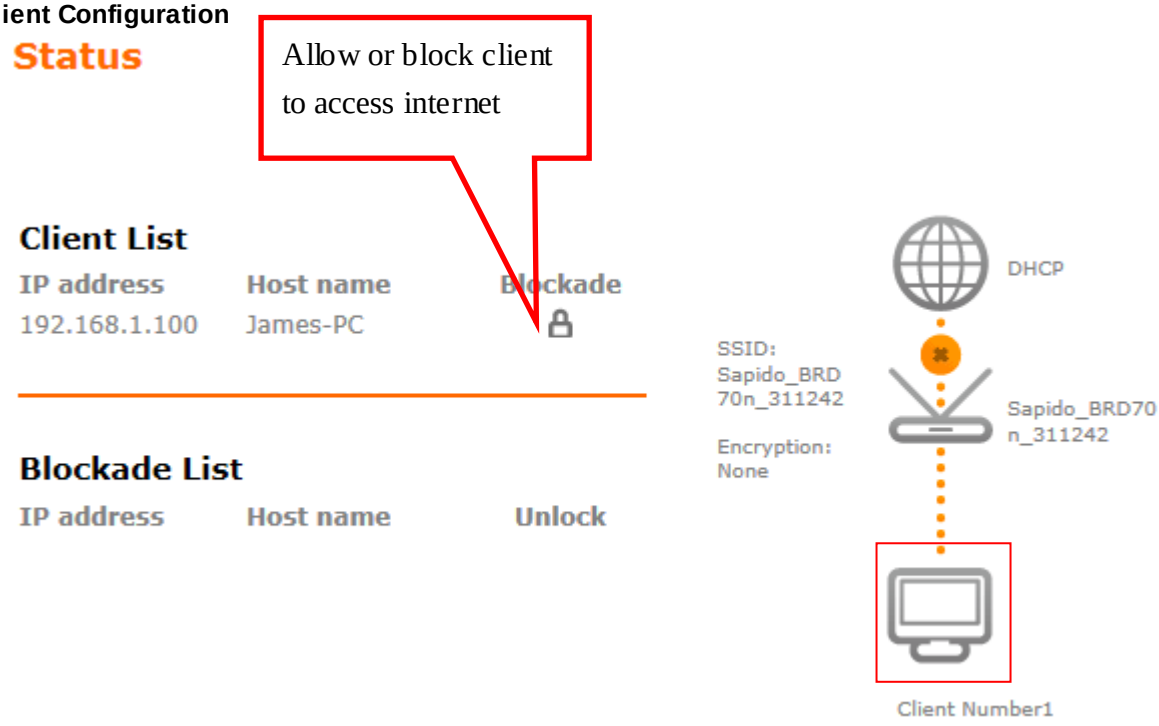
WAN Configuration

LAN Configuration

User can enable/disable wireless、PdNet、web server on WAN from this page.

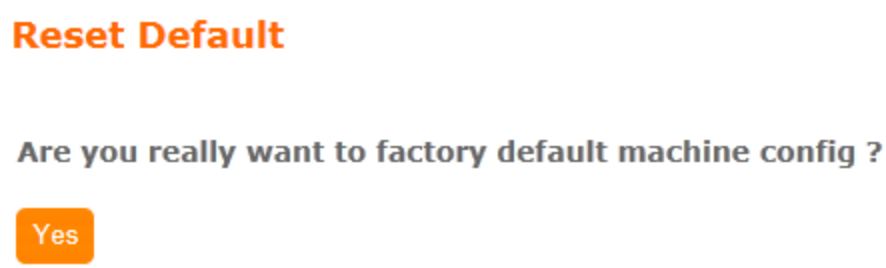


Client Configuration



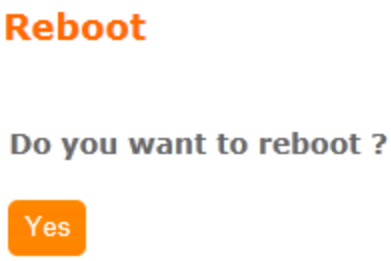
5.8 Factory Default

You could reset the current configuration to factory default.



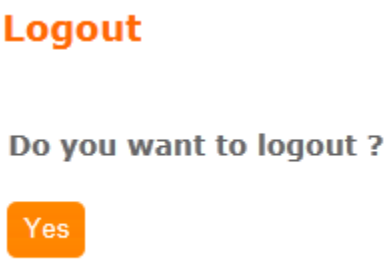
5.9 Reboot

This function is used to reboot



5.10 Logout

This page is used to logout



Chapter 6 Advance Setup

6.1 Internet Mode

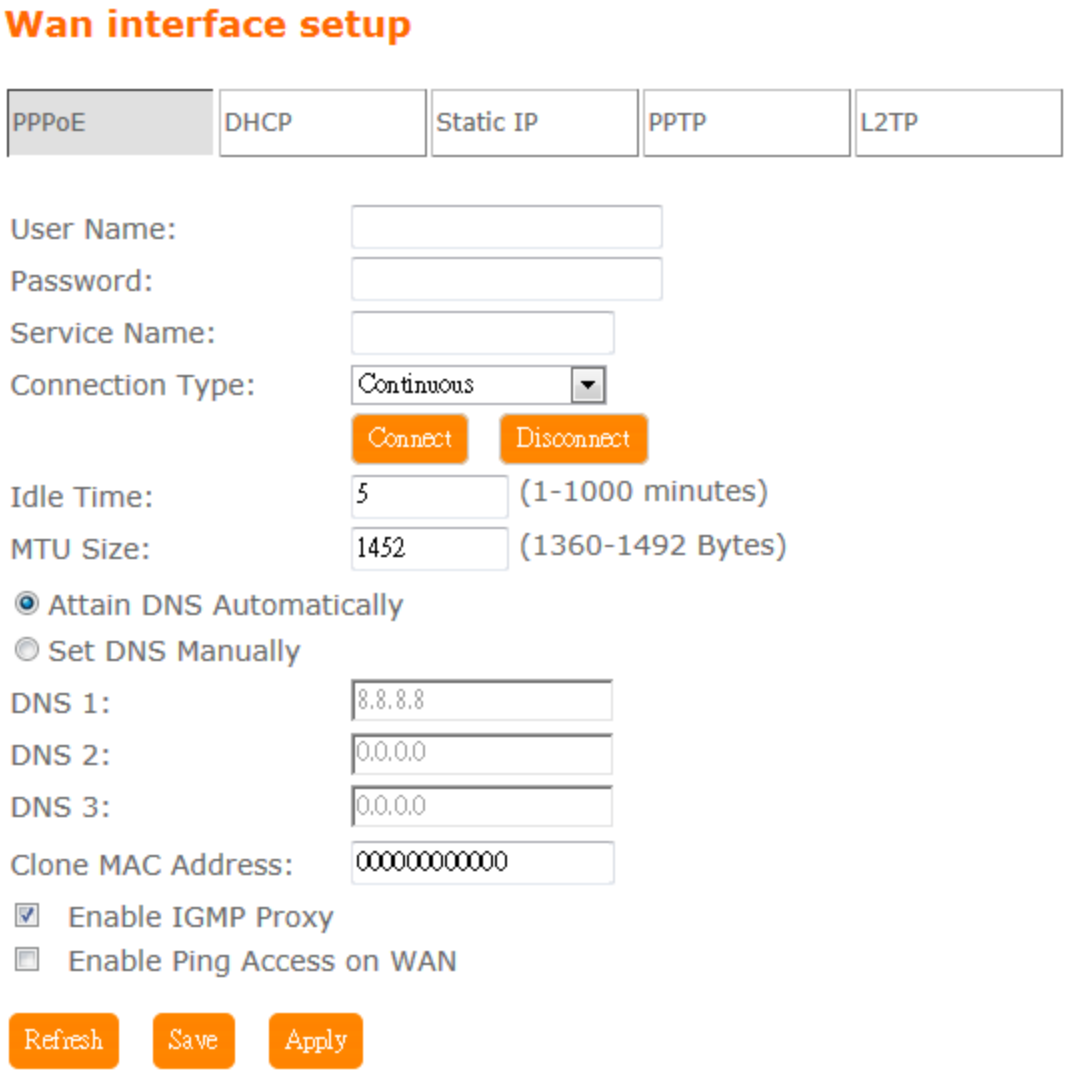
6.1.1 Internet Setup

Please refer Internet Setup

6.2 IP Config

6.2.1 WAN

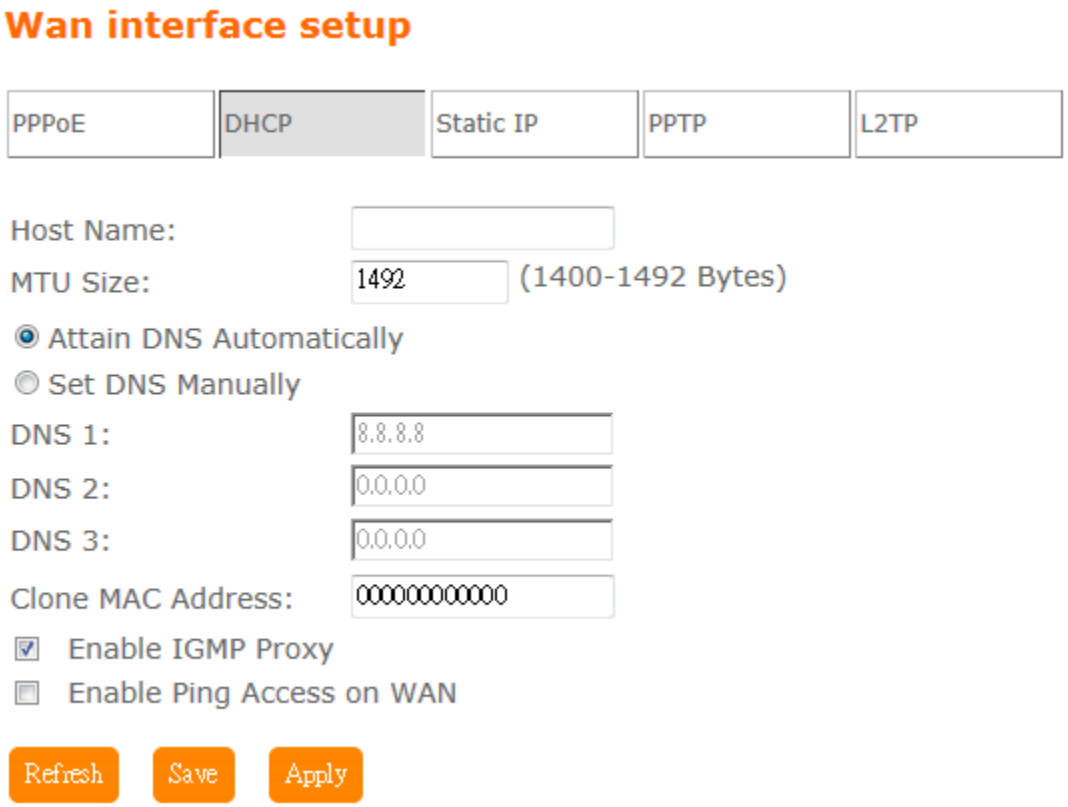
6.2.1.1 PPPoE



Item	Description
User Name	Input your user name provided by your ISP. If you don't know, please check with your ISP.
Password	Input the password provided by your ISP.
Service Name	Input the service name provided by your ISP.
Connection Type	Three types for select: **Continues, Connect on Demand,** and **Manual.**
MTU Size	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC

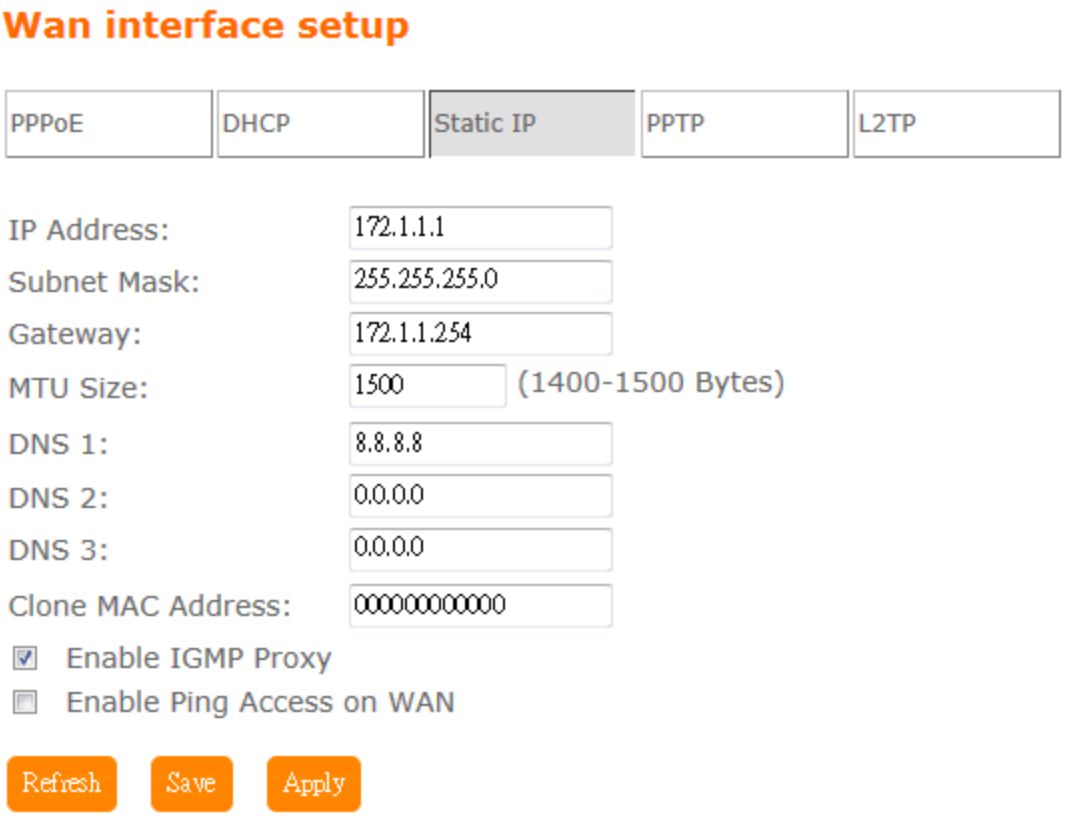
	Address"
Save & Apply	Click on Save to save the setting date, the Apply button for execute current configuration.

6.2.1.2 DHCP



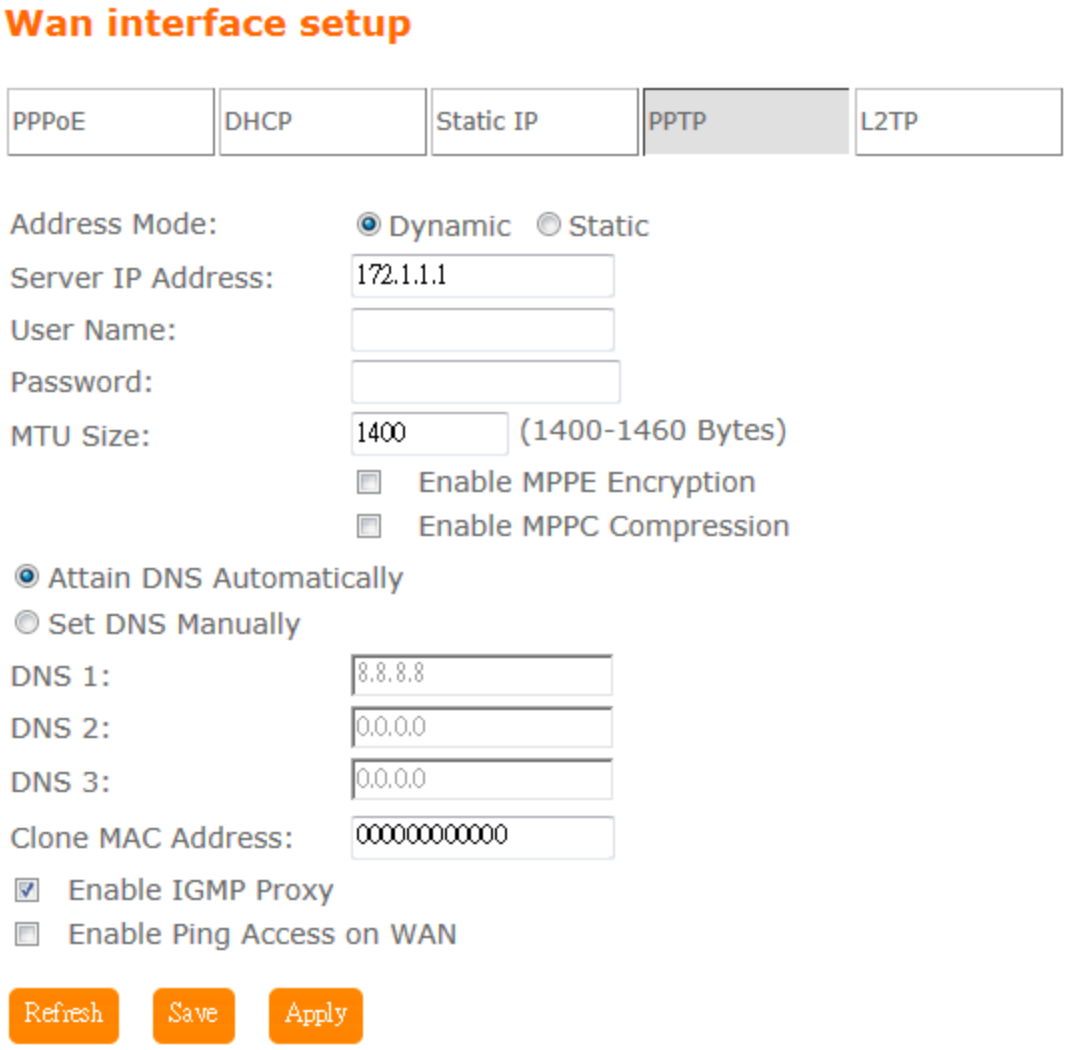
Item	Description
Host Name	You can keep the default as the host name, or input a specific name if required by your ISP.
MTU Size	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Save & Apply	Click on Save to save the setting date, the Apply button for execute current configuration.

6.2.1.3 Static IP



Item	Description
IP Address	Enter the IP address which is provided by your ISP.
Subnet Mask	Please enter the Subnet Mask address
Gateway	Input ISP Default Gateway Address, .
MTU Size	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
DNS	Input DNS information which is provided by your ISP
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Save & Apply	Click on Save to save the setting date, the Apply button for execute current configuration.

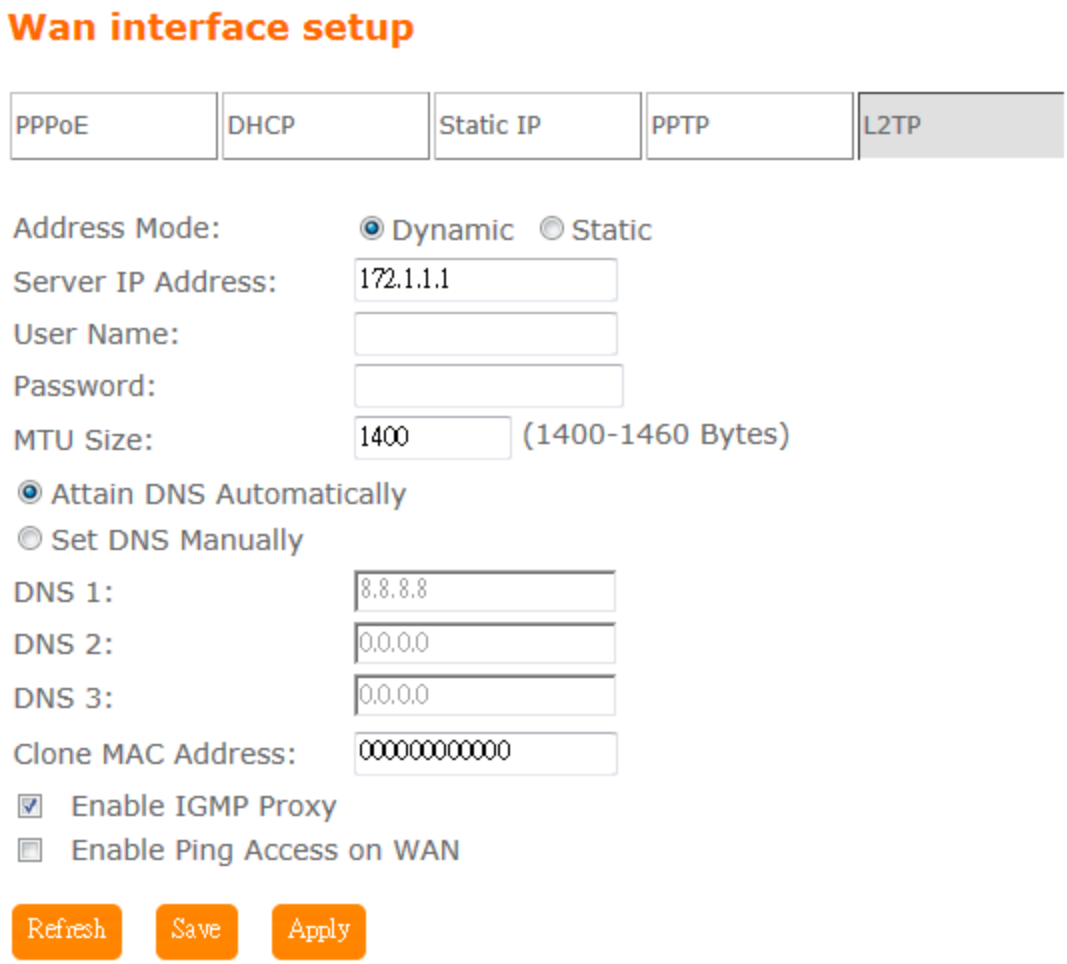
6.2.1.4 PPTP



Item	Description
Server IP Address	Input your server IP address provided by your ISP. If you don't know, please check with your ISP.
User Name	Input PPTP account provided by your ISP.
Password	Input the password provided by your ISP.
MTU Size	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
Enable MPPE Encryption	Microsoft Point-to-Point Encryption (MPPE) provides data security for the PPTP connection that is between the VPN client and VPN server.
Enable MPPC Compression	Microsoft Point-to-Point Compression (MPPC) is a scheme used to compress Point-to-Point Protocol (PPP) packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ) based algorithm with a continuous history buffer, called a dictionar
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Save & Apply	Click on Save to save the setting date, the Apply button for execute

	current configuration.

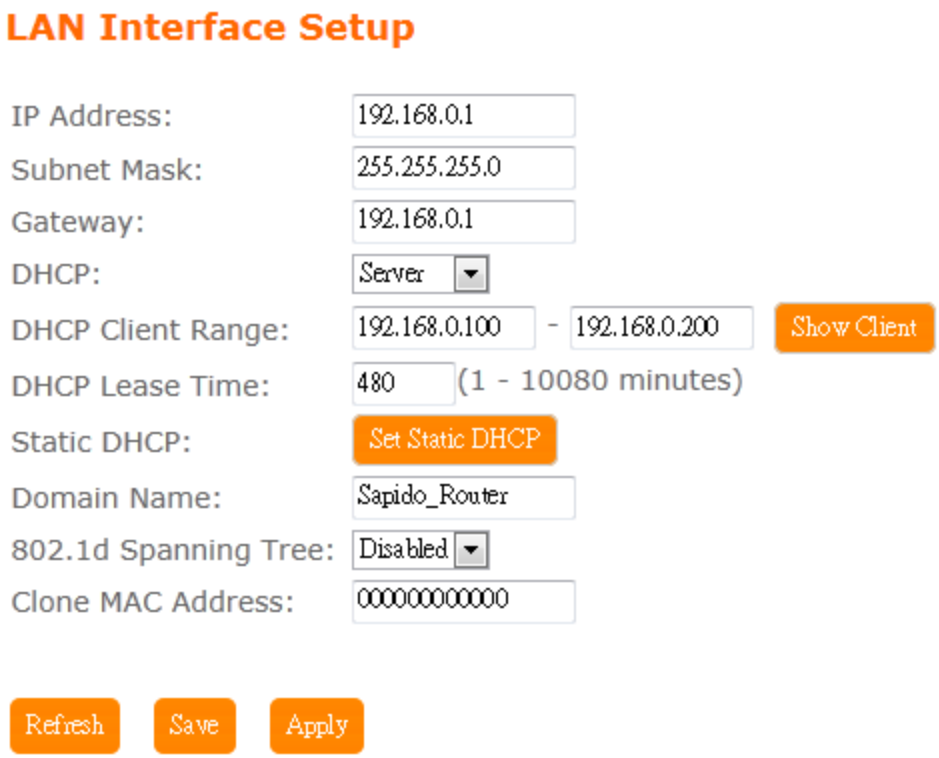
6.2.1.5 L2TP



Item	Description
Server IP Address	Input your server IP address or Host Name provided by your ISP. If you don't know, please check with your ISP.
User Name	Input PPTP account provided by your ISP.
Password	Input the password provided by your ISP.
MTU Size	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Save & Apply	Click on Save to save the setting date, the Apply button for execute current configuration.

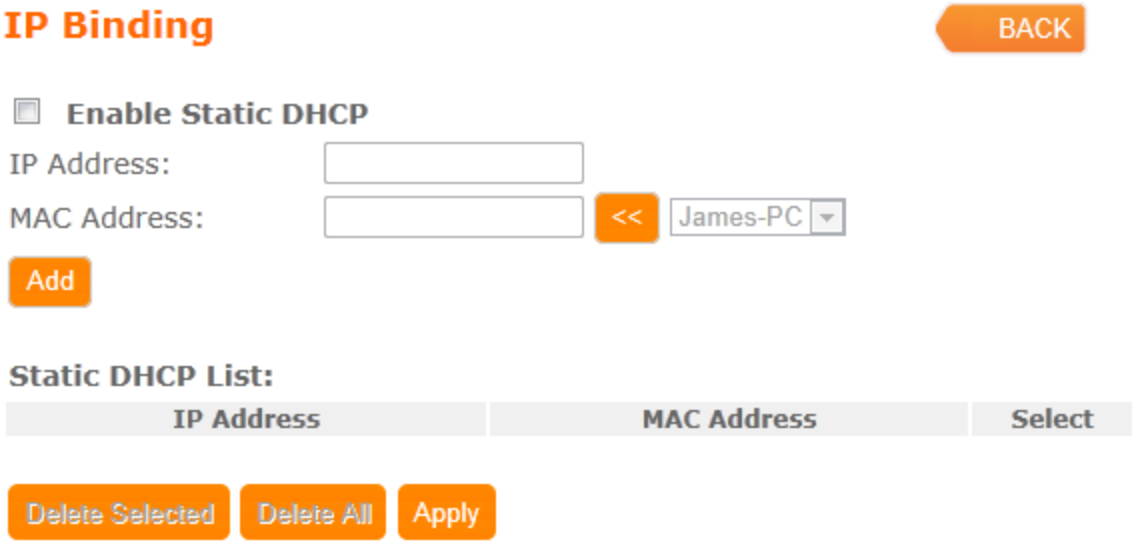
6.2.2 LAN

Use this page to set up the local IP address and subnet mask for your router. Please select **LAN Interface Setup** under the **IP Config** menu and follow the instructions below to enter the LAN setting page to configure the settings you want.



Item	Description
IP Address	The default value of LAN IP address is **192.168.1.1** for this router.
Subnet Mask	Input Subnet Mask, normally it is 255.255.255.0.
Gateway	Input ISP Default Gateway Address. If you don't know, please check with your ISP.
DHCP	Enable or disable DHCP services. The DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer if enabled.
DHCP Client Range	Define the DHCP client range and then the DHCP server will assign an IP to the requesting computer from this range. The **Show Client** will display every assigned IP address, MAC address, and expired time. The default range is 192.168.1.100 - 192.168.1.200.
DHCP Lease Time	IP avaliable time
Set Static DHCP	This function allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server
Domain Name	The name of device
802.1d Spanning Tree	**IEEE 802.1d Spanning Tree Protocol (STP)** is a link layer network protocol that ensures a loop-free topology for any bridged LAN. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.
CloneMACAddress	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.

Set Static DHCP：

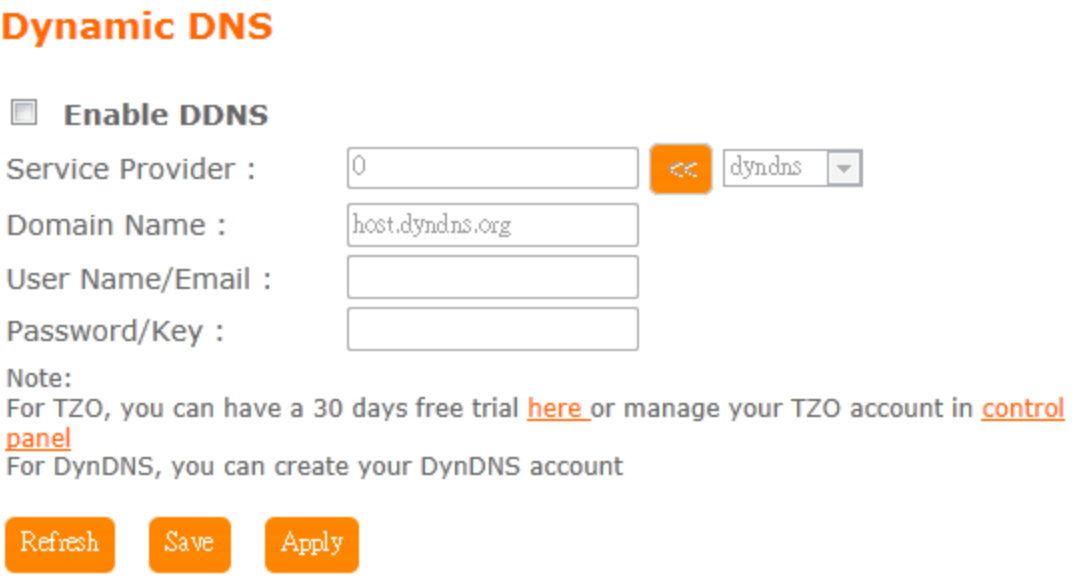


Item	Description
Enable Static DHCP	Select enable to use Static DHCP function
IP Address	Please enter IP address to limit
MAC address	Please enter MAC address to limit
Static DHCP List	**It will display all IP and MAC address you made.**
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

6.2.3 DDNS

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

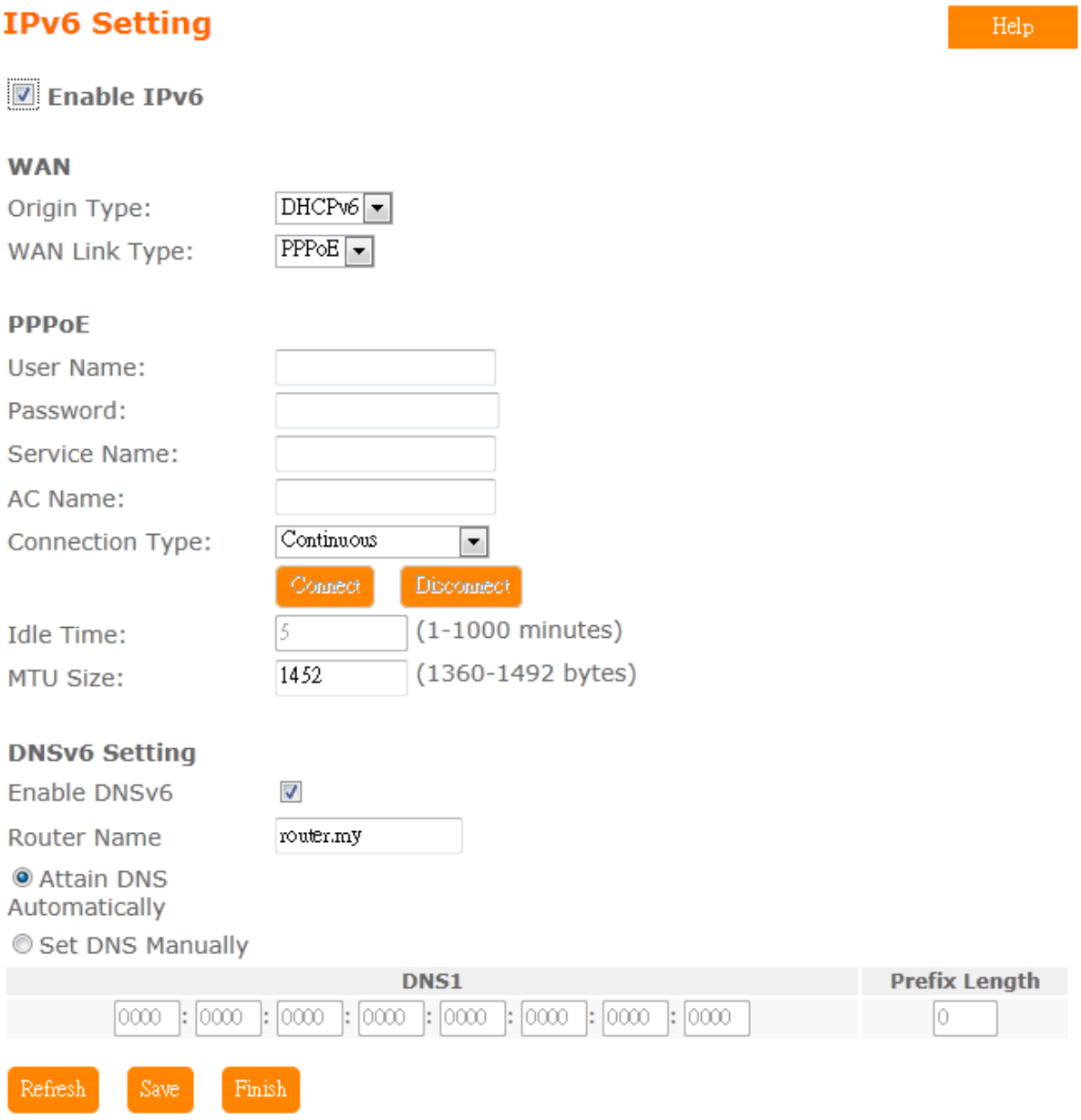
Note: make sure that you have registered with a DDNS service provider before enabling this feature.



Please enter Domain Name, User Name/Email, and Password/Key. After entering, click on Apply Changes to save the setting, or you may click on Reset to clear all the input data.

Item	Description
Enable/Disable DDNS	Select enable to use DDNS function. Each time your IP address to WAN is changed, and the information will be updated to DDNS service provider automatically.
Service Provider	Choose correct Service Provider from drop-down list, here including DynDNS, TZO, ChangeIP, Eurodns, OVH, NO-IP, ODS, Regfish embedded in BRD70N .
User Name/Email	User name is used as an identity to login Dynamic-DNS service.
Password/Key	Password is applied to login Dynamic-DNS service.
Save & Apply	Click on “Save” to save the setting data. The “Apply” button can execute current configuration

6.3 IPv6 Config

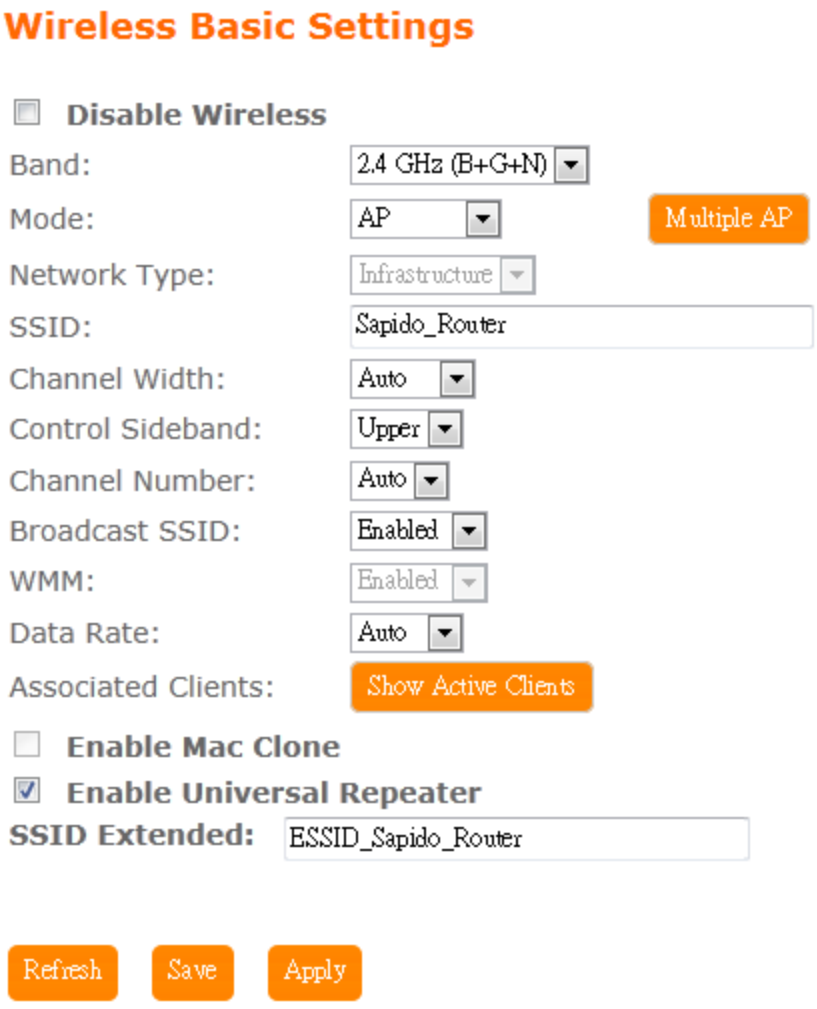


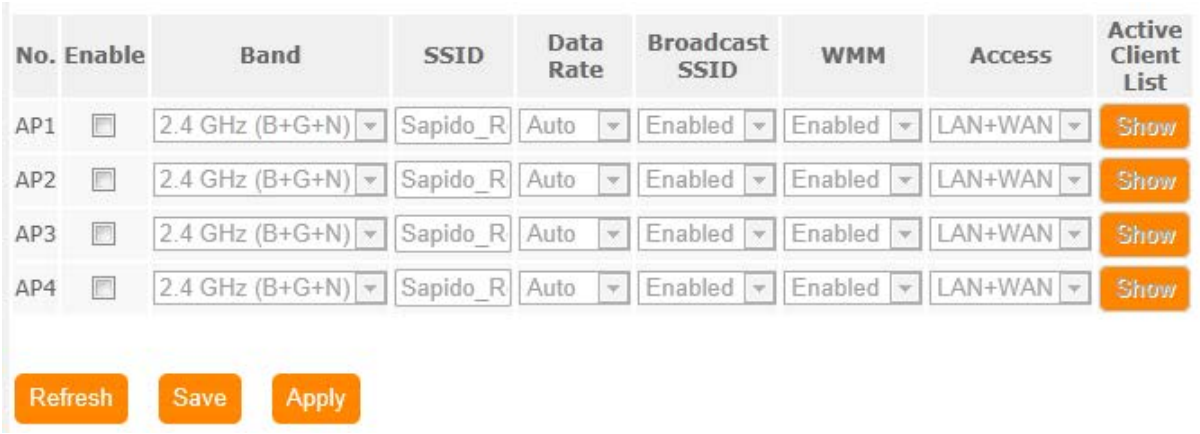
Item	Description
Origin Type	SLAAC、DHCPv6、IP。Please check ISP to get correct type
WAN Link Type	PPPoE、IP
PPPoE	Use IPv4 PPPoE account and password to do IPv6 connect
Child Prefix Address	Check ISP to get this data
Static IP	Check ISP to get IP address and default gateway IP address
Router Name	Router domain
DNSv6	Select Attain DNS Automatically. Or select Set DNS Manually, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS

6.4 Wireless

6.4.1 Basic Settings

This page is used to configure the parameters for wireless LAN clients who may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters

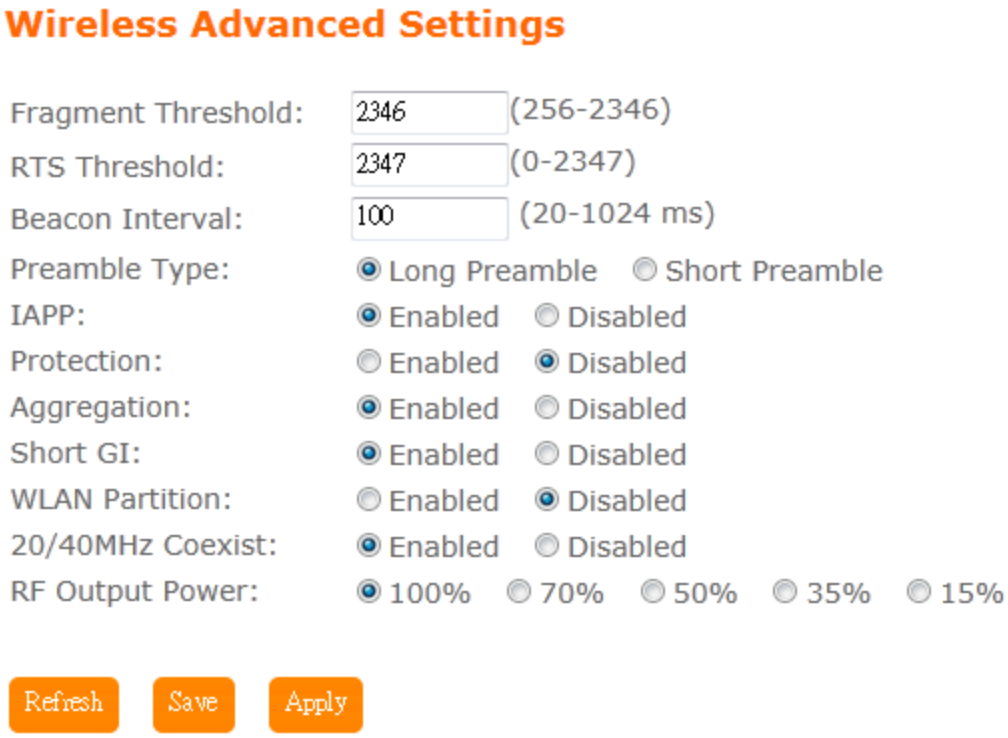




Item	Description
Disable Wireless	Turn off the wireless service.
Band	Select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
Mode	Select the mode. It has 3 modes to select: (AP, Client, WDS, AP+WDS). Multiple AP: Please check Section 4.1.2.1. * In Wi-Fi AP mode only support Client mode.
Network Type	↙ Infrastructure：one of the two methods for connecting to wireless networks with Wi-Fi enabled devices such as laptops, Pda's I-phone etc. These devices are connected to wireless network with the help of Access point (AP). Wireless Access Points are usually routers or switches which are connected to internet by Ethernet port. ↙ Ad hoc：By using ad hoc mode, devices are capable for communicating directly with each other. No Access point (routers / switches) is required for communication between devices and all devices in the range connect in peer to peer communication mode.
SSID	Service Set identifier, users can define to any or keep as default.
Channel Width	Please select the channel width, it has 3 options: 20MHz / 40MHz / Auto
Control Sideband	Enable this function will control your router use lower or upper channel.
Channel Number	Please select the channel; it has Auto, 1, 2~11 options.
Broadband SSID	User may choose to enable **Broadcast SSID** or not.
WMM	Enable / Disable Wi-Fi Multimedia
Data Rate	Please select the data transmission rate.
Associate Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
Enable Universal Repeater Mode (Acting as AP and Client simultaneously)	Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (The IP that bottom layer obtains is from upper level.)
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Multiple AP	BRD70n can register up to 4 SSIDs (wireless LAN group). It can be used as if there are multiple wireless LAN access points with one product. Each SSID could be set with different data rate, WMM and access type
Save & Apply	Click on "Save" to save the setting data. The "Apply" button can

	execute current configuration

6.4.2 Advanced Settings

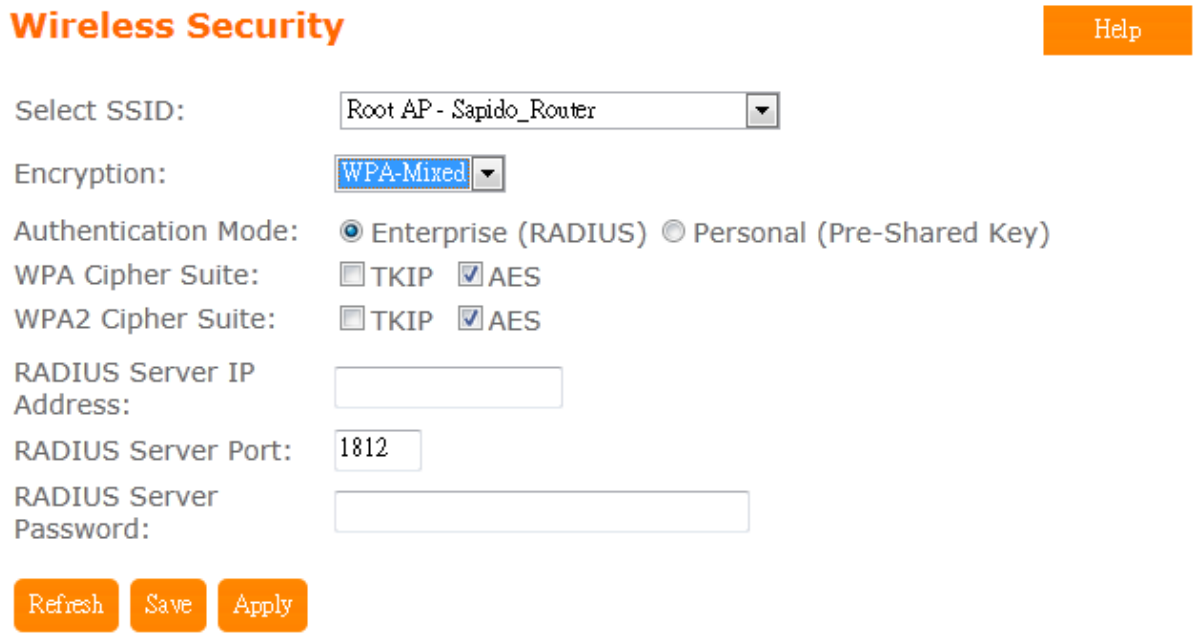


Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms..
Preamble Type	PLCP is Physical layer convergence protocol and PPDU is PLCP protocol data unit during transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. It has 2 options: Long Preamble and Short Preamble.
IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
WLAN Partition	Shut down the communication between the connected

	wireless LAN devices. If you set up as "Enabled", devices connected with the router, such as a printer, will not be able to use. Default Setting: "Disabled"
20/40MHz Coexist	Configure 20/40MHz coexisting scheme. If you set up as "Enabled", "20MHz" and "40MHz" will coexist. Normally use as "Disabled". Default Setting: "Disabled"
RF Output Power	Users can adjust RF output power to get the best wireless network environment. Users can choose from 100%, 70%, 50%, 35%, and 15%.

6.4.3 Security

Here users define the security type and level of the wireless network. Selecting different methods provides different levels of security. **Please note that using any encryption may cause a significant degradation of data throughput on the wireless link.** There are five Encryption types supported: “None”, “WEP”, “WPA”, ”WPA2”, and “WPA-Mixed”. Enabling WEP can protect your data from eavesdroppers. If you do not need this feature, select “None” to skip the following setting

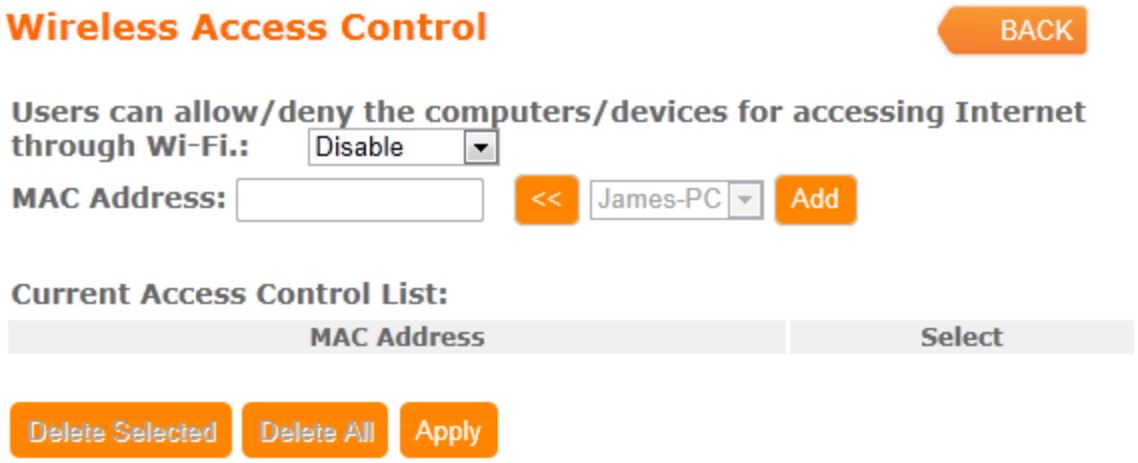


Item	Description
WEP	WEP is the most general encryption scheme among wireless LAN security, configure the common encrypted key (WEP Key) for access point and wireless LAN handset. WEP key length are "64bit", "128bit", and "256bit" (This product corresponds up to 128bit), larger the value is, more the character can be set, and encryption strength will enhanced. * If you configure the encryption key as "5 letters in half-width alphabets and numbers" or "Hexadecimal in 10 digits", please select "64-bit". * If you configure the encryption key as "13 letters in half-width alphabets and numbers" or "Hexadecimal in 26 digits", please select "128-bit".
WPA / WPA2	WPA/WPA2 is wireless LAN security standard which is

	strengthen over WEP. On WPA-PSK/WPA2-PSK, uses encrypted key called pre-shared key, and set up common encryption key for access point and wireless LAN handset like WEP. There are "AES" and "TKIP" as encryption scheme. "TKIP" automatically updates the key at regular intervals, check and approve the communication, so it can communicate safer than WEP key which uses single encryption key for long time. "AES" is harder to decode comparing to "TKIP", so it can say tougher encryption scheme than "TKIP"
WPA-Mixed	Support WPA and WPA2 at the same time
802.1x Authentication Radius	For radius server authentication
Personal (Pre-Shared Key)	* If you configure Pre-Shared Key as "Hexadecimal in 64 digits", please select "Hex (64 characters) ". * If you configure encryption key in "8 to 63 letters in half-width alphabets and numbers", please select "Passphrase

6.4.4 Access Control

Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on “Apply Change” to save the new addition. To delete a MAC address, select its corresponding checkbox under the Select column and click on “Delete Selected” button.



6.4.5 WPS

This page allows user to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client atomically synchronize it’s setting and connect to the Access Point in a minute without any hassle. SAPIDO BRD70N could support both Self-PIN or PBC modes, or use the WPS button (at real panel) to easy enable the WPS function.
PIN model, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.
PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

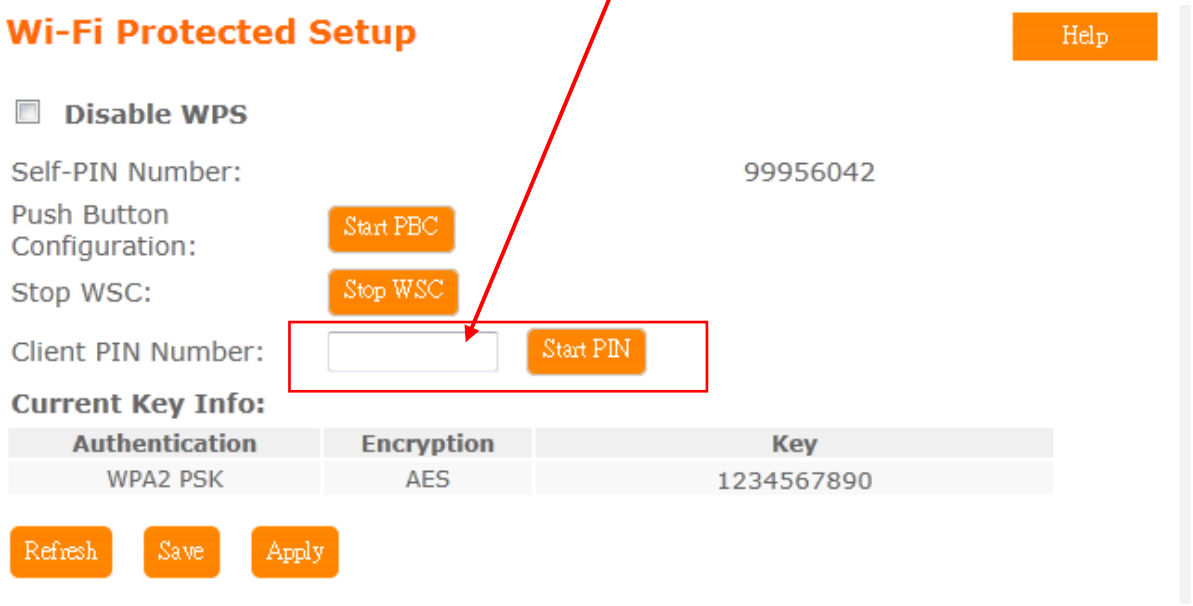
BRD70n WPS only support no encryption and WPA2

Please follow instructions below to enable the WPS function.

1. Setup Wireless LAN with WPS PIN :

(1). Get the WPS PIN number from wireless card and write it down.

(2). Fill in the PIN number from the wireless card in Client PIN Number field, and then click "Start PIN".



(3). Click PIN from Adapter Utility to complete the WPS process with the wireless router.

(4). Wireless dongle should connect to BRD70n

2. Start PBC:

(1). Press the BRD70n WPS button and wait for WPS LED blinking
(2). Press the dongle WPS button
(3). Wireless dongle should connect to BRD70n

6.5 Firewall

6.5.1 DoS

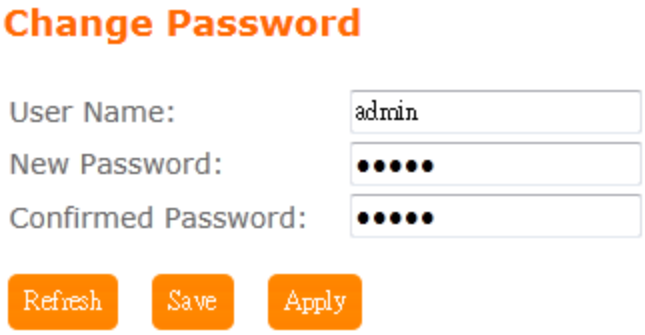
Please refer DoS

6.6 System Management

This section including , **Change Username/Password, Upgrade Firmware, Profiles Save, Remote Management, Time Zone, UPnP, Route Setup, VPN Passthrough, and Wan Type Auto Detection** . It is easy and helpful for users making more detailed settings.

6.6.1 Change Password

Users can set or change user name and password used for accessing the web management interface in this section.



Input User Name and New Password, then input Confirm Password again.

6.6.2 Firmware Upgrade

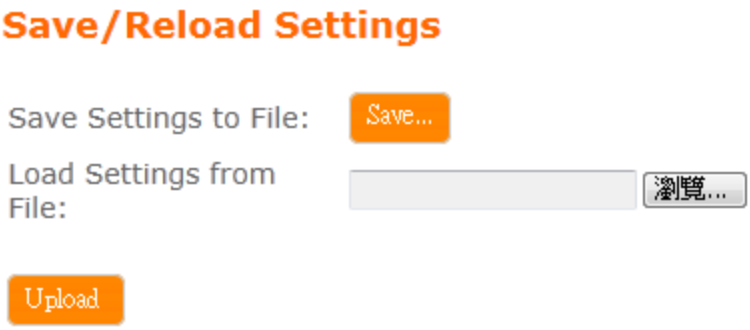
Please refer Firmware Upgrade

6.6.3 Profiles Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

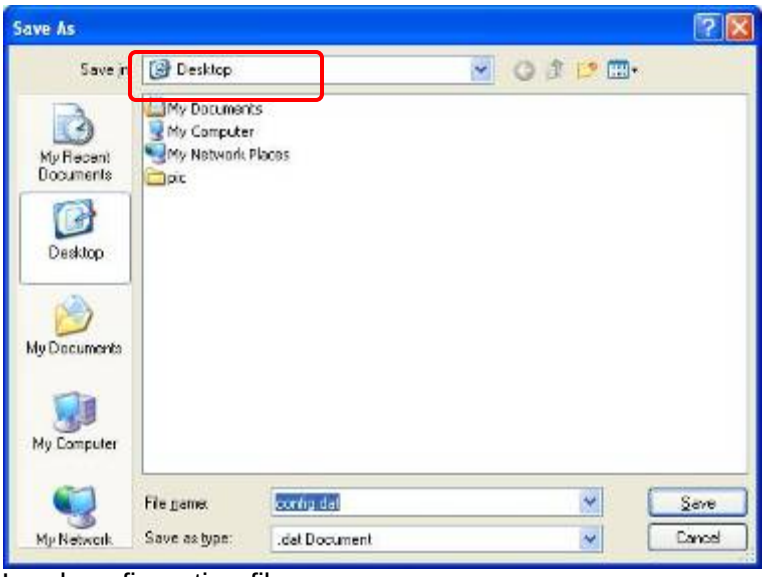
1. Save Configuration

(1). Click Save



(2). Please click “Save” to save the configuration to your computer.

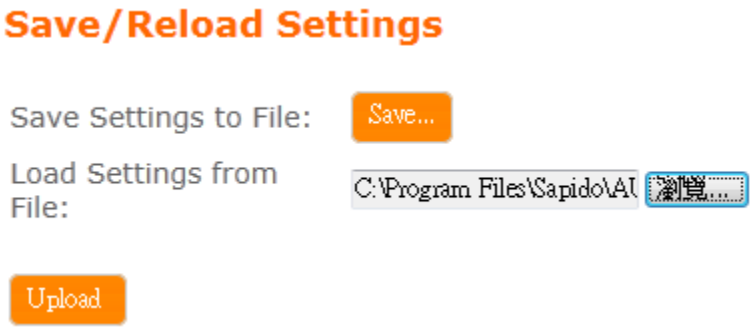
(3). Select the location which you want to save file, then click Save.



2. Load configuration file

(1). Tap “browse” and select configuration file then click Open

(2). Click Upload to upload configuration file to BRD70N .



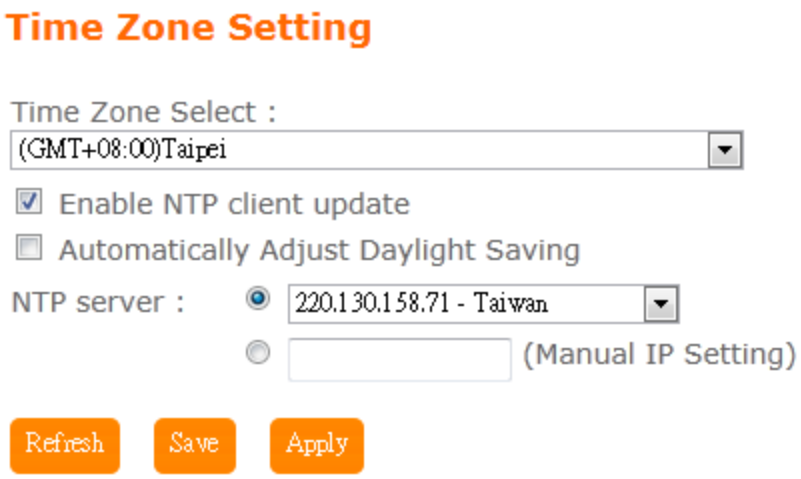
(3). After 60 seconds, BRD70N will reboot automatically.

6.6.4 Remote Management

Please refer Remote Management

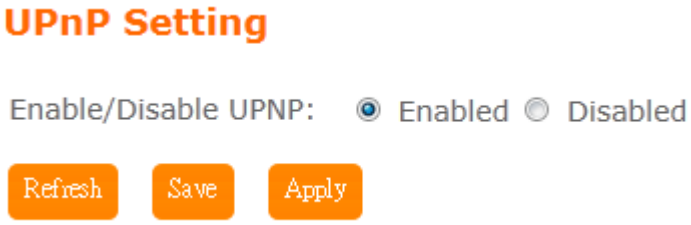
6.6.5 Time Zone

Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.



Item	Description
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable Automatically Adjust Daylight Saving or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Save & Apply	Click on Save to save the setting date, the Apply button for execute current configuration.

6.6.6 UpnP



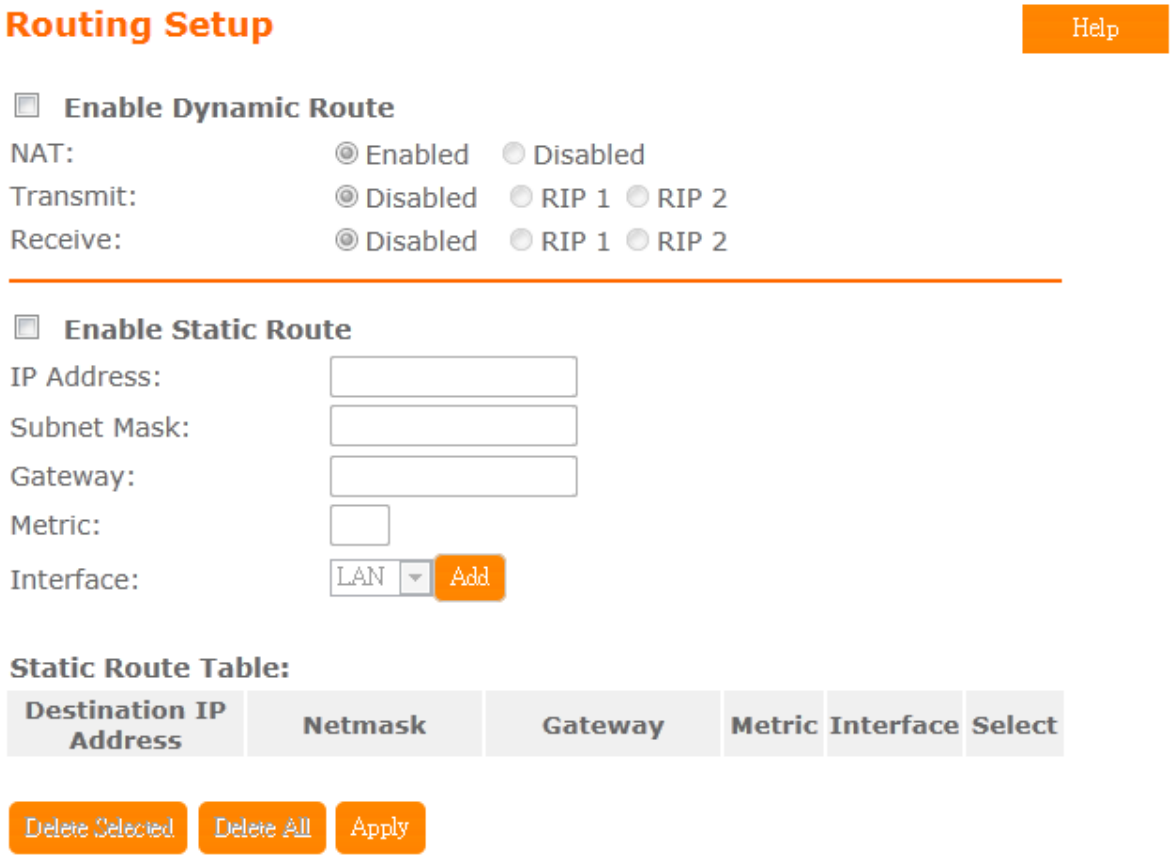
↙ **UPNP**

Universal Plug and Play (UPnP) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. BRD70N supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click My Network Places. Users will see an Internet Gateway Device icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.

6.6.7 Route Setup

Dynamic routing is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15

Static routing is a data communication concept describing one way of configuring path selection of routers in computer networks. It is the type of routing characterized by the absence of communication between routers regarding the current topology of the network. This is achieved by manually adding routes to the router routing table.

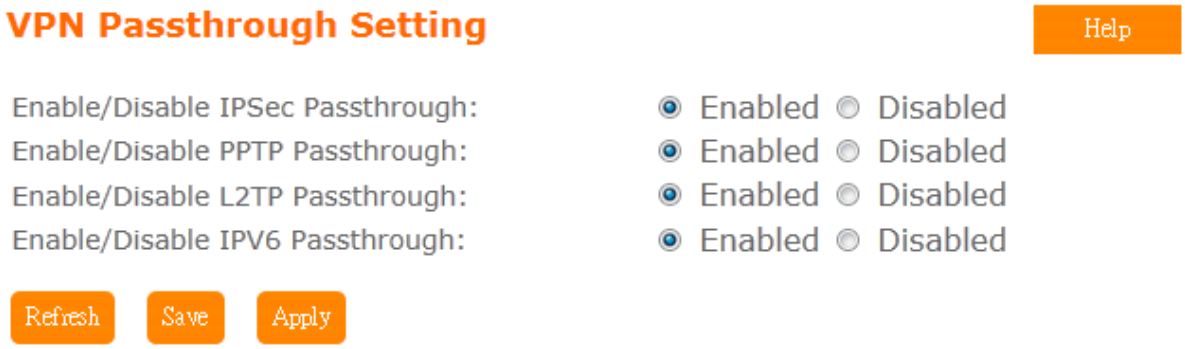


Item	Description
Enable Dynamic Route	Enable or Disable dynamic route
NAT	Enable or Disable NAT function
Transmit	There are 3 options： 1. Disable：do not send any RIP packet out 2. Send RIP1 packet out 3. Send RIP2 packet out
Receive	There are 3 options： 4. Disable：do not receive any RIP packet 5. Only receive RIP1 packet 6. Only receive RIP2 packet

Item	Description
Enable Static Route	Enable or Disable dynamic route
IP Address	Destination IP address
Subnet Mask	Destination IP subnet mask
Gateway	Gateway IP address for destination
Metric	Metric number on router's routing table
Interface	Static route rule for LAN or WAN interface

6.6.8 VPN Passthough

Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports IPSec, Pass-through, PPTP Pass-through, and L2TP Pass-through.



Item	Description
IPSec Pass-through	Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the router, IPSec Pass-through is enabled by default. To disable IPSec Pass-through , select Disable
PPTP Pass-through	Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the router, PPTP Pass-through is enabled by default. To disable PPTP Pass-through, select Disable.
L2TP Pass-through	To allow the L2TP network traffic to be forwarded to its destination without the network address translation tasks.
IPV6 Pass-through	Allow IPV6 packet to be forwarded to its destination without the network address translation tasks.

6.6.9 Wan Type Auto Detection

Chapter 7 USB to Ethernet + Wireless AP

7.1 Auto install

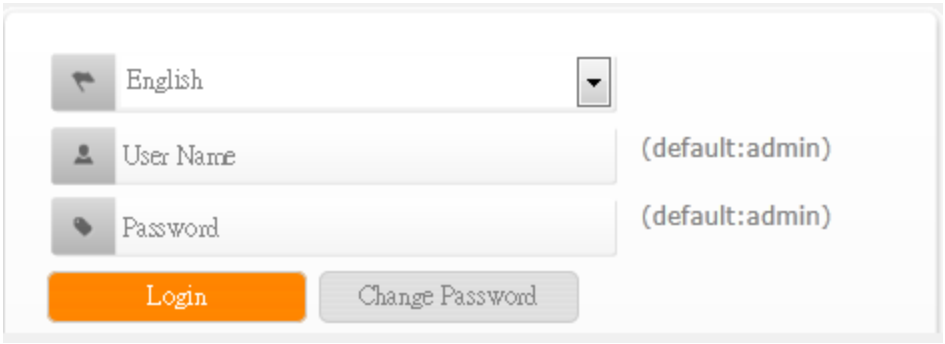
HW switch to “USB to Ethernet + Wireless AP” mode and insert it to PC/NB USB port，it can run auto install process. After that，PC/NB has a USB ethernet NIC card

7.2 Access internet

Plug in internet cable into BRD70n RJ45 ethernet port，then NB/PC can access internet，this mode is a USB ethernet card

7.3 If you want to manage BRD70n

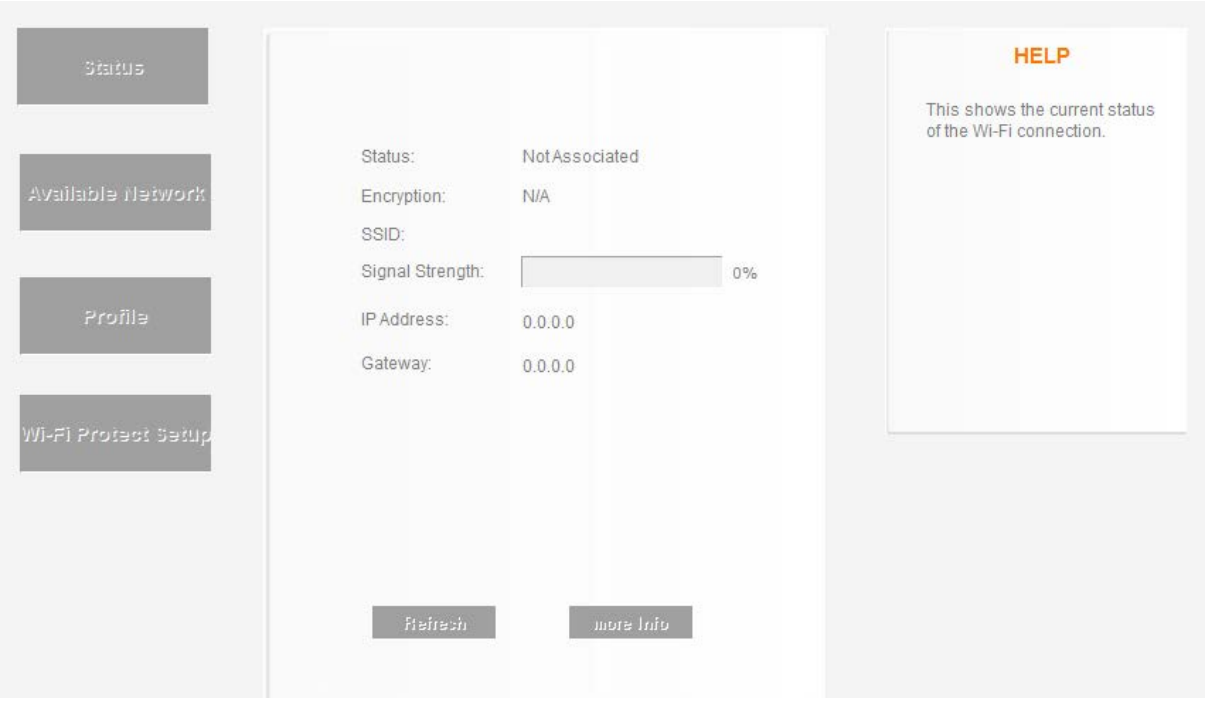
Set PC/NB BRD70n NIC card IP as 192.168.1.x，then open brower and type 192.168.1.254。The detail feature please refer BRD70n router mode



Chapter 8 Wireless dongle

8.1 Auto install

HW switch to “USB to Wireless” mode and insert it to PC/NB USB port，it can run auto install process. After that，PC/NB has BRD70n wireless utility

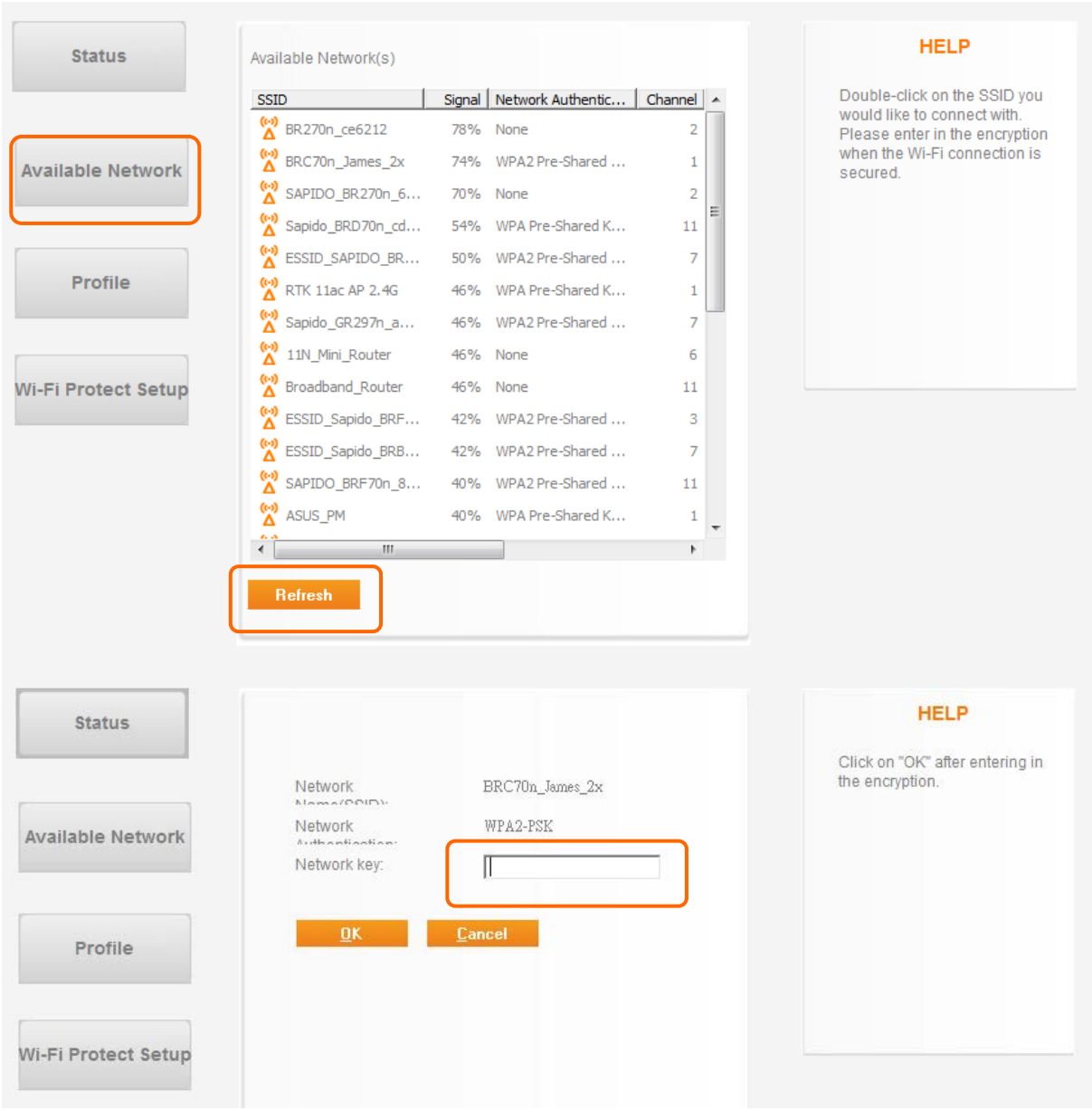


8.2 Configuring your wireless network (with Wireless Utility)

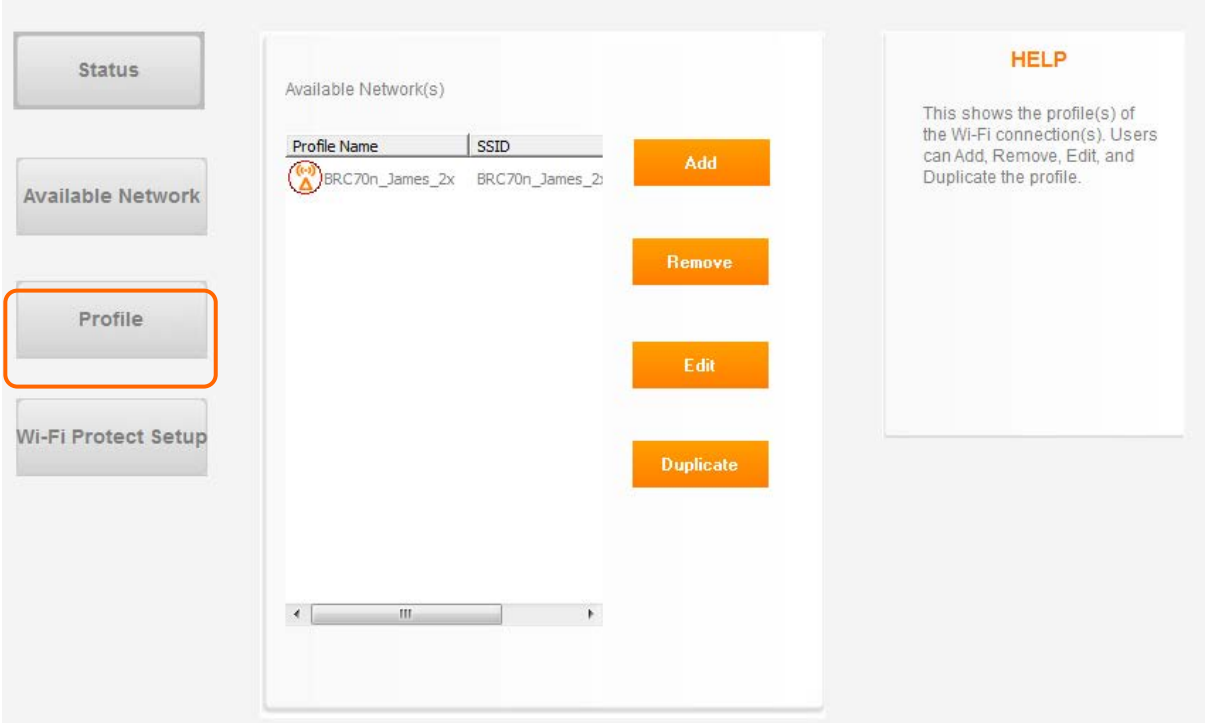
8.2.1 Double click on the computer with wireless signal icon in your taskbar or the shortcut icon on the desktop.

8.2.2 Status：Status page shows connection status.

8.2.3 Available Network：It display available wireless network. The “Refresh” button can scan the area for wireless network(s). Once the scan completed, select the desired wireless network from the list and double click it，it should pop up the wireless Network Properties window for security setting (WEP, WPA, WPA2, and etc.).

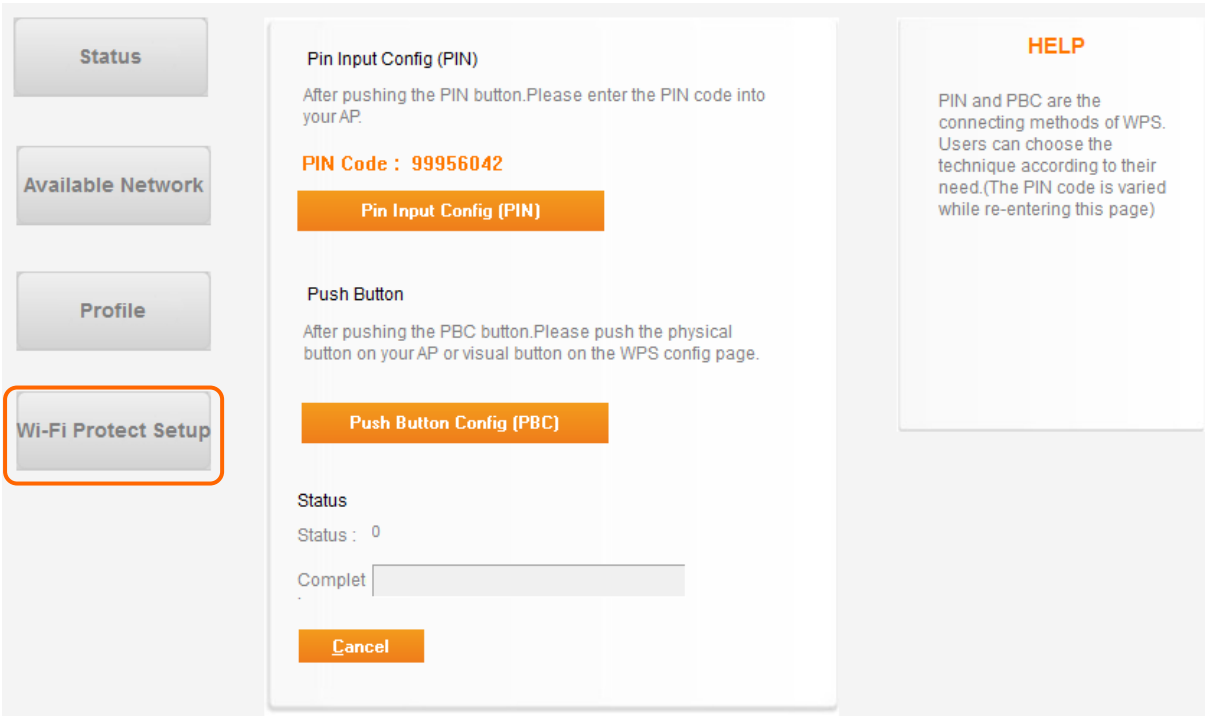


8.2.4 Profile：User can add、remove、edit, duplicate wireless connection profile in this page.



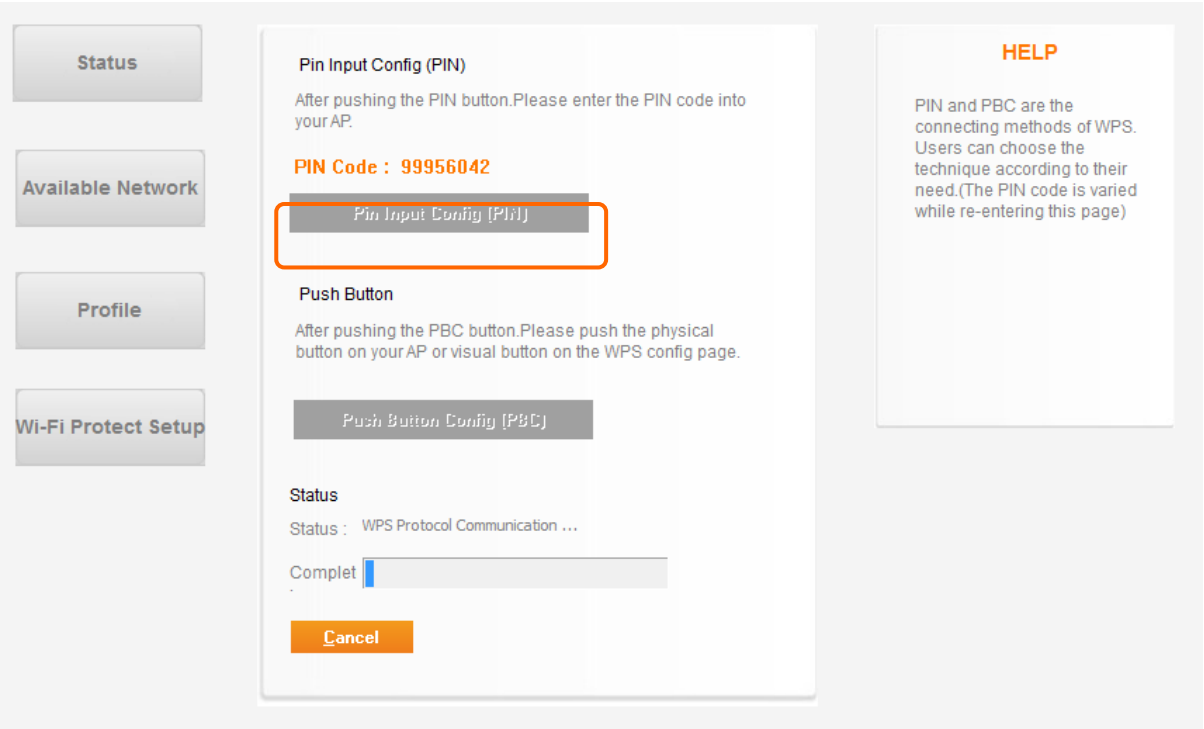
8.2.5 Wi-Fi Protect Setup (WPS)

WPS is an easy and secure setup solution for Wi-Fi network. Please click the Wi-Fi Protect Setup tab. BRD70N has two methods, PIN (Pin Input Config) and PBC (Push Button Config), to setup the network.



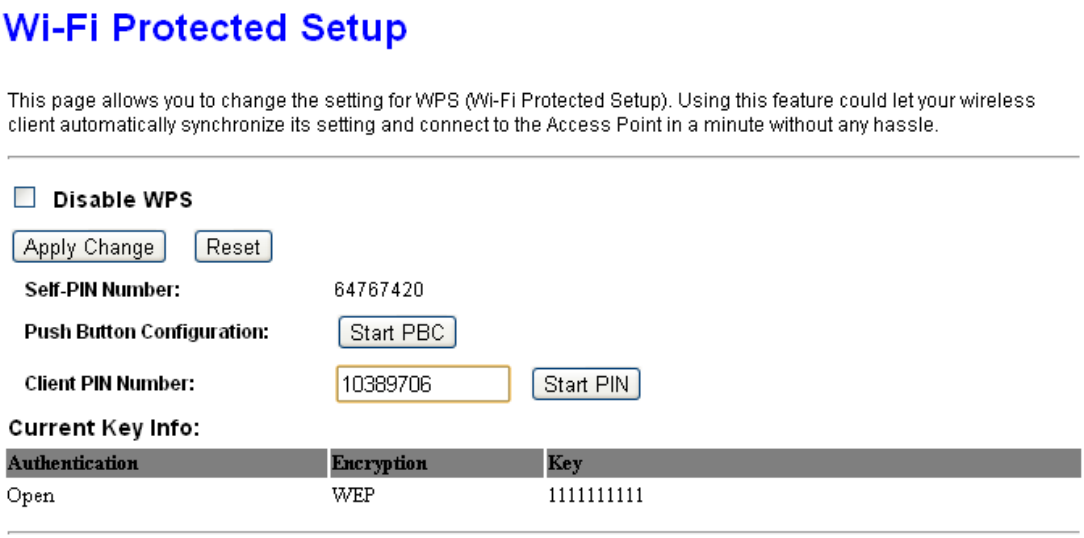
8.2.5.1 Pin Input Config (PIN)

↙ Click on the “Pin Input Config (PIN)” button, And then enter the PIN code into the AP that you want to connect. For example, the AP uses BR360n to be the connecting device. Enter the PIN code into client pin number and then clicks the “Start PIN” button.



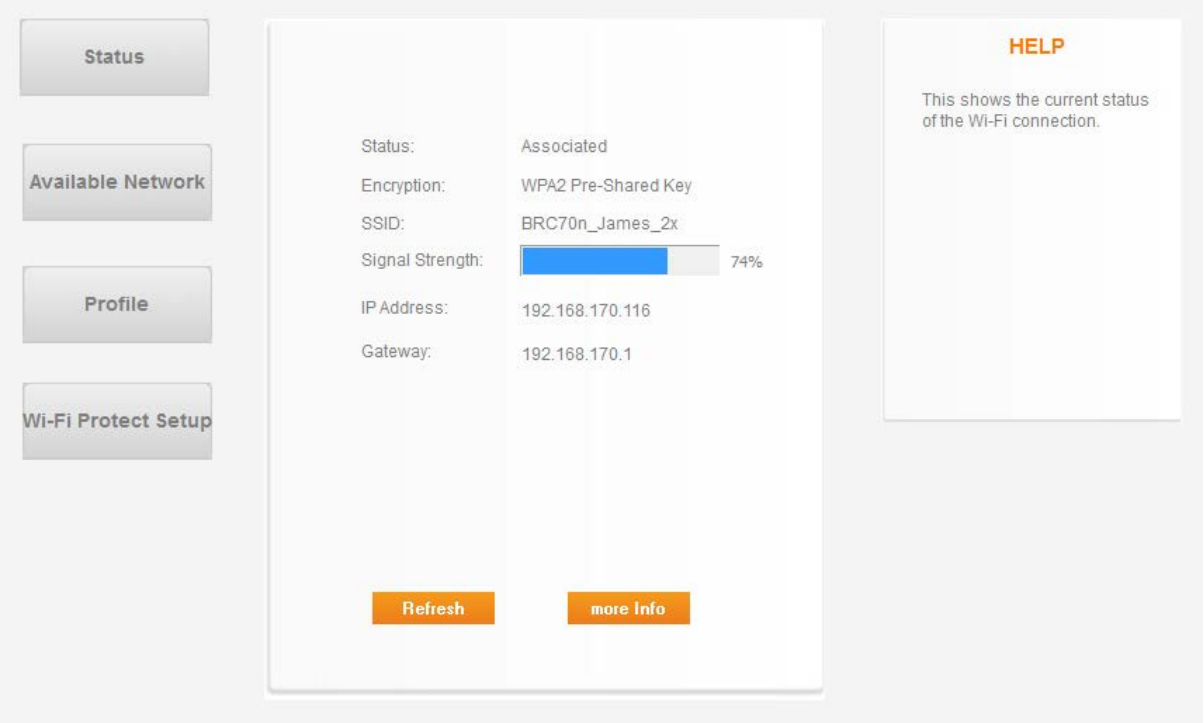
Note:

- ▶ Every time you click the tab to change the page, the PIN code will be changed.
- ▶ The PIN function in AP should be started before the WPS setup in BRD70N times out.



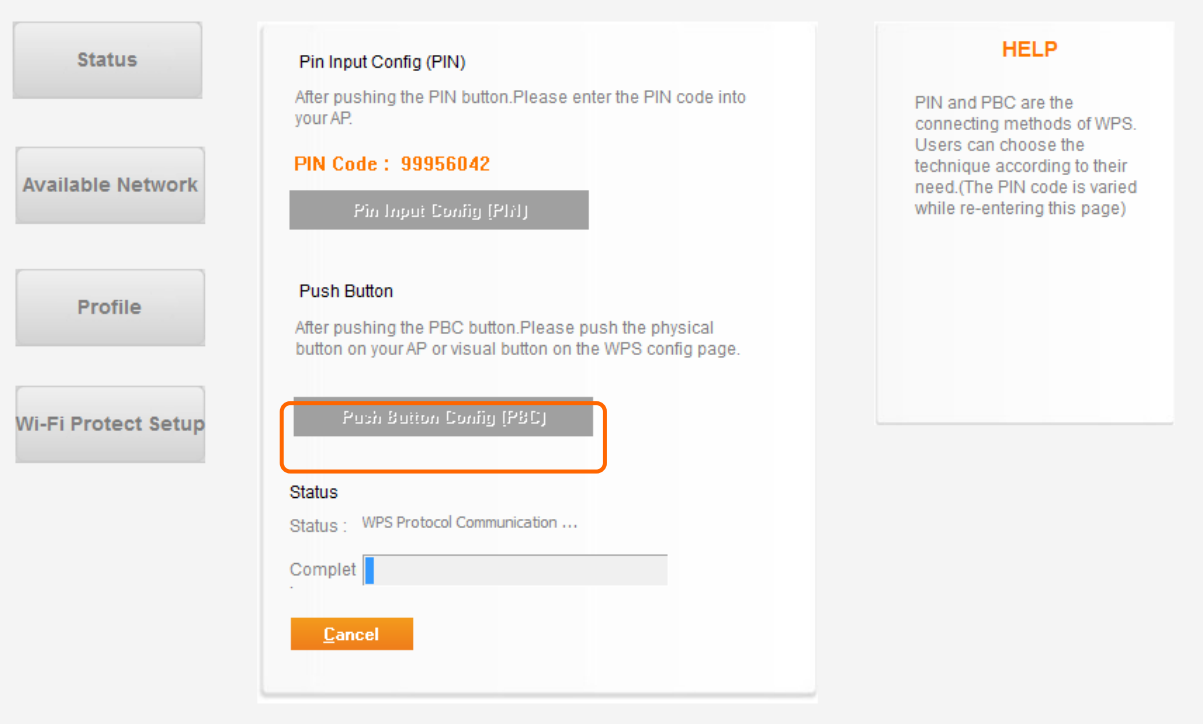
↙ BRD70N is waiting for the other AP to start the PBC function. The other AP starts the PBC function should be before BRD70N WPS times out.

2. Once the WPS connected successfully, wireless utility will show the connection status.



8.2.5.2 Push Button (PBC)

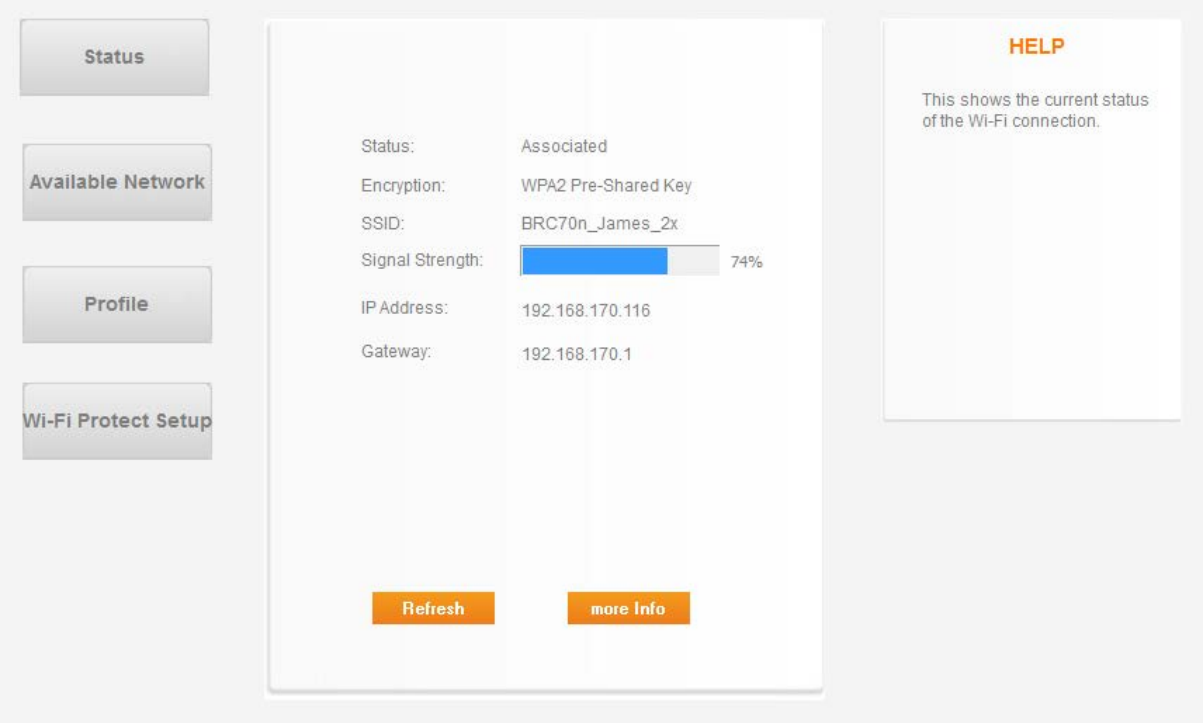
↙ Click on the “Push Button Config (PBC)” button.



Note: The PBC button can click the visual button on the page or push the physical button on AP.

↙ BRD70N is waiting for the other AP to start the PBC function. The other AP starts the PBC function should be before BRD70N WPS times out.

↙ Once WPS connected successfully, Wireless Utility will show the connection status.



8.3 Configure GUI

Please refer BRD70n router mode（login IP address：http://192.168.253.1/）