SAPIDO BRF70n User Manual

AC in Mobile Router

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

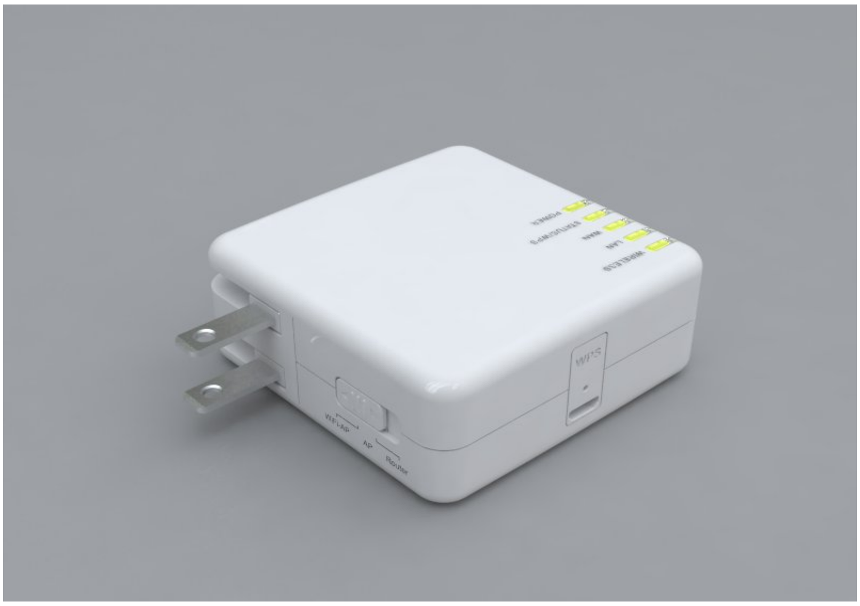
Our product has been tested in typical configuration by Ecom Sertech Corp and was found to comply with the essential requirement of "Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility” (89/336/EEC; 92/31/EEC; 93/68/EEC)

Chapter 1 Introduction

1.1 Hardware Features

Item	Specification
Key Components	
Main Processor	Realtek RTL8196E 400MHz Network Processor
Flash	4Mbytes Serial Flash
RAM	32Mbytes SDRAM
Wireless Chip	Realtek RTL8188ER 1T1R single chip
Communication Interfaces	
WAN Port	1 x 10/100Mbps RJ45 with auto MDI/MDIX
LAN Port	1 x 10/100Mbps RJ45 with auto MDI/MDIX
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˚F) Storage Temp.: -20 to 70℃(-4 to 158˚F) Operating Humidity: 10% to 85% Non-Condensing Storage Humidity: 5% to 90% Non-Condensing
Power Supply	Power Adapter DC5V/0.5A
Dimensions	66(L) x 66(W) x28 (H) mm
Device Weight	TBD

1.2 Product Appearance



LED Indicator Status Description:

LED	Function	Color	Status	Description
Power x 1	Power indicator	Green	On	Power is being applied to this product
Status / WPS x 1	Status / WPS activity	Green	On	System is ready to work
			Blinking 30ms	Reset is in progress
			Blinking 120ms	WPS function in progress
Wireless x 1	Wireless activity	Green	On	Wireless is connected
			Blinking 120ms	Wireless Tx/Rx activity
WAN x 1	WAN 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
LAN x 1	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 System and Network Setup

The BRF70N 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 BRF70N , 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.

λ Internet Account for XDSL/Cable Modem

λ One Ethernet (10/100mbps) network interface card.

λ TCP/IP and at least one web browser software installed (E.g.: Internet Explorer, Firefox, Safari、Chrome latest version).

λ 802.11b、g、n wireless adapter for wireless mobile clients.

λ Recommended OS: WinXP, Visata or Win7 / Linux.

λ

2.1 Build Network Connection

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, VPN, Firewall, etc.

Please confirm the network environment or the purpose before setting this product.

2.2 Connecting BRF70N

Prepare the followings before the connection:

λ PC or Notebook for setup

λ Ethernet cable

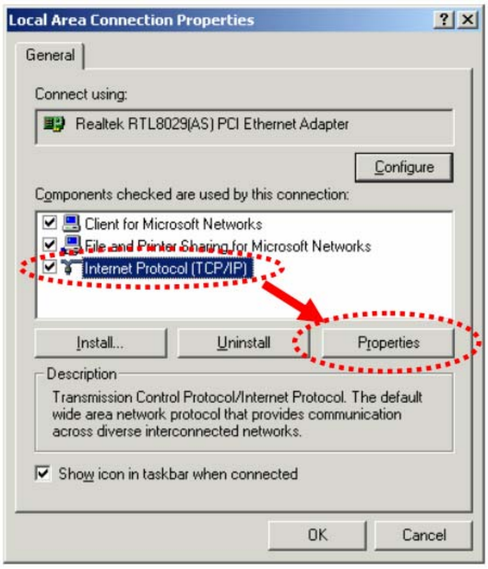
1. Make sure you are under "Router Mode".
2. Connect BRF70N to xDSL/ Cable modem with the Ethernet cable, WAN to LAN.
3. Turn on your Computer.

2.3 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:

2.3.1 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".



Local Area Connection Properties

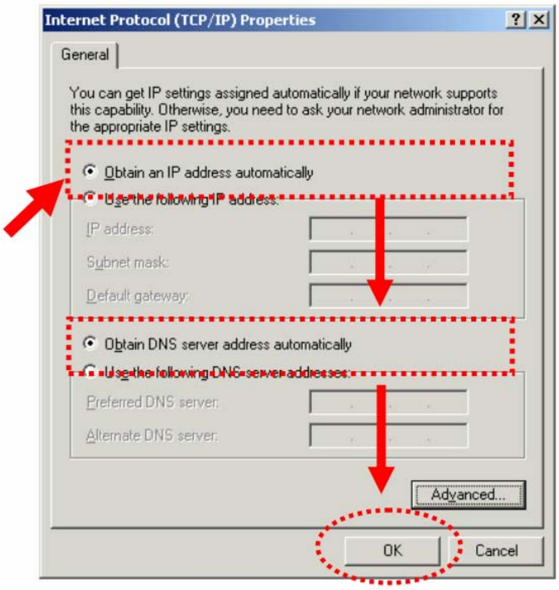
Connect using:
Realtek RTL8029(AS) PCI Ethernet Adapter

Components checked are used by this connection:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

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



Internet Protocol (TCP/IP) Properties

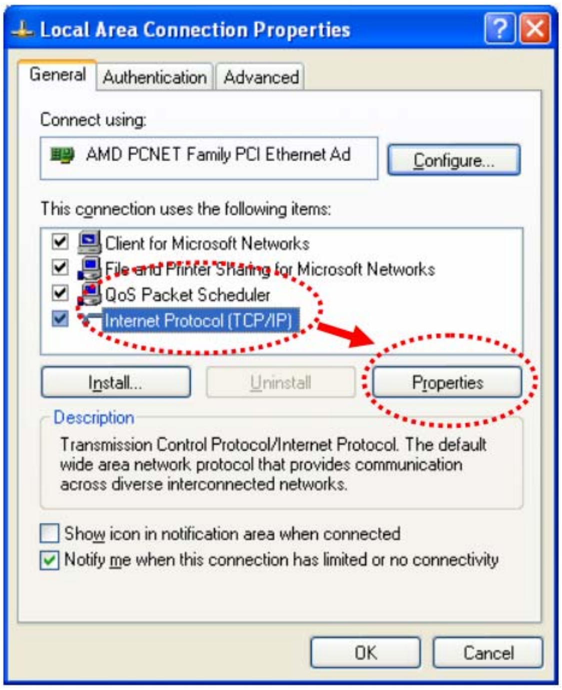
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

2.3.2 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”.



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

AMD PCNET Family PCI Ethernet Ad

This connection uses the following items:

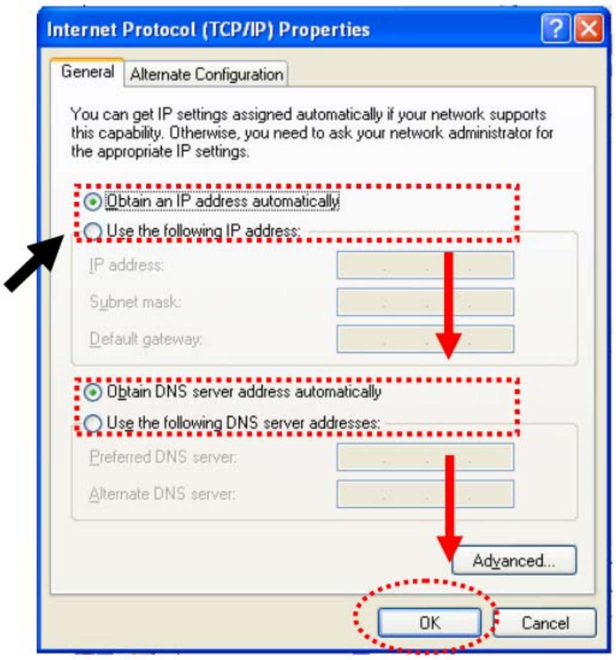
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

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



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address:
Subnet mask:
Default gateway:

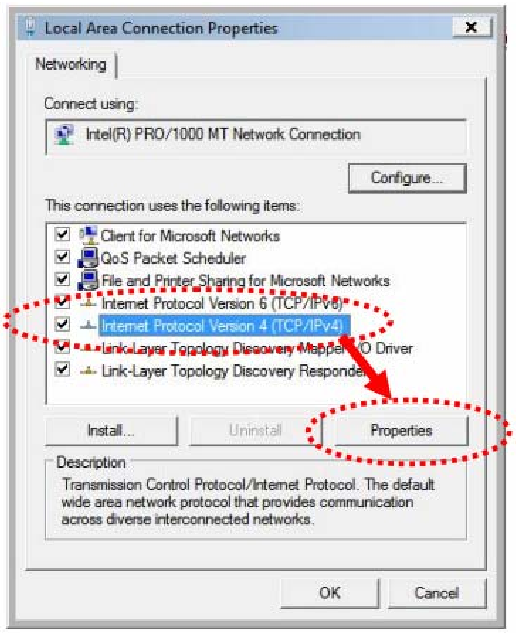
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

2.3.3 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”.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

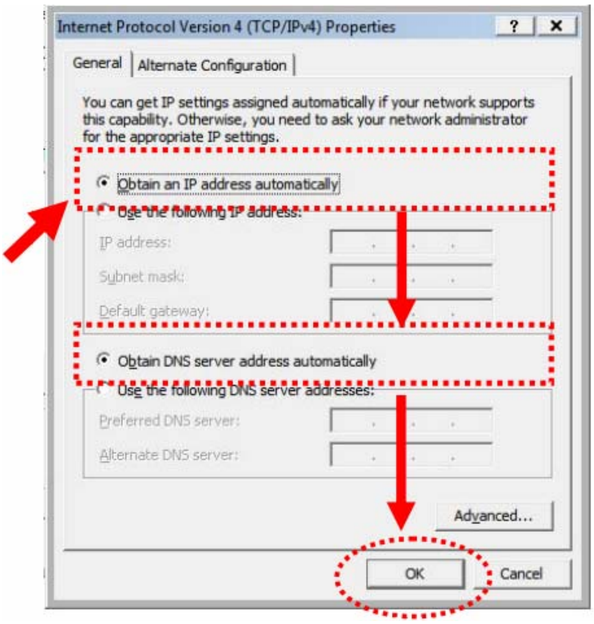
Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

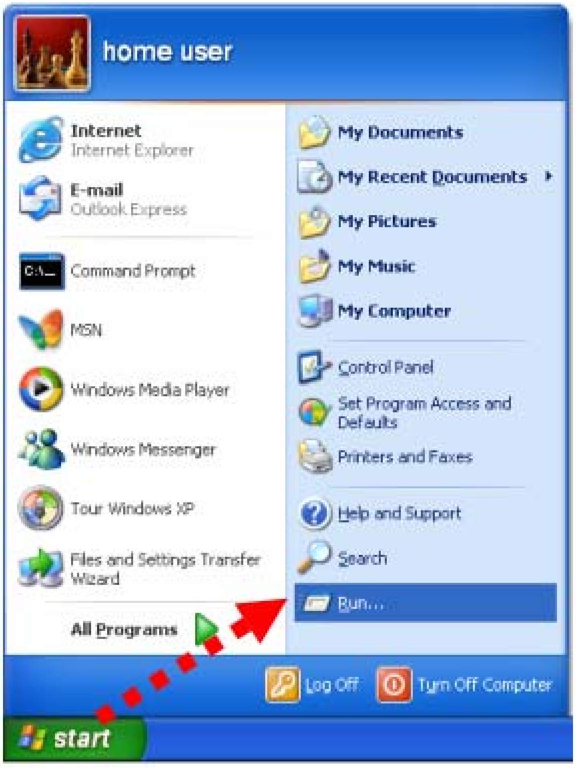
● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Advanced...

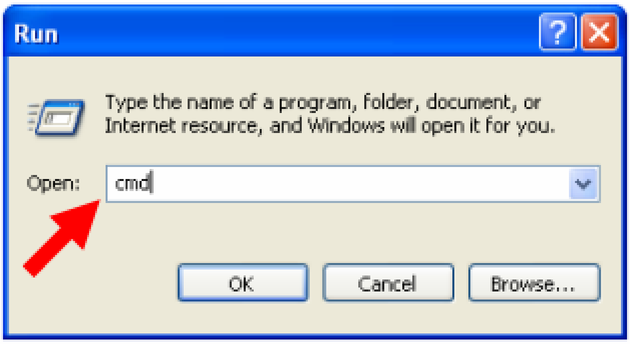
OK | Cancel

2.4 Router IP Address Lookup

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



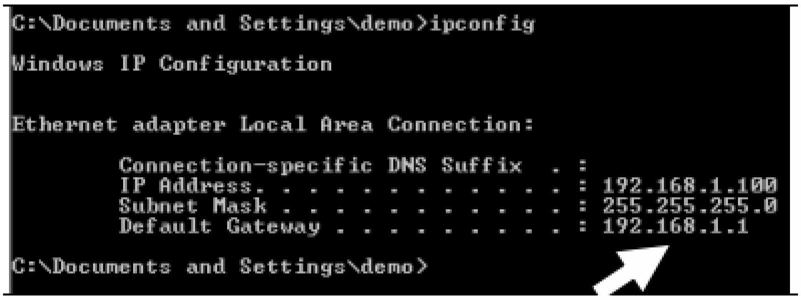
Input “cmd”, and then click “OK”.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

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)

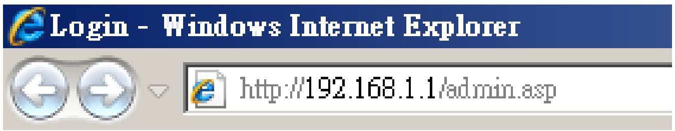


```
C:\Documents and Settings\demo>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\demo>
```

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.

2.4.1 Log into Web GUI

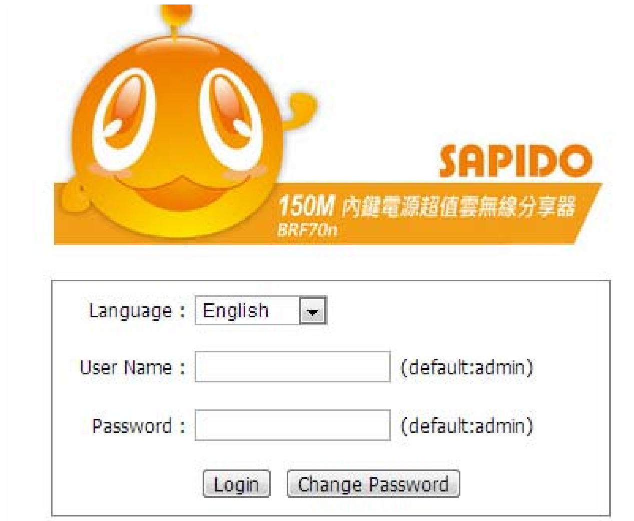
After your computer obtained an IP address from wireless router, please start your web browser, and input the IP address of the wireless router in address bar, and the following message should be shown. Please click “admin” to login the BRF70N .



Login - Windows Internet Explorer

http://192.168.1.1/admin.asp

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).

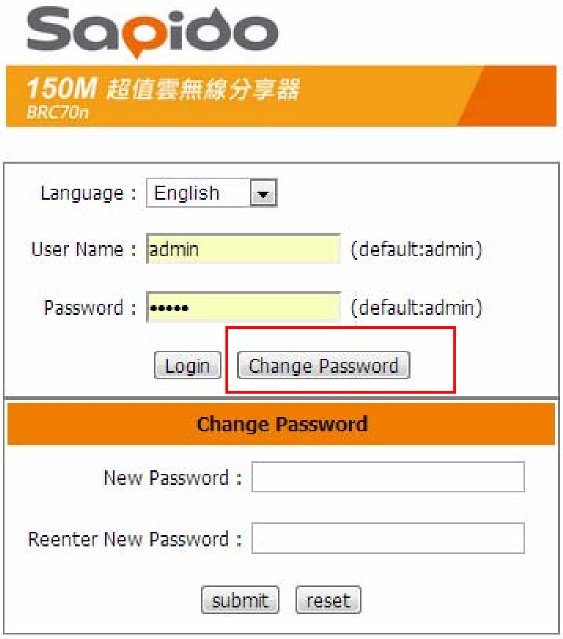


Language : English

User Name : (default:admin)

Password : (default:admin)

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



Language : English

User Name : admin (default:admin)

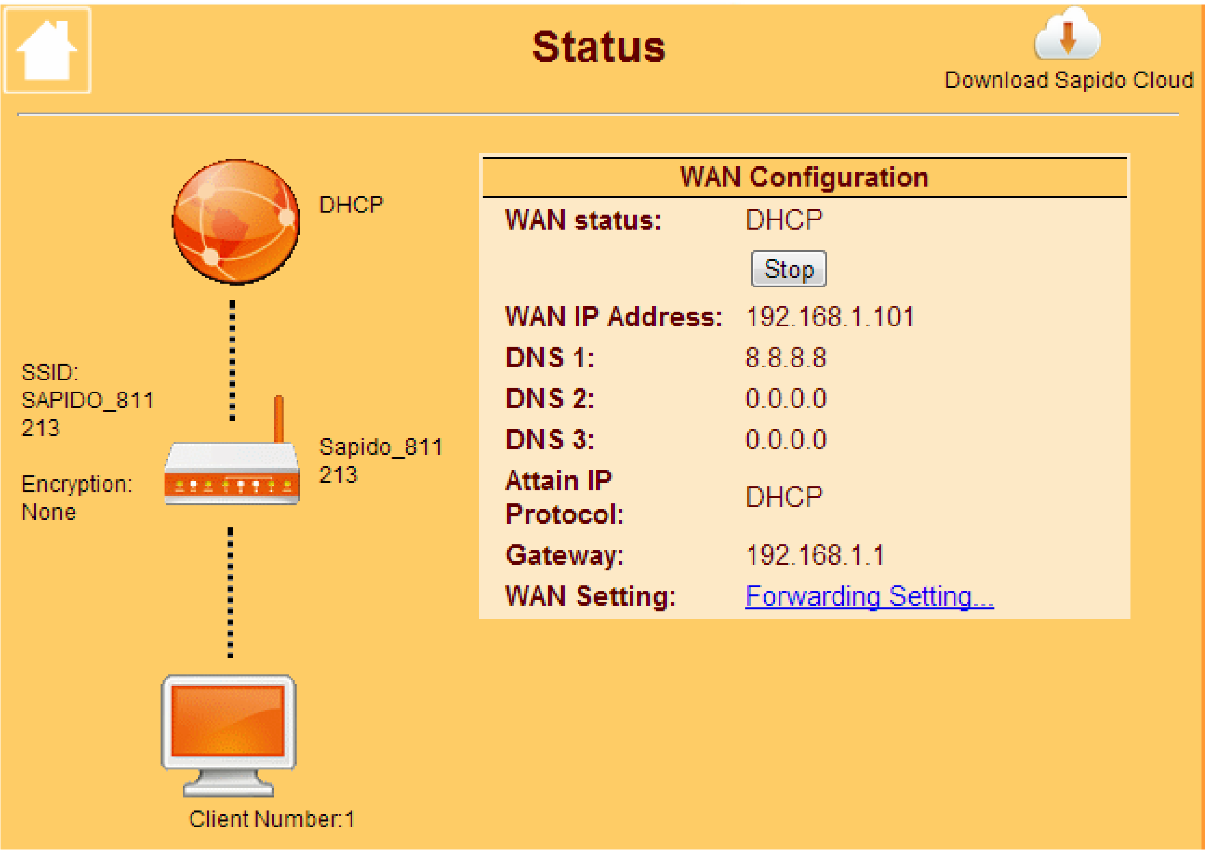
Password : ••••• (default:admin)

Change Password

New Password :

Reenter New Password :

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



Status

WAN Configuration

WAN status:	DHCP Stop
WAN IP Address:	192.168.1.101
DNS 1:	8.8.8.8
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
Attain IP Protocol:	DHCP
Gateway:	192.168.1.1
WAN Setting:	Forwarding Setting...

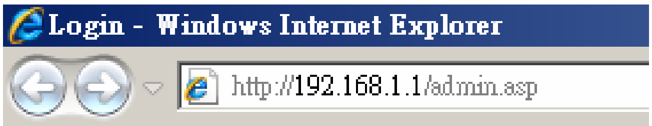
Chapter 3 Internet Connection

This Chapter describes how to setup BRF70N to the internet. The BRF70N 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

3.1 Using as a broadband router

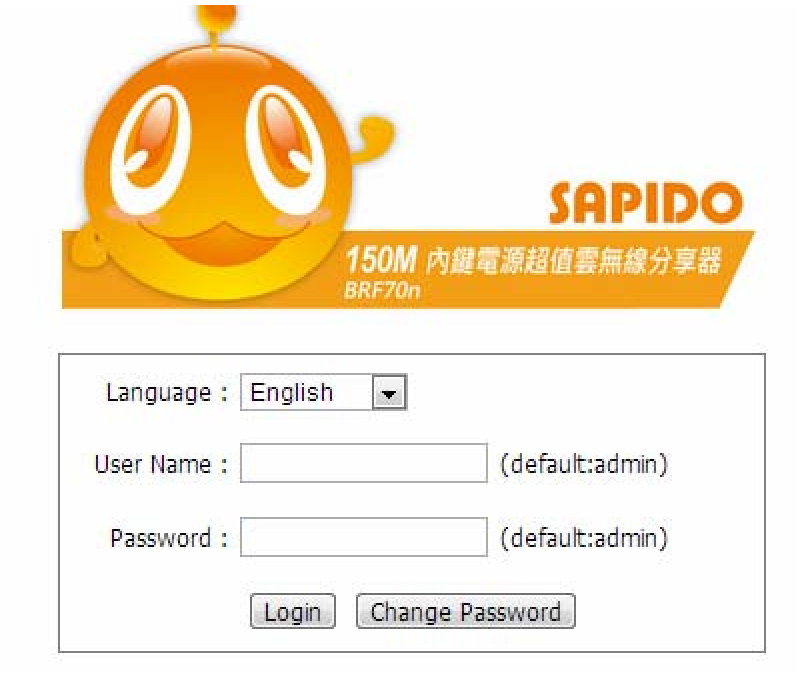
1. Open a Web browser, and enter http://192.168.1.1 (Default Gateway) into the blank.



Login - Windows Internet Explorer

http://192.168.1.1/admin.asp

2. 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).



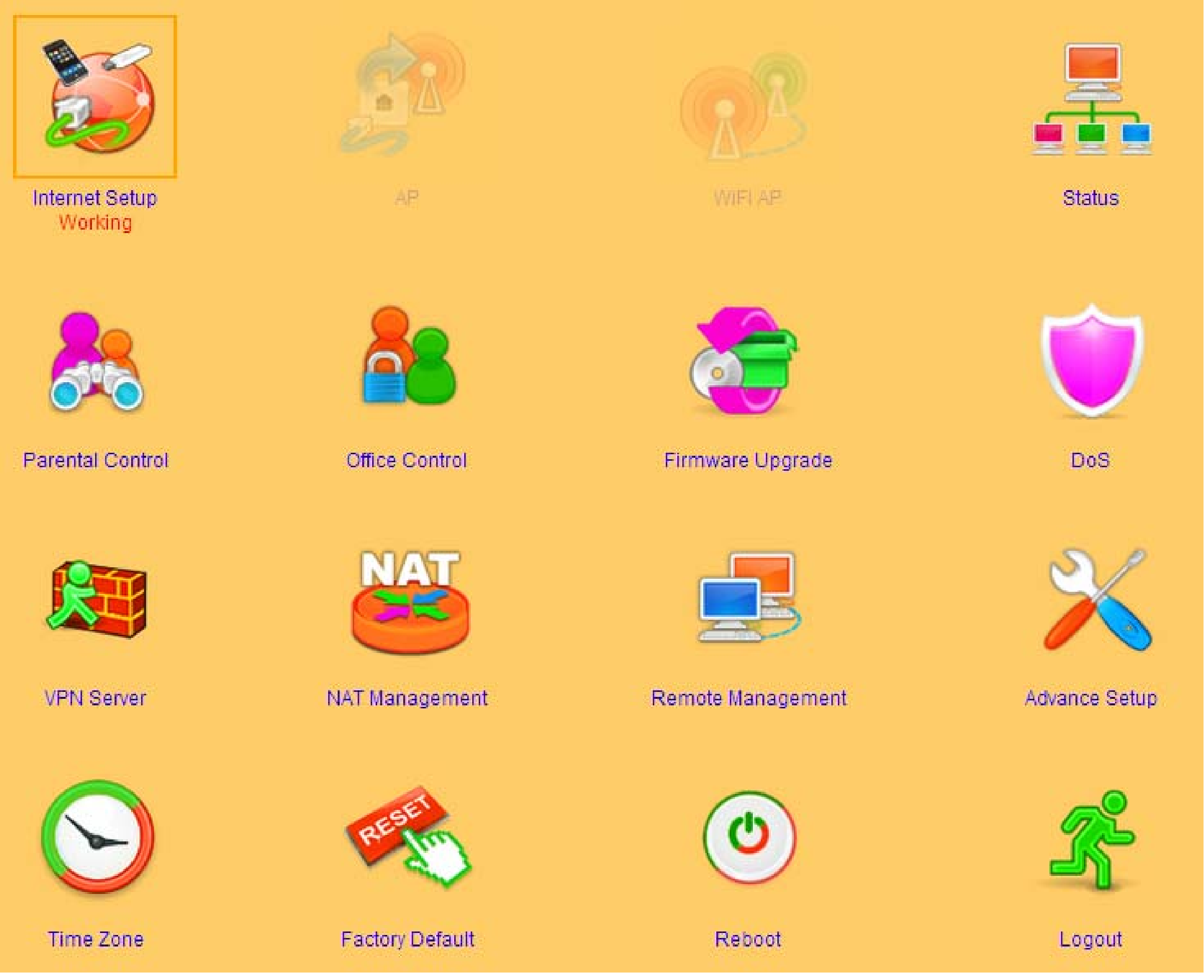
Language : English

User Name : (default:admin)

Password : (default:admin)

3.2 Home button menu

Click Home button icon to enter MENU as below.

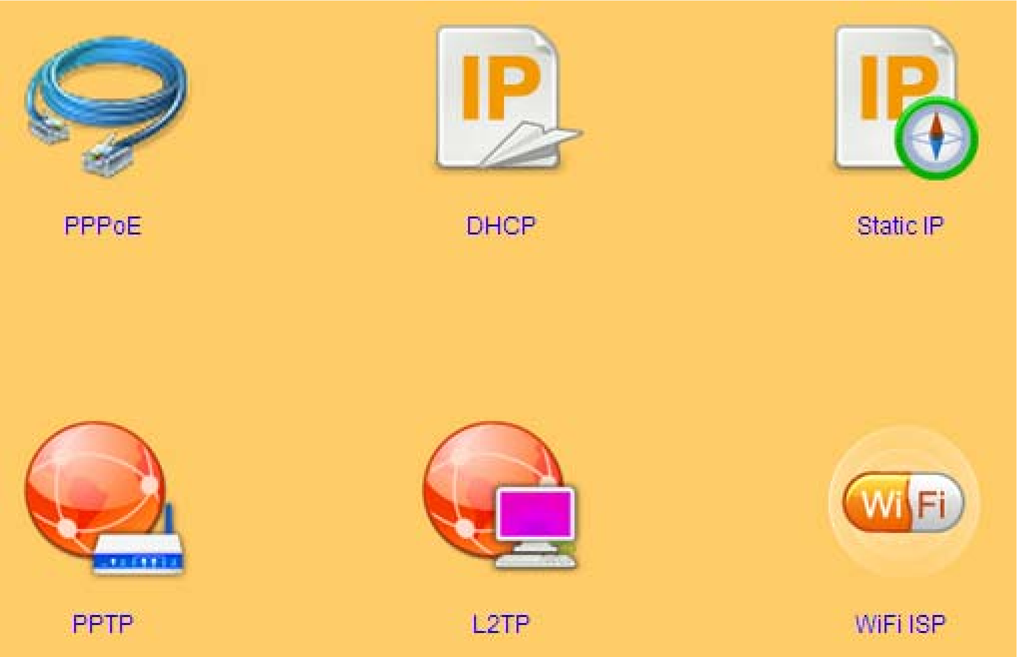


Item	Description
Internet Setup	There are several different method to access Internet，PPPoE、DHCP、Static IP、PPTP、L2TP、WiFi ISP
AP（switch to AP mode）	If a router is already set at the house, and you want to make the wireless LAN communication
WiFi AP（switch to WiFi AP mode）	When you connect to the internet wirelessly through PC and wireless device without wireless LAN function equipped.
Status	You could check WAN, LAN, Client network in status.
Parental control	You can use URL filter 、MAC Filter Schedule and Wireless Schedule to limit access Internet.
Office Control	For office environment，there are wlmultipleap_simple、Wireless Access Control、IP Filtering、IP Binding and QoS
Firmware Upgrade	This function allows you upgrade the BRF70N firmware to new version. Please note do not power off the device during the upload because it may crash the system.
DoS	Denial of Service

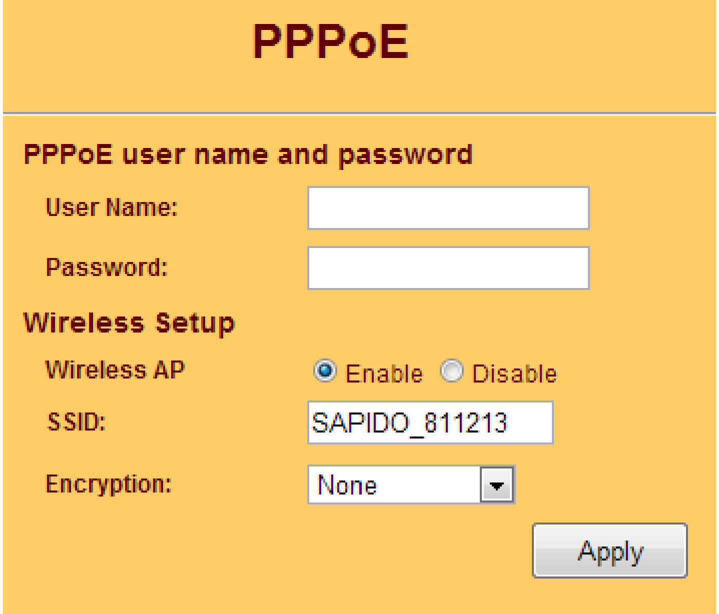
VPN Server	**PPTP/L2TP** general setup introduction.
NAT Management	There are port forwarding and DMZ function
Remote management	This page allow you to access the GUI on WAN.
Advance Setup	Advance setting menu
Time Zone	You can maintain the system time by synchronizing with a public time server over the Internet.
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.

3.3 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 BRF70N 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.



3.3.1 PPPoE


PPPoE

PPPoE user name and password

User Name:

Password:

Wireless Setup

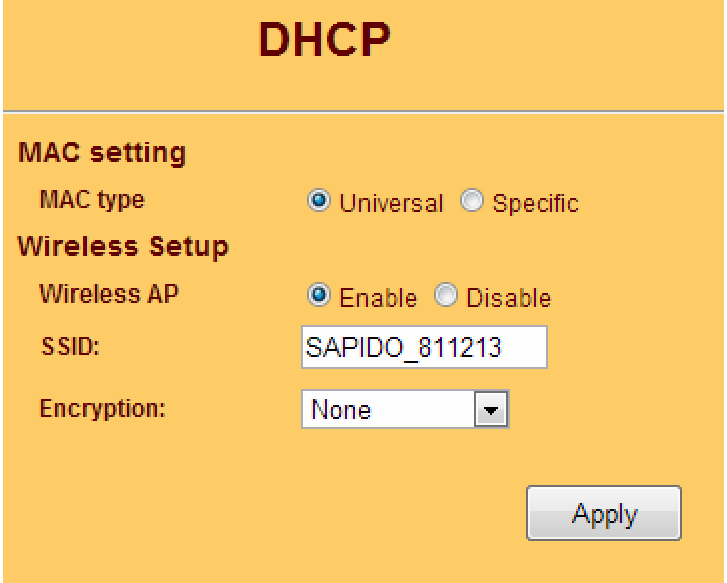
Wireless AP ● Enable ○ Disable

SSID: SAPIDO_811213

Encryption: None

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.

3.3.2 DHCP


DHCP

MAC setting

MAC type ● Universal ○ Specific

Wireless Setup

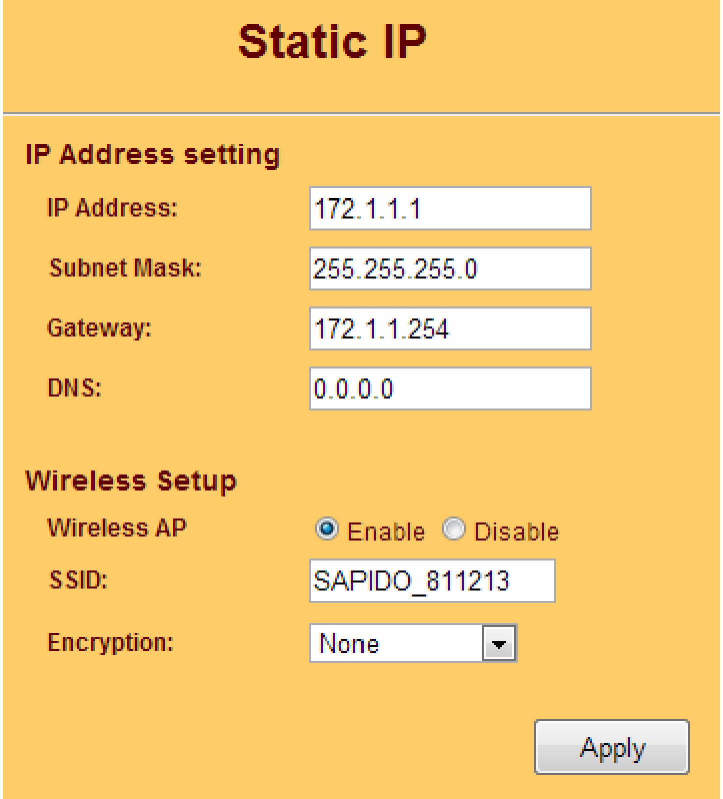
Wireless AP ● Enable ○ Disable

SSID: SAPIDO_811213

Encryption: None

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.

3.3.3 Static IP



Static IP

IP Address setting

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Gateway: 172.1.1.254

DNS: 0.0.0.0

Wireless Setup

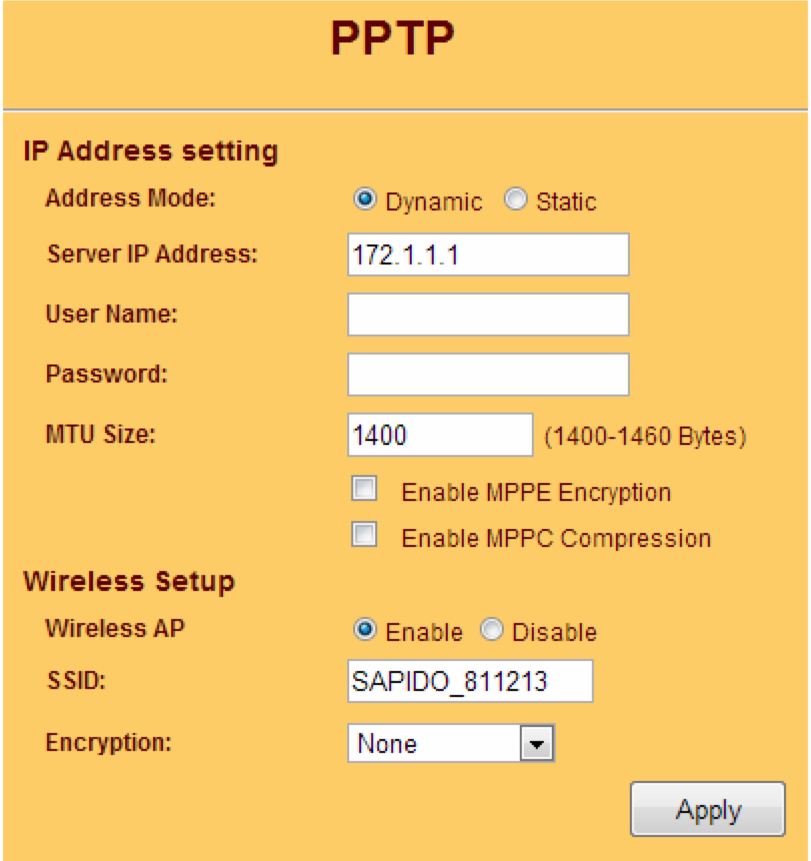
Wireless AP ● Enable ○ Disable

SSID: SAPIDO_811213

Encryption: None

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.

3.3.4 PPTP



PPTP

IP Address setting

Address Mode:	● Dynamic ○ Static
Server IP Address:	172.1.1.1
User Name:	
Password:	
MTU Size:	1400 (1400-1460 Bytes)
	□ Enable MPPE Encryption
	□ Enable MPPC Compression

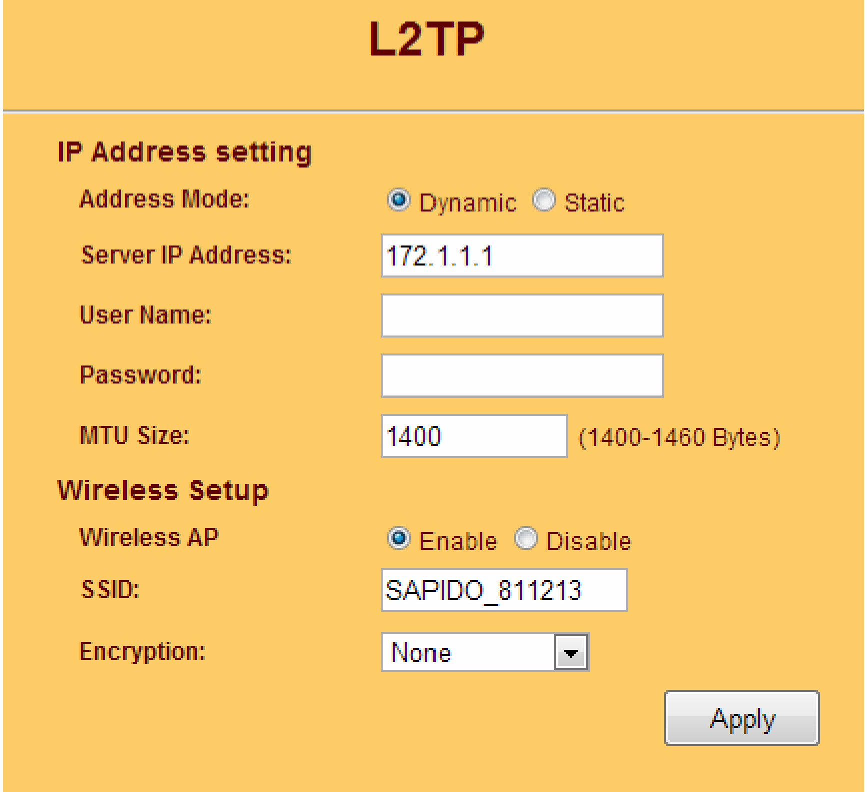
Wireless Setup

Wireless AP	● Enable ○ Disable
SSID:	SAPIDO_811213
Encryption:	None

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.

3.3.5 L2TP



L2TP

IP Address setting

Address Mode: ● Dynamic ○ Static

Server IP Address: 172.1.1.1

User Name:

Password:

MTU Size: 1400 (1400-1460 Bytes)

Wireless Setup

Wireless AP ● Enable ○ Disable

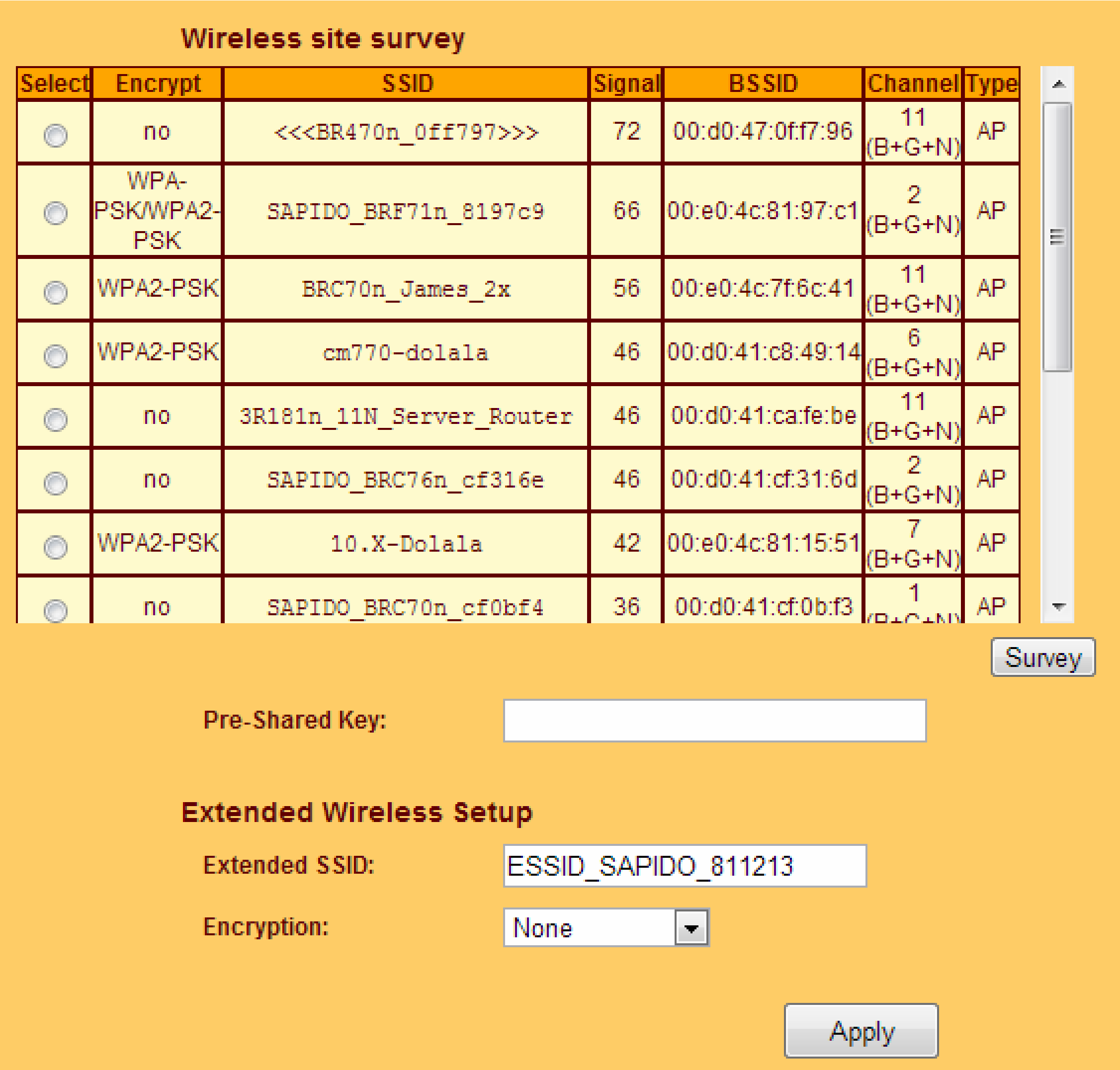
SSID: SAPIDO_811213

Encryption: None

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.

3.3.6 WiFi ISP

BRF70n WAN get IP address from other wireless AP and LAN/Wireless LAN client get IP from BRF70n.



Wireless site survey

Select	Encrypt	SSID	Signal	BSSID	Channel	Type
○	no	<<<BR470n_0ff797>>>	72	00:d0:47:0f:f7:96	11 (B+G+N)	AP
○	WPA-PSK/WPA2-PSK	SAPIDO_BRF71n_8197c9	66	00:e0:4c:81:97:c1	2 (B+G+N)	AP
○	WPA2-PSK	BRC70n_James_2x	56	00:e0:4c:7f:6c:41	11 (B+G+N)	AP
○	WPA2-PSK	cm770-dolala	46	00:d0:41:c8:49:14	6 (B+G+N)	AP
○	no	3R181n_11N_Server_Router	46	00:d0:41:ca:fe:be	11 (B+G+N)	AP
○	no	SAPIDO_BRC76n_cf316e	46	00:d0:41:cf:31:6d	2 (B+G+N)	AP
○	WPA2-PSK	10.X-Dolala	42	00:e0:4c:81:15:51	7 (B+G+N)	AP
○	no	SAPIDO_BRC70n_cf0bf4	36	00:d0:41:cf:0b:f3	1	AP

Pre-Shared Key:

Extended Wireless Setup

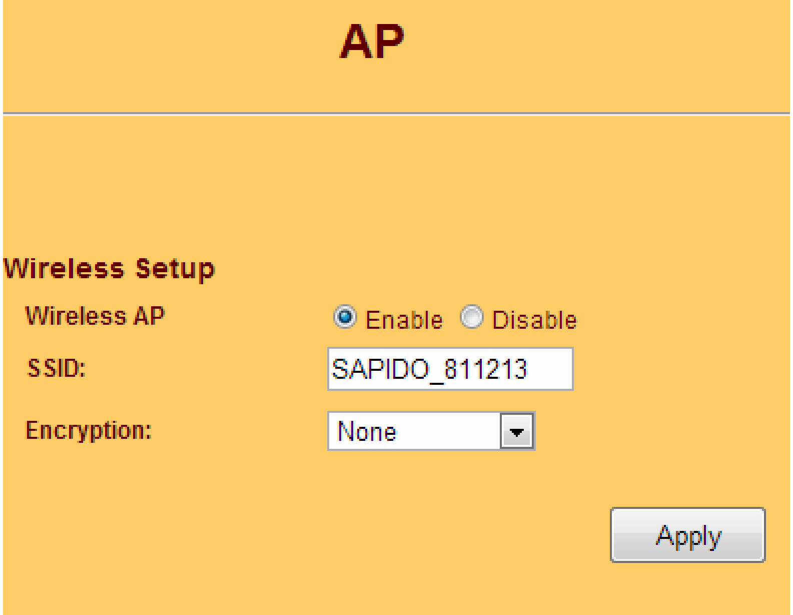
Extended SSID: ESSID_SAPIDO_811213

Encryption: None

Item	Description
Survey	List all available wireless AP
Pre-Shared Key	Input the wireless AP key which you want to connect
Extend SSID	Provide SSID for wireless client which want to connect to BRF70n
Encryption	Select wireless encryption type form the drop-down list.

3.4 AP

If a router is already set at the house, and you want to make the wireless LAN communication. This mode does not support WAN、DHCP、NAT、DDNS、QoS、Firewall、Static/Dynamic route、VPN Server features.



AP

Wireless Setup

Wireless AP ● Enable ○ Disable

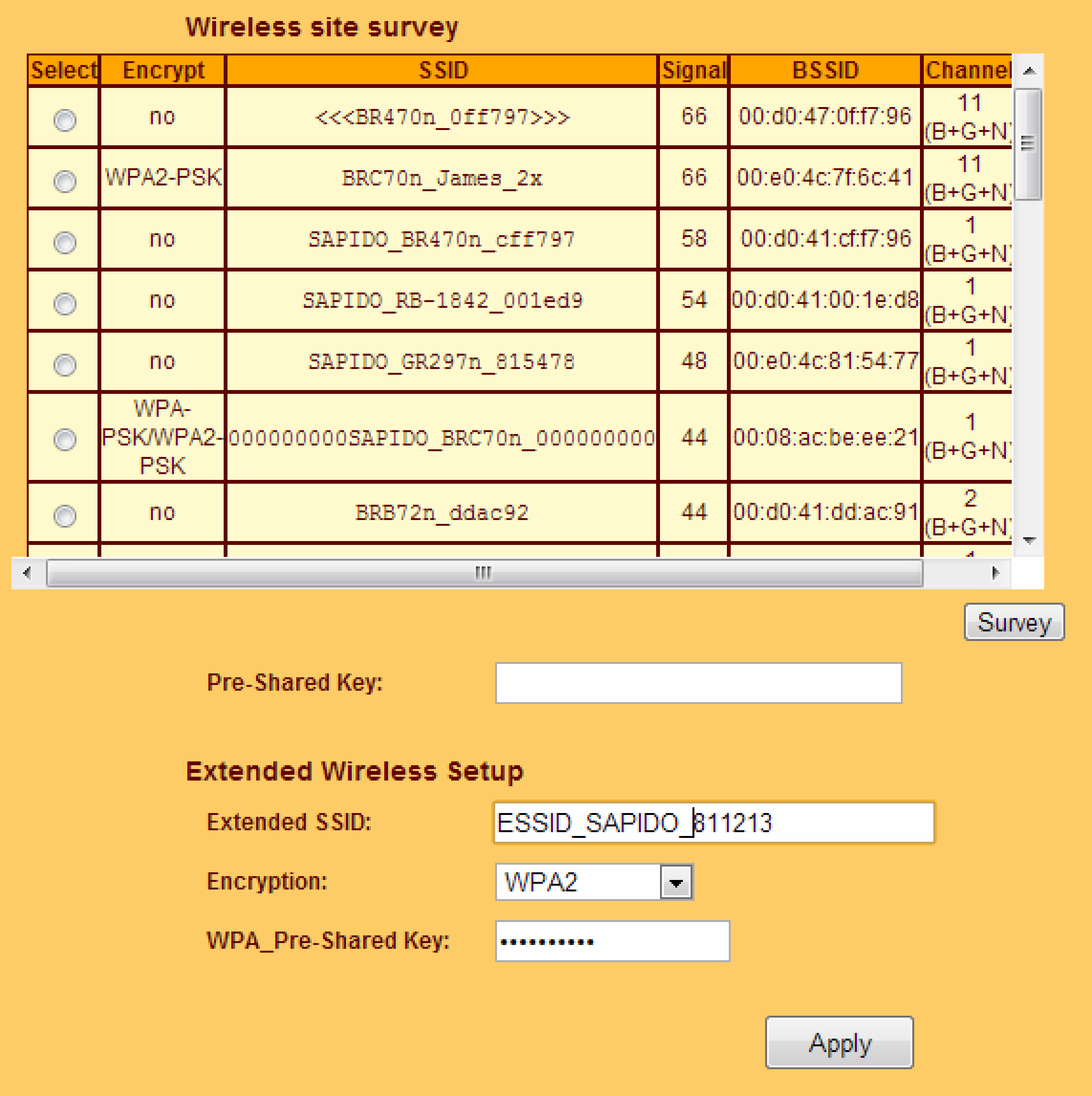
SSID: SAPIDO_811213

Encryption: None

Item	Description
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.
Wireless AP	Turn on/off wireless

3.5 WiFi AP

When you connect to the internet wirelessly through PC and wireless device without wireless LAN function equipped. This mode does not support WAN、DHCP、NAT、DDNS、QoS、Firewall、Static/Dynamic route、VPN Server features.



Wireless site survey

Select	Encrypt	SSID	Signal	BSSID	Channel
○	no	<<<BR470n_0ff797>>>	66	00:d0:47:0f:f7:96	11 (B+G+N)
○	WPA2-PSK	BRC70n_James_2x	66	00:e0:4c:7f:6c:41	11 (B+G+N)
○	no	SAPIDO_BR470n_cff797	58	00:d0:41:cf:f7:96	1 (B+G+N)
○	no	SAPIDO_RB-1842_001ed9	54	00:d0:41:00:1e:d8	1 (B+G+N)
○	no	SAPIDO_GR297n_815478	48	00:e0:4c:81:54:77	1 (B+G+N)
○	WPA-PSK/WPA2-PSK	000000000SAPIDO_BRC70n_000000000	44	00:08:ac:be:ee:21	1 (B+G+N)
○	no	BRB72n_ddac92	44	00:d0:41:dd:ac:91	2 (B+G+N)

Pre-Shared Key:

Extended Wireless Setup

Extended SSID: ESSID_SAPIDO_811213

Encryption: WPA2

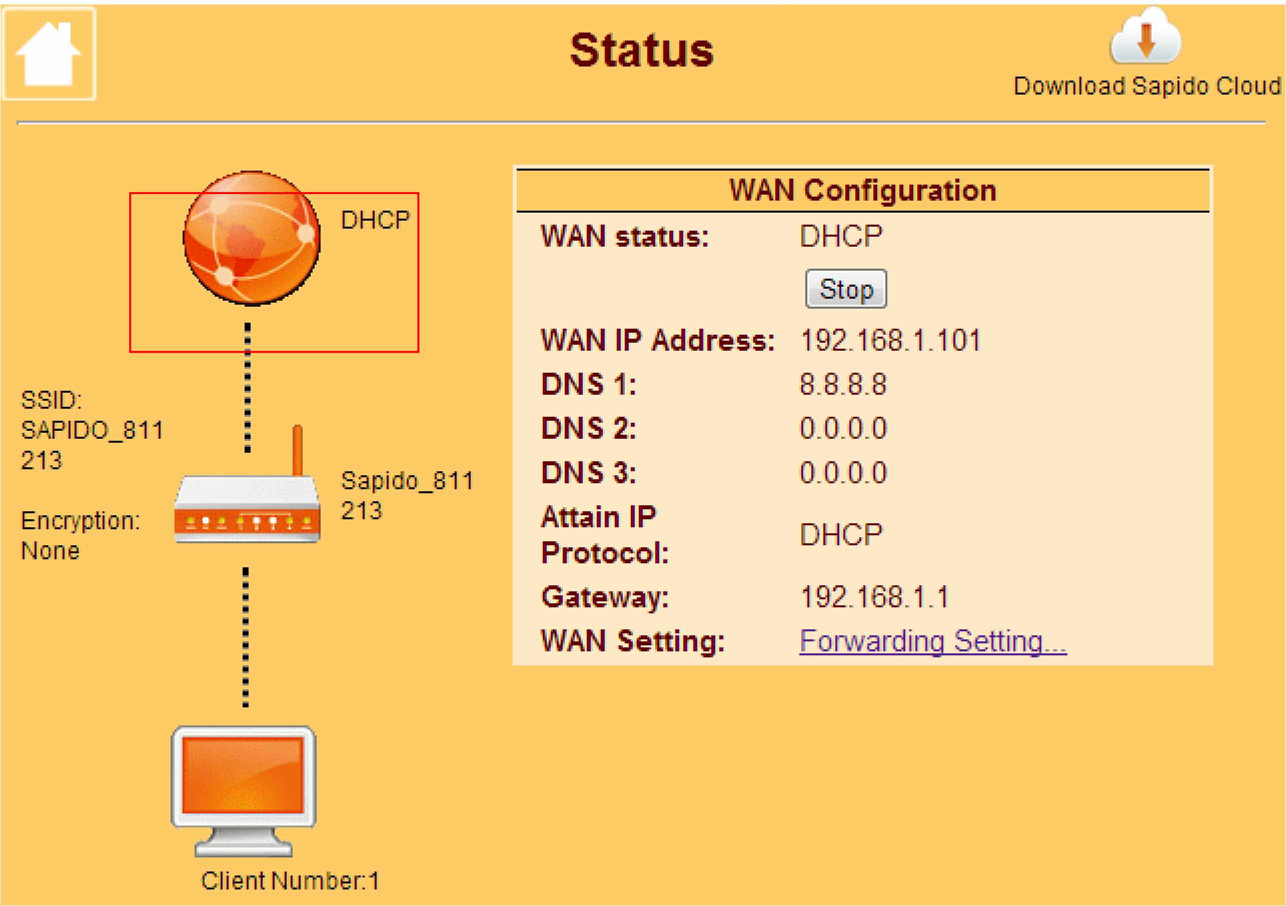
WPA_Pre-Shared Key: •••••••••••

Chapter 4 GUI Function Setup

4.1 Status

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

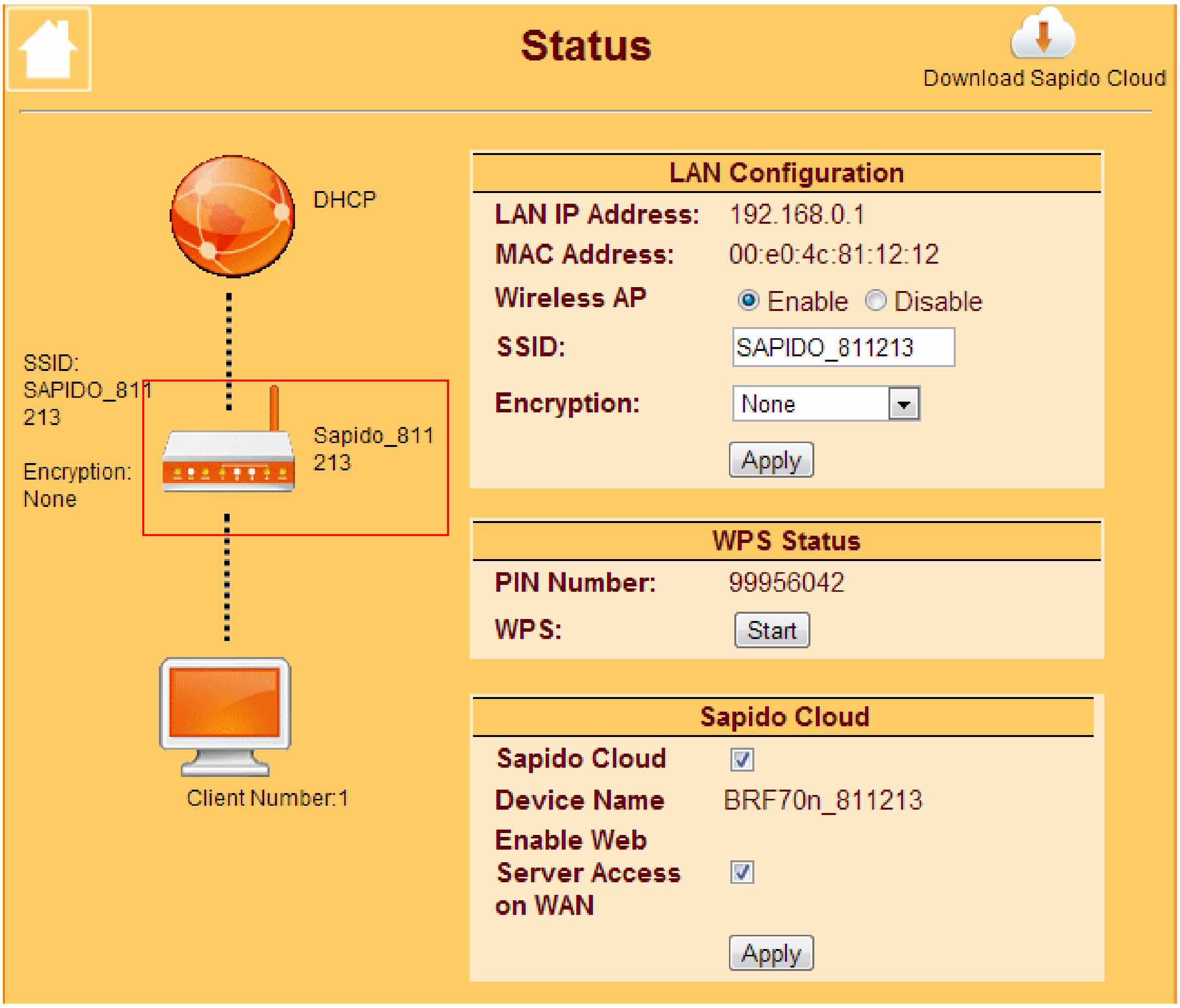
WAN Configuration



WAN Configuration

WAN status:	DHCP
WAN IP Address:	192.168.1.101
DNS 1:	8.8.8.8
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
Attain IP Protocol:	DHCP
Gateway:	192.168.1.1
WAN Setting:	Forwarding Setting...

LAN Configuration



Status

SSID:
SAPIDO_811
213

Encryption:
None

LAN Configuration

LAN IP Address:	192.168.0.1
MAC Address:	00:e0:4c:81:12:12
Wireless AP	● Enable ○ Disable
SSID:	SAPIDO_811213
Encryption:	None

Apply

WPS Status

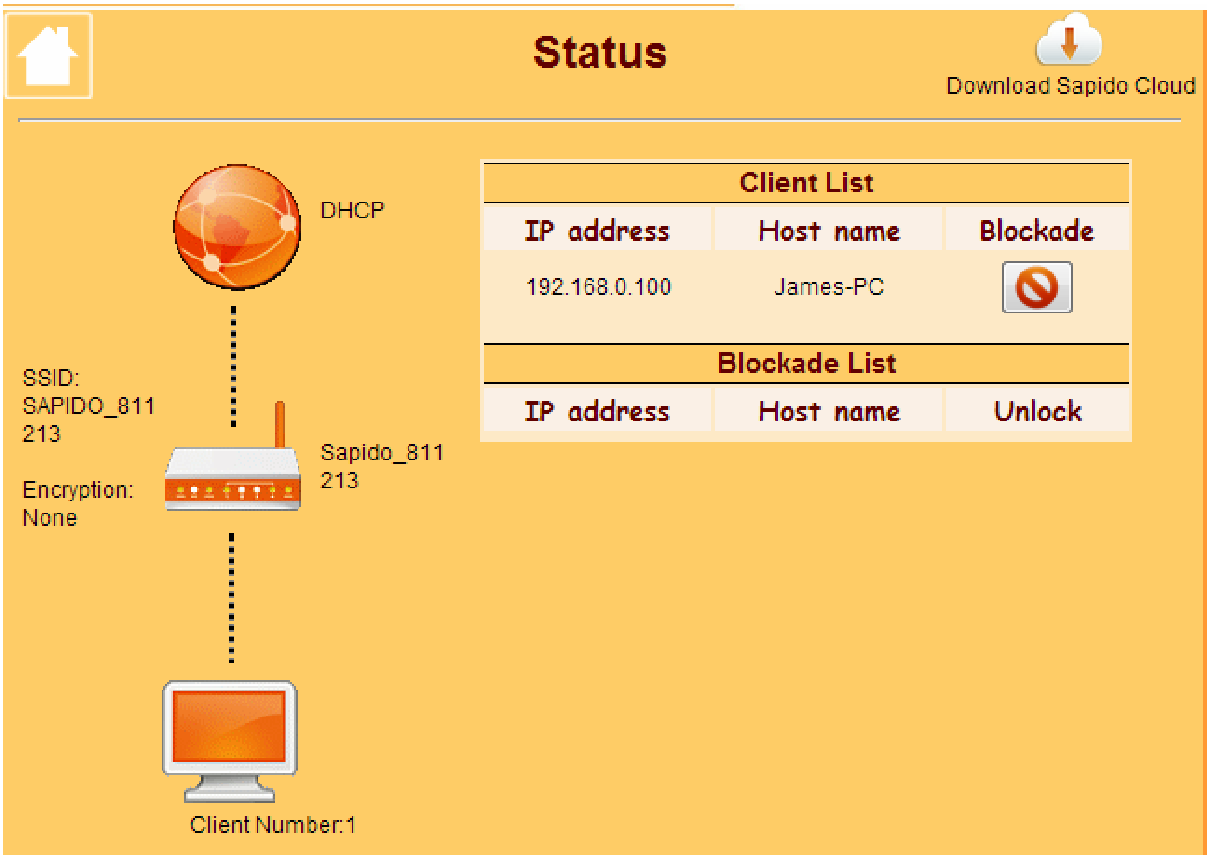
PIN Number:	99956042
WPS:	Start

Sapido Cloud

Sapido Cloud	☑
Device Name	BRF70n_811213
Enable Web Server Access on WAN	☑

Apply

Client Configuration

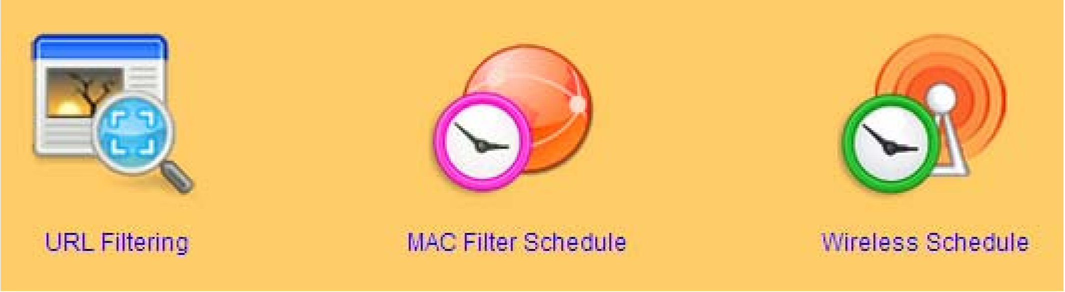


Client List		
IP address	Host name	Blockade
192.168.0.100	James-PC	🚫

Blockade List		
IP address	Host name	Unlock

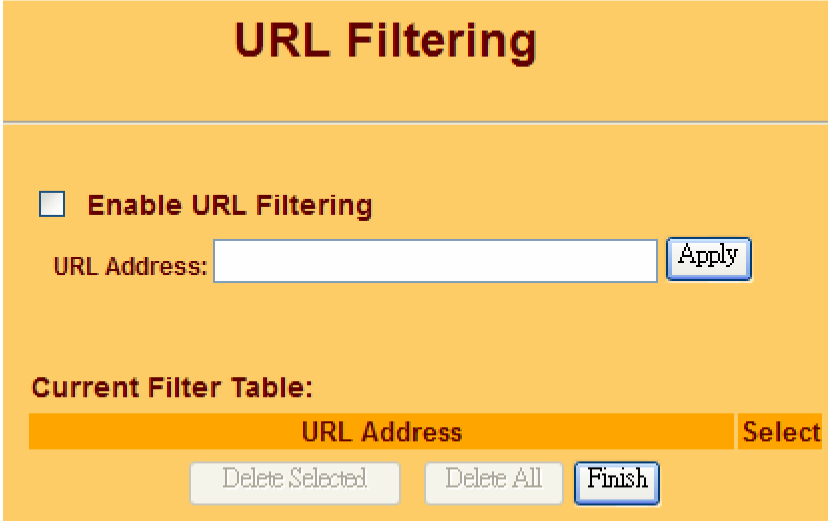
4.2 Parental Control

Parental Control provide URL Filtering and MAC Filter Schedule for setup



4.2.1 URL Filtering

URL Filtering is used to restrict users to access specific websites in internet



URL Filtering

□ Enable URL Filtering

URL Address:

Current Filter Table:

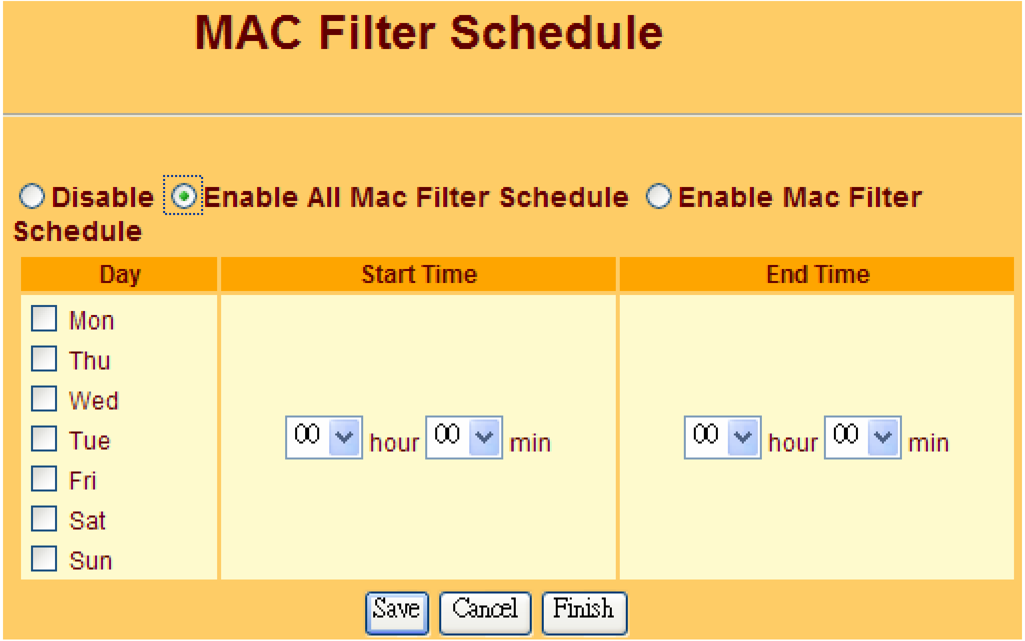
URL Address	Select

Item	Description
Enable URL Filtering	Please select Enable MAC Filtering to filter MAC addresses
URL Address	Please enter the MAC address that needs to be filtered.
Apply	Click on Apply to save the setting data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

Notes: This function will not be in effect when the Virtual Server is enabled. Please disable Virtual Server before activate the URL Filtering function.

4.2.2 MAC Filter Schedule

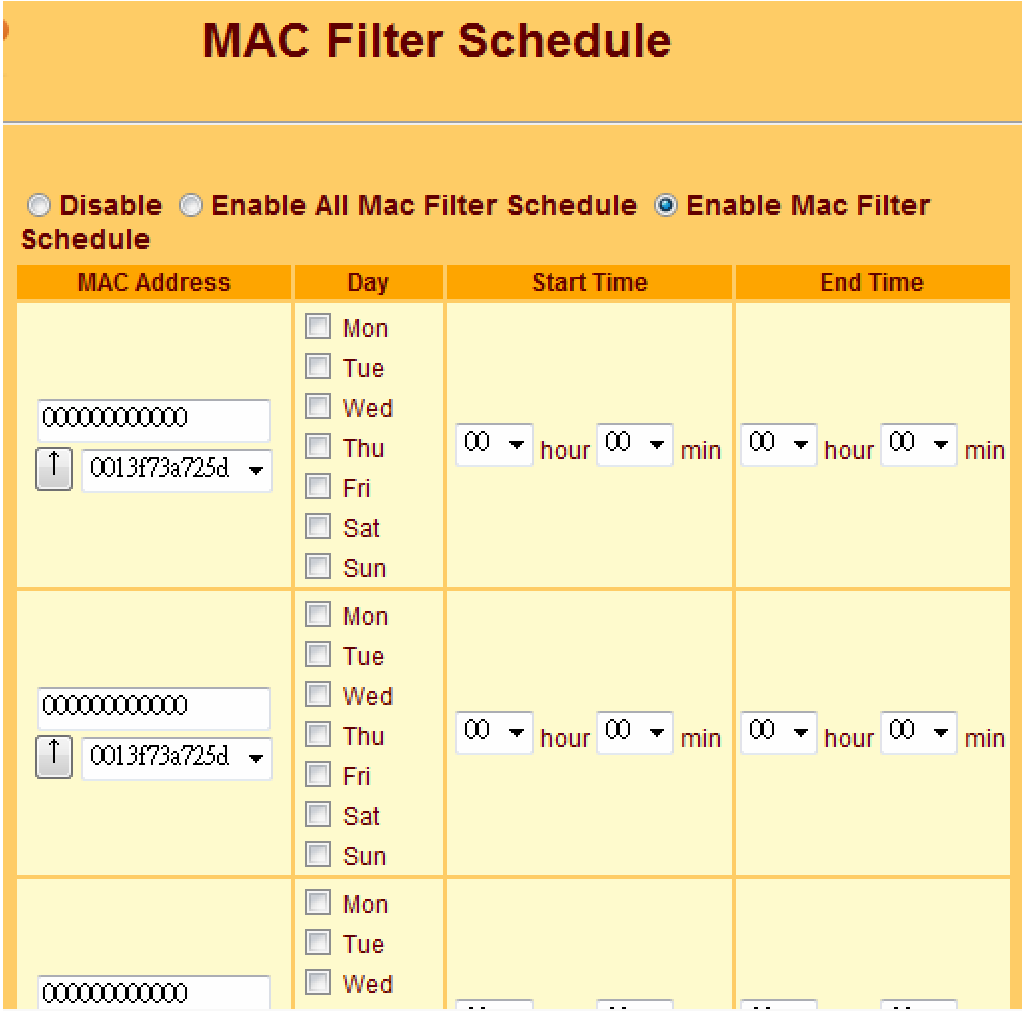
When enabled, filtering will be based on the MAC address of LAN computers. Any computer with its MAC address on this list will be blocked from accessing the Internet.



MAC Filter Schedule

○ Disable ● Enable All Mac Filter Schedule ○ Enable Mac Filter Schedule

Day	Start Time	End Time
□ Mon □ Thu □ Wed □ Tue □ Fri □ Sat □ Sun	00 hour 00 min	00 hour 00 min



MAC Filter Schedule

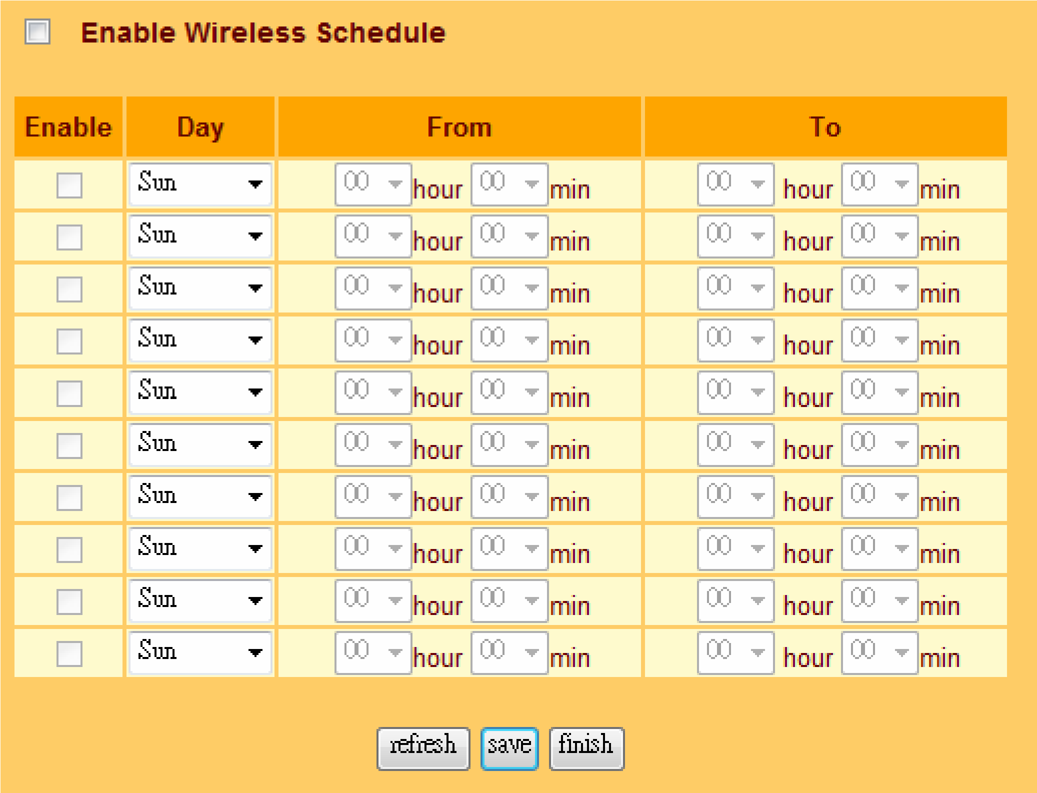
○ Disable ○ Enable All Mac Filter Schedule ● Enable Mac Filter Schedule

MAC Address	Day	Start Time	End Time
000000000000 0013f73a725d	□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun	00 hour 00 min	00 hour 00 min
000000000000 0013f73a725d	□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun	00 hour 00 min	00 hour 00 min
000000000000	□ Mon □ Tue □ Wed		

Item	Description
Enable MAC Filtering	Please select Enable MAC Filtering to filter MAC addresses.

4.2.3 Wireless Schedule

Wireless available schedule, this page allows you setup the wireless schedule rule. Please do not forget to configure systeim before enable this feature

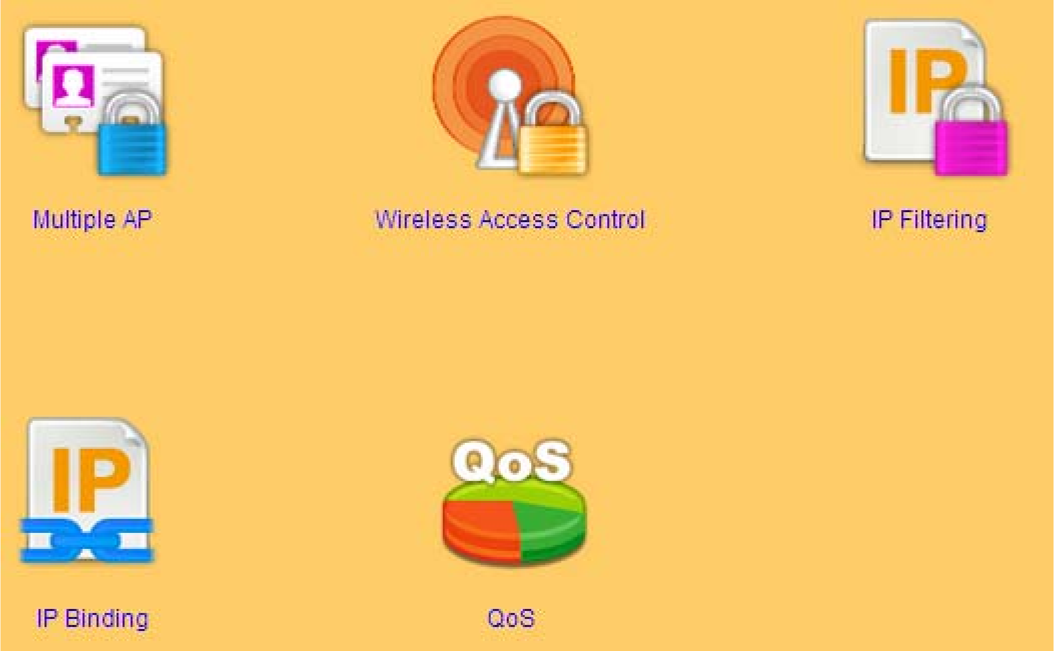


☐ Enable Wireless Schedule

Enable	Day	From	To
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min
☐	Sun	00 hour 00 min	00 hour 00 min

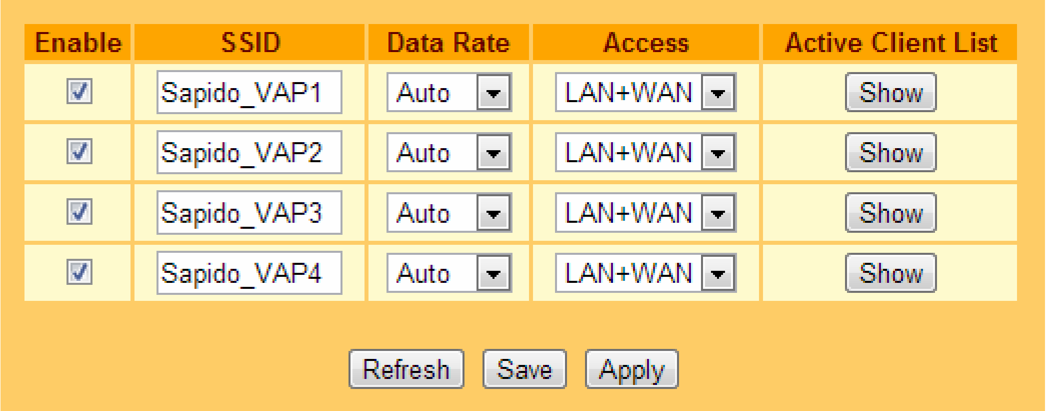
4.3 Office Control

Office control provide Multiple AP、Wireless Access Control、IP Filtering、IP Binding、QoS



4.3.1 Multiple AP

The BRF70n 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.

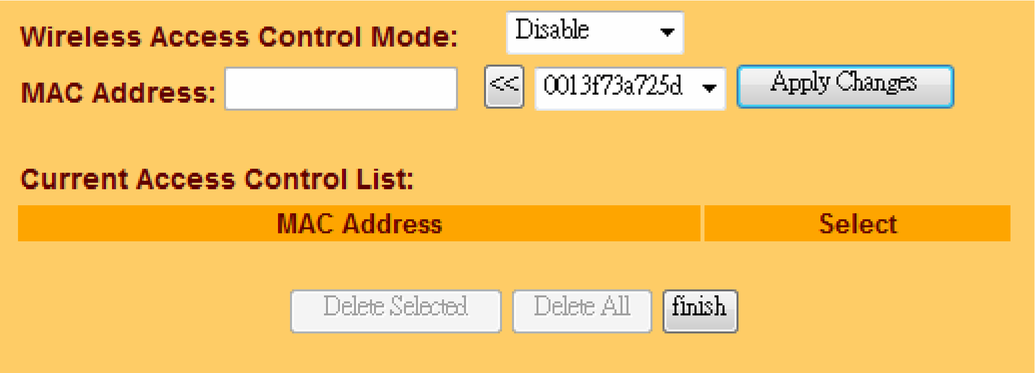


Enable	SSID	Data Rate	Access	Active Client List
☑	Sapido_VAP1	Auto	LAN+WAN	Show
☑	Sapido_VAP2	Auto	LAN+WAN	Show
☑	Sapido_VAP3	Auto	LAN+WAN	Show
☑	Sapido_VAP4	Auto	LAN+WAN	Show

Item	Description
Enable	Enable or disable the service.
SSID	Enter the SSID
Data Rate	Select the data transmission rate.
Access	Enable this function can let clients use two access types: a. LAN+WAN: the client can access to the Internet and access in the router's GUI. b. WAN: the client can only access to the Internet.
Active Client List	Display the properties of the client which is connecting successfully.

4.3.2 Wireless 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.



Wireless Access Control Mode: Disable

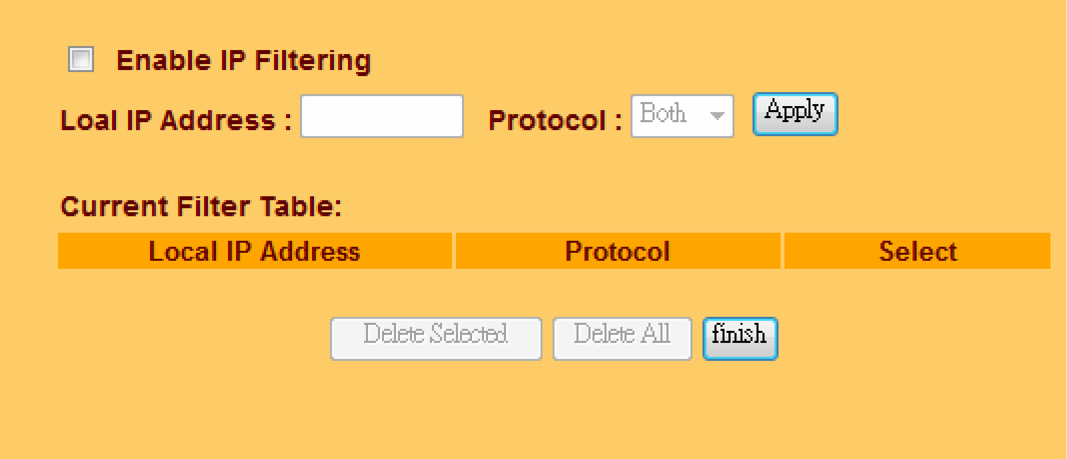
MAC Address: 0013f73a725d

Current Access Control List:

MAC Address	Select

4.3.3 IP Filtering

When enabled, LAN clients are blocked / filtered from accessing the Internet based on their IP addresses



□ Enable IP Filtering

Loal IP Address :

Protocol : Both

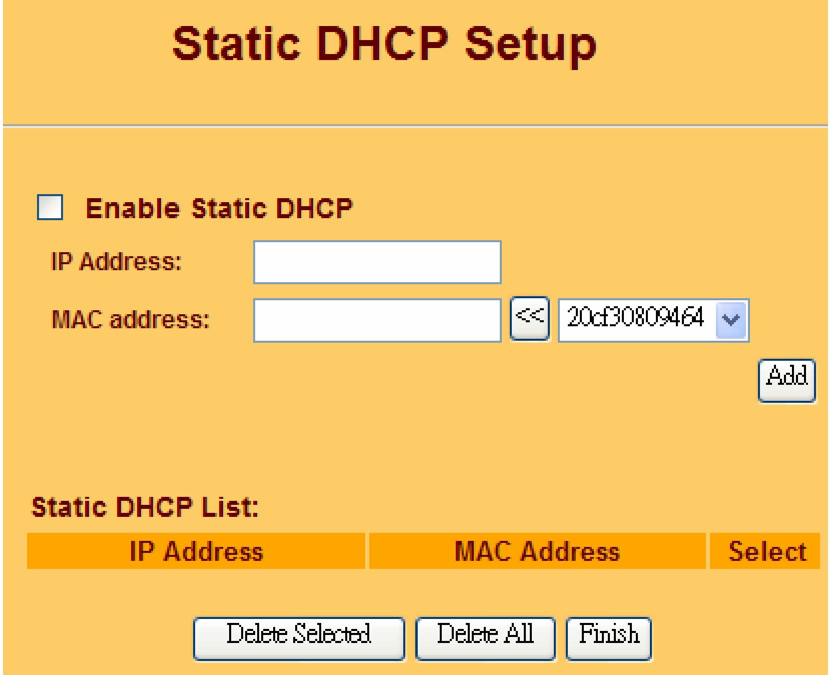
Current Filter Table:

Local IP Address	Protocol	Select

Item	Description
Enable IP Filtering	Please select Enable IP Filtering to filter IP addresses.
Local IP Address	Please enter the IP address that needs to be filtered.
Protocol	Please select the protocol type of the IP address
Apply	Click on **Apply** to add the setting data
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

4.3.4 IP Binding

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.

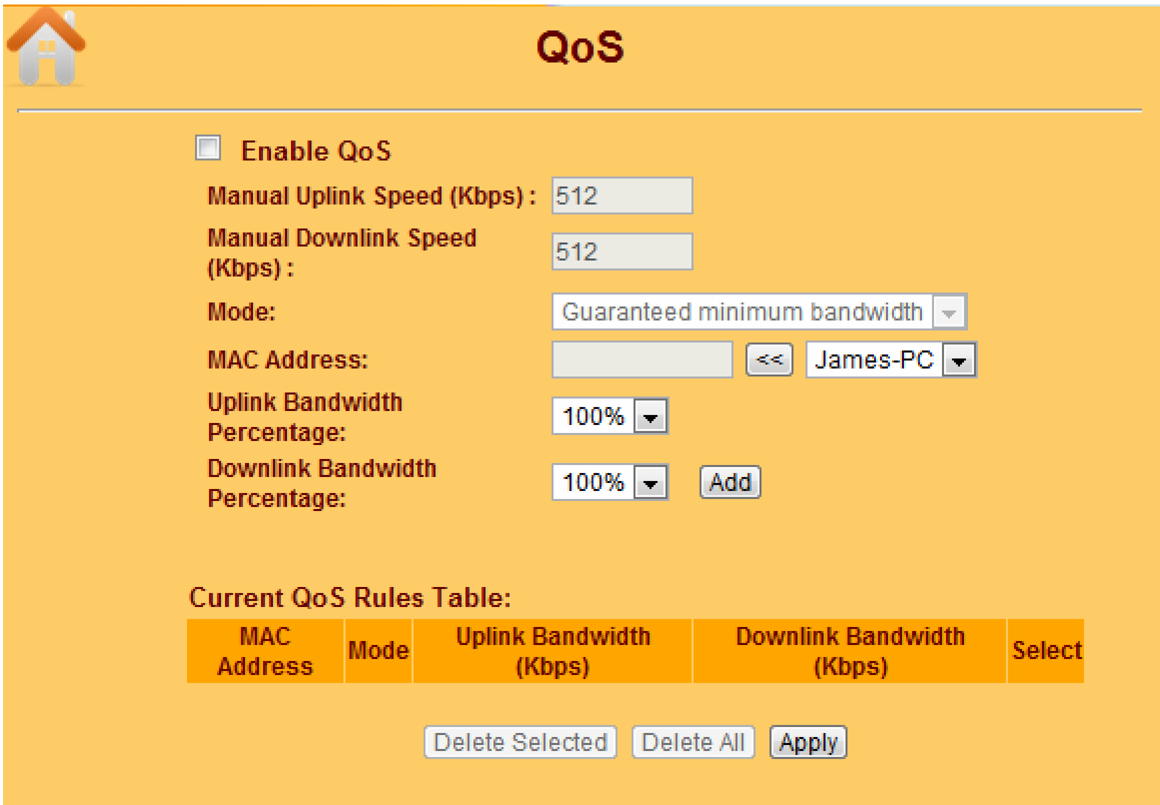


Item	Description
Enable Static DHCP	Select enable to use Static DHCP function
IP Address	Please enter IP address to limit
MAC address	Please enter MAC address to limit
Static DHCP List	**It will display all IP and MAC address you made.**
Delete Selected & Delete All	Click **Delete Selected** will delete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

4.3.5 QoS

The QoS can let you classify Internet application traffic by source/destination IP address and port number.

To assign priority for each type of application and reserve bandwidth can let you have a better experience in using critical real time services like Internet phone, video conference …etc.



QoS

□ Enable QoS

Manual Uplink Speed (Kbps) : 512

Manual Downlink Speed (Kbps) : 512

Mode: Guaranteed minimum bandwidth

MAC Address: James-PC

Uplink Bandwidth Percentage: 100%

Downlink Bandwidth Percentage: 100%

Current QoS Rules Table:

MAC Address	Mode	Uplink Bandwidth (Kbps)	Downlink Bandwidth (Kbps)	Select

Item	Description
Enable QoS	Check “Enable QoS” to enable QoS function for the WAN port. You also can uncheck “Enable QoS” to disable QoS function for the WAN port.
Manual Uplink Speed	Set the uplink speed by manual to assign the download or upload bandwidth by the unit of Kbps.
Manual Downlink Speed	Set the downlink speed by manual to assign the download or upload bandwidth by the unit of Kbps.
Mode	Select Guaranteed minimum bandwidth or Restricted maximum bandwidth
MAC Address	Set MAC Address if the address type is by MAC Address
Uplink Bandwidth Percentage	LAN device bandwidth of uplink bandwidth
Download Bandwidth Percentage	LAN device bandwidth of download bandwidth
Add	Add the setting data
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

4.4 Firmware Upgrade

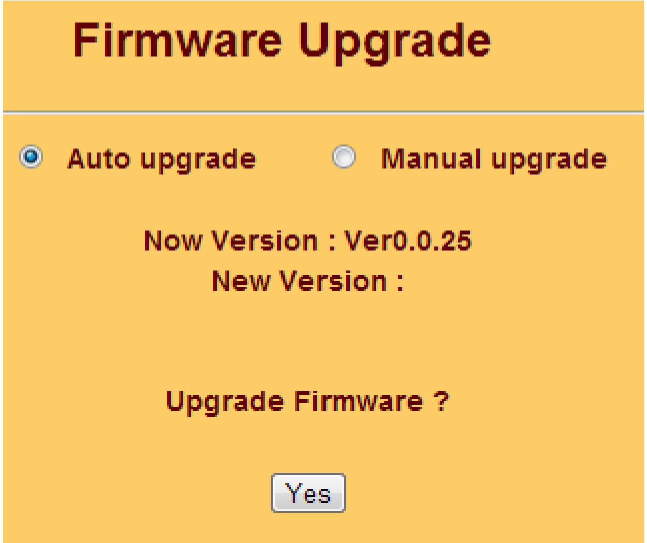
This function can upgrade the firmware of the router. There are two methods for user upgrade firmware: Auto upgrade and Manual upgrade.

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.

4.4.1 Auto upgrade

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



Firmware Upgrade

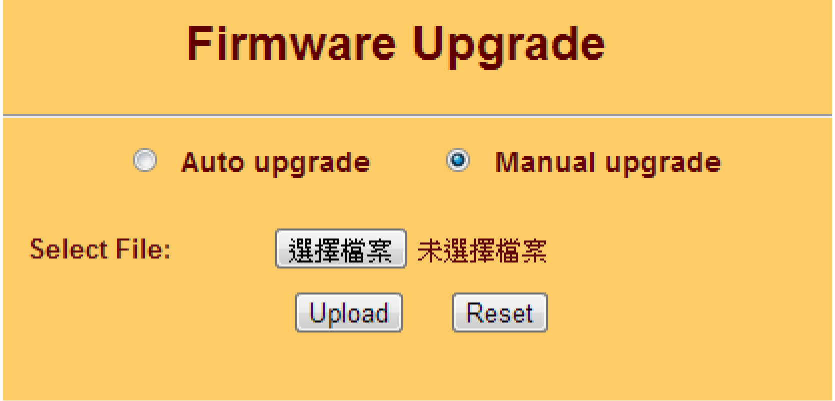
● Auto upgrade ○ Manual upgrade

Now Version : Ver0.0.25
New Version :

Upgrade Firmware ?

4.4.2 Manual upgrade

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



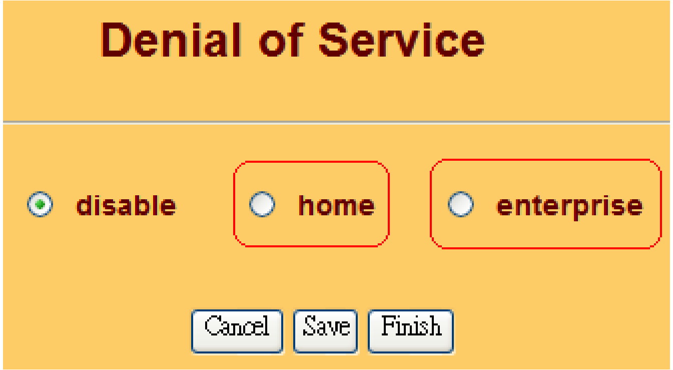
Firmware Upgrade

○ Auto upgrade ● Manual upgrade

Select File: 選擇檔案 未選擇檔案

4.5 DoS

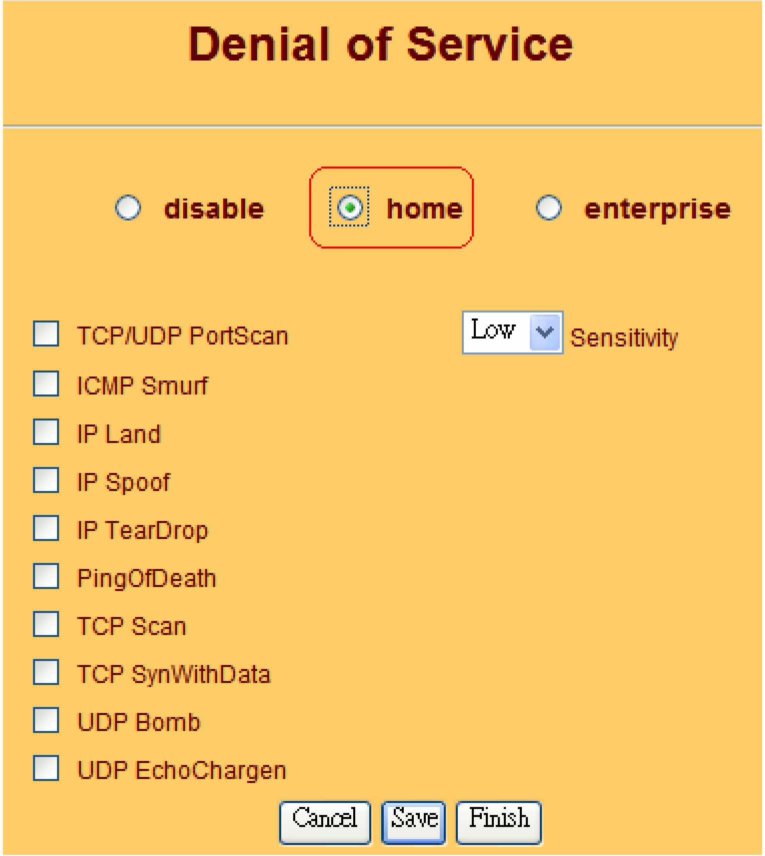
It provide 2 kind of Denial of Service: Home and Enterprise



Denial of Service

● disable ○ home ○ enterprise

Home:



Denial of Service

○ disable ● home ○ enterprise

□ TCP/UDP PortScan Low Sensitivity

□ ICMP Smurf

□ IP Land

□ IP Spoof

□ IP TearDrop

□ PingOfDeath

□ TCP Scan

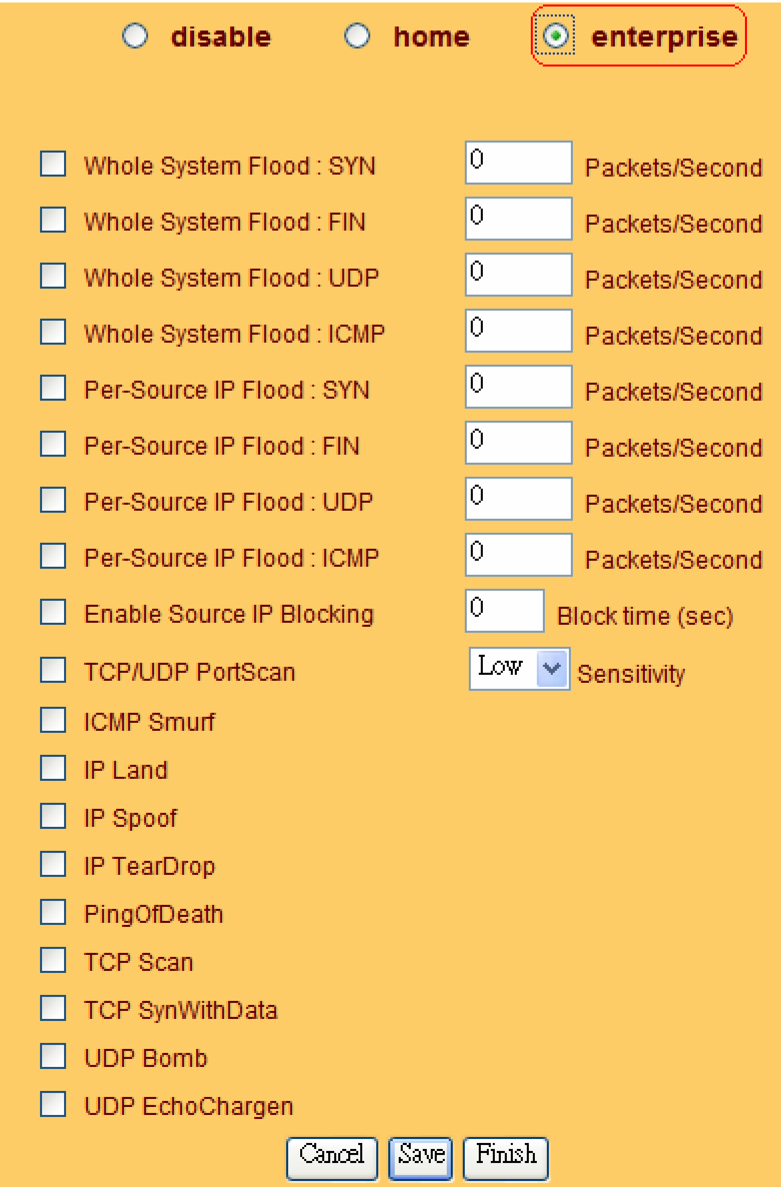
□ TCP SynWithData

□ UDP Bomb

□ UDP EchoChargen

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

Enterprise:



○ disable ○ home ● enterprise

☐ Whole System Flood : SYN 0 Packets/Second

☐ Whole System Flood : FIN 0 Packets/Second

☐ Whole System Flood : UDP 0 Packets/Second

☐ Whole System Flood : ICMP 0 Packets/Second

☐ Per-Source IP Flood : SYN 0 Packets/Second

☐ Per-Source IP Flood : FIN 0 Packets/Second

☐ Per-Source IP Flood : UDP 0 Packets/Second

☐ Per-Source IP Flood : ICMP 0 Packets/Second

☐ Enable Source IP Blocking 0 Block time (sec)

☐ TCP/UDP PortScan Low Sensitivity

☐ ICMP Smurf

☐ IP Land

☐ IP Spoof

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

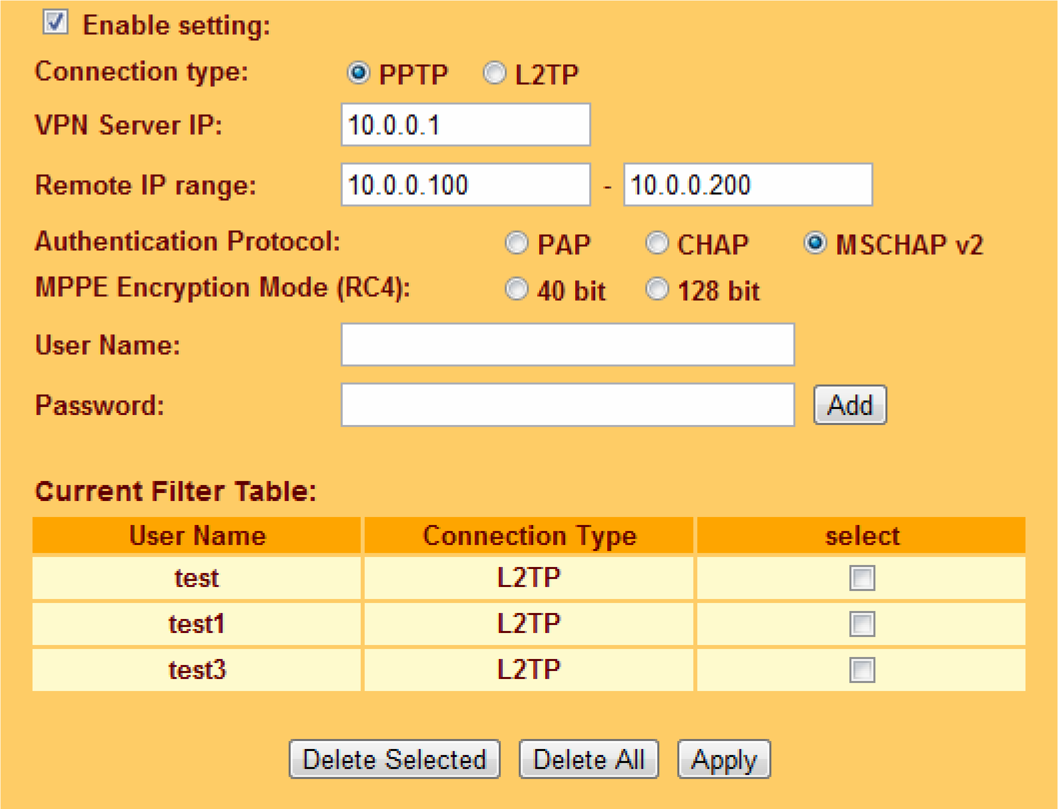
☐ UDP Bomb

☐ UDP EchoChargen

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

4.6 VPN Server

The VPN Server function providing PPTP/L2TP mode are designed to allow users to an external network device / computer and office local area network to establish a secure network connection. And User can safe login office local area network and access to personal documents, files Sharing and other resources. It provides the most convenient VPN encryption.



☑ Enable setting:

Connection type: ● PPTP ○ L2TP

VPN Server IP: 10.0.0.1

Remote IP range: 10.0.0.100 - 10.0.0.200

Authentication Protocol: ○ PAP ○ CHAP ● MSCHAP v2

MPPE Encryption Mode (RC4): ○ 40 bit ○ 128 bit

User Name:

Password:

Current Filter Table:

User Name	Connection Type	select
test	L2TP	□
test1	L2TP	□
test3	L2TP	□

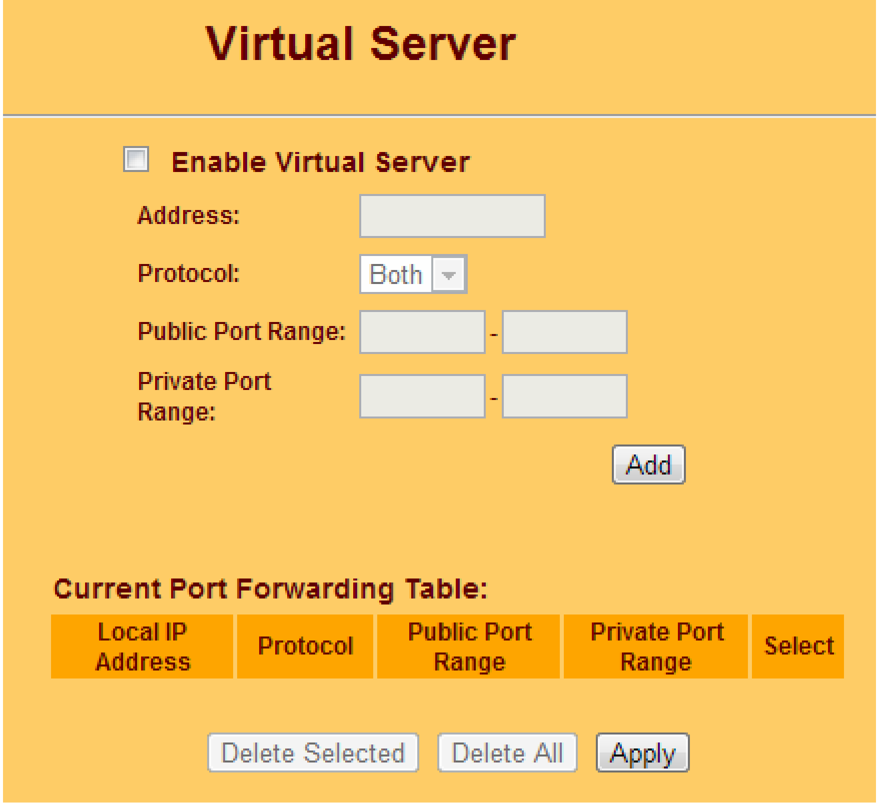
Item	Description
Enable Setting	Check this option, will start the VPN Server feature.
Connection Type	Provide PPTP or L2TP access connection type.
VPN Server IP	Input the IP address of VPN server
Remote IP range	It is the IP range of assigned to the VPN Client
Authentication Protocol	It is provided three types of authentication protocol
MPPE Encryption Mode (RC4)	It is provided three encryption modes
User Name	Input the login name of the client user
Password	Input the login password of the client user
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

4.7 NAT Management

This section contains configurations for the BRF70N 's advanced functions such as: virtual server, and DMZ to provide your network under a security environment.

4.7.1 Virtual Server

The Virtual Server feature allows users to create Virtual Servers by re-directing a particular range of service port numbers (from the WAN port) to a particular LAN IP address.



Virtual Server

□ Enable Virtual Server

Address:	
Protocol:	Both
Public Port Range:	-
Private Port Range:	-

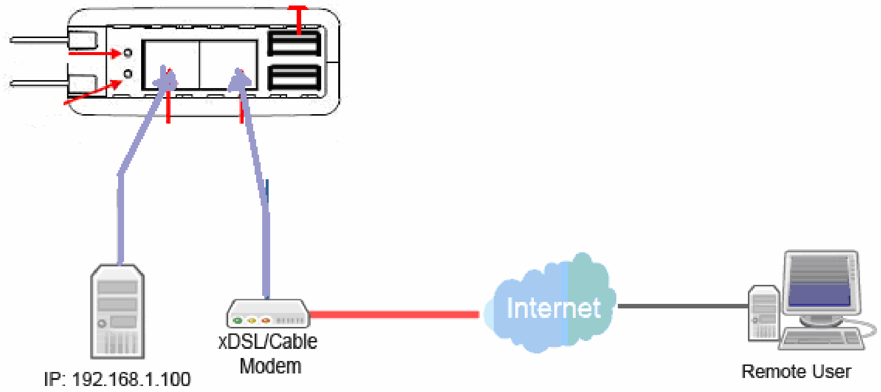
Current Port Forwarding Table:

Local IP Address	Protocol	Public Port Range	Private Port Range	Select

Item	**Description**
Enable Port Forwarding	Select to enable Port Forwarding service or not.
Address	Specify the IP address which receives the incoming packets.
Protocol	Select the protocol type.
Public Port Range	Enter the port number, for example 80-80.
Private Port Range	Enter the port number, for example 20-22.
Current Port Forwarding Table	**It will display all port forwarding regulation you made.**

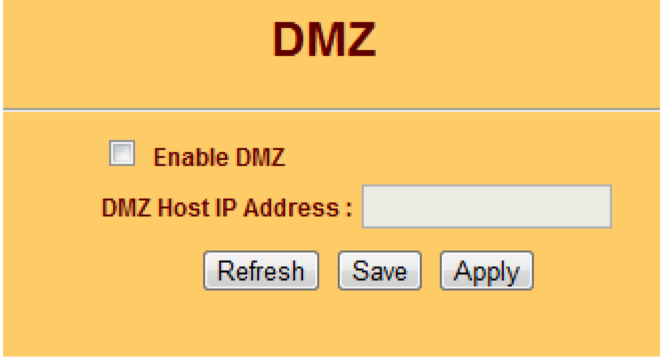
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

Please find the following figure to know that what the virtual server is. The web server is located on 192.168.1.100, forwarding port is 80, and type is TCP+UDP.



4.7.2 DMZ

The DMZ feature allows one local user to be exposed to the Internet for special-purpose applications like Internet gaming or videoconferencing. When enabled, this feature opens all ports to a single station and hence renders that system exposed to intrusion from outside. The port forwarding feature is more secure because it only opens the ports required by that application.



DMZ

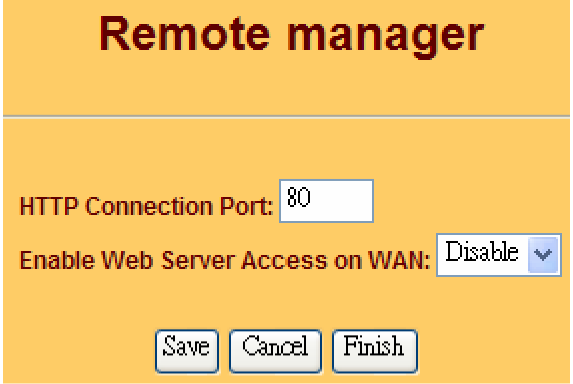
□ Enable DMZ

DMZ Host IP Address :

Item	Description
Enable DMZ	It will enable the DMZ service if you select it.
DMZ Host IP Address	Please enter the specific IP address for DMZ host.

4.8 Remote Management

This page allows you to access the GUI on WAN.



Remote manager

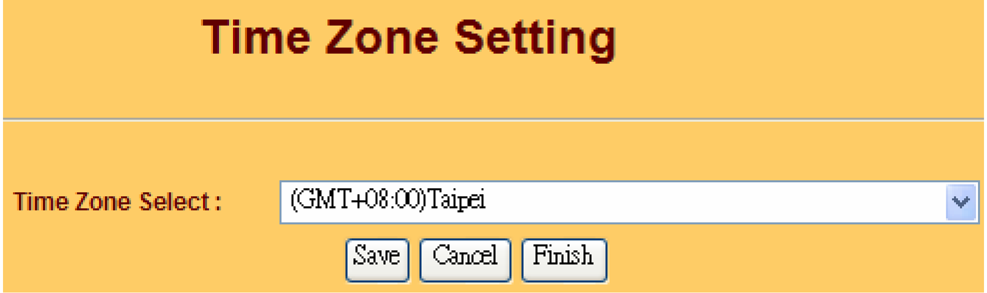
HTTP Connection Port: 80

Enable Web Server Access on WAN: Disable

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

4.9 Time Zone

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



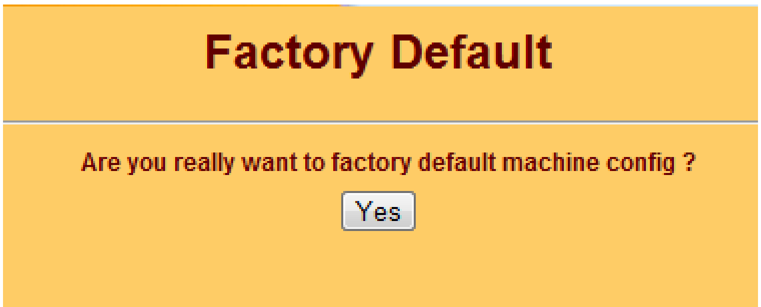
Time Zone Setting

Time Zone Select : (GMT+08:00)Taipei

Item	Description
Time Zone Select	Please select the time zone.

4.10 Factory Default

You could reset the current configuration to factory default.

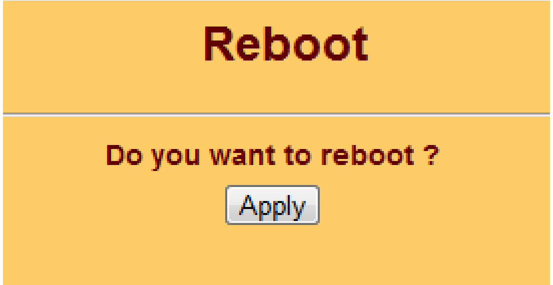


Factory Default

Are you really want to factory default machine config ?

4.11 Reboot

This function is used to reboot

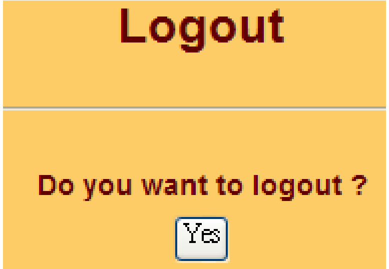


Reboot

Do you want to reboot ?

4.12 Logout

This page is used to logout



Logout

Do you want to logout ?

Chapter 5 Advance Setup

5.1 Internet Mode

5.1.1 Internet Setup

Please refer Internet Setup

5.1.2 AP

Please refer AP

5.1.3 WiFi AP

Please refer WiFi AP

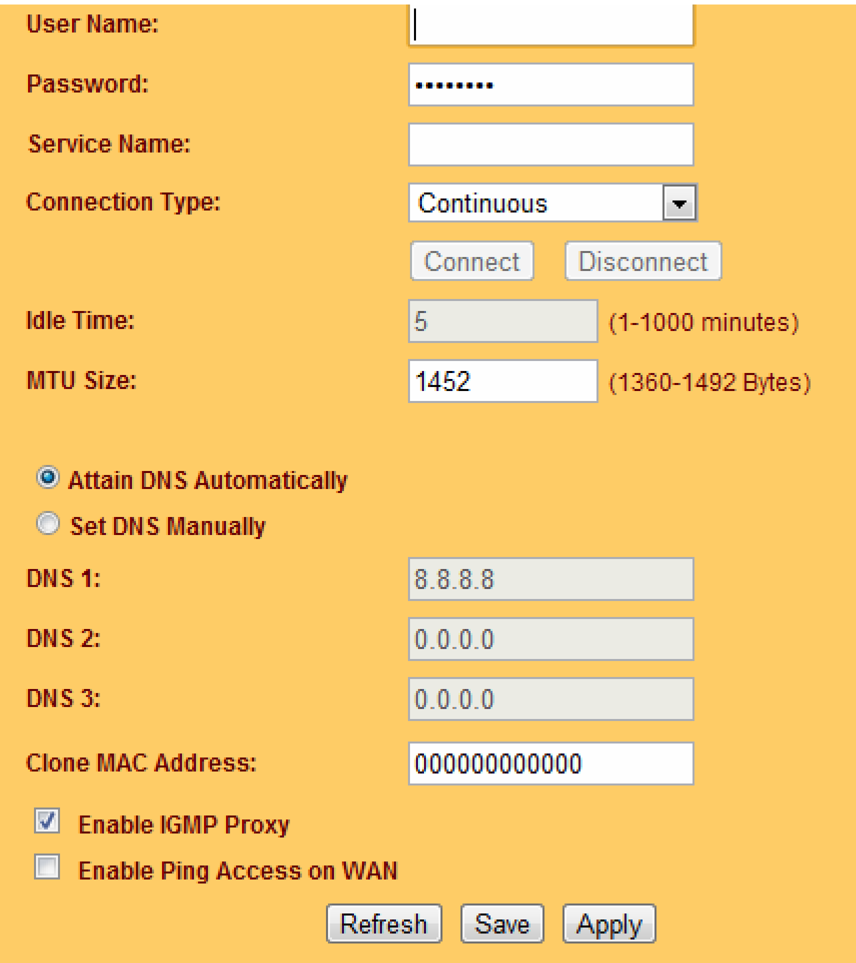
5.1.4 WiFi ISP

Please refer WiFi ISP

5.2 IP Config

5.2.1 WAN

5.2.1.1 PPPoE



User Name:

Password: ••••••••

Service Name:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1452 (1360-1492 Bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 8.8.8.8

DNS 2: 0.0.0.0

DNS 3: 0.0.0.0

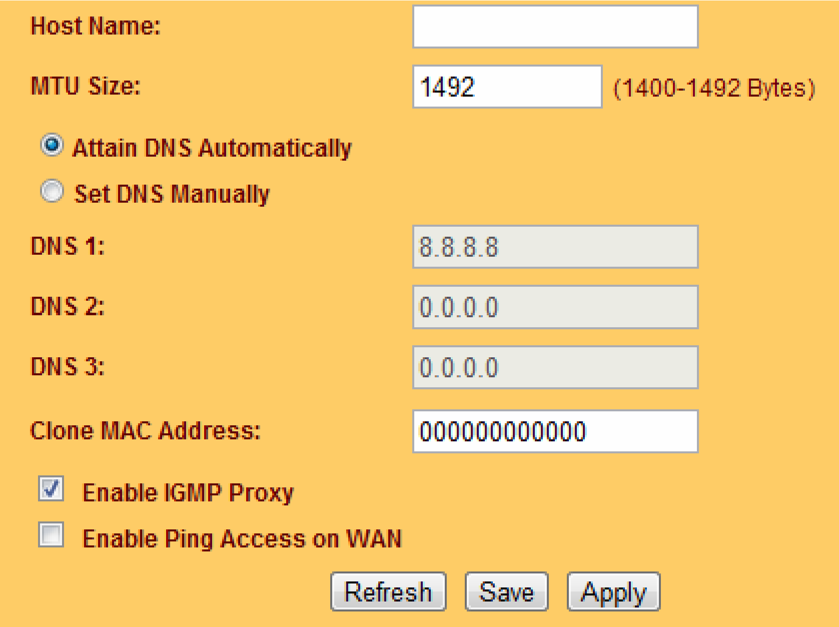
Clone MAC Address: 000000000000

☑ Enable IGMP Proxy

□ Enable Ping Access on WAN

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.

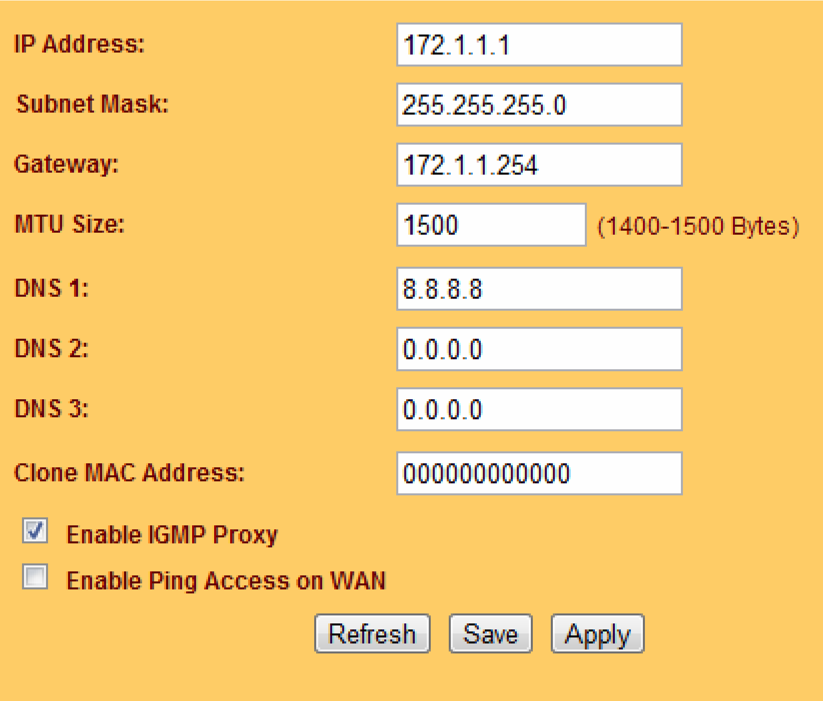
5.2.1.2 DHCP



Host Name:	
MTU Size:	1492 (1400-1492 Bytes)
● Attain DNS Automatically	
○ Set DNS Manually	
DNS 1:	8.8.8.8
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
Clone MAC Address:	000000000000
☑ Enable IGMP Proxy	
□ Enable Ping Access on WAN	

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.

5.2.1.3 Static IP



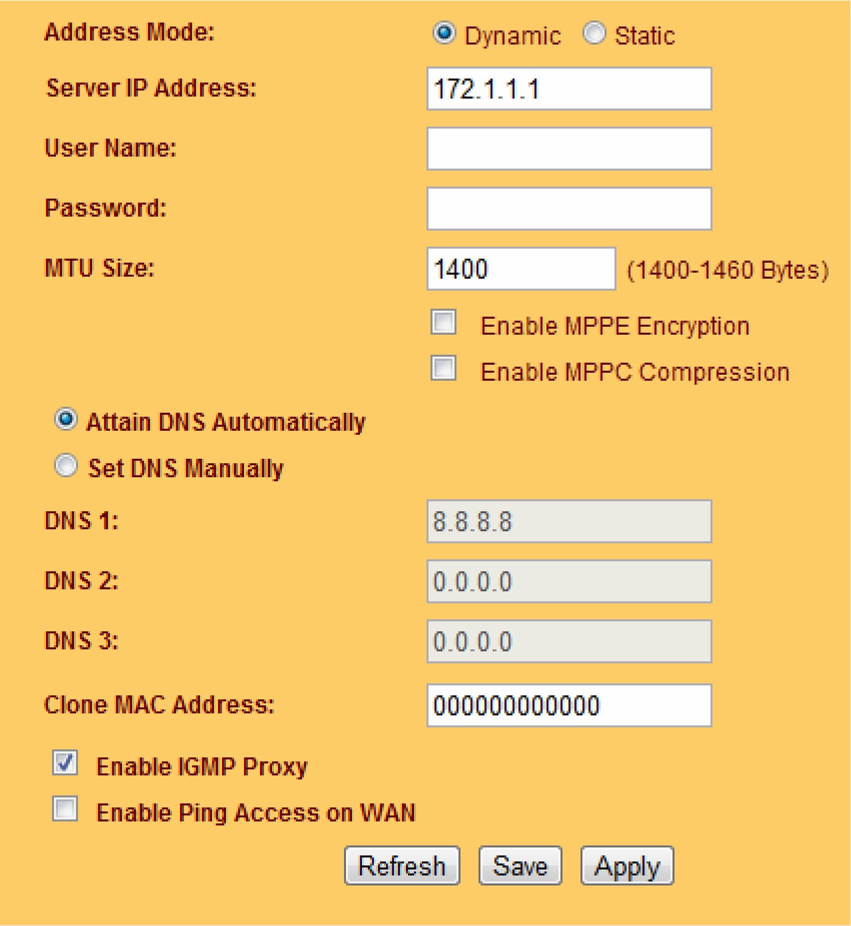
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Gateway:	172.1.1.254
MTU Size:	1500 (1400-1500 Bytes)
DNS 1:	8.8.8.8
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
Clone MAC Address:	000000000000

☑ Enable IGMP Proxy

☐ Enable Ping Access on WAN

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.

5.2.1.4 PPTP



Address Mode: ● Dynamic ○ Static

Server IP Address: 172.1.1.1

User Name:

Password:

MTU Size: 1400 (1400-1460 Bytes)

□ Enable MPPE Encryption

□ Enable MPPC Compression

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 8.8.8.8

DNS 2: 0.0.0.0

DNS 3: 0.0.0.0

Clone MAC Address: 000000000000

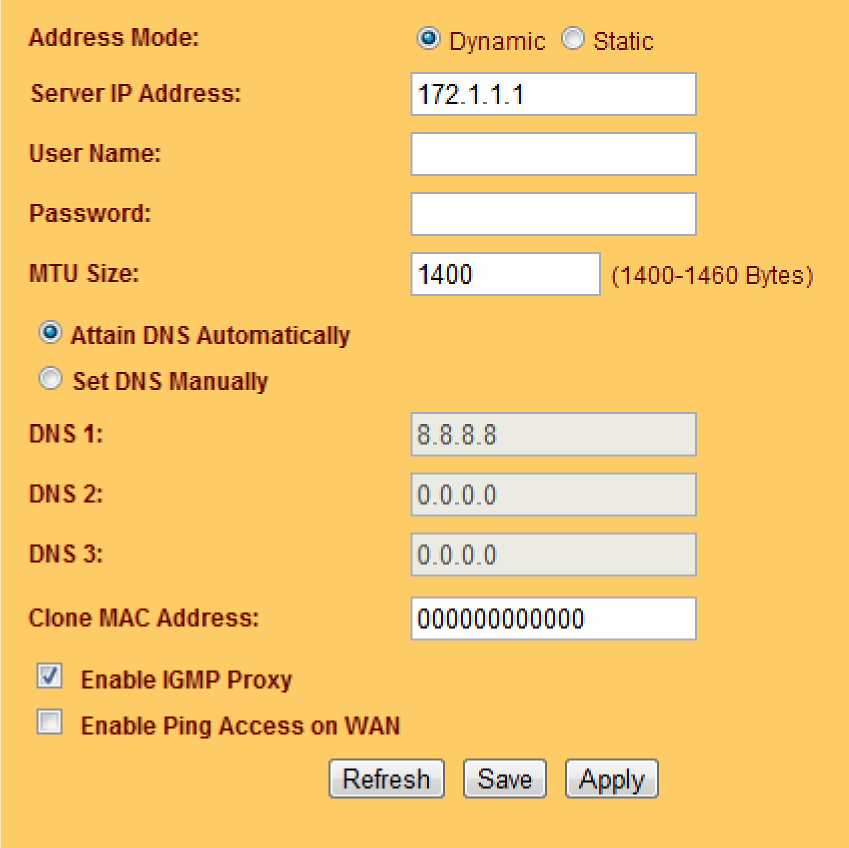
☑ Enable IGMP Proxy

□ Enable Ping Access on WAN

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.

5.2.1.5 L2TP



Address Mode:	● Dynamic ○ Static
Server IP Address:	172.1.1.1
User Name:	
Password:	
MTU Size:	1400 (1400-1460 Bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:	8.8.8.8
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
Clone MAC Address:	000000000000

☑ Enable IGMP Proxy

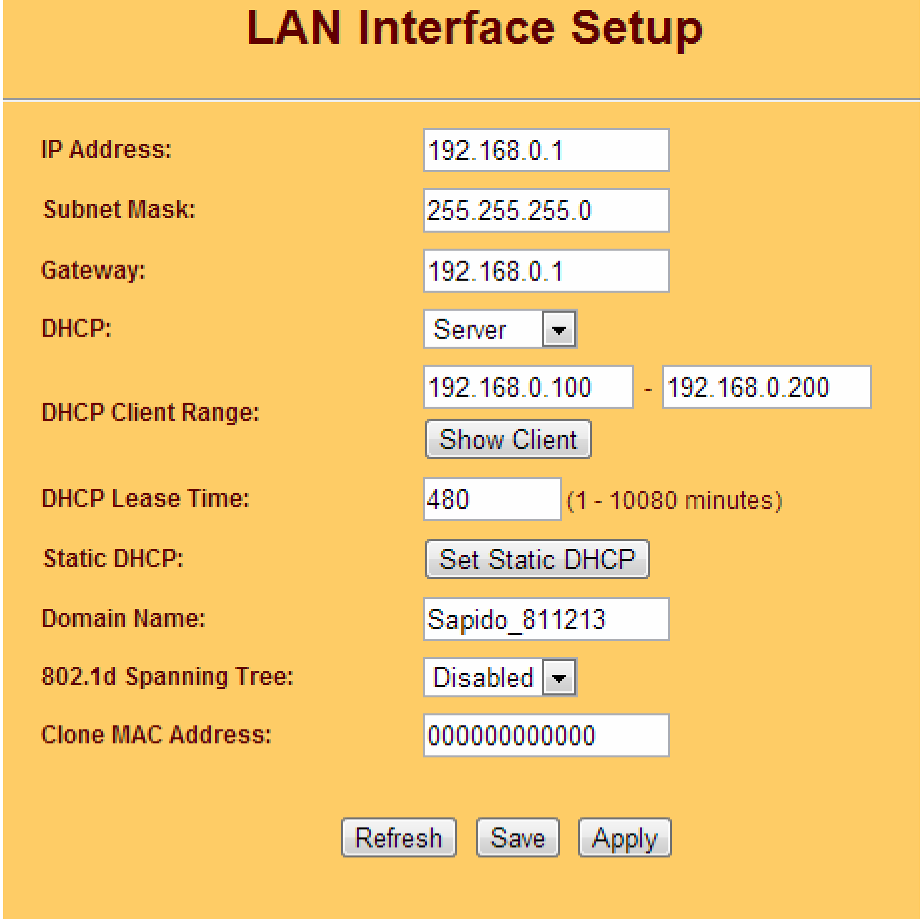
□ Enable Ping Access on WAN

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.

5.2.2 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.



LAN Interface Setup

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

DHCP: Server

DHCP Client Range: 192.168.0.100 - 192.168.0.200

DHCP Lease Time: 480 (1 - 10080 minutes)

Static DHCP:

Domain Name: Sapido_811213

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

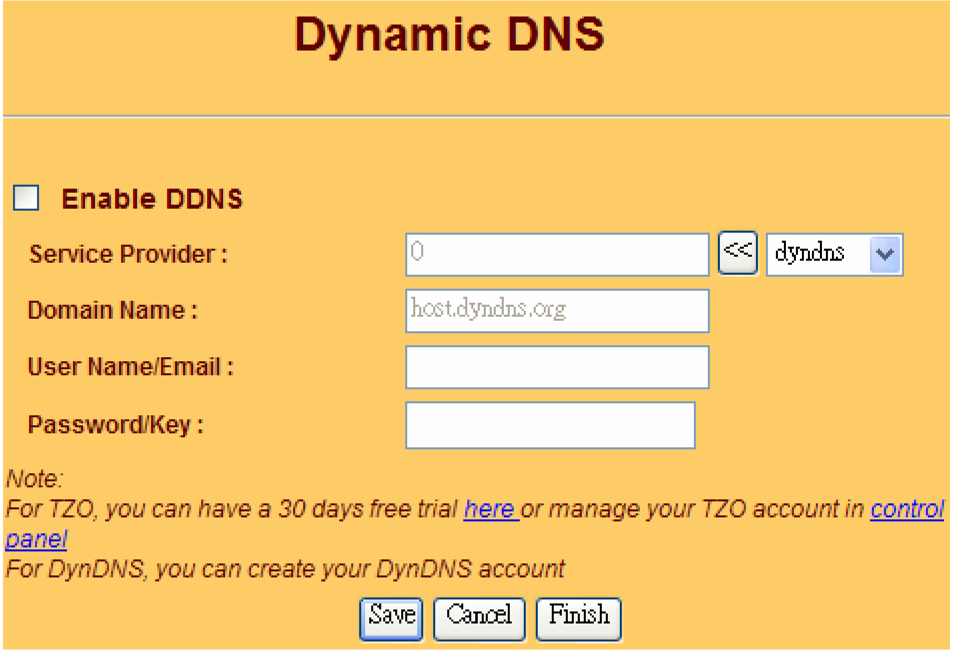
Item	Description
IP Address	The default value of LAN IP address is **192.168.1.1** for this router.
Subnet Mask	Input Subnet Mask, normally it is 255.255.255.0.
Gateway	Input ISP Default Gateway Address. If you don’t know, please check with your ISP.
DHCP	Enable or disable DHCP services. The DHCP server 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
Static DHCP	Please refer IP Binding
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.

5.2.3 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.



Dynamic DNS

□ Enable DDNS

Service Provider : 0 << dyndns

Domain Name : host.dyndns.org

User Name/Email :

Password/Key :

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account

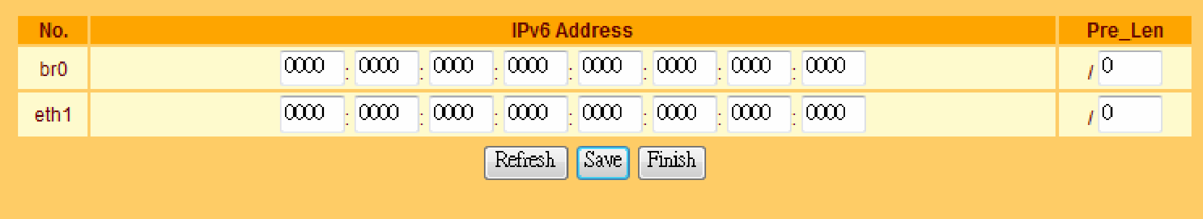
Please enter Domain Name, User Name/Email, and Password/Key. After entering, click on Apply Changes to save the setting, or you may click on Reset to clear all the input data.

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 BRF70N .
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

5.3 IPv6 Config

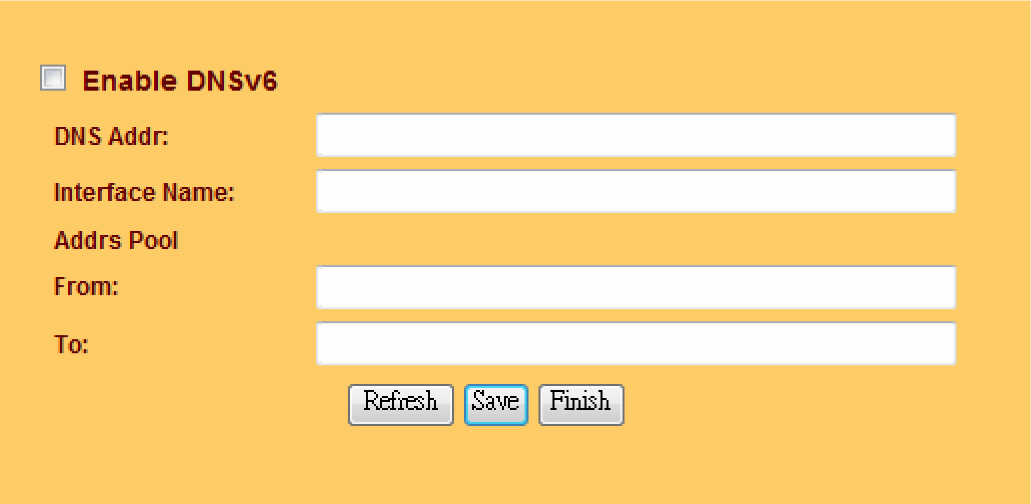
5.3.1 IPv6 basic



No.	IPv6 Address	Pre_Len
br0	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000	/ 0
eth1	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000	/ 0

Item	Description
Br0	LAN IPv6 address
Eth1	WAN IPv6 address

5.3.2 IPv6 dhcp



□ Enable DNSv6

DNS Addr:

Interface Name:

Addrs Pool

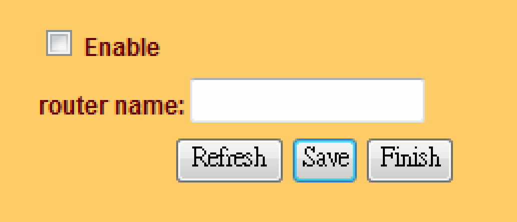
From:

To:

Item	Description
DNS Addr	DNS server IPv6 address
Interface Name	Which Ethernet interface provide IPv6 DHCP service

Addrs Pool From / To	IPv6 DHCP service range

5.3.3 IPv6 dns

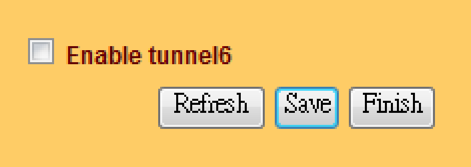


□ Enable

router name:

Item	**Description**
router name	IPv6 DNS server name

5.3.4 IPv6 tunnel

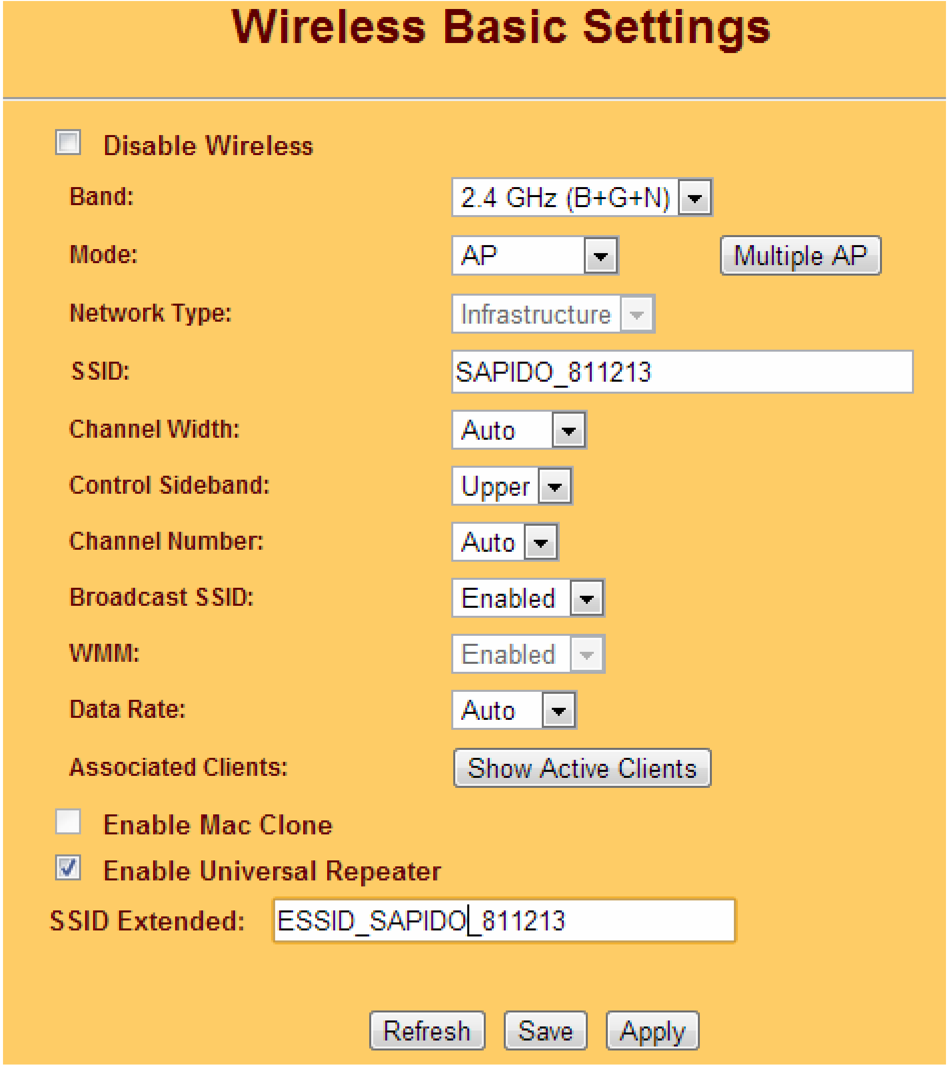


□ Enable tunnel6

5.4 Wireless

5.4.1 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



Wireless Basic Settings

☐ Disable Wireless

Band: 2.4 GHz (B+G+N)

Mode: AP [Multiple AP]

Network Type: Infrastructure

SSID: SAPIDO_811213

Channel Width: Auto

Control Sideband: Upper

Channel Number: Auto

Broadcast SSID: Enabled

WMM: Enabled

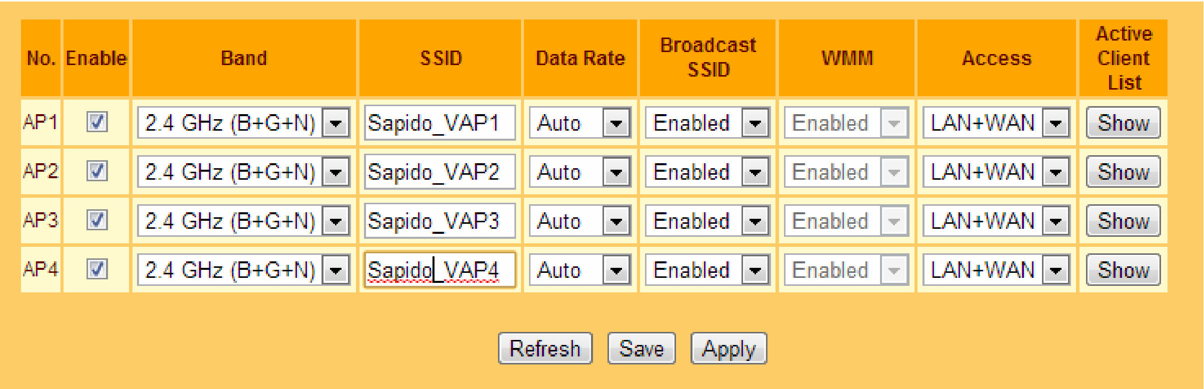
Data Rate: Auto

Associated Clients: [Show Active Clients]

☐ Enable Mac Clone

☑ Enable Universal Repeater

SSID Extended: ESSID_SAPIDO_811213

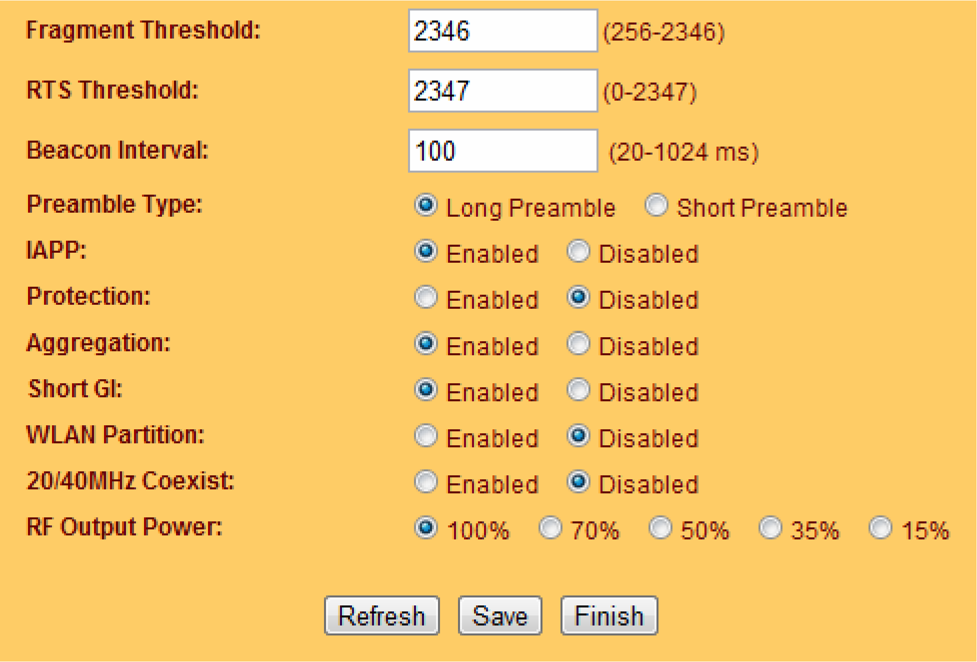


No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List
AP1	☑	2.4 GHz (B+G+N)	Sapido_VAP1	Auto	Enabled	Enabled	LAN+WAN	Show
AP2	☑	2.4 GHz (B+G+N)	Sapido_VAP2	Auto	Enabled	Enabled	LAN+WAN	Show
AP3	☑	2.4 GHz (B+G+N)	Sapido_VAP3	Auto	Enabled	Enabled	LAN+WAN	Show
AP4	☑	2.4 GHz (B+G+N)	Sapido_VAP4	Auto	Enabled	Enabled	LAN+WAN	Show

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 or 13 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.) Please also check Section 4.1.2.2
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	BRF70n 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

5.4.2 Advanced Settings



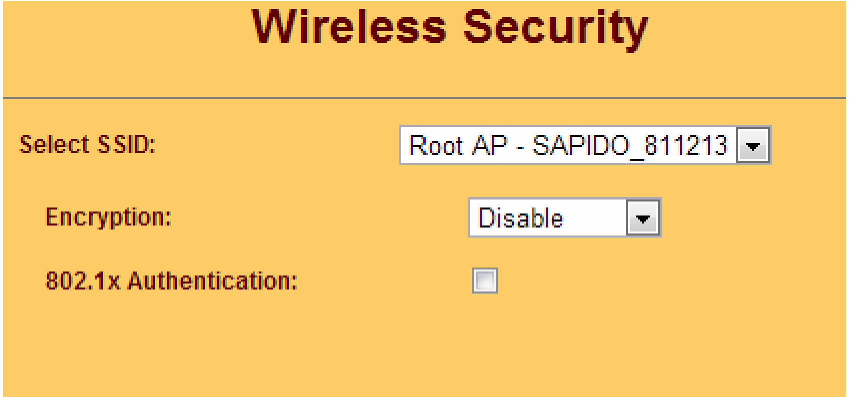
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Preamble Type:	● Long Preamble ○ Short Preamble
IAPP:	● Enabled ○ Disabled
Protection:	○ Enabled ● Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled
WLAN Partition:	○ Enabled ● Disabled
20/40MHz Coexist:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 70% ○ 50% ○ 35% ○ 15%

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%.

5.4.3 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



Wireless Security

Select SSID: Root AP - SAPIDO_811213

Encryption: Disable

802.1x Authentication: □

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

5.4.4 Access Control

Please refer Wireless Access Control

5.4.5 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 BRF70N 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.

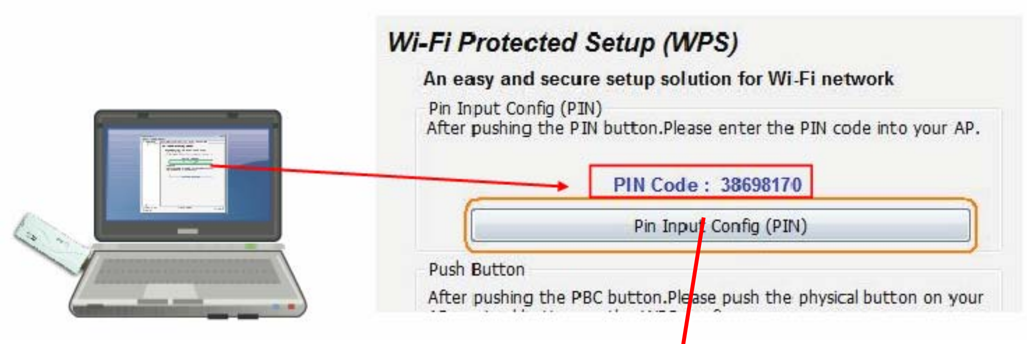
PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

BRF70n 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.



Wi-Fi Protected Setup (WPS)

An easy and secure setup solution for Wi-Fi network

Pin Input Config (PIN)

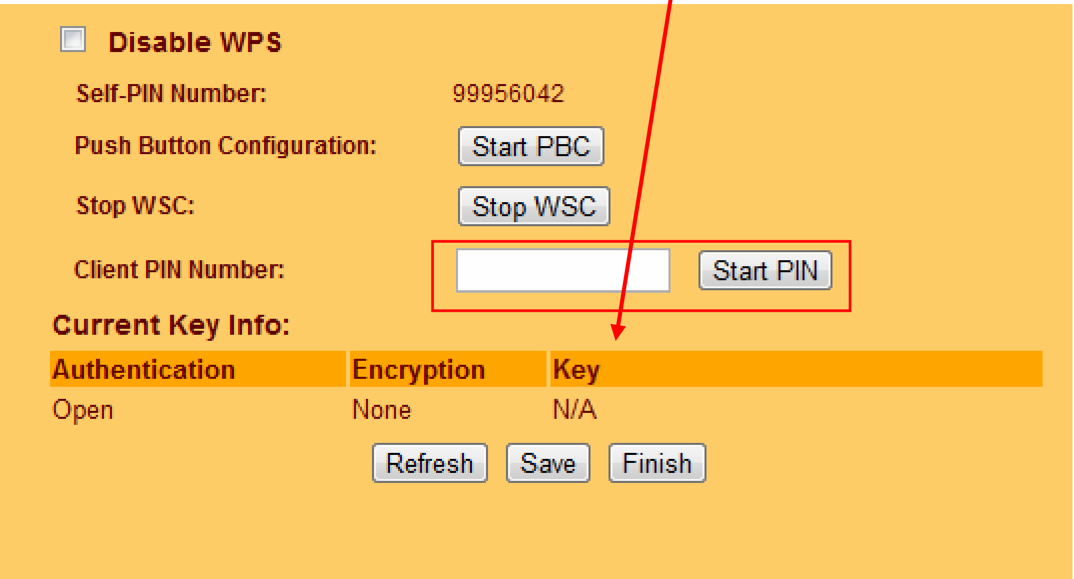
After pushing the PIN button.Please enter the PIN code into your AP.

PIN Code : 38698170

Push Button

After pushing the PBC button.Please push the physical button on your

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



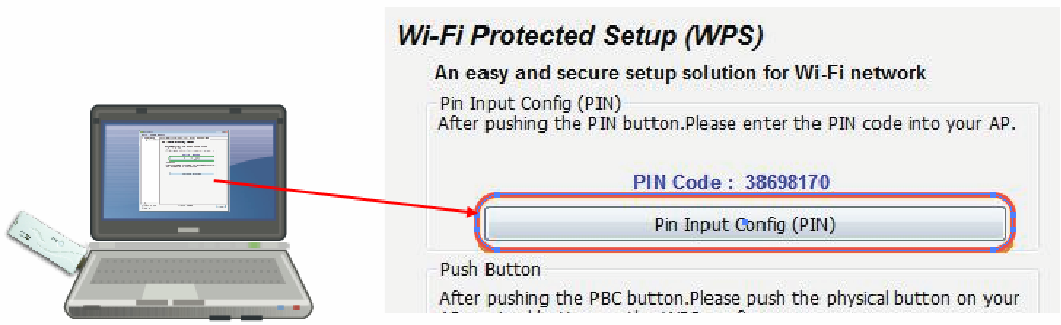
☐ Disable WPS

Self-PIN Number:	99956042
Push Button Configuration:	Start PBC
Stop WSC:	Stop WSC
Client PIN Number:	Start PIN

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

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



Wi-Fi Protected Setup (WPS)

An easy and secure setup solution for Wi-Fi network

Pin Input Config (PIN)

After pushing the PIN button.Please enter the PIN code into your AP.

PIN Code : 38698170

Push Button

After pushing the PBC button.Please push the physical button on your

(4). Wireless dongle should connect to BRF70n

2. Start PBC:

(1). Press the BRF70n WPS button and wait for WPS LED blinking

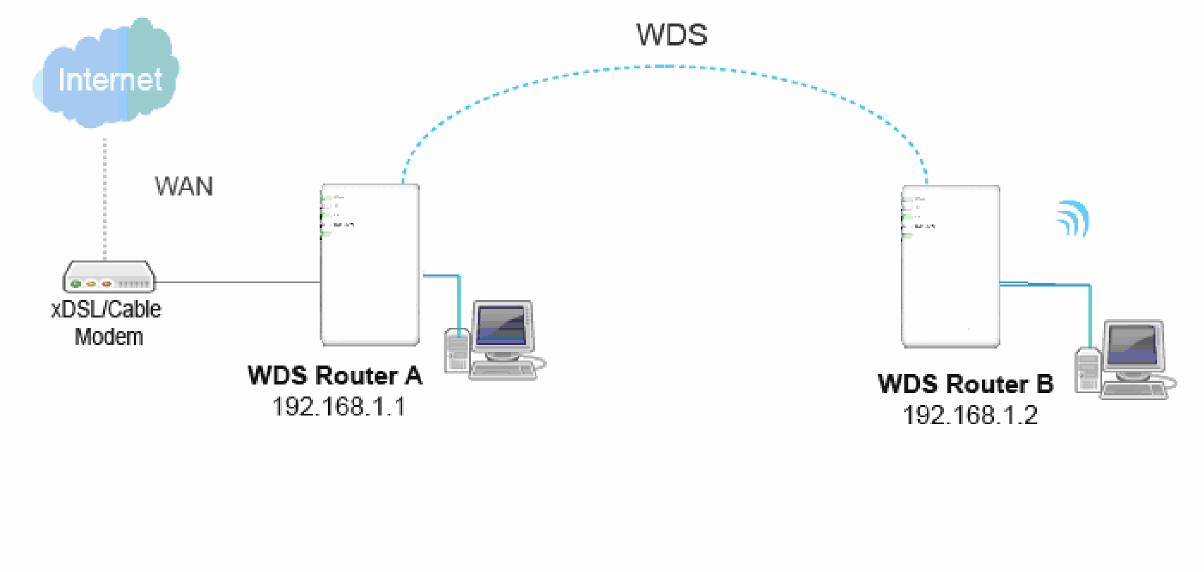
(2). Press the dongle WPS button

(3). Wireless dongle should connect to BRF70n

5.4.6 WDS

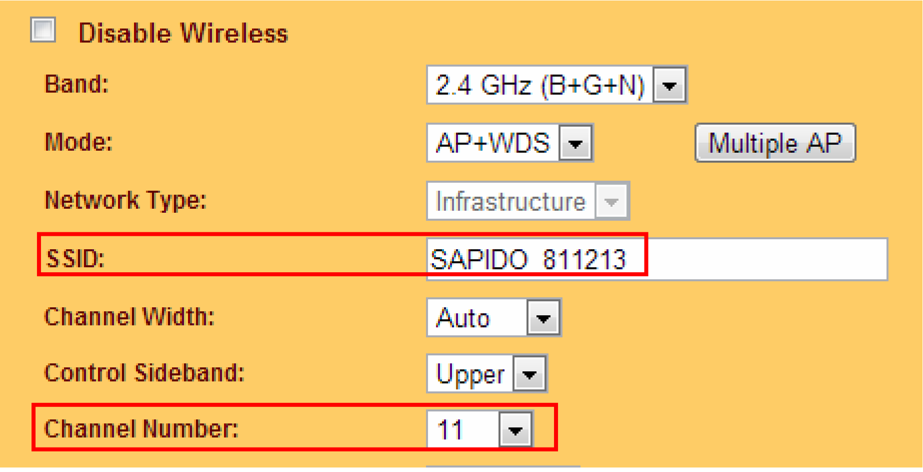
When selected in the Basic Settings page and enabled here, Wireless Distribution System (WDS) enables the router to be used as a wireless bridge. Two Wireless-N Routers in bridge mode can communicate with each other through their wireless interfaces. To accomplish this, all wireless routers should be set to the same channel and the MAC address of other AP / Routers should be entered in the table.

The WDS explanation is as the following picture.



Router_A：

1. Set the connection mode to “AP+WDS” from “Wireless Basic Setting”, and then select the channel number (in this example is "11”). Click Apply Changes to save the setting.



□ Disable Wireless

Band: 2.4 GHz (B+G+N)

Mode: AP+WDS

Network Type: Infrastructure

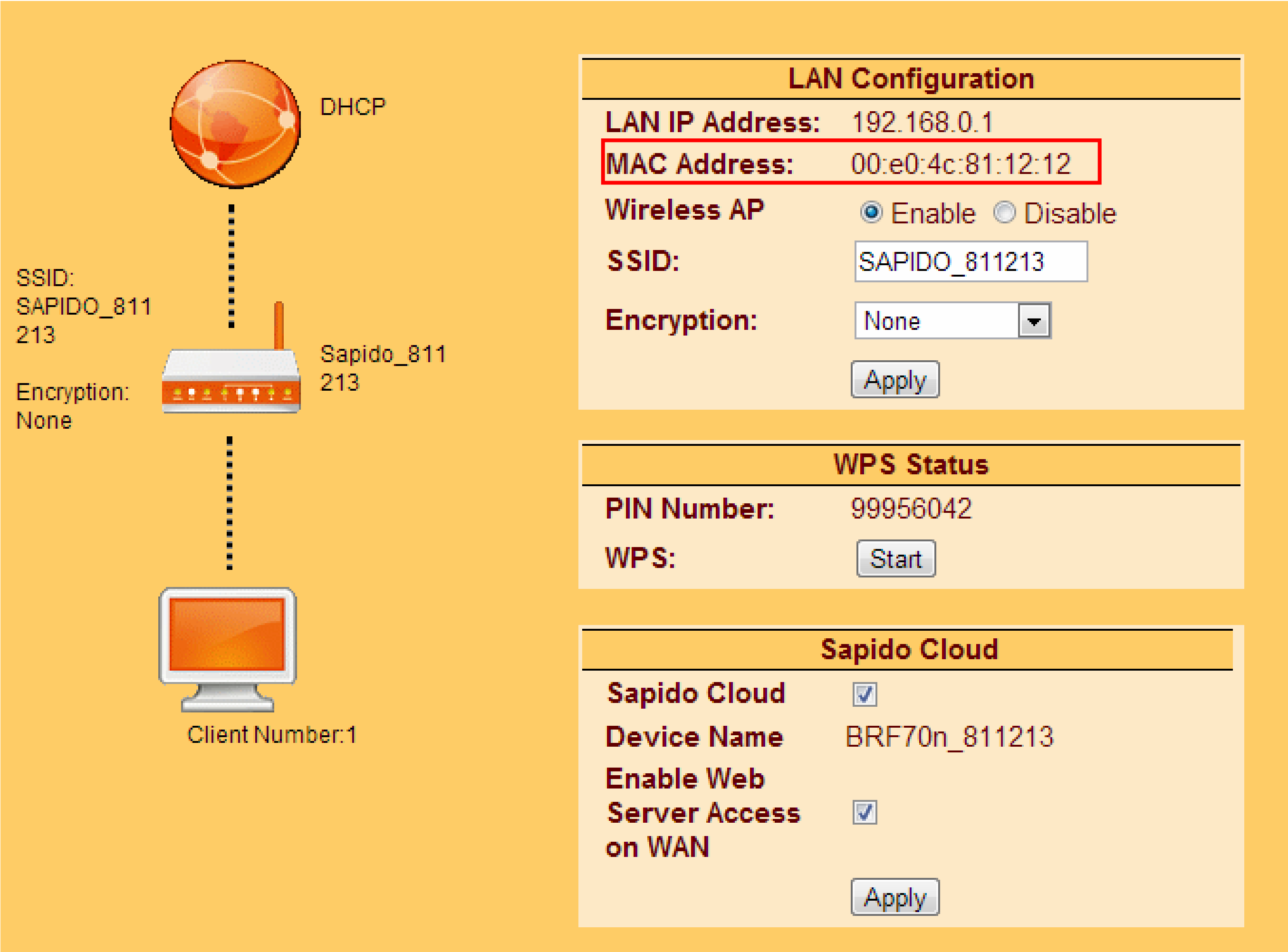
SSID: SAPIDO_811213

Channel Width: Auto

Control Sideband: Upper

Channel Number: 11

2. Please check the MAC address



SSID: SAPIDO_811 213

Encryption: None

LAN Configuration

LAN IP Address: 192.168.0.1

MAC Address: 00:e0:4c:81:12:12

Wireless AP ● Enable ○ Disable

SSID: SAPIDO_811213

Encryption: None

WPS Status

PIN Number: 99956042

WPS:

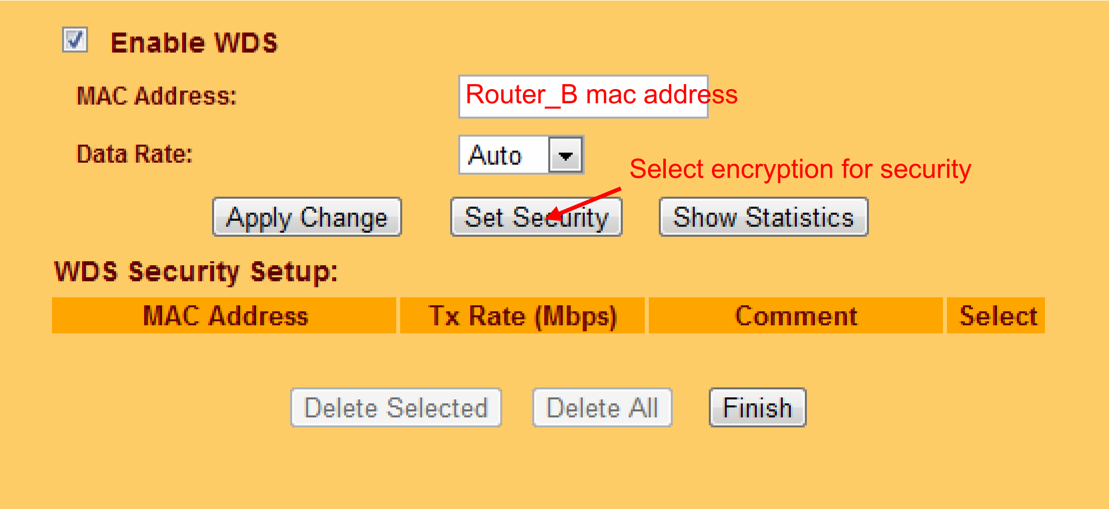
Sapido Cloud

Sapido Cloud ☑

Device Name BRF70n_811213

Enable Web Server Access on WAN ☑

3. Enable WDS function from the page – "WDS Setting", and then fill in the MAC address of Router_B. Click Apply Changes to save the setting data.



☑ Enable WDS

MAC Address: Router_B mac address

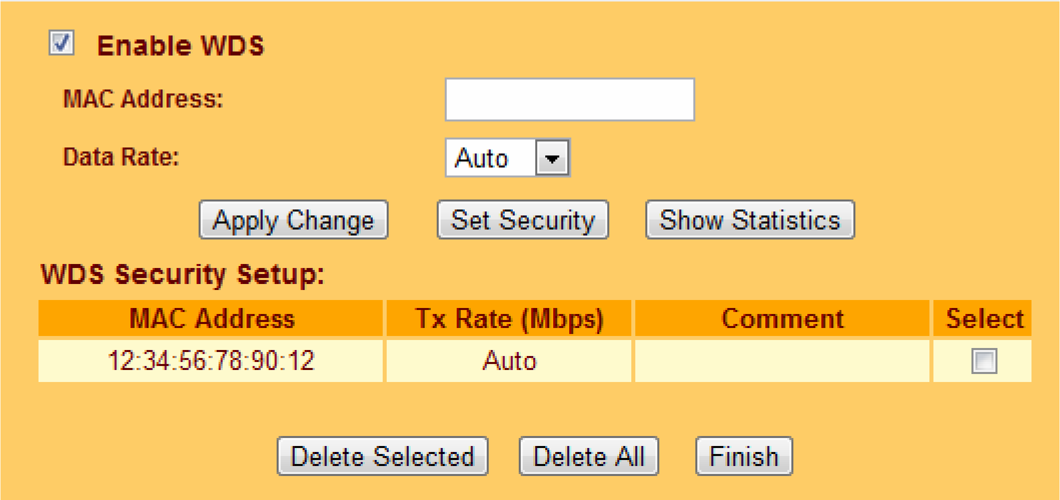
Data Rate: Auto

Select encryption for security

WDS Security Setup:

MAC Address	Tx Rate (Mbps)	Comment	Select

4. The WDS AP List will show the WDS device MAC address.



☑ Enable WDS

MAC Address:

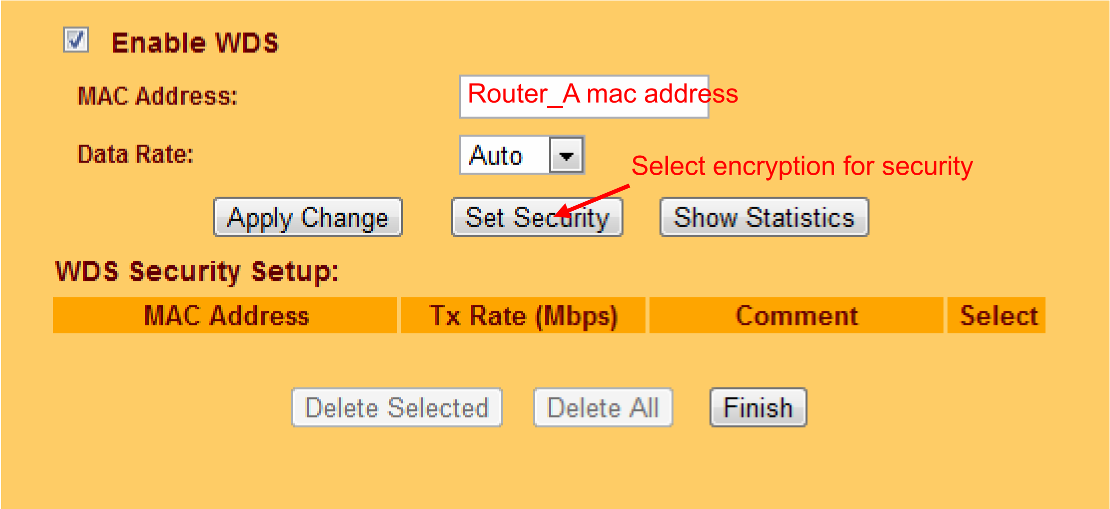
Data Rate: Auto

WDS Security Setup:

MAC Address	Tx Rate (Mbps)	Comment	Select
12:34:56:78:90:12	Auto		□

Router_B：

1. Setup Router_B WDS.



☑ Enable WDS

MAC Address: Router_A mac address

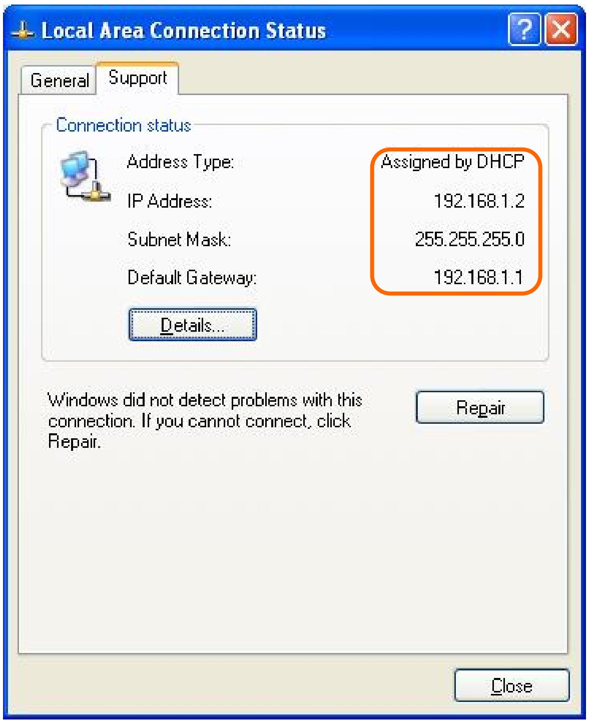
Data Rate: Auto

Select encryption for security

WDS Security Setup:

MAC Address	Tx Rate (Mbps)	Comment	Select

2. Router_B LAN PC will get IP address from Router_A.



Address Type: Assigned by DHCP

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Windows did not detect problems with this connection. If you cannot connect, click Repair.

If you failed the WDS setting, please check you setting with refer to the list below.

	Router_A	**Router_B**
Wireless Mode	AP+WDS	WDS
LAN IP Address	Set the same segment as the router B(Note 1) Example :192.168.1.1	Set the same segment as the router_A(Note 1) Example :192.168.1.2
Security	Set the same security as Router_B	Set the same security as Router_A
DHCP	Enable	Disable

Note 1: LAN IP address should be under the same segment but cannot be the same number.

5.4.7 Schedule

Please refer Wireless Schedule

5.5 NAT

Please refer NAT Management

5.6 VPN Server

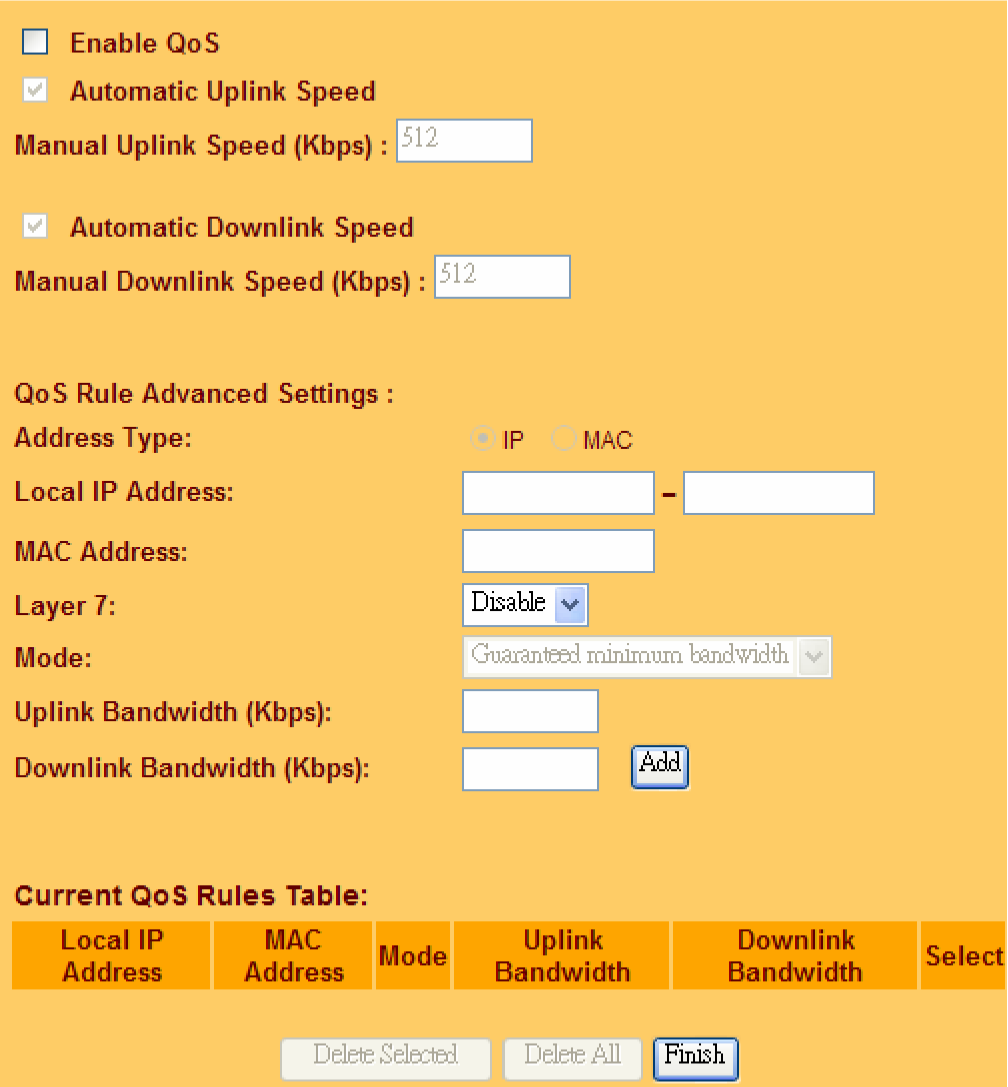
Please refer VPN server

5.7 Firewall

5.7.1 DoS

Please refer DoS

5.5.2 QoS



□ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps) : 512

☑ Automatic Downlink Speed

Manual Downlink Speed (Kbps) : 512

QoS Rule Advanced Settings :

Address Type: ● IP ○ MAC

Local IP Address: -

MAC Address:

Layer 7: Disable

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Current QoS Rules Table:

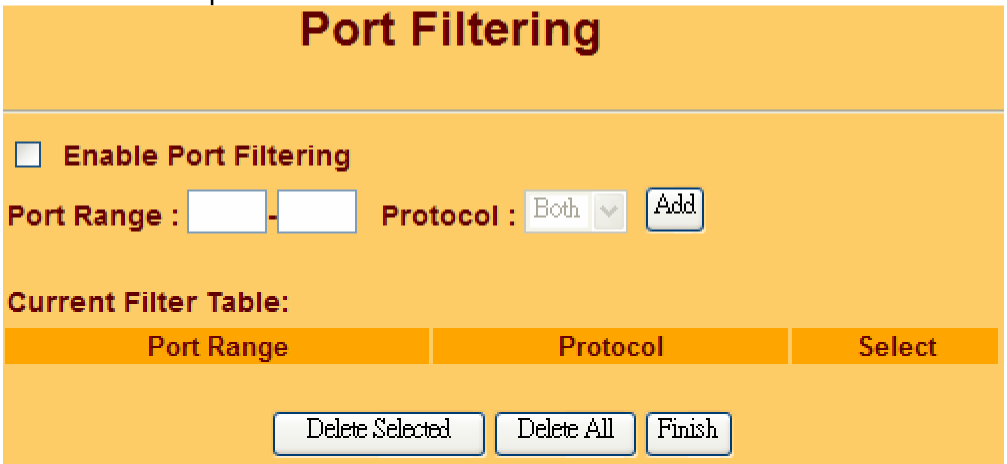
Local IP Address	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Select

Item	Description
Enable QoS	Check “Enable QoS” to enable QoS function for the WAN port. You also can uncheck “Enable QoS” to disable QoS function for the WAN port.
Automatic uplink speed	Check the Automatic uplink speed.
Manual Uplink speed	Input **uplink** bandwidth manually
Automatic downlink	Check the Automatic downlink speed.

speed	
Manual Downlink speed	Input **downlink** bandwidth manually
Address Type	Set QoS by IP Address or MAC address
Local IP Address	Set local IP Address if the address type is by IP Address
MAC Address	Set MAC Address if the address type is by MAC Address
Mode	Select Guaranteed minimum bandwidth or Restricted maximum bandwidth
Uplink Bandwidth	Key in the bandwidth.
Downlink Bandwidth	Key in the bandwidth.

5.5.3 Port Filtering

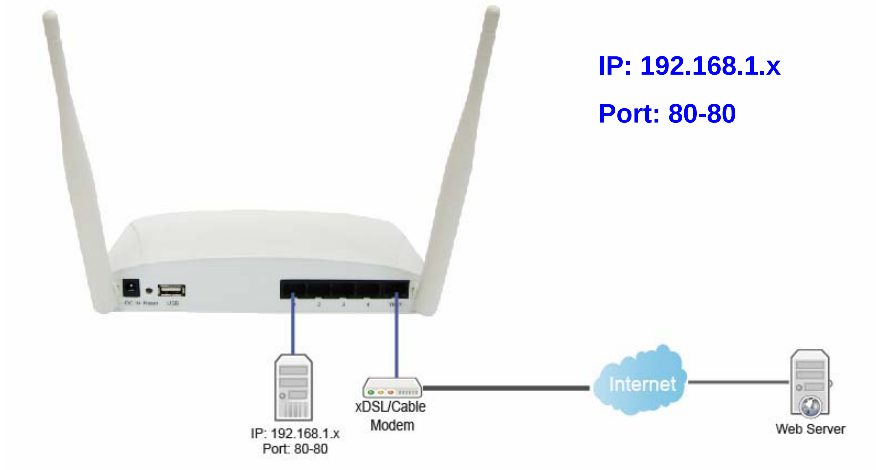
When enabled packets are denied access to Internet/filtered based on their port address.



Protocol : Both

Item	Description
Enable Port Filtering	Select Enable Port Filtering to filter ports.
Port Range	Enter the port number that needs to be filtered.
Protocol	Please select the protocol type of the port.
Add	Click on **Add** to save the setting data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

Port 80 has been blocked as the following illustrate.



5.5.4 IP Filtering

Please refer IP Filtering

5.5.5 Mac Filter Schedule

Please refer Mac Filter Schedule

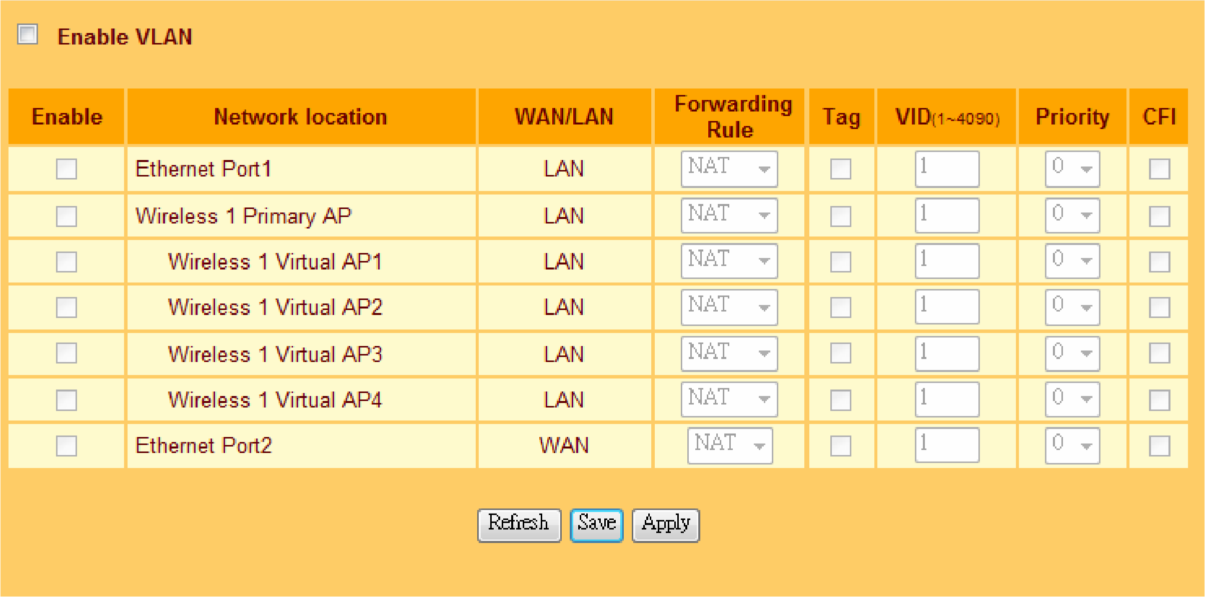
5.5.6 URL Filtering

Please refer URL Filtering

5.5.7 IP Binding

Please refer IP Binding

5.5.8 VLAN



☐ Enable VLAN

Enable	Network location	WAN/LAN	Forwarding Rule	Tag	VID(1~4090)	Priority	CFI
☐	Ethernet Port1	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Primary AP	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP1	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP2	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP3	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP4	LAN	NAT	☐	1	0	☐
☐	Ethernet Port2	WAN	NAT	☐	1	0	☐

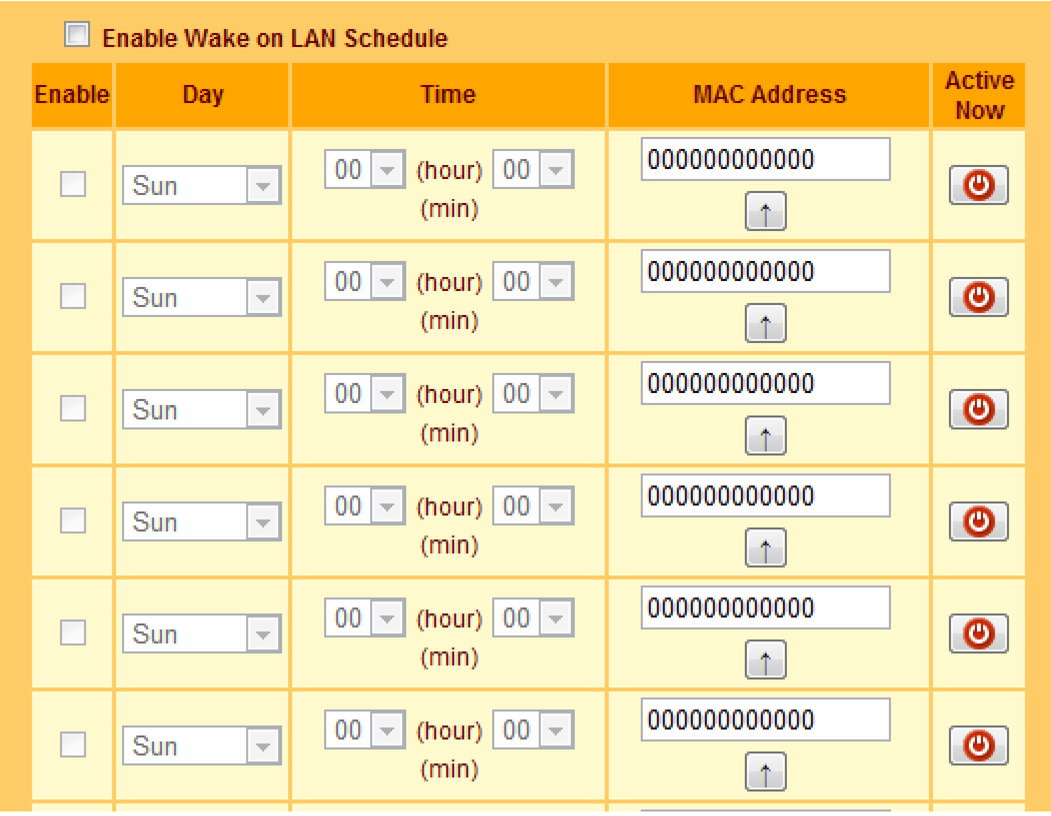
Item	Description
Forwarding Rule	Bridge or NAT mode
Tag	Add VLAN tag to packet
VID	Set VLAN ID（1~4096）
Priority	It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority
CIF	Enable or Disable CIF

5.6 System

This section including **Wake on LAN, 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.

5.6.3 Wake on Lan

Switch your computer ON through your LAN or the Internet . To support WOL you must have a computer with Motherboard that supports WOL, as well as a Network Controller (NIC) supporting this function. Most of the newer Motherboard (circa 2002 and On), have an On Board NIC that supports WOL. Otherwise you need to install a PCI NIC that is WOL capable.

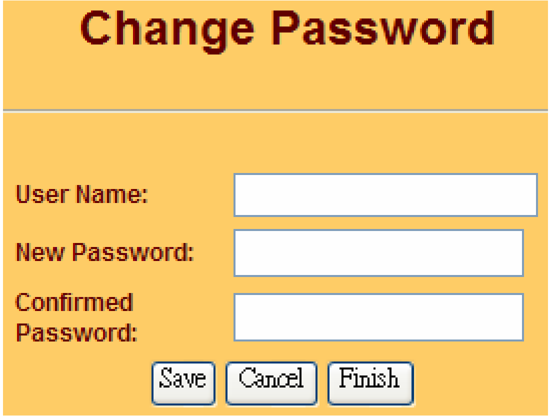


☐ Enable Wake on LAN Schedule

Enable	Day	Time	MAC Address	Active Now
☐	Sun	00 (hour) 00 (min)	000000000000 ↑	⏻
☐	Sun	00 (hour) 00 (min)	000000000000 ↑	⏻
☐	Sun	00 (hour) 00 (min)	000000000000 ↑	⏻
☐	Sun	00 (hour) 00 (min)	000000000000 ↑	⏻
☐	Sun	00 (hour) 00 (min)	000000000000 ↑	⏻
☐	Sun	00 (hour) 00 (min)	000000000000 ↑	⏻

5.6.4 Change User name/Password

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



Change Password

User Name:

New Password:

Confirmed Password:

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

5.6.5 Upgrade Firmware

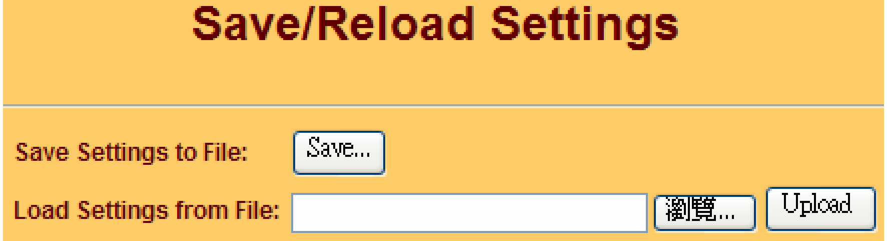
Please refer Firmware Upgrade

5.6.6 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

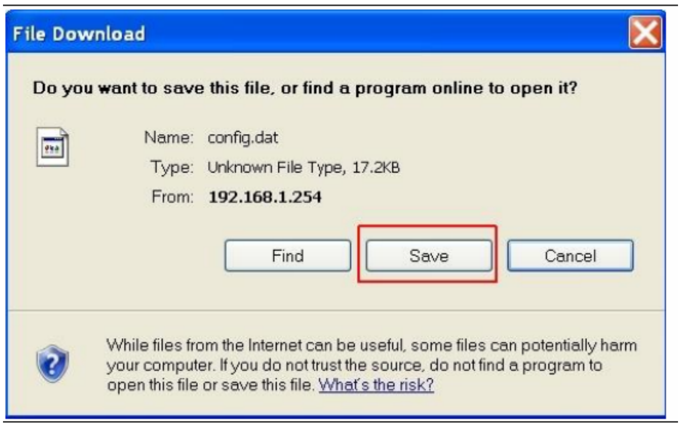


Save/Reload Settings

Save Settings to File:

Load Settings from File:

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



File Download

Do you want to save this file, or find a program online to open it?

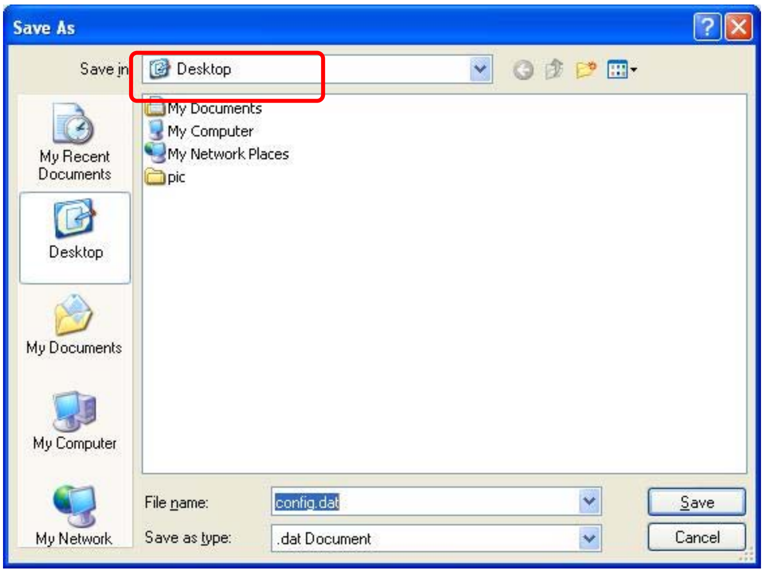
Name: config.dat

Type: Unknown File Type, 17.2KB

From: 192.168.1.254

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

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



Save As

Save in: Desktop

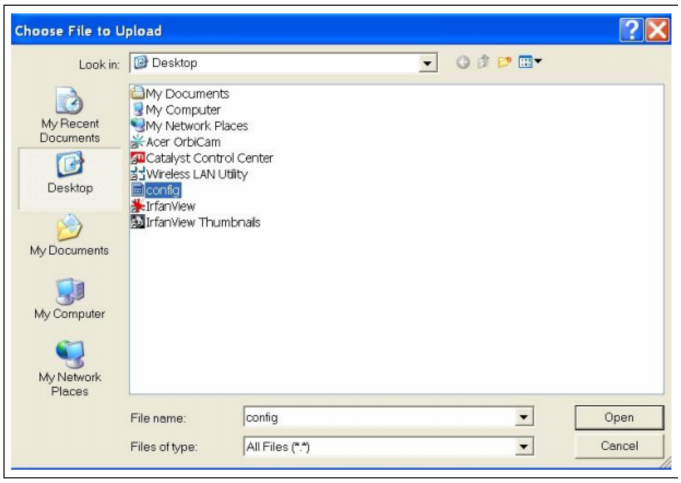
My Documents
My Computer
My Network Places
pic

File name: config.dat

Save as type: .dat Document

2. Load configuration file

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



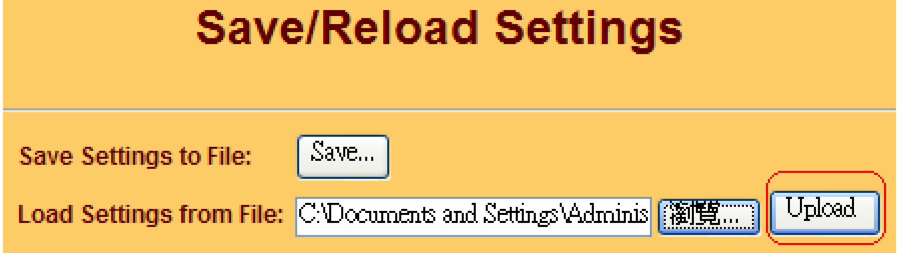
Choose File to Upload

Look in: Desktop

File name: config

Files of type: All Files (*.*)

(2). Click Upload to upload configuration file to BRF70N .



Save/Reload Settings

Save Settings to File: Save...

Load Settings from File: C:\Documents and Settings\Adminis

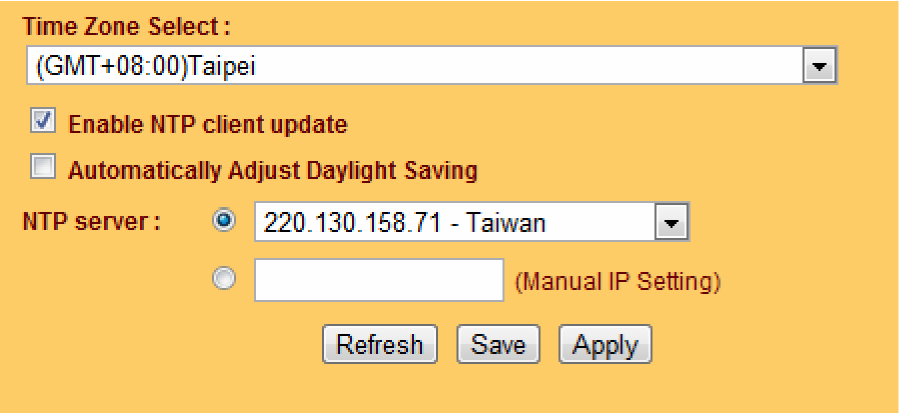
(3). After 60 seconds, BRF70N will reboot automatically.

5.6.7 Remote Management

Please refer Remote Management

5.6.8 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.



Time Zone Select :

(GMT+08:00)Taipei

☑ Enable NTP client update

□ Automatically Adjust Daylight Saving

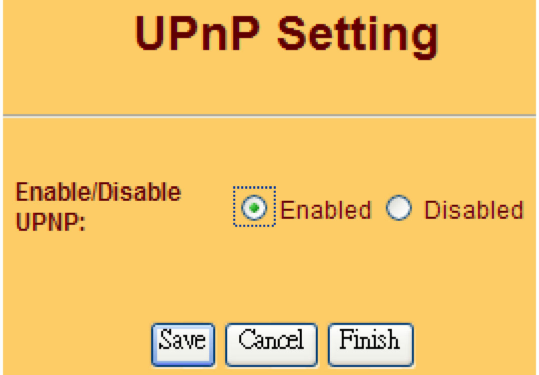
NTP server : ● 220.130.158.71 - Taiwan

○ (Manual IP Setting)

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.

5.6.9 UpnP



UPnP Setting

Enable/Disable UPNP: ● Enabled ○ Disabled

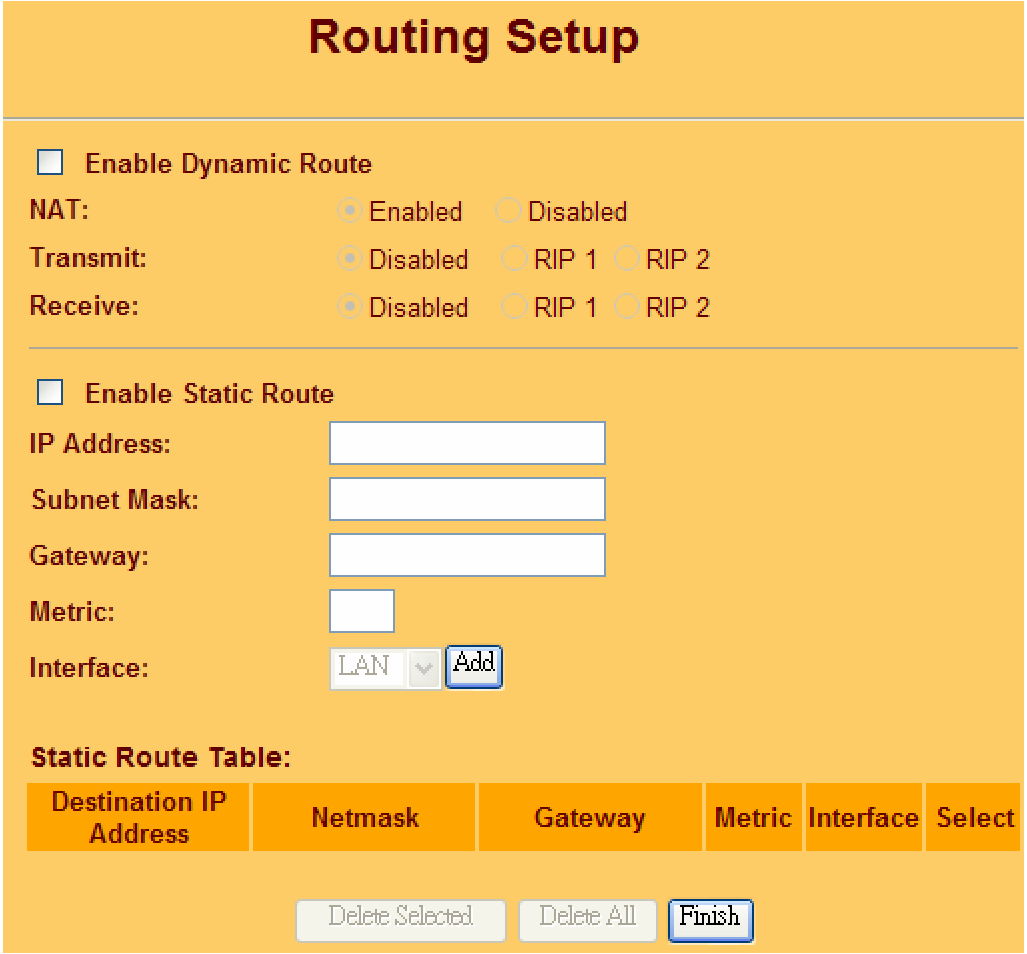
- **UPNP**

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. BRF70N 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.

5.6.10 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.



Routing Setup

☐ Enable Dynamic Route

NAT: ● Enabled ○ Disabled

Transmit: ● Disabled ○ RIP 1 ○ RIP 2

Receive: ● Disabled ○ RIP 1 ○ RIP 2

☐ Enable Static Route

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface: LAN

Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select

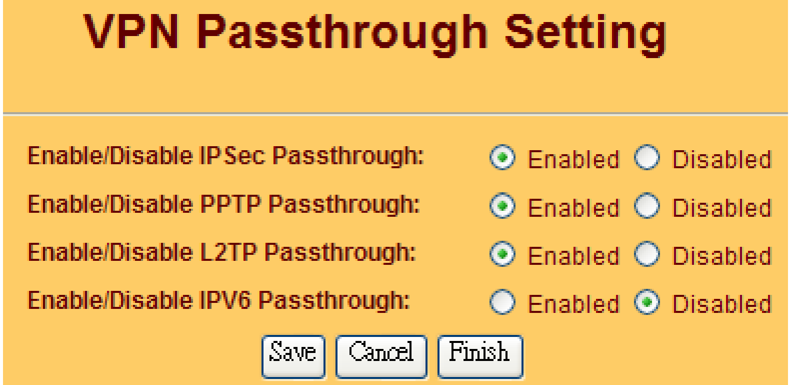
Item	Description
Enable Dynamic Route	Enable or Disable dynamic route
NAT	Enable or Disable NAT function
Transmit	There are 3 options： 1. Disable：do not send any RIP packet out 2. Send RIP1 packet out 3. Send RIP2 packet out
Receive	There are 3 options： 4. Disable：do not receive any RIP packet 5. Only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

5.6.11 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.



VPN Passthrough Setting

Enable/Disable IPSec Passthrough: ● Enabled ○ Disabled

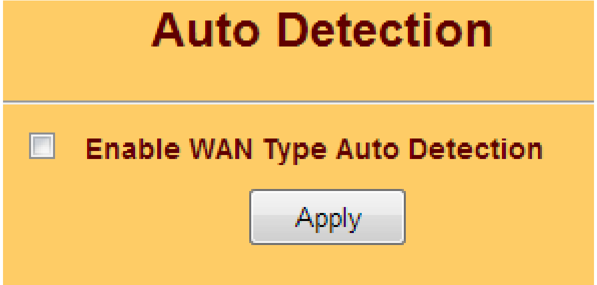
Enable/Disable PPTP Passthrough: ● Enabled ○ Disabled

Enable/Disable L2TP Passthrough: ● Enabled ○ Disabled

Enable/Disable IPV6 Passthrough: ○ Enabled ● Disabled

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.

5.6.12 Wan Type Auto Detection



Auto Detection

□ Enable WAN Type Auto Detection

6 Q & A

6.5 Installation

1. **Q: Where is the XDSL Router installed on the network?**

   A: In a typical environment, the Router is installed between the XDSL line and the LAN. Plug the XDSL Router into the XDSL line on the wall and Ethernet port on the Hub (switch or computer).

2. **Q: Why does the throughput seem slow?**

   A: To achieve maximum throughput, verify that your cable doesn't exceed 100 meter. If you have to do so, we advise you to purchase a bridge to place it in the middle of the route in order to keep the quality of transmitting signal. Out of this condition you would better test something else.

   - Verify network traffic does not exceed 37% of bandwidth.
   - Check to see that the network does not exceed 10 broadcast messages per second.
   - Verify network topology and configuration.

6.6 LED

1. **Why doesn't BRF70N power up?**

   A: Check if the output voltage is suitable, or check if the power supply is out of order.

2. **The Internet browser still cannot find or connect to BRF70N after verifying the IP address and LAN cable, the changes cannot be made, or password is lost.**

   A: In case BRF70N is inaccessible; you can try to restore its factory default settings. Please press the "Reset" button and keep it pressed for over 7 seconds and the light of STATUS will vanish. The LEDs will flash again when reset is successful.

3. **Why does BRF70N shut down unexpectedly?**

   A: Re-plug your power adapter. Then, check the STATUS indicator; if it is off, the internal flash memory is damaged. For more help, please contact with your provider.

6.7 IP Address

1. **Q: What is the default IP address of the router for LAN port?**

   A: The default IP address is 192.168.1.1 with subnet mask 255.255.255.0

2. **Q: I don't know my WAN IP.**

   A: There are two ways to know.

   Way 1: Check with your Internet Service Provider.

   Way 2: Check the setting screen of BRF70N . Click on **Status & Log** item to select **Network Configuration** on the Main Menu. WAN IP is shown on the WAN interface.

3. How can I check whether I have static WAN IP Address?

A: Consult your ISP to confirm the information, or check Network Configuration in BRF70N 's Main Menu.

4. Will the Router allow me to use my own public IPs and Domain, or do I have to use the IPs provided by the Router?

A: Yes, the Router mode allows for customization of your public IPs and Domain.

6.8 OS Setting

1. Why can't my computer work online after connecting to BRF70N ?

A: It's possible that your Internet protocol (TCP/IP) was set to use the following IP address. Please do as the following steps. (Windows 2000 & XP) **Start**＞**Settings**＞**Network and Dial-up Connections**＞double click on **Internet Protocol(TCP/IP)**＞select **obtain IP address automatically**＞ Click on **OK** button. Then, open Internet browser for testing. If you still can't go online, please test something else below.

- Verify network configuration by ensuring that there are no duplicate IP addresses.
- Power down the device in question and ping the assigned IP address of the device. Ensure no other device responds to that address.
- Check that the cables and connectors or use another LAN cable.

2. Q: Why can't I connect to the router's configuration utility?

A: Possible Solution 1: Make sure that your Ethernet connect properly and securely. Make sure that you've plugged in the power cord.

Possible Solution 2: Make sure that your PC is using an IP address within the range of 192.168.1.2 to 192.168.1.254. Make sure that the address of the subnet mask is 255.255.255.0. If necessary, the Default Gateway data should be at 192.168.1.1. To verify these settings, perform the following steps:

Windows 2000, or XP Users:

1. Click on Windows **Start** > click on **Run** > input **cmd** > click on **OK** button.
2. At the DOS prompt, type ipconfig/all.
3. Check the IP Address, Subnet Mask, Default Gateway data. Is this data correct? If the data isn't correct. Please input **ipconfig/release** > press **Enter** > input **ipconfig/renew** > press **Enter**.

Possible Solution 3: Verify the connection setting of your Web browser and verify that the HTTP Proxy feature of your Web browser is disabled. Make these verifications so that your Web browser can read configuration pages inside your router. Launch your Web browser.

Internet Explorer Users:

1. Click on **Tools** > **Internet Options** > **Connections tab**.
2. Select **never dial a connection**, click on **Apply** button, and then click on **OK** button.
3. Click on **Tools** and then click on **Internet Options**.
4. Click on **Connections** and then click on **LAN Settings**.

5. Make sure none of the check boxes are selected and click on **OK** button.
6. Click on OK button.

Netscape Navigator Users:

1. Click on **Edit** > **Preferences** > double-click **Advanced** in the Category window.
2. Click on **Proxies** > select **Direct connection to the Internet** > click on **OK** button.
3. Click on **Edit again** and then click on **Preferences**.
4. Under category, double-click on **Advanced** and then click on **Proxies**.
5. Select **Direct connection to the Internet** and click on **OK** button.
6. Click on **OK** button.

3. Q: Web page hangs, corrupt downloads, or nothing but junk characters is being displayed on the screen. What do I need to do?

A: Force your NIC to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your NIC as a temporary measure. (Please look at the Network Control Panel, in your Ethernet Adapter's Advanced Properties tab.)

4. Q: Why can't I connect to the Web Configuration?

A: you can remove the proxy server settings in your web browser.

6.9 BRF70N Setup

1. Q: Why does BRF70N 's setup page shut down unexpectedly?

A: If one of the pages appears incompletely in BRF70N 's setup pages, please click on Logout item on the Main Menu before shutting it down. Don't keep it working. Then, close Internet browser and open it again for going back to the previous page.

2. Q: I don't know how to configure DHCP.

A: DHCP is commonly used in the large local network. It allows you to manage and distribute IP addresses from 2 to 254 throughout your local network via BRF70N . Without DHCP, you would have to configure each computer separately. It's very troublesome. Please Open **Internet browser** > Input **192.168.1.1 in the website blank field** > Select **DHCP Server under** the **IP Config Menu**. For more information, please refer to 3.3.2 (Router Mode) or 4.3.1 (AP Mode).

3. Q: How do I upgrade the firmware of BRF70N ?

A: Periodically, a new Flash Code is available for BRF70N on your product supplier's website. Ideally, you should update BRF70N 's Flash Code using **Firmware Upgrade** on the **System Management** menu of BRF70N Settings.

4. Q: Why is that I can ping to outside hosts, but cannot access Internet websites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router assign the DNS settings to the DHCP-client-enabled PC.

5. Q: BRF70N couldn't save the setting after click on Apply button?

A: BRF70N will start to run after the setting finished applying, but the setting isn't written into memory. Here we suggest if you want to make sure the setting would be written into memory, please reboot the device via **Reboot** under **System Management** directory**.**

6.10 Wireless LAN

1. **Q: Why couldn’t my wireless notebook work on-line after checking?**

   A: Generally, Wireless networks can sometimes be very complicated to set up, particularly if you're dealing with encryption and products from different vendors. Any number of variables can keep your workstations from talking to each other. Let's go over some of more common ones.

   For starters, verify that your router and your workstation are using the same SSID descriptions. SSID acts as a password when a mobile device tries to connect to the wireless network. The SSID also differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A workstation will not be permitted to connect to the network unless it can provide this unique identifier. This is similar to the function of your network's Workgroup or Domain name.

   When you're experiencing conductivity problems, it is always best to keep things simple. So next you are going to do is that, please disable any WEP encryption you might have configured.

   Successful implementation of encryption also includes the use of a shared key. A HEX key is the most common, but other formats are also used. This key identifies the workstation to the router as a trusted member of this network. Different manufacturers can implement this key technology in ways that might prevent them from working correctly with another vendor's products. So pay attention to detail is going to be the key to a successful installation.

   Next make sure the router and the NIC are configured to use the same communications channel. There are normally 11 of them, and the default channel can also vary from vendor to vendor. You might also want to confirm that the router has DHCP services enabled and an address pool configured. If not, the NIC won't be able to pick up an IP address. I have run across a few access points that offer DHCP services but do not assign all of the needed IP information to the NIC. As a result, I was able to connect to the network, but could not browse the web. The point is, don't assume anything. Verify for yourself that all of the required settings are being received by the workstation.

   Finally, you might want to keep the system you're trying to configure in the same room as the router, at least during the initial configuration, in order to minimize potential interference from concrete walls or steel beams.

2. **Q: My PC can’t locate the Wireless Access Point.**

   A: Check the following:

   - Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode.)
   - The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example “Workgroup” does NOT match “workgroup”.
   - Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
   - If WEP is enabled on the Wireless Router, your PC must have WEP enabled, and the key must match.
   - If the Wireless Router’s Wireless screen is set to Allow LAN access to selected Wireless Stations only, then each of your Wireless stations must have been selected, or access will be blocked.

- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point. Remember that the connection range can be as little as 100 feet in poor environments.

3. **Q: Wireless connection speed is very slow.**

A: The wireless system will connect at highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with following:

- Access Point location: Try adjusting the location and orientation of the Access Point.
- Wireless Channel: If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference: Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding: Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

4. **Q: Some applications do not run properly when using the Wireless Router.**

A: The Wireless Router processes the data passing through it, so it is not transparent. Use the Special Application feature to allow the use of Internet applications which do not function correctly. If this does solve the problem, you can use the DMZ function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

5. **Q: I can't connect to the Wireless Router to configure it.**

A: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Make sure that your PC and the Wireless Router are on the same network segment.
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, make sure that it is using an IP Address within the range 192.168.1.129 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using Control Panel ~ Network to check the Properties for the TCP/IP protocol.

6. **Q: The WinXP wireless interface couldn't communicate the WEP with SAPIDO BRF70N's wireless interface.**

A: The default WEP of WinXP is **Authentication Open System - WEP**, but the WEP of SAPIDO BRF70N is only for **Shared Key - WEP**, it caused both sides couldn't communicate. Please select the WEP of WinXP from Authentication Open System to **Pre-shared Key - WEP**, and then the WEP wireless interface between WinXP and SAPIDO BRF70N would be communicated.

6.11 Support

1. **Q: What is the maximum number of IP addresses that the XDSL Router will support?**

   A: The Router will support to 253 IP addresses with NAT mode.

5. **Q: Is the Router cross-platform compatible?**
   A: Any platform that supports Ethernet and TCP/IP is compatible with the Router.

6.12 Others

1. **Q: Why does the router dial out for PPPoE mode very often?**

   A: Normally some of game, music or anti-virus program will send out packets that trigger the router to dial out, you can close these programs. Or you can set the idle time to 0, then control to dial out manually.

2. **Q: What can I do if there is already a DHCP server in LAN?**

   A: If there are two DHCP servers existing on the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in router and configure your PC manually.

7 Appendices

7.5 Operating Systems

1. Microsoft：Windows 2000, XP, Vista, Windows 7.
2. Apple：Mac OS X 10.4.7, Leopard and the following related versions.
3. Linux：Redhat 9, Fedora 6 & 7, Ubuntu 7.04 and the following related versions.

7.6 Browsers

1. Internet Explorer ver. 6 and 7 and the following related versions.
2. FireFox ver. 2.0.0.11 and the following related versions.3.
3. Safari ver. 3.04 and the following related versions.

7.7 Communications Regulation Information

Should any consumers need to learn more information, services and supports, please contact the supplier of your product directly.