WPS Settings

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi networks for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.

WPS State: Display whether the WPS is **configured** or **unconfigured**.

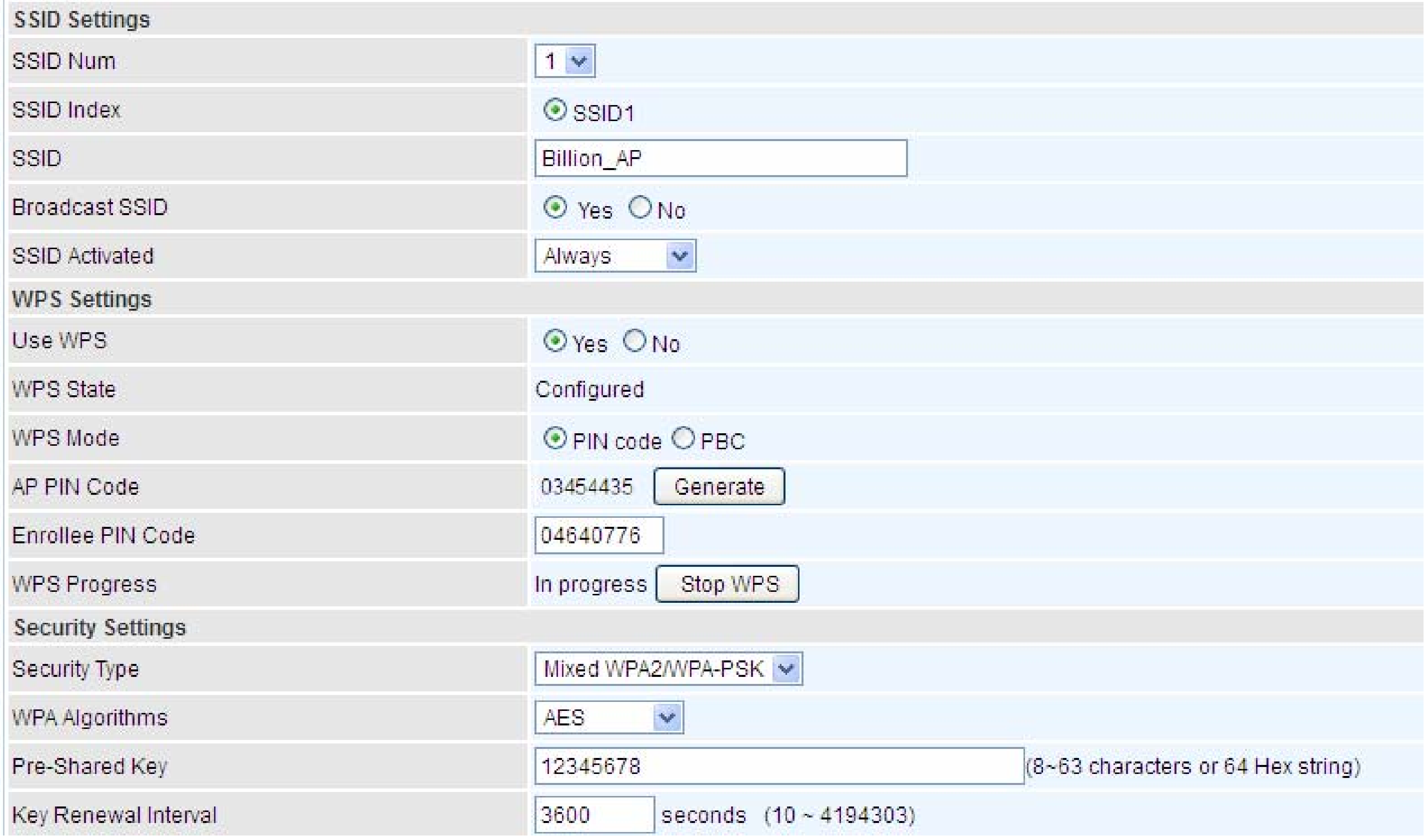
WPS Mode: Select the mode which to start WPS, choose between **PIN Code** and **PBC** (Push Button). Selecting **Pin Code** mode will require you to know the enrollee PIN code.

To future understand the two modes of configuration; please refer to the following **Wi-Fi Protected Setup.**

Wi-Fi Protected Setup

PIN Method: Configure AP as Registrar

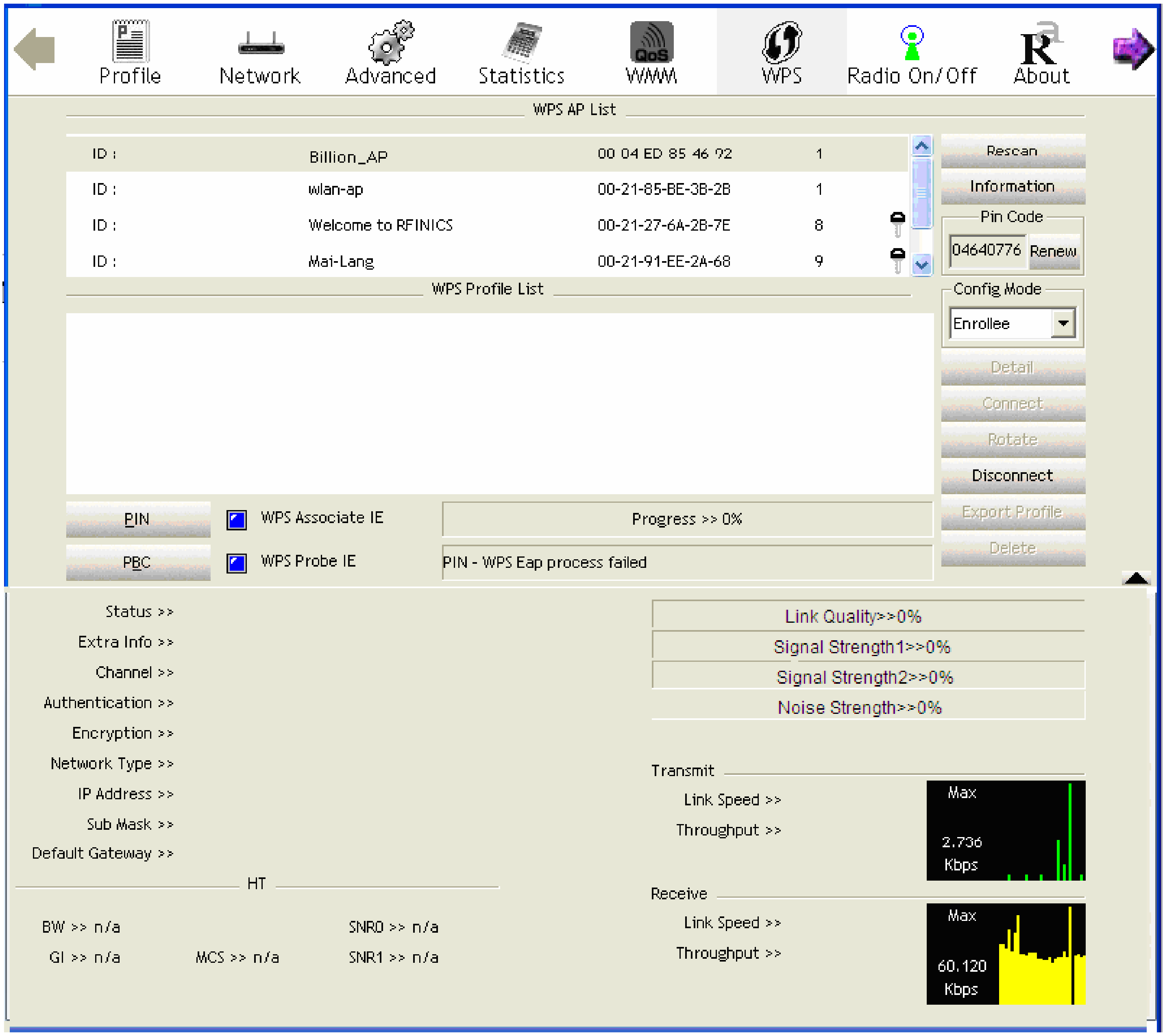
1. Jot down the client's Pin (eg. 04640776).



SSID Settings	
SSID Num	1
SSID Index	● SSID1
SSID	Billion_AP
Broadcast SSID	● Yes ○ No
SSID Activated	Always
WPS Settings	
Use WPS	● Yes ○ No
WPS State	Configured
WPS Mode	● PIN code ○ PBC
AP PIN Code	03454435 Generate
Enrollee PIN Code	04640776
WPS Progress	In progress Stop WPS
Security Settings	
Security Type	Mixed WPA2/WPA-PSK
WPA Algorithms	AES
Pre-Shared Key	12345678 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

2. Enter the Enrollee(Client) PIN code and then press Start WPS.

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. Billion_AP) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



WPS AP List

ID :	Billion_AP	00 04 ED 85 46 72	1
ID :	wlan-ap	00-21-85-BE-3B-2B	1
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8
ID :	Mai-Lang	00-21-91-EE-2A-68	9

WPS Profile List

Pin Code: 04640776

Config Mode: Enrollee

■ WPS Associate IE

■ WPS Probe IE

Progress >> 0%

PIN - WPS Eap process failed

Status >>
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

Link Quality>>0%
Signal Strength1>>0%
Signal Strength2>>0%
Noise Strength>>0%

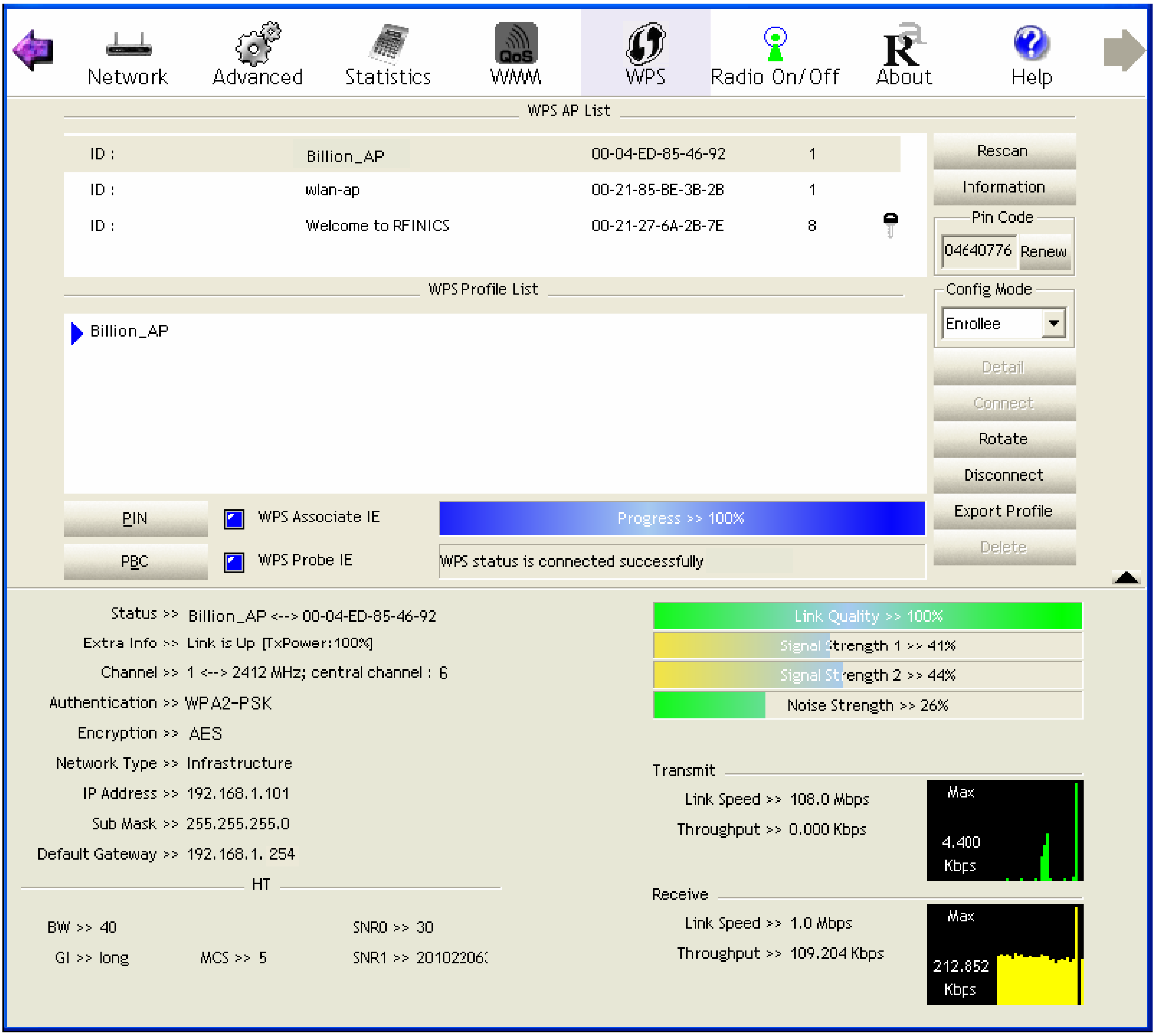
HT

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Transmit
Link Speed >>
Throughput >>
Max
2.736 Kbps

Receive
Link Speed >>
Throughput >>
Max
60.120 Kbps

4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar (router).



WPS AP List

ID :	Billion_AP	00-04-ED-85-46-92	1
ID :	wlan-ap	00-21-85-BE-3B-2B	1
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8

Pin Code: 04640776

WPS Profile List

Billion_AP

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfully

Status >> Billion_AP <--> 00-04-ED-85-46-92

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <--> 2412 MHz; central channel : 6

Authentication >> WPA2-PSK

Encryption >> AES

Network Type >> Infrastructure

IP Address >> 192.168.1.101

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1. 254

HT

BW >> 40

GI >> long

MCS >> 5

SNR0 >> 30

SNR1 >> 20102206:

Link Quality >> 100%

Signal Strength 1 >> 41%

Signal Strength 2 >> 44%

Noise Strength >> 26%

Transmit

Link Speed >> 108.0 Mbps

Throughput >> 0.000 Kbps

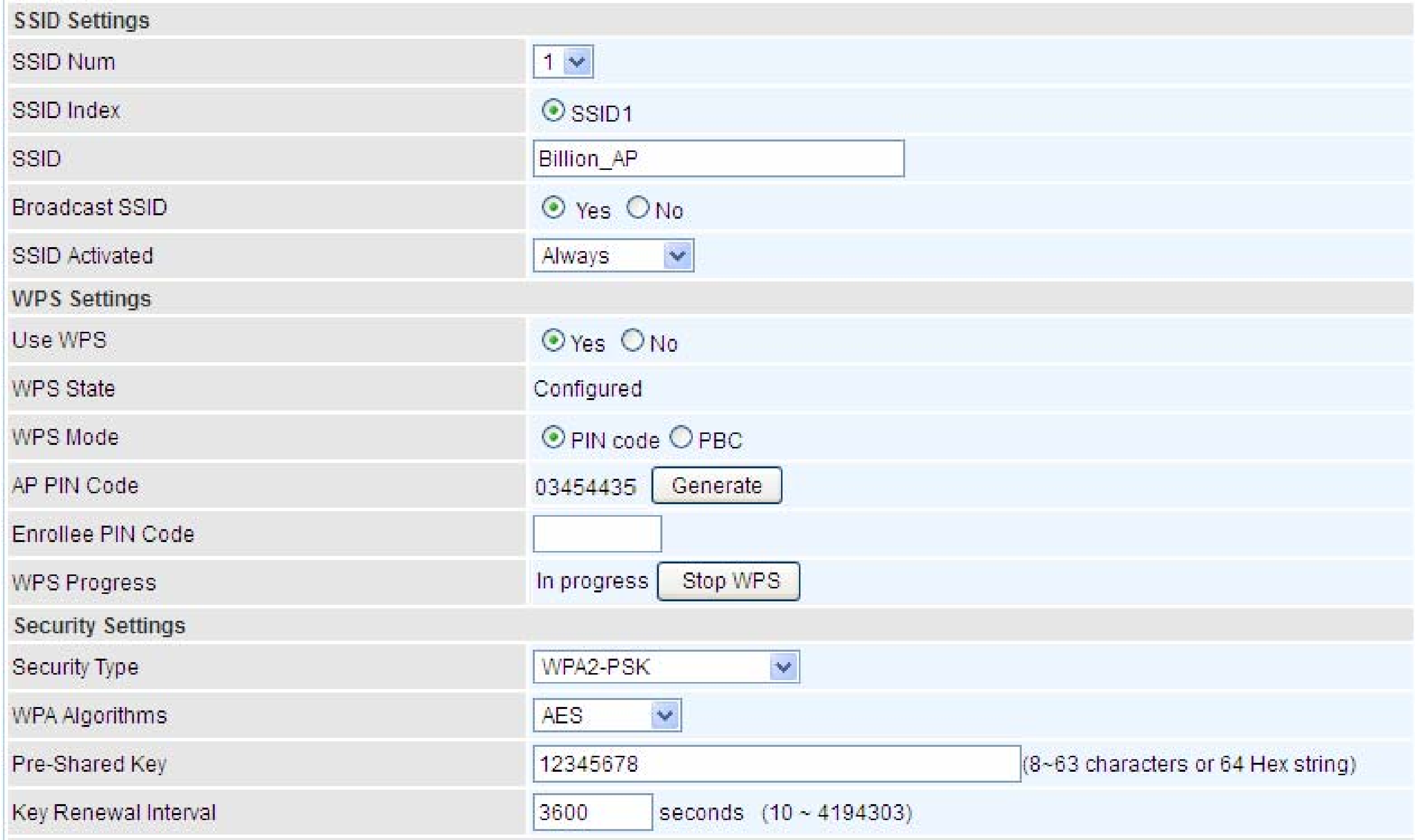
Receive

Link Speed >> 1.0 Mbps

Throughput >> 109.204 Kbps

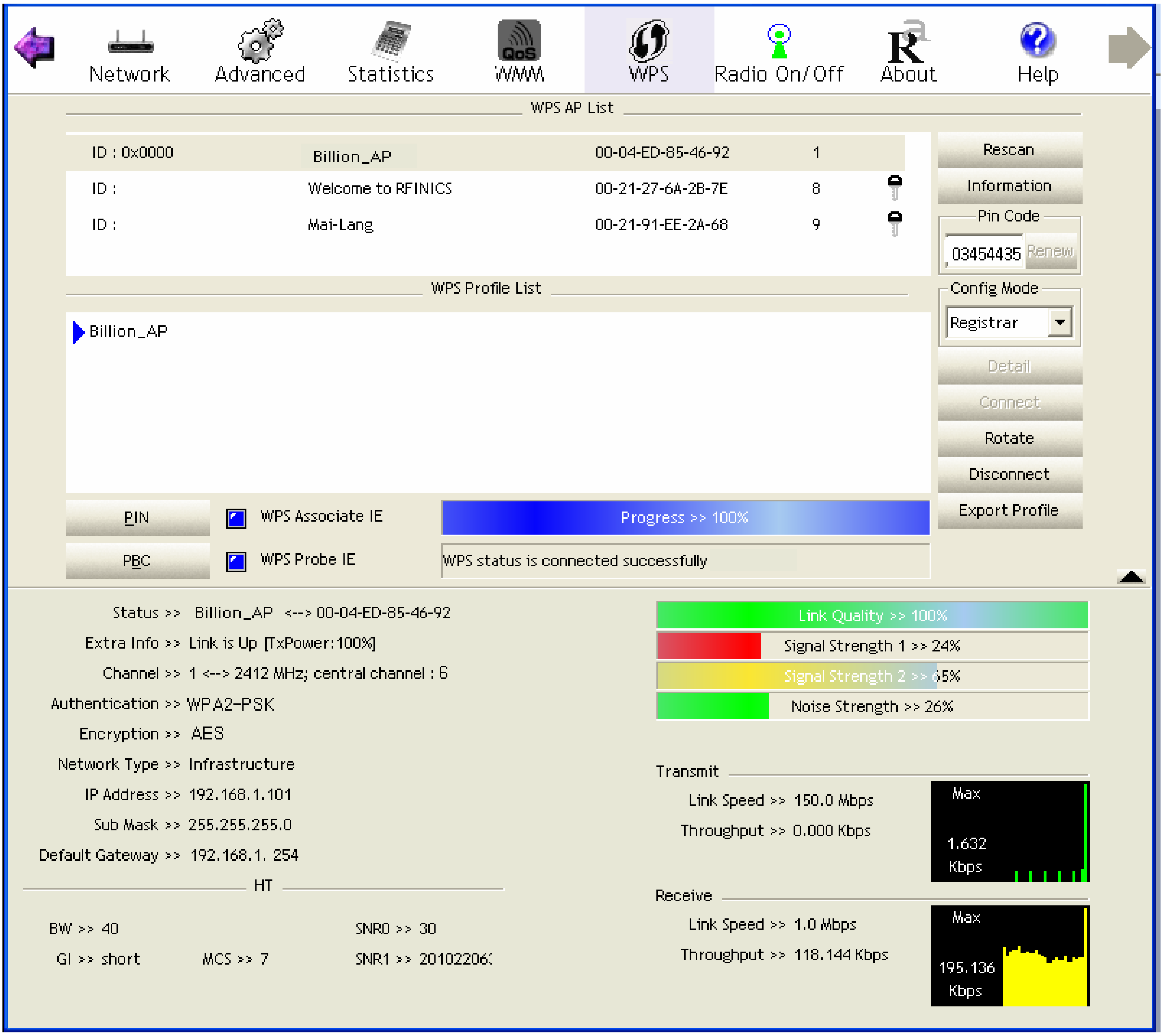
PIN Method: Configure AP as Enrollee

1. Jot down the WPS PIN (eg. 03454435).Press Start WPS.



SSID Settings	
SSID Num	1
SSID Index	● SSID1
SSID	Billion_AP
Broadcast SSID	● Yes ○ No
SSID Activated	Always
WPS Settings	
Use WPS	● Yes ○ No
WPS State	Configured
WPS Mode	● PIN code ○ PBC
AP PIN Code	03454435 Generate
Enrollee PIN Code	
WPS Progress	In progress Stop WPS
Security Settings	
Security Type	WPA2-PSK
WPA Algorithms	AES
Pre-Shared Key	12345678 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

2. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. Billion_AP) from the WPS AP List before pressing the PIN button to run the scan.



WPS AP List

ID : 0x0000	Billion_AP	00-04-ED-85-46-92	1
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8
ID :	Mai-Lang	00-21-91-EE-2A-68	9

Pin Code: 03454435

Config Mode: Registrar

WPS Profile List

Billion_AP

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfully

Status >> Billion_AP <--> 00-04-ED-85-46-92

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <--> 2412 MHz; central channel : 6

Authentication >> WPA2-PSK

Encryption >> AES

Network Type >> Infrastructure

IP Address >> 192.168.1.101

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1. 254

HT

BW >> 40

GI >> short MCS >> 7

SNR0 >> 30

SNR1 >> 20102206:

Link Quality >> 100%

Signal Strength 1 >> 24%

Signal Strength 2 >> 65%

Noise Strength >> 26%

Transmit

Link Speed >> 150.0 Mbps

Throughput >> 0.000 Kbps

Max 1.632 Kbps

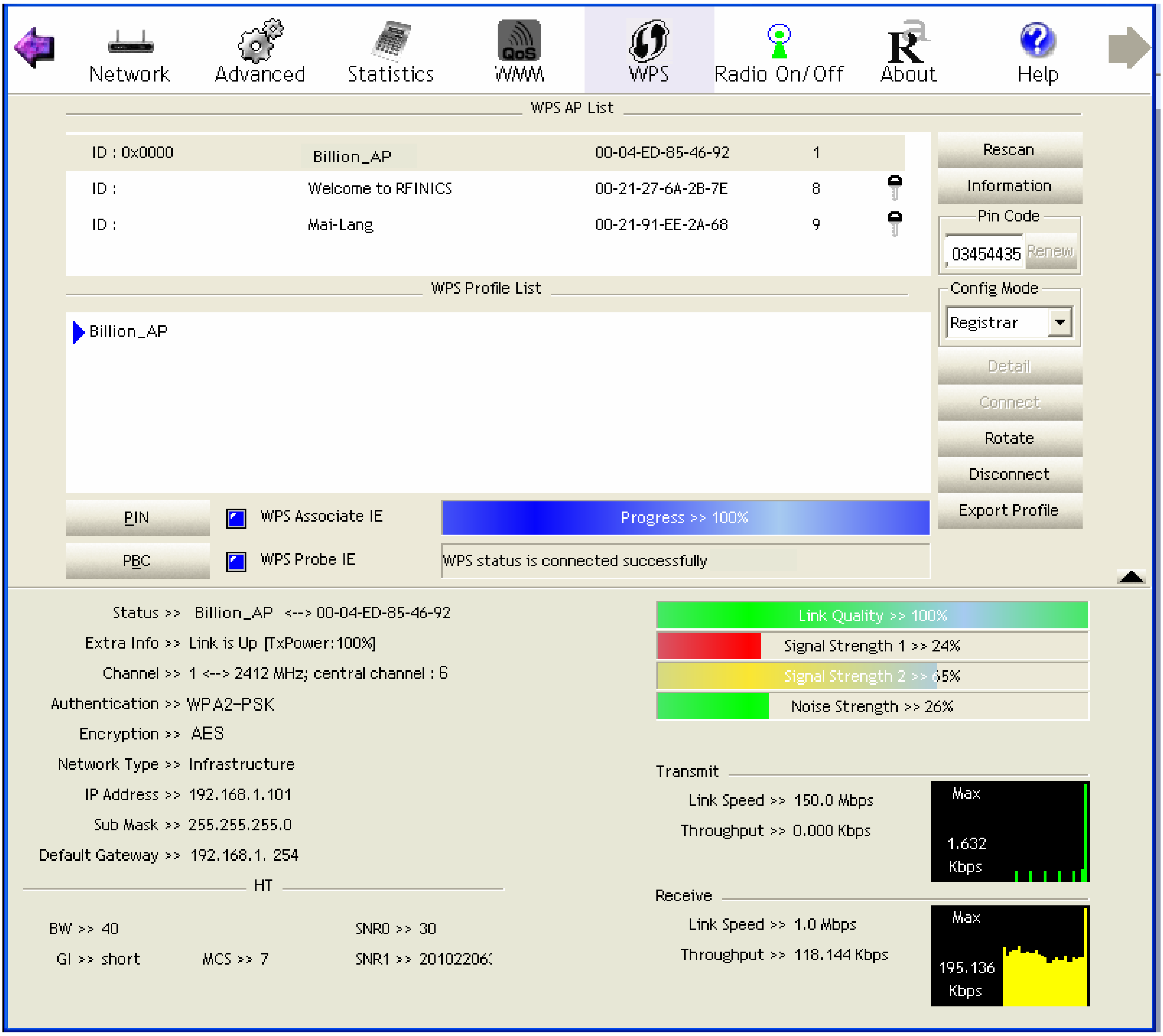
Receive

Link Speed >> 1.0 Mbps

Throughput >> 118.144 Kbps

Max 195.136 Kbps

3. The router’s (AP’s) SSID and security setting will now be configured to match the SSID and security setting of the registrar (client).



WPS AP List

ID : 0x0000	Billion_AP	00-04-ED-85-46-92	1	
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8	
ID :	Mai-Lang	00-21-91-EE-2A-68	9	

Pin Code: 03454435

Config Mode: Registrar

WPS Profile List

Billion_AP

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfully

Status >> Billion_AP <--> 00-04-ED-85-46-92
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 6
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192.168.1.101
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1. 254

HT

BW >> 40
GI >> short
MCS >> 7
SNR0 >> 30
SNR1 >> 20102206:

Link Quality >> 100%
Signal Strength 1 >> 24%
Signal Strength 2 >> 65%
Noise Strength >> 26%

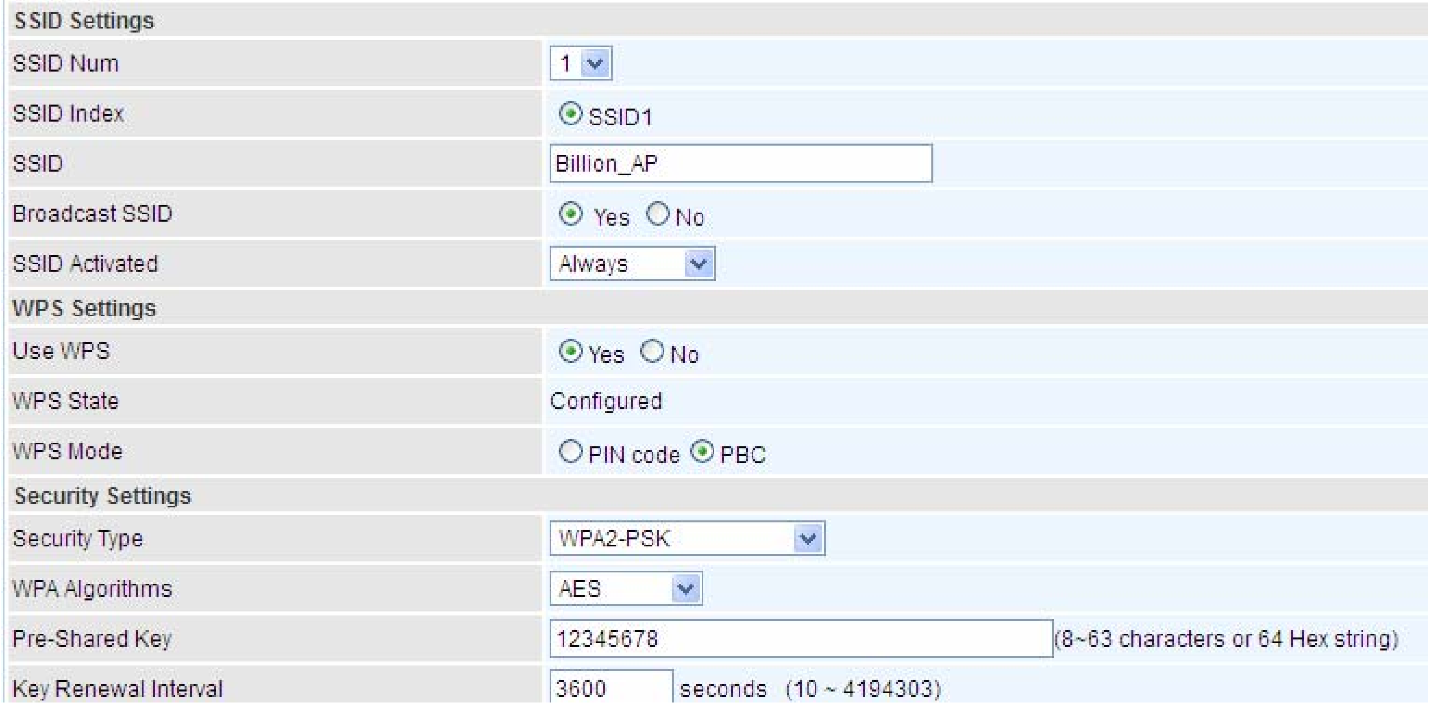
Transmit
Link Speed >> 150.0 Mbps
Throughput >> 0.000 Kbps
1.632 Kbps

Receive
Link Speed >> 1.0 Mbps
Throughput >> 118.144 Kbps
195.136 Kbps

4. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.

PBC Method:

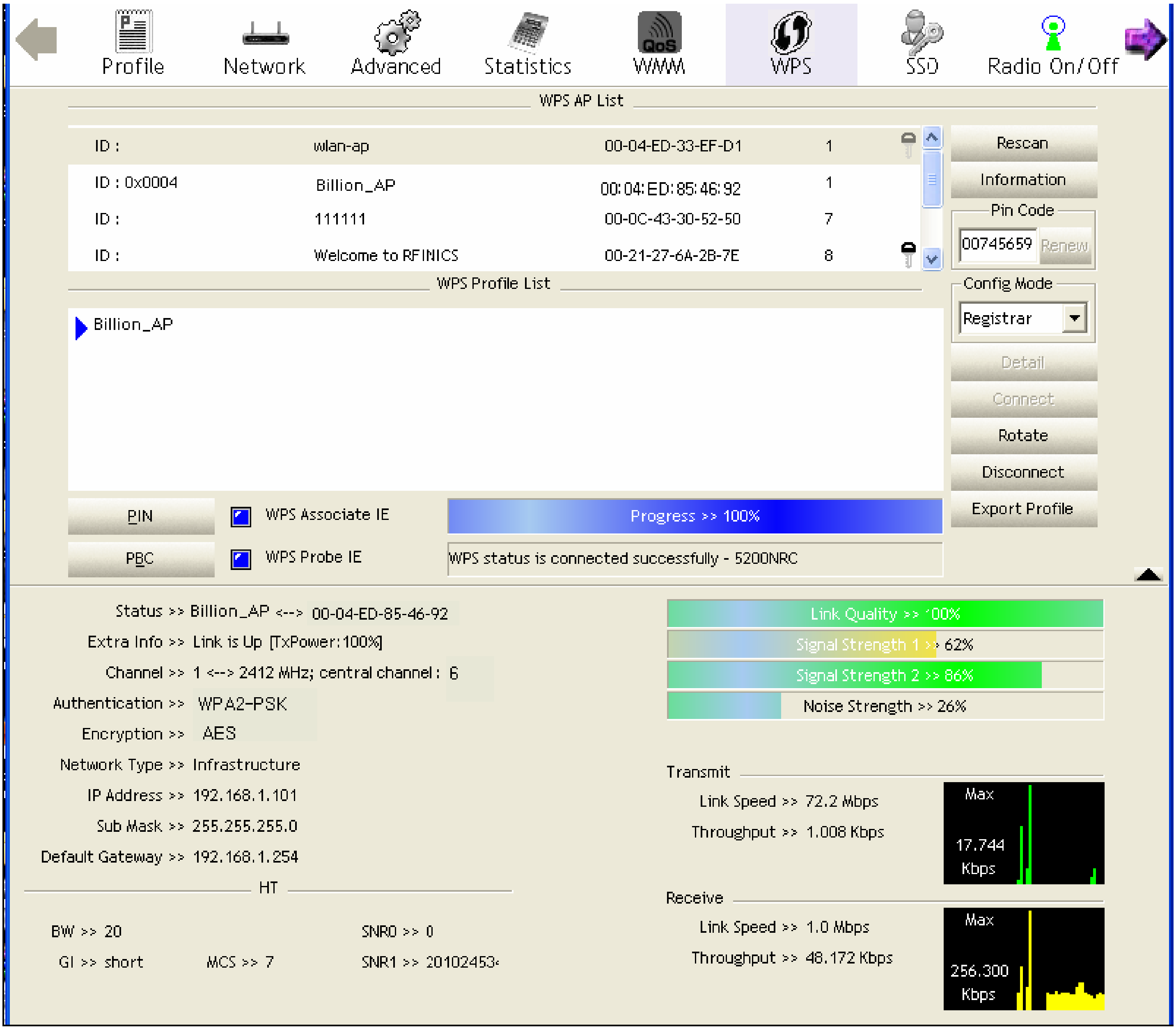
1. Press the PBC radio button, Then Start WPS.



SSID Settings	
SSID Num	1
SSID Index	● SSID1
SSID	Billion_AP
Broadcast SSID	● Yes ○ No
SSID Activated	Always
WPS Settings	
Use WPS	● Yes ○ No
WPS State	Configured
WPS Mode	○ PIN code ● PBC
Security Settings	
Security Type	WPA2-PSK
WPA Algorithms	AES
Pre-Shared Key	12345678 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

2. Launch the wireless client’s WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. Billion_AP) from the WPS AP List section before pressing the PBC button to run the scan.

3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.



WPS AP List

```
ID :           wlan-ap              00-04-ED-33-EF-D1   1
ID : 0x0004    Billion_AP           00:04:ED:85:46:92   1
ID :           111111               00-0C-43-30-52-50   7
ID :           Welcome to RFINICS   00-21-27-6A-2B-7E   8
```

Pin Code: 00745659

Config Mode: Registrar

WPS Profile List

- Billion_AP

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfully - 5200NRC

```
               Status >> Billion_AP <--> 00-04-ED-85-46-92
           Extra Info >> Link is Up [TxPower:100%]
              Channel >> 1 <--> 2412 MHz; central channel : 6
       Authentication >> WPA2-PSK
           Encryption >> AES
         Network Type >> Infrastructure
           IP Address >> 192.168.1.101
             Sub Mask >> 255.255.255.0
      Default Gateway >> 192.168.1.254
```

HT

```
BW >> 20                          SNR0 >> 0
GI >> short       MCS >> 7        SNR1 >> 20102453‹
```

Link Quality >> 100%

Signal Strength 1 >> 62%

Signal Strength 2 >> 86%

Noise Strength >> 26%

Transmit

```
Link Speed >> 72.2 Mbps
Throughput >> 1.008 Kbps
```

Max 17.744 Kbps

Receive

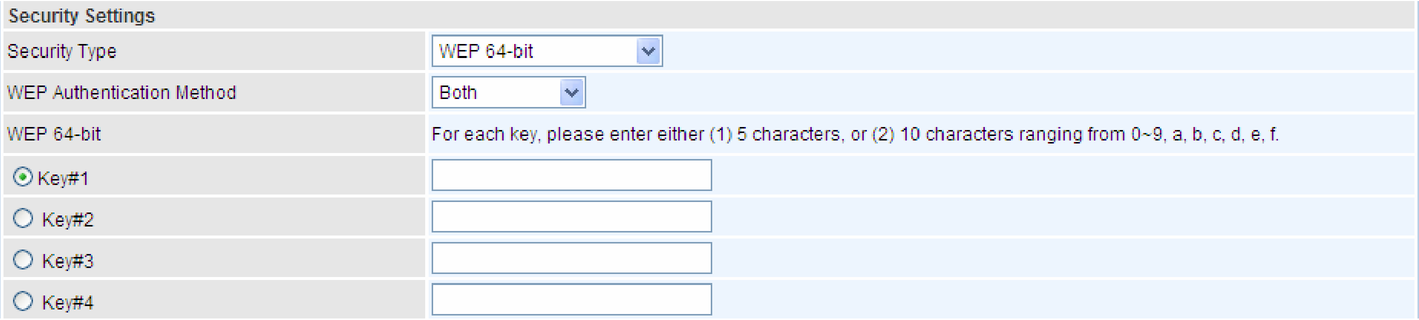
```
Link Speed >> 1.0 Mbps
Throughput >> 48.172 Kbps
```

Max 256.300 Kbps

Security Settings

Security Type: You can disable or enable wireless security for protecting wireless network. The default type of wireless security is OPEN and to allow all wireless stations to communicate with the access points without any data encryption.
To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP and WPA.
There are five alternatives to select from: WEP 64-bit, WEP 128-bit, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK. If you require high security for transmissions, please select WPA-PSK, WPA2-PSK or WPA/WPA2-PSK.

➢ WEP



Security Settings	
Security Type	WEP 64-bit
WEP Authentication Method	Both
WEP 64-bit	For each key, please enter either (1) 5 characters, or (2) 10 characters ranging from 0~9, a, b, c, d, e, f.
● Key#1	
○ Key#2	
○ Key#3	
○ Key#4	

WEP Authentication Method: WEP authentication method, there are two methods of authentication used, Open System authentication (OPENWEB) and Share Key authentication (SHAREDWEB). We suggest you select OPENWEB.

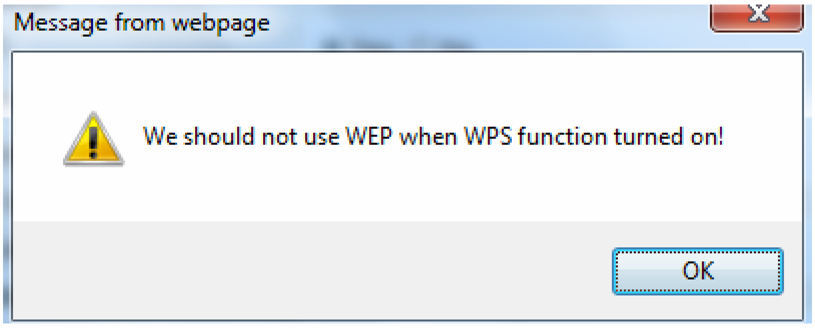
Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP and 128-bitWEP respectively.

If you chose **WEP 64-bit**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

If you chose **WEP 128-bit**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.

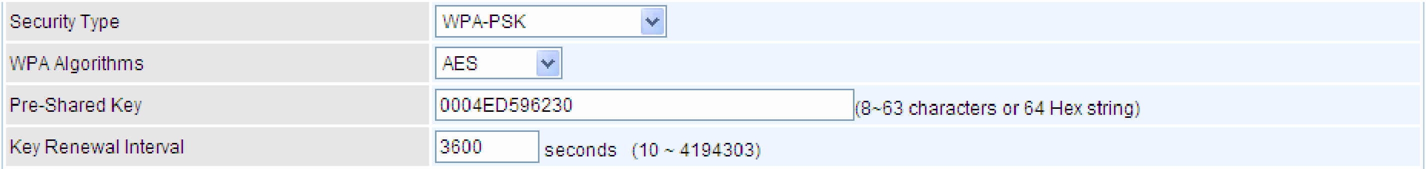
Note: When you enable **WPS** function, this **WEP** function will be invalid. And if you select one of **WEP-64Bits/ WEP-128Bits,** the following prompt box will appear to notice you.



Message from webpage

We should not use WEP when WPS function turned on!

➢ WPA-PSK & WPA2-PSK



Security Type	WPA-PSK
WPA Algorithms	AES
Pre-Shared Key	0004ED596230 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption System) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

Pre-Shared key: The key for network authentication. The input format should be 8-63 ASKII characters or 64 hexadecimal characters

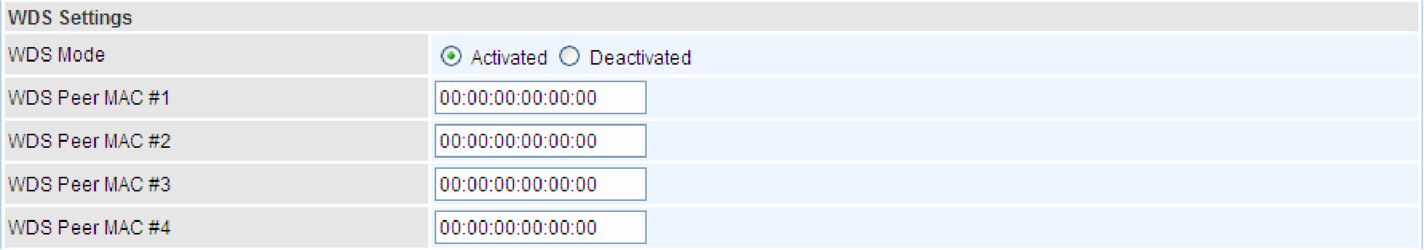
Key Renewal Interval: The time interval for changing the security key automatically between wireless client and AP.

WDS Settings

WDS (Wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, just define the peer's MAC of the connected AP.

WDS Mode: select Activated to enable WDS feature and Deactivated to disable this feature.

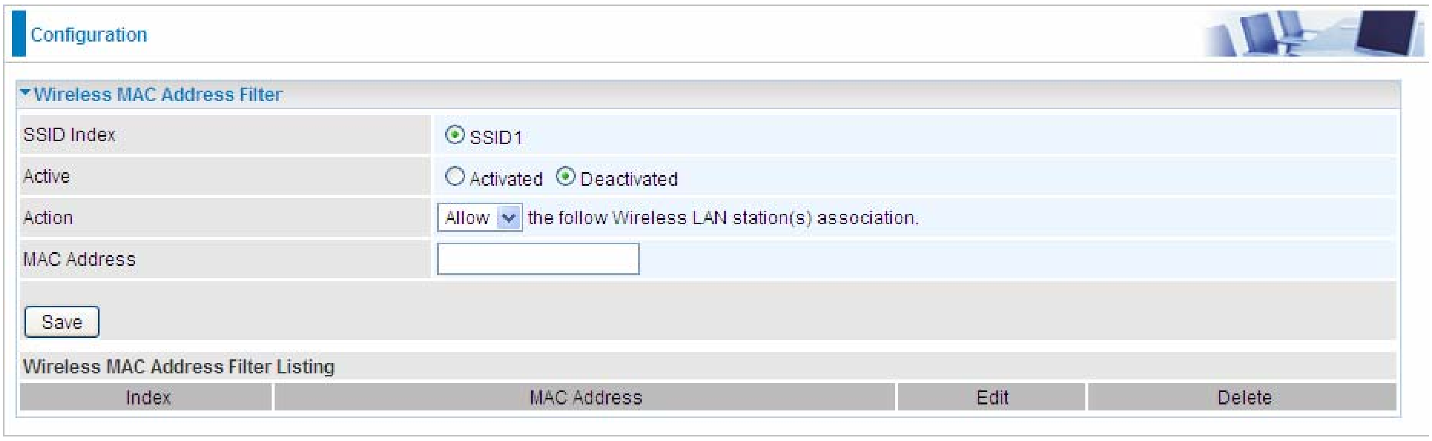
MAC Address: Enter the AP MAC addresses (in XX:XX:XX:XX:XX:XX format) of the peer connected AP.



WDS Settings	
WDS Mode	● Activated ○ Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00

4.4.1.4 Wireless MAC Filter

The MAC filter screen allows you to configure the router to give exclusive access to up to 8 devices (Allow Association) or exclude up to 8 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02. You need to know the MAC address of the devices to configure this screen.



Configuration

▾Wireless MAC Address Filter

SSID Index	● SSID1
Active	○ Activated ● Deactivated
Action	Allow ▾ the follow Wireless LAN station(s) association.
MAC Address	

Save

Wireless MAC Address Filter Listing

Index	MAC Address	Edit	Delete

SSID Index: Select the targeted SSID you want the MAC filter rules to apply to.

Active: Select **Activated** to enable MAC address filtering.

Action: Define the filter action for the list of MAC addresses in the MAC address filter table.

Select **Deny** to block access to the AP, MAC addresses not listed will be allowed to access the router. Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.

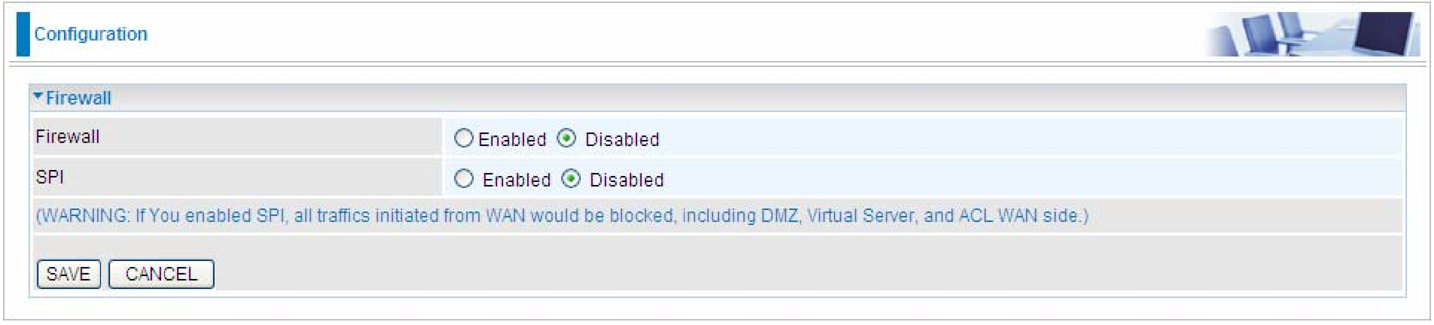
MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the specified in these address fields.

4.4.2 Advanced Setup

Advanced Step provides some advanced features including **Firewall**, **Routing**, **NAT**, **Static DNS**, **QoS**, **Internet Grouping**, **Port Isolation** and **Time Schedule** for all advanced users. Please move on to have a picture of what the exact feature is about and how to use it.

4.4.2.1 Firewall

Your router includes a firewall for helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.



Configuration

▾Firewall

Firewall	○ Enabled ● Disabled
SPI	○ Enabled ● Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

Firewall: To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

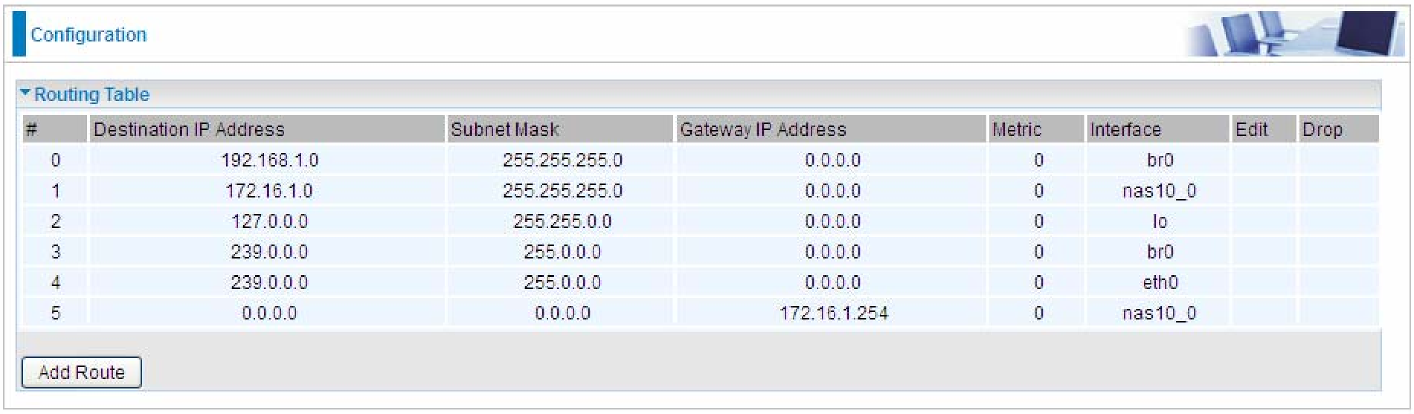
- **Enabled:** It activates your firewall function.
- **Disabled:** It disables the firewall function.

SPI: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

- **Enabled:** It activates your SPI function.
- **Disabled:** It disables the SPI function.

4.4.2.2 Routing

This is static route feature. You are equipped with the capability to control the routing of all the traffic across your network. With each routing rule created, user can specifically assign the destination where the traffic will be routed to.



#	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
1	172.16.1.0	255.255.255.0	0.0.0.0	0	nas10_0		
2	127.0.0.0	255.255.0.0	0.0.0.0	0	lo		
3	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		
4	239.0.0.0	255.0.0.0	0.0.0.0	0	eth0		
5	0.0.0.0	0.0.0.0	172.16.1.254	0	nas10_0		

#: Item number

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

Gateway IP Address: IP address of the gateway or existing interface that this route uses.

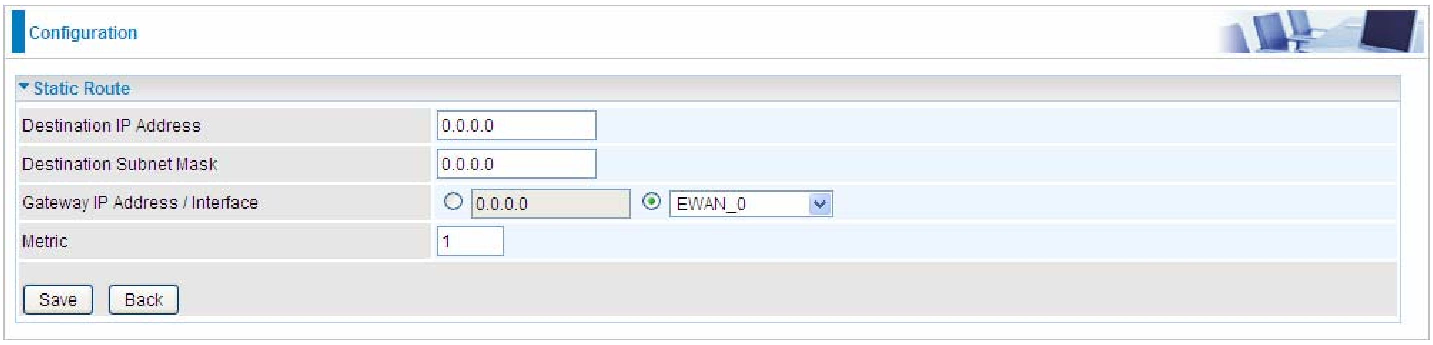
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Interface: Media/channel selected to append the route.

Edit: Edit the route; this icon is not shown for system default route.

Drop: Drop the route; this icon is not shown for system default route.

ADD Route



Configuration

Static Route

Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Gateway IP Address / Interface	○ 0.0.0.0 ● EWAN_0
Metric	1

Destination IP Address: This is the destination subnet IP address.

Destination Subnet Mask: The subnet mask of destination network.

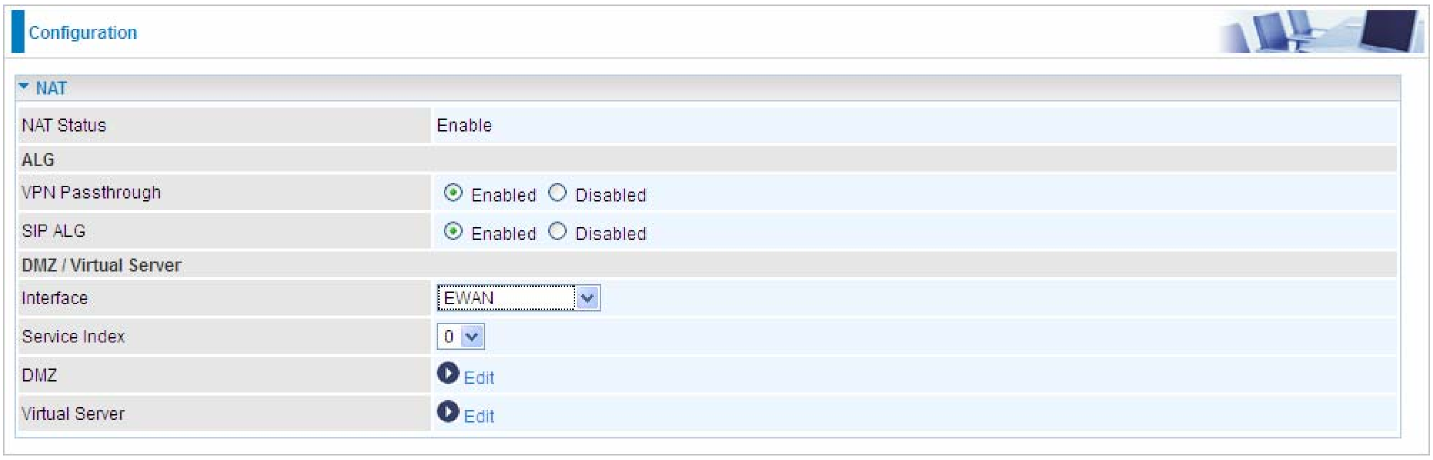
Gateway IP Address/Interface：This is the gateway IP address or existing interface to which packets are to be forwarded.

Metric：It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

4.4.2.3 NAT

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

In this session, there are “VPN Passthrough”, “SIP ALG”, “DMZ” and “Virtual Server” provided to solve these nasty problems.



Configuration

▾ NAT

NAT Status	Enable
ALG	
VPN Passthrough	● Enabled ○ Disabled
SIP ALG	● Enabled ○ Disabled
DMZ / Virtual Server	
Interface	EWAN
Service Index	0
DMZ	Edit
Virtual Server	Edit

NAT Status: Enabled. It depends on ISP Connection Type in Internet settings.

VPN Passthrough: VPN pass-through is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

SIP ALG: Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP ALG when SIP phone includes NAT-Traversal algorithm.

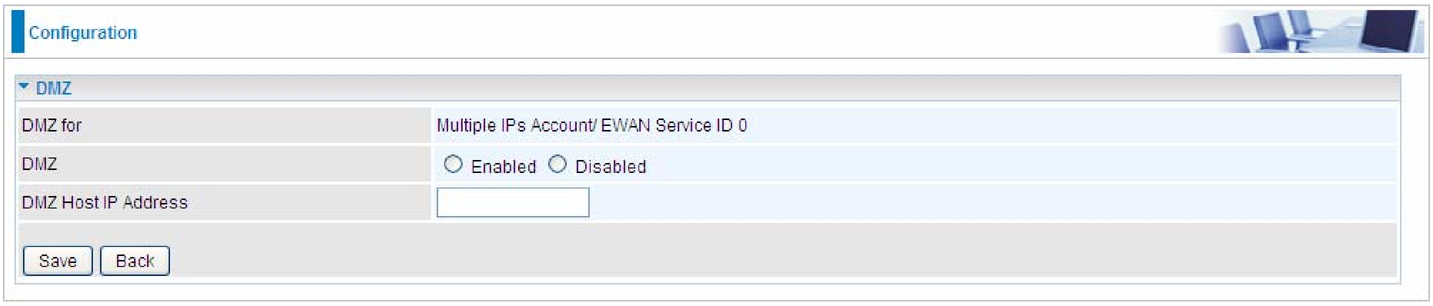
Interface: Select to set DMZ/Virtual Server for “EWAN”.

Service Index: Associated to EWAN interface marking each EWAN service (0-7), to select which EWAN service the DMZ and Virtual server are applied to.

Click **DMZ** Edit or **Virtual Server** Edit to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.



Configuration

▾ DMZ

DMZ for	Multiple IPs Account/ EWAN Service ID 0
DMZ	○ Enabled ○ Disabled
DMZ Host IP Address	

DMZ for: Indicate the related WAN interface which allows outside network to connect in and communicate. **Note:** Here you can see the Multiple IPs Account/EWAN Service ID 0. It is the interface set in the previous NAT page.

DMZ:

- **Enabled:** It activates your DMZ function.
- **Disabled:** It disables the DMZ function.

DMZ Host IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Select the **Save** button to apply your changes.

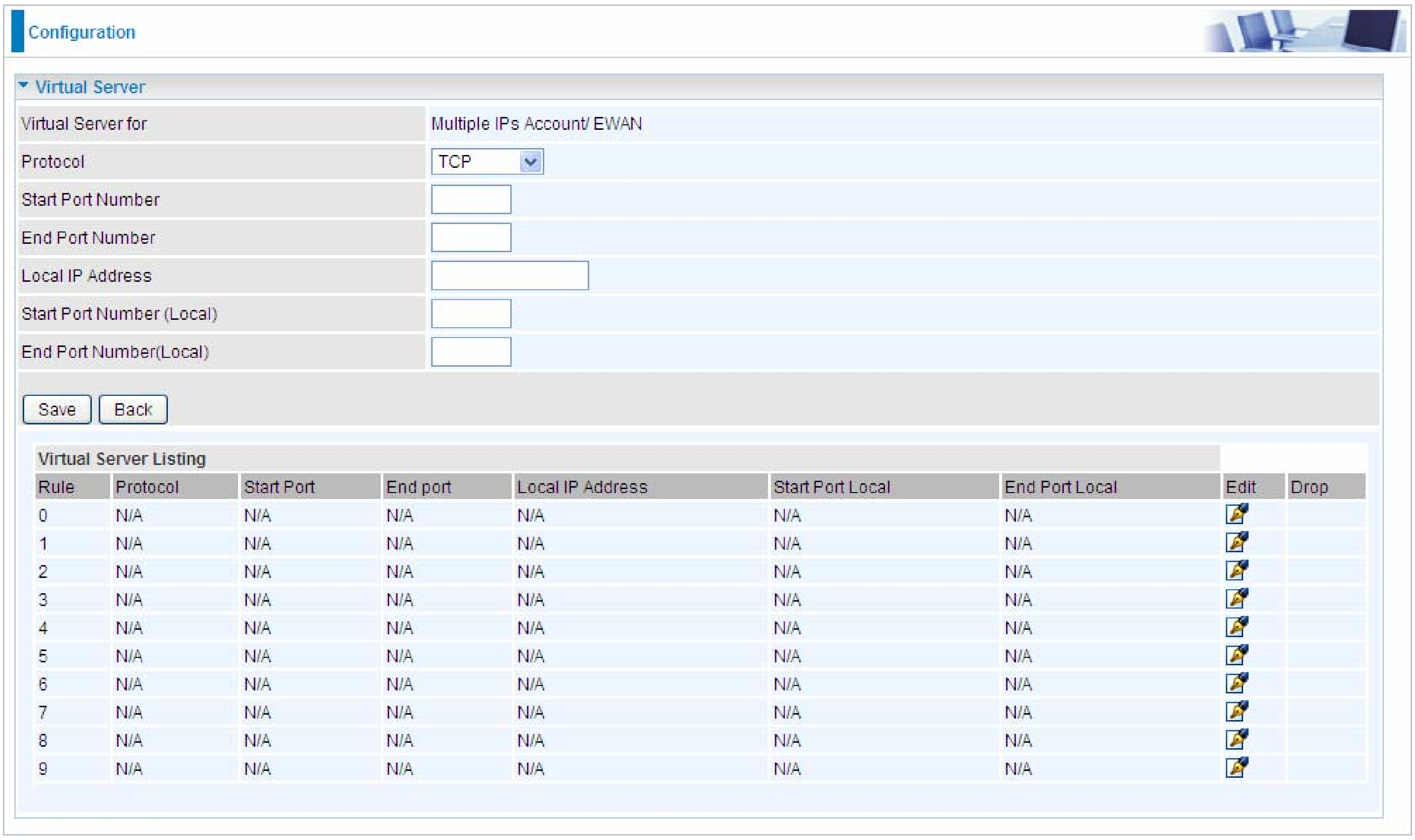
Virtual Server

In TCP/IP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.



Configuration

▾ Virtual Server

Virtual Server for	Multiple IPs Account/ EWAN
Protocol	TCP
Start Port Number	
End Port Number	
Local IP Address	
Start Port Number (Local)	
End Port Number(Local)	

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	N/A	N/A	N/A	N/A	N/A	N/A	✎	
1	N/A	N/A	N/A	N/A	N/A	N/A	✎	
2	N/A	N/A	N/A	N/A	N/A	N/A	✎	
3	N/A	N/A	N/A	N/A	N/A	N/A	✎	
4	N/A	N/A	N/A	N/A	N/A	N/A	✎	
5	N/A	N/A	N/A	N/A	N/A	N/A	✎	
6	N/A	N/A	N/A	N/A	N/A	N/A	✎	
7	N/A	N/A	N/A	N/A	N/A	N/A	✎	
8	N/A	N/A	N/A	N/A	N/A	N/A	✎	
9	N/A	N/A	N/A	N/A	N/A	N/A	✎	

Virtual Server for: Indicate the related WAN interface which allows outside network to connect in and communicate.

Protocol: Choose the application protocol.

Start Port Number: Enter a port number as the starting number of the range which you want to give access to internal server.

End Port Number: Enter a port number as the end number of the range which you want to give access to internal server..

Local IP Address: Enter your server IP address in this field.

Start Port Number (Local): Please enter the start port number of the local application (service).

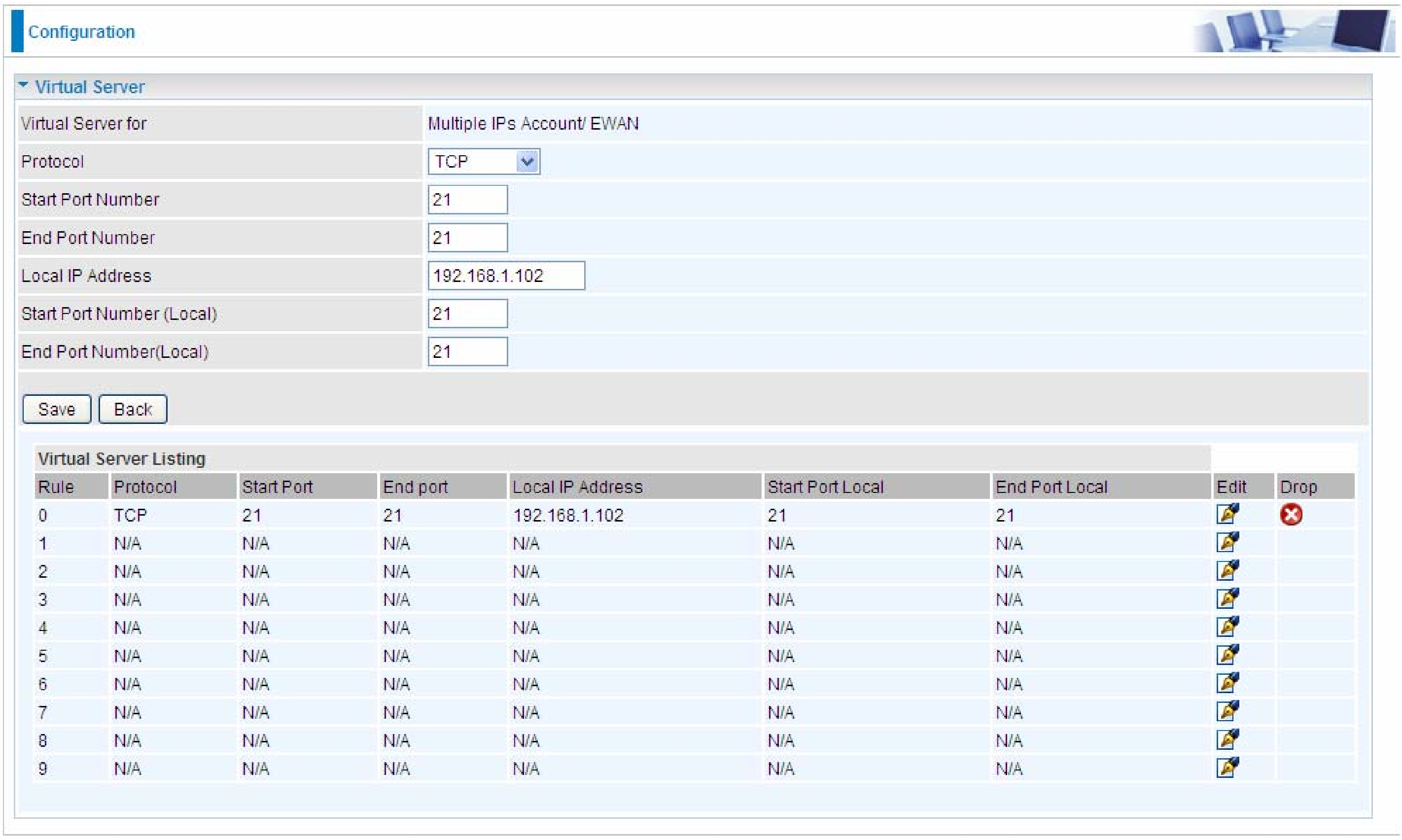
End Port Number (Local): Please enter the end port number of the local application (service).

Examples of well-known and registered port numbers are shown below. For further information, please see IANA's website at http://www.iana.org/assignments/port-numbers

Well-known and Registered Ports

Port Number	Protocol	Description
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
7070	UDP	RealAudio

If you have a FTP server in your LAN network, and want to be accessing through WAN, you can have it set as virtual server.



Virtual Server for	Multiple IPs Account/ EWAN
Protocol	TCP
Start Port Number	21
End Port Number	21
Local IP Address	192.168.1.102
Start Port Number (Local)	21
End Port Number(Local)	21

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.102	21	21	✎	⊗
1	N/A	N/A	N/A	N/A	N/A	N/A	✎	
2	N/A	N/A	N/A	N/A	N/A	N/A	✎	
3	N/A	N/A	N/A	N/A	N/A	N/A	✎	
4	N/A	N/A	N/A	N/A	N/A	N/A	✎	
5	N/A	N/A	N/A	N/A	N/A	N/A	✎	
6	N/A	N/A	N/A	N/A	N/A	N/A	✎	
7	N/A	N/A	N/A	N/A	N/A	N/A	✎	
8	N/A	N/A	N/A	N/A	N/A	N/A	✎	
9	N/A	N/A	N/A	N/A	N/A	N/A	✎	

Some tips for using DMZ and Virtual Server:

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

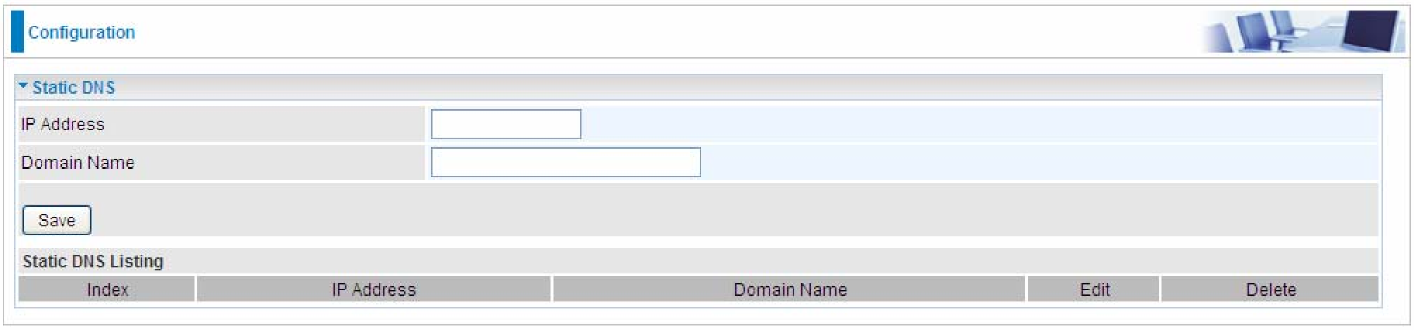
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

4.4.2.4 Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com can be translated into the addresses 192.0.32.10 (IPv4).

Static DNS is a concept relative to Dynamic DNS, in static DNS system, the IP mapped is static without change.



Static DNS Listing

Index	IP Address	Domain Name	Edit	Delete

IP Address: The IP address you are going to give a specific domain name.

Domain Name: The friendly domain name for the IP address.

Press **Save** button to apply your settings.

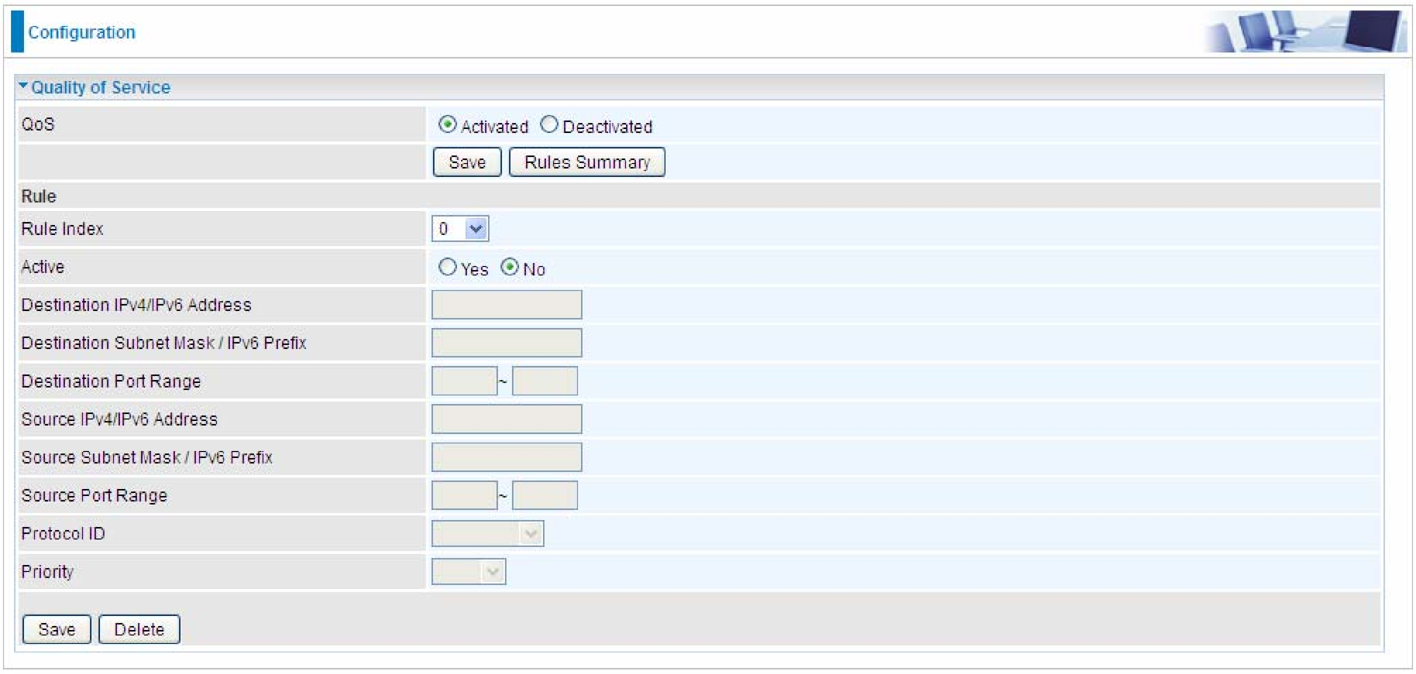
4.4.2.5 QoS

QoS helps you control the upload traffic of each application from LAN(Ethernet and/or Wireless) to WAN (Internet).

It facilitates you the features to control the quality of throughput for each application. This is useful when there on certain types of data you want giver higher priority to, such as voice data packets given higher priority than web data packets.

QoS can be toggled Activated and Deactivated. QoS must be activated before you can edit the following options. When you are done making changes, click on **Save** to save your changes.

Click on **Rule Summary** to view the list of QoS rules that have been added.



Configuration

▾Quality of Service

QoS	● Activated ○ Deactivated
	Save Rules Summary
Rule	
Rule Index	0
Active	○ Yes ● No
Destination IPv4/IPv6 Address	
Destination Subnet Mask / IPv6 Prefix	
Destination Port Range	~
Source IPv4/IPv6 Address	
Source Subnet Mask / IPv6 Prefix	
Source Port Range	~
Protocol ID	
Priority	

Save   Delete

Rule

You can set 16 different QoS rules. Each QoS rule has its detail setting conditions like: Physical Ports, IP, Port, Protocol, etc, you can modify the value to any new one you wish. Please notice that only when the packet fulfill every detail setting conditions here, then this packet will be remarked as the priority queue of each rule. The non-selected setting part will be treated as “don’t care” and the system will not handle this setting part.

Rule: Select 16 different rules, each rule’s detail can be set and saved.

Active: Select whether to activate the rule.

Destination IPv4/IPv6: Set the IPv4/IPv6 address that you want to filter on destination side.

Destination Subnet Mask / IPv6 Prefix: Specify the Destination Subnet Mask for IPv4 or prefix for IPv6.

Destination Port Range: Set the port range value that you want to filter on destination side.

Source IPv4/IPv6 Address: Set the IP address value that you want to filter on source side in IPv4 or IPv6.

Source Subnet Mask / IPv6 Prefix: Specify the Source Subnet Mask for IPv4 or prefix for IPv6.

Source Port Range: Set the port range value that you want to filter on source side.

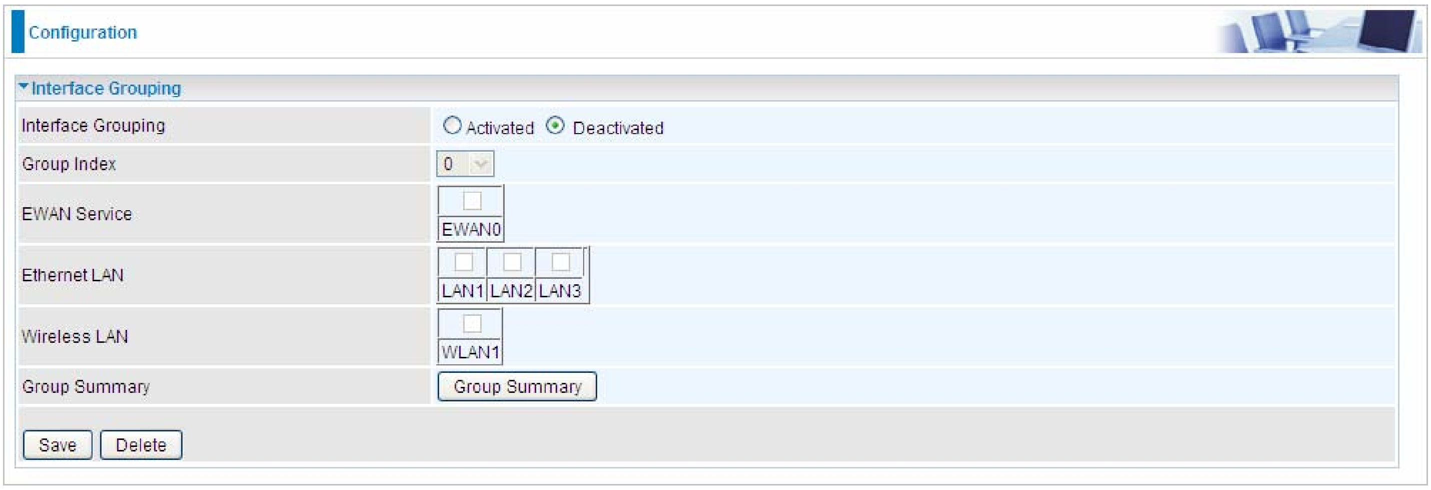
Protocol ID: Set the protocol ID type of packets that you want to filter (TCP, UDP, ICMP, IGMP).

Priority: Select to prioritize the traffic which the rule categorizes. High and Low.

4.4.2.6 Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Similarly, they may also have been split into two different groups, even if they are on the same switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Save** button.



Configuration

Interface Grouping

Interface Grouping	○ Activated ● Deactivated
Group Index	0
EWAN Service	□ EWAN0
Ethernet LAN	□ LAN1 □ LAN2 □ LAN3
Wireless LAN	□ WLAN1
Group Summary	Group Summary

Interface Grouping: Select Yes to enable Interface Grouping feature.

Group Index: The index number indicating the current goup ranging from 0 to 15.

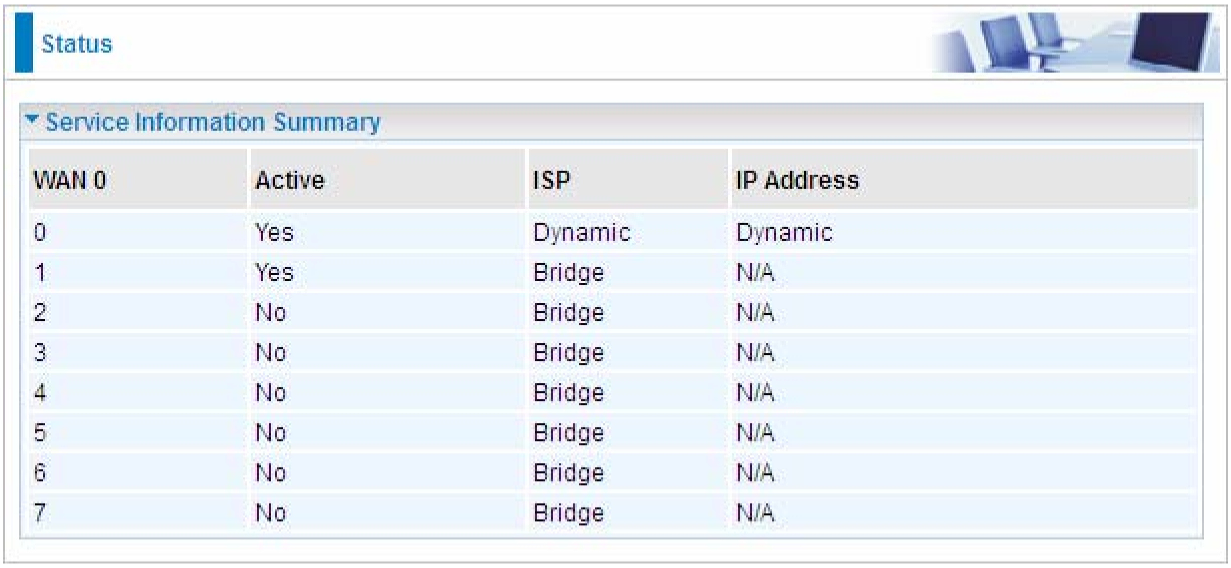
EWAN Service: The available EWAN interface. Move to 4.4.1 Interface Setup to add other EWAN interface.

Ethernet LAN: The available Ethernet ports.

Wireless LAN: The available wireless ports.

Group Summary: Press **PortBinding Summary** to check the current group information.

For example, you can create two EWAN services, Service0(PPPoE) and Service1(Bridge).



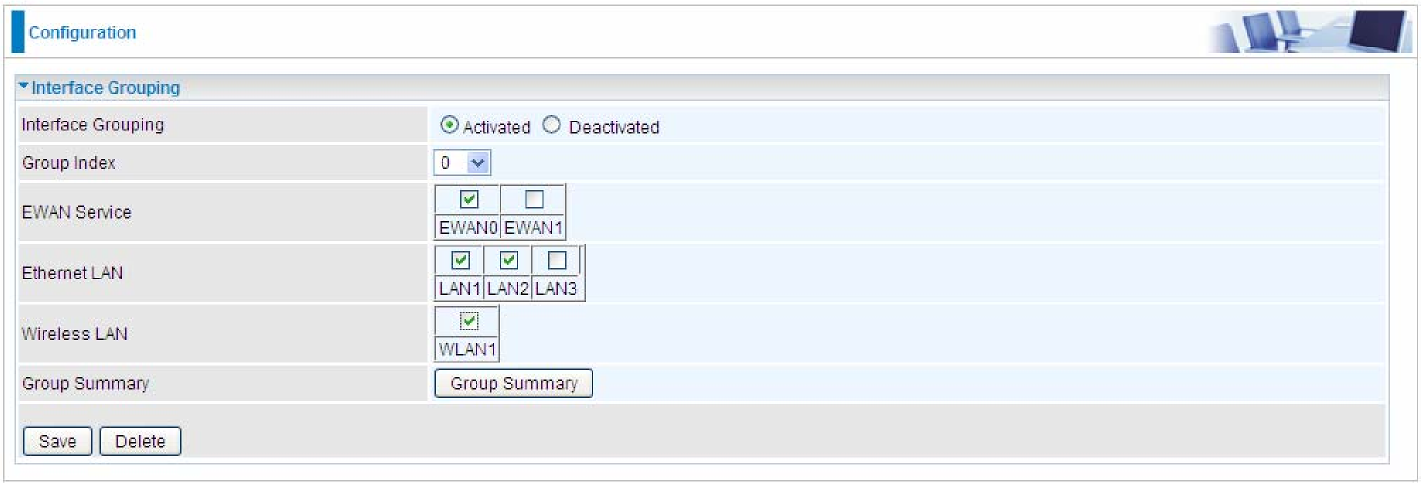
Status

Service Information Summary

WAN 0	Active	ISP	IP Address
0	Yes	Dynamic	Dynamic
1	Yes	Bridge	N/A
2	No	Bridge	N/A
3	No	Bridge	N/A
4	No	Bridge	N/A
5	No	Bridge	N/A
6	No	Bridge	N/A
7	No	Bridge	N/A

You are going to group the ports and services into two working group, as shown below.

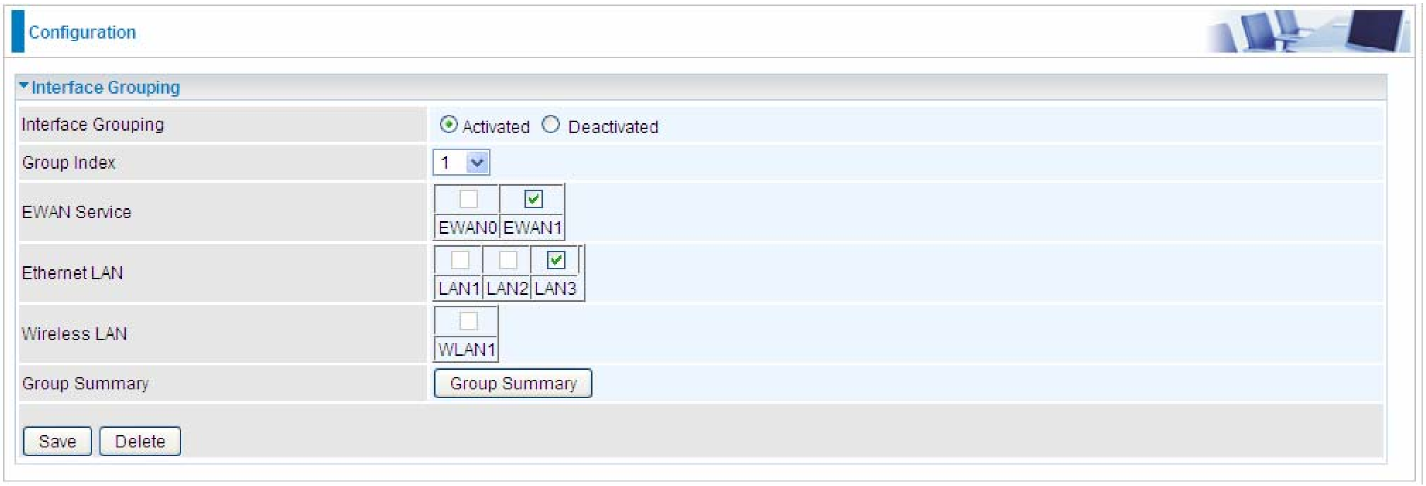
Group Index	Group Port
0	EWAN0,LAN1, LAN2, WLAN1
1	EWAN1, LAN3



Configuration

Interface Grouping

Interface Grouping	● Activated ○ Deactivated
Group Index	0
EWAN Service	☑ EWAN0 □ EWAN1
Ethernet LAN	☑ LAN1 ☑ LAN2 □ LAN3
Wireless LAN	☑ WLAN1
Group Summary	Group Summary

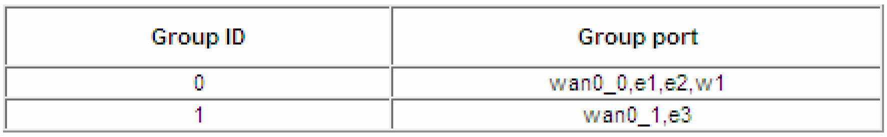


Configuration

Interface Grouping

Interface Grouping	● Activated ○ Deactivated
Group Index	1
EWAN Service	□ EWAN0 ☑ EWAN1
Ethernet LAN	□ LAN1 □ LAN2 ☑ LAN3
Wireless LAN	□ WLAN1
Group Summary	Group Summary

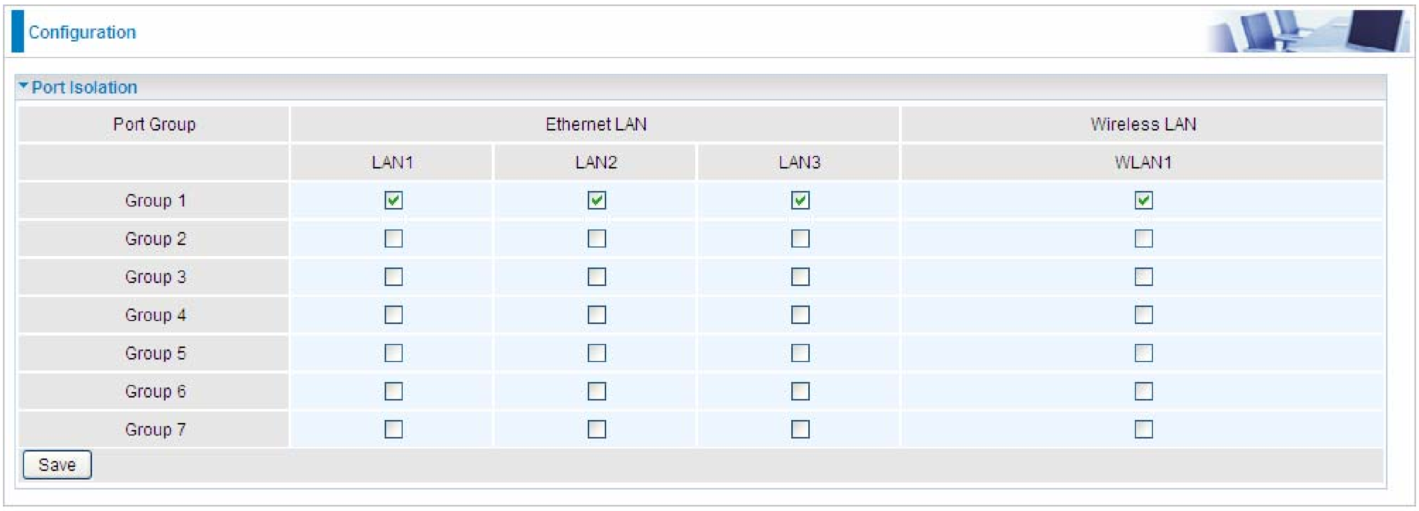
Click **Group Summary** to show the configuration results.



Group ID	Group port
0	wan0_0,e1,e2,w1
1	wan0_1,e3

4.4.2.7 Port Isolation

Port isolation is a mechanism to allow or block devices in one port (indicates the LAN1 - LAN3 and WLAN1 - WLAN4, need to enable multiple SSID in wireless section) to access other devices in other ports. By default, all ports (LAN port and WLAN port) are sharing one group, and devices in all these ports can have access to each other.

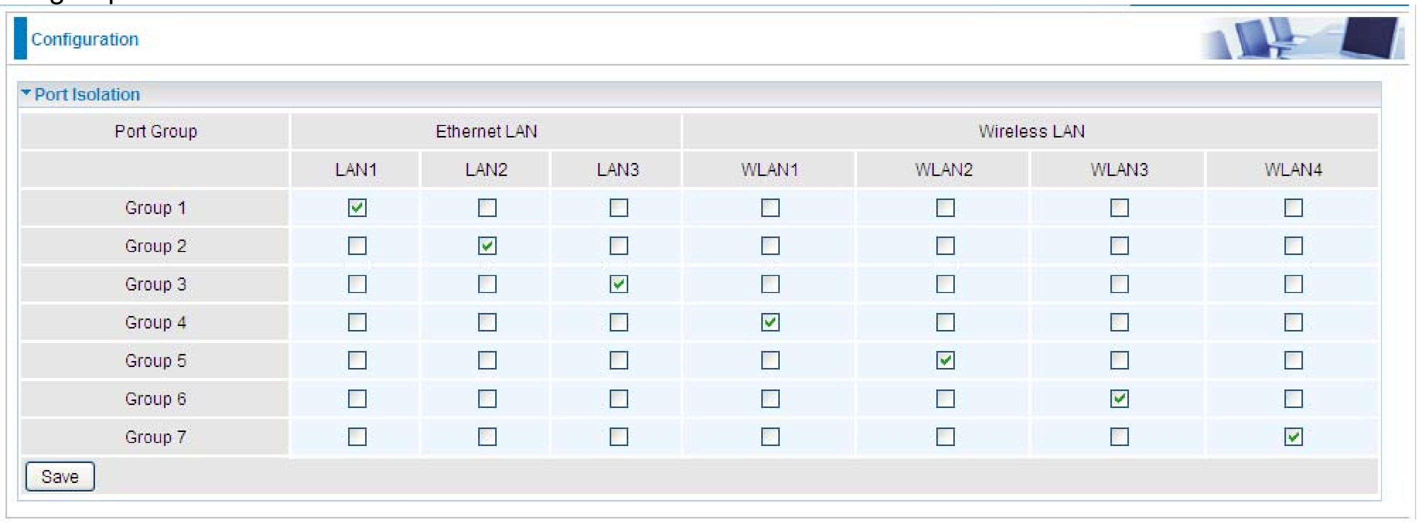


Configuration

Port Isolation

Port Group	Ethernet LAN			Wireless LAN
	LAN1	LAN2	LAN3	WLAN1
Group 1	☑	☑	☑	☑
Group 2	□	□	□	□
Group 3	□	□	□	□
Group 4	□	□	□	□
Group 5	□	□	□	□
Group 6	□	□	□	□
Group 7	□	□	□	□

The most typical one example is to isolate all port from each other shown below. Each port has its own group, under this circumstance, devices connected to each port have no access to other devices connected to other ports. This is a special example, and users can change the settings to determine how the ports are belonged to the group.



Configuration

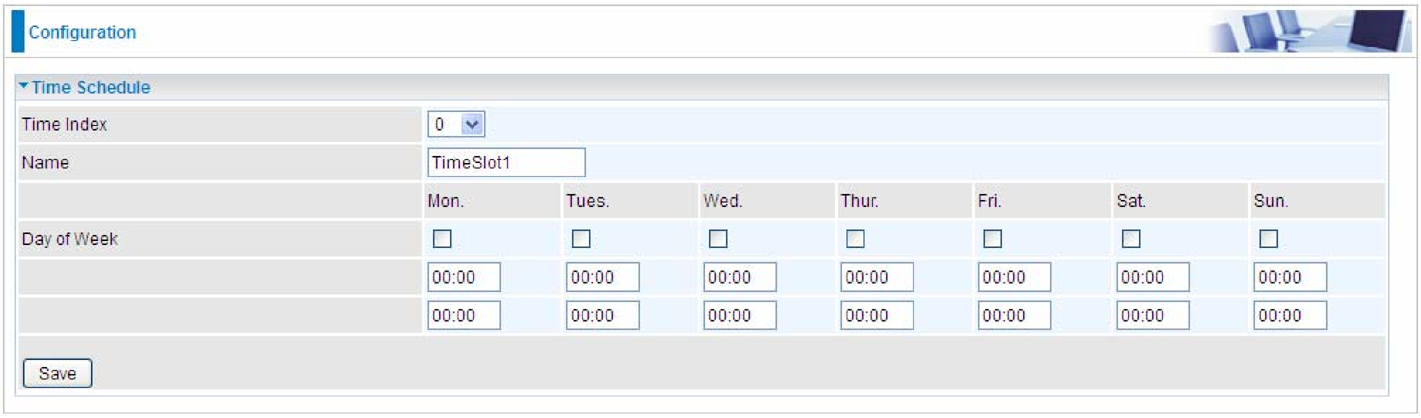
Port Isolation

Port Group	Ethernet LAN			Wireless LAN			
	LAN1	LAN2	LAN3	WLAN1	WLAN2	WLAN3	WLAN4
Group 1	☑	□	□	□	□	□	□
Group 2	□	☑	□	□	□	□	□
Group 3	□	□	☑	□	□	□	□
Group 4	□	□	□	☑	□	□	□
Group 5	□	□	□	□	☑	□	□
Group 6	□	□	□	□	□	☑	□
Group 7	□	□	□	□	□	□	☑

4.4.2.8 Time Schedule

The Time Schedule supports up to **16** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet.



Configuration

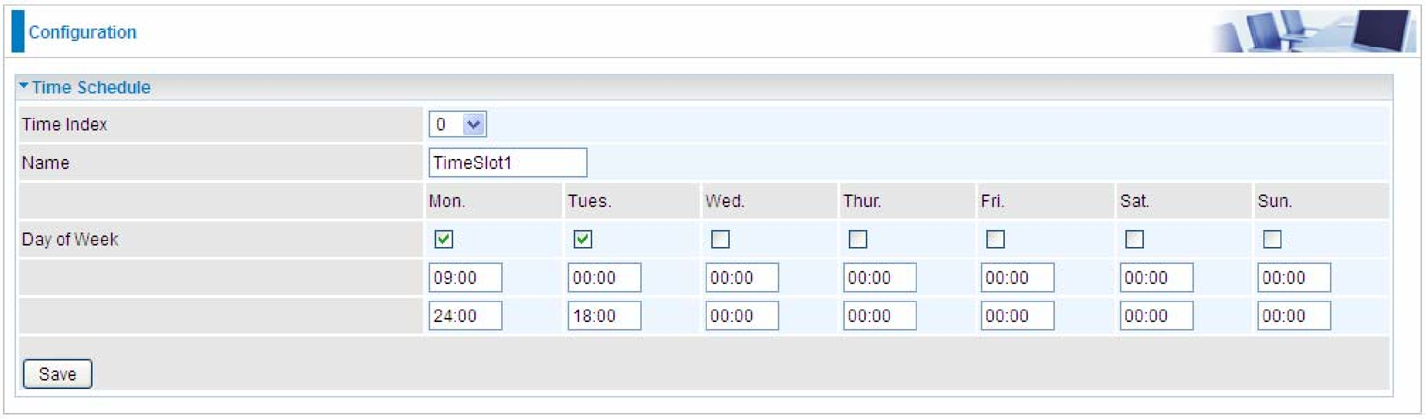
▾Time Schedule

Time Index	0 ▾						
Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	□	□	□	□	□	□	□
	00:00	00:00	00:00	00:00	00:00	00:00	00:00
	00:00	00:00	00:00	00:00	00:00	00:00	00:00

Time Index: The rule index(0-15) for identifying each timeslot.

Name: User-defined identification for each time period.

Day of Week: Mon. to Sun. Specify the time interval for each timeslot from "Day of Week". For example, user can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.

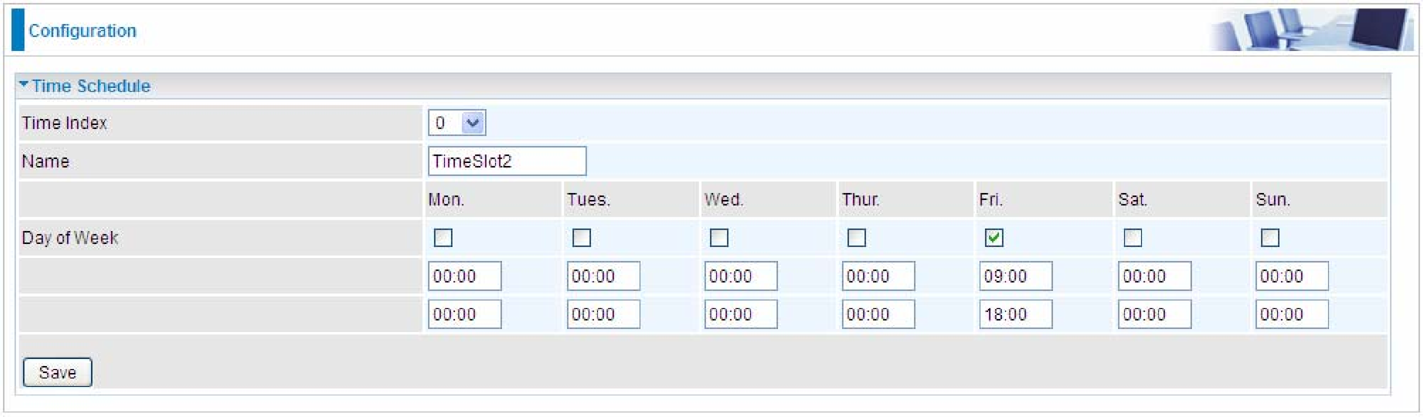


Configuration

▾Time Schedule

Time Index	0 ▾						
Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	☑	☑	□	□	□	□	□
	09:00	00:00	00:00	00:00	00:00	00:00	00:00
	24:00	18:00	00:00	00:00	00:00	00:00	00:00

Another TimeSlot2 spanning from 09:00 to 18:00 of Friday



Configuration

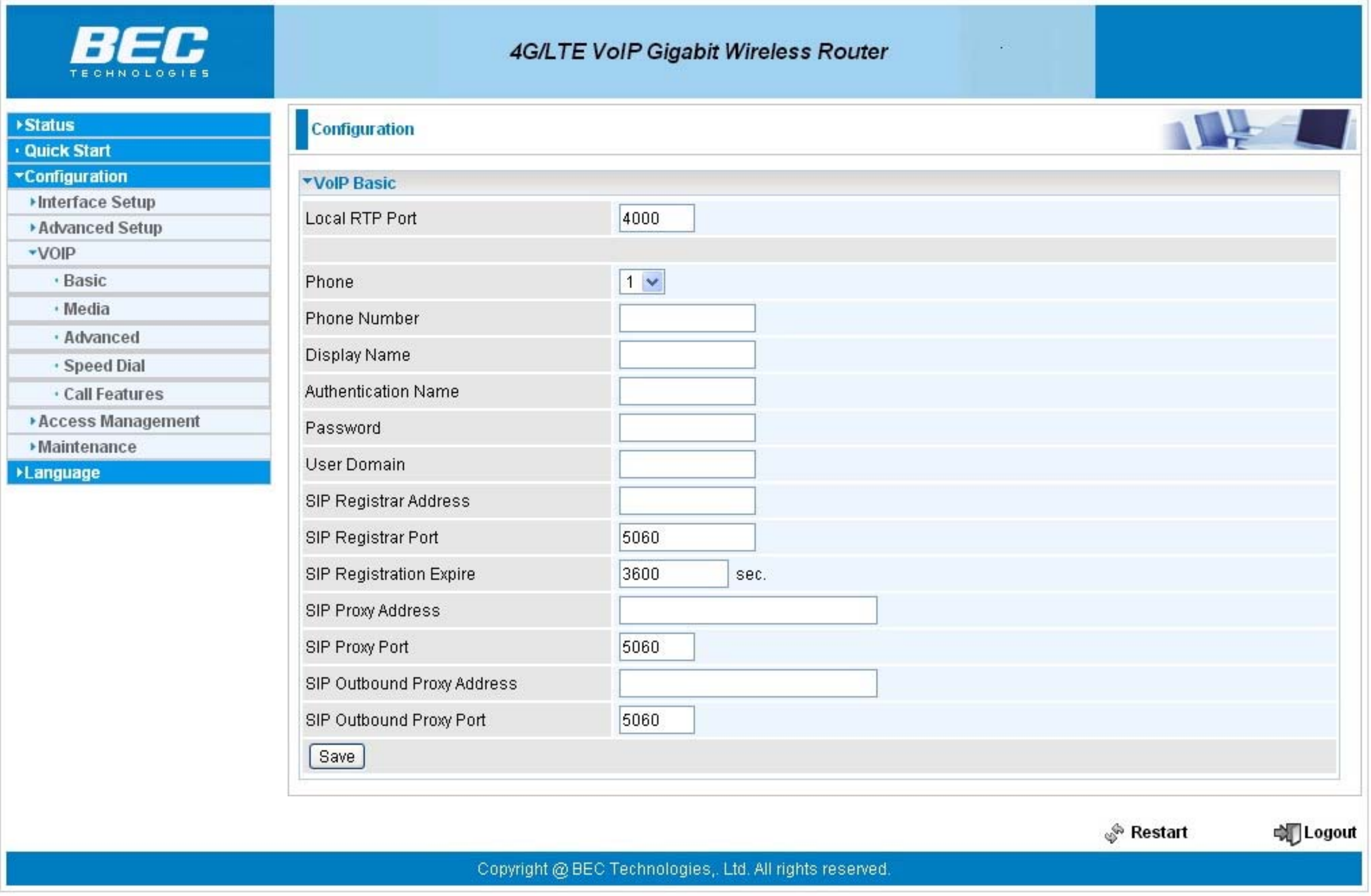
▾Time Schedule

Time Index	0 ▾						
Name	TimeSlot2						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	□	□	□	□	☑	□	□
	00:00	00:00	00:00	00:00	09:00	00:00	00:00
	00:00	00:00	00:00	00:00	18:00	00:00	00:00

4.4.3 VoIP

VoIP, or Voice over Internet Protocol, enables telephone calls through existing internet connections instead of going through the traditional PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long-distance call, but also top quality voice calls over the internet.

Five sub-items to be covered to configure the VoIP feature, namely **Basic**, **Media**, **Advanced**, **Speed Dial**, **Call Features**.



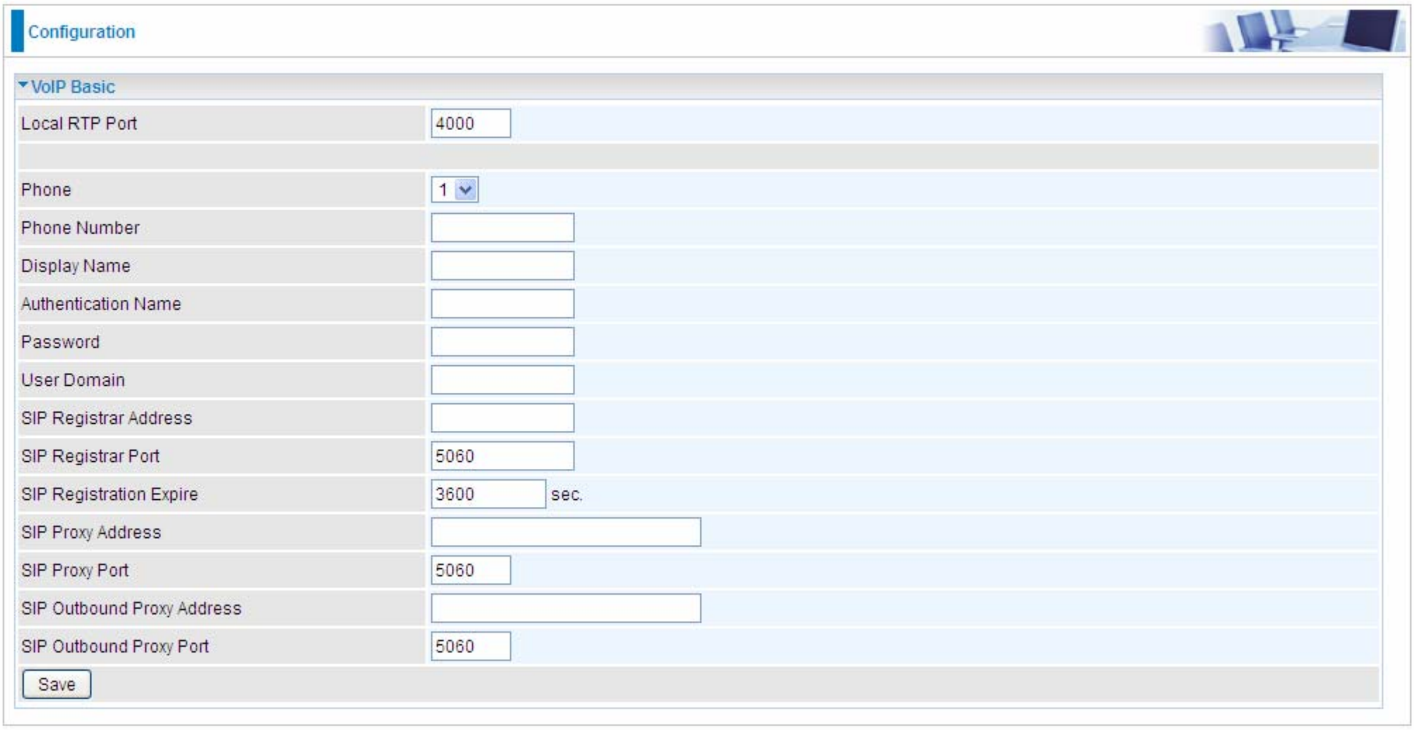
VoIP Basic

Local RTP Port	4000
Phone	1
Phone Number	
Display Name	
Authentication Name	
Password	
User Domain	
SIP Registrar Address	
SIP Registrar Port	5060
SIP Registration Expire	3600 sec.
SIP Proxy Address	
SIP Proxy Port	5060
SIP Outbound Proxy Address	
SIP Outbound Proxy Port	5060

Save

4.4.3.1 Basic

Register to a SIP service provider is an essential step before making the VoIP call. Users can find out SIP service provider, and register a SIP account, jotting down the registration information and configuring in router.



Configuration

VoIP Basic

Local RTP Port	4000
Phone	1
Phone Number	
Display Name	
Authentication Name	
Password	
User Domain	
SIP Registrar Address	
SIP Registrar Port	5060
SIP Registration Expire	3600 sec.
SIP Proxy Address	
SIP Proxy Port	5060
SIP Outbound Proxy Address	
SIP Outbound Proxy Port	5060

Locale RTP Port: Set the local RTP port used to receive voice packet. The setting is to be applied to the two FXS, name phone 1 and phone 2, and the two FXS share the same local RTP port.

Phone: Select “1”, the following parameters will be applicable to Phone1. In 6300VNOZ, phone 1 and phone 2 are allowed to be of different characteristics, including different SIP registrar. So, user needs to configure individually for phone1 and phone 2.

Phone Number: Set you phone number or outgoing call number, which is usually obtained when registering in your ITSP. It is used for destination to identify which this call is made from.

Display Name: A user-friendly display name for the phone number to be easily identified.

Authentication Name: Set the account used to register, usually the Phone Number.

Password: Set the registering account password.

User Domain: Set the SIP Registrar Domain name you are going to register to, usually just the SIP registrar address.

SIP Registrar Address: Enter the SIP registrar address where offers the service of registering the VoIP account. It is definitely a VoIP server.

SIP Registrar Port: Type the port; it will listen to register requests from VoIP devices.

SIP Registration Expire: Set the time interval. The device can update (usually re-login the account) the VoIP account information with the SIP server very the time interval.

SIP Proxy Address: Enter the SIP proxy address provided by your ITSP. When destination and source phones are not sharing the same SIP registrar domain, the SIP proxy is needed to deliver call information and make the communication through.

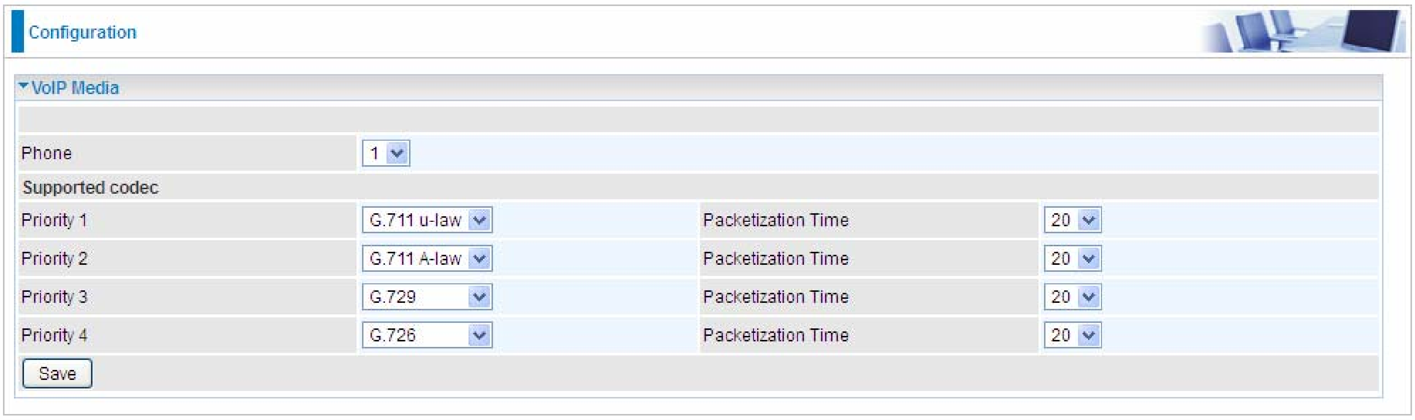
SIP Proxy Port: Set the SIP proxy port.

SIP Outbound Proxy Address: Set the SIP outbound proxy address. It is usually used to realize the communication between two phones when at least one of them is located behind a NAT router.

SIP Outbound Proxy Port: Set the SIP Outbound proxy port.

4.4.3.2 Media

Media offers for kinds of codec, G.711 u-law, G.711 A-law, G.729, G.726, from greatest to lowest in priority.



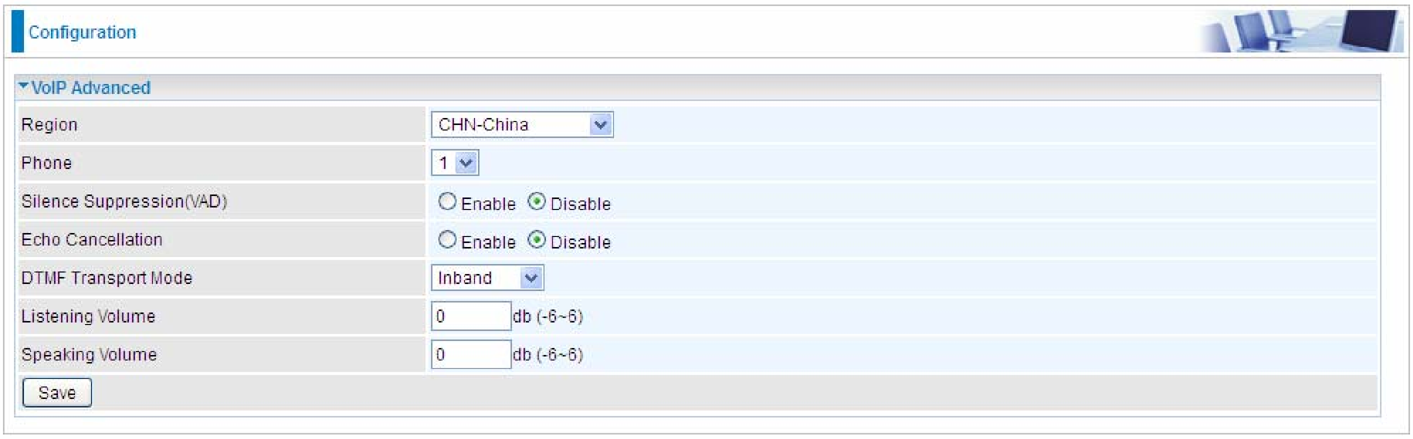
Phone	1		
Supported codec			
Priority 1	G.711 u-law	Packetization Time	20
Priority 2	G.711 A-law	Packetization Time	20
Priority 3	G.729	Packetization Time	20
Priority 4	G.726	Packetization Time	20

Phone: Select to set the following configurations for Phone 1 or Phone2. When phone1 is selected, the following set media codec will be applied to phone1.

- **G.711u-Law:** It is a basic non-compressed encoder and decoder technique. μ-LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample.
- **G.711A-LAW:** It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample into 8-bit value.
- **G.729**: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.
- **G.726:** It is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 32kbit/s.

4.4.3.3 Advanced

Advance section equipement the users with the ability to do some advanced settings to each phone port. Go on to see.



Configuration

VoIP Advanced

Region	CHN-China
Phone	1
Silence Suppression(VAD)	○ Enable ● Disable
Echo Cancellation	○ Enable ● Disable
DTMF Transport Mode	Inband
Listening Volume	0 db (-6~6)
Speaking Volume	0 db (-6~6)

Region: Select the exact region from the drop-down menu to adjust the phone custom in the exact region, like ring tone, busy tone, dial tone, etc, as different regions may have different phone using traditions. The setting is to be applied to both phone 1 and phone 2.

Phone: Select the phone 1 or Phone 2 to have the following configurations applied to the phone.

Silence Suppression (VAD): Enable to minimize the use of bandwidth by automatically decreasing transmission of background noise when the device detects on voice input by the user on the phone.

Echo Cancellation: Enable to cancel echo for the other side in communication so as to make a clear listening environment. In order to avoid the other side in communication hearing the echo, please enable echo cancellation.

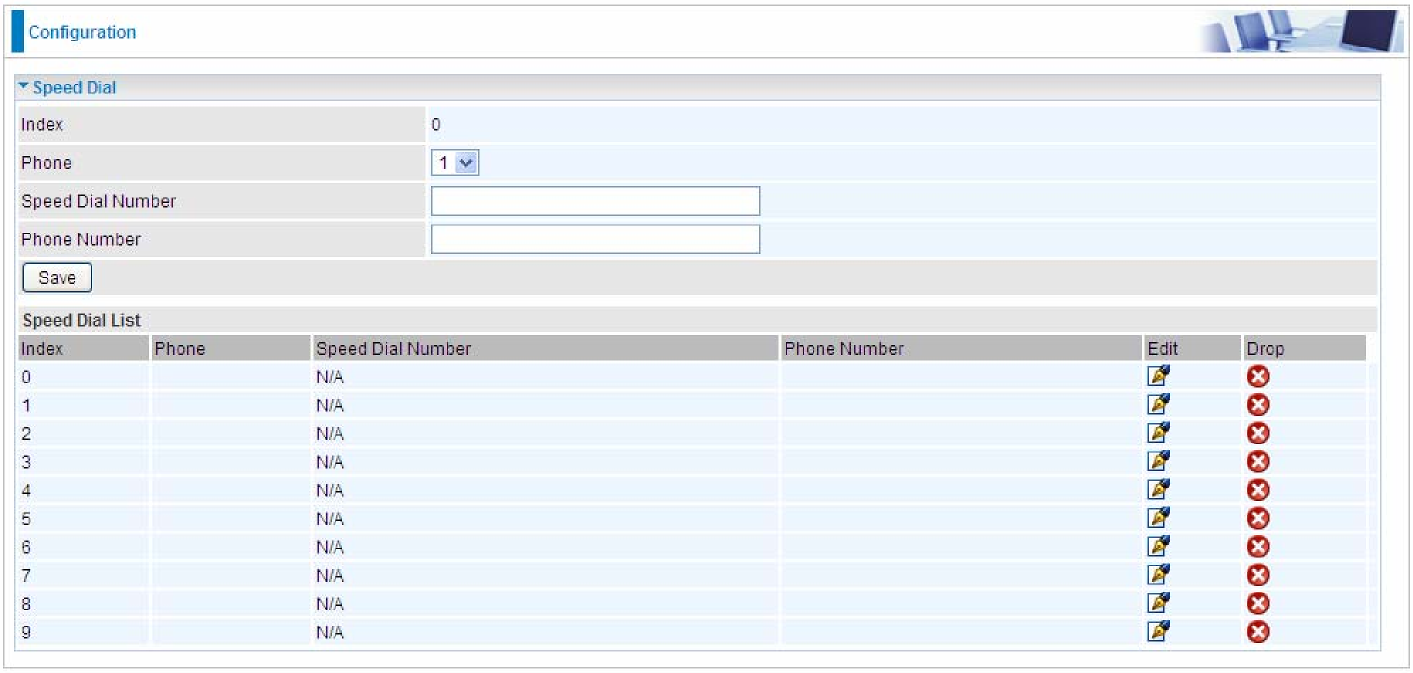
DTMF Transport Mode: Select the DTMF mode.

Listening Volume: Adjust the volume of listener, -6 to 6, from lowest to highest.

Speaking Volume: Adjust the volume of microphone; -6 to 6, from lowest to highest.

4.4.3.4 Speed Dial

Speed Dial comes at hand to store frequently used telephone number(s) that you can press set ‘speed dial number’ instead of the exact dialing-out number on the phone keyboard to make a quick dialing.



Configuration

▾ Speed Dial

Index	0
Phone	1
Speed Dial Number	
Phone Number	

Save

Speed Dial List

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0		N/A		✎	✖
1		N/A		✎	✖
2		N/A		✎	✖
3		N/A		✎	✖
4		N/A		✎	✖
5		N/A		✎	✖
6		N/A		✎	✖
7		N/A		✎	✖
8		N/A		✎	✖
9		N/A		✎	✖

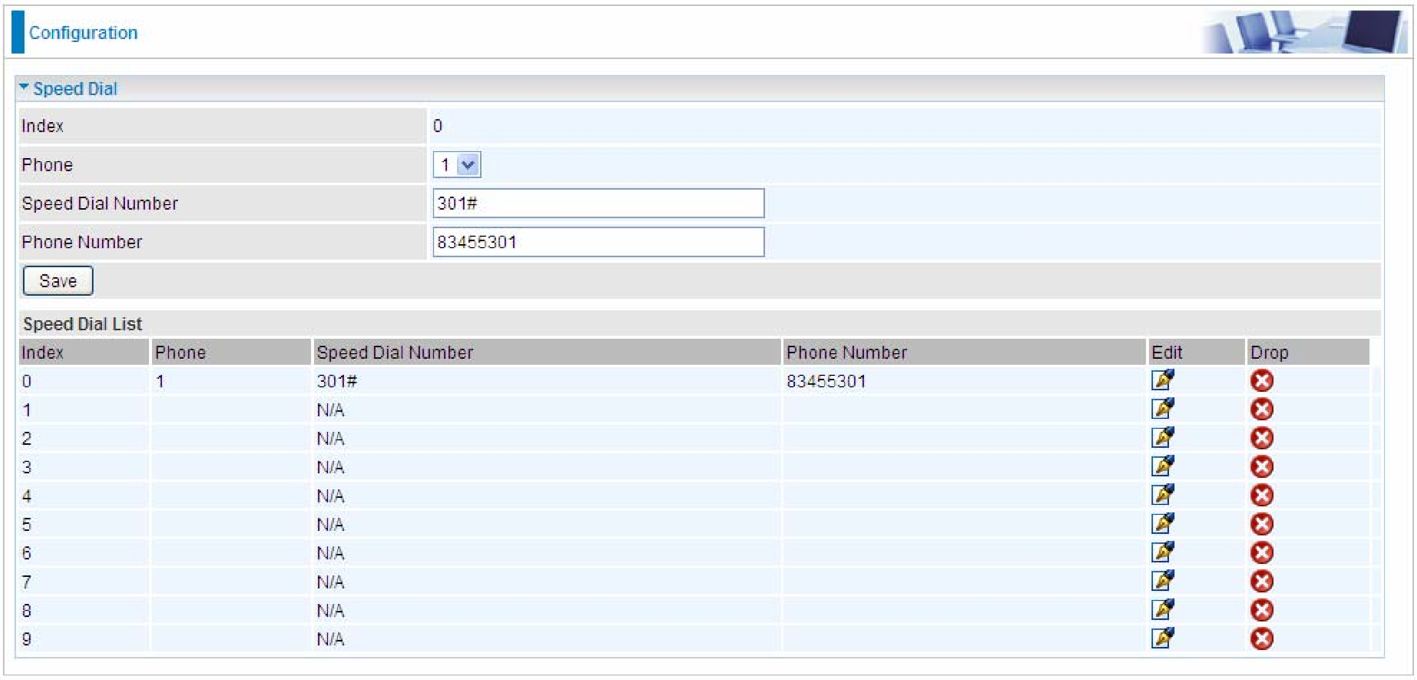
Index: The index to mark the speed dial number mapping, 0-9.

Phone: Select Phone 1 or Phone 2 to have your set speed dial number applied to the phone. If phone 1 is selected, your set speed dial number is about to be applied to phone 1.

Speed Dial Number: Set a easily remembered and simplied number to replace the Phone number, it can be a sequence in variing length from 0, 1,2, 3, 4, 5, 6, 7, 8,9 *. #, but note * or # must be included in the sequence.

Phone Number: The complete destination number

For example, a destination: 83455301. You want to replace it with a friendly speed dial numbr stored in your speed dial list , then set as follows.



Configuration

▾ Speed Dial

Index	0
Phone	1
Speed Dial Number	301#
Phone Number	83455301

Save

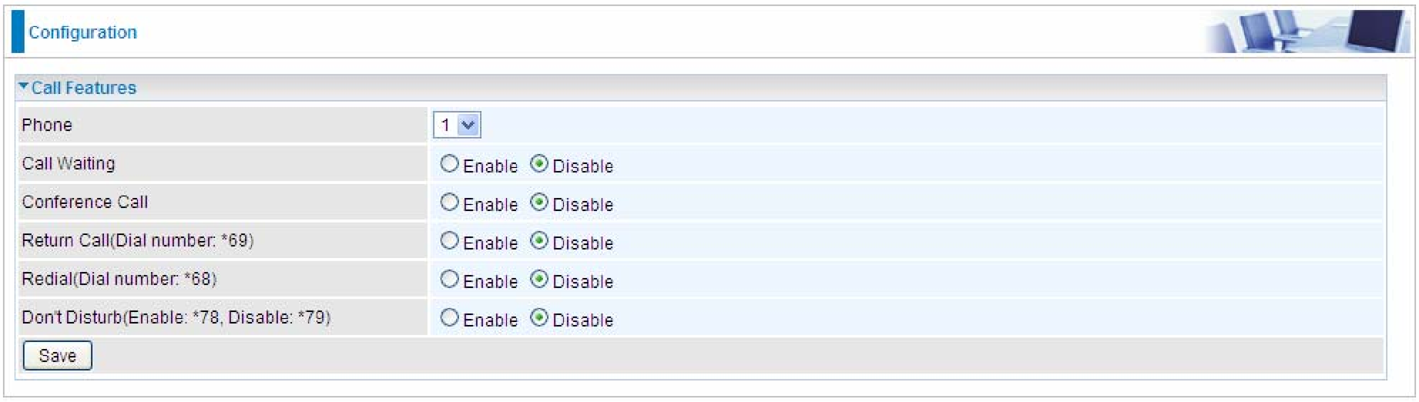
Speed Dial List

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0	1	301#	83455301	✎	✖
1		N/A		✎	✖
2		N/A		✎	✖
3		N/A		✎	✖
4		N/A		✎	✖
5		N/A		✎	✖
6		N/A		✎	✖
7		N/A		✎	✖
8		N/A		✎	✖
9		N/A		✎	✖

When you want call 83455301 through phone 1, you can simply dial 301# to make your desired call.

4.4.3.5 Call Features

Call Features provides usrs with some advanced phone characteristics, including Call waiting, Conference Call, etc.



Configuration

▾Call Features

Phone	1
Call Waiting	○ Enable ● Disable
Conference Call	○ Enable ● Disable
Return Call(Dial number: *69)	○ Enable ● Disable
Redial(Dial number: *68)	○ Enable ● Disable
Don't Disturb(Enable: *78, Disable: *79)	○ Enable ● Disable

Phone: Select the phone 1 or Phone 2 to have the following characteristics applied to the phone.

Call Waiting: Enable to activate Call Waiting feature. When you are busy on a call with, for example, A, and another call comes in, B, while the Call Waiting feature is enabled, you can hear a hint sound indicating there is another call in for you to decide to answer B by slightly pressing Hook to keep the original call with A.

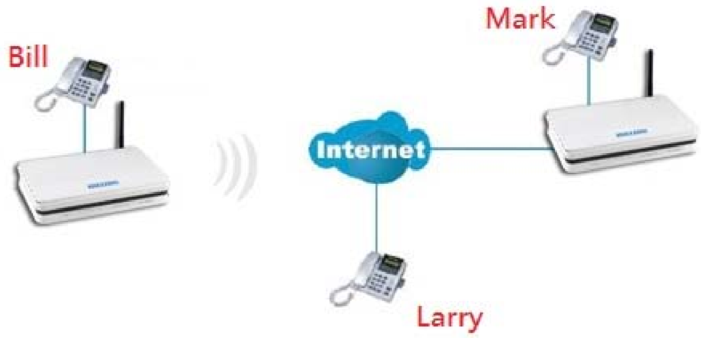
Conference Call: Enable to allow 3-way conference call. Please note, only 3 parties are allowed (device, A, and B)

Return Call (Dial number: *69): Dial *69 to redial the latest incoming call number.

Redial (Dial number: *68): Dial *68 to redial the latest outgoing call number.

Don’t Disturb (Enable: *78, Disable: *79): Press *78 to enable Don’t Disturb feature so as to make it not ring when a call comes in; while press *79 to disable Don’t Disturb feature, if a call comes with a ringing indication.

How to establish 3-way conference call



Case 1: Bill and Larry are talking. Bill wants to invite Mark to join a conference call.

Step – 1: Billy and Larry are discussing on the phone. Bill tells Larry that he wants to set up a conference call with Mark.

Step – 2: Bill presses flash (hold original call), and Bill hears the dial tone.

Step – 3: Bill calls Mark. Bill and Mark are on a new call.

Step – 4: Bill tells Mark that Mark is invited to join a conference call.

Step – 5: Bill presses flash (hold new call) and return to original call.

Step – 4: Bill tells Larry that Mark is on the phone.

Step – 6: Bill presses flash again to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

Case 2: When Bill and Larry are talking on the phone, Bill received a phone call from Mark. Bill decided to ask Mark to join the conference call.

Step – 1: Bill and Larry on a call, then Mark dials Bill and Bill hears a waiting tone.

Step – 2: Bill presses flash and picks up the call waiting call.

Step – 3: Bill tells Mark that he and Larry are talking on the phone, they can have a conference call.

Step – 4: Bill presses flash to hold the call with Mark and return to original call with Larry.

Step – 5: Bill tells Larry that it is Mark and he wants to set up a conference with Mark.

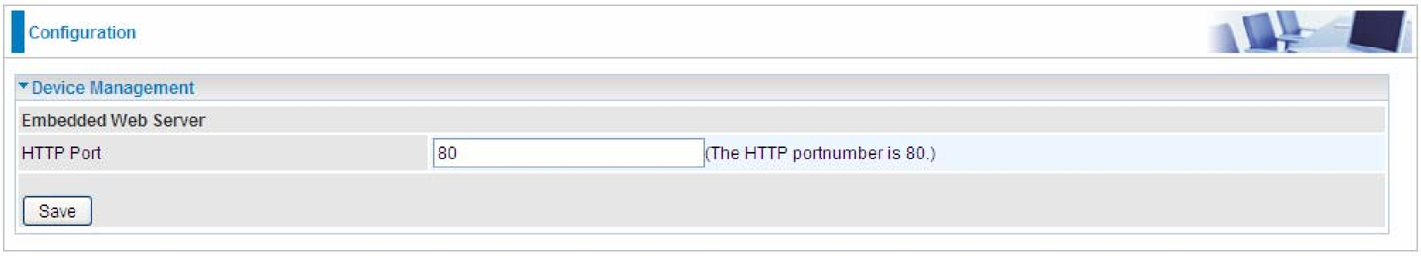
Step – 6: Bill presses flash again to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

4.4.4 Access Management

4.4.4.1 Device Management

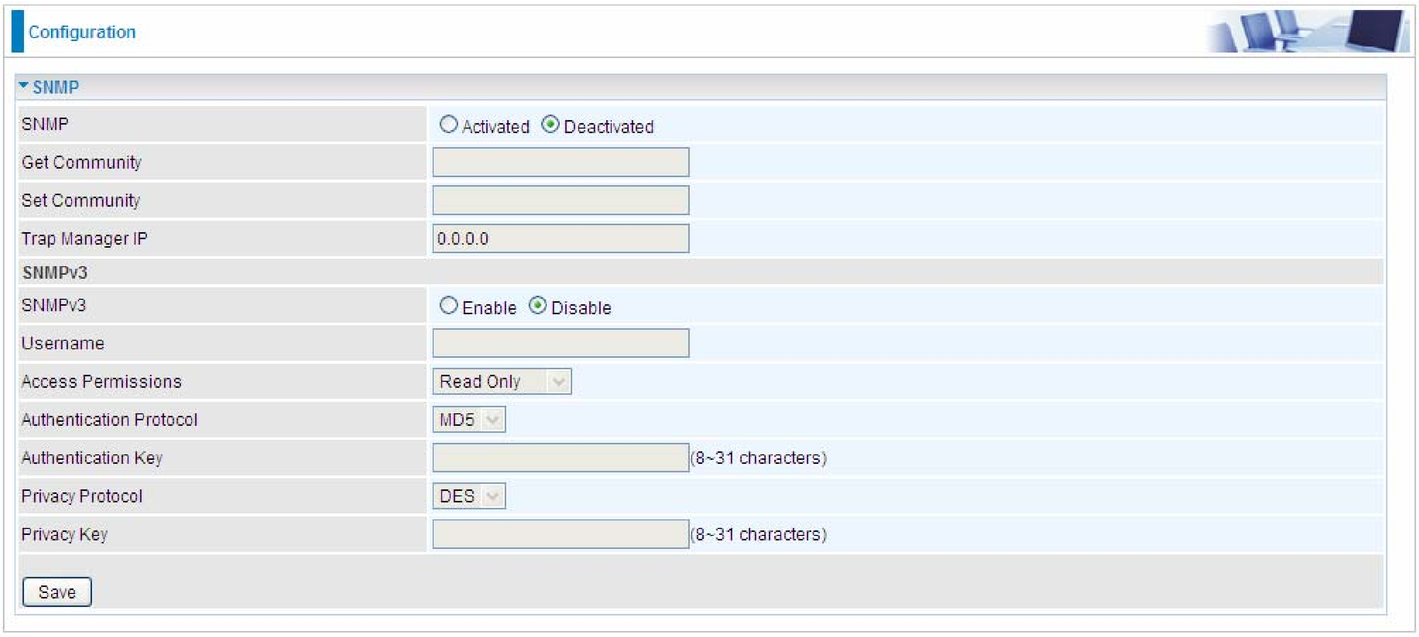
Device management offers users a way to change the embeded web server accessing port, default 80. User can change the http port to 8080 or something else here.



HTTP Port: 80 (The HTTP portnumber is 80.)

4.4.4.2 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. BIPAC 6300VNOZ serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.



Configuration

▾ SNMP

SNMP	○ Activated ● Deactivated
Get Community	
Set Community	
Trap Manager IP	0.0.0.0
SNMPv3	
SNMPv3	○ Enable ● Disable
Username	
Access Permissions	Read Only
Authentication Protocol	MD5
Authentication Key	(8~31 characters)
Privacy Protocol	DES
Privacy Key	(8~31 characters)

SNMP: Select to enable SNMP feature.

Get Community: Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

Set Community: Type the Set Community, which is the password for incoming Set requests from the management station.

Trap Manager IP: Enter the IP of the server receiving the trap message(when some exception occurs) sent by this SNMP agent.

SNMPv3: Enable to activate the SNMPv3.

User Name: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Authentication Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

Authentication Key: Set the authentication key, 8-31 characters.

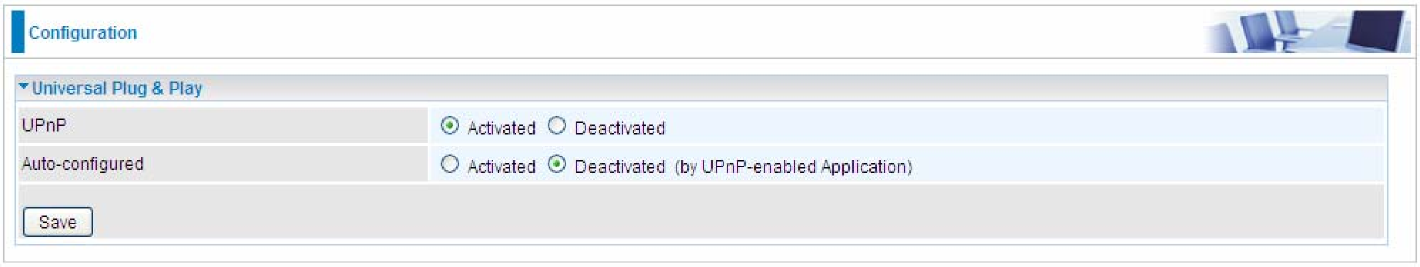
Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Key: Set the privacy key, 8-31 characters.

4.4.4.3 Universal Plug & Play

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



Configuration

▾Universal Plug & Play

UPnP	● Activated ○ Deactivated
Auto-configured	○ Activated ● Deactivated (by UPnP-enabled Application)

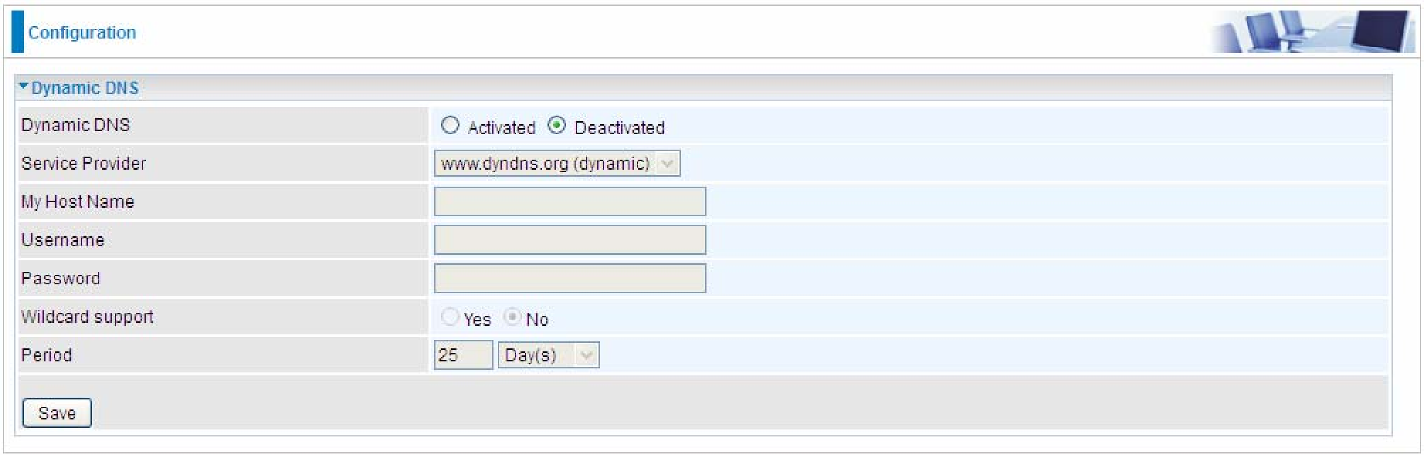
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering the BIPAC 6300VNOZ' IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BIPAC 6300VNOZ so that they can communicate through the BIPAC 6300VNOZ, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

4.4.4.4 Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es). But note that first users have to go to the Dynamic DNS registration service provider to register an account.



Configuration

▾Dynamic DNS

Dynamic DNS	○ Activated ● Deactivated
Service Provider	www.dyndns.org (dynamic)
My Host Name	
Username	
Password	
Wildcard support	○ Yes ● No
Period	25 Day(s)

Dynamic DNS: Select this check box to activate Dynamic DNS.

Service Provider: Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

My Host Name: Type the domain name assigned to your BIPAC 6300VNOZ by your Dynamic DNS provider.

Username: Type your user name.

Password: Type the password.

Wildcard support: Select this check box to enable DYNDNS Wildcard.

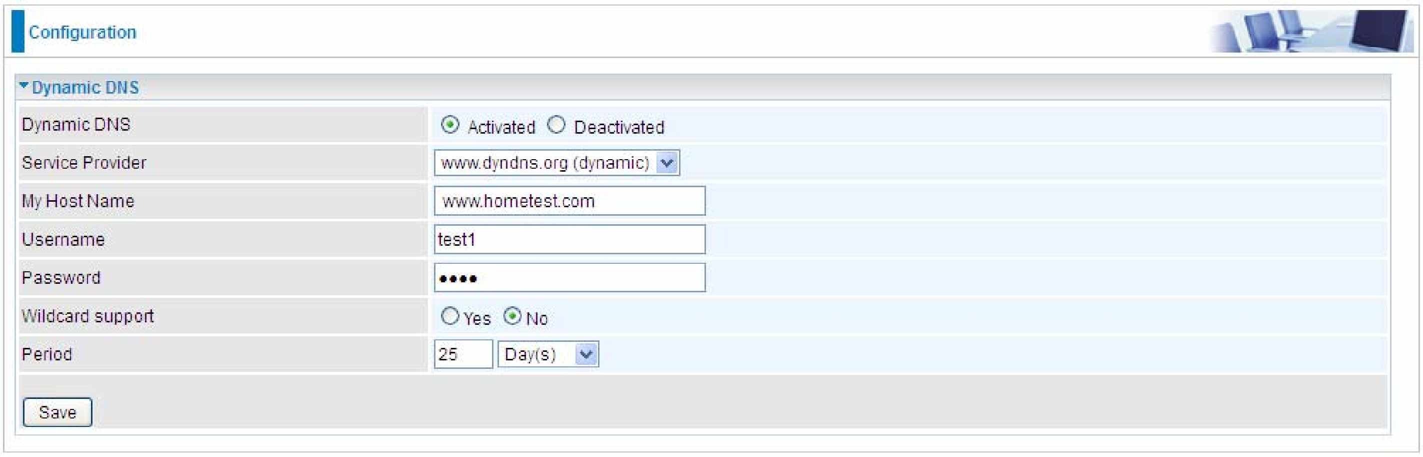
Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

User can register a DDNS

Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

User ***test1*** register a Dynamic Domain Names in DDNS provider **http://www.dyndns.org/** .

DDNS: www.hometest.com using username/password test/test



Configuration

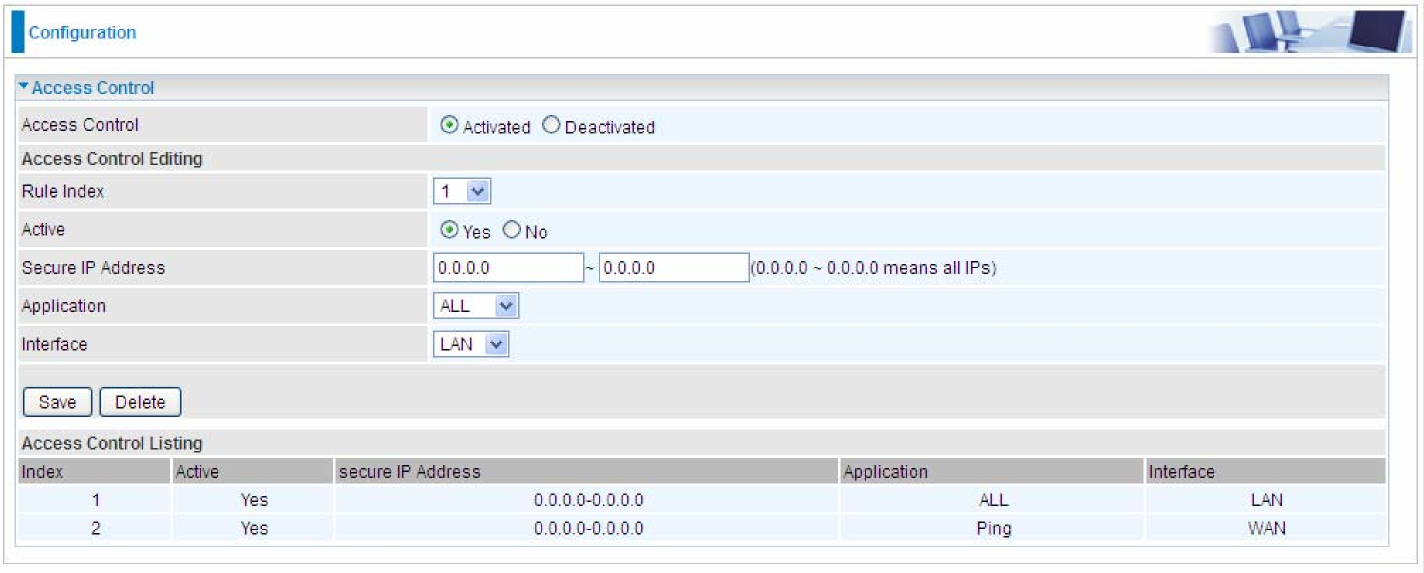
▾ Dynamic DNS

Dynamic DNS	● Activated ○ Deactivated
Service Provider	www.dyndns.org (dynamic)
My Host Name	www.hometest.com
Username	test1
Password	●●●●
Wildcard support	○ Yes ● No
Period	25 Day(s)

4.4.4.5 Access Control

Access Control Listing allows you to determine which services/protocols can access BIPAC 6300VNOZ interface from which computers. It is a management tool aimed to allow IPs(set in secure IP address) to access specified embedded applications (Web, etc, user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entries is 16.



Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	1
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL
Interface	LAN

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Access Control: Select whether to make Access Control function available.

Rule Index: This is item number

Active: Select to activate the rule.

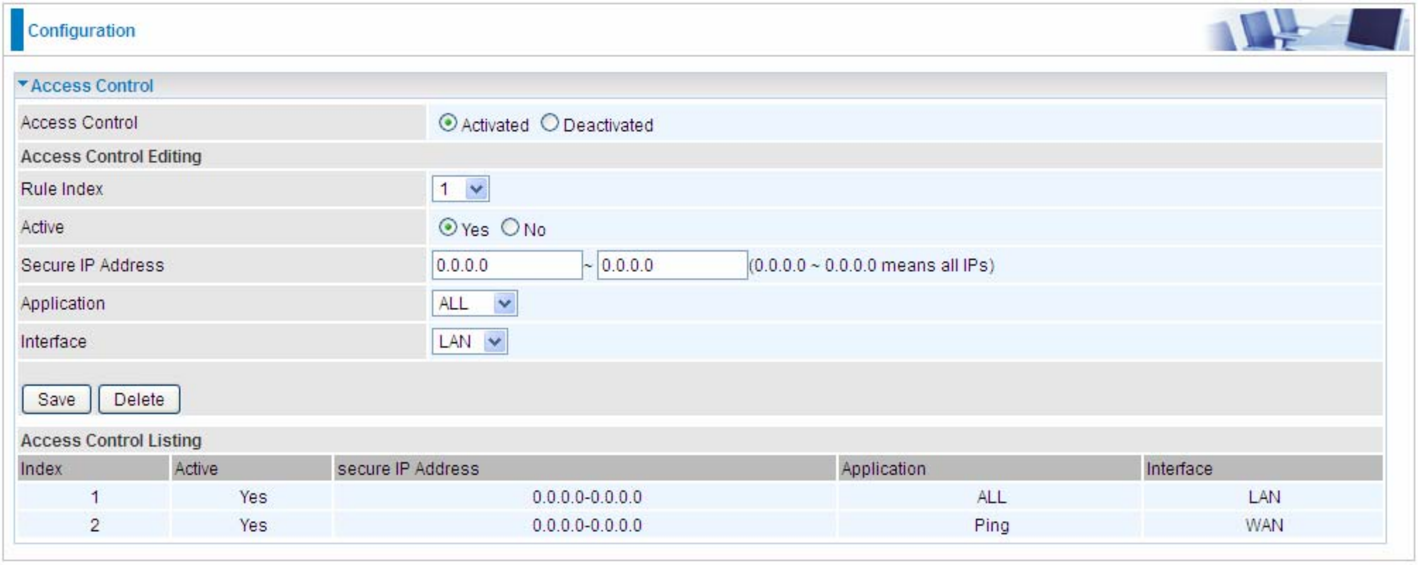
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the BIPAC 6300VNOZ. Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the common used applications.

Interface: Select the access interface. Choices are **LAN**, **WAN** and **Both**.

By default, the "Access Control" has two default rules.

1. Rule 1(Index 1), a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc). Under this situation, clients from WAN can not access the router even from Ping.



Configuration

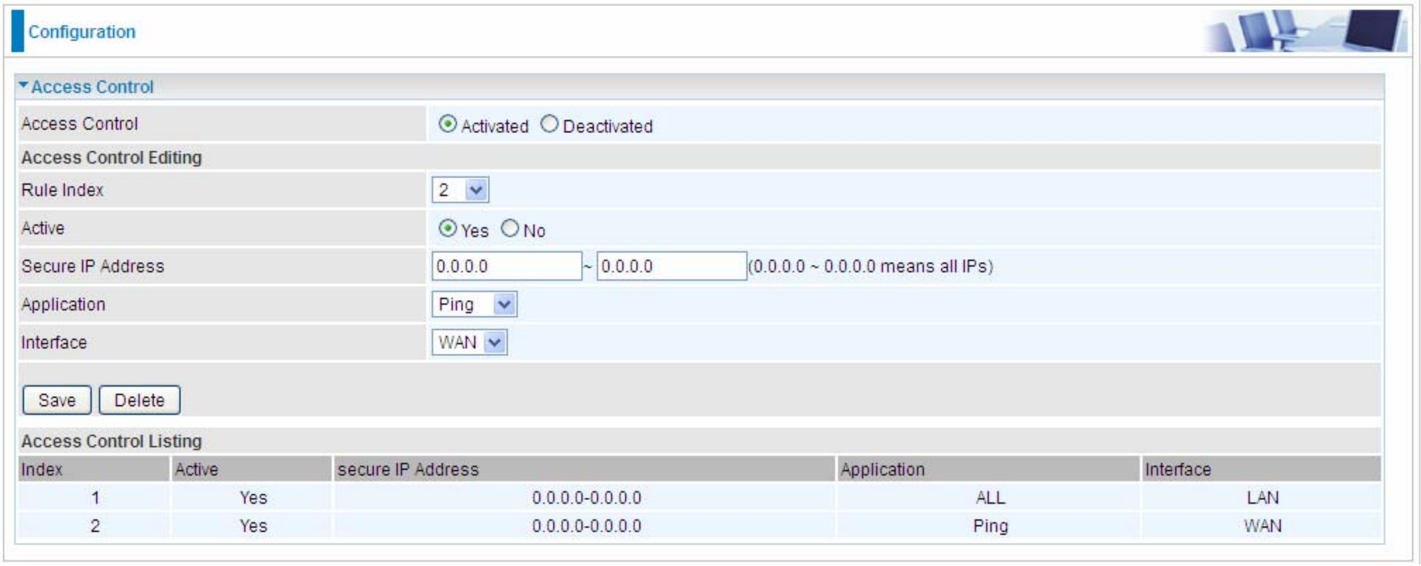
Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	1
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL
Interface	LAN

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

2, Rule 2(Index 2), a ACL rule to open Ping to WAN side.



Configuration

Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	2
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	Ping
Interface	WAN

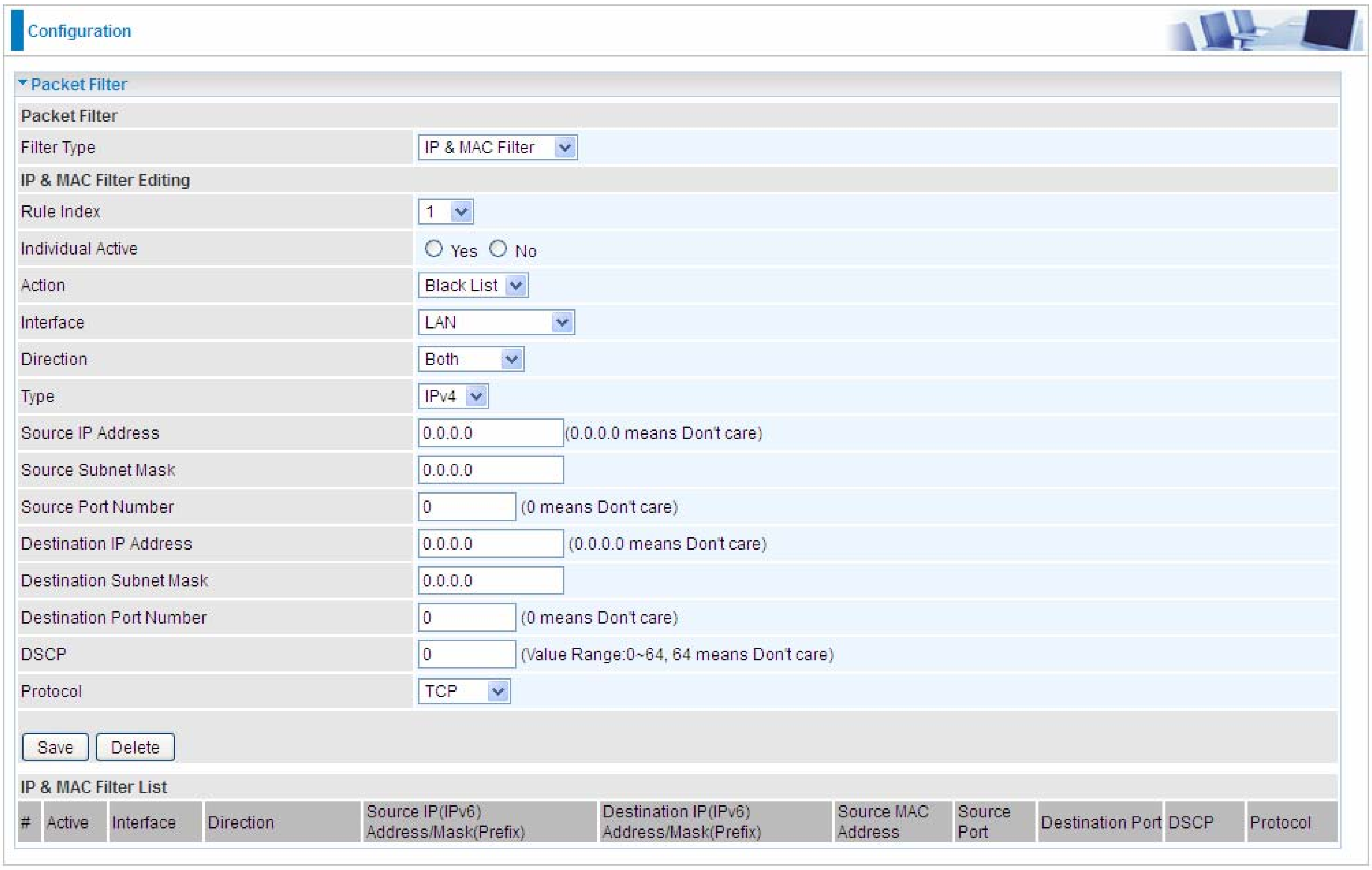
Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

4.4.4.6 Packet Filter

You can filter the packages by MAC address, IP address, Protocol, Port number and Application or URL.

- **IP & MAC Filter**



Packet Filter	
Filter Type	IP & MAC Filter
IP & MAC Filter Editing	
Rule Index	1
Individual Active	○ Yes ○ No
Action	Black List
Interface	LAN
Direction	Both
Type	IPv4
Source IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Source Subnet Mask	0.0.0.0
Source Port Number	0 (0 means Don't care)
Destination IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Destination Subnet Mask	0.0.0.0
Destination Port Number	0 (0 means Don't care)
DSCP	0 (Value Range:0~64, 64 means Don't care)
Protocol	TCP

IP & MAC Filter List

#	Active	Interface	Direction	Source IP(IPv6) Address/Mask(Prefix)	Destination IP(IPv6) Address/Mask(Prefix)	Source MAC Address	Source Port	Destination Port	DSCP	Protocol

Packet Filter

Filter Type: There are three types “**IP & MAC Filter**”, “**Application Filter**”, and “**URL Filter**” that user can select for this filter rule. Here we set **IP & MAC Filter**.

IP & MAC Filter Editing

Rule Index: This is item number

Individual Active: Select **Yes** to activate the rule.

Action: This is how to deal with the packets matching the rule. Allow please select White List or block selecting Black List.

Interface: Select to determine which interface the rule will be applied to.

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

Type: Choose type of field you want to specify to monitor. Select “IPv4” for IPv4 address, port number and protocol. Select “IPv6” for IPv6 address, port number and protocol. Select “MAC” for MAC address.

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Source Subnet Mask: Enter the subnet mask of the source network.

Source Port Number: The source port number of packets to be monitored. 0 means “Don’t care”.

Destination IP Address: The destination IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Destination Subnet Mask: Enter the subnet mask of the destination network.

Destination Port Number: This is the Port that defines the application. (E.g. HTTP port 80.)

DSCP: DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)

Protocol: Specify the packet type (TCP, UDP, ICMP, ICMPv6) that the rule applies to.

IP/MAC Filter Listing

#: Item number**.**

Active: Whether the connection is currently active.

Interface: show the interface the rule applied to.

Direction: show the direction the rule applied to.

Source IP(IPv6) Address/Mask(Prefix): The source IP address or range of packets to be monitored.

Destination IP(IPv6) Address/Mask(Prefix): This is the destination subnet IP address.

Source MAC Address: show the MAC address of the rule applied.

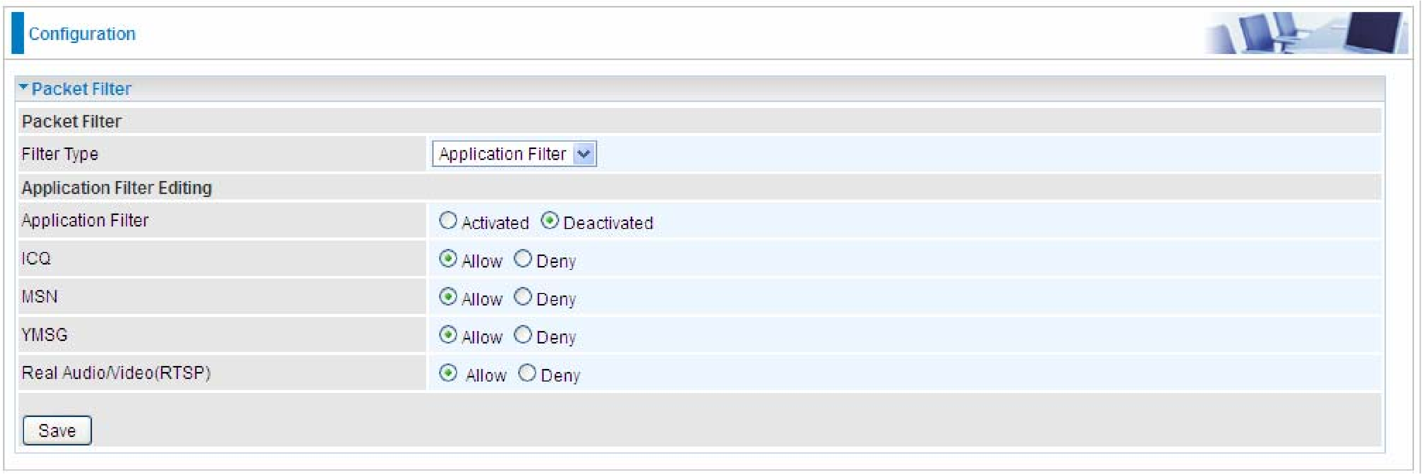
Source Port: The source port number of packets to be monitored.

Destination Port: This is the Port or Port Ranges that defines the application.

DSCP: show the set DSCP.

Protocol: It is the packet protocol type used by the application. Select either **TCP** or **UDP** or **ICMP or ICMPv6**

➢ Application Filter



Packet Filter	
Filter Type	Application Filter
Application Filter Editing	
Application Filter	○ Activated ● Deactivated
ICQ	● Allow ○ Deny
MSN	● Allow ○ Deny
YMSG	● Allow ○ Deny
Real Audio/Video(RTSP)	● Allow ○ Deny

Application Filter: Select this option to Activated/Deactivated the Application filter.

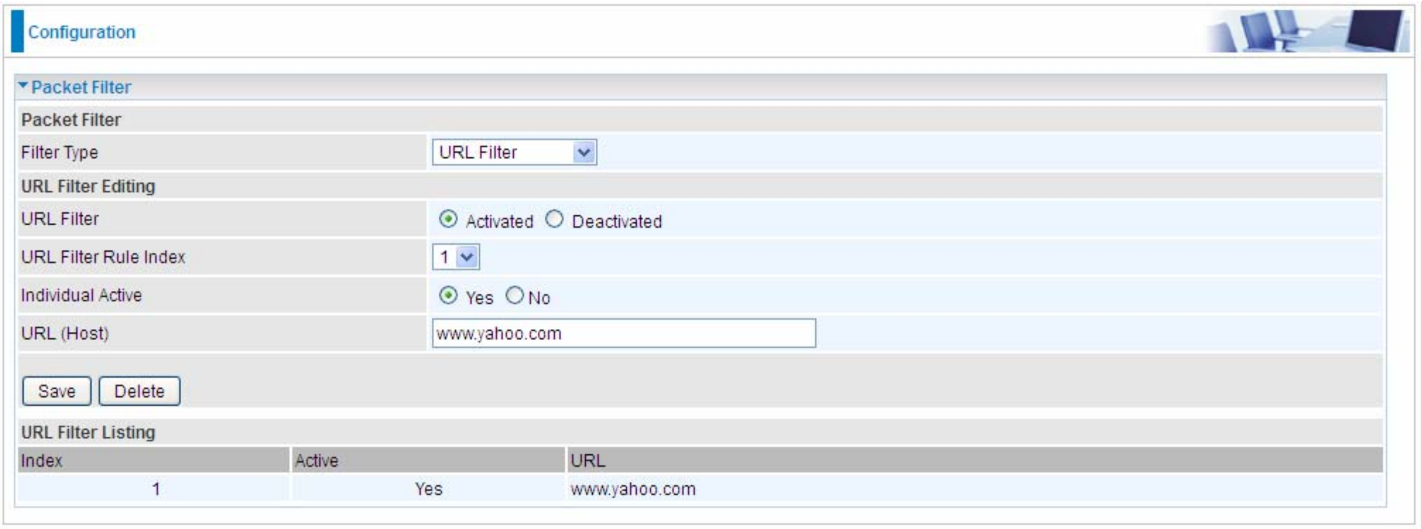
ICQ: Select this option to Allow/Deny ICQ.

MSN: Select this option to Allow/Deny MSN.

YMSG: Select this option to Allow/Deny Yahoo messenger.

Real Audio/Video(RTSP): Select this option to Allow/Deny Real Audio/Video (RTSP).

➢ URL Filter



Configuration

▾Packet Filter

Packet Filter	
Filter Type	URL Filter
URL Filter Editing	
URL Filter	● Activated ○ Deactivated
URL Filter Rule Index	1
Individual Active	● Yes ○ No
URL (Host)	www.yahoo.com

URL Filter Listing

Index	Active	URL
1	Yes	www.yahoo.com

URL Filter: Select **Activated** to enable URL Filter.

URL Filter Rule Index: This is item number.

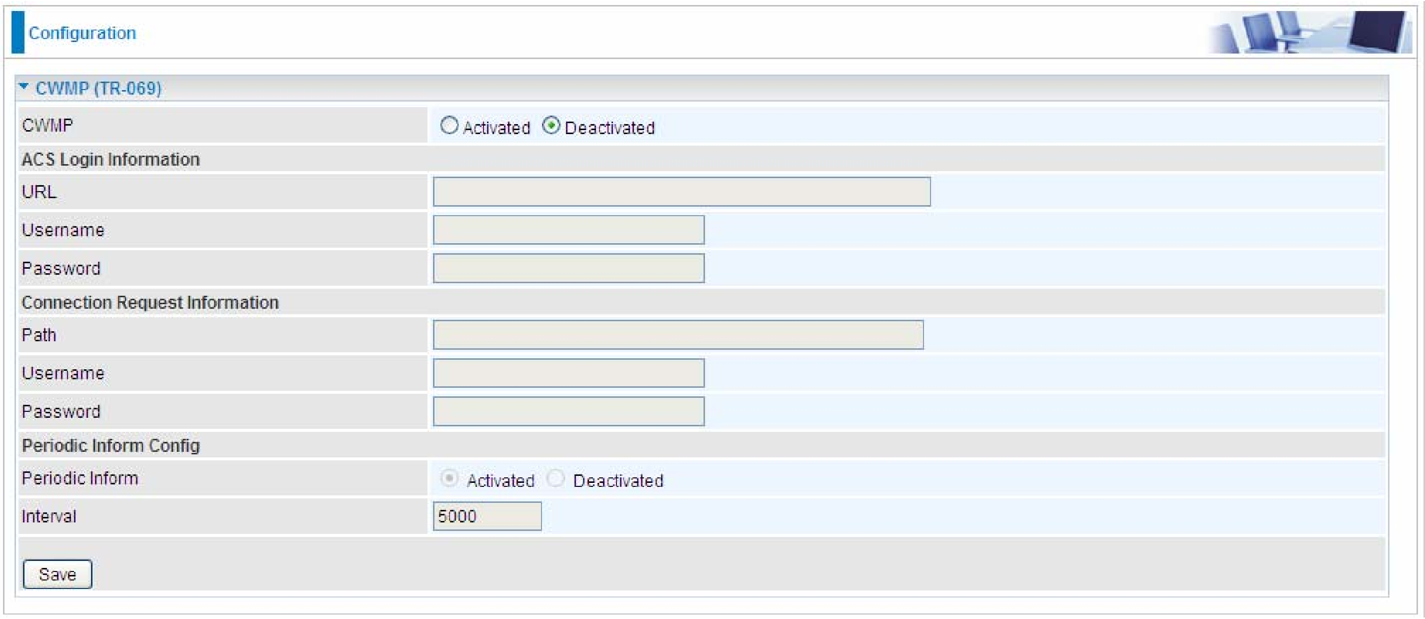
Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in “URL Filter” field, and also Yes in “Individual Active” field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

URL(Host): Specified URL which is prohibited from accessing.

4.4.4.7 CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Configuration

▾ CWMP (TR-069)

CWMP	○ Activated ● Deactivated
ACS Login Information	
URL	
Username	
Password	
Connection Request Information	
Path	
Username	
Password	
Periodic Inform Config	
Periodic Inform	● Activated ○ Deactivated
Interval	5000

CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

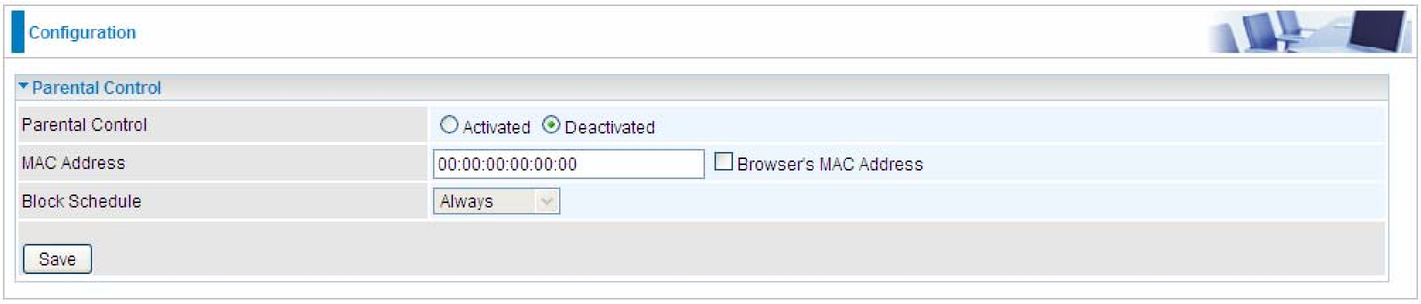
Periodic Inform Config

Periodic Inform: Select activated to enable to let CPE be authorized to send Inform message to automatically connect to ACS.

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

4.4.4.8 Parental Control

With this feature, router can reject to provide **internet** services to the specified computer during some specified time interval. This can be very useful for parents to give control to children using computer without restraint.



Configuration

Parental Control

Parental Control: ○ Activated ● Deactivated

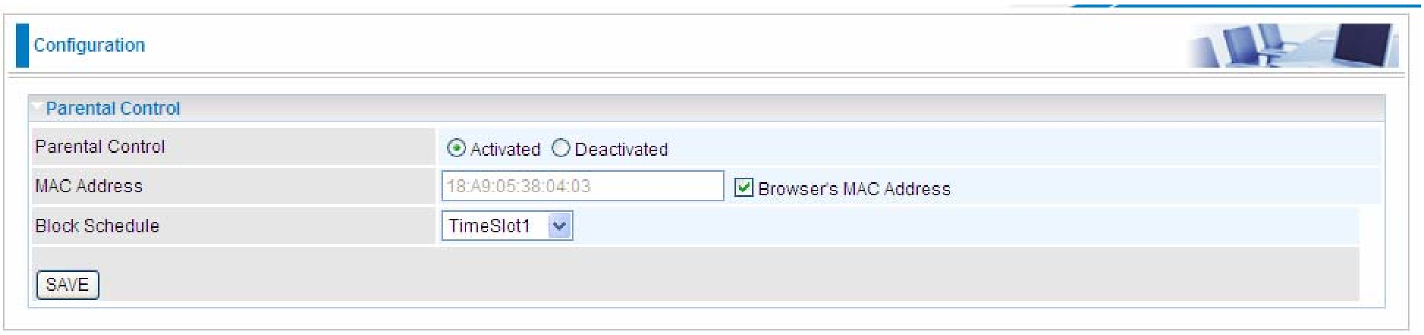
MAC Address: 00:00:00:00:00:00 □ Browser's MAC Address

Block Schedule: Always

Parent Control: Select Activated to enable this feature.

MAC Address: Type the MAC address(es) you want to block to access the internet (access to the router is sustained). The format of MAC address could be: xx:xx:xx:xx:xx:xx . If you want to set restriction to the Browser PC, you can directly check the checkbox of Browser's MAC Address.

Block Schedule: Select a timeslot throughout which the above set MAC is restricted to access internet. See 4.4.2.8 Time Schedule to set the exact timeslot.



Configuration

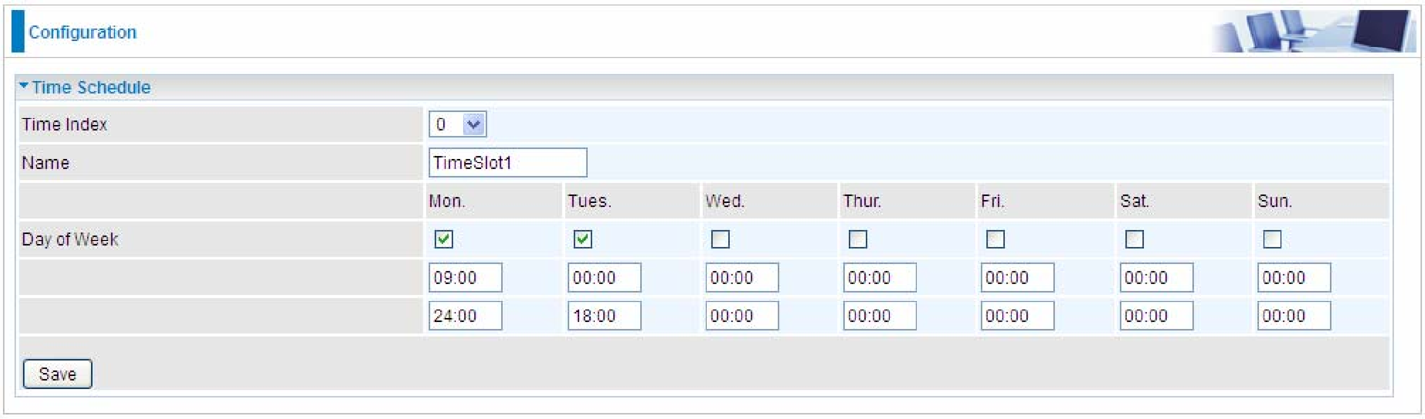
Parental Control

Parental Control: ● Activated ○ Deactivated

MAC Address: 18:A9:05:38:04:03 ☑ Browser's MAC Address

Block Schedule: TimeSlot1

Timeslot1 at Time Schedule:



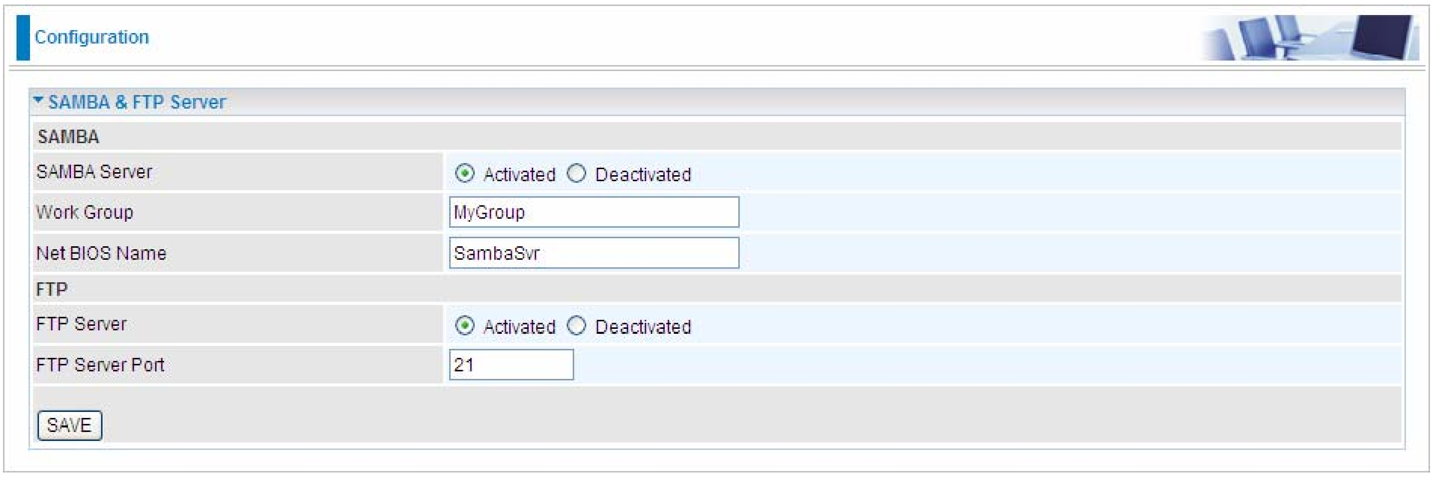
Configuration

Time Schedule

Time Index	0						
Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	☑	☑	□	□	□	□	□
	09:00	00:00	00:00	00:00	00:00	00:00	00:00
	24:00	18:00	00:00	00:00	00:00	00:00	00:00

4.4.4.9 SAMBA & FTP Server

Samba and FTP are served as network sharing.



▾ SAMBA & FTP Server

SAMBA	
SAMBA Server	● Activated ○ Deactivated
Work Group	MyGroup
Net BIOS Name	SambaSvr
FTP	
FTP Server	● Activated ○ Deactivated
FTP Server Port	21

SAMBA Server: Activated to enable SAMBA sharing.

Work Group: The same mechanism like in Microsoft work group, please set the Work Group name.

NetBIOS Name: The sharing NetBIOS name.

FTP Server: Activated to enable FTP sharing.

FTP Server Port: Set the working port. Well-known one is 21. User can change it.

SAMBA/FTP login account:

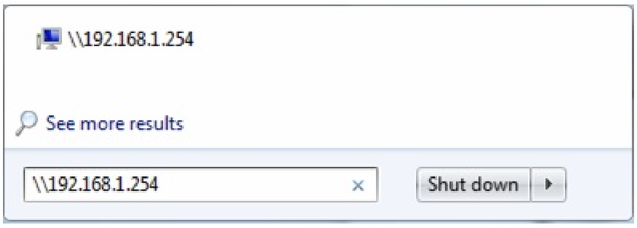
1) **Default user:** admin/admin, it is the administrative user and a super user, it has the full authority of SAMBA /FTP access and operation permission of objects in SAMBA and FTP server.

2) **New user:** users can create new user(s) to grant it (them) access and permission to the SAMBA & FTP server.

Please see 4.4.5.1 User Management.

Samba Usage：

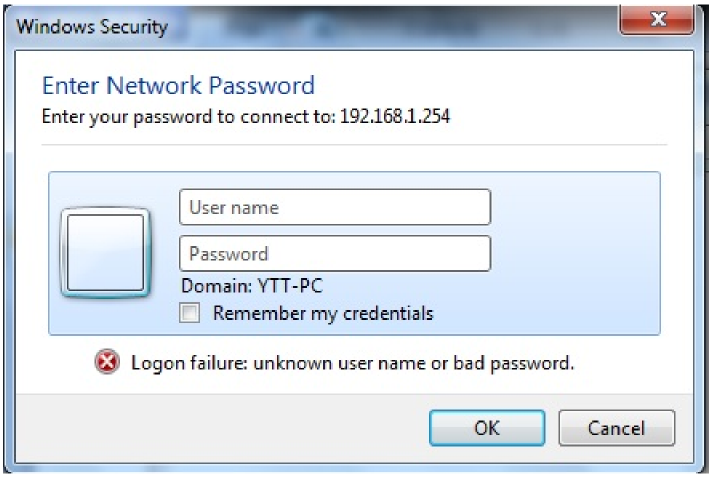
1. Go directly to Start > Run (enter \\192,168,1,254 (from LAN side), \\SambaSvr , but if you enter \\SambaSvr, please be sure your working PC is in the same workgroup as set in the samba server set above.)



\\192.168.1.254

\\192.168.1.254

2. Enter the Username and password.



Windows Security

Enter Network Password

Enter your password to connect to: 192.168.1.254

User name

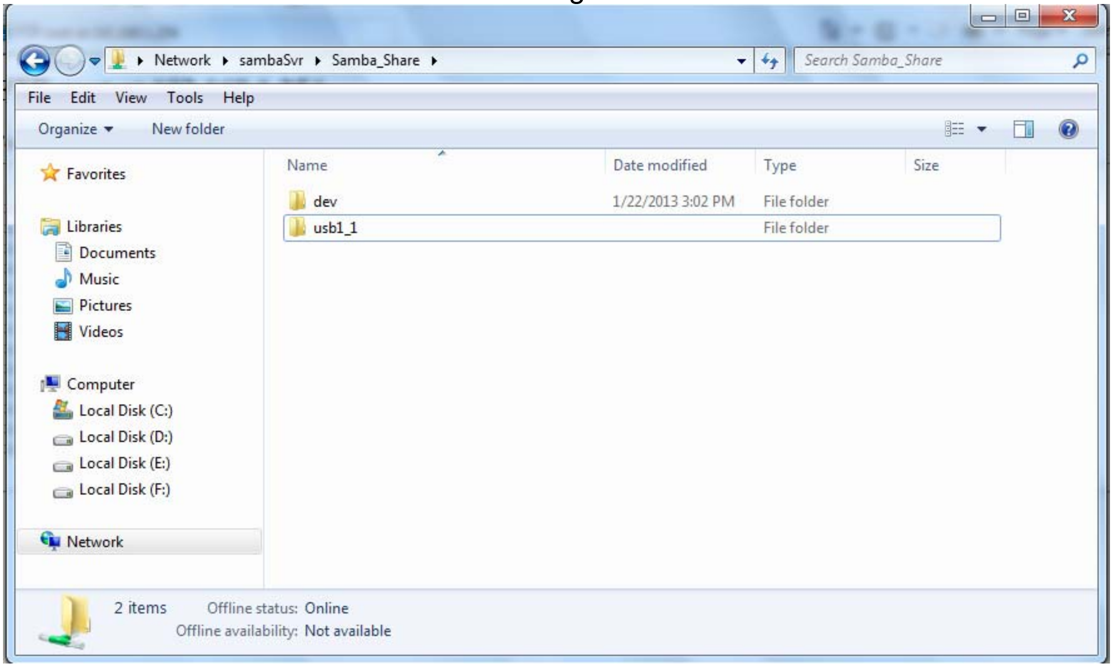
Password

Domain: YTT-PC

□ Remember my credentials

Logon failure: unknown user name or bad password.

3. Users can browse and access USB storage.



Name	Date modified	Type	Size
dev	1/22/2013 3:02 PM	File folder	
usb1_1		File folder	

2 items Offline status: Online
Offline availability: Not available

FTP usage:

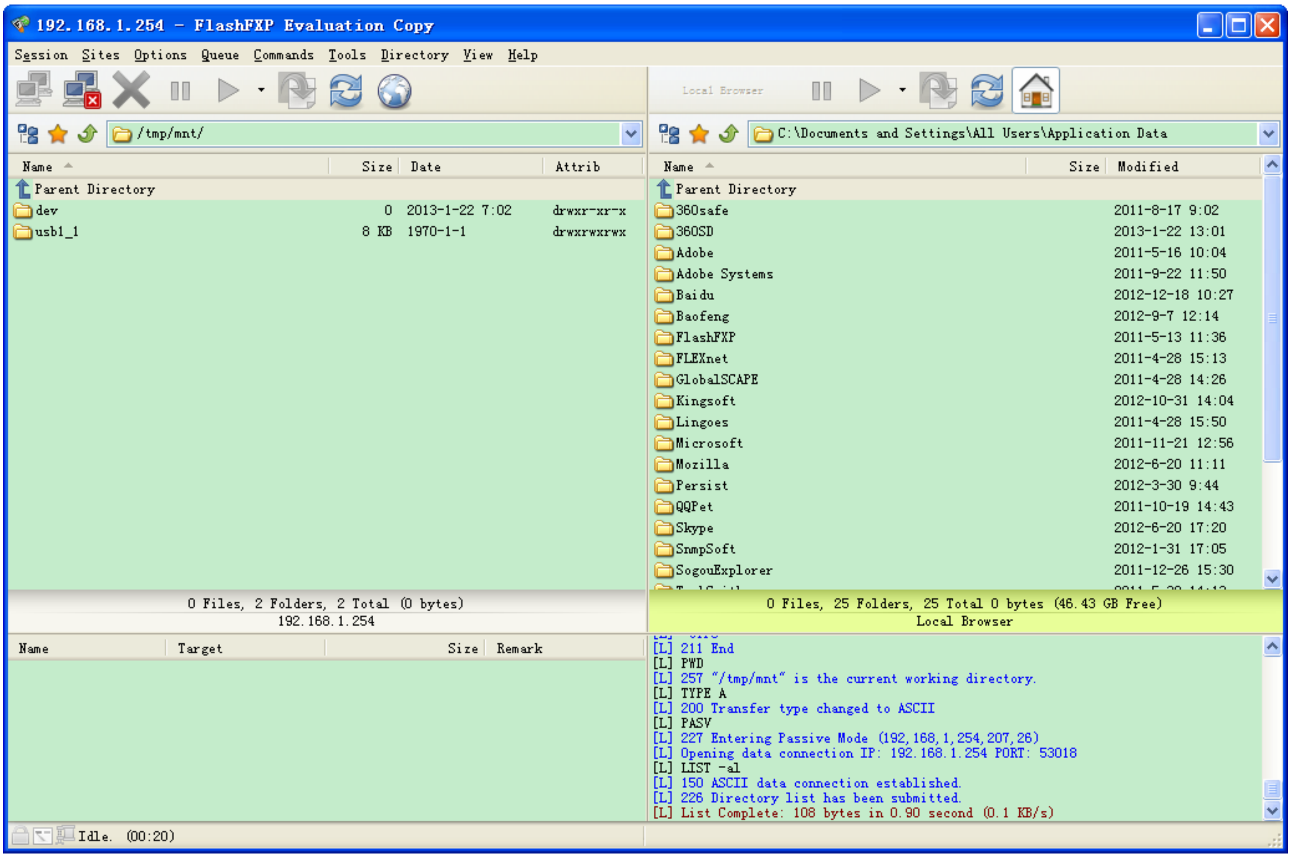
1. **Access via FTP tools**

Take popular FTP tool of FlashFXP for example:

1) Open FlashFXP

2) Create ftp sites (LAN IP / WAN IP, 192.168.1.254, and set the account, port).

3) Connect to the ftp site.



/tmp/mnt/

Name	Size	Date	Attrib
Parent Directory			
dev	0	2013-1-22 7:02	drwxr-xr-x
usb1_1	8 KB	1970-1-1	drwxrwxrwx

0 Files, 2 Folders, 2 Total (0 bytes)
192.168.1.254

C:\Documents and Settings\All Users\Application Data

Name	Size	Modified
Parent Directory		
360safe		2011-8-17 9:02
360SD		2013-1-22 13:01
Adobe		2011-5-16 10:04
Adobe Systems		2011-9-22 11:50
Baidu		2012-12-18 10:27
Baofeng		2012-9-7 12:14
FlashFXP		2011-5-13 11:36
FLEXnet		2011-4-28 15:13
GlobalSCAPE		2011-4-28 14:26
Kingsoft		2012-10-31 14:04
Lingoes		2011-4-28 15:50
Microsoft		2011-11-21 12:56
Mozilla		2012-6-20 11:11
Persist		2012-3-30 9:44
QQPet		2011-10-19 14:43
Skype		2012-6-20 17:20
SnmpSoft		2012-1-31 17:05
SogouExplorer		2011-12-26 15:30

0 Files, 25 Folders, 25 Total 0 bytes (46.43 GB Free)
Local Browser

Name	Target	Size	Remark

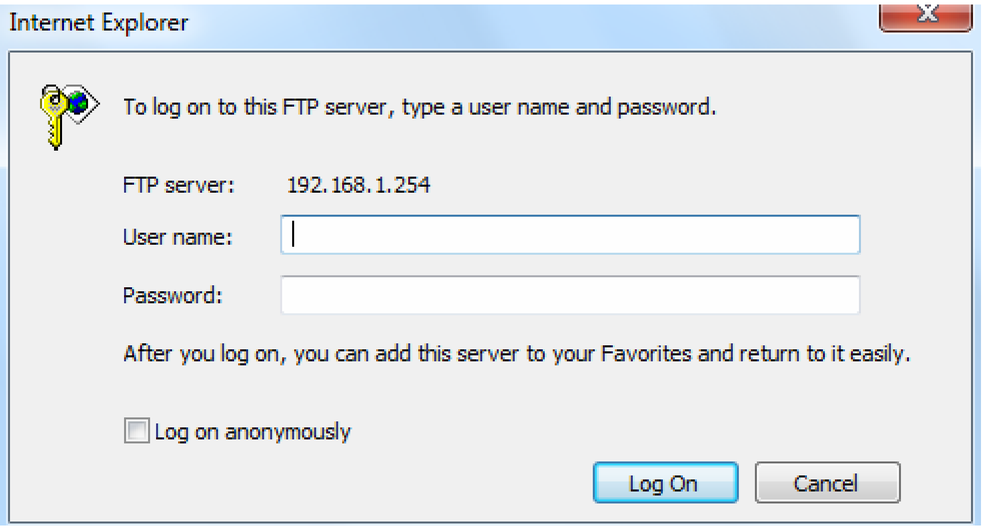
```
[L] 211 End
[L] PWD
[L] 257 "/tmp/mnt" is the current working directory.
[L] TYPE A
[L] 200 Transfer type changed to ASCII
[L] PASV
[L] 227 Entering Passive Mode (192,168,1,254,207,26)
[L] Opening data connection IP: 192.168.1.254 PORT: 53018
[L] LIST -al
[L] 150 ASCII data connection established.
[L] 226 Directory list has been submitted.
[L] List Complete: 108 bytes in 0.90 second (0.1 KB/s)
```

Idle. (00:20)

2. **Web FTP access**

1) Enter ftp://192.168.1.254 at the address bar of the web page.

2) Enter the account's username and password.



Internet Explorer

To log on to this FTP server, type a user name and password.

FTP server: 192.168.1.254

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

□ Log on anonymously

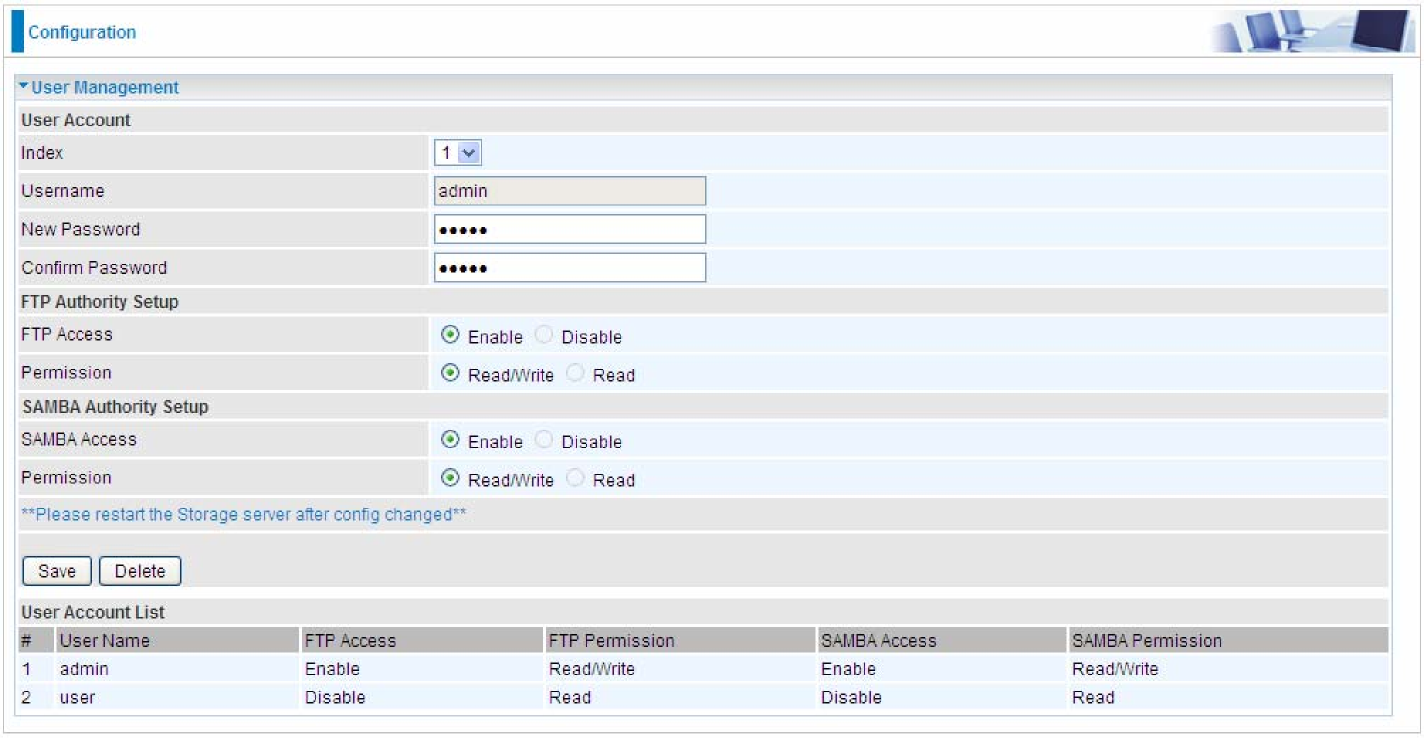
4.4.5 Maintenance

Maintenance equipments the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including **User Management**, **Time Zone**, **Firmware & Configuration**, **System Restart**, **Diagnostic Tool.** Usage of each feature is to be presented in the following scenarios.

4.4.5.1 User Management

In factory setting, the default accounts are **admin/admin** and **user/user.** The default account admin has been authorized to web access of router, Samba access, and FTP access. The user **user/user** has only access to the FTP and Samba server, but disabled by default. A total of **6** other accounts can be created to grant access to the access of Samba and FTP but not router's web.

Note: Please go to 4.4.4.9 SAMBA & FTP Server to re-activate FTP and SAMBA server to enable the changes to the FTP and SAMBA account set here.



User Account

Index	1
Username	admin
New Password	•••••
Confirm Password	•••••

FTP Authority Setup

FTP Access	● Enable ○ Disable
Permission	● Read/Write ○ Read

SAMBA Authority Setup

SAMBA Access	● Enable ○ Disable
Permission	● Read/Write ○ Read

Please restart the Storage server after config changed

User Account List

#	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to SAMBA and FTP.

New Password: Type the password for the user account. Default user admin's password can be changed here and confirmed in the next field.

Confirmed Password: Type password again for confirmation.

FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read/Write or Read.

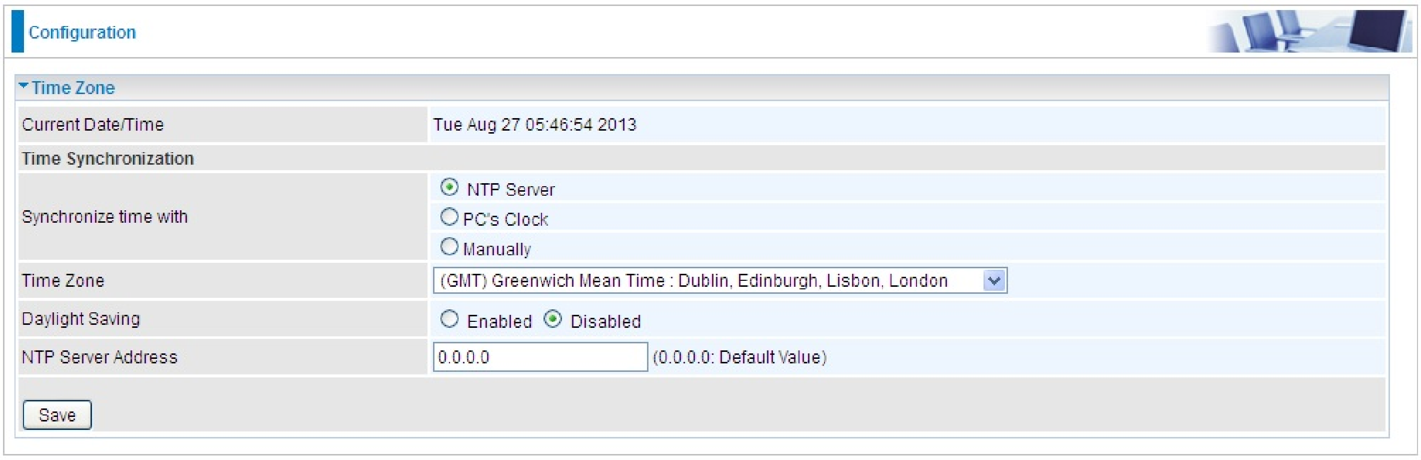
SAMBA Authority

SAMBA Access: Enable to grant the user access to the SAMBA server.

Permission: Set the operation permission for the user, Read/Write or Read.

4.4.5.2 Time Zone

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those default, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.



Configuration

▾Time Zone

Current Date/Time	Tue Aug 27 05:46:54 2013
Time Synchronization	
Synchronize time with	● NTP Server ○ PC's Clock ○ Manually
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Daylight Saving	○ Enabled ● Disabled
NTP Server Address	0.0.0.0 (0.0.0.0: Default Value)

Synchronize time with: Select the methods to synchronize the time.

- **NTP Server automatically:** To synchronize time with the NTP server.
- **PC's Clock:** To synchronize time with the PC's clock.
- **Manually:** Select this, user need to set the time yourself manually.

Time Zone: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

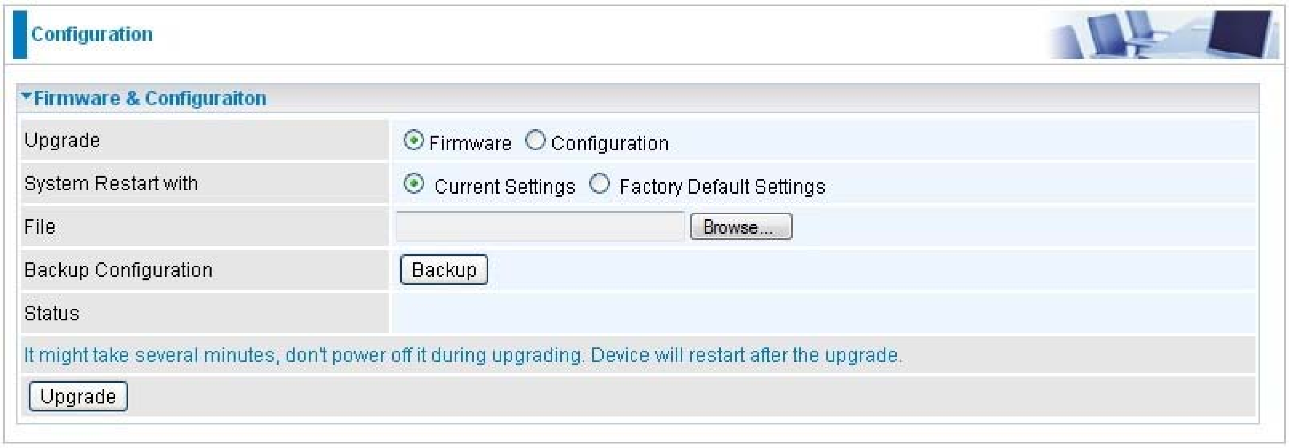
Daylight Saving: Select this option if you use daylight savings time.

NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

4.4.5.3 Firmware & Configuraion

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified, and your router allows you to upgrade the software it runs to take advantage of these changes.

To upgrade the firmware of BIPAC 6300VNOZ, you should download or copy the firmware to your local environment first. Press the **"Browse…"** button to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading. When the procedure is completed, BIPAC 6300VNOZ will reset automatically to make the new firmware work.



Configuration

▾Firmware & Configuraiton

Upgrade	● Firmware ○ Configuration
System Restart with	● Current Settings ○ Factory Default Settings
File	Browse...
Backup Configuration	Backup
Status	

It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.

Upgrade

Upgrade: Choose Firmware or Configuration you want to update.

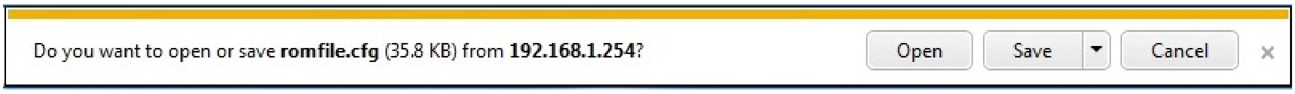
System Restart with:

- **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.

File: Type in the location of the file you want to upload in this field or click **Browse** to find it.

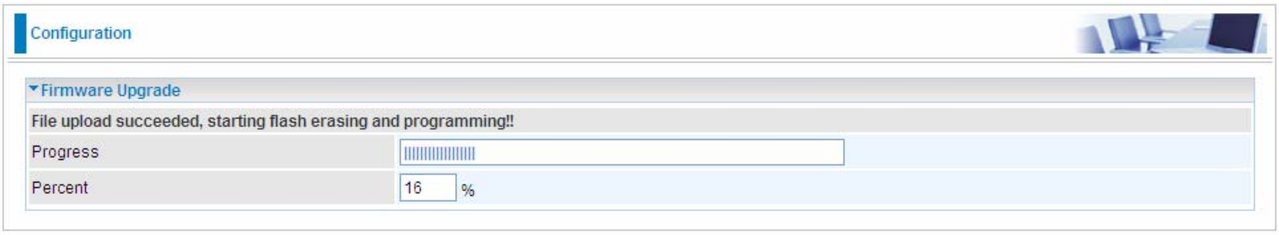
Browse: Click **Browse...** to find the configuration file or firmware file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

Backup Configuration: Click **Backup** button to back up the now running configuration file to your computer in the event that you need this configuration file to restore the device especially when you make some wrong configurations and you need to restore the original settings.



Do you want to open or save **romfile.cfg** (35.8 KB) from **192.168.1.254**?

UPGRADE: Click **UPGRADE** to begin the upload process. This process may take up to two minutes.



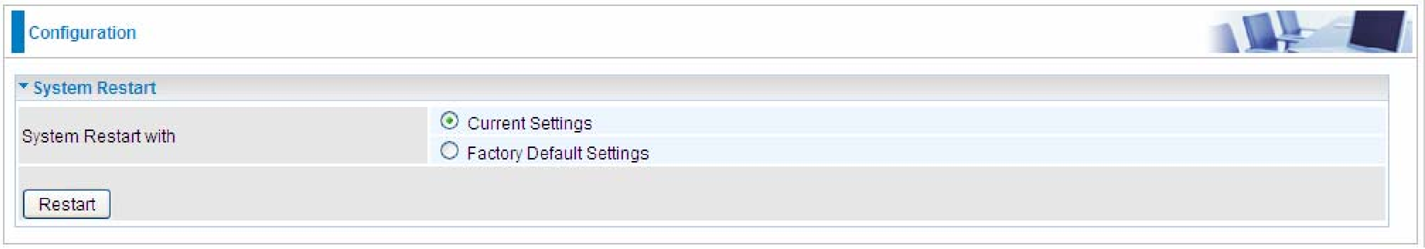
File upload succeeded, starting flash erasing and programming!!

Progress	|||||||||||||||||
Percent	16 %

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

4.4.5.4 System Restart

Click **System Restart** with option **Current Settings** to reboot your router.



System Restart with: ● Current Settings ○ Factory Default Settings

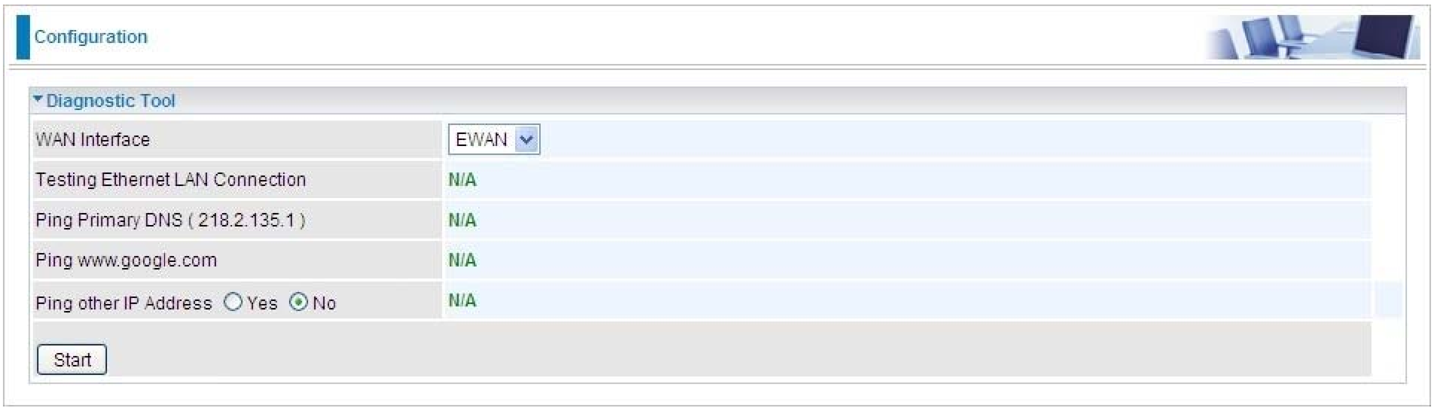
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to restore to factory default settings.

You may also restore your router to factory settings by holding the small Reset pinhole button on the back of your router in about more than 6s seconds whilst the router is turned on.

4.4.5.5 Diagnostics Tool

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

EWAN:

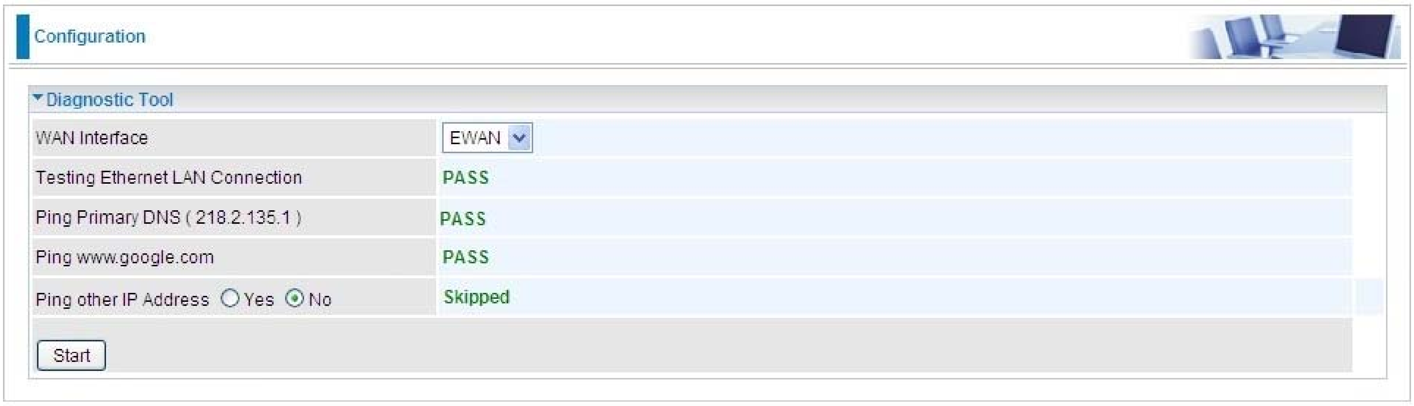


Configuration

▾ Diagnostic Tool

WAN Interface	EWAN
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (218.2.135.1)	N/A
Ping www.google.com	N/A
Ping other IP Address ○ Yes ● No	N/A

Click START to begin to diagnose the connection.



Configuration

▾ Diagnostic Tool

WAN Interface	EWAN
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (218.2.135.1)	PASS
Ping www.google.com	PASS
Ping other IP Address ○ Yes ● No	Skipped

Chapter 5
Troubleshooting

If the router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save your time and effort but if the symptoms persist, then consult your service provider.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login username and/or password.	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds

Problems with the WAN Interface

Problem	Corrective Action
Obtaining WAN IP failure	Check that your internet settings are the same as those provided by your ISP. Reboot the router if you still have problems, you may need to verify these settings with your ISP.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	1. Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. 2. Verify that the IP address and the subnet mask are consistent between the router and the PC.

Recovery procedures for non-working routers

Problem	Corrective Action
Recovery procedures for non-working routers(e.g. after a failed firmware upgrade flash)	1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately. 2. The router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (192.168.1.1), and will not respond to ping request from your PC or other telnet operations.

APPENDIX

Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User’s Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Billion

WORLDWIDE

http://www.billion.com

Federal Communication Commission Interference Statement

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

- 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.

FCC Caution:

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

(2) This device must accept any interference received, including interference that may cause undesired operation.

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

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

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.