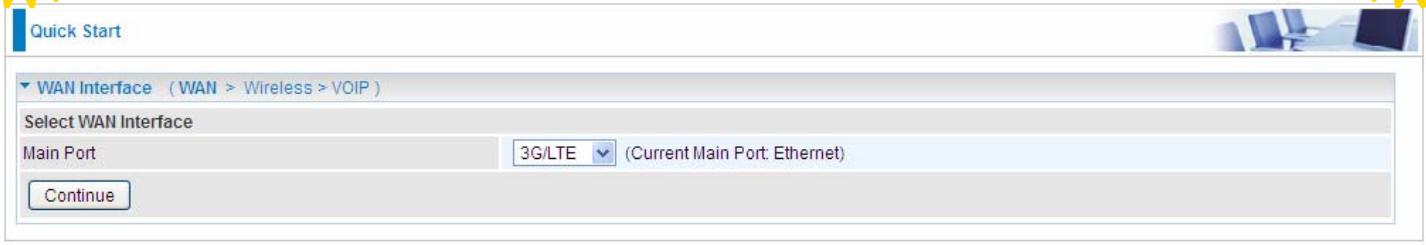
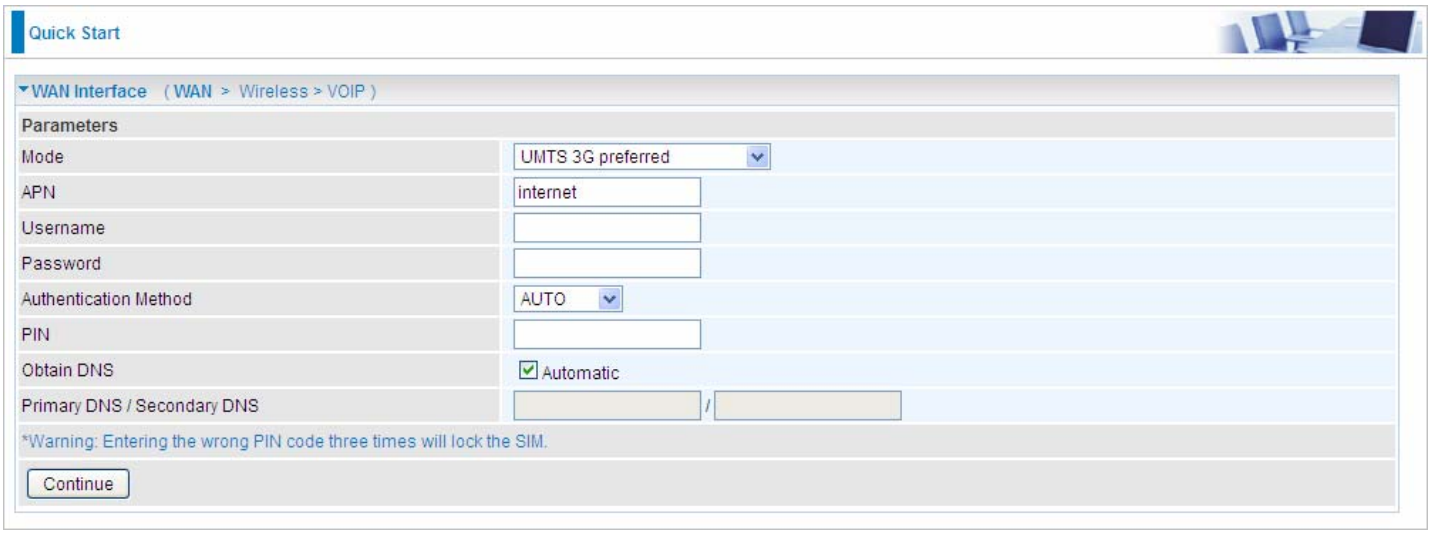
1. Select **3G/LTE,** press **Continue** to go on to next step。

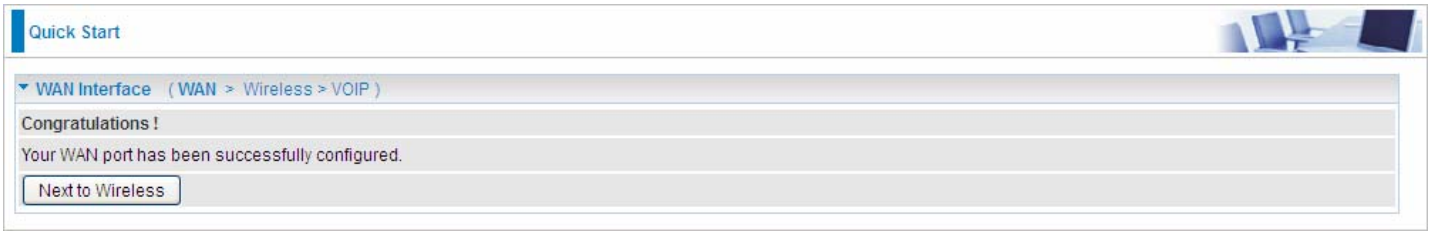


2. Select the 3G mode, and enter the APN, username, password from your ISP; and check with your ISP with the authentication method setting.

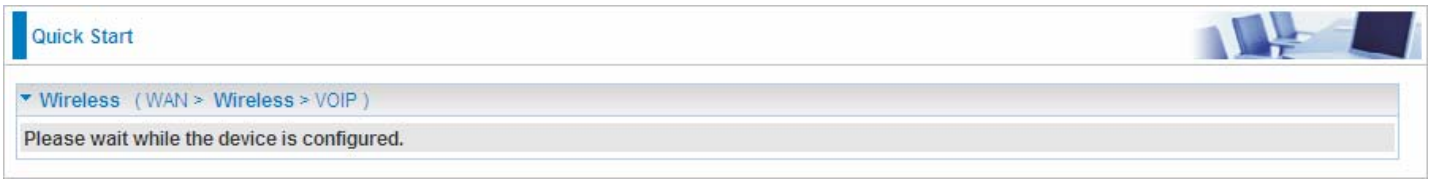


3. Wait while the device is configured.

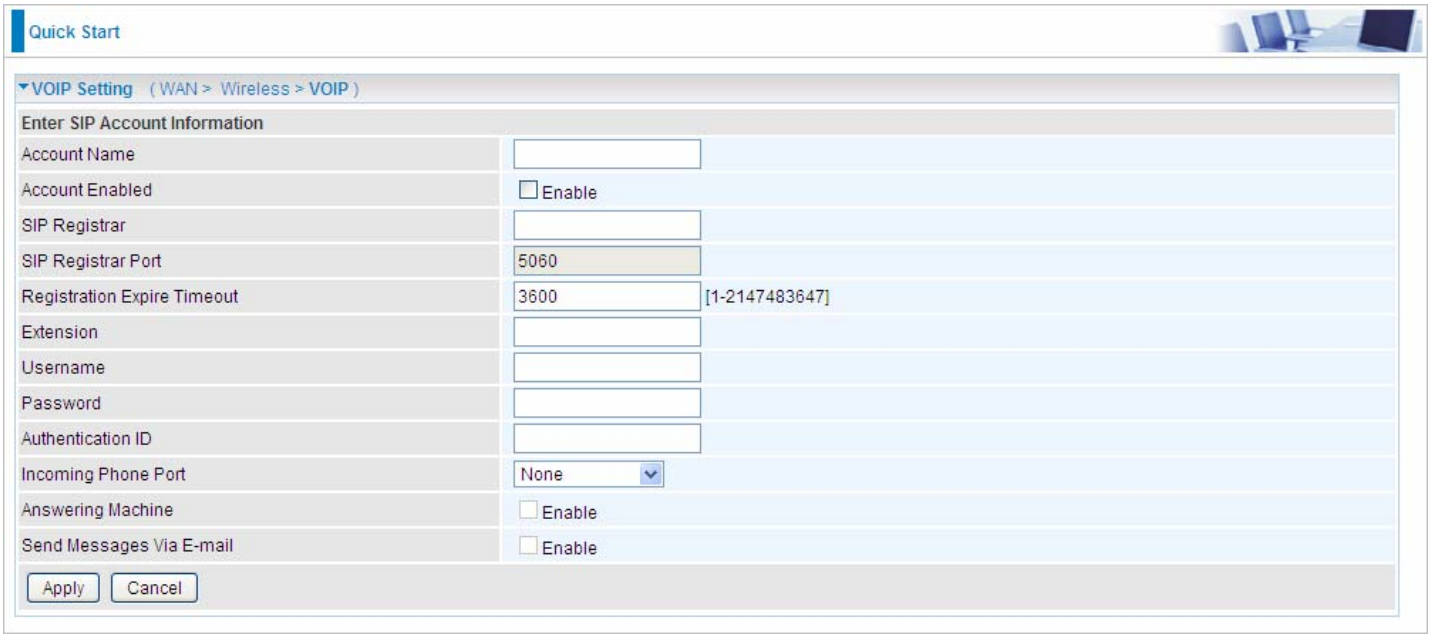
4. WAN port configuration is successful.

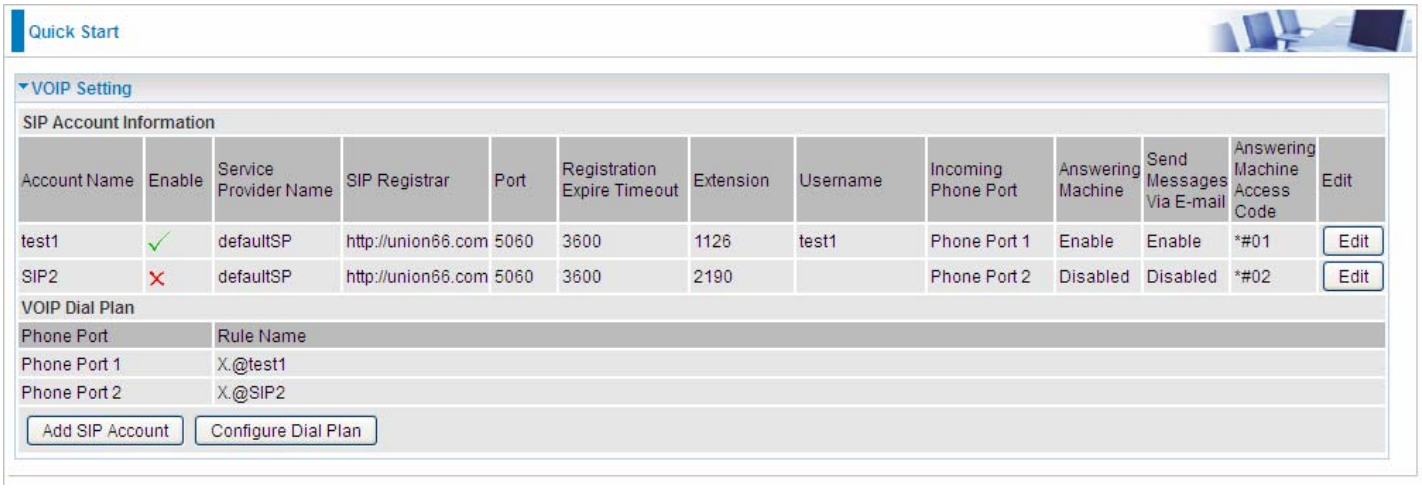


After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. In Quick Start part, users can only enable or disable the wireless and the exact SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. ... the Key, and the encryption mode will be WPA2-PSK/AES). For detail setting, please go to the Wireless part in this Manual.



7. Set the VoIP parameters. First user should turn to a VoIP service provider to register a SIP account, write down the registration information and fill it in the following blanks.





In this page, user can continue to add SIP account and configure dial plan, for more, please refer to SIP Account and VoIP Plan.

Quick Start is finished, user can turn to Status > Summary to see the basic information.

Device Information

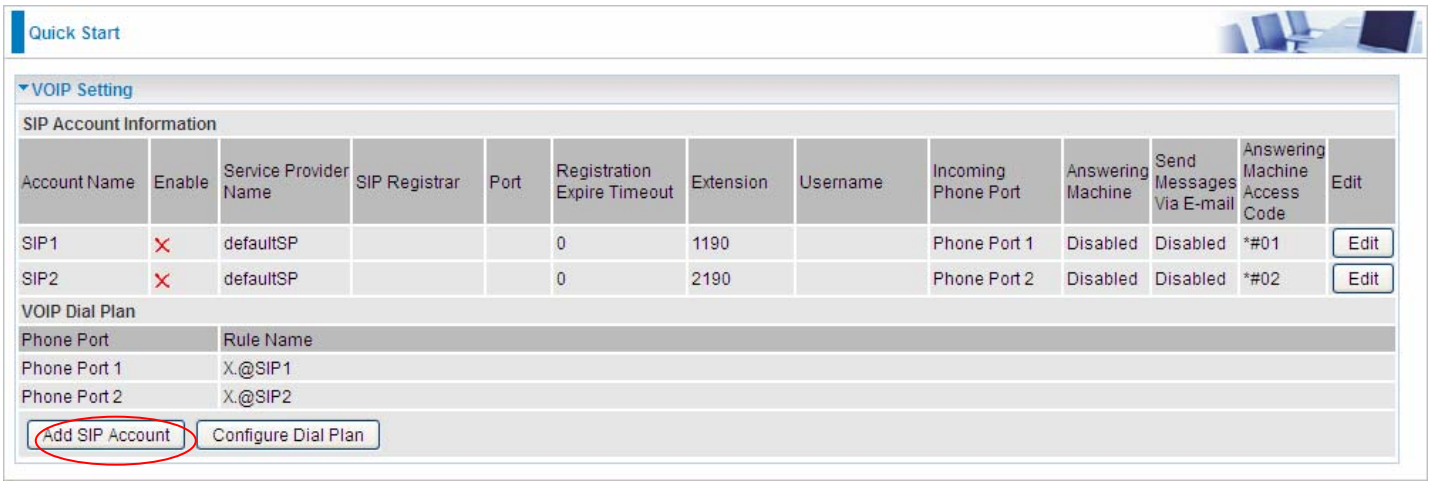
Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 15M 26S
Date/Time	Fri Jan 4 07:14:16 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:fe02:1/64
MAC Address	00:04:ed:02:00:01
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp3g0 (3G/LTE)
Connection Time	00:03:21
Primary DNS Server	221.6.4.66
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway	ppp0.1 (DSL)

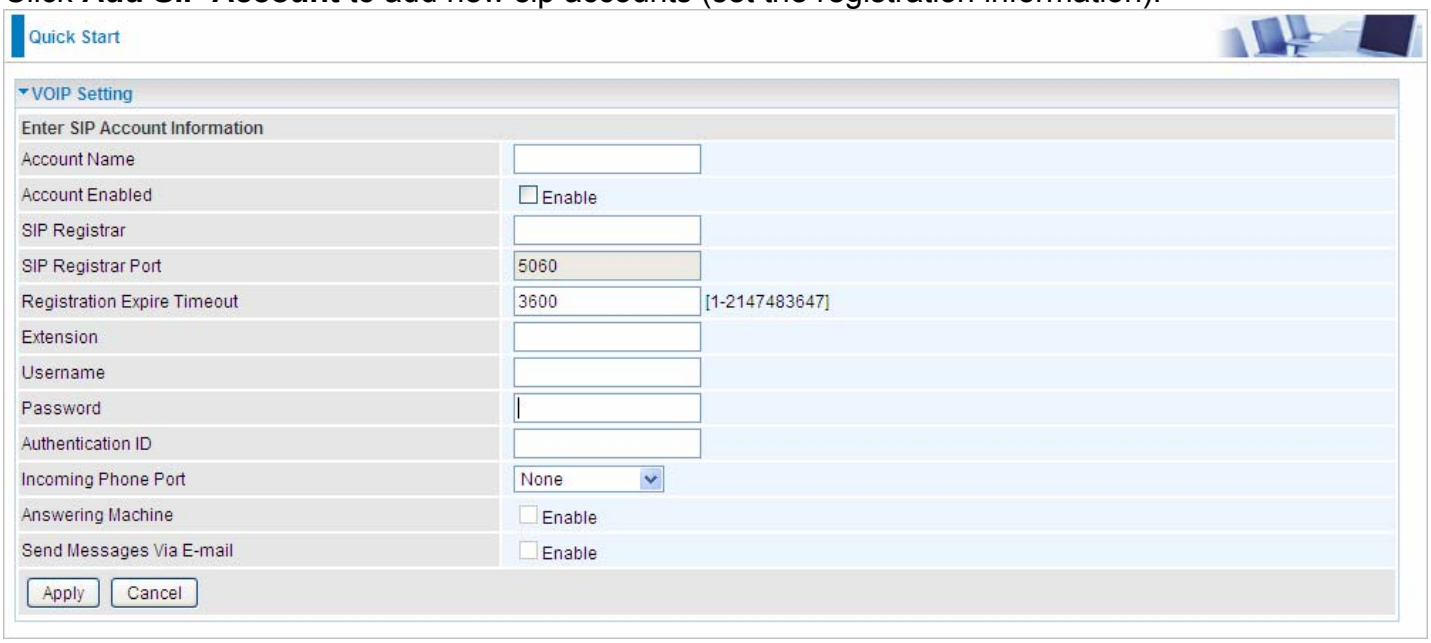
VoIP Quick Setup

"VoIP Quick Setup" links to quick VoIP setting pages. In this part, users can conduct the necessary settings (SIP account, VoIP Dial Plan, etc) of VoIP for use. For detail settings, please refer to VoIP.



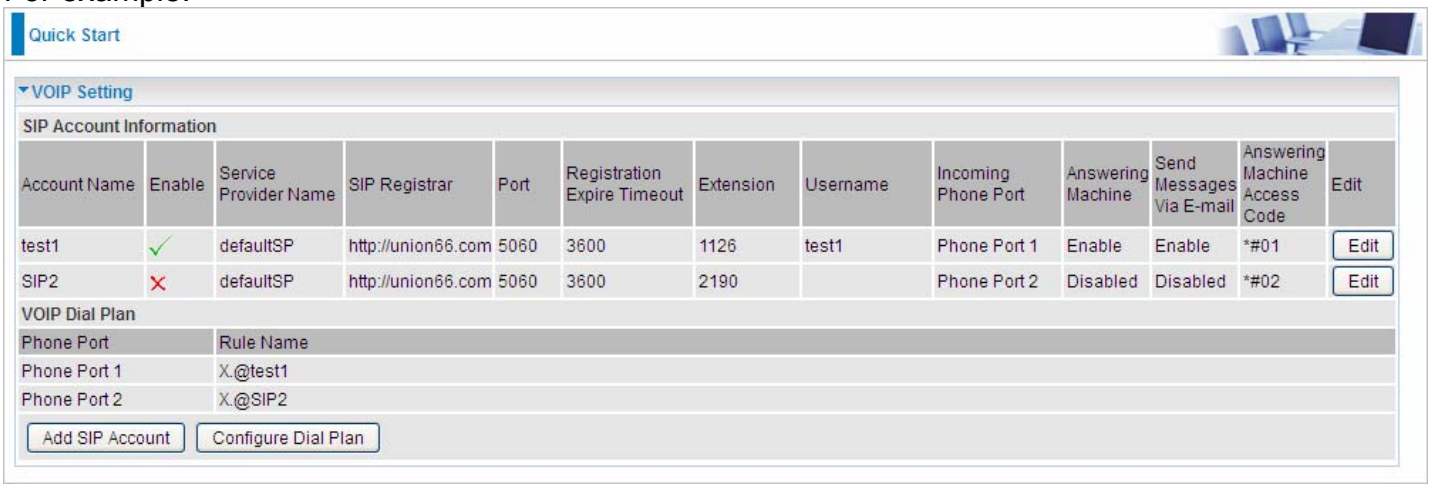
Picture1

Click **Add SIP Account** to add new sip accounts (set the registration information).

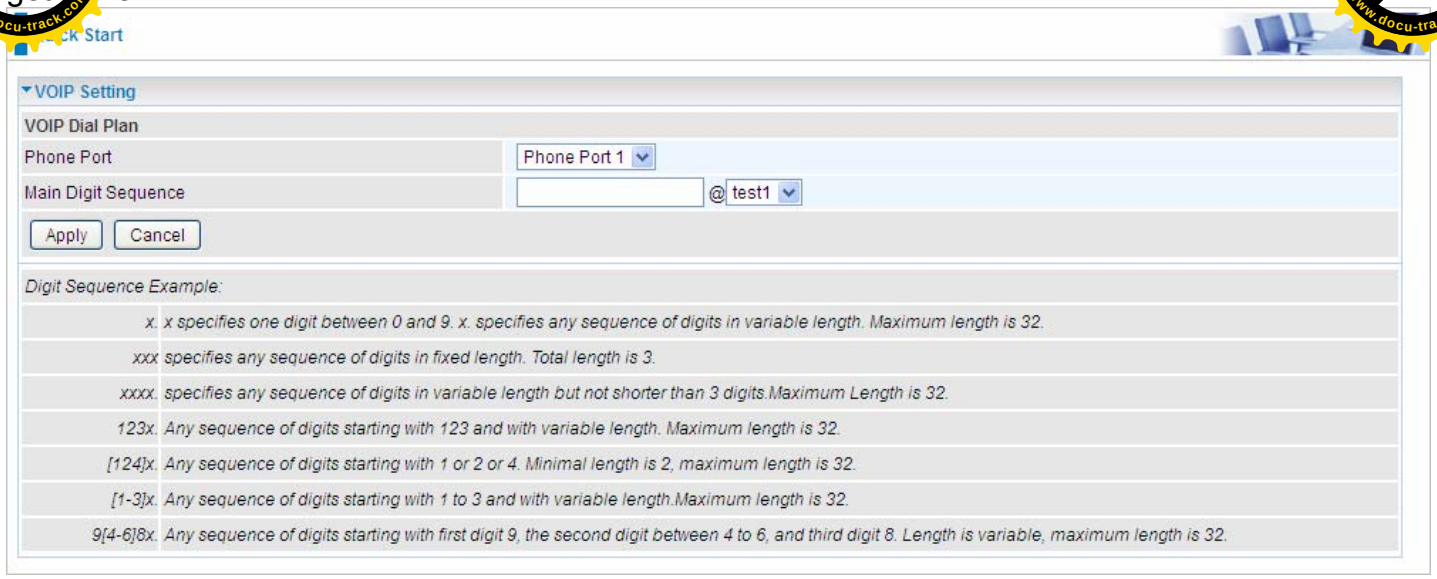


Picture2

Click **Apply** to save the settings.
For example:



In picture1, click **Configure Dial Plan** to extend to configure the dial plan. Please go to VOIP plan to get more.



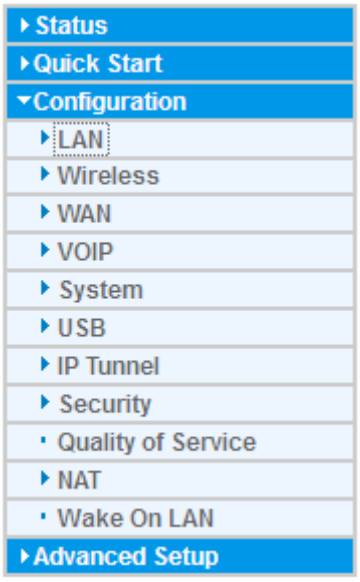
Picture3

Configuration

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

LAN, **Wireless**, **WAN**, **VOIP**, **System**, **USB**, **IP Tunnel**, **Security**, **Quality of Service**, **NAT** and **Wake On LAN**.



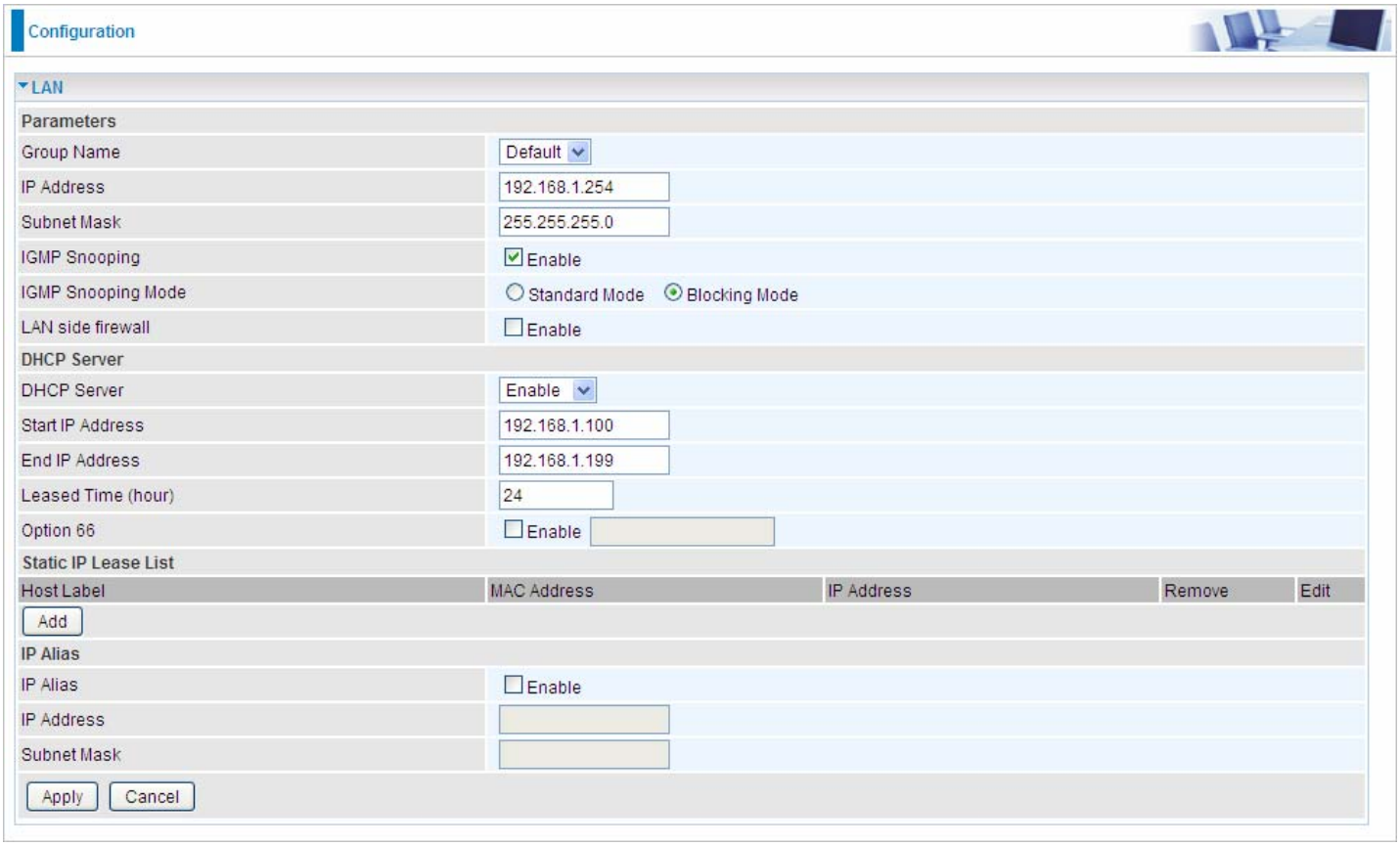
(7800VNPX)

The function of each configuration sub-item is described in the following sections.

LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building.

Ethernet



Parameters

Group Name: This refers to the group you set in **Interface Grouping** section; you can set the parameters for the specific group. Select the group via the drop-down box. For more information please refer to Interface Grouping of this manual.

IP address: the IP address of the router. Default is 192.168.1.254.

Subnet Mask: the default Subnet mask on the router.

IGMP Snooping: Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

When enabled, you will see two modes:

- **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- **Blocking Mode:** In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

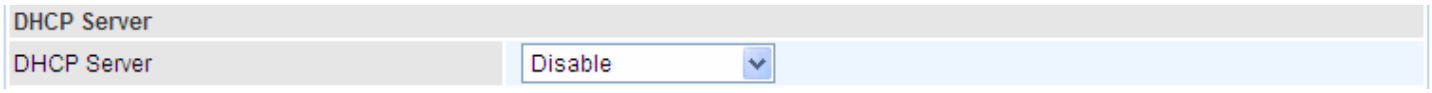
LAN side firewall: Enable to drop all traffic from the specified LAN group interface. After activating it, all incoming packets by default will be dropped, and the user on the specified LAN group interface can't access CPE anymore. But, you can still access the internet service. If user wants to manage the CPE, please turn to IP Filtering Incoming to add the allowing rules. **Note** that all incoming packets by default will be dropped if the LAN side firewall is enabled and user cannot manage this

CPE from the specified LAN group.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

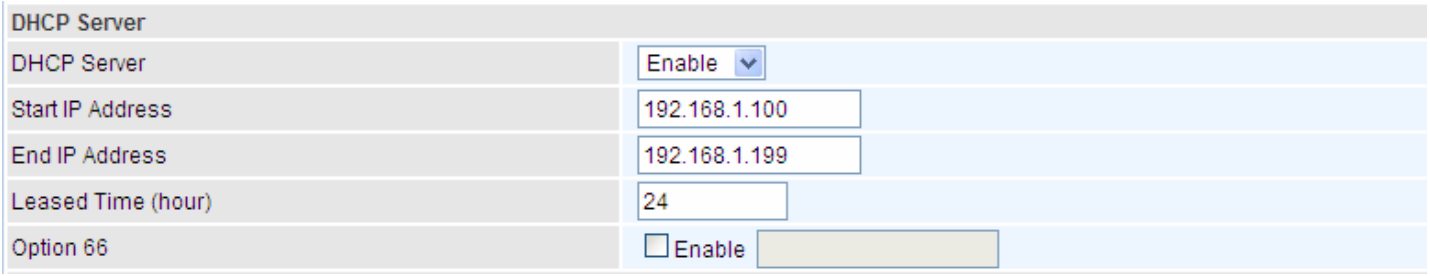
ⓘ Disable



Disable the DHCP Server function.

ⓘ Enable

Enable the DHCP function, enter the information wanted. Here as default.



Start IP Address: The start IP address of the range the DHCP Server used to assign to the Clients.

End IP Address: The end IP address f the range the DHCP Server used to assign to the Clients.

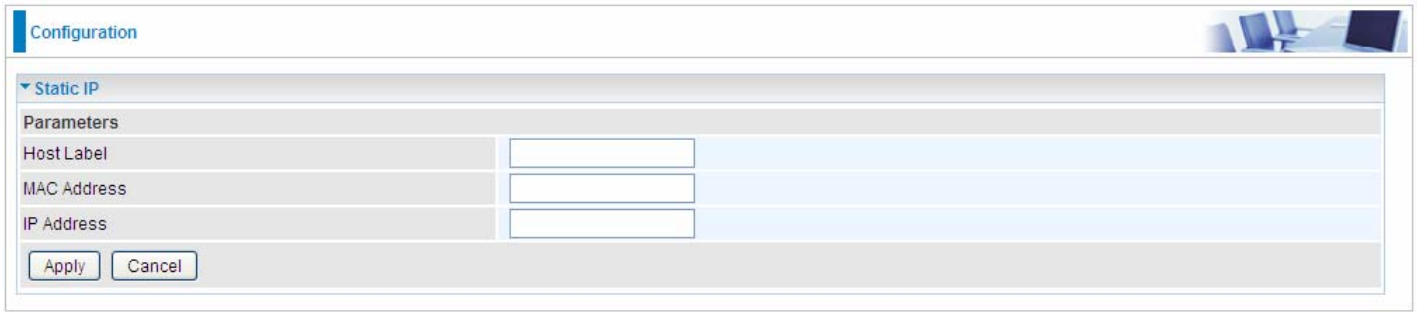
Leased Time (hour): The leased time for each DHCP Client.

Option 66: Click Enable to activate DHCP option 66 for some special devices, like IPTV Set Box. The devices can get firmware or some special service from the TFTP server. User needs to set the IP or hostname of the TFTP server.

Static IP List

The specified IP will be assigned to the corresponding MAC Address listed in the following table when DHCP Server assigns IP Addresses to Clients.

Press **Add** to the Static IP List.

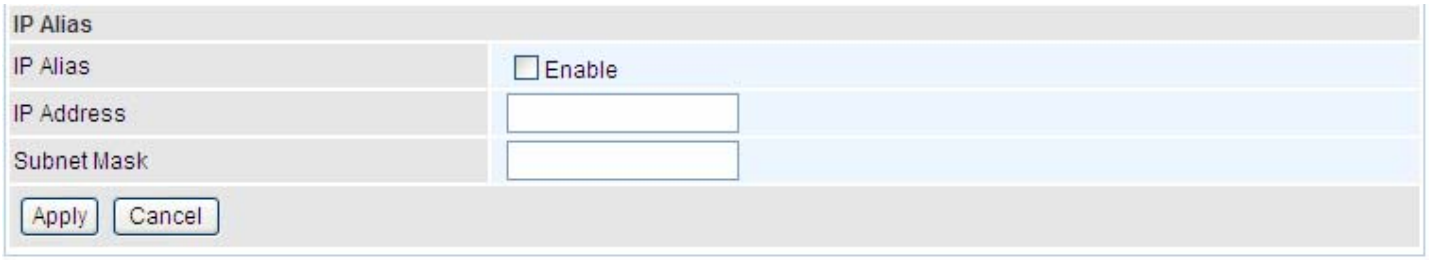


Enter the MAC Address, IP Address, and then click Apply to confirm your settings. But the IP

Assigned should be outside the range of 192.168.1.100-192.168.1.199.

IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node.



IP Alias: Check whether to enable this function.
IP Address: Specify an IP address on this virtual interface.
Subnet Mask: Specify a subnet mask on this virtual interface.

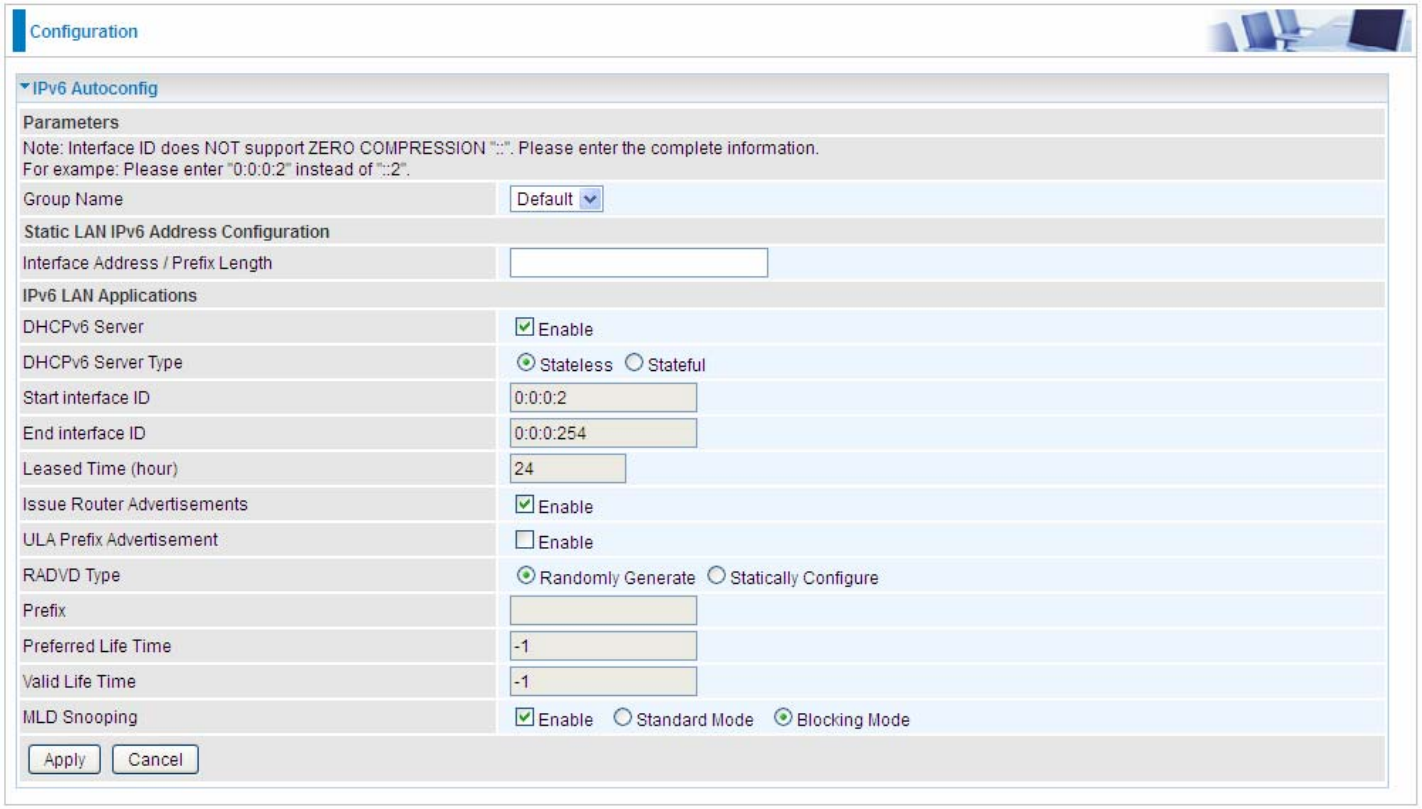
Click **Apply** to apply your settings.

IPv6 Autoconfig

The IPv6 address composes of two parts, the prefix and the interface ID.

There are two ways to dynamically configure IPv6 address on hosts. One is “stateful” configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto-configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

The second way is “stateless” configuration. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn’t configure anything on the client.



Group Name: Here group refers to the group you set in **Interface Grouping** section, you can set the parameters for the specific group. Select the group by the drop-down box. For more information please refer to **Interface Grouping** of this manual.

Static LAN IPv6 Address Configuration

Interface Address / Prefix Length: Enter the static LAN IPv6 address.

IPv6 LAN application

DHCPv6 Server: Check whether to enable DHCPv6 server.

DHCPv6 Server Type: Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is

...ilable. **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server. **Stateful:** if selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

Start interface ID: Enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

End interface ID: Enter the end interface ID.

Note: Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.
For example: Please enter "0:0:0:2" instead of "::2".

Leased Time (hour): The leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

Issue Router Advertisement: Check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

ULA Prefix Advertisement: Enable this parameter to include the ipv6 ULA address in the RA messages. ULA, unique local address, is an IPv6 address in the block fc00::/7. It is approximately the IPv6 counterpart of the IPv4 private address. They are not routable in the global IPv6 Internet.

RADVD Type: The way that ULA prefix is generated.

- ⓘ Randomly Generated
- ⓘ Statically Configured: select to set manually in the following parameters.

Prefix: Set the prefix manually.

Preferred Life Time: The ULA prefix life time. When the time is over, the ULA prefix is invalid any more, -1 means no limit.

Valid Life Time: It is a time threshold, when the time is over, clients should obtain new IPv6 address from the router through RA; -1 means to be limitless.

MLD snooping: Similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

- ⓘ **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ⓘ **Blocking Mode:** In blocking mode, the multicast data will be blocked when there is no client subscribes to a multicast group, it won't flood to the bridge ports.

State ss and Stateful IPv6 address Configuration

Stateless: Two methods can be carried.

ⓘ With DHCPv6 disabled, but Issue Router Advertisement Enabled

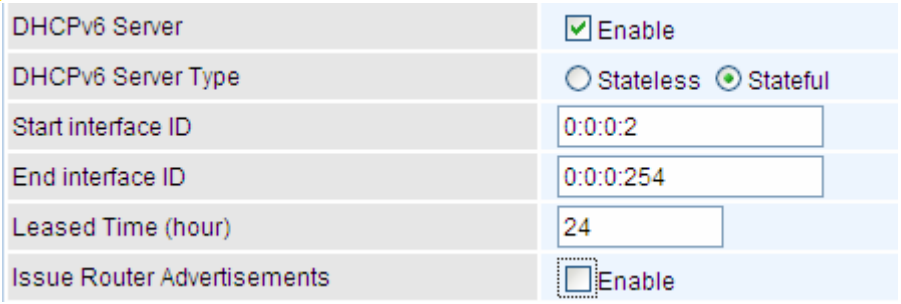
With this method, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers.

ⓘ With both DHCPv6 and Issue Router Advertisement Enabled

With this method, the PCs' addresses in LAN are configured like above method, but they can obtain such information like DNS from DHCPv6 Server.

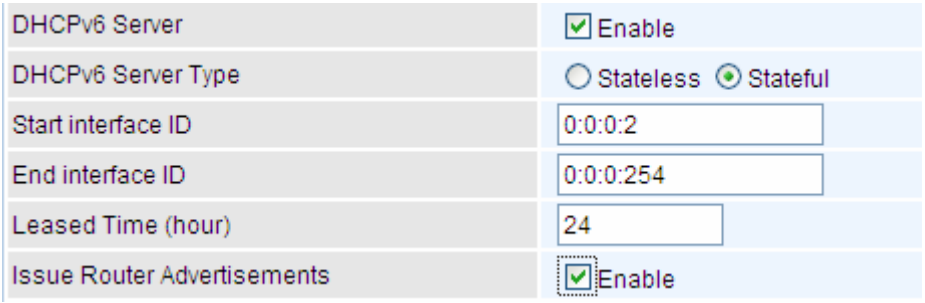
Stateful: two methods can be adopted.

With only DHCPv6 enabled



With this method, the PCs' addresses are configured the same as in IPv4, that is addresses are assigned by DHCPv6 server.

ⓘ With both DHCPv6 and Issue Router Advertisement Enabled



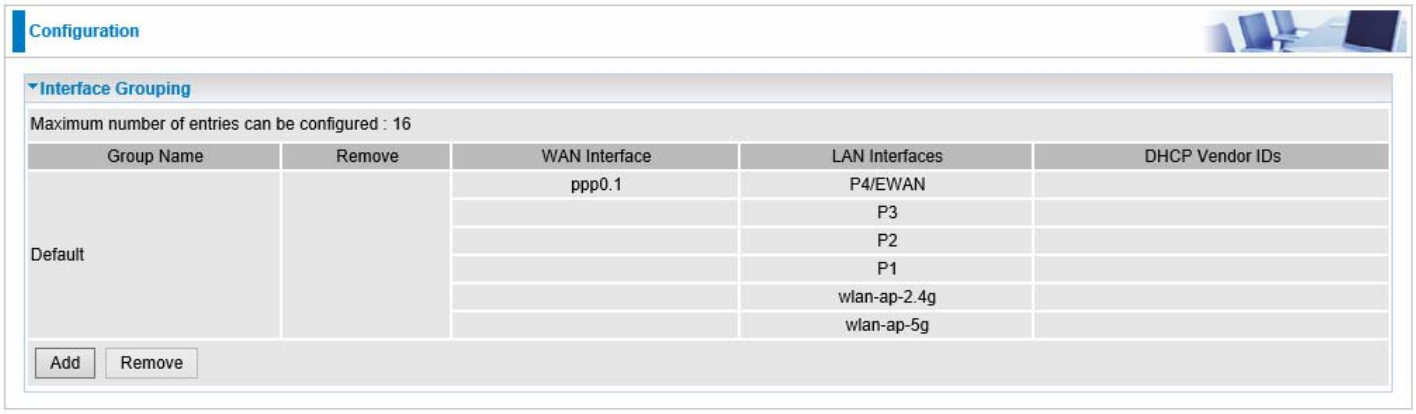
With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.

Interface Grouping

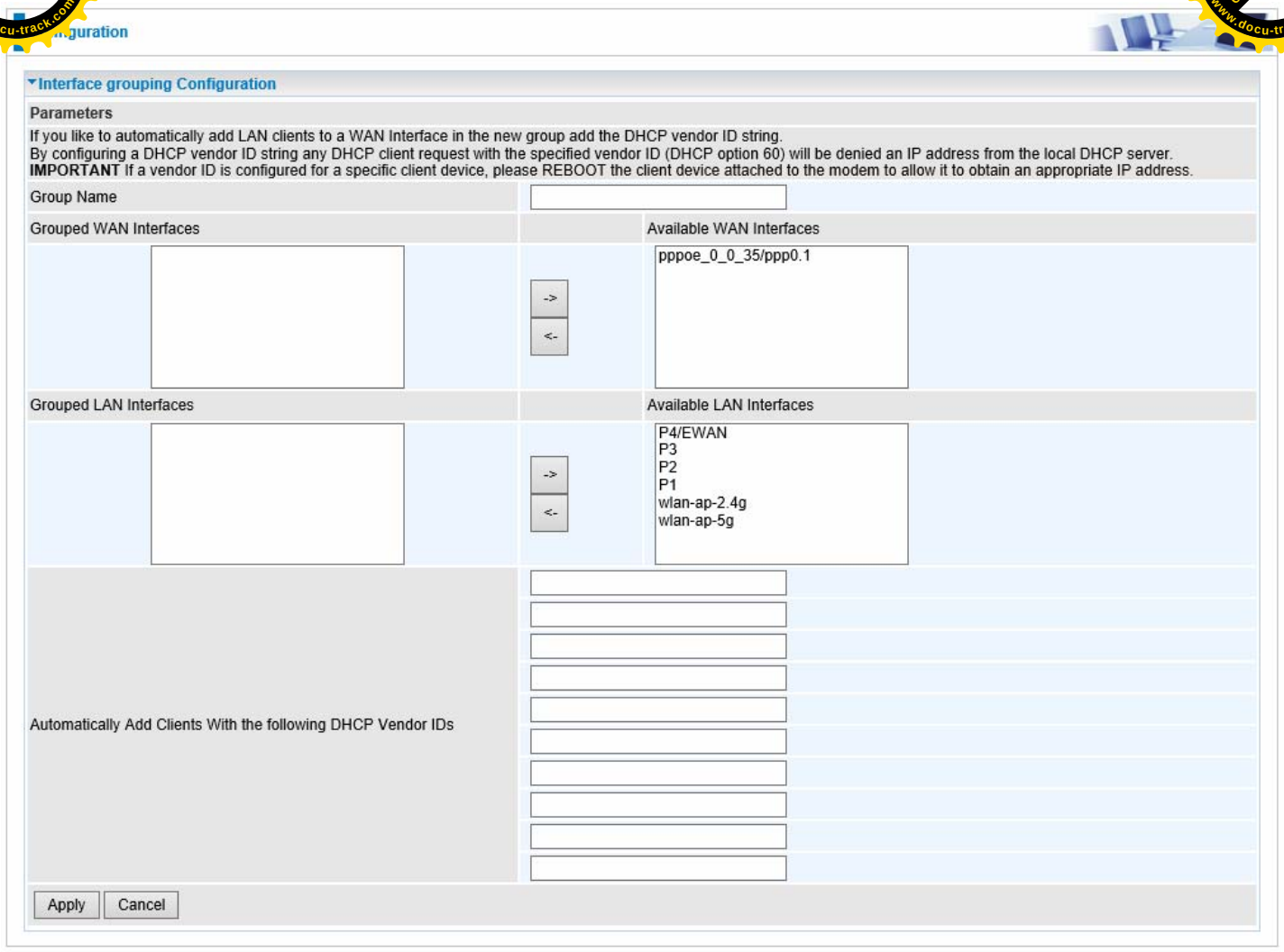
Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes 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.

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 Add button.

(Please **Note:** P4 can be configured as EWAN, and when the device is in EWAN profile, there is no P4/EWAN interface as P4 is working as a WAN port.)



Click **Add** to add groups.



Group Name: Type a group name.

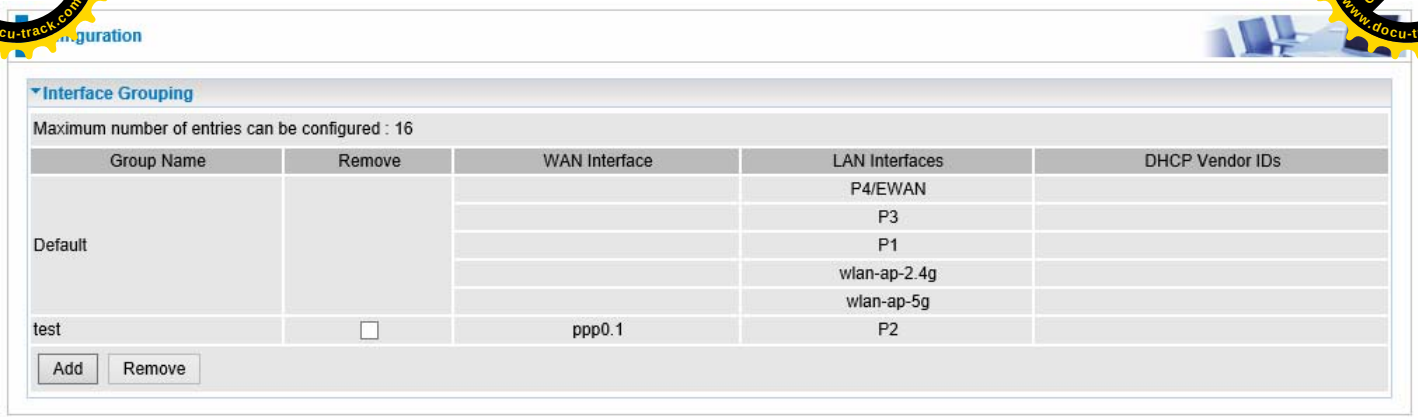
Grouped WAN Interfaces: Select from the box the WAN interface you want to applied in the group.

Grouped LAN Interfaces: Select the LAN interfaces you want to group as a single group from ***Available LAN Interfaces***.

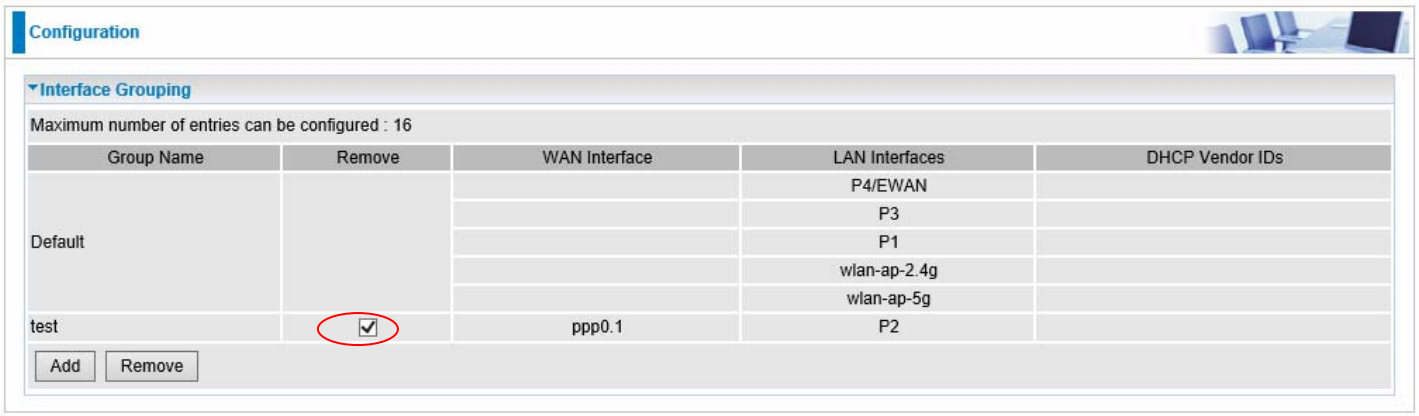
Automatically Add Clients with following DHCP Vendor IDs: Enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Click **Apply** to confirm your settings and your added group will be listed in the Interface Grouping table below.

n gro p "test", P2 and PPP0.1 are grouped in one group, they have their only network , see E N



If you want to remove the group, check the box as the following and press **Remove**.



Note: If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.

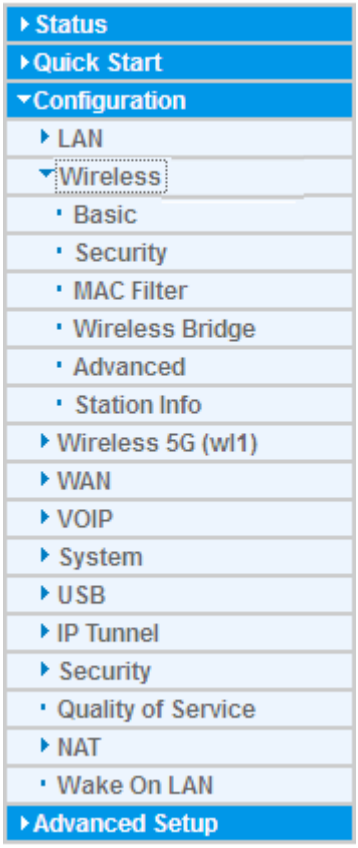
By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Each LAN interface can only be added into one group and one WAN interface can only be used in one group.

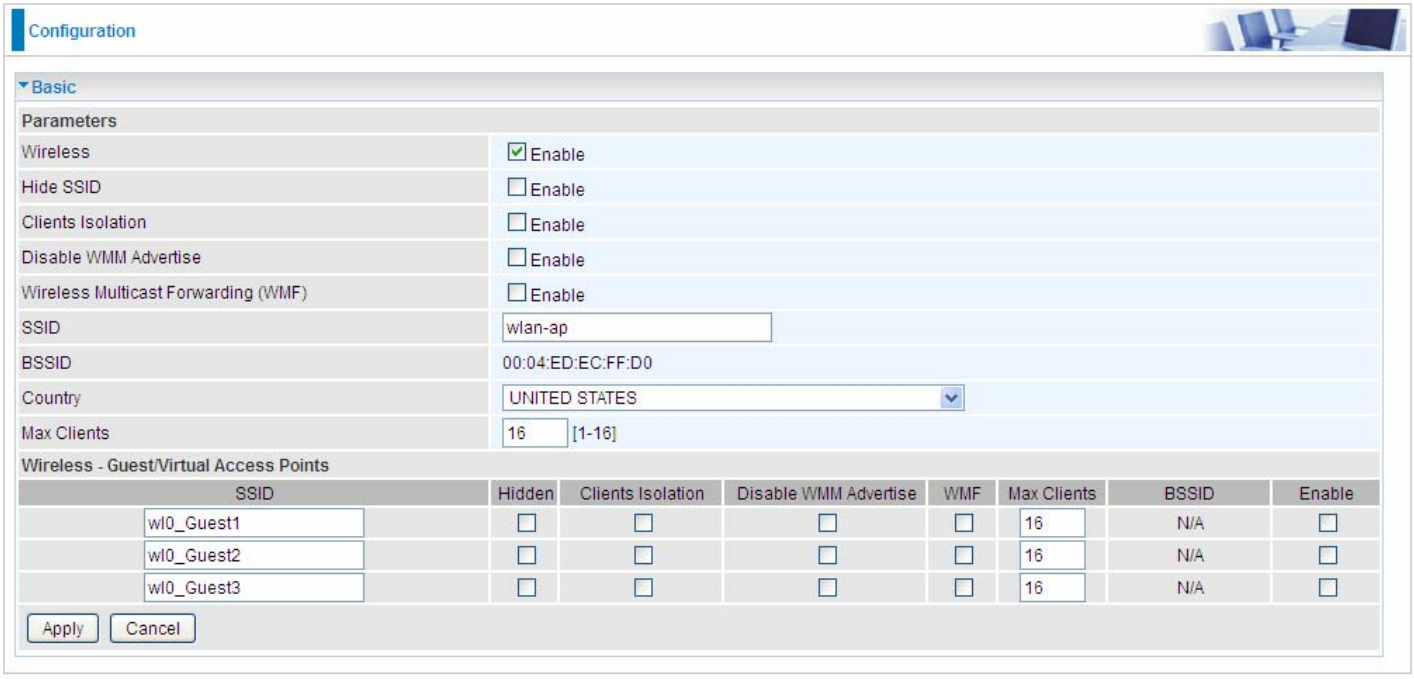
Wireless

This section provides you ways to configure wireless access. The BiPAC 7800VNP(O)X supports wireless on the 2.4GHz for users. This part has sub-items as **Basic**, **Security**, **MAC Filter**, **Wireless Bridge**, **Advanced** and **Station Info** here.



(7800VNPX)

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs.



Wireless: Default setting is set to Enable. If you do not have any wireless devices, check the checkbox again to unselect.

Hide SSID: It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

Clients Isolation: if you enabled this function, then each of your wireless clients will not be able to communicate with each other.

Disable WMM Advertise: Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).

Check to disable or enable this function.

Wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Note: SSID is case sensitive and must not exceed 32 characters.

BSSID: Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

Country: Different countries have different wireless band resources, so you can select the appropriate Country according to your location.

Max Clients: enter the number of max clients the wireless network can supports,1-16.

Guest/virtual Access Points: A "Virtual Access Point" is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple "Virtual APs", each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA

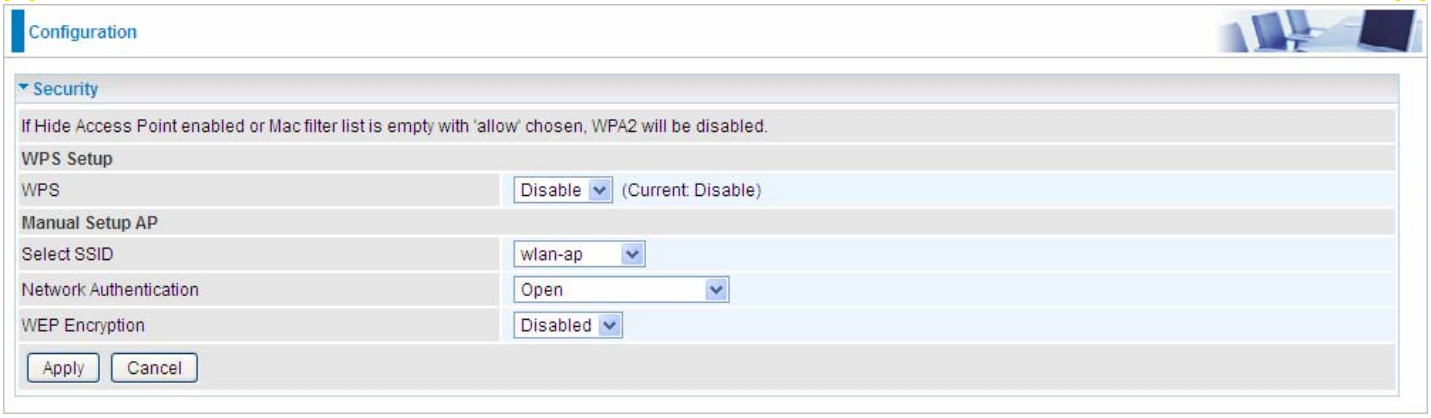
simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click **Apply** to apply your settings.

Security

Wireless security prevents unauthorized access or damage to computers using wireless network.



Note:

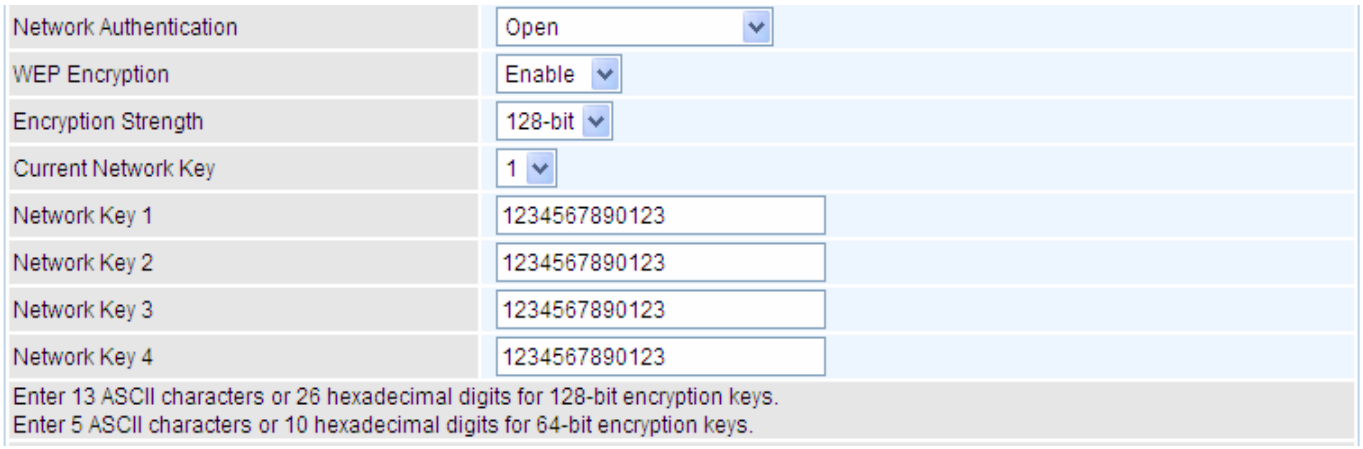
The WPS feature will also be unavailable when the security setting is not WPA2 or OPEN. So, if you manually set the wireless security setting, you should give notice to it, but you can find prompt indicating configuration.

Manual Setup AP

Select SSID: select the SSID you want these settings apply to.

Network Authentication

ⓘ **Open**



WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Encryption Strength: Select the strength, 128-bit or 64-bit.

Current Network Key: Select the one to be the current network key. Please refer to key 1- 4 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

ⓘ Shared

This is similar to network authentication 'Open'. But here the WEP Encryption must be enab

Network Authentication	Shared
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.	

ⓘ 802.1x

Network Authentication	802.1X
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.	

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

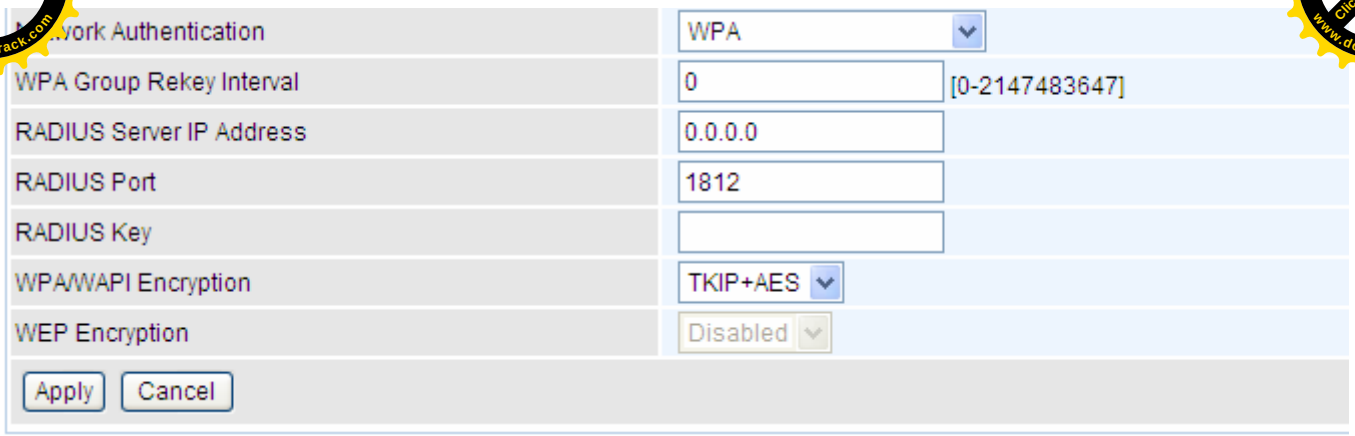
RADIUS Key: Enter the password of RADIUS authentication server.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: Select the one to be the current network key. Please refer to key 2- 3 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

ⓘ WPA



WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

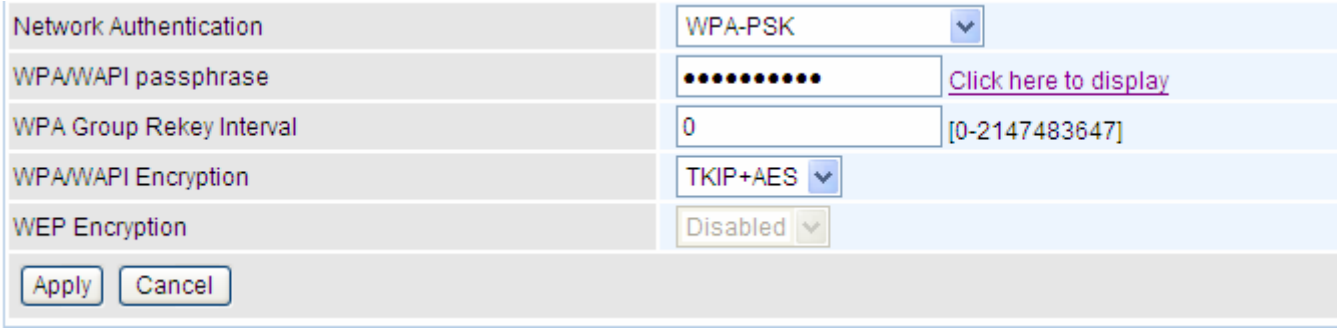
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ WPA-PSK / WPA2-PSK

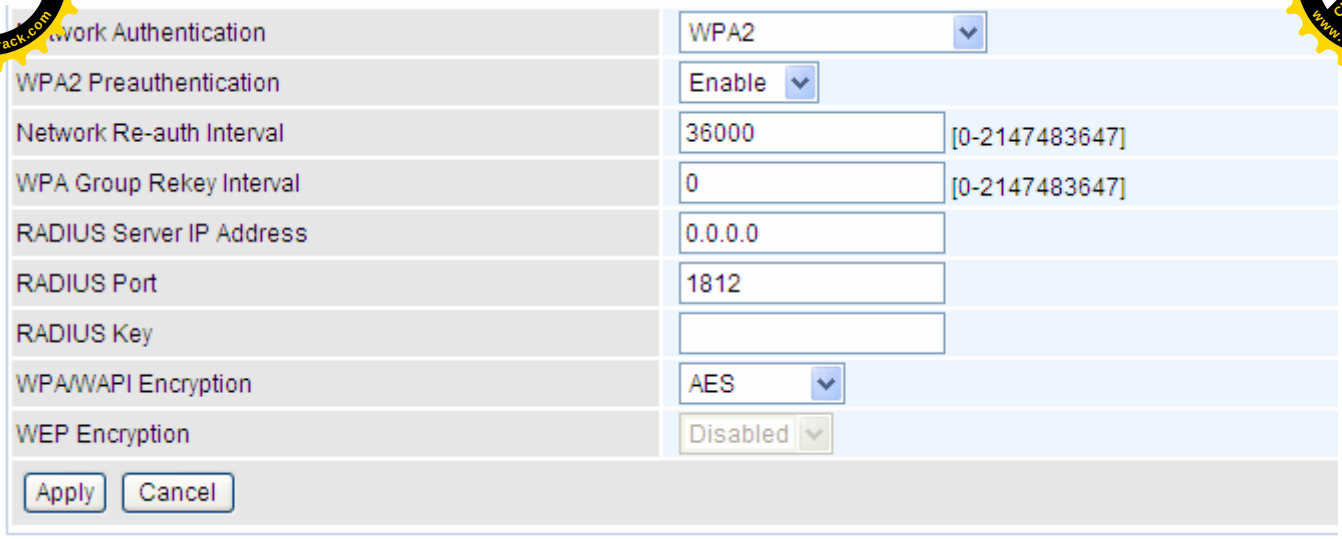


WPA/WAPI passphrase: Enter the WPA.WAPI passphrase; you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ WPA2



WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentication to the new AP, and when handoff happens, this mode will help reduce the association time.

Network Re-auth Interval: the interval for network Re-authentication. This is in seconds.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

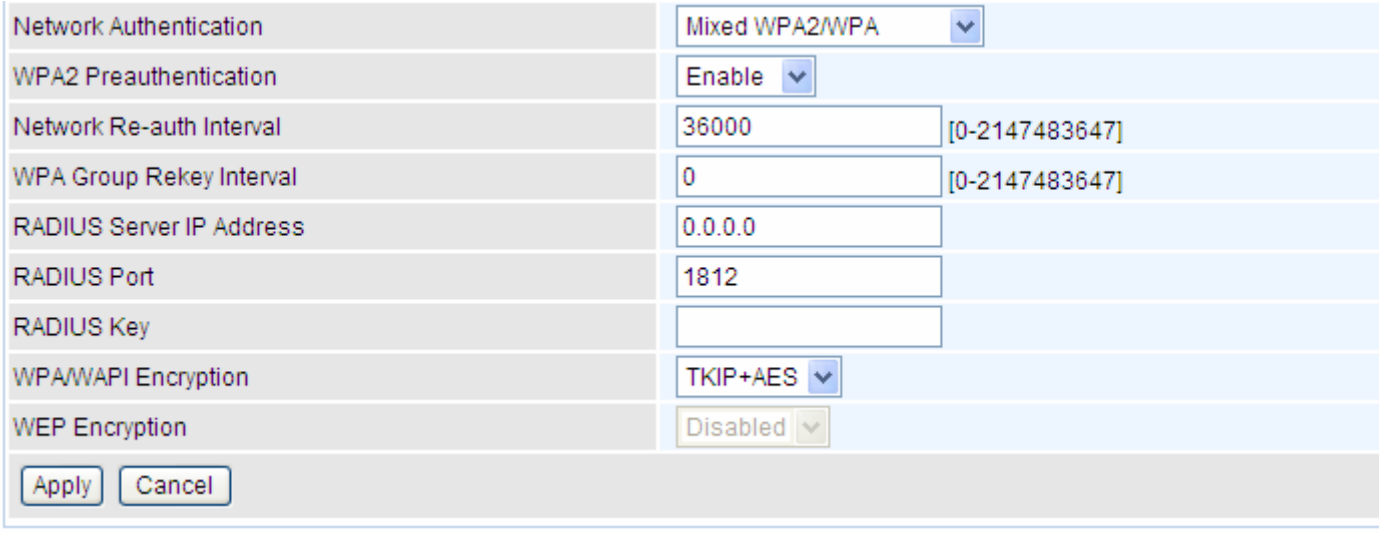
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server. This is in seconds.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ Mixed WPA2/WPA



WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ Mixed WPA2/WPA-PSk

WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPS Setup

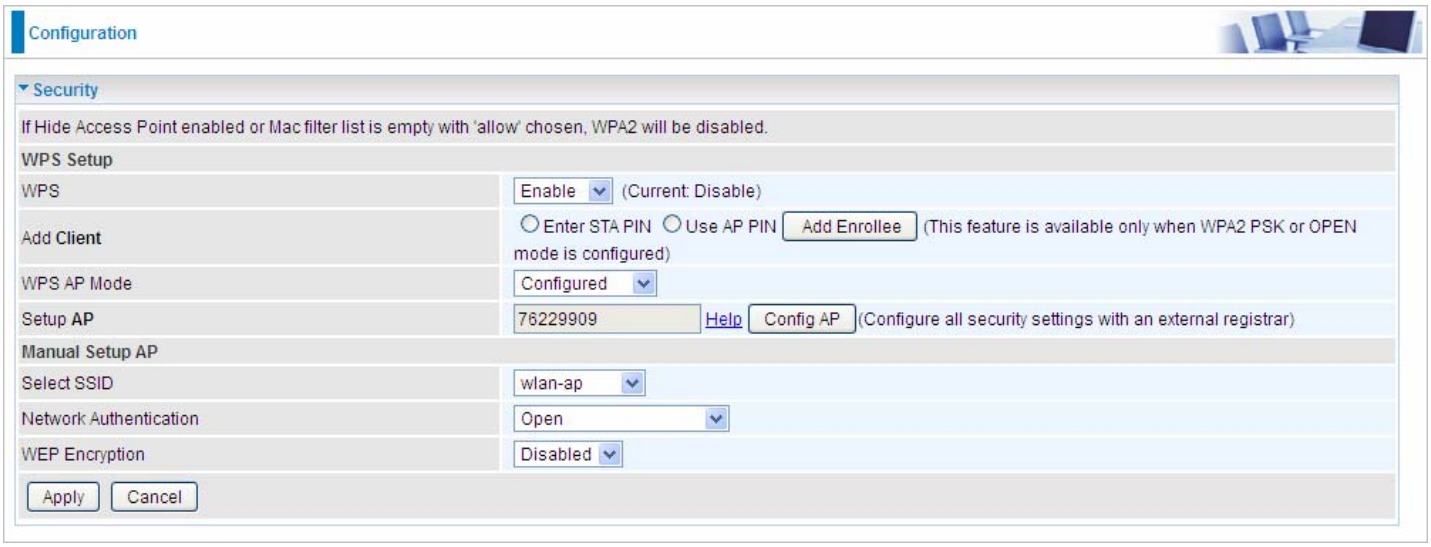
WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure Ap settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known **PIN method** is supported to configure WPS.

WPS: Select enable to enable WPS function. Please note that WPS can only be available when WPA2-PSK or OPEN mode is configured.

Note:

1) WPS feature is only available when in WPA2 or OPEN mode in security settings.

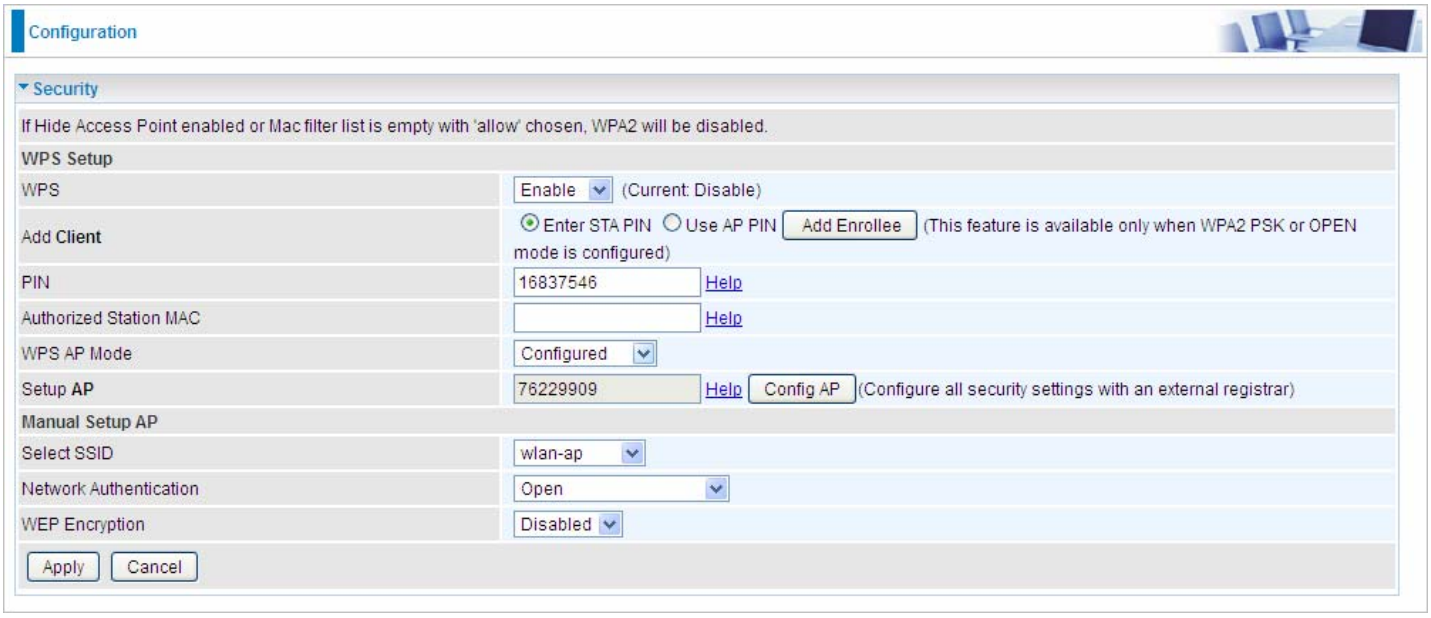
2) Here wireless can be configured as **Registrar** and **Enrollee** mode respectively. When AP is configured as Registrar, you should select “Configured” in the WPS AP Mode below, and default WPS AP Mode is “Configured”. When AP is configured as Enrollee, the WPS AP Mode below should be changed to “Unconfigured”. Follow the following steps.



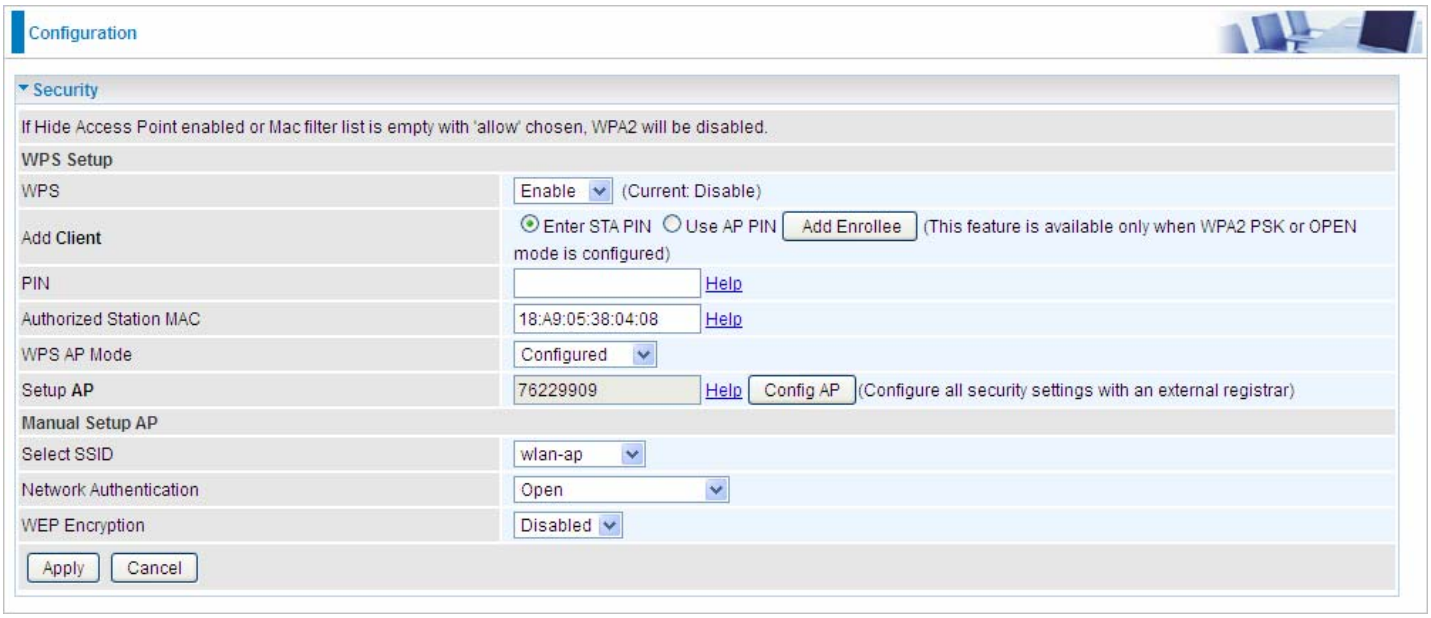
Configure AP as Registrar

Add Enrollee with PIN method

1. Select radio button "***Enter STA PIN***".
2. Input PIN from Enrollee Station (16837546 in this example), Or else users can **alternatively** enter the authorized station MAC ***Help:*** it is to help users to understand the concept and correct operation.
3. Click Add Enrolee.



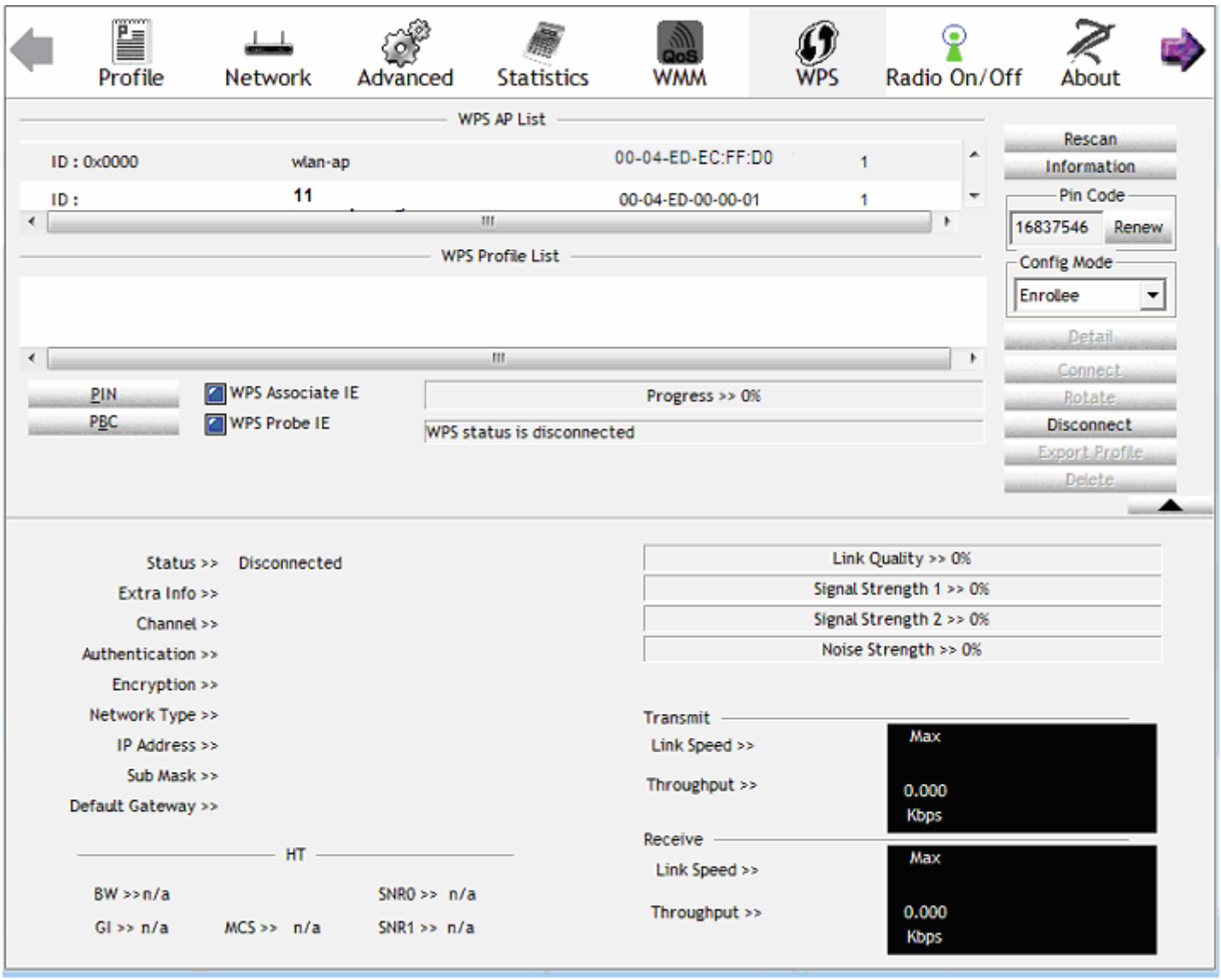
(Station PIN)



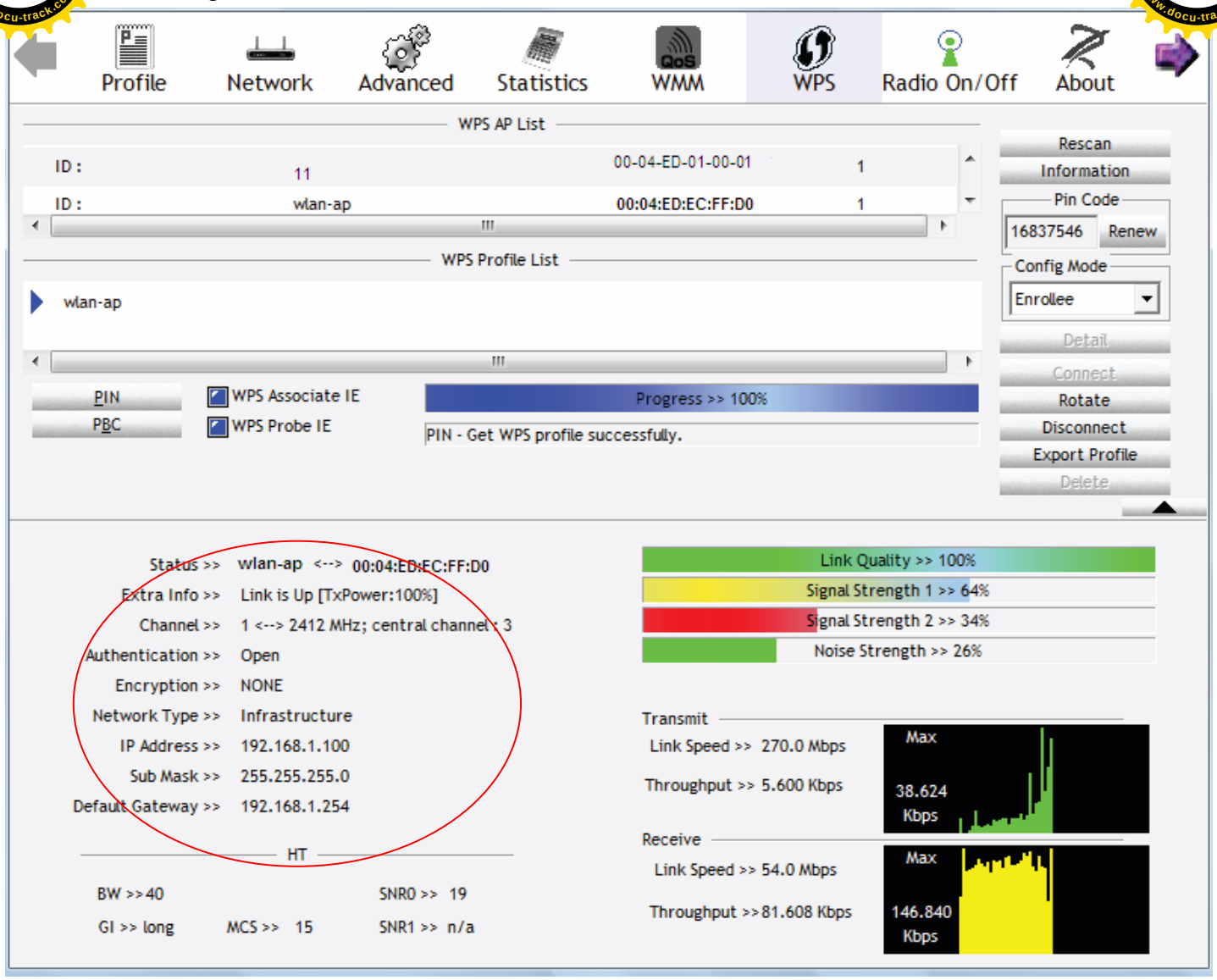
(Station MAC)

Note: Users can **alternatively** input PIN from Enrollee Station or enter the authorized station MAC.

7. Operate Station to start WPS Adding Enrollee. 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. Wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



The client's SSID and security settings will now be configured to match the SSID and security settings of the registrar.



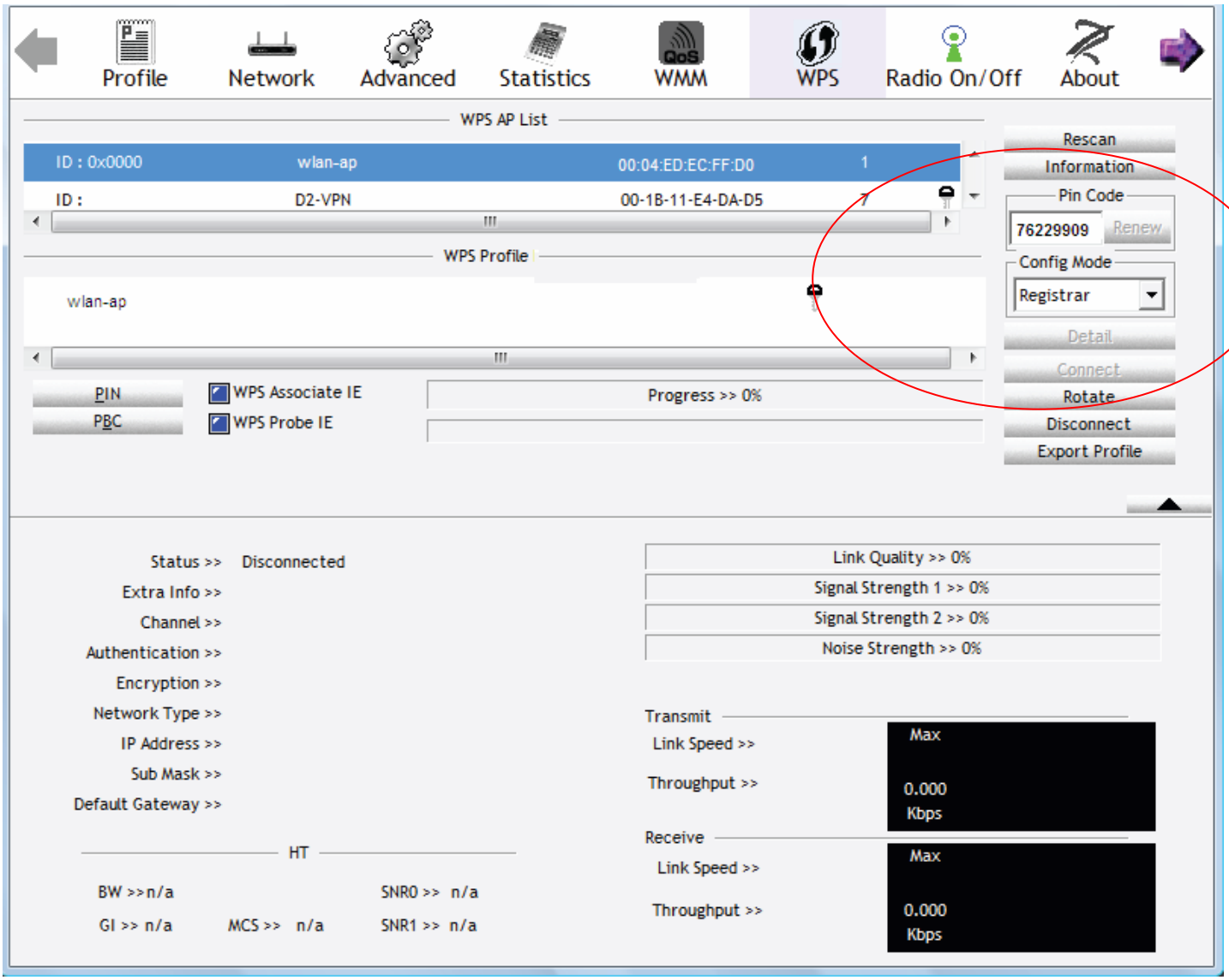
You can check the message in the red ellipse with the security parameters you set, here we all use the default.

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

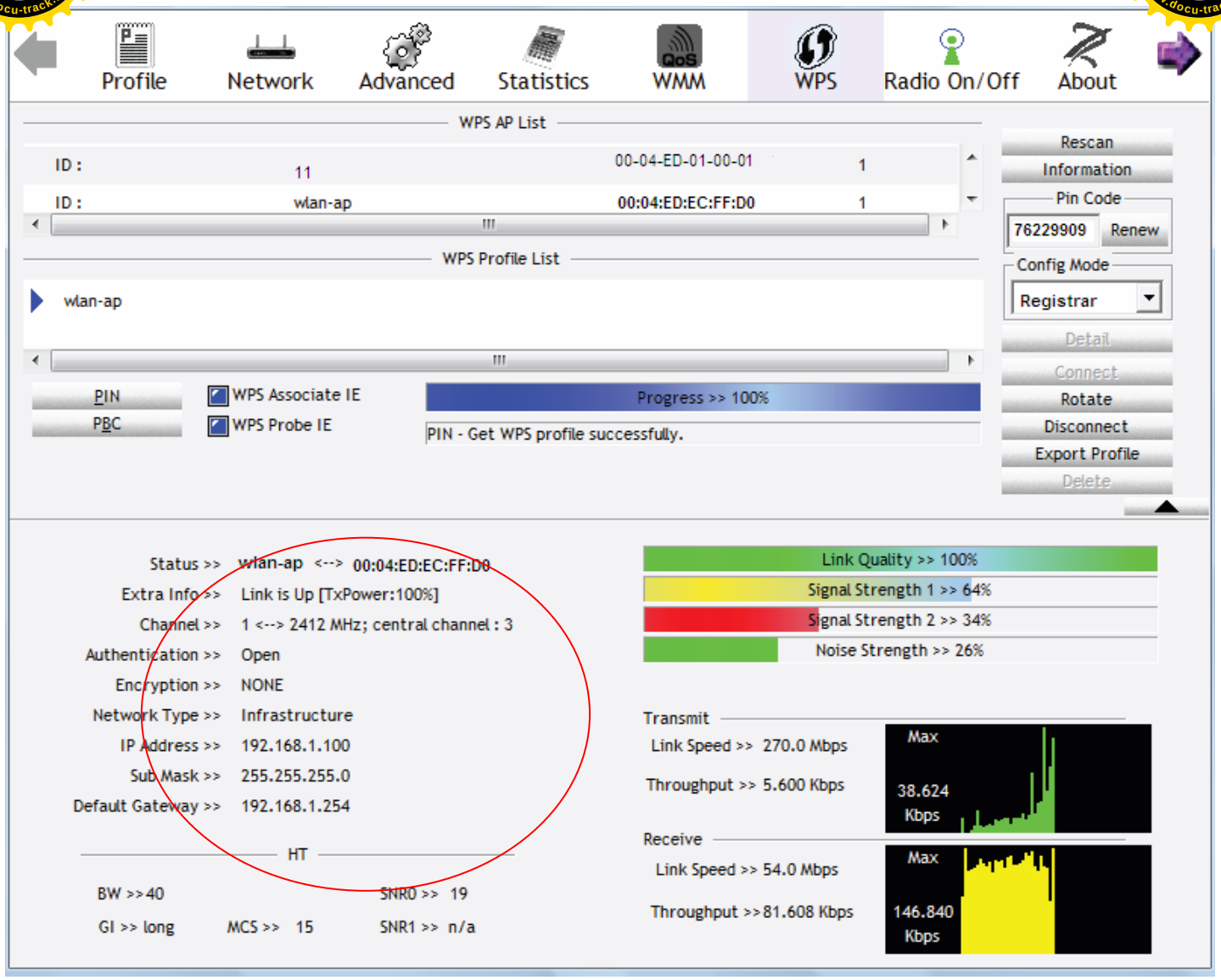
Add Registrar with PIN Method

1. Set AP to “***Unconfigured Mode***” and Click “***Config AP***” button.

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as **Registrar**. Enter the **PIN** number (76229909 (device) for example) in the PIN Code column then choose the select AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run scan.



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



4. Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.

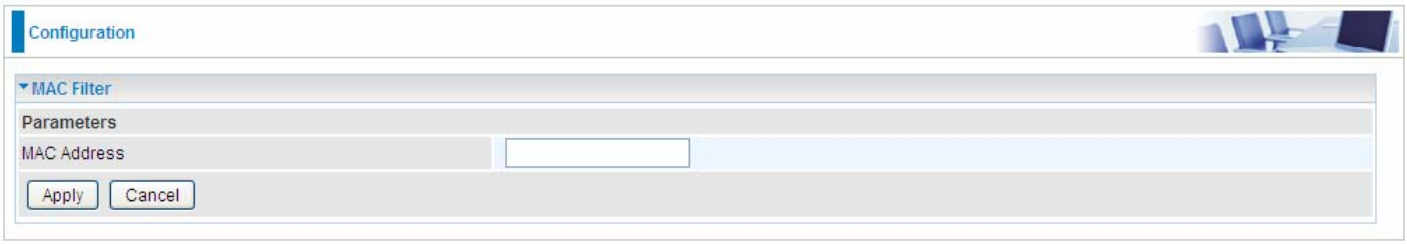
MAC Filter

Select SSID: select the SSID you want this filter applies to.

MAC Restrict Mode:

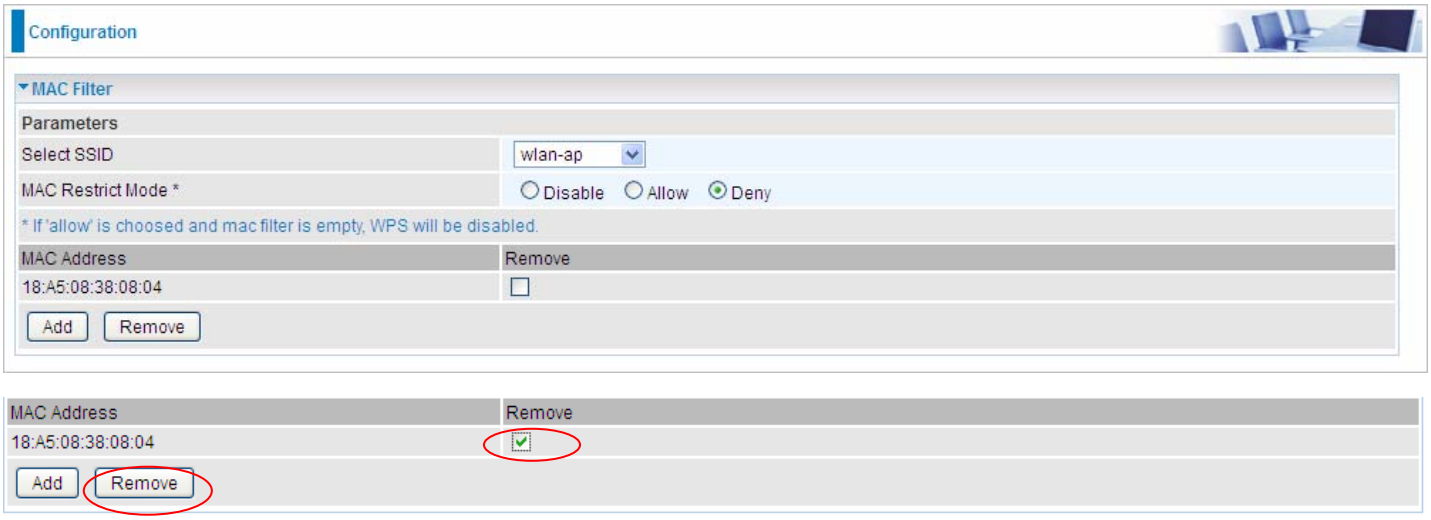
- **Disable:** disable the MAC Filter function.
- **Allow**: allow the hosts with the following listed MACs to access the wireless network.
- **Deny**: deny the hosts with the following listed MACs to access the wireless network.

Click **Add** to add the MACs.



MAC Address: enter the MAC address(es). The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click **Apply** to apply your settings and the item will be listed below.

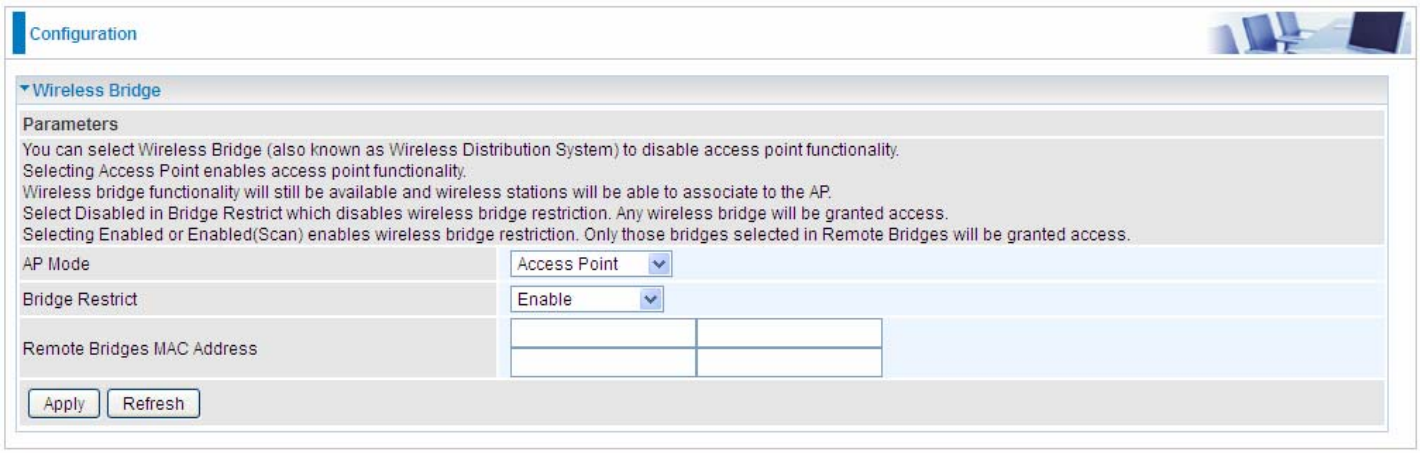


If you don't need a rule, check the remove checkbox and press **Remove** to delete it.

Wireless Bridge

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access points. It's easy to install, simply define the peer's MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

Here you can select what role the AP server has, AP or wireless bridge (WDS).



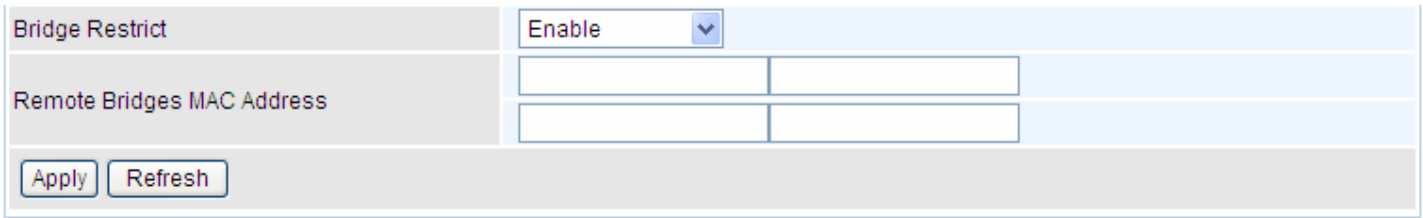
AP Mode: determines whether the gateway will act as an Access point or as a Bridge.

- **Access Point**: the gateway communicates with both clients and bridges.
- **Wireless Bridge**: the gateway communicates with other WDS devices only. In this mode, the gateway doesn't communicate with client devices.

If your wireless network includes repeaters that use WDS, the gateway in wireless bridge mode will also communicate with your repeaters. The gateway in wireless bridge mode will not communicate with a repeater that uses a proprietary (non-WDS) mode.

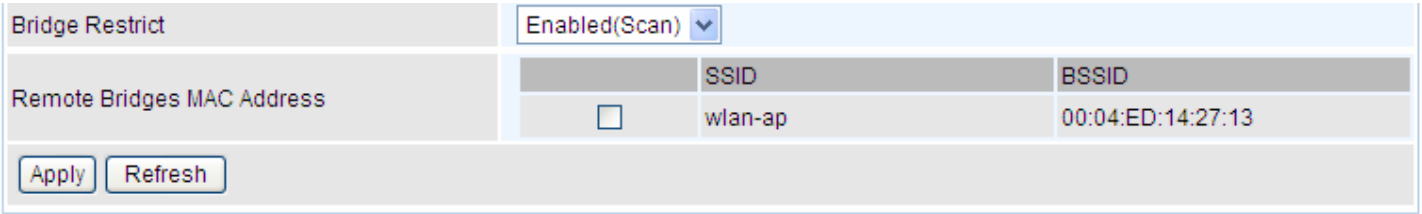
Bridge Restrict: When **AP Mode** is set to **Wireless Bridge**, this determines whether the gateway will communicate with all other bridges or only specific ones:

- **Enable:** to enable wireless bridge restriction. Only those specified in the Remote MAC Address the gateway can communicate with.



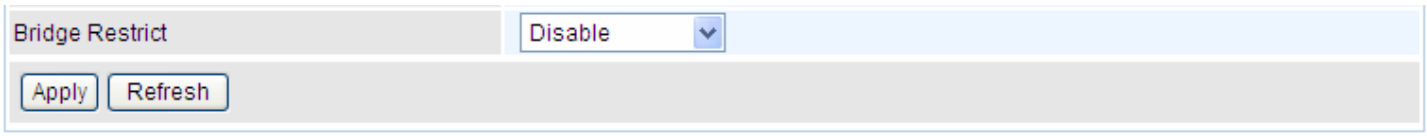
Remote Bridge MAC Address: enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

- **Enabled (Scan):** to enable wireless bridge restriction. Only those scanned by the gateway can communicate.



Remote Bridge MAC Address: select the remote bridge MAC addresses.

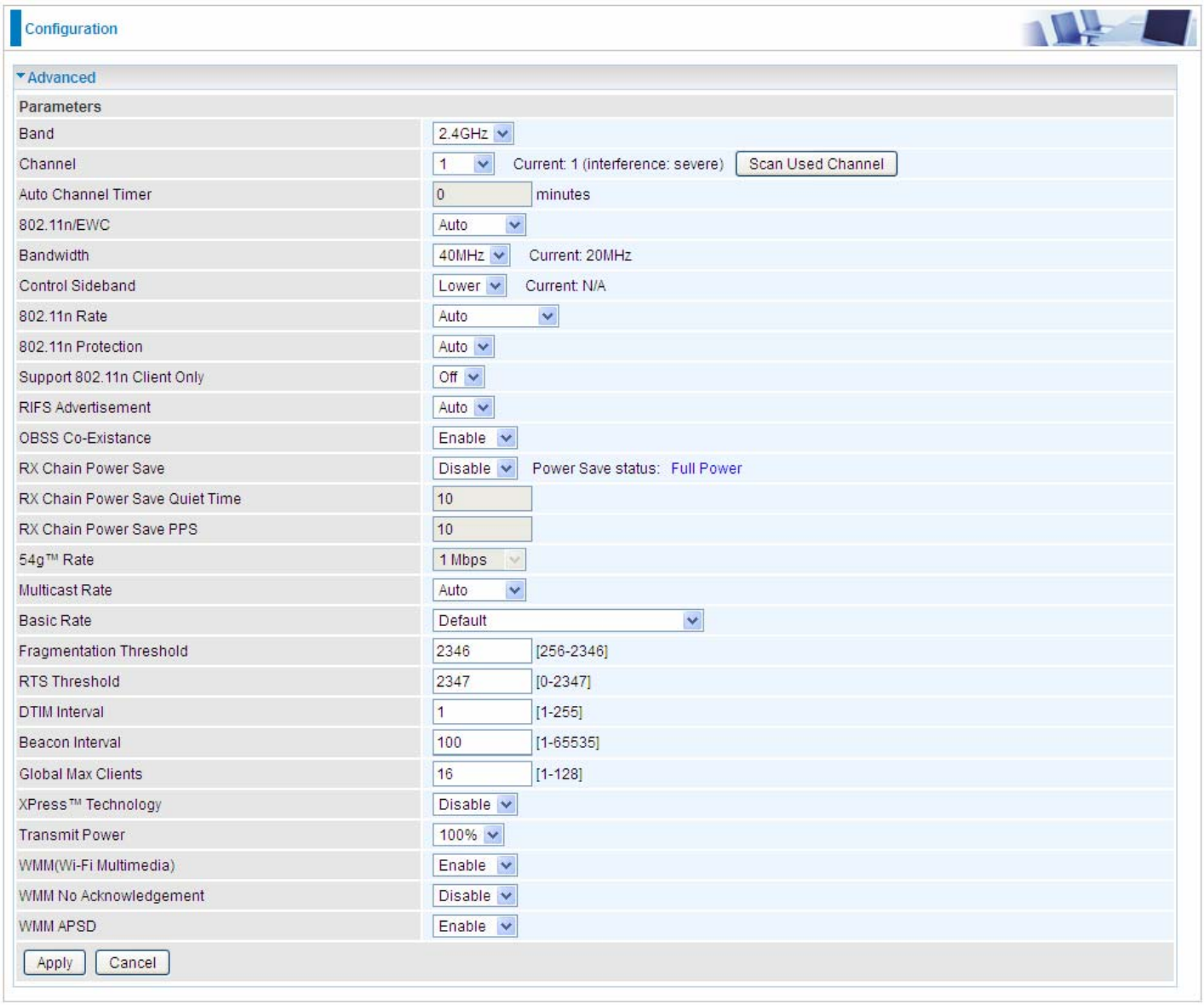
- **Disable:** Does not restrict the gateway communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.



Click **Apply** to apply your settings.

Advanced

Advanced users can set some advanced parameters about wireless.



Band: Select frequency band.

Channel: Allows channel selection of a specific channel (1-7) or Auto mode.

Scan Used Channel: Press the button to scan and list all channels being used.

Auto Channel Timer (min): The auto channel times length it takes to scan in minutes. Only available for auto channel mode.

802.11n/EWC: select to auto enable or disable 802.11n.

Bandwidth: Select bandwidth. The higher the bandwidth the better the performance will be.

Control Sideband: only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower sideband**) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: This allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximize throughput. Auto for greater security.

Support 802.11n Client Only: turn on the option to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is a 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select to disable this function or auto to enable this function.

OBSS Co-Existence: coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

RX Chain Power Save: Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

RX Chain Power Save Quiet Time: The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

RX Chain Power Save PPS: The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a specific kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Regulatory Mode: select to deny any regulatory mode. There are two regulatory modes:

802.11h: The standard solves interference problems with e.g. satellites and radar using the same band as 802.11a or 802.11n dual-band access points.

802.11d: This standard automatically adjusts its allowed frequencies, power levels and bandwidth accordingly to the country it's located in.
This means that manufacturers don't need to make country specific products.

Transmit Power: select the transmitting power of your wireless signal.

WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Station Info

Here you can view information about the wireless clients.

MAC Address: The MAC address of the wireless clients.

Associated: List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list

Authorized: List those devices with authorized access**.**

SSID: Show the current SSID of the client.

Interface: To show which interface the wireless client is connected to.

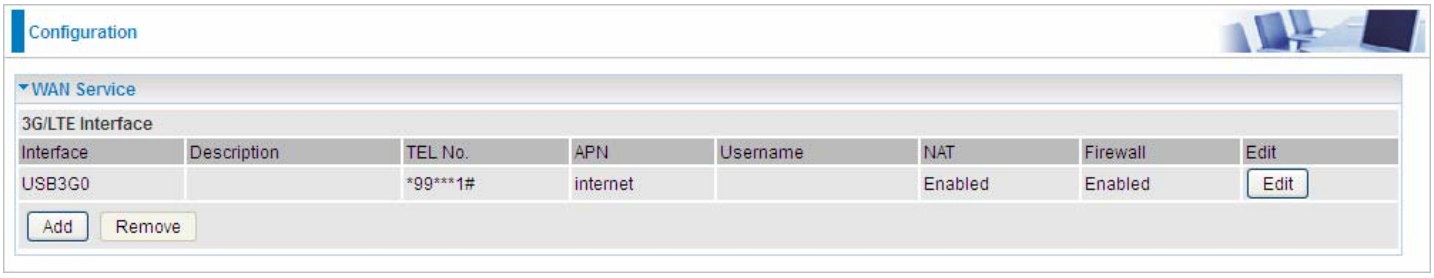
Refresh: To get the latest information.

WAN-Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems.

WAN Service

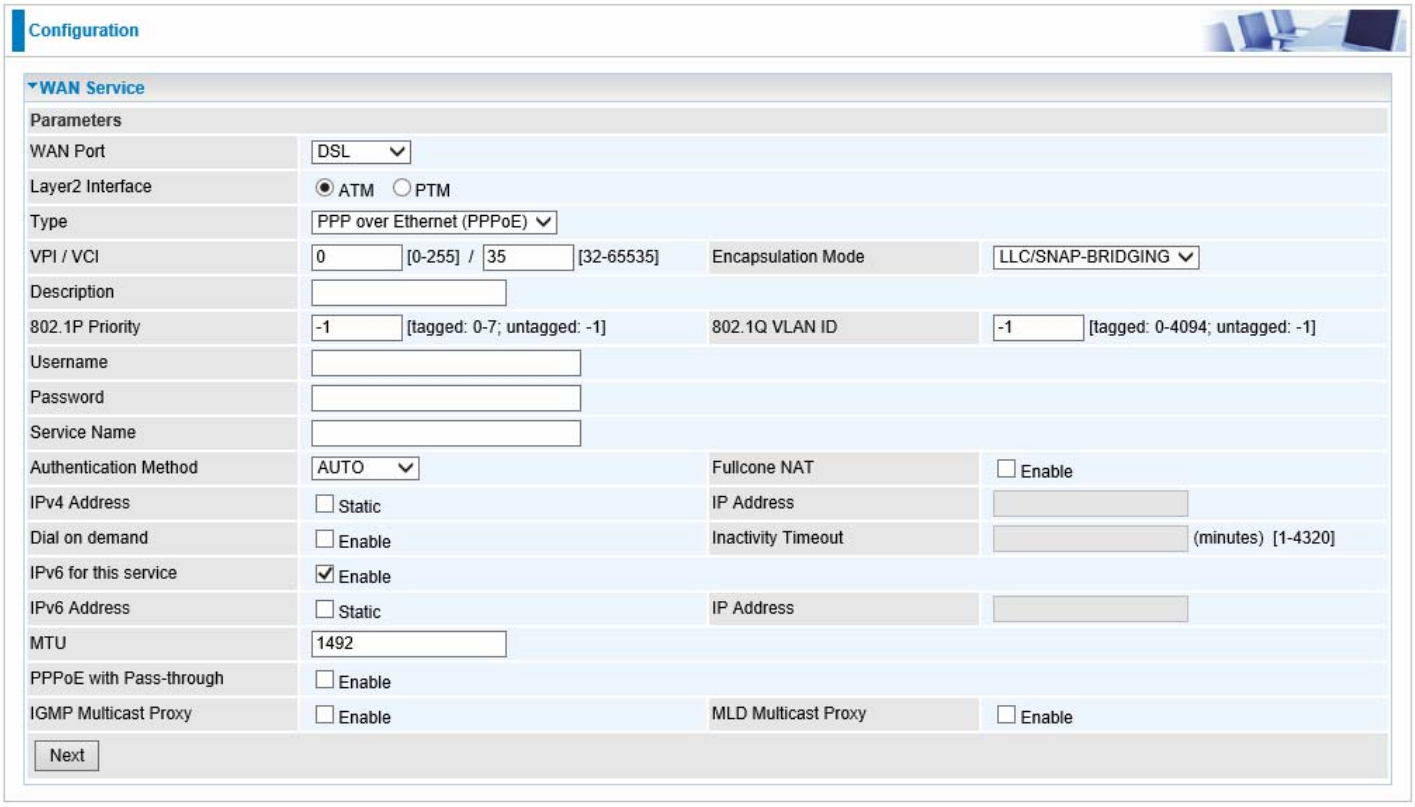
Two WAN interfaces are provided for WAN connection: DSL and Ethernet.



Click **Add** to add new WAN connections.

ⓘ DSL

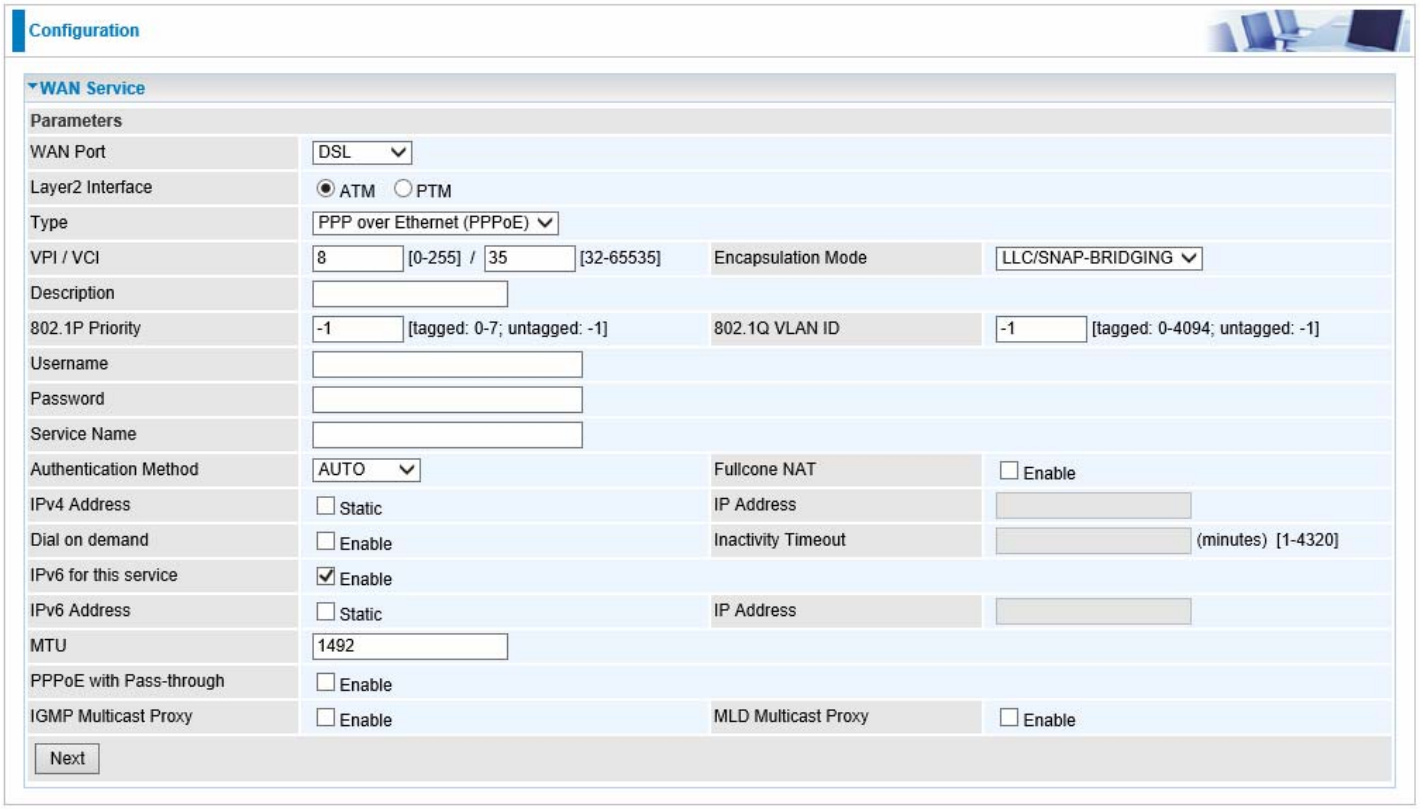
In DSL mode, there are two transfer modes for you to configure for WAN connection, namely ATM and PTM, configuration of PTM mode is similar as ATM mode, here take ATM mode WAN configuration for example.



Layer2 Interface: 2 transfer mode, ATM or PTM.

PPPoE

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purpose, user can define it yourselfe.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the IS

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address.

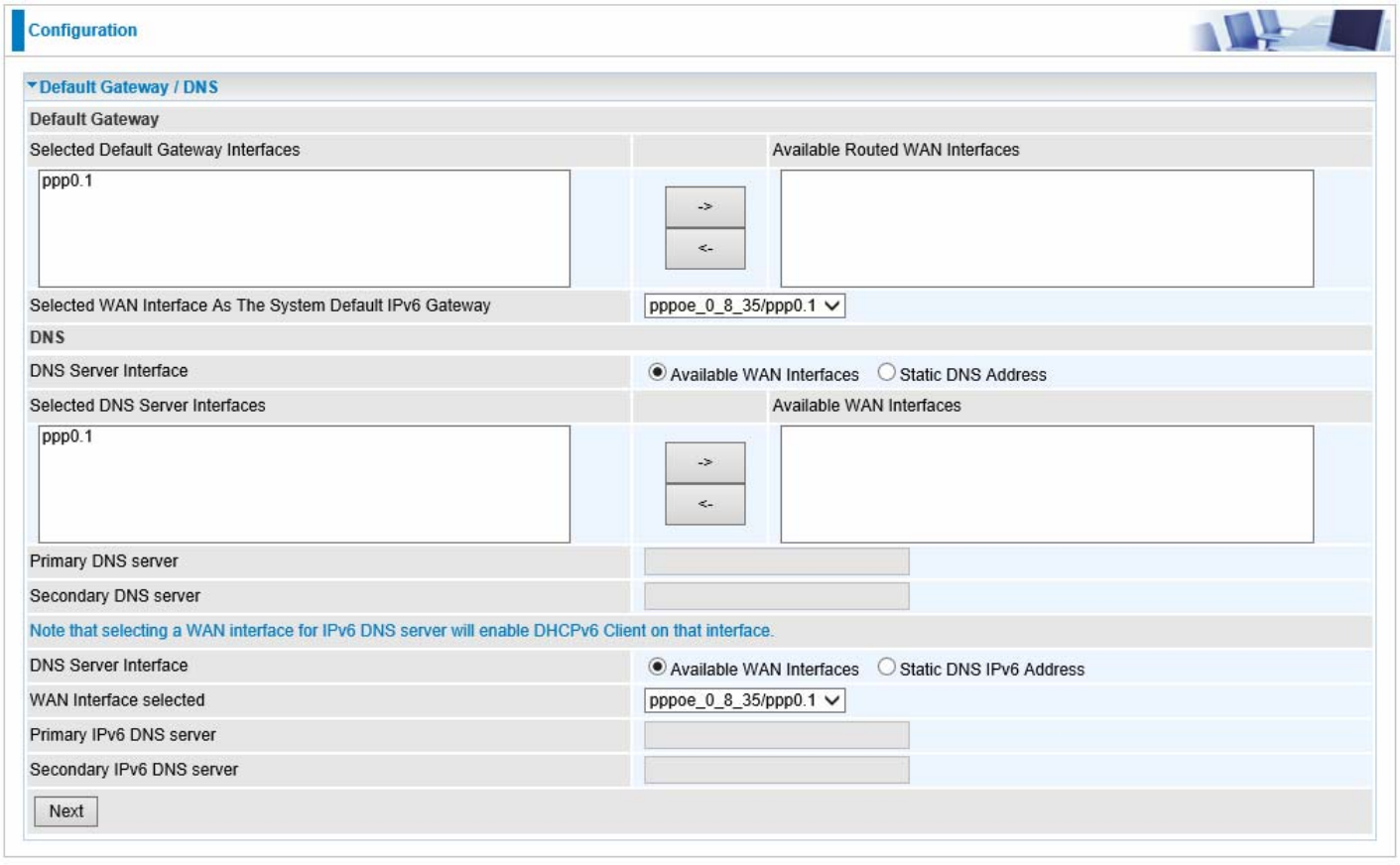
MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE with Pass-through: Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Default Gateway

Select default gateway for you connection (IPv4 and IPv6).

DNS

Either IPv4 or IPv6, you can choose static setting or select from available interfaces.

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and static mode.

Obtain IPv6 DNS info from a WAN interface

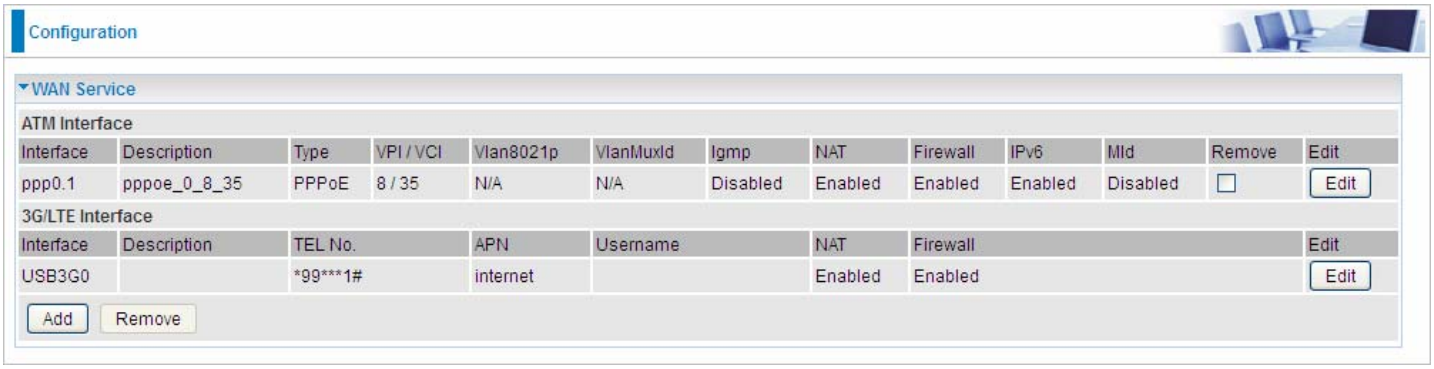
WAN Interface selected: select one configured IPv6 WAN connection from the menu to be as an IPv6 DNS.

Static DNS IPv6 Address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: type the specific primary and secondary IPv6 DNS Server address.

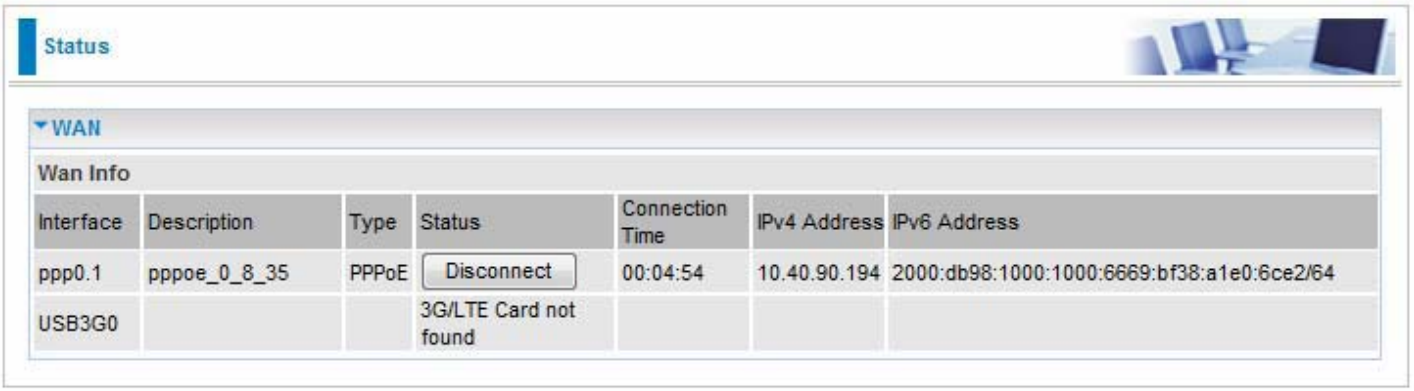
If you don't need a service, select the item you want to remove, check the checkbox, then press **Remove**.

Press **Edit** button to re-edit this service settings.



Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service then you will obtain an IPv6 address).

(IPv4 or IPv6)

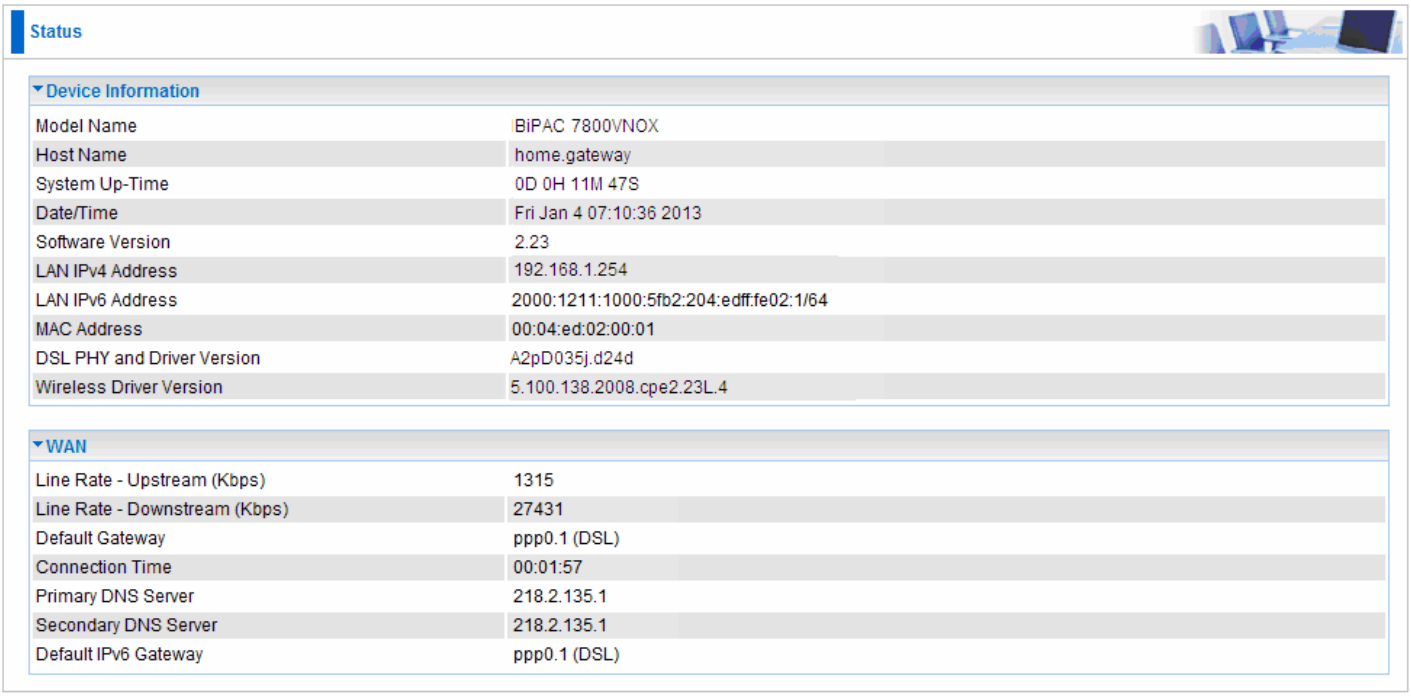


Status

WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address
ppp0.1	pppoe_0_8_35	PPPoE	Disconnect	00:04:54	10.40.90.194	2000:db98:1000:1000:6669:bf38:a1e0:6ce2/64
USB3G0			3G/LTE Card not found			



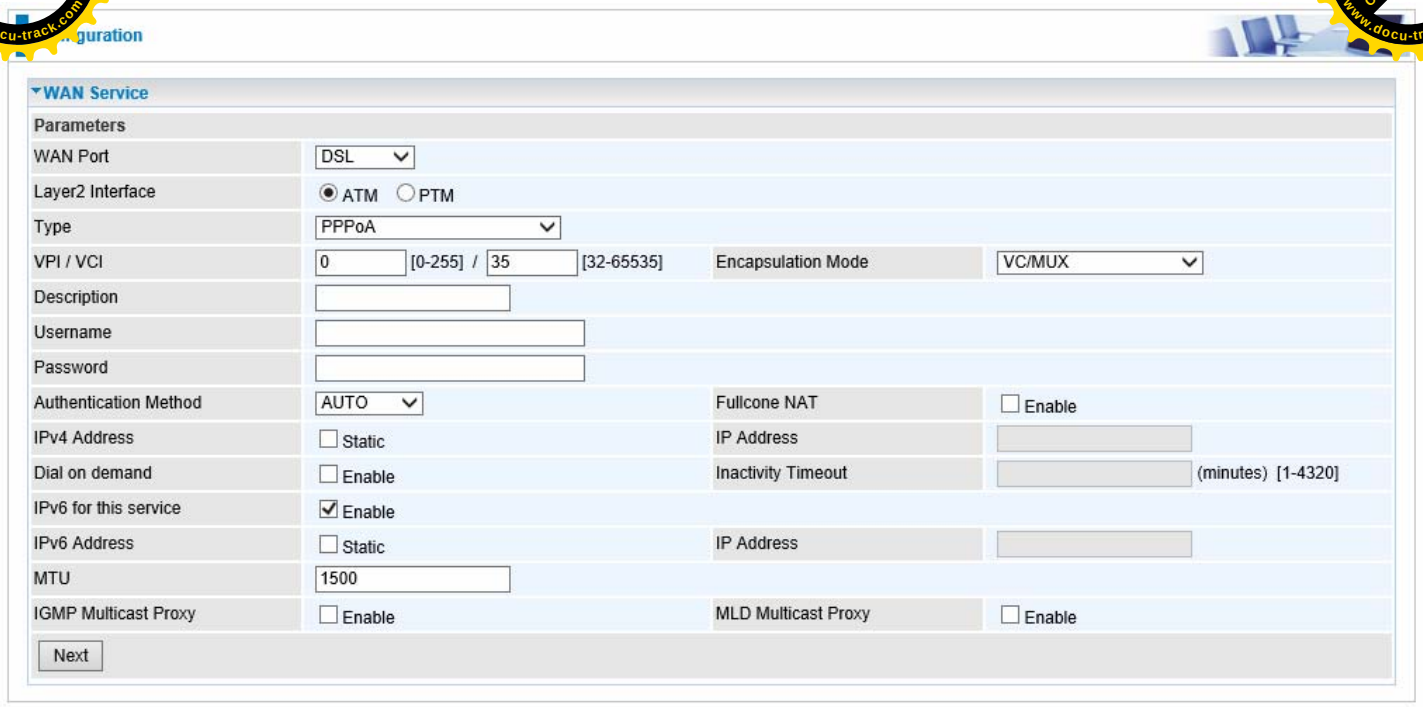
Status

Device Information

Model Name	BiPAC 7800VNOX
Host Name	home.gateway
System Up-Time	0D 0H 11M 47S
Date/Time	Fri Jan 4 07:10:36 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edff:fe02:1/64
MAC Address	00:04:ed:02:00:01
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

WAN

Line Rate - Upstream (Kbps)	1315
Line Rate - Downstream (Kbps)	27431
Default Gateway	ppp0.1 (DSL)
Connection Time	00:01:57
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (DSL)



VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purposes, user can define this.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.

Note: In this connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. With Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

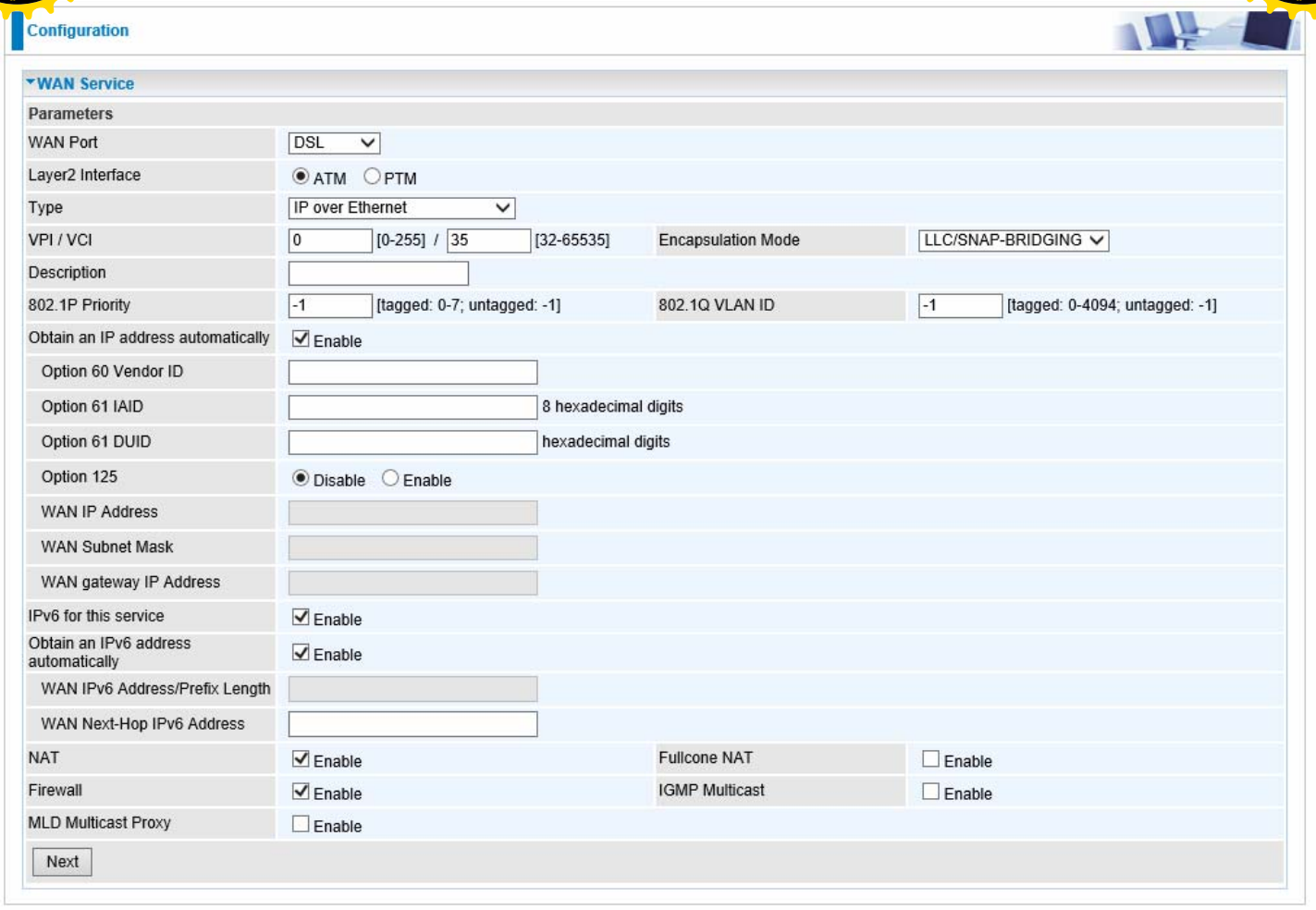
IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address.

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection, commonly for friendly use.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

Obtain an IP address automatically: Check whether to enable this function.

Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

Option 61 IAID: Enter the associated information provided by your ISP. You should input 8 hexadecimal numbers.

Option 61 DUID: Enter the associated information provided by your ISP. You should input hexadecimal number(s).

Option 125: Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the prestored message, if it is matched, the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is ***Disable***.

WAN IP Address: Enter your IPv4 address to the device provided by your ISP.

WAN Subnet Mask: Enter your submask to the device provided by your ISP.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

IPv6 for this service: Enable to use IPv6 service.

Obtain an IPv6 address automatically: check whether to enable or disable this feature.

WAN IPv6 Address/Prefix Length: Enter the WAN IPv6 Address/Prefix Length from your ISP.

WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

Note: If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

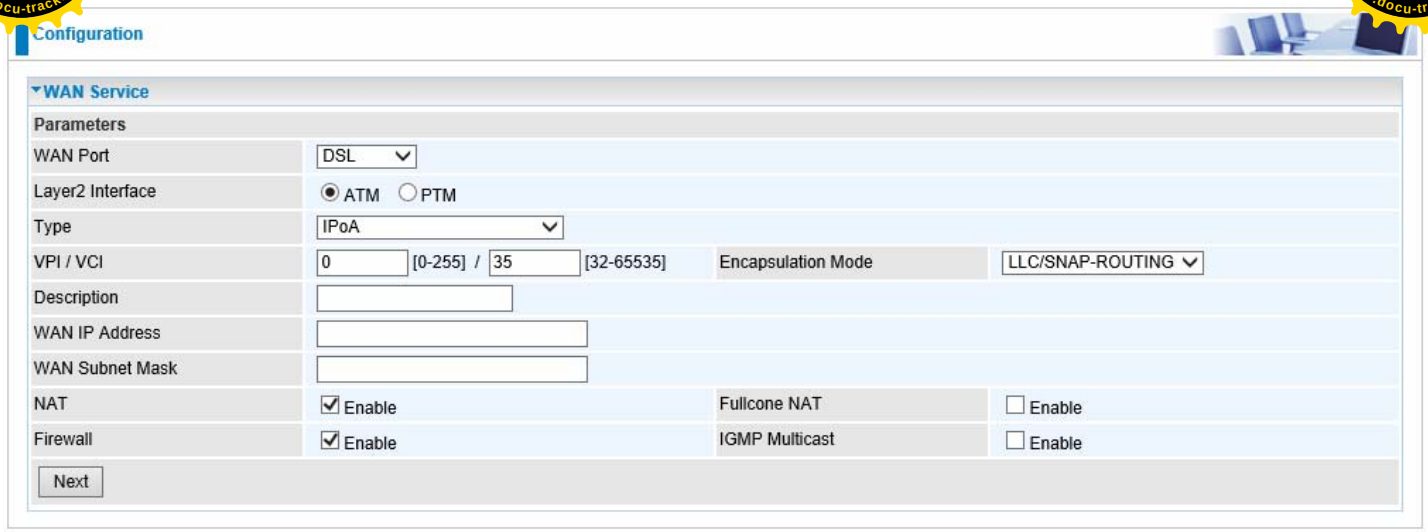
Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

IGMP Multicast: IGMP (**Internet Group Membership** Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection, commonly for friendly use.

WAN IP: Enter the WAN IP from the ISP.

WAN Subnet Mask: Enter the WAN Subnet Mask from the ISP.

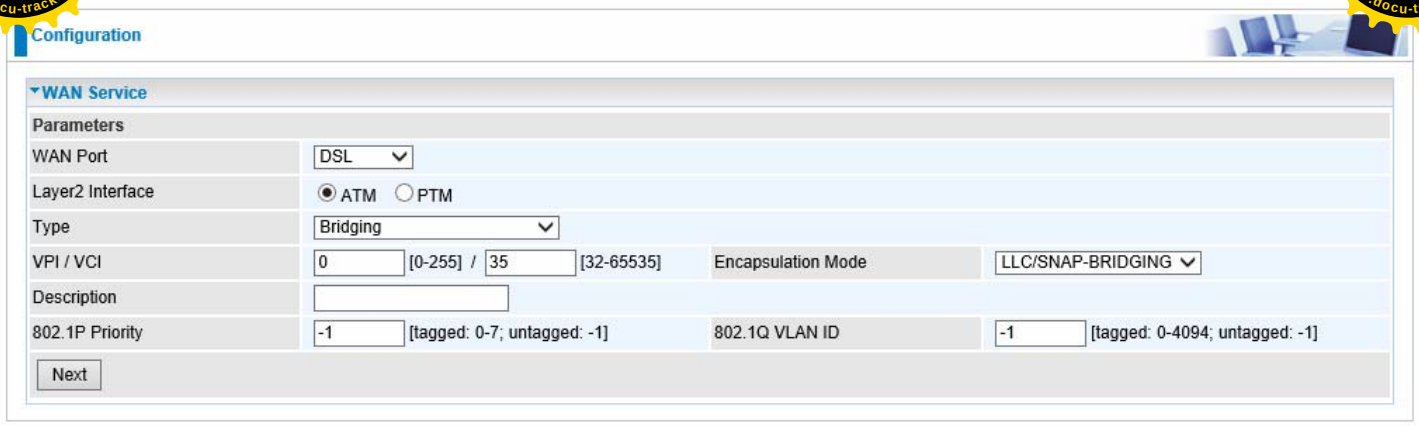
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

IGMP Multicast: IGMP (**Internet Group Membership** Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

Bridging



VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

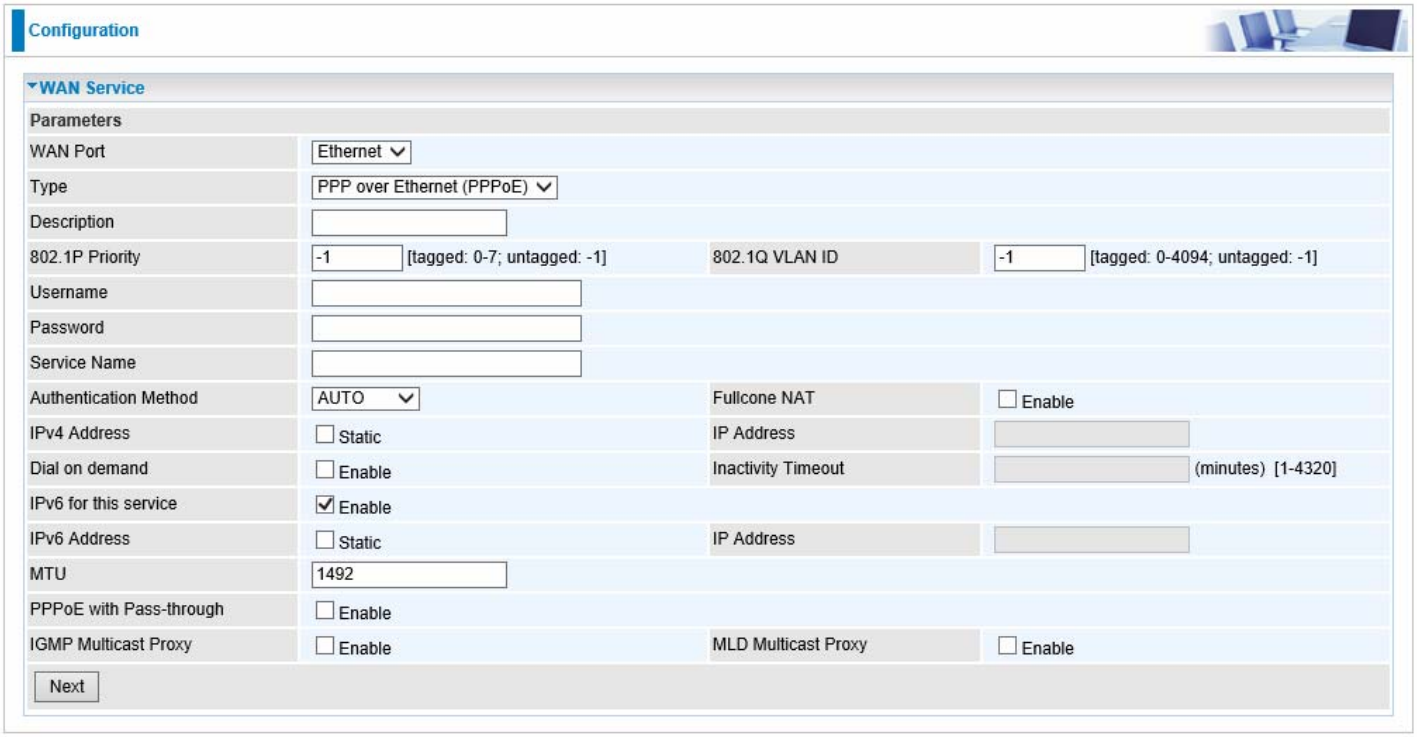
Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

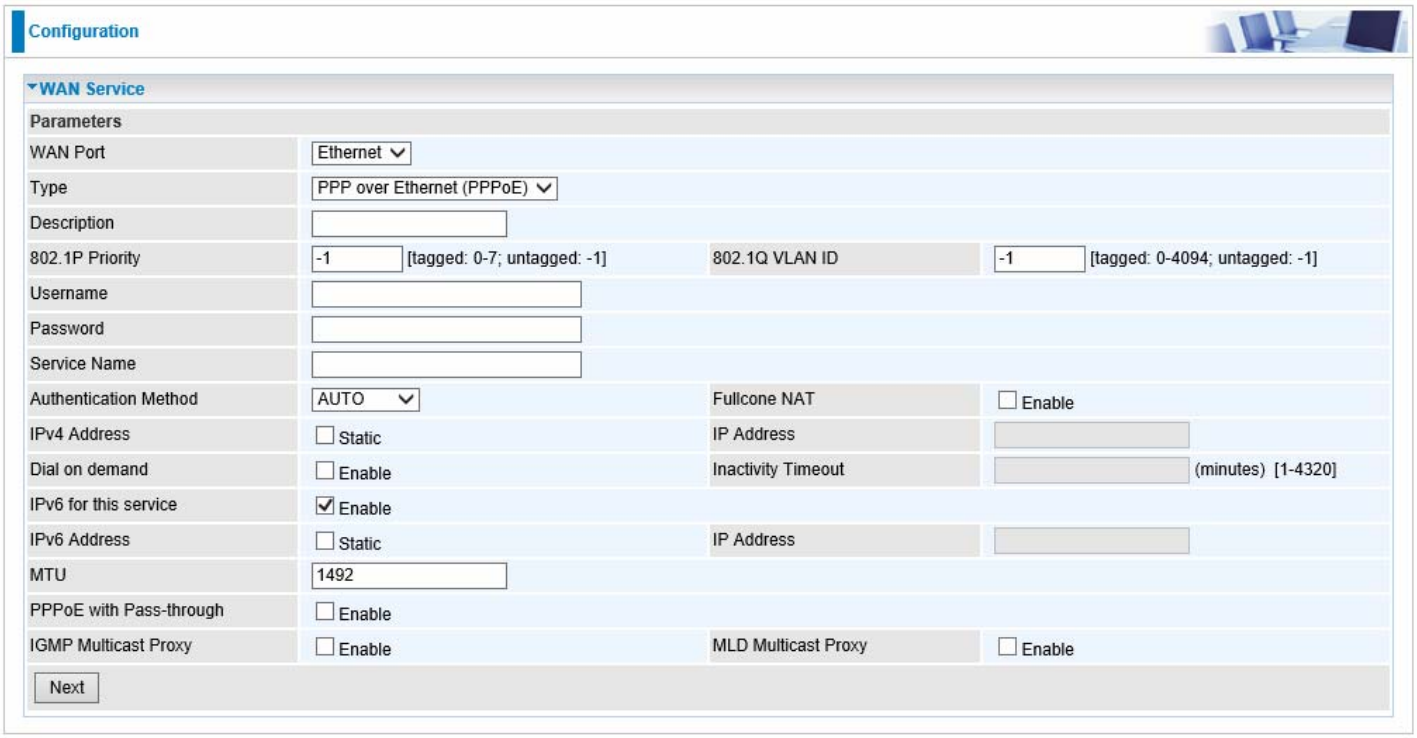
802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Ethernet

Ethernet WAN connection is well known as directly broadband WAN connection.



PPPoE



Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purpose, user can define it yourselfe.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT. and while you disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted or Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address.

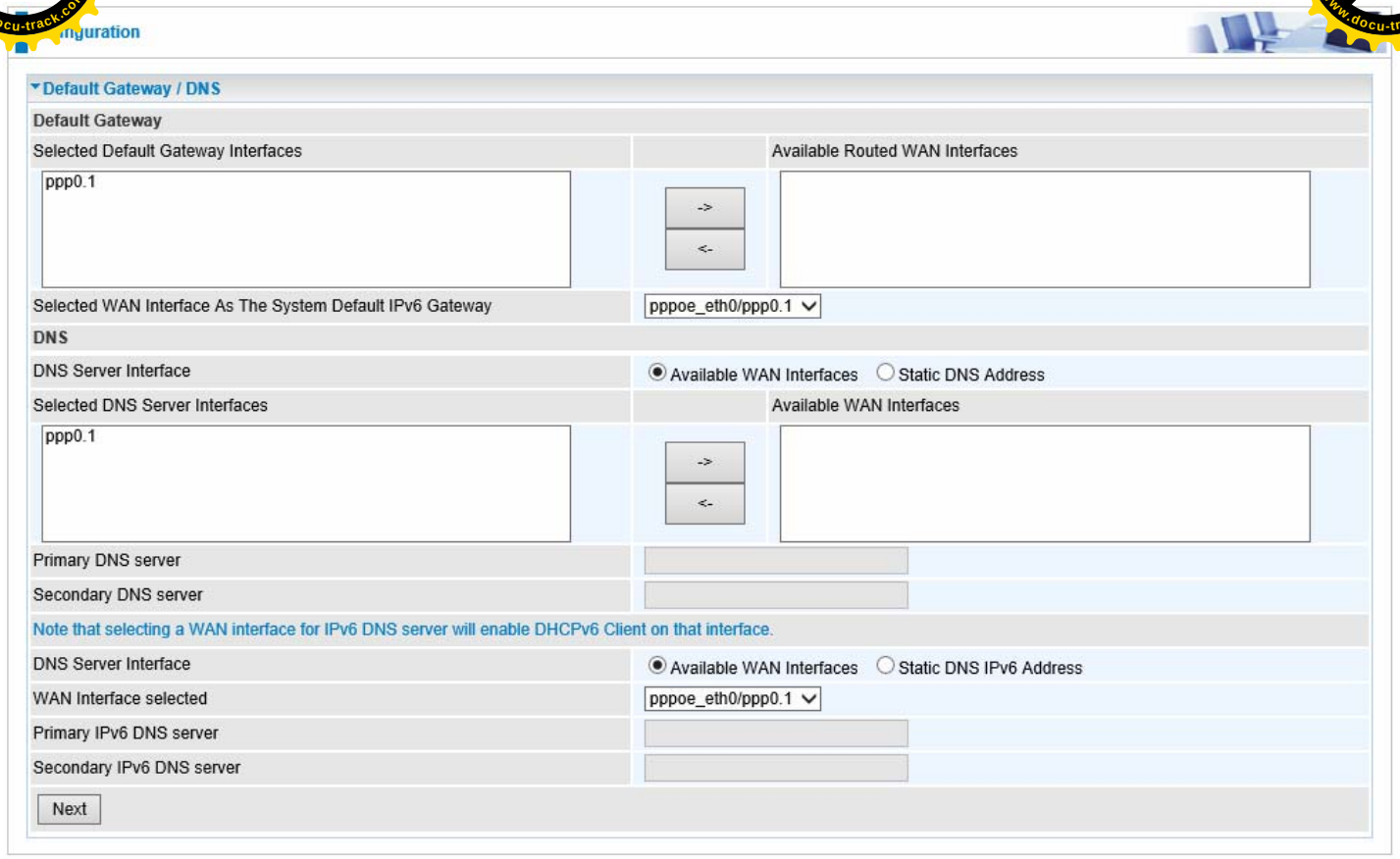
MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE with Pass-through: Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Default Gateway

Select a default gateway for you connection (IPv4 and IPv6).

DNS

Either IPv4 or IPv6, you can choose a static setting or select from available interfaces.

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and static mode.

Obtain IPv6 DNS info from a WAN interface

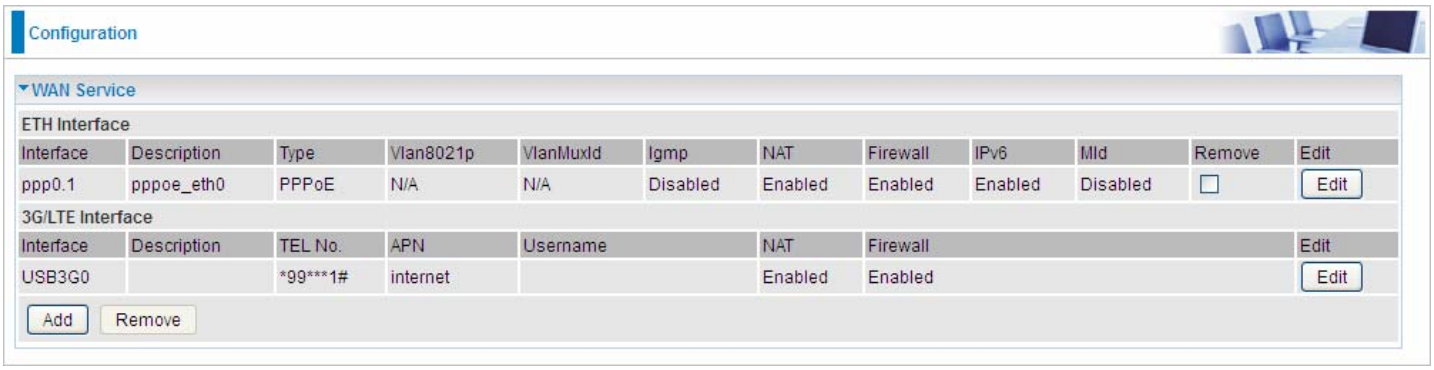
WAN Interface selected: Select one configured IPv6 WAN connection from the menu to be as an IPv6 DNS.

Static DNS IPv6 Address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

If you don't need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

Press **Edit** button to re-edit this service settings.



Configuration

WAN Service

ETH Interface

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	MId	Remove	Edit
ppp0.1	pppoe_eth0	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	☐	Edit

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Edit

Add Remove

Here the corresponding WAN Service have been configured, if it is OK, you can access the internet. You can go to **Status>WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).

(IPv4 or IPv6)

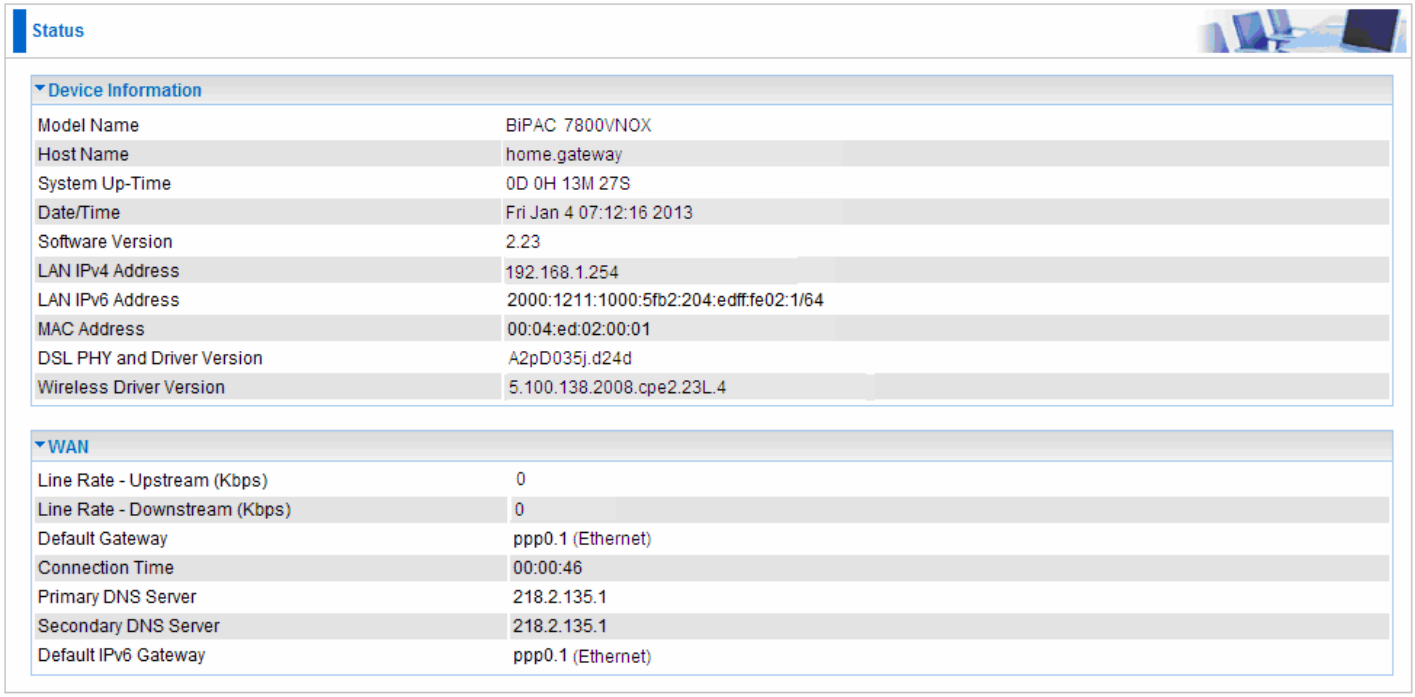
Status

WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address
ppp0.1	pppoe_eth0	PPPoE	Disconnect	00:04:54	10.40.90.194	2000:db98:1000:1000:6669:bf38:a1e0:6ce2/64
USB3G0			3G/LTE Card not found			

The device summary information



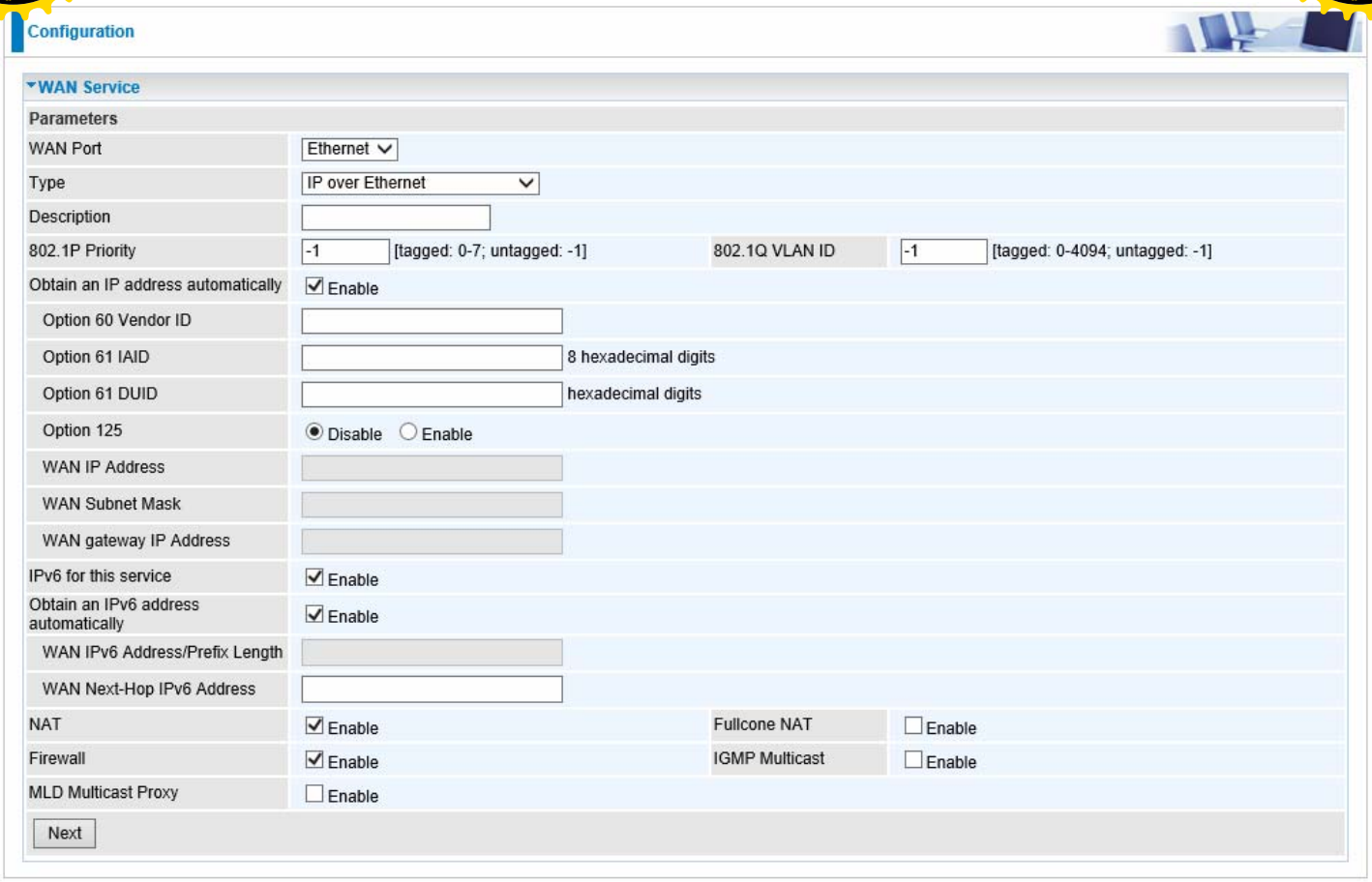
Status

Device Information

Model Name	BiPAC 7800VNOX
Host Name	home.gateway
System Up-Time	0D 0H 13M 27S
Date/Time	Fri Jan 4 07:12:16 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edff:fe02:1/64
MAC Address	00:04:ed:02:00:01
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp0.1 (Ethernet)
Connection Time	00:00:46
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (Ethernet)



Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

Obtain an IP address automatically: Check whether to enable this function.

Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

Option 61 IAID: Enter the associated information provided by your ISP. You should input 8 hexadecimal numbers.

Option 61 DUID: Enter the associated information provided by your ISP. You should input hexadecimal number(s).

Option 125: Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the pre-stored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is ***Disable***.

WAN [illegible] Address: Enter your IPv4 address to the device provided by your ISP.

WAN Subnet Mask: Enter your submask to the device provided by your ISP.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

IPv6 for this service: Enable to use IPv6 service.

Obtain an IPv6 address automatically: check whether to enable or disable this feature.

WAN IPv6 Address/Prefix Length: Enter the WAN IPv6 Address/Prefix Length from your ISP.

WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

Note: If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

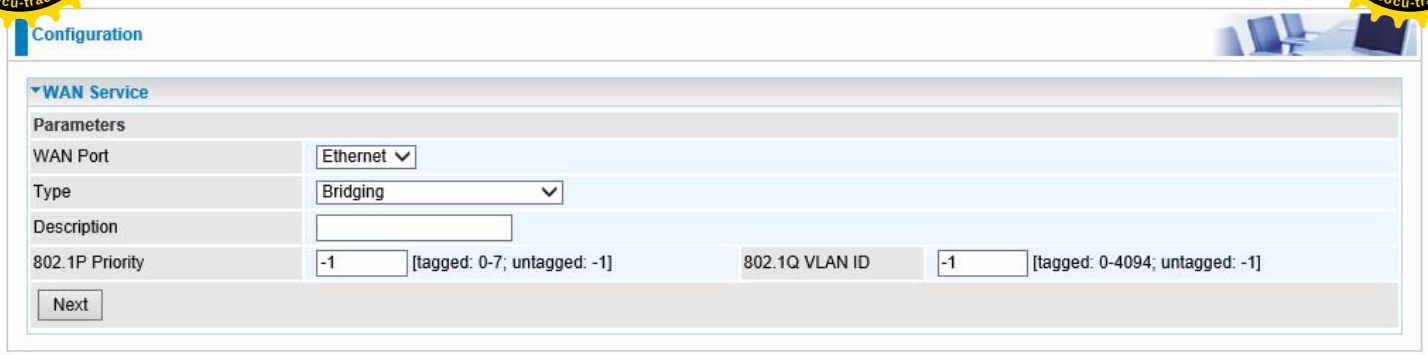
Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

IGMP Multicast: IGMP (**Internet Group Membership** Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Bridging



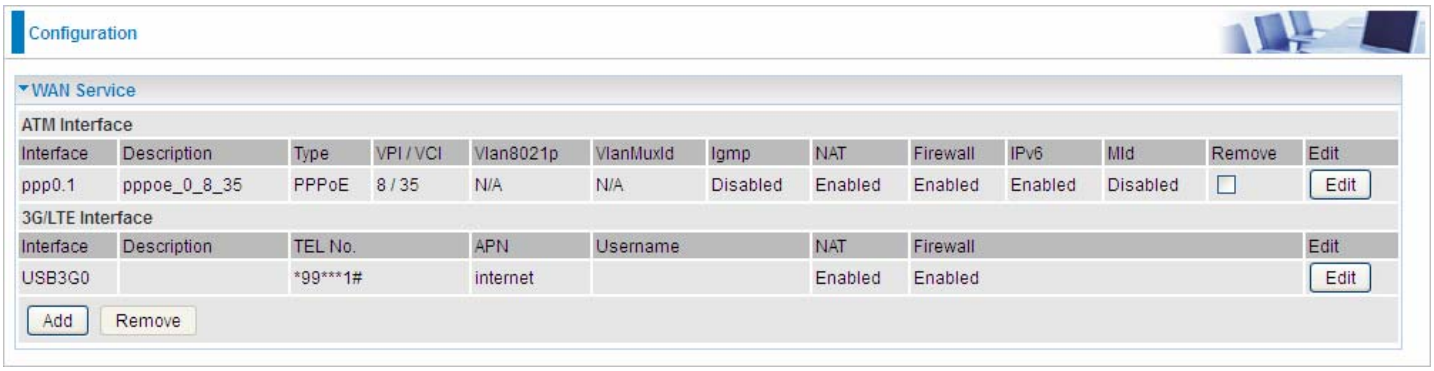
Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

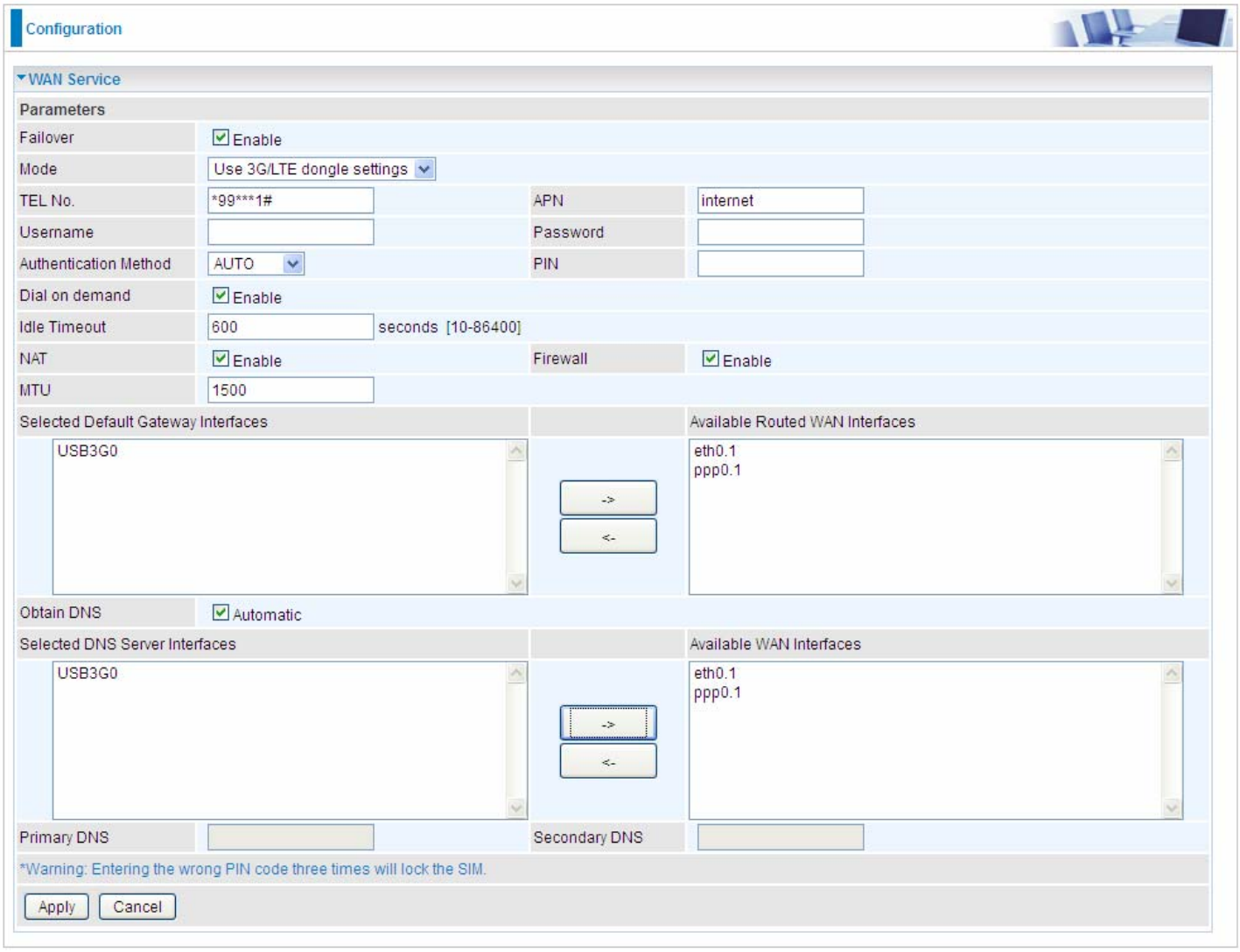
802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

G/LTE

Sele 3G/LTE to configure the route to enjoy the mobility. By default the 3G/LTE interface is on. User can edit the parameters to meet your own requirements.



Click **Edit** button to enter the 3G/LTE configuration page.



Failover: If enabled, the 3G/LTE will work in failover mode and be brought up only when there is no active default route. In this mode, 3G/LTE work as a backup for the WAN connectivity. While if disabled, 3G/LTE serves as a normal interface, and can only be brought up when it has been configured to achieve a mobile connectivity.

Mode: There are 6 options of phone service standards: GSM 2G only, UTMS 3G only, GSM 2G preferred, UMTS 3G preferred, Automatic, and Use 3G/LTE 3g dongle settings. If you are uncertain what services are available to you, and then please select Automatic.

TEL No.: The dial string to make a 3G/LTE user internetworking call. It may provide by your mobile

service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call to. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

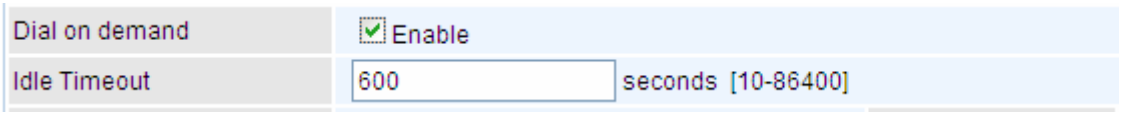
Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/ service provider.

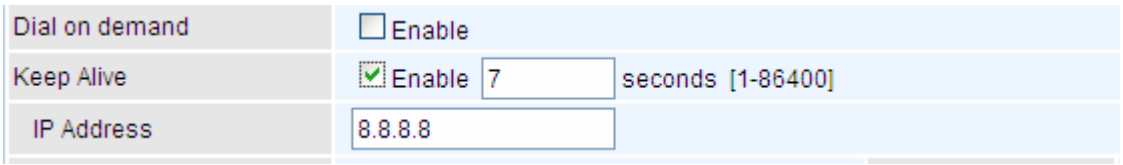
- **Connect on Demand:** If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Click on Connect on Demand, the Idle Timeout field will display.

  Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Default is 600 seconds.



- **Keep Alive:** Check Enable to allow the router to send message out every 7 seconds (can be changed base on need) to prevent the connection being dropped by ISP.

  IP Address: The IP address is used to "ping", and router will ping the IP to find whether the connection is still on.



NAT: Check to enable the NAT function.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

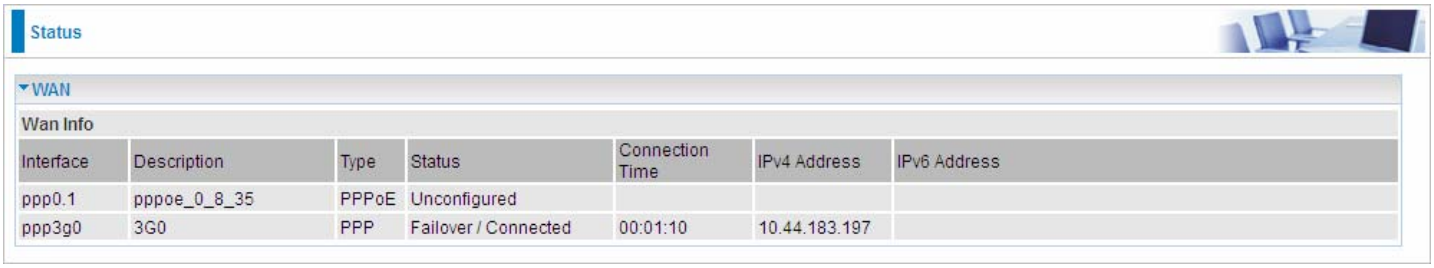
MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram that IP will attempt to send through the interface.

Select default gateway interfaces: Select from the interfaces the default gateway, here commonly we select ppp3g0.

Selected DNS Server Interfaces: Select the IP addresses of the DNS servers.

Click **Apply** to confirm the settings.

Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (Here user can see the 3G/LTE failover).

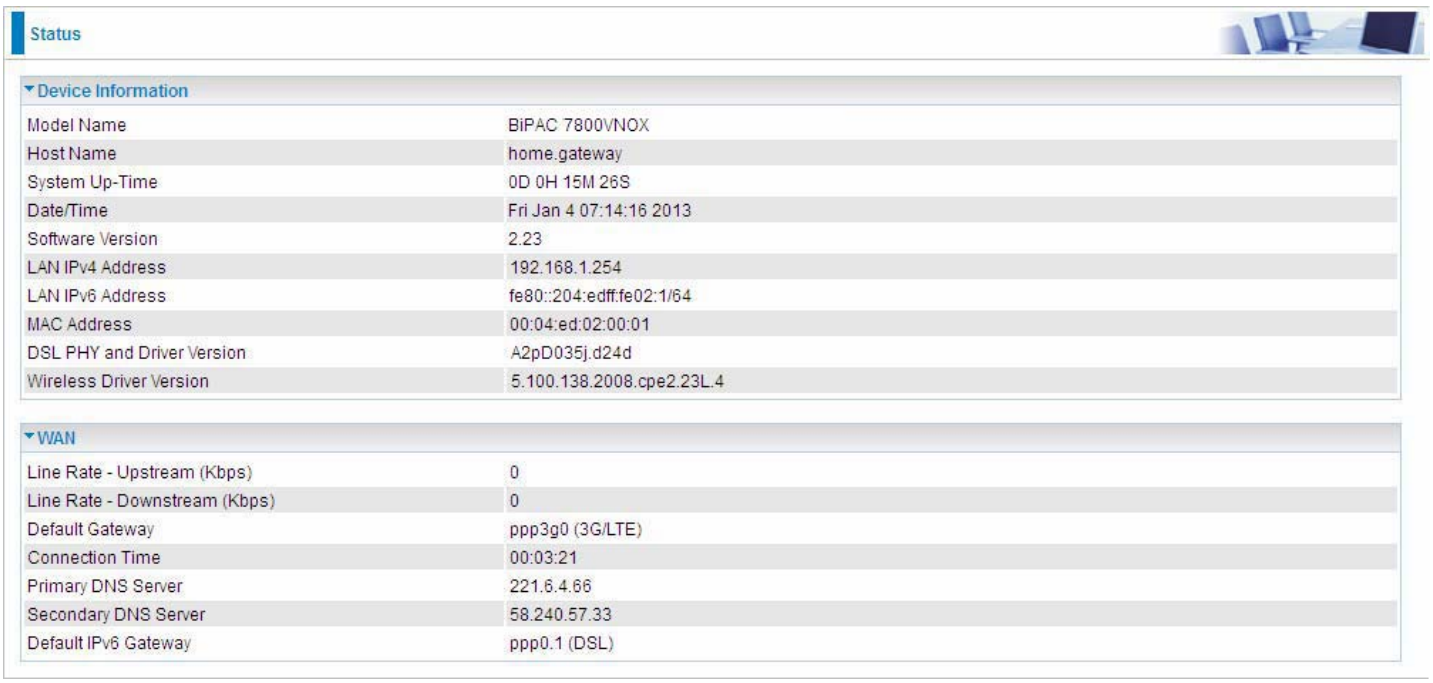


Status

WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address
ppp0.1	pppoe_0_8_35	PPPoE	Unconfigured			
ppp3g0	3G0	PPP	Failover / Connected	00:01:10	10.44.183.197	



Status

Device Information

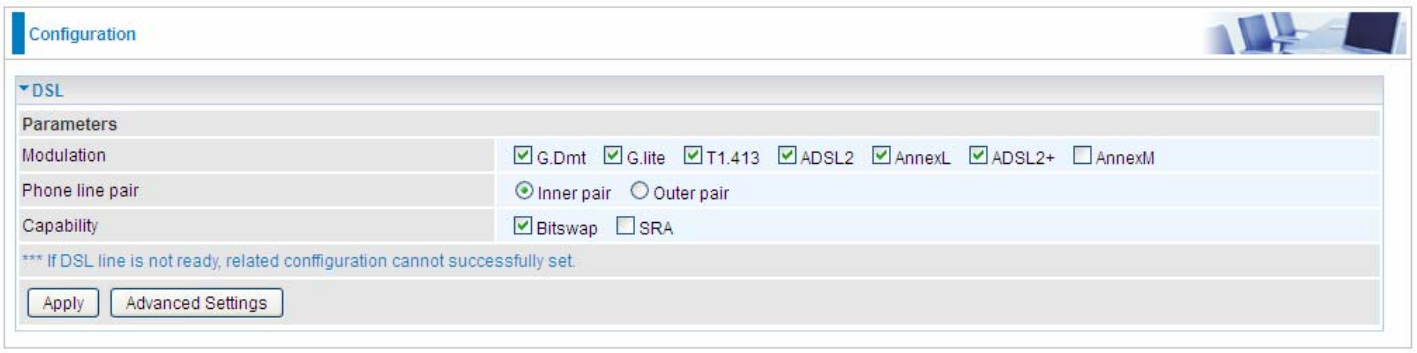
Model Name	BiPAC 7800VNOX
Host Name	home.gateway
System Up-Time	0D 0H 15M 26S
Date/Time	Fri Jan 4 07:14:16 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:fe02:1/64
MAC Address	00:04:ed:02:00:01
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp3g0 (3G/LTE)
Connection Time	00:03:21
Primary DNS Server	221.6.4.66
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway	ppp0.1 (DSL)

DSL

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.



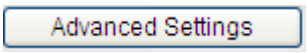
Modulation: There are 7 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, ”ADSL2+”, “AnnexM” that user can select for this connection.

Phone line pair: This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

Capability: There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

- Bitswap Enable: Allows bitswaping function.
- SRA Enable: Allows seamless rate adaptation.

Click **Apply** to confirm the settings.

Click  to future configure DSL.

Select the Test Mode, or leave it as default.

Tone Selection: This should be left as default or be configured by an advanced user.

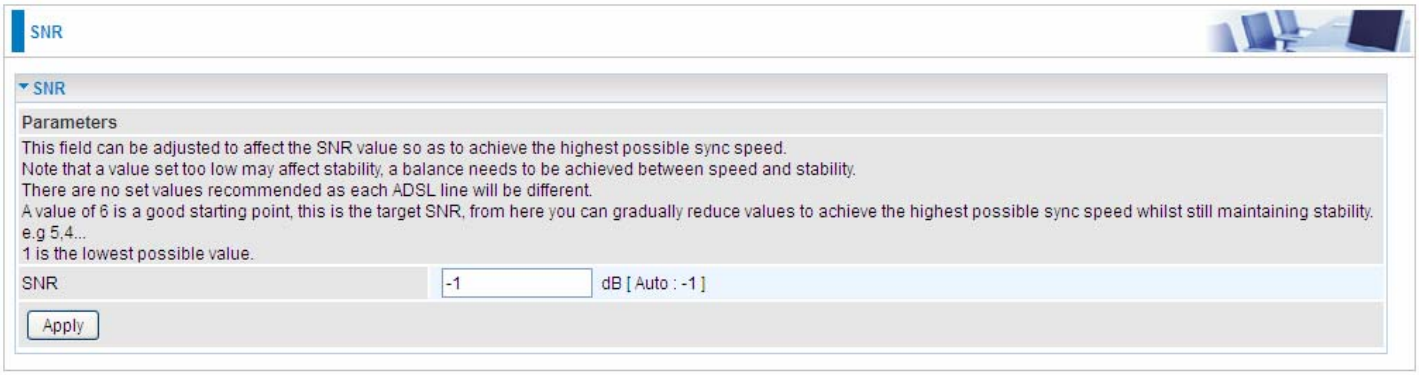
The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart.

With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream。

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

SNR

Signal-to-noise ratio (often abbreviated **SNR** or **S/N**) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.

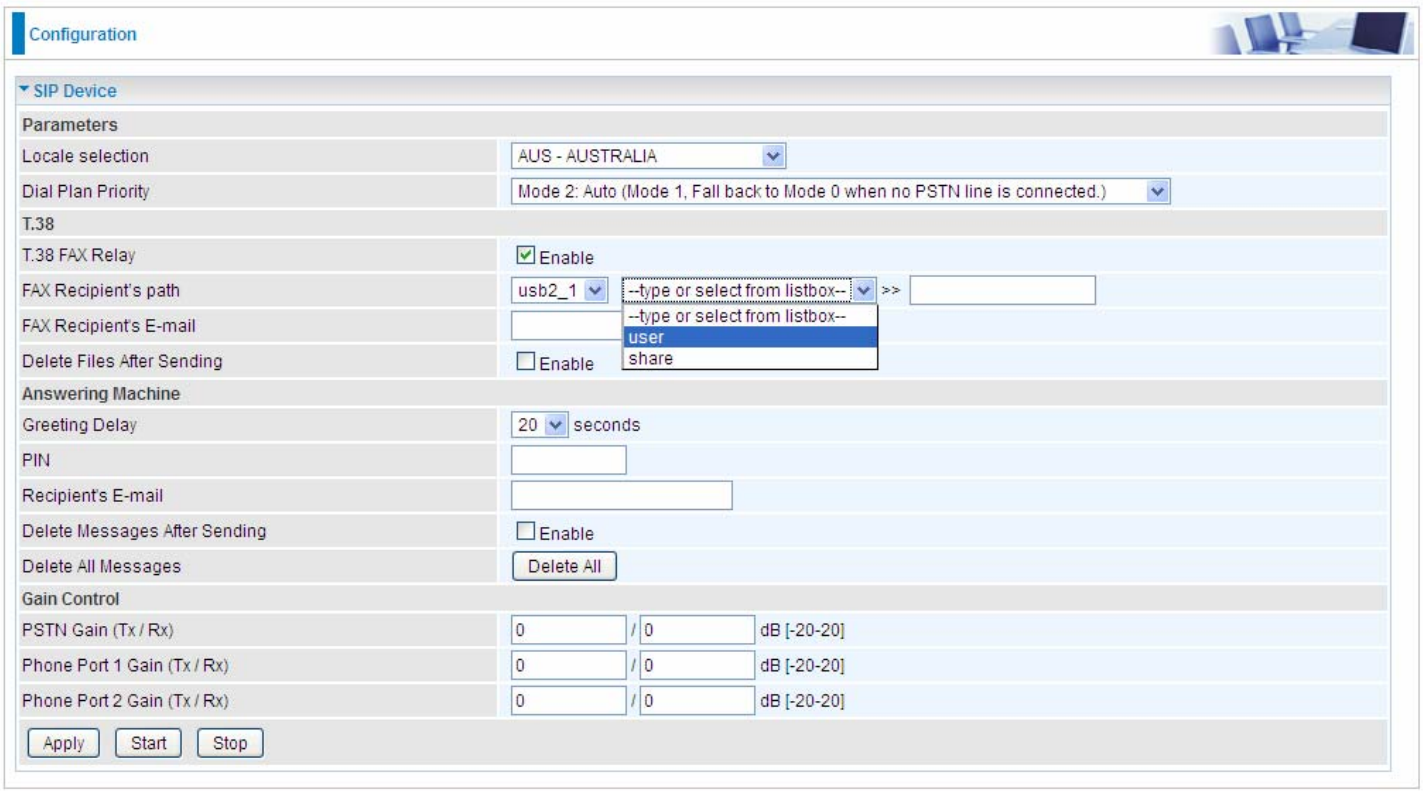


SNR: Change the value to adjust the DSL link rate, more suitable for an advanced user.

VoIP, or Voice over Internet Protocol, enables telephone calls through existing internet connect 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 **SIP Device**, **Service Provider**, **SIP Account**, **VoIP Dial Plan**, **PSTN Dial Plan, Phone Book**

SIP Device



Locale: This selection is a drop-down box, which allows users to select the country for which the VoIP device is operating. When a country is selected, the country parameters are automatically loaded. Different countries can have their special ring mechanism.

Dial Plan Priority: Three modes for users to set the dial mechanism, default is set to Auto, thus PSTN only with exception.

- **Mode 0:** VoIP only and ignore all PSTN dial plans, send all calls to VoIP, including Emergency calls.
- **Mode 1:** Default, which means that under this mode, the dial mechanism always match PSTN plan first, then move to VoIP plan.
- **Auto:** Auto, this means the dial system will fall back to Mode 0 (VoIP) when no PSTN is connected.

T.38

T.38 relay is a way to permit faxes to be transported across IP networks between existing fax terminals. The T.38 fax gateway converts and encapsulates the fax sent from the terminal fax machines into a T.38 date stream. Then the gateway send the converted date packets to a T.38 enabled end point such as a fax or fax server or another T.38 gateway that converts it back to the analog signal to realize the communication between two fax terminals.

T.38 Delay: Click Enable to allow transmission of fax over IP network between two fax machines. If T.38 Delay is disabled, the analog fax signal is transmitted as the normal audio data. If T.38 Delay is enabled, the fax signal is converted to T.38 signal.

FAX Recipient's path: Set the path directly for storing the fax file to the storage.

Note: For common fax usage, user should have a fax connected to the router, creating a fax environment between two fax terminals, and the fax file(s) would be received through fax connected to the router as what we usually perform.

But if user does not get a fax or he wants to store the fax to the file directly, he then can enable Fax Reception feature. Select or enter manually the reception path for the file. (Here user can turn to USB for help.)

1) Set the field "Incoming Phone Port" to "FAX Reception" at the "VoIP Account" page.

2) Set the path user wants fax file saved at "FAX Recipient's path" at the "SIP Device" page.

3) The incoming VoIP call for the specified VoIP account will be treated as Fax and saved to path.

FAX Recipient's E-mail: Enter the recipient's email address. Once the fax file is delivered, the fax file will be mailed to the account specified by the "Recipient's Email",

Delete Files After Sending: The files will be deleted from system once the mail is sent out.

Answering Machine

The answering machine is a device for answering telephones and recording callers' messages and being enabled for both VoIP and PSTN.

The operation for the answering machine:

***#00:** Record user own greeting message;

1) Start the recording after the beep sound
2) Press # while finished.
3) Hang up after the beep is heard. (system needs time on file translation and save to storage).

***#99:** Delete the user's greeting message

***#98:** Play the greeting message

***#xx:** Access the specified answering machine where xx (automatically designated by the system) can be found at the "SIP Account" page.

***#96:** Enable the answering machine

***#97:** Disable the answering machine

1) After the beep sound, dial the specified code xx where xx can be found at the "SIP Account" page.
2) Hang up after the beep is heard. (system needs time on file translation and save to storage).

***#90:** Access the PSTN A/M.
Note: 7800VNP(O)X uses the 1st available phone port to record the PSTN message. So, the answer machine stops recording if user picks up the specified phone.

Greeting Delay: The parameter is used as a threshhold for the answer machine to automatically answer and record the messgae. There are seven items marking 0, 5, 10, 15, 20, 25, 30 respectively. For example, if set to 0s, when there is an incoming call, the answering machine will respond

immediately and record the message. And if it is set to 20s, then the call will keep ringing until time out of 20s (without user picking up the phone) before it can respond and record the meassge.

PIN: The set password (no exceeding 8 digits) for listening to message. The customer should press the PIN number so as to listen to the message. Leave it empty, and user can listen to the message without entering password first.

Recipient's Email: Enter the recipient's email address. Once the voice message is left (answering machine operation), the voice message will be mailed to the account specified by the "Recipient's Email",

Deleting Messages After Sending: The message will be deleted from system once the mail is sent out.

Delete All Messages: Press the "Delete All" button to delete all messages stored in the system all at once.

Gain Control

Gain control is to reduce the bad performance of quality issue caused by noise or echo, etc. Rx means the performance of receiving and the Tx implies the performance of transimitting. A plus quantity is to raise the performance while a negative quantity is to cut the performance (Rx: +1 to increase the performance of receiving by 1 point and if set -1, the performance will be cut by 1 point, the range is -20- 20.).

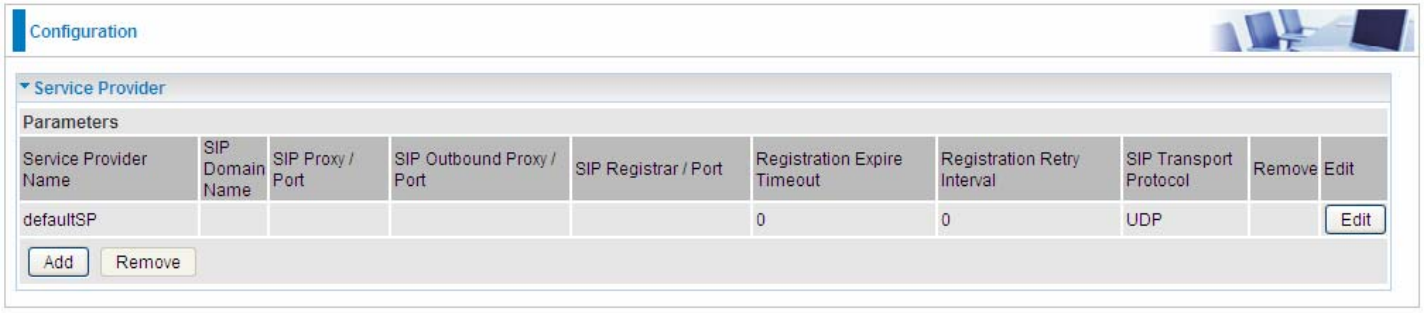
PSTN Gain: Set the PSTN gain, Tune the gain between -20-20 of the Rx and Tx respectively to obtain a appropriate PSTN call environment.

Phone Port 1 Gain: Set the gain. Tune the gain between -20-20 of the Rx and Tx respectively to ensure a clear phone call.

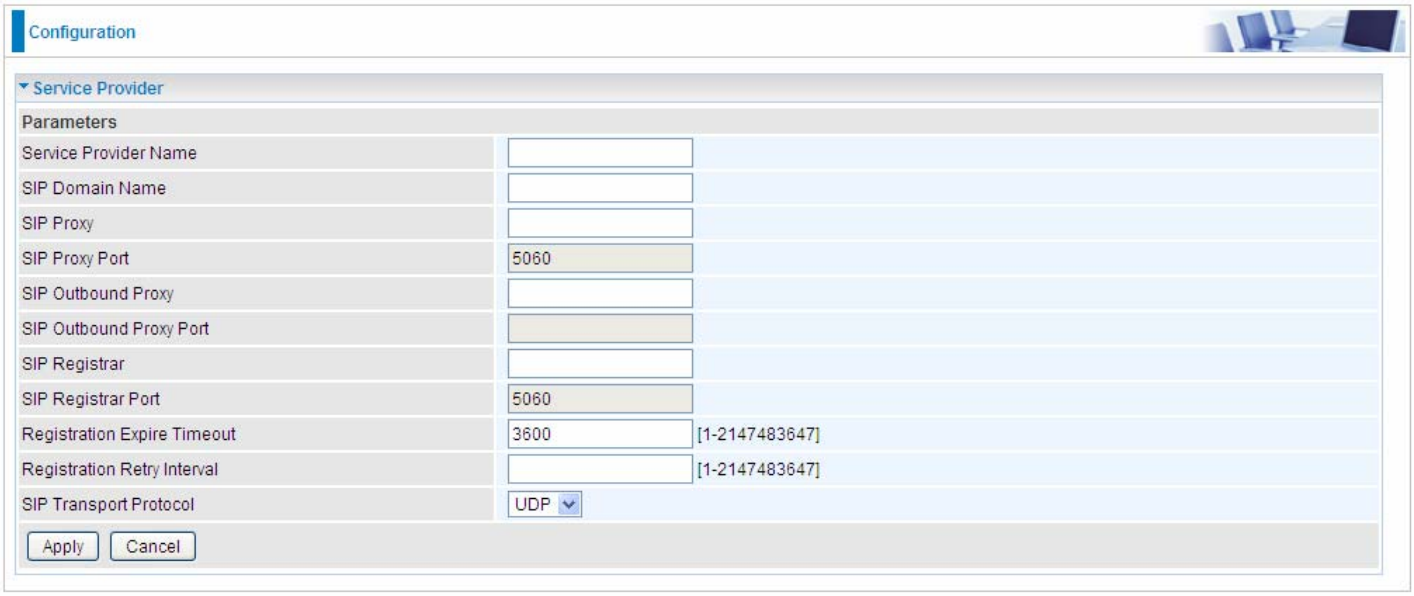
Phone Port 2 Gain: Set the gain. Tune the gain between -20-20 of the Rx and Tx respectively to ensure a clear phone call.

Service Provider

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.



BiPAC 7800VNP(O)X offers a defaultSP item, you can change the settings or add a new Service Provider yourself.



Service Provider Name: Name of provider of the VoIP service

SIP Domain Name: Enter the SIP registrar domain name.

SIP Proxy: Also seen as SIP server, it manages the setup of calls between SIP devices including the controlling of call routing and some necessary functions such as registration, authentication, and network access control. Type the SIP Proxy address you obtain after you register from the service provider.

SIP Proxy Port: The port number set on your SIP proxy serve that the SIP proxy server uses to make network connections, default is 5060.

SIP Outbound Proxy: SIP outbound proxy is in similar use as SIP proxy, but when the SIP devices are behind a firewall or a router or NAT, the SIP outbound proxy is the useful way to let SIP traffic to pass from the internal network to the internet. Enter the SIP outbound proxy server address here.

SIP Outbound Proxy port: Enter the port, normally 5060.

SIP Registrar: Type the VoIP SIP registrar IP address.

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

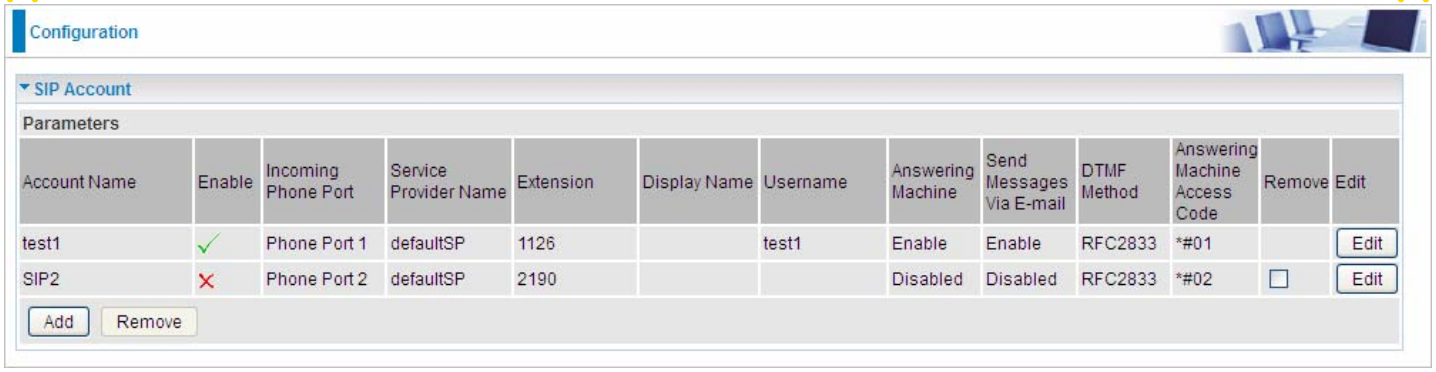
Registration Expire Timeout: This sets time interval before timeout.

Registration Retry Interval: The interval set to retry sending registration message.

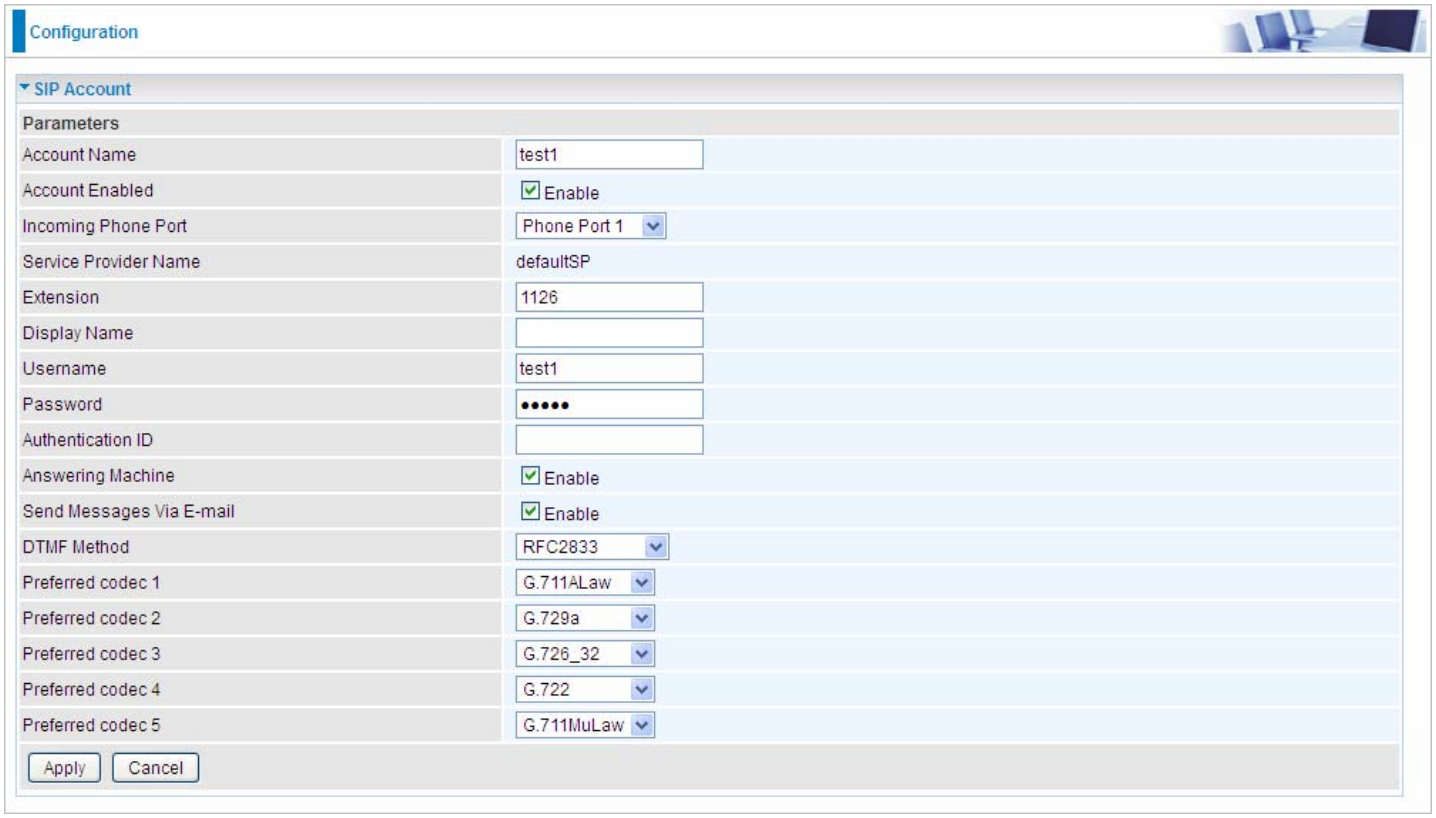
SIP Transport Protocol: The protocol adopted to transport SIP, UDP commonly used.

SIP Account

account is an independent section for SIP account settings, including Extension number, etc.



Click **Add** or **Edit** to add new account or modify the existing sip account.



Account Name: User-defined account name.

Account Enabled: Enable to activate the sip account.

Incoming Phone Port: Select which phone port you are setting.

Extension: The Phone number.

Display Name: Enter a display name to identify the phone, like indicating the phone usage.

User Name: The user name user registers in the sip server.

Password: The password user registers in the sip server.

Authentication ID: It is an authentication code required for some ISP, and can be left empty if not required.

Answering Machine: Enable to activate the answering machine feature so that user can record and listen to the messages of this phone.

Send Message Via E-mail: Enable to send message left by callers via e-mail to the user.

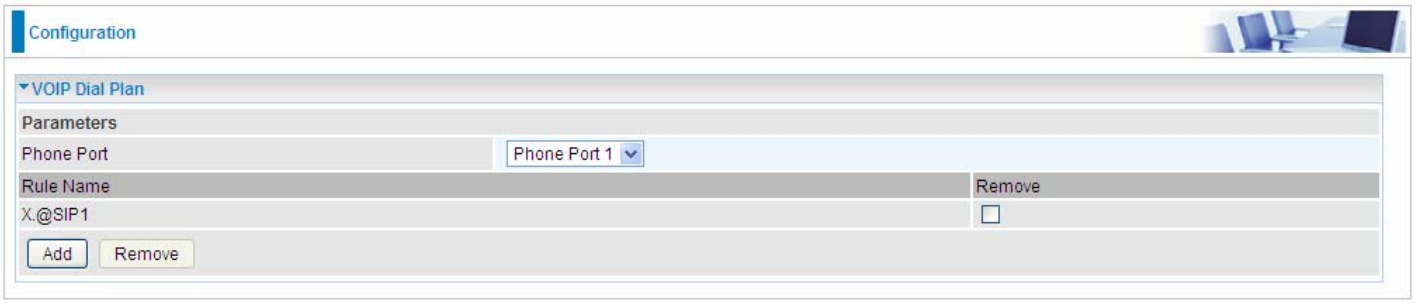
DTMF Method: DTMF stands for "Dual-Tone Multi-Frequency", and is a telecommunication signaling over analog telephone lines widely used between telephone handsets and other communication devices and the switching center. “DTMG method” provides ways to transmit DTMF for VoIP, such as RFC 2833, SIP Info, SIP Info (short), Inband and Auto, and RFC2833 is the widely used one.

Preferred codec#1,2,3,4,5: Codec is known as Coder-Decoder used for data signal conversion. Set the priority of voice compression; Priority 1 owns the top priority.

- **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.**729a: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.
- **G.726_32:** It is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 32kbit/s.
- **G.722:** G.722 is an ITU standard codec that provides 7 kHz wideband audio at data rates from 48, 56 and 64 kbit/s. G.722 sample audio data at a rate of 16 kHz (using 14 bits), double that of traditional telephony interfaces, which results in superior audio quality and clarity.
- **G.711Mu-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.

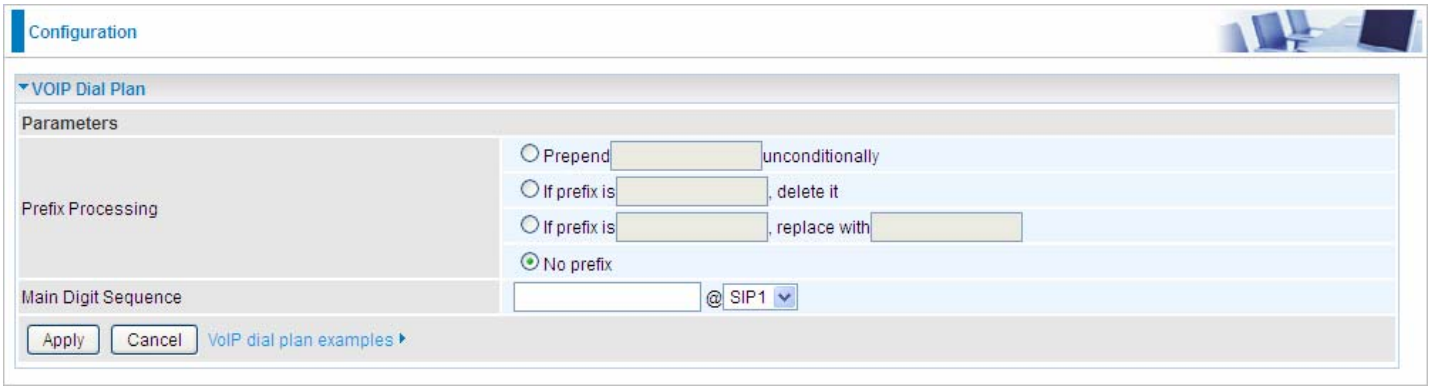
VOIP Plan

This section helps you to make a number dial via VoIP. You no longer need to memorize a long dial string or number for making a VoIP call. Go to Configuration > VOIP > VOIP Dial Plan.



Phone Port: Set the phone the VoIP dial rule relates to. When phone port is set to Phone Port 1, the rules will apply to phone1.

Click **Add** to create new rules.



Prefix Processing:

- **Prepend xxx unconditionally:** xxx number is appended unconditionally to the front of the dialing number when making a call. Prefix can also be included with any number and/or character such as ***,** #.

Note: For special service with *, #, you may need to check with your VoIP or Local Telephone Service Provider for information.

- **If Prefix is xxx, delete it:** Prefix xxx is removed from the dialed numbers before making a call.
- **If Prefix is xxx, replace with yyy:** Prefix xxx is replaced with yyy when making a call.
- **No prefix:** No prefix is appended to the front of the dialed numbers. It is set as in default settings.

Main Digit Sequence: The call(s) can be called out via SIP. VoIP dial plan examples leads us to regular usage for this parameter.

<@ SIPgateway>: This is used for the Intelligent Call Routing feature where you need to set up your **SIP account** on the VoIP User-defined Profiles link on the VoIP Wizard page.

Digit sequence Example	Description
x.	x specifies one digit between 0 and 9. x. specifies any sequence of digits in variable length. Maximum length is 32.
xxx	Specifies any sequence of digits in fixed length. Total length is 3.
xxxx.	Specifies any sequence of digits in variable length but not shorter than 4 digits. Maximum Length is 32.
123x.	Any sequence of digits starting with 123 and with variable length. Maximum length is 32.
[124]x.	Any sequence of digits starting with 1 or 2 or 4. Minimal length is 2, maximum length is 32.
[1-3]x.	Any sequence of digits starting with 1 to 3 and with variable length. Maximum length is 32.
9[4-6]8x.	Any sequence of digits starting with first digit 9, the second digit between 4 to 6, and third digit 8. Length is variable, maximum length is 32.

Specific Examples

1) I want to route all 13, 1300 & 1800 numbers via My Provider which is configured on SIP1

- Firstly enter 1[38]x. in the 'Main Digit Sequence' Box
- Next Select 'SIP1' from adjacent dropdown
- Press 'Apply'
- You'll then end up with the following rule - 1[38]x.@SIP1

2) I want to prefix area code (08) to all local calls starting with 2,3,4,5

- Type 08 in the 'Prepend unconditionally' box
- Next type [2-5]x. in the 'Main Digit Sequence' Box.
- Then select provider/port from adjacent dropdown
- Press 'Apply'
- You'll then end up with the following rule - <:08>[2-5]x.@SIP2

3) I want to create a prefix (#) that when dialled can be used to manually route a call via a specific provider:

- Firstly type # in the 'if prefix is – delete it' field
- Type x. in the 'Main Digit Sequence' Box
- Select port/provider from adjacent dropdown
- Press 'Apply'
- You'll then have the following rule – <#:>x.@SIP2
- Now when you prefix number with # the call will route via selected provider
- The # is not dialled, only the digits following.

4) I want to create a rule that uses exact number of digits (instead of timeout) to make dialling quicker, eg 13 numbers.

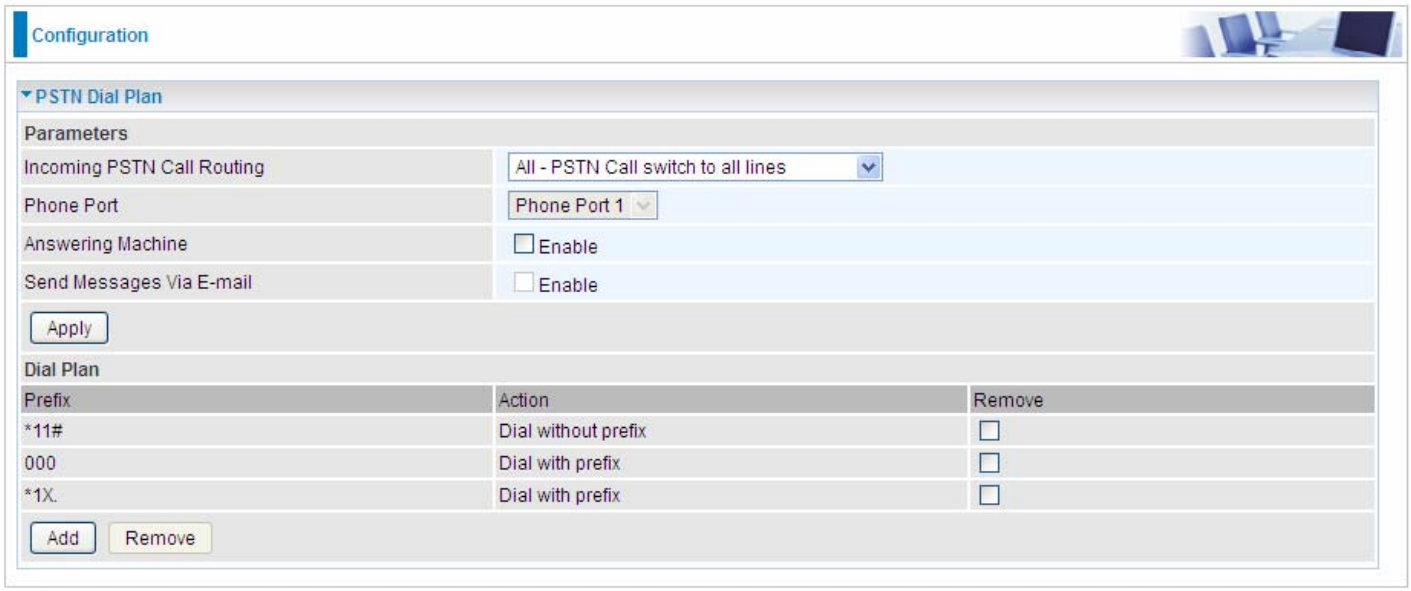
- Type 13xxxx in the 'Main Digit Sequence' box.
- Select your provider from adjacent dropdown
- Press Apply
- You'll then end up with the following rule - 13xxxx@Provider3
- The call will now dial after 6th digit is dialled instead of waiting for dial out.

Digit Sequence Example:

x.	*x specifies one digit between 0 and 9. x. specifies any sequence of digits in variable length. Maximum length is 32.*
xxx	*specifies any sequence of digits in fixed length. Total length is 3.*
xxxx.	*specifies any sequence of digits in variable length but not shorter than 3 digits.Maximum Length is 32.*
123x.	*Any sequence of digits starting with 123 and with variable length. Maximum length is 32.*
[124]x.	*Any sequence of digits starting with 1 or 2 or 4. Minimal length is 2, maximum length is 32.*
[1-3]x.	*Any sequence of digits starting with 1 to 3 and with variable length.Maximum length is 32.*
9[4-6]8x.	*Any sequence of digits starting with first digit 9, the second digit between 4 to 6, and third digit 8. Length is variable, maximum length is 32.*

PSTN Dial Plan

PSTN Dial Plan assists in routing calls via PSTN. You can define a range of dial plans to [illegible] regular calls from VoIP switching to PSTN line. Prefix numbers are essential in distinguishing between VoIP and Regular phone calls. If actual numbers dialed matches with prefix number defined in this dial plan, the dialed number will be routed via PSTN. Otherwise, the number will be routed via VoIP network.



Parameters

Incoming PSTN Call Routing: Measures to deal with incoming PSTN calls.

- **Auto:** Change the incoming call to another idle line, for example, if Phone 1 is busy, then the incoming call would be switched to Phone port 2.
- **Line:** If a PSTN call rings on phone 1, and when Phone 1 is busy, there will be a warning of the incoming call.
- **All:** Both Phone1 and Phone2 ring when a PSTN call is received.

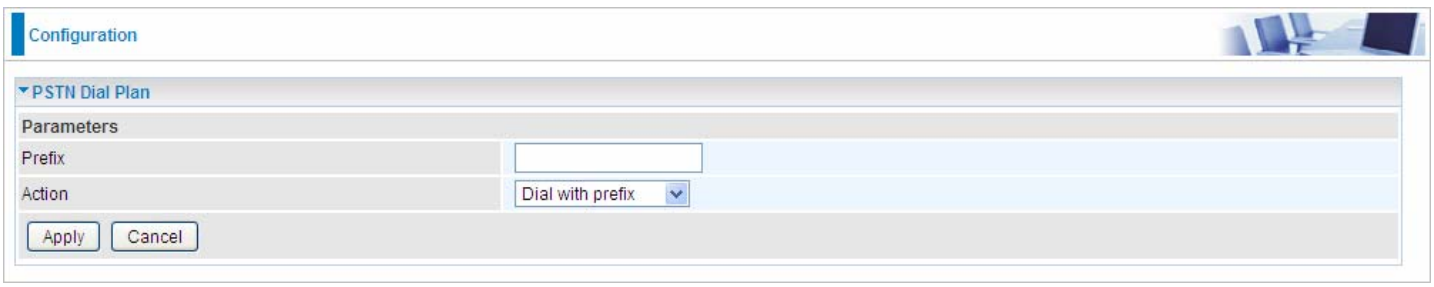
Phone Port: Decide which phone the incoming PSTN call routing applies to.

Answering Machine: Enable to activate the answering machine feature for PSTN so that user can record and listen to the messages of this phone.

Send Message Via E-mail: Enable to send message left by callers via e-mail to the user.

Dial Plan

Click **Add** to add new rules.



Prefix: Specify number(S) marking as the tag for switching to a PSTN call.

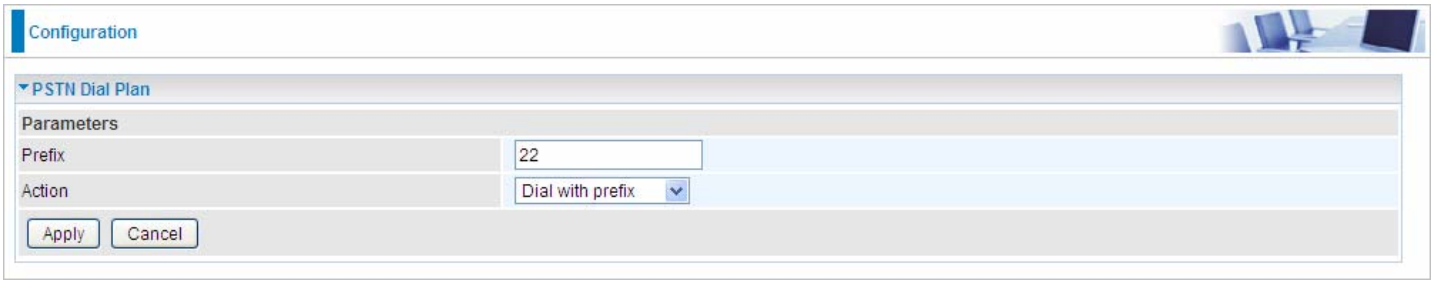
Action: The dialing mechanism.

- **Dial with Prefix:** The dialed number together with the prefix will be sent to call through PSTN.
- **Dial without Prefix:** The dialed number will be sent to call through PSTN without prefix.

Note: The x. wildcard character is supported here by PSTN dial plan. x specifies one digit between 0 and 9. x. specifies any sequence of variable length, the maximum length is 32.

Examples of PSTN dial plan:

1. Dial with Prefix

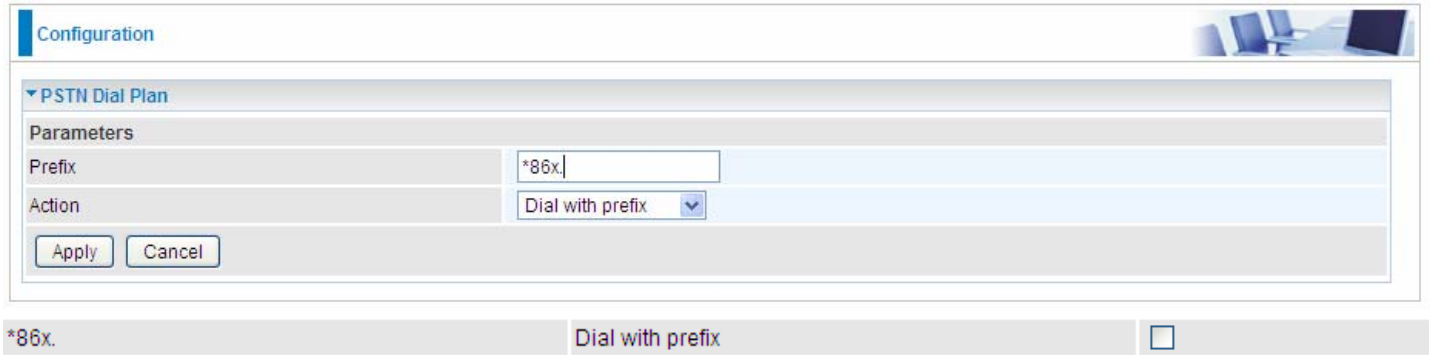


If you dial 2250505, number 2250505 will be dialed out via FXO to make a regular phone call.

2. Dial without Prefix

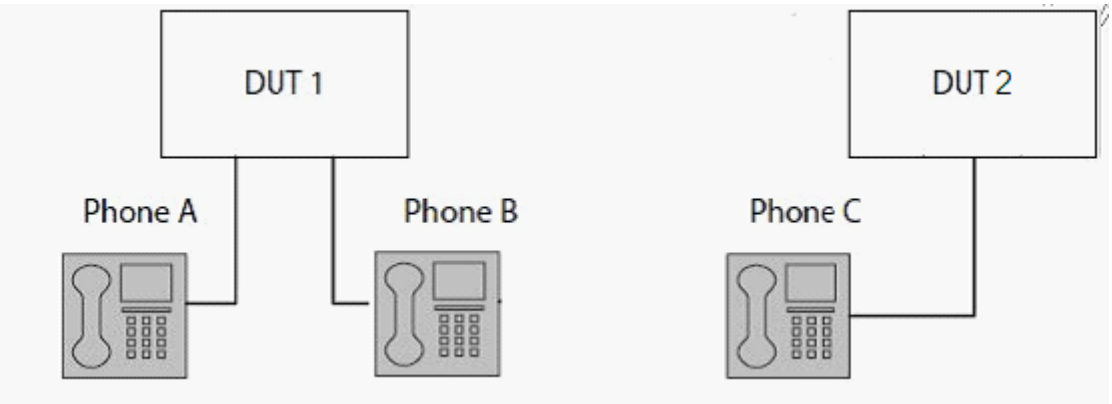
In this example, if user wants to dial out 50505(the destination extension number), please first dial 22 and it will get the PSTN dial tone from CO site and then dial 50505 to make a regular phone call.

3. With x wildcard character.



If User wants numbers with prefix *860, *8601, *862, etc all to be dialed out via FXO together with these prefix, and then he could turn to the reference above..

How to establish conference call: 3 –way call scenario



Case 1: Phone A invites Phone C to join a conference call

Step – 1: Phone A presses flash (hold original call), and A hears the dial tone

Step – 2: Phone A calls Phone C. C and A are on a new call.

Step – 3: Phone A presses flash (hold new call) and return to original call

Step – 4: Phone A tells Phone B that he wants to set up a conference with Phone C.

Step – 5: Phone A presses flash again to merge all 3 calls

Case 2: Phone C dials in and wants to join Phone A and Phone B's conference

Step – 1: Phone A and Phone B on a call, then Phone C dials Phone A and A hears a waiting tone

Step – 2: Phone A presses flash and picks up the call waiting call

Step – 3: Phone A presses flash to hold the call with Phone C and return to original call with Phone B

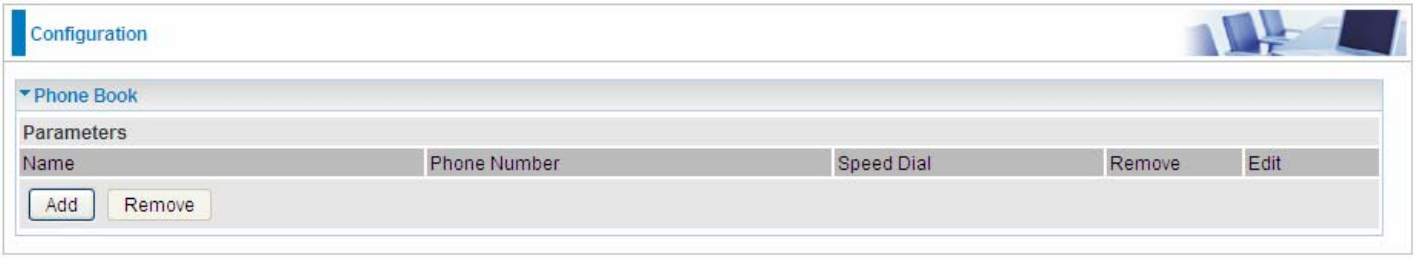
Step – 4: Phone A tells Phone B that he wants to set up a conference with Phone C.

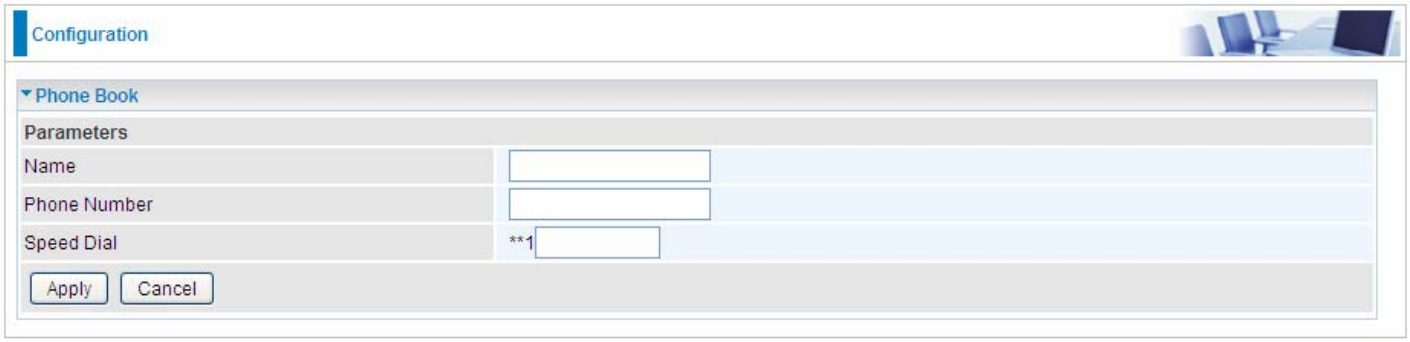
Step – 5: Phone A presses flash again to merge all 3 calls.

Phone Book

Phone Book / Speed Dial comes at hand to store frequently used telephone number(s) that you can press **1xx instead of the exact dialing-out number on the phone keyboard to make a quick dialing. For example, if the destination number 5522772 was mapped to a speed-dial number of **105, and then user can easily press **105 on the phone keyboard, you will be linked to the destination of 5532772, call established..

Note: xx, please remember only two digits (0-9) allowed to identify the phone number.





Name: User-defined identification.

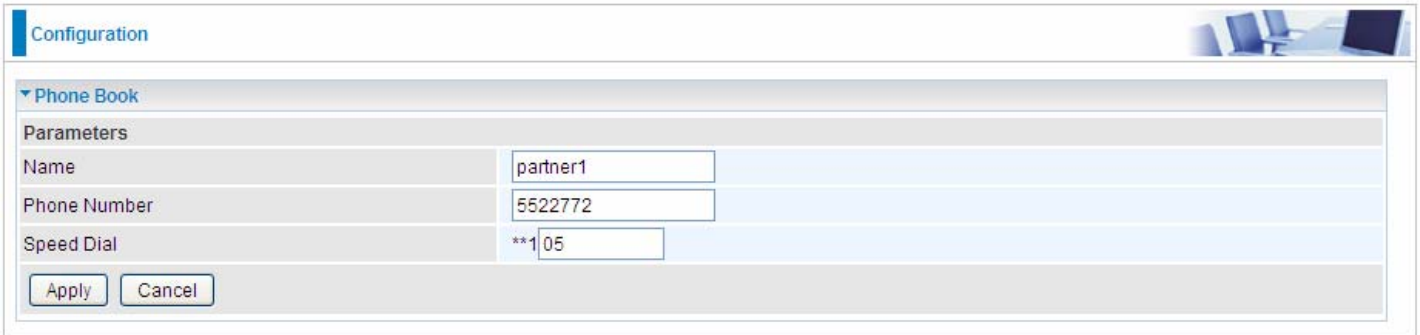
Phone Number: The full destination phone number user wants to be simplified to a speed-dial number.

Speed Dial: Set the speed-dial number for the destination number.

Simple example:

A user wants to simplify a frequently used phone number to an easy and friendly number for a quick dialing, and then speed dial is a good choice for him.

For example, the frequently used phone number is 5522772, and mapped to **105, then he can only dial out **105 to make the call.



PDF-XChange Viewer Click to buy NOW! www.docu-track.com

Configuration

Phone Book

Parameters

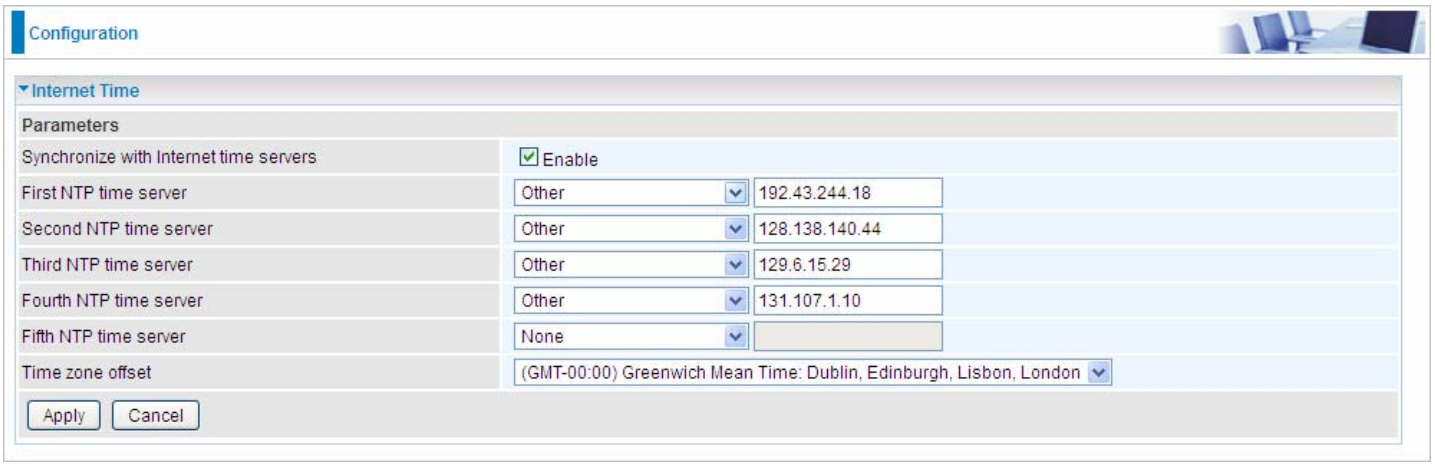
Name	Phone Number	Speed Dial	Remove	Edit
partner1	5522772	**105	☐	Edit

Add Remove

Internet Time

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.



Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an NTP server for you to use.

Click **Apply** to apply your settings.