ADSL2+ Modem With
150Mbps Wireless-N Router

User Manual

Certification
FCC CE

FCC Statement

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

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

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This unit complies with Part 15 & 68 of FCC Rules. Operation is subject to following two conditions:

1) This device may not cause harmful interference
2) This device must accept any interference received, including. Interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

INFORMATION TO BE SUPPLIED TO USERS
We confirm that the following information will supplied to the users of this equipment. This information will be provided with the user's manual.

FCC REQUIREMENTS
This equipment complies with Part 68 of the FCC rules and the requirements adopted by the

ACTA. On the exterior of the cabinet of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. A product identifier in the format US: SX5DL04BDL4302R. If requested, this number must be provided to the telephone company.

FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. See Installation Instructions for details. The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. Typically, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line (as determined by the total RENs) contact the local telephone company. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary. The telephone company may make changes to its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice so you can make the necessary modifications to maintain uninterrupted service.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

CONTENTS

1. Introduction

Thank you for choosing the **150Mbps Wireless-N ADSL2+ Modem Router**.

1.1. Product Overview

The device is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or IEEE 802.11n/ IEEE 802.11g/ IEEE 802.11b wireless network.

The router connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, IP/MAC Filter, Application Filter and DNS Filter can help to protect your network from potentially devastating intrusions by malicious agents from the outside of your network.

Quick Start of the Web-based Utility is supplied and friendly help messages are provided for the configuration. Network and Router management is done through the Web-based Utility which can be accessed through local Ethernet using any web browser.

ADSL

The product supports full-rate ADSL2+ connectivity conforming to the ITU and ANSI specifications. In addition to the basic DMT physical layer functions, the ADSL2+ PHY supports dual latency ADSL2+ framing (fast and interleaved) and the I.432 ATM Physical Layer.

Wireless

In the most attentive wireless security, the Router provides multiple protection measures. It can be set to turn off the wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The Router provides wireless LAN 64/128-bit WEP encryption security, WPA-PSK/WPA2-PSK authentication.

1.2. Package Contents

The following contents should be found in your package:

- One 150Mbps Wireless N ADSL2+ Modem Router
- One Power Adapter
- User Manual
- RJ45 cable
- RJ11 cables
- One ADSL splitter
- CD-ROM

1.3. Main Features

- Four 10/100Mbps Auto-Negotiation RJ45 LAN ports (Auto MDI/MDIX), one RJ11 port.
- Wireless N speed up to 150Mbps.
- 5dBi antenna provides extended range for better performance of signal coverage and reception.
- Adopts Advanced DMT modulation and demodulation technology.
- Multi-user sharing a high-speed Internet connection.
- Downstream data rates up to 24Mbps, upstream data rates up to 1Mbps.
- Supports long transfers, the max line length can reach to 6.5Km.
- Supports PPPoE, it allows connecting the internet on demand and disconnecting from the internet when idle.
- Provides reliable ESD and surge-protect function with quick response semi-conductive surge protection circuit.
- High speed and asymmetrical data transmit mode, provides safe and exclusive bandwidth.
- Supports All ADSL industrial standards.
- Provides integrated access of internet and route function which face to SOHO user.
- Built-in DHCP server.
- Built-in firewall, supporting MAC filter, IP filter and DNS filter.
- Supports Virtual Server, DMZ host and IP Address Mapping.
- Supports Dynamic DNS, UPnP and Static Routing.
- Supports system log and flow Statistics.
- Supports firmware upgrade and Web management.
- WPS (PIN/PBC) enabled, easy one-touch WPA wireless security encryption with the WPS button.
- Provides WPA-PSK/WPA2-PSK data security.
- 802.1Q VLAN binds specific LAN ports and PVCs for differential services.
- Supports TR-069 and SNMP.

1.4. Conventions

The Router or device mentioned in this User Manual stands for the product without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

2. Hardware Installation

2.1. The Front Panel

Figure 2-1

The LEDs locate on the front panel, they indicate the device's working status. For details, please refer to LED Explanation.

LED Explanation:

Name	Status	Indication
PWR	On	Power is on
	Off	Power is off
ADSL	Flash	The ADSL negotiation is in progress
	On	The LINE port is linked up.
	Off	The LINE port is linked down.
Internet	Flash	Data is being transferred over the Internet.
	On	A successful PPP connection has been built.
	Off	There is no successful PPP connection or the Router works on Bridge mode.
WLAN	Flash	There is wireless data being transmitted.
	On	The wireless function is enabled but no data is being transmitted.
	Off	The wireless function is disabled.
LAN(1-4)	Flash	Data is being transferred over the 1-4 (LAN) port.
	On	There is a successful connection on the corresponding 1-4 (LAN) port but no activity.
	Off	There is no connection on the corresponding 1-4 (LAN) port or the connection is abnormal.
WPS	Slow Flash	Wi-Fi Protected Setup (WPS) are ongoing
	Off	Wi-Fi Protected Setup (WPS) is disabled or a wireless device has been connected to the Router by WPS function.

2.2. The Back Panel

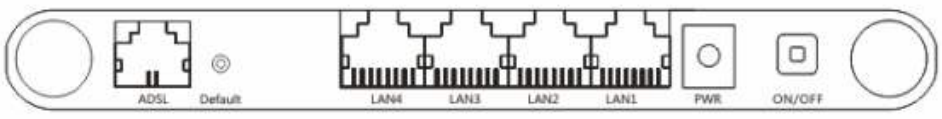


Figure 2-2

- **PWR**: The Power plug is where you will connect the power adapter.

- **1, 2, 3, 4 (LAN)**: Through the port, you can connect the Router to your PC or the other Ethernet network device.
- **Default**: There are two ways to reset the Router's factory defaults. **Method one:** With the Router powered on, use a pin to press and hold the Reset button for at least 5 seconds. And the Router will reboot to its factory default settings. **Method two**: Restore the default setting from "System Management - Restore" of the Router's Web-based Utility.
- **ADSL**: Through the port, you can connect the router with the telephone. Or you can connect them by an external separate splitter. For details, please refer to 2.4.
- **Antenna**: Used for wireless operation and data transmit.

2.3. Installation Environment

- The product should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.
- The Router can be placed on a shelf or desktop.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

2.4. Connecting the Router

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.**Step 1**: Connect the ADSL Line.

Method one: Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of the router, and insert the other end into the wall socket. **Method two:** You can use a separate splitter. External splitter can divide the data and voice, and then you can access the Internet and make calls at the same time. The external splitter has three ports: • Line: Connect to the wall jack • Phone: Connect to the phone sets • Modem: Connect to the ADSL LINE port of the router Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of the router. Connect the other end to the MODEM port of the external splitter.

Step 2: Connect the Ethernet cable. Attach one end of a network cable to your computer's Ethernet port or a regular hub/switch port, and the other end to the LAN port on the router.

Step 3: Power on the computers and LAN devices.

Step 4: Attach the power adapter. Connect the power adapter to the power connector on the rear of the device and plug in the adapter to a wall outlet or power extension.

Figure 2-3

3. Quick Installation Guide

3.1. Configure PC

After you directly connect your PC to the product or connect your adapter to a Hub/Switch which has connected to the Router, you need to configure your PC's IP address. Follow the steps below to configure it.

3.1.1. For Windows 2000 or Windows XP as below.

Step 1: Right Click My Network Places. Then select Properties (shown in Figure 3-1).

Figure 3-1

Step 2: Right Click **Local Area Connection**. Then select **Properties**.

Figure 3-2

Step 3: Double click the **Internet Protocol [TCP/IP]**.

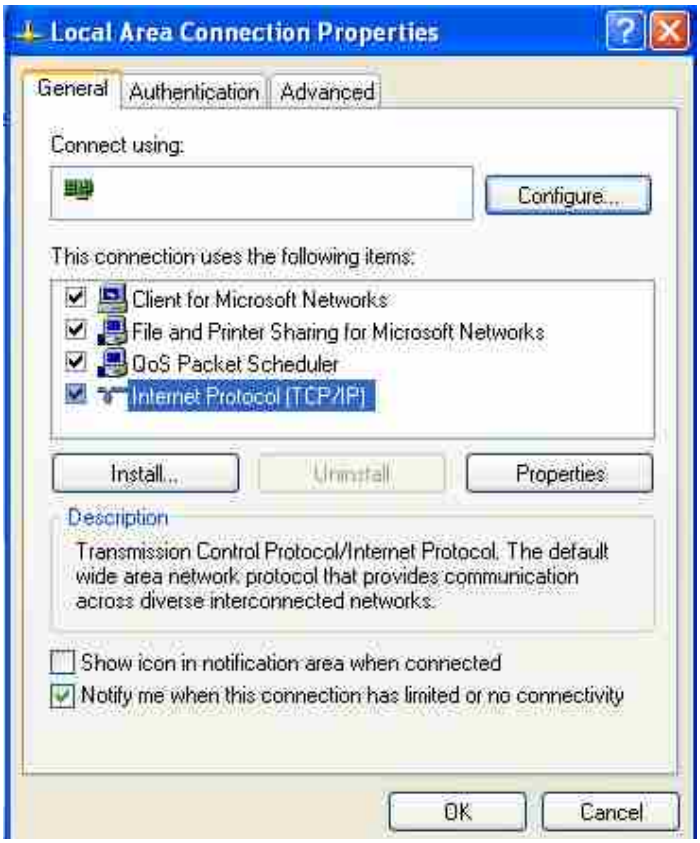


Figure 3-3

Step 4: Configure the IP address as Figure 3-4 shows. After that, click **OK**.

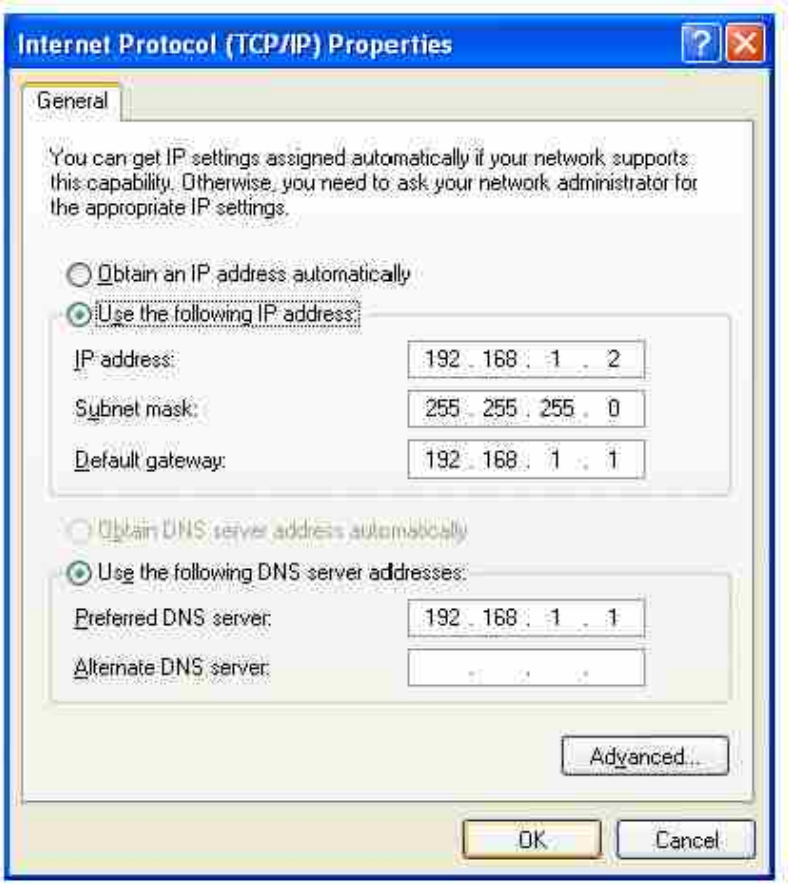


Figure 3-4

Note:

You can configure the PC to get an IP address automatically, select "Obtain an IP address automatically" and "Obtain DNS server address automatically" in the screen above.

3.1.2. For Windows 7 or Windows Vista as below.

Step 1: Click  , then select the **Open Network and Sharing Center.**

Figure 3-5

Step 2: Click the **Change adapter settings**.

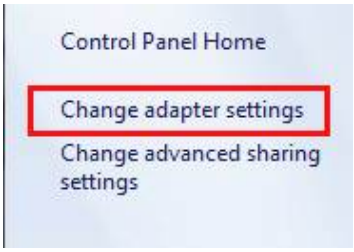


Figure 3-6

Step 3: Click **Local Area Connection** with the right button of your mouse. Then select **Properties**.

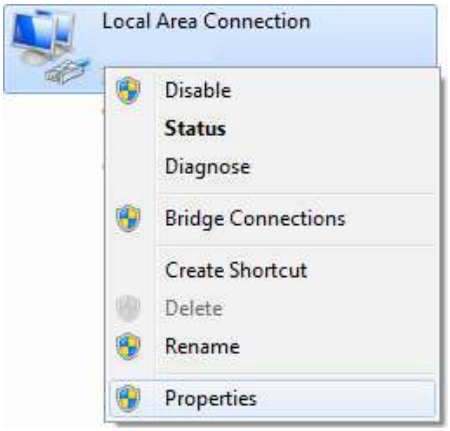


Figure 3-7

Step 4: Double click the "**Internet Protocol Version 4(TCP/IPv4)**".

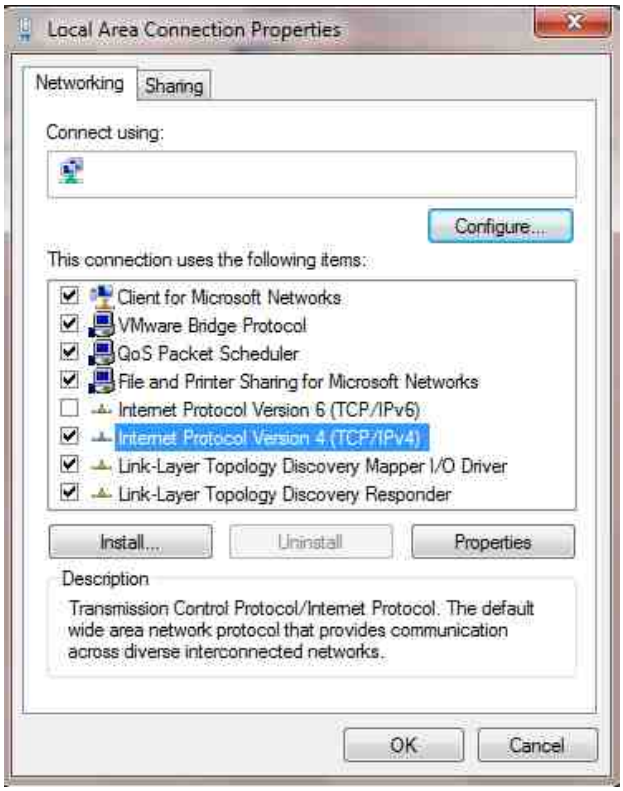


Figure 3-8

Step 5: Select the "**Obtain an IP address automatically**" as below. Then click "**OK**".

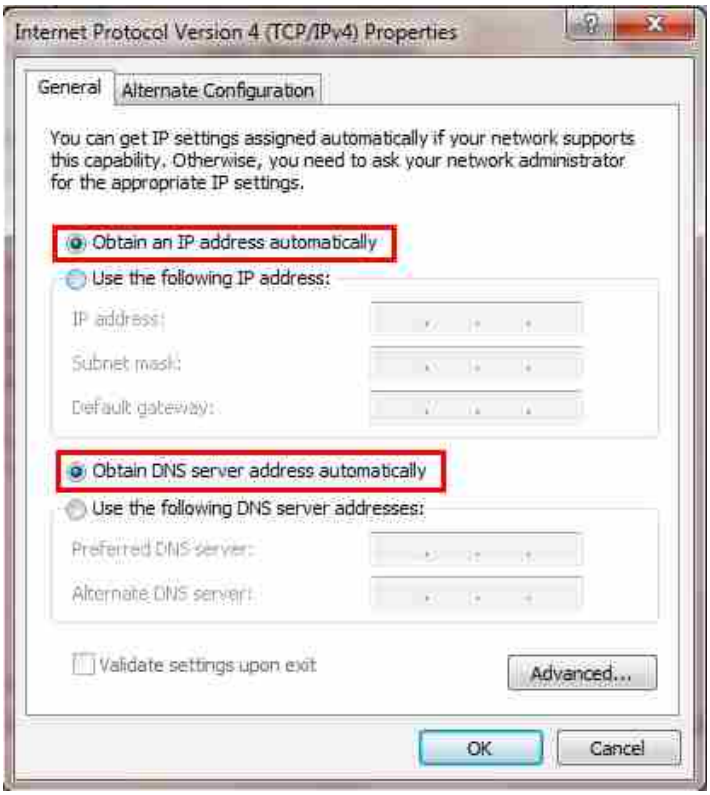


Figure 3-9

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd or command** in the field and press **Enter**. Type ***ping 192.168.1.1*** on the next screen, and then press **Enter**.

If the result displayed is similar to the screen below, the connection between your PC and the Router has been established.

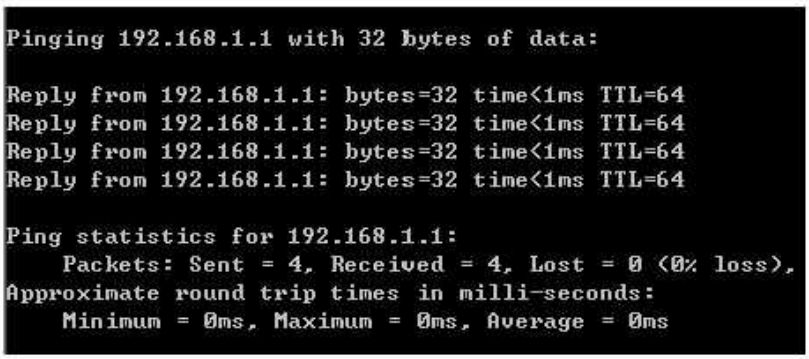


Figure 3-10

If the result displayed is similar to the screen shown below, it means that your PC has not connected to the Router.

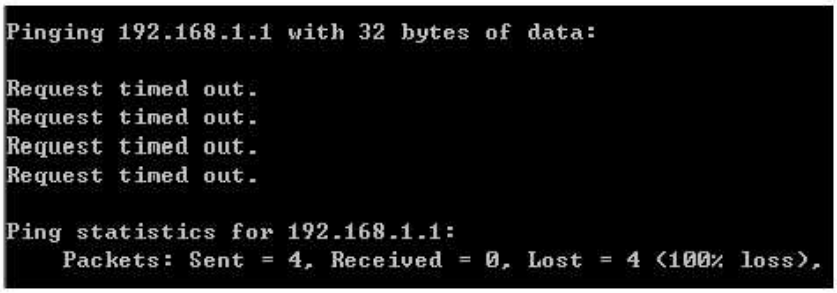


Figure 3-11

You can check it follow the steps below:

1) **Is the connection between your PC and the Router correct?**
   The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.
2) **Is the TCP/IP configuration for your PC correct?**
   If the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254.

3.2. Login

Once your host PC is properly configured please proceed as follows to use the Web-based Utility:

Start your web browser and type the private IP address of the Router in the URL field: **192.168.1.1**.

After that, you will see the screen shown below, enter the default User Name **guest** and the default Password **guest**.

Figure 3-12

And then click **OK** to access to the **Wireless Modem Management Panel** screen.

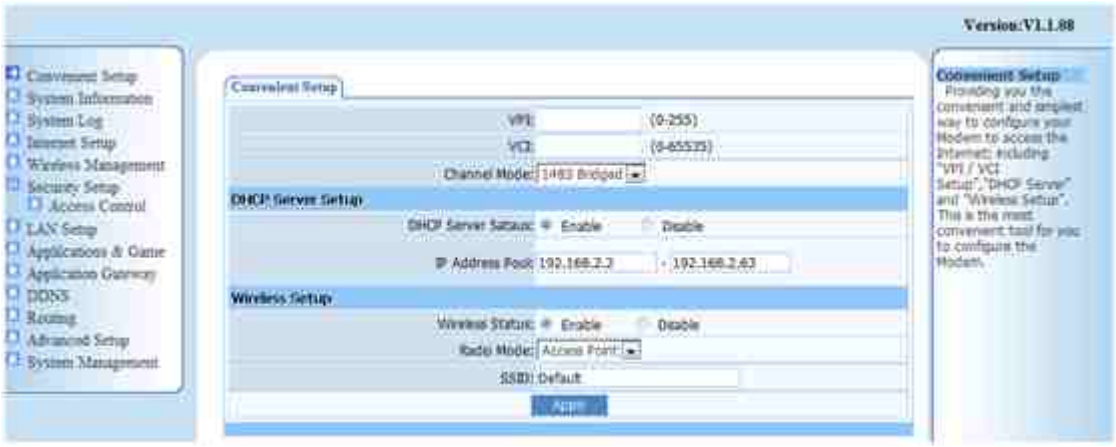


Figure 3-8

4. Modem Management

After your successful login, you can configure and manage the device. There are main menus on the left of the Web-based Utility. To apply any settings you have altered on the page, please click the **Apply** or **Save** button.

4.1. Convenient Setup

This webpage provides you the convenient and simplest way to configure your Modem to access the internet.

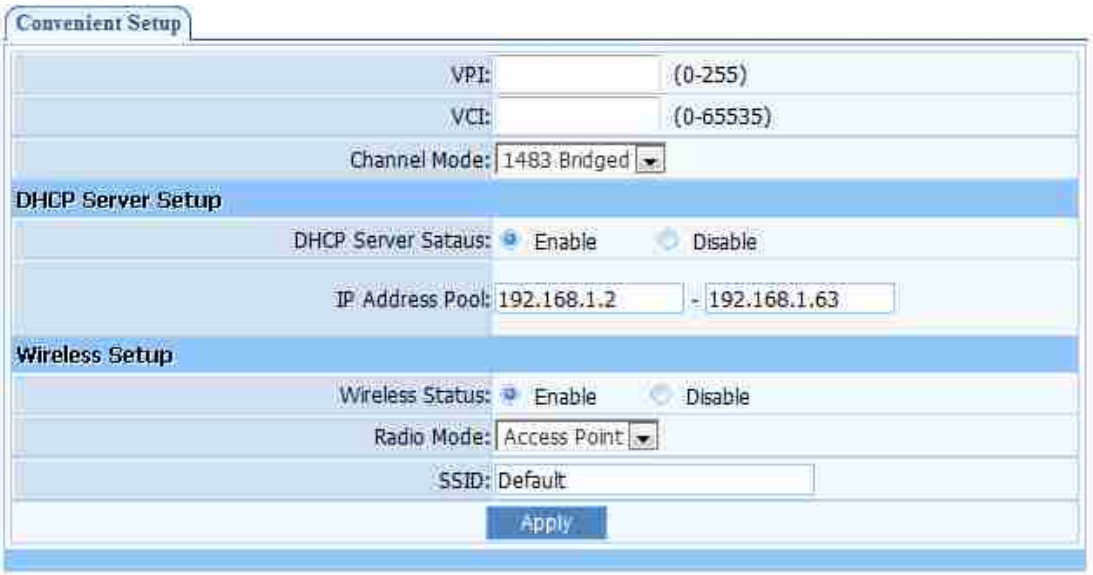


Figure 4-1

1) .....

VPI: Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. Please input the value provided by your ISP.

2) .....

VCI: Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.

3) .....

NAPT: Select this option to Enable/Disable the NAPT (Network Address Port Translation) function for this PVC. The NAPT function can be activated or deactivated per PVC basis.

4) .....

Channel Mode:

a) .....

1483 Bridged: If you select this type of connection, the modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN. This mode allows you use the product as an ADSL modem. You could set up a dial-up connection to the Internet by using your own computer without sharing.

b) .....

1483 MER: When RFC 1483 MER (MAC Encapsulated Routing) is enabled on a router, it allows configuration of an ATM Access Concentrator for both modem and router deployment since it supports bridge encapsulation as well as IP encapsulation. ATM cells are encapsulated with an IP address header when routing; ATM cells are encapsulated with a MAC address header when bridging.

What all this techno-speak means is that RFC 1483 MER allows you to do IP routing with NAT on the LAN side of the CPE router and bridging on the WAN side. And when NAT and MER are enabled on the CPE router, a customer network of many workstations will appear the same as a single workstation behind a modem.

If you select this channel mode, you will see a screen show in below.

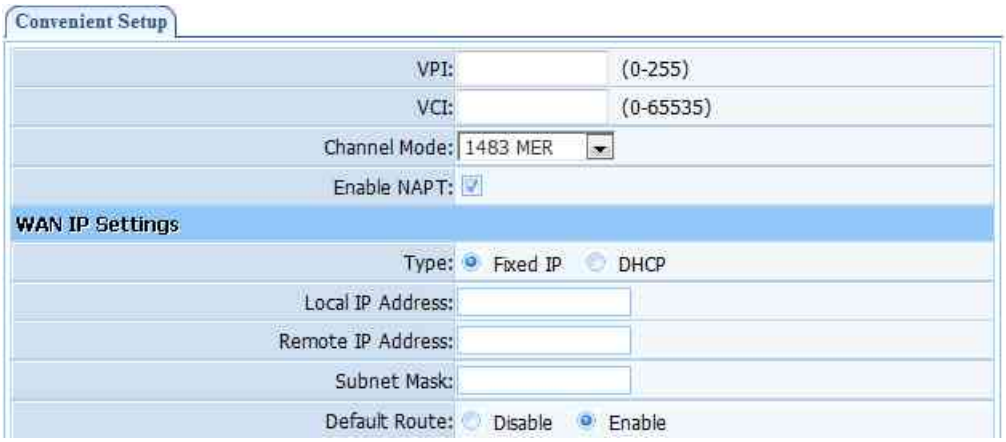


Figure 4-2

You can configure IP routing automatically using DHCP, or manuanlly by providing the following information:

- .....
  Local IP Address
- .....
  Remote IP Address
- .....
  Subnet Mask

If you NSP has not provided specifics for these settings, and you are unsure what is appropriate, choose this type **DHCP** and **NAPT** enabled.

c) .....

PPPoE/PPPoA: If you want to share an ADSL among your local network, please select this mode and type in the PPPoE/PPPoA account and password to make your the product connect to Internet. (show in Figure 4-3).

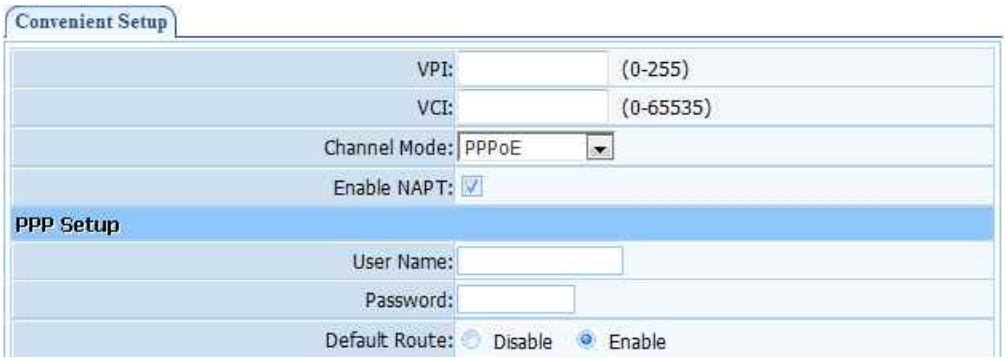


Figure 4-3

➢ .....

User Name: Enter your username for your PPPoE connection.

➢ .....

Password: Enter your password for your PPPoE connection.

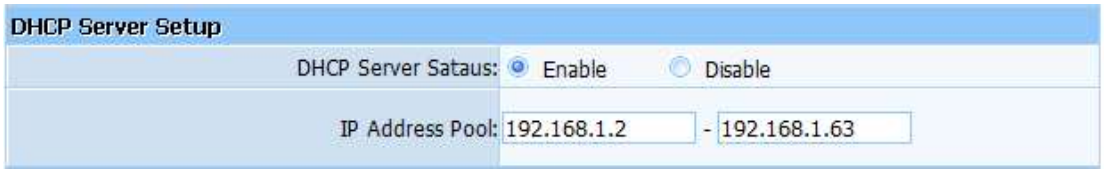
➢ .....

Default Route: You should select **Enable** to configure the PVC as the default gateway to internet from this device.

5) .....

DHCP Server Setup

Here you can select the DHCP Server Status enable or disable and configure IP Address Pool range.



Figuer 4-4

6) .....

Wirelss Setup

Here you can select Wielress Status enable or disable and configure SSID for your wireless network.

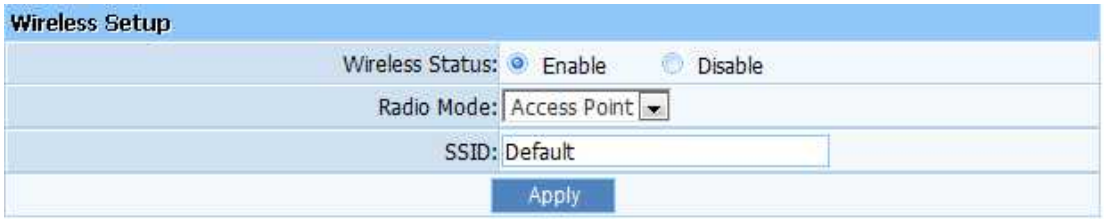


Figure 4-5

After configuring all the Settings, click **Apply** to take effect.

4.2. Internet Setup

Choose "**Interface Setup**", you can see the next submenus: **Internet Setup, QoS for PVC, ADSL Setup** and **Port Mapping**. Click any of them, and you will be able to configure the corresponding function.

4.2.1. Internet Setup

Choose "**Interface Setup Internet Setup**" menu, you can configure the parameters for your internet.

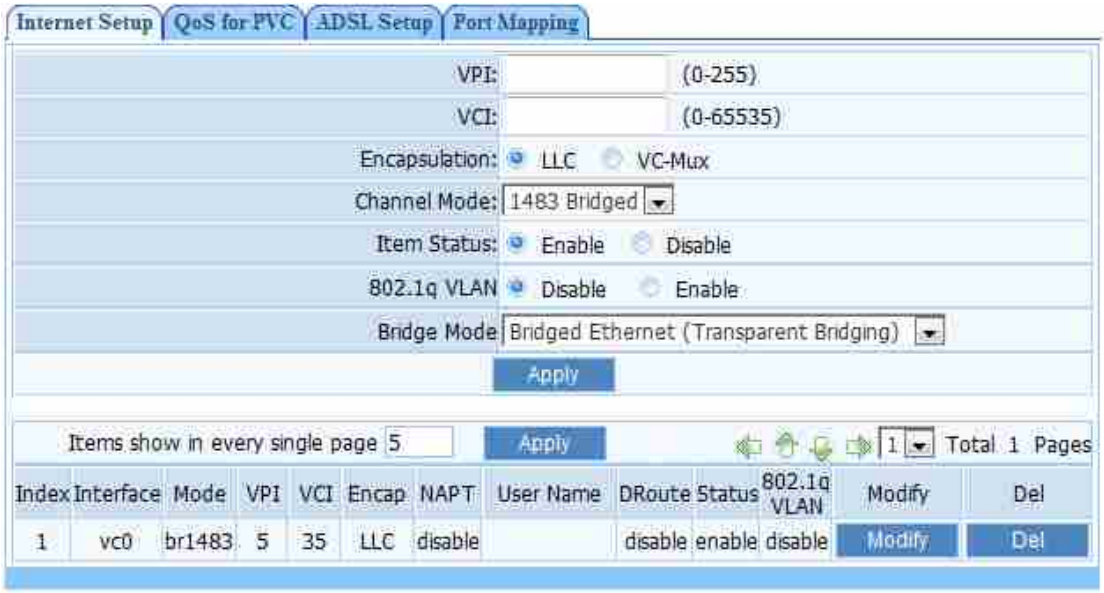


Figure 4-6

1) .....

VPI/VCI: Refer to **4.1**.

2) .....

Encapsulation: Select the encapsulation mode for the Dynamic IP Address, you can leave it default.

3) .....

Channel Mode: Refer to **4.1**.

4) .....

Item Status: you can configure the item take effect or not.

5) .....

802.1q VLAN: Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same LAN, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.

802.1q VLAN in this router binds specific LAN ports and VCs for differential services such as IPTV. Select **Enable** to enable this function, and then enter the specified VLAN ID which is provided by your IPTV provider. (show in Figure 4-7)

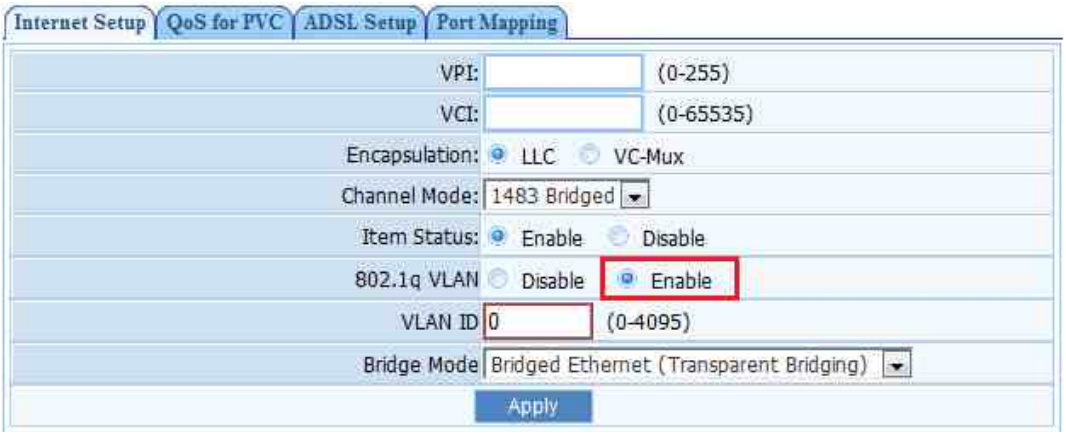


Figure 4-7

Note:

Some VCs for IPTV do not needs to configure 802.1q VLAN, please get more details from your ISP.

6) .....

Bridge Mode:

a) .....

Bridged Ethernet (Transparent Bridging): Default Bridge Mode.

b) .....

Bridged PPPoE (implies Bridged Ethernet): In this mode only PPPoE data packets can through the PVC.

c) .....

Disable Bridge

After you finish configuration, please click **Apply** to make the settings take effect. Then the system will generated a record in the screen below. You can also modify or delete the record which you configured.

Figure 4-8

4.2.2. QoS for PVC

Choose menu "**Interface Setup QoS for PVC**" menu, you can see the next screen. (show in Figure 4-9)

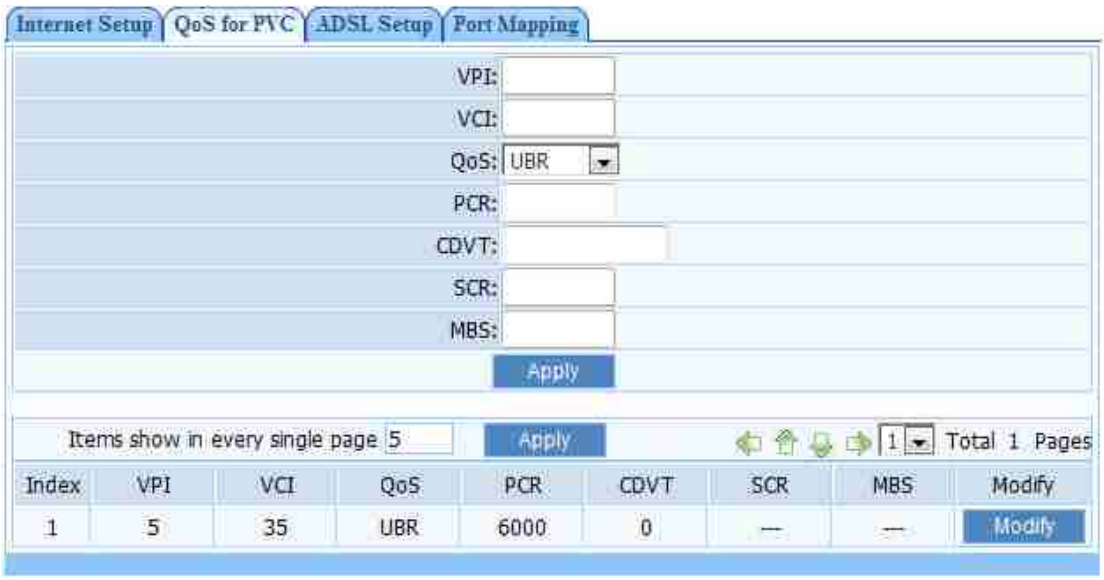


Figure 4-9

This settings are used to connect to your ISP. Your ISP provides VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) settings to you. In this Device, you can totally setup 8 VCs on different encapsulations, if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority. Click the **Modify** button to configure. (show in Figure 4-10)

➢ .....

VPI & VCI: Refer to **4.1**.

➢ .....

QoS: Select the Quality of Service types for this Virtual Circuit, including CBR (Constant Bit Rate), UBR (Unspecified Bit Rate) and VBR (Variable Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR (Peak Cell Rate), SCR (Sustained Cell Rate),CDVT (Cell Delay Variation Tolerance) and MBS (Maximum Burst Size), please configure them according to your needs.

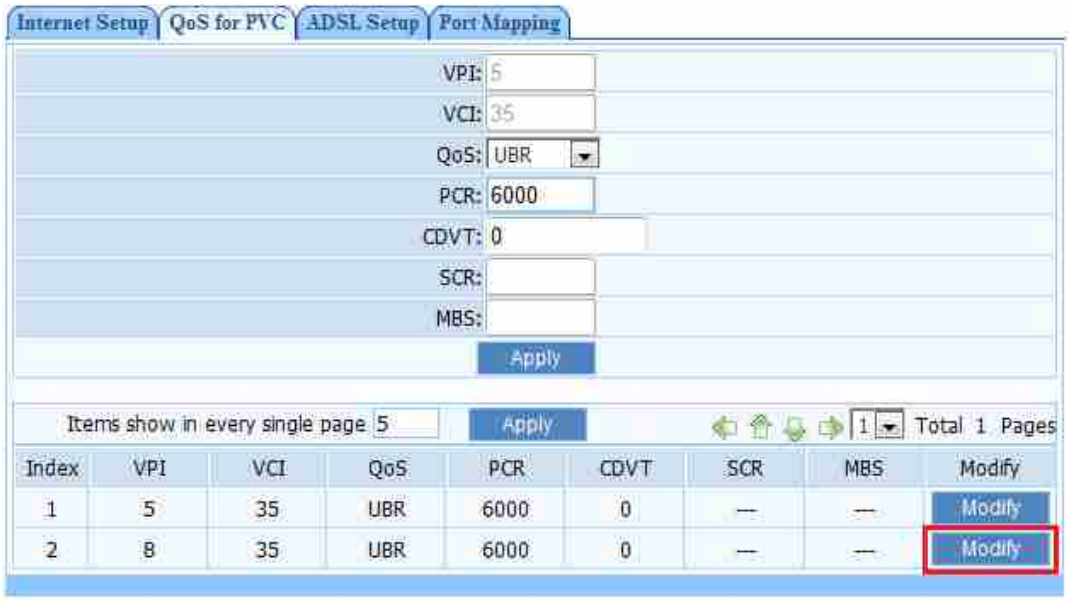


Figure 4-10

4.2.3. ADSL Setup

Choose "**Interface Setup ADSL Setup**" menu, you can see the ADSL Setup webpage show in Figure 4-11.

This feature provides options for user to setup ADSL modulation mode, AnnexL option, AnnexM option, ADSL Capability and ADSL Tone. Please configure them according to your needs.

Figure 4-11

4.2.4. Port Mapping

Choose "**Interface Setup Port Mapping**" menu, you can see the next screen show in Figure 4-12.

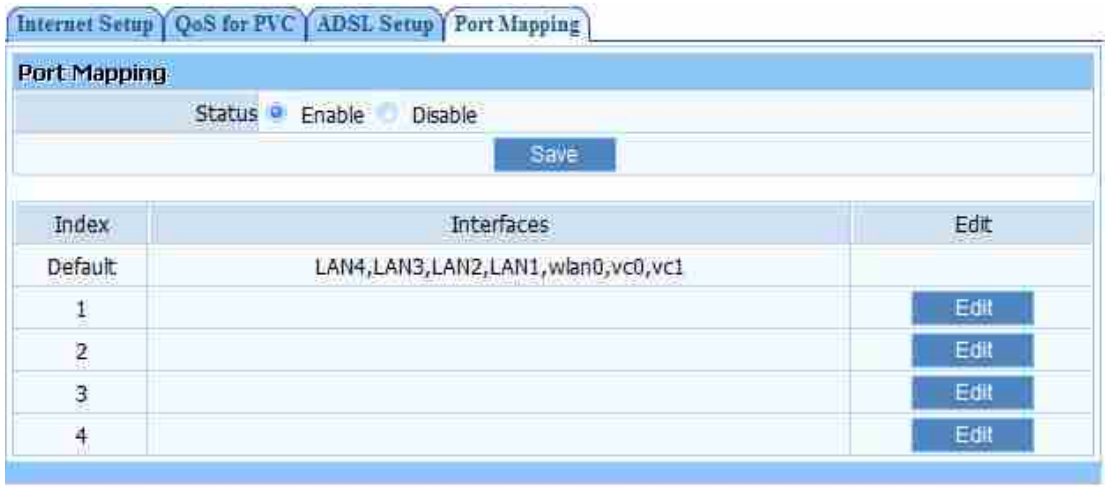


Figure 4-12

This router can supports 4 groups editable Port Mapping. This function is similar to Port-VLAN, it binds specified LAN port to VCs to implement some special network applications, such as IPTV.

The bound port will not be used on other VCs.

For Example:

If you want to add a Port Mapping entry binds “LAN4” to “vc1”, please follow these instruction:

1. Configure PVC “vc1”, refer to **4.2.1**.
2. Select **Enable** marquee to enable the Port Mapping status, click the **Save** button to make it effective.
3. Click one of the **Edit** button, select the LAN/WLAN port and PVCs you want to bind. (show in Figure 4-12)

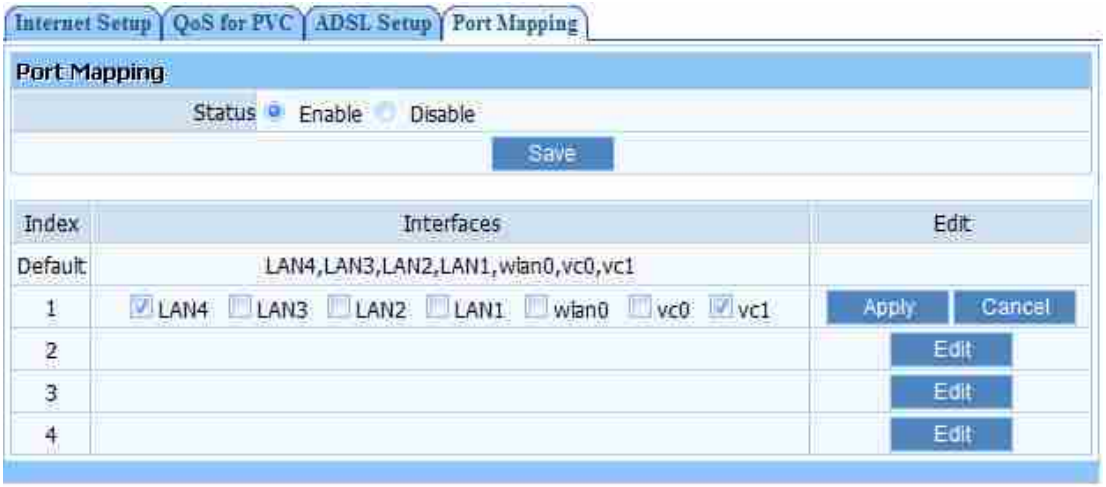


Figure 4-12

4. Then click **Apply** button to make it effective. (show in Figure 4-13)

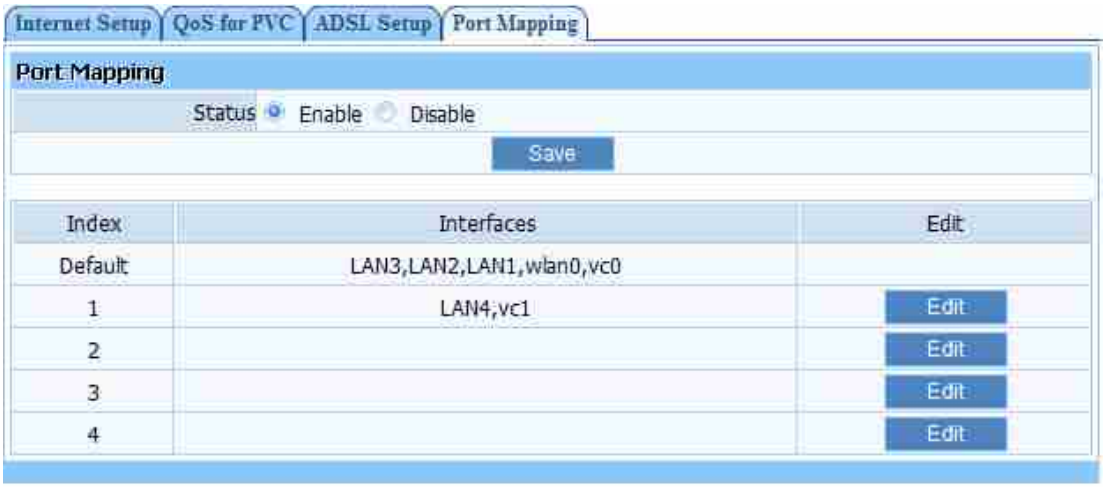


Figure 4-13

If you want to modify Port Mapping entries, click the **Edit** button.

4.3. System Information

Choose "**System Information**” menu, you can see the screen show in Figure 4-14.

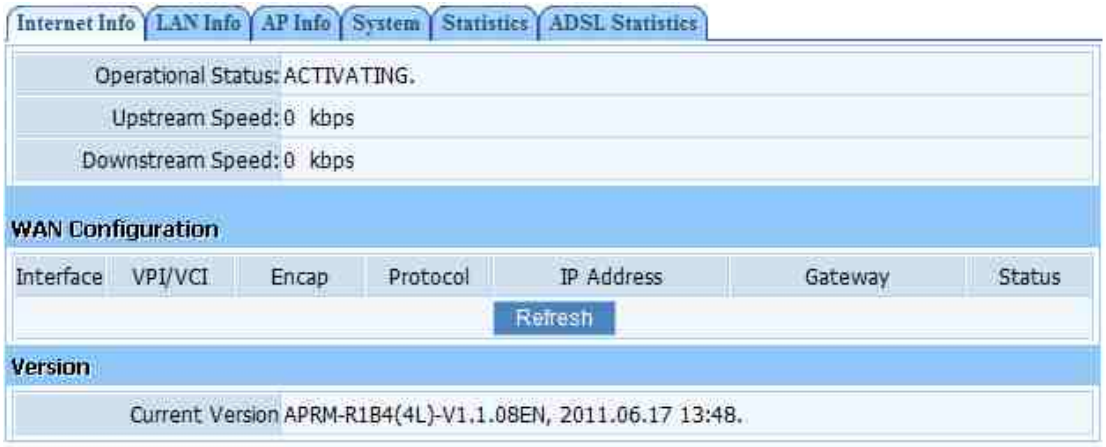


Figure 4-14

This feature displays current status of the Router.

➢ .....

Internet Info: This feature provides running status information of the WAN port (The port connect to the Internet), and displays the current version of the software.

➢ .....

LAN Info: This item provides information about Modem's LAN port, display LAN port's MAC address, IP address and current situation of DHCP server.

➢ .....

AP Info: This item provides current running information of Primary AP.

a) .....

Wireless Status: Display wireless interface status is enabled or not.

b) .....

Wireless Status: Display the current number of wireless stations associated with router.

c) .....

Wireless Mode: Current wireless mode of wireless router.

d) .....

Channel: Display current channel of your wireless router.

e) .....

SSID: SSID (Service Set Identifier) is your wireless network's name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. So make sure all points in the wireless network have the same SSID, we suggested to user the default SSID.

f) .....

Wireless MAC Address: The MAC address is used for wireless communication.

g) .....

SSID Broadcasting: You can select "enable" or "disable" to enable or disable the broadcast SSID function, if the setting of the field is disable, wireless client can not obtain this SSID to login in, the user have to input the SSID value manually.

h) .....

Security Mode: Display whether your security wireless function have been applied.

➢ .....

System: This item provides current running information of System.

➢ .....

Statistics: This item provides statistics information about the bits router sends and received, including LAN, WAN and WLAN.

➢ .....

ADSL Statistics: Statistical information about the current ADSL lines.

4.4. System Log

Choose "**System Log**" menu, and you will be able to query the logs of the Modem.The Modem can keep logs of all traffic. You can query the logs to find what happened to the Modem.

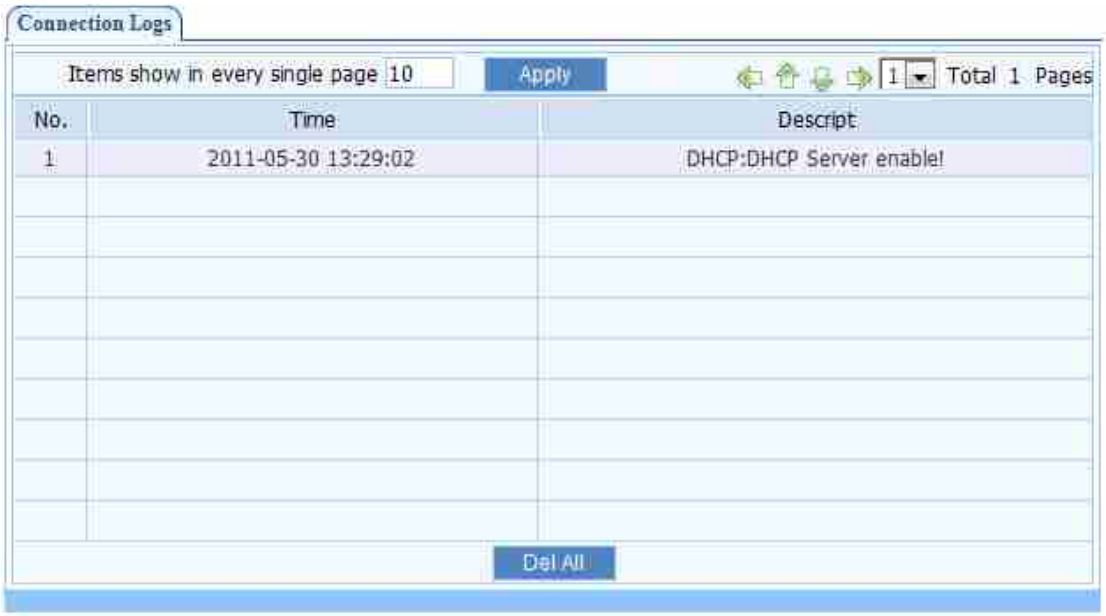


Figure 4-15

Click the **Del All** button to clear the logs.

4.5. Wireless Management

Choose "**Wireless Management**" menu, and you will see the submenus. (show in Figure 4-8)

Figure 4-16

Please configure the parameters for wireless according to the descriptions below.

4.5.1. Basic

Providing basic configuration items for wireless router users, including "Wireless network status ", "Band", " Radio mode", nine basic configuration items.

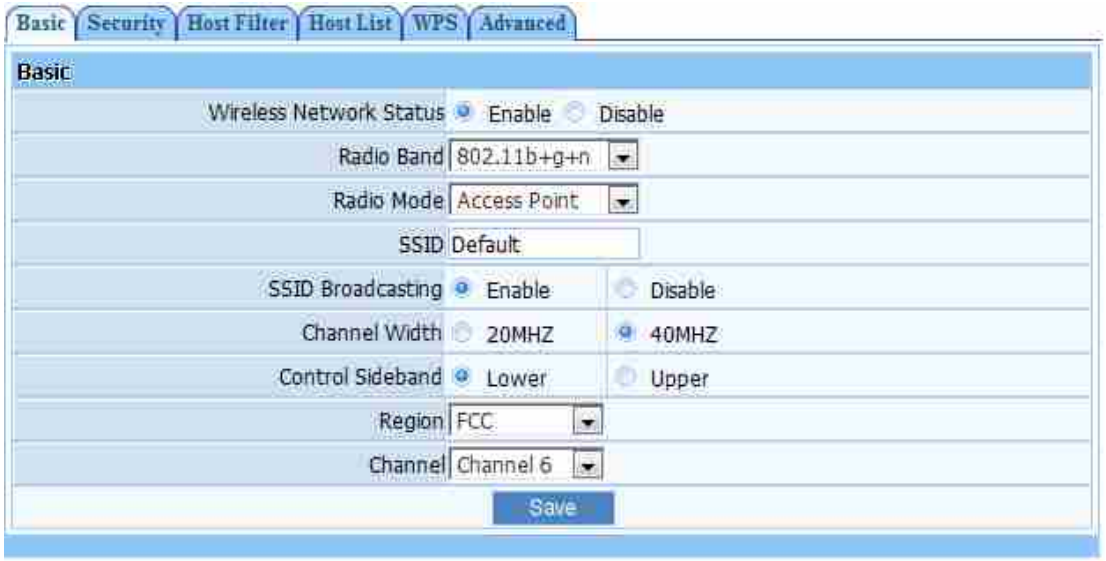


Figure 4-17

➢ .....

Wireless Network Status: You can choose "enable" or "disable" to enable or disable the "Wireless Network Status", if you choose "Disable", the AP function of wireless router will be turned off.

➢ .....

Radio Band: You can select the wireless standards running on your network, the default setting is 802.11b/g/n Mixed.

➢ .....

Radio Mode: You can select radio mode of wireless router, the default setting is AP mode.

➢ .....

SSID: SSID (Service Set Identifier) is your wireless network's name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. So make sure all points in the wireless network have the same SSID, we suggested to user the default SSID.

➢ .....

SSID Broadcasting: You can select "enable" or "disable" to enable or disable the broadcast SSID function, if the setting of the field is disable, wireless client can not obtain this SSID to login in, the user have to input the SSID value manually.

➢ .....

Channel Bandwidth: This switch allows you to set Router's wireless bandwidth modes:

a) .....

20MHz: Setting the Router to this mode only allows 20MHz operation. This mode is compatible with 802.11n, 802.11g and 802.11bgear, but will limit Wireless N routers' bandwidth by half the rate.

b) .....

40MHz: Setting the Router to this mode allows only 40MHz operation. This mode is compatible only with router, draft 802.11n compliant devices. It may affect legacy 802.11b/g devices. Use only when you have a pure router, draft 802.11n wireless network.

➢ .....

Control Sideband: It controls your wireless router use the higher or lower channel to tranfer related datas while it working on 40Mhz mode.

➢ .....

Channel: You can set the working channel from 1 to 14 manually to avoid interference.

4.5.2. Security

Choose "**Security Setup** **Access Control**", you can see the Security screen shown below.

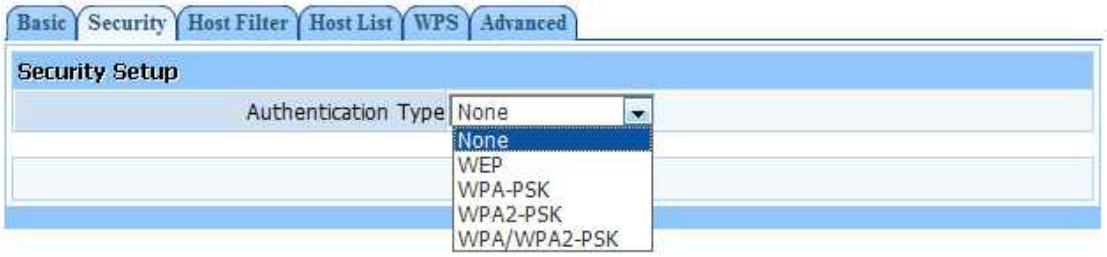


Figure 4-18

The item allows you to encrypt your wireless communication, and you can also protect your wireless network from unauthorized user access

➢ .....

Authentication Type: There supplies "**None**", "**WEP**", "**WPA-PASK**", "**WPA2-PSK**" and "**WPA/WPA2-PSK**" five different encryption modes. "**None**" means do not encrypt wireless data.

✧.....

WEP: There are two basic levels of WEP encryption, 64 bits and 128 bits, the more bits password have, the better security wireless network is, at the same time the speed of wireless is more slower. If you select WEP to encrypt your data, choose the bits of password, it should be 64 bits or 128 bits. Then choose the format of password; it should be HEX or ASCII. The valid character for HEX format should be numbers from 0 to 9 or letters from A to F. HEX doesn't support mixed letter and number mode. And ASCII supports mixed both letters and numbers. By default, router provides four fields to input four groups of password, you can input all of them or only one of them, and the client 's password only need to match one group of password.

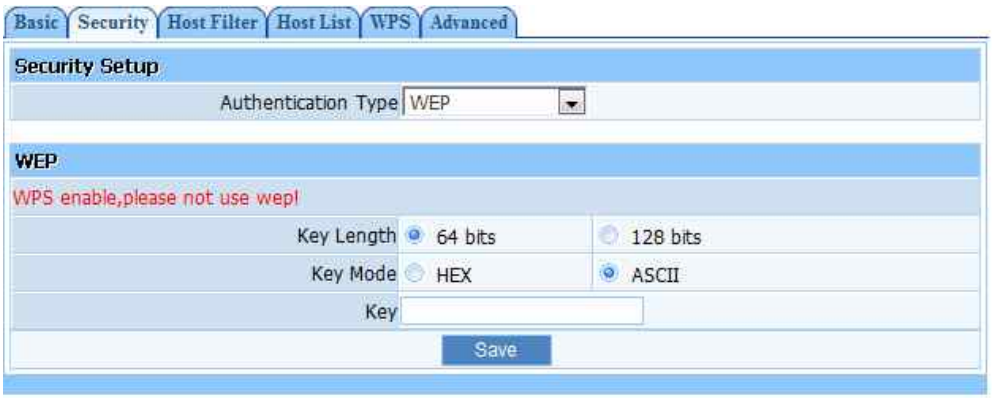


Figure 4-19

Note:

When WPS function enabled, please don't use WEP authentication. More details

about WPS, please refer to 4.5.5.

✧.....

WPA-PSK: You can select the algorithm you want to use, TKIP or AES. TKIP means "Temporal Key Integrity Protocol", which incorporates Message Integrity Code (MIC) to provide protection against hackers. AES, means "Advanced Encryption System", which utilizes a symmetric 128-Bit block data encryption. You can set key renewal time in the "Key Renewal" field.

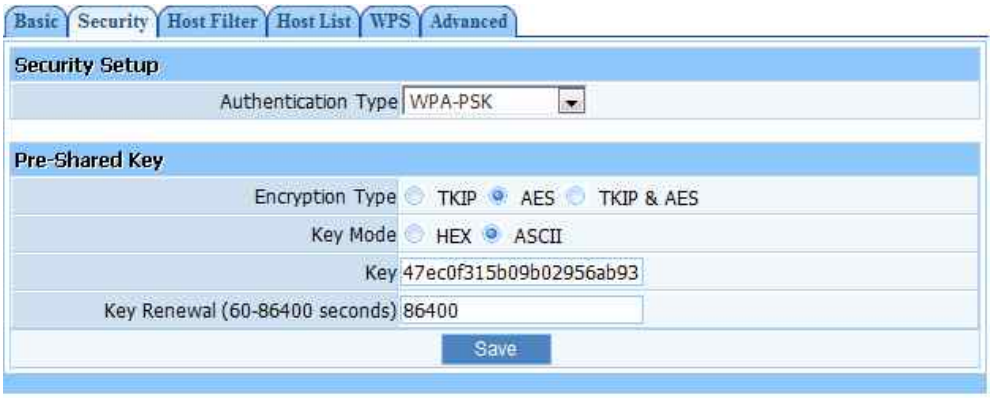


Figure 4-20

✧.....

WPA2-PSK: The WPA2-PSK is similar to WPA -PSK and with stronger encryption method than WPA-PSK, using WPA2-PSK; you should input password (leave this value in the range of 8 to 63 characters) and key renewal time (leave this value in the range of 60 to 86400 seconds).

✧.....

WPA&WPA2-PSK: This item mixed WPA-PSK and WPA2-PSK mode, which provides higher security level; you can configure it according with WPA-PSK or WPA2-PSK.

4.5.3. Host Filter

Choose "**Security Setup** **Host Filter**", you can see the next screen shown below.

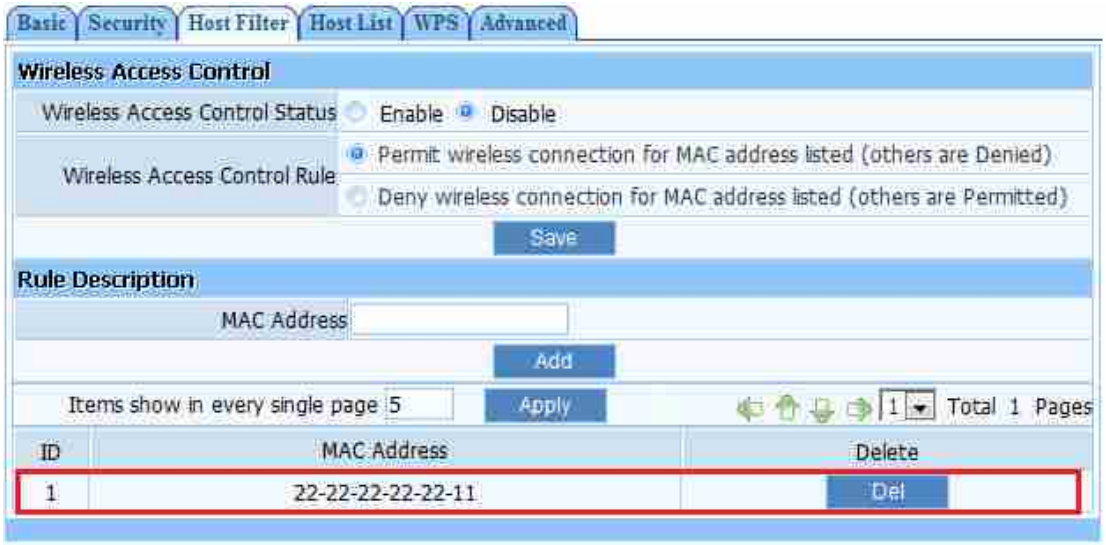


Figure 4-21

You can filter wireless users by enabling this function; thus unauthorized users can not access the

network. To disable "Wireless Host Filter", keep the default setting "Disable". To enable "Wireless Host Filter", follow these steps to set "Wireless Host Filter".

➢ .....

Add MAC address you want to control in the "MAC address" field (the format is XX-XX-XX-XX-XX-XX), then click "Add" button, and you will see the MAC address has displayed in the MAC list.

➢ .....

There are two items supplied, "Permit wireless connection for MAC address listed (others are Denied)" and "Deny wireless connection for MAC address listed (others are Permitted)", Select the item you want, and click "Save Settings" button.

4.5.4. Host List

Choose "**Security Setup** **Host List**", you can see the next screen shown below.

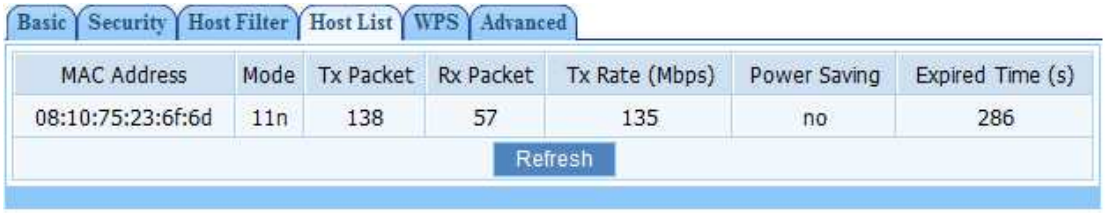


Figure 4-22

This page display current status of the wireless client associate with AP.

4.5.5. WPS

Choose "**Security Setup** **WPS**", you can see the WPS screen shown below.

Figure 4-23

Wi-Fi Protected Setup (WPS) is a standard for easy and secure establishment of a wireless network. Traditionally, users would have to manually create a wireless network name (SSID), and then manually entering a creative, yet predictable security key on both the access point and client to prevent unwanted access to their wireless network. This whole process requires the

users to have the background knowledge of the Wi-Fi devices and the ability to make the necessary configuration changes. With WPS, it will automatically configure a wireless network with a network name (SSID) and strong WPA data encryption and authentication. WPS is designed to support various Wi-Fi certified 802.11 products ranging from access points, wireless adapters, Wi-Fi phones, and other consumer electronics devices.

Note:

More configuration details about WPS, please refer to 5.2.

4.5.6. Advanced

Choose "**Security Setup** **Advanced**", you can see the next screen shown below.

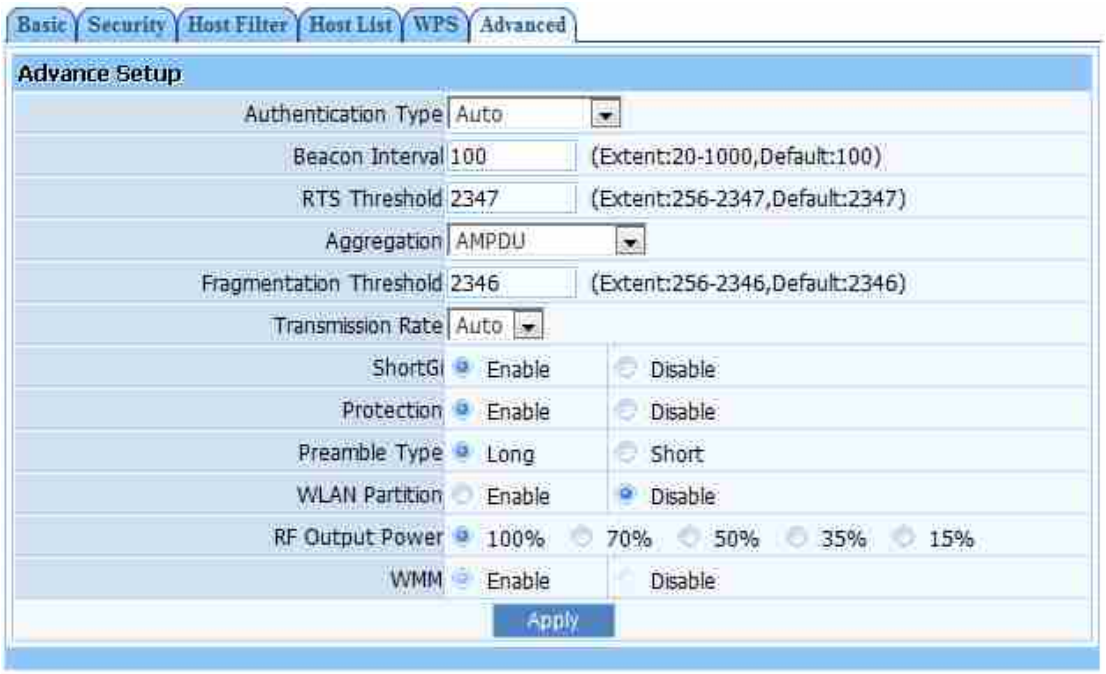


Figure 4-24

This page display current status of the wireless client associate with AP, If you have no special requirements, we suggest that you do not change the settings.

➢ .....

Authentication Type: The default is set to "Auto Select", which allows "Open System" or "Shared Key" authentication to be used. Select "Shared Key" if you only want to use "Shared Key" authentication (the sender and recipient use a WEP key for authentication).

➢ .....

Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. You should leave this value in the 256 to 2346 range. In most cases, it should remain as its default value of 2346. Setting the Fragmentation Threshold too low may result in poor network performance.

➢ .....

RTS Threshold: You can set RTS Threshold value in this field, the valid range should be 256-2347 and default value is 2347. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled.

➢ .....

Aggregation: You can accelerate the wireless transmission speed by enabling the aggregation function.

➢ .....

Transmit Rate: Transmit rate indicates the transmission speed of wireless LAN access .The default setting is "Auto" and you can set this value between 1 – 54Mbps range.

➢ .....

Preamble Type: "Short Preamble" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability; the default setting is "Long Preamble".

4.6. Security Setup

Choose "**Security Setup** **Access Control**", you can see submenus shown below.

Figure 4-25

These features make it possible for administrators to control user's access to the Internet, protect the networks.

4.6.1. MAC Filter

You can filter users by enabling this function, thus unauthorized users can not access the network. Follow these steps below to set MAC filter:

Step 1. Add MAC address you want to control in the "MAC address" field (the format is XX:XX:XX:XX:XX:XX), select the filter rules you want to set, then click "Add" button, and you will see the MAC address has displayed in the MAC list.

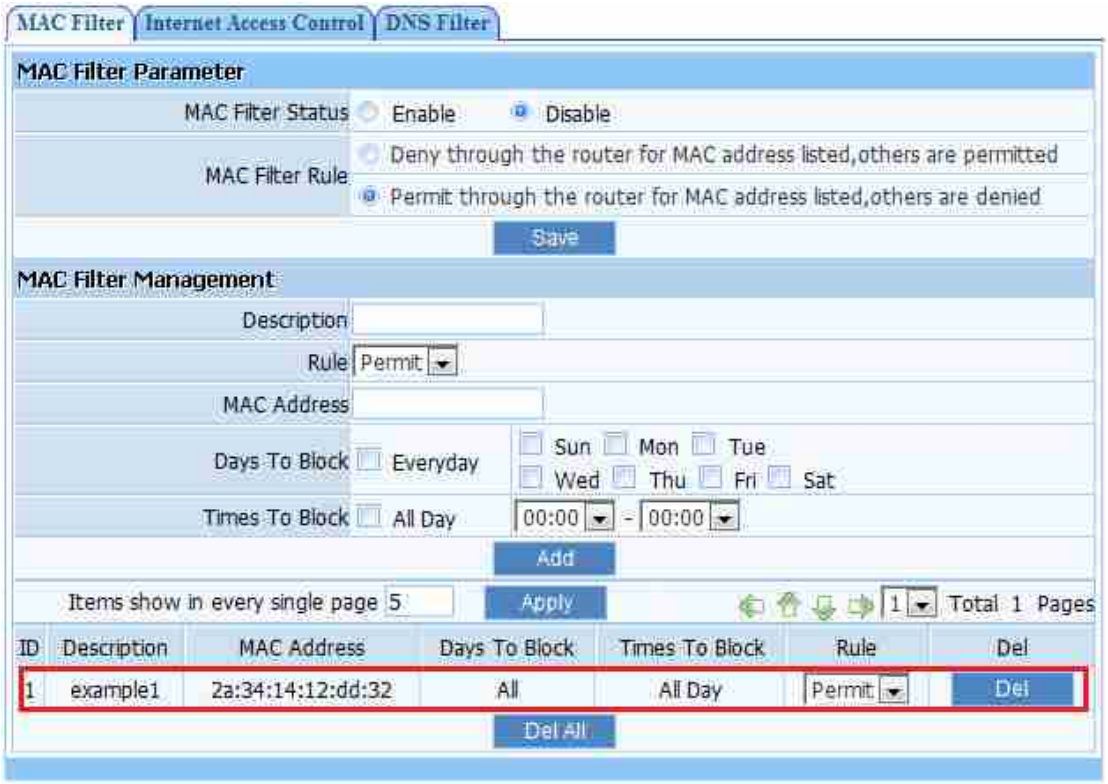


Figure 4-26

Step 2. There are two items supplied, "Permit wireless connection for MAC address listed (others

are Denied)" and "Deny wireless connection for MAC address listed (others are Permitted)", Select the item you want, and click "Save " button.

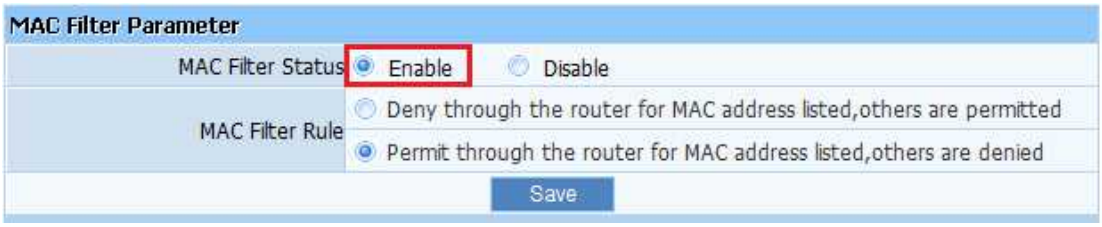


Figure 4-27

4.6.2. Internet Access Control

The rules of "**Internet Access Control**" based on source IP, port number and protocol. Follow these steps to set Internet Access Control:

Step 1. You can select "**Default IP Firewall Rule**" and click "**Save Settings**" to enable "**Internet Access Control**" function. This is only the first step, you should continued to create appropriate rules for "**Internet Access Control**".

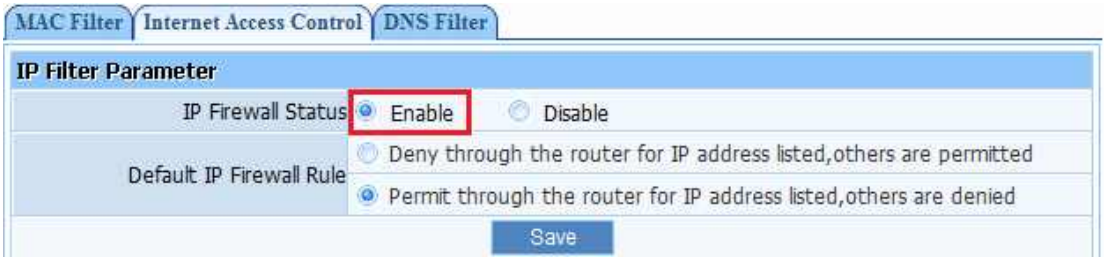


Figure 4-28

Step 2. Input description information for current access control rule in the "**Description**" field. Input IP address of host you want to restrict .If the rule has already existed in "Protocol Template". You can select appropriate item and apply it. Or you can input protocol type and port number manually, click "**Add**" button, then the item will displayed in the list.

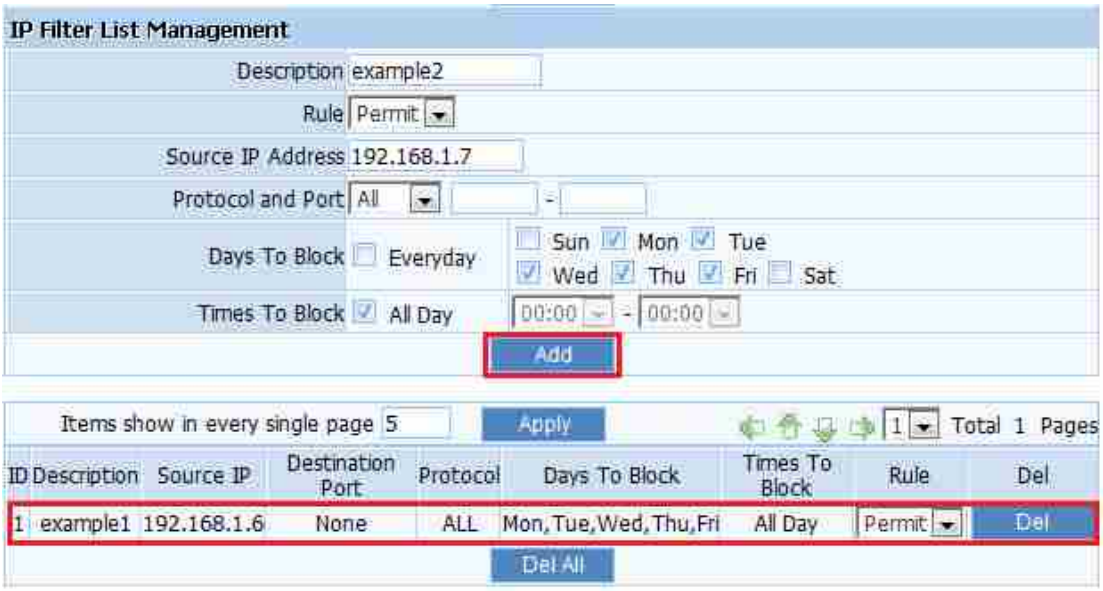


Figure 4-29

Step 3. If you want to delete certain item on the list, select appropriate item on the list, click

"**Del**" to delete it (show in 4-29).

4.6.3. DNS Filter

"**DNS filter**"is able to filter certain domain name such as www.sina.com. Follow these steps to set DNS filter:

Step 1. You can select "**Default DNS filter rule**" and click "**Save**" to enable "**DNS Filter**" function. This is only the first step, you should continued to create appropriate rules for "**DNS Filter**".

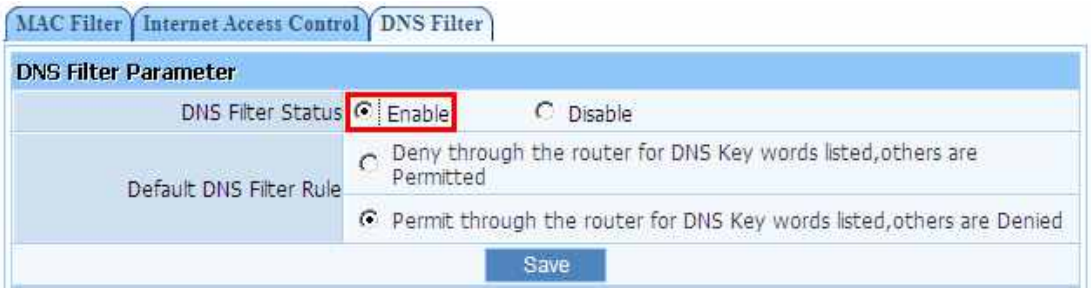


Figure 4-30

Step 2. Input description information in the "**Description**" field for current access control rule, input website name or Domain name in the "**DNS Key Words**" field, such as www.163.com.

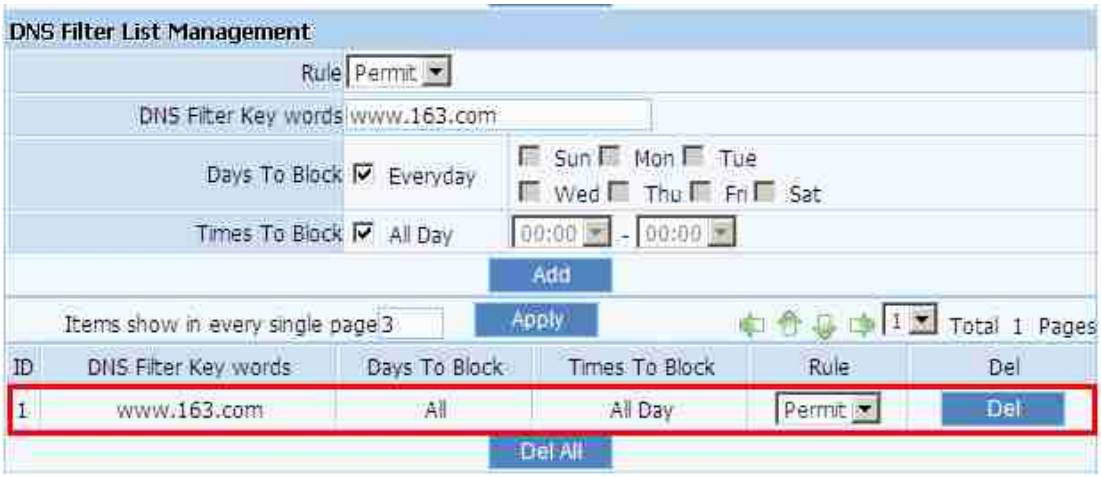


Figure 4-31

4.7. LAN Setup

Choose "**LAN Setup**" menu, and you will see the LAN Setup screen shown below.

Figure 4-32

Please configure the parameters for LAN ports according to the descriptions below.

4.7.1. LAN IP Address

Choose "**LAN Setup** **LAN IP Address**", you can see the next screen shown below.

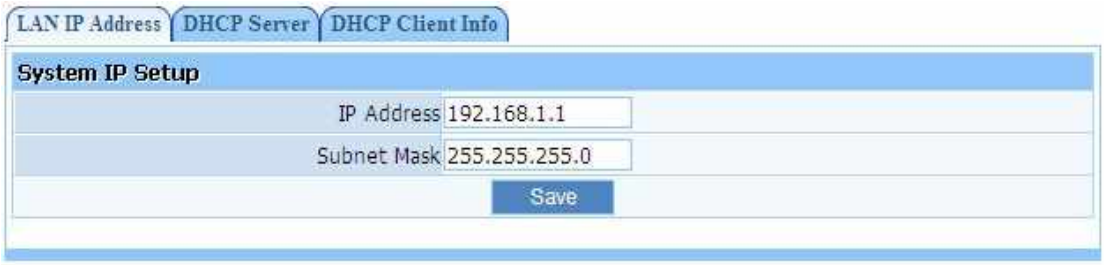


Figure 4-33

These are the IP settings of the LAN interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

➢ .....

IP Address: Enter the Router's local IP Address, then you can access to the Web-based Utility via the IP Address, the default value is 192.168.1.1.

➢ .....

IP Subnet Mask: Enter the Router's Subnet Mask, the default value is 255.255.255.0.

4.7.2. DHCP Server

Choose "**LAN Setup** **DHCP Server**", you can see the next screen shown below.

Figure 4-34

Select **Enabled**, then the Router will work as a DHCP Server, it becomes the default gateway for DHCP client connected to it. DHCP stands for Dynamic Host Control Protocol. The DHCP Server gives out IP addresses when a device is booting up and request an IP address to be logged on to the network. That device must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled.

➢ .....

DHCP Server Setup

✧.....

Status: Keep the default setting “Enable”, so router is able to user DHCP function, if a DHCP server has already existed in the network, please select “Disable”.

✧.....

IP Address Pool: The DHCP pool is used for allocate IP address by DHCP server, the DHCP pool range is also changeable.

✧.....

Lease Time: Display the rest time that router allows dynamic IP users connect to router.

➢ .....

DHCP IP Address Reserving

This function is used to allocate reserve IP address to designated MAC address.

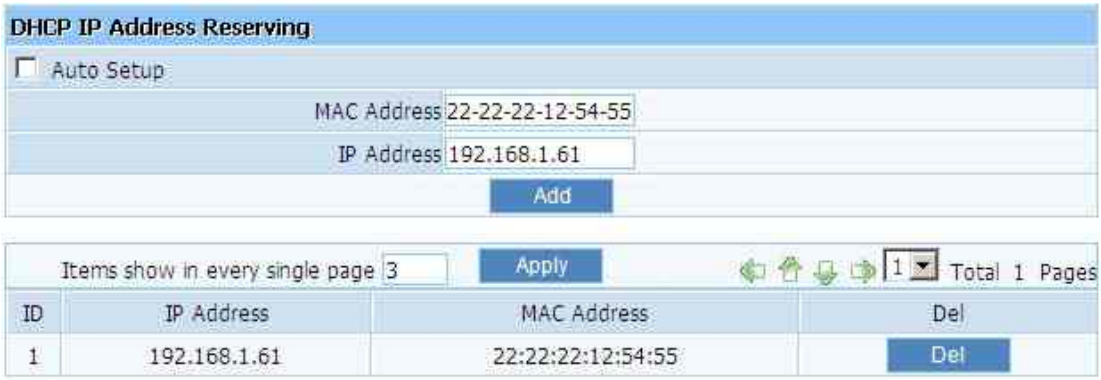


Figure 4-35

4.7.3. DHCP Client Info

Choose "**LAN Setup** **DHCP Server**", you can see the next screen shown below.

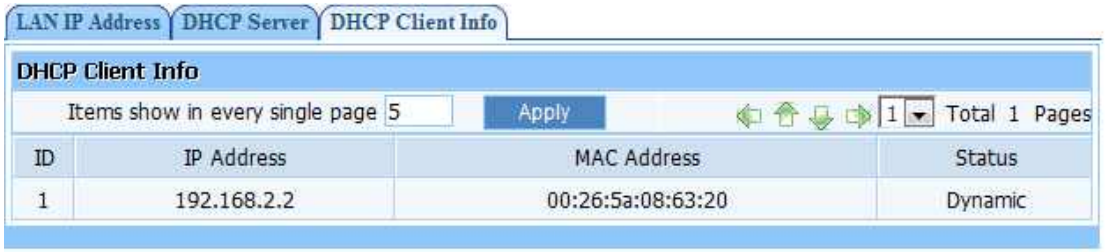


Figure 4-36

This page display DHCP server assigned IP address situation.

4.8. Applications & Games

Choose "**Applications & Games**", you can see the next screen shown below.

Figure 4-37

This item provides configuration items and related templates about optimize games and applications, including "**Virtual server**", "**DMZ**", "**UPnP** " , "**Port Trigger** " and "**IGMP Snooping**".

4.8.1. Virtual Service

Choose "**Applications & Games** **Virtual Service**", you can see the next screen shown below.

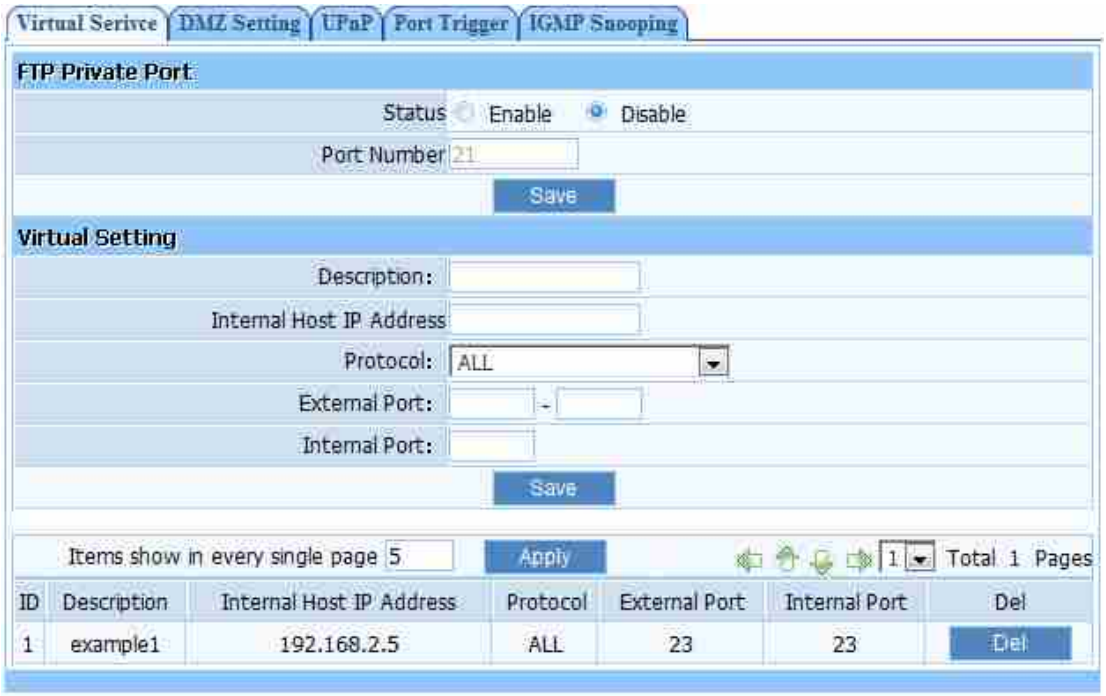


Figure 4-37

Some games, servers, and applications (such as BT, QQ video, Edunkey, Web server) are no longer effect when behind the firewall, so this item provides function of port mapping from LAN to WAN.

➢ .....

FTP Private Port: If you need this function, please choose "Enable".

➢ .....

Virtual Setting

✧.....

Description: Describe current virtual service item.

✧.....

Internal Host IP Address: Indicates IP address of the internal host using virtual server.

✧.....

Protocol: The protocol item supplies several protocols. Such as TCP, HTTP, UDP, POP3, etc. If you have web server within LAN, you can select the HTTP template then the router will set port 80 automatically.

✧.....

External Port: Enter the specific Start and End Port number you want to forward. If it is one port only, you can enter the End port number the same as Start port number. For example, if you want to set the FTP Virtual server, you can set the start and end port number to 21.

✧.....

Internal Port: Enter an intranet port number.

To add a virtual server entry, please enter all items as shown in Figure 4-25. After that, click **"Save"** to make the entry take effect.

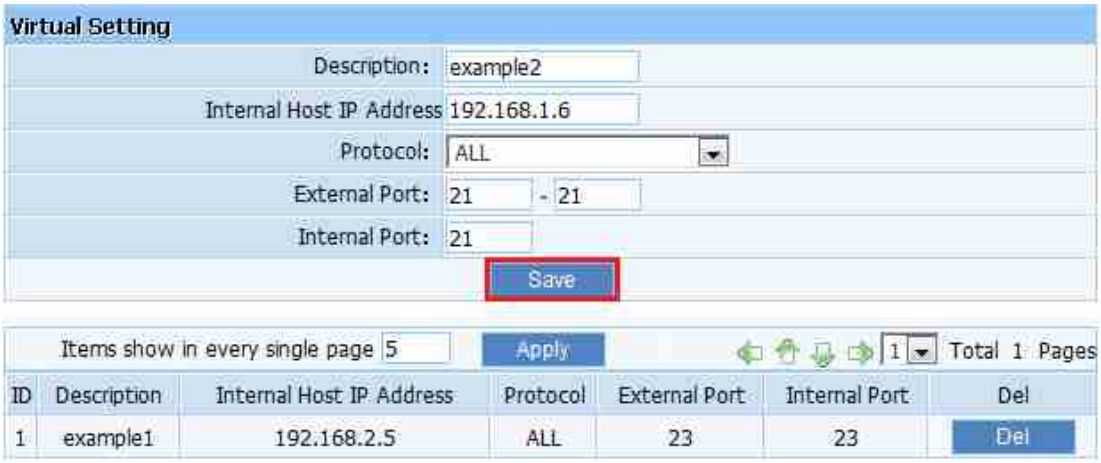


Figure 4-38

4.8.2. DMZ Setting

Choose "**Applications & Games** **DMZ Setting**", you can see the next screen shown below.

Figure 4-39

DMZ opens all the ports of one computer, exposing the computer to the Internet. So it should only be used for some special-purpose, especial for Internet online games. Using this function you can select "**DMZ**" item and input IP address of DMZ host, then click "**Save**" (show in Figure 4-26). For the purpose of security, we suggested that using "**Virtual server**" instead of "**DMZ**".

4.8.3. UPnP

Choose "**Applications & Games** **UPnP**", you can see the next screen shown below.

Figure 4-40

UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN. Select "**Enable**" to enable this function.

4.8.4. Port Trigger

Choose "**Applications & Games** **Port Trigger**", you can see the next screen shown below.

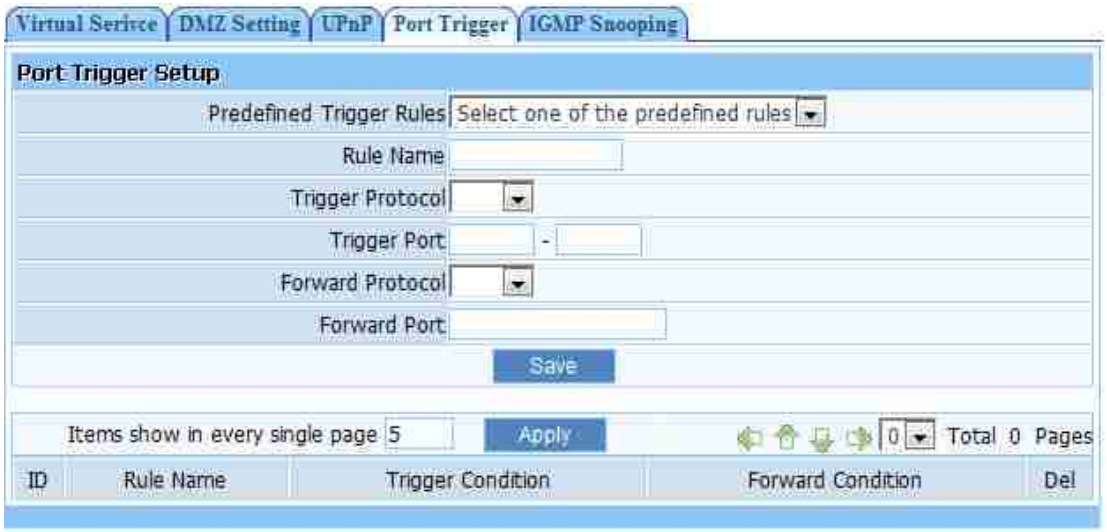


Figure 4-41

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.

➢ .....

Predefined Trigger Rules: Select one of the predefined rules. There are five rules by default.

➢ .....

Trigger Port: The port for outgoing traffic. An outgoing connection using this port will trigger this rule.

➢ .....

Trigger Protocol: The protocol used for Trigger Ports, either TCP, UDP, or All (all protocols supported by the Router).

➢ .....

Forward Port: The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

➢ .....

Forward Protocol: The protocol used for Incoming Ports Range, either TCP or UDP.

To add a new rule, follow the steps below.

1.....

Select a predefined rule from the Predefined Trigger Rules drop-down list, then the Trigger

Port field and the Forward Ports field will be automatically filled. If the Common Applications do not have the application you need, enter the Trigger Port and the Incoming Ports manually.

2.....

Select the protocol used for Trigger Port from the Trigger Protocol drop-down list, either TCP or UDP.

3.....

Select the protocol used for Forward Ports from the Forward Protocol drop-down list, either TCP or UDP.

4.....

Click "**Save**" button to save the new rule.

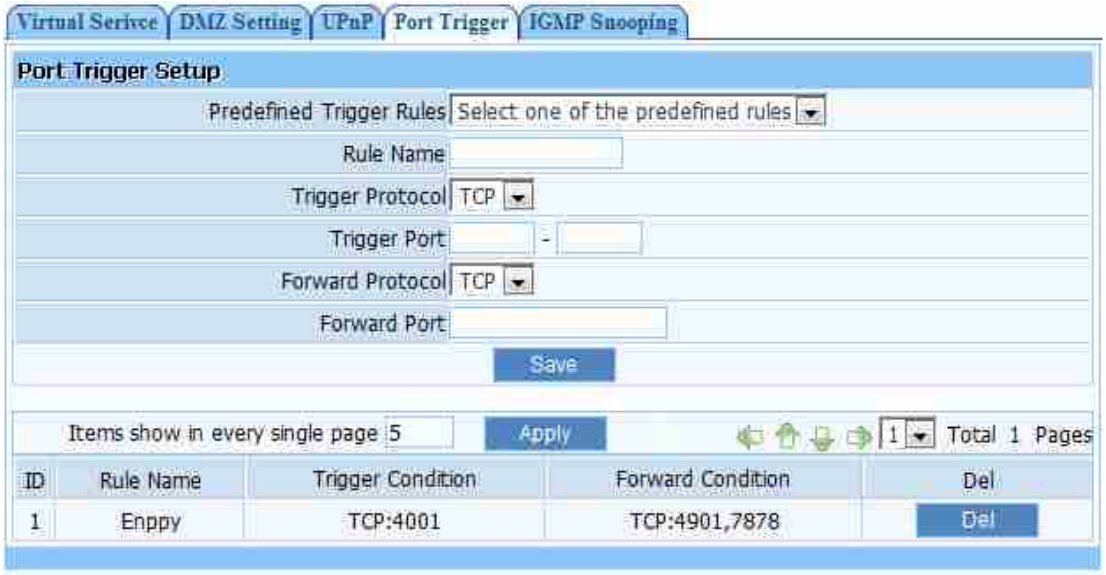


Figure 4-42

4.8.5. IGMP Snooping

Choose menu "**Application & Games→ IGMP Snooping**", you can enable or disable IGMP snooping function in the screen as shown below.

Figure 4-43

- **Status**: IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (IGMP v1) and IGMP v2. Select "Enable" to enable the IGMP Snooping function if you need.

4.9. Applications Gateway

4.9.1. VPN Pass-through

Choose menu "**Applications Gateway→ VPN Pass-through**", you can enable or disable the VPN Pass-through function in the screen as shown below.

Figure 4-44

VPN is commonly used for encapsulate and encrypt data across the public network. For VPN tunnel, the router supports IPSEC pass-through, PPTP pass-through and L2TP pass-through.

➢ .....

PPTP Pass-through: PPTP means the "Point to Point Tunneling Protocol", select "enable" to allow PPTP pass-through the router.

➢ .....

L2TP Pass-through: PPTP means the "Point to Point Tunneling Protocol", select "enable" to allow PPTP pass-through the router.

➢ .....

IPSEC Pass-through: IPSEC (Internet Protocol Security) is a suite of protocols used to implement secure exchange; select "enable" to allow IPSEC pass-through the router.

4.10. DDNS

Choose menu "**DDNS→ DDNS**", you can configure the DDNS function in the screen shown in below.

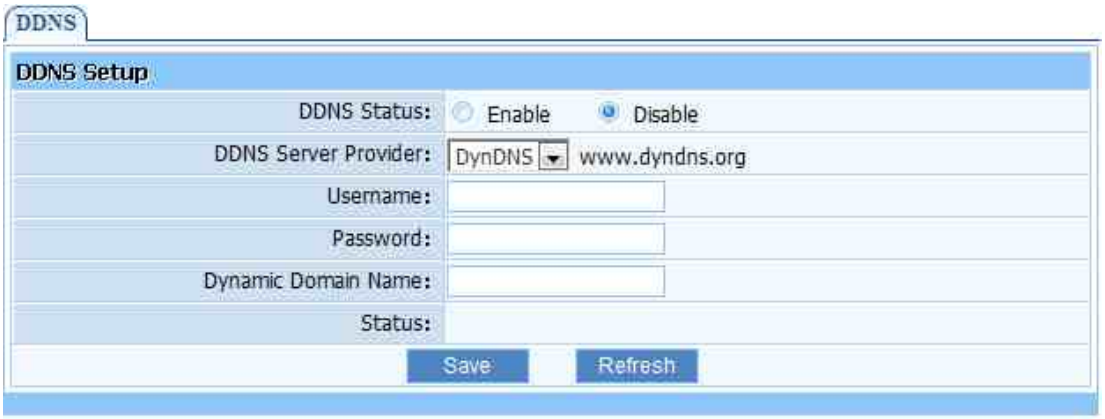


Figure 4-45

The router offers a Dynamic Domain Name System (**DDNS**) feature. The feature lets you use a static host name with a dynamic IP address. User should type the host name, user name and password assigned to your ADSL Router by your Dynamic DNS provider.

➢ .....

DDNS Status: Enable or disable DDNS function.

➢ .....

DDNS Server Provider: For example, if you want to user service of "DynDNS", you have to register an account first. Other DNS service providers as the same.

➢ .....

Username & Password: Type the "User Name" and "Password" for your DDNS account.

➢ .....

Dynamic Domain Name: Enter your DDNS server domain name here.

➢ .....

Status: The status of the DDNS service connection is displayed here.

To set up for DDNS, follow these instructions:

1.....

Enable DDNS function by select the “Enable” marquee.

2.....

Type the User Name for your DDNS account.

3.....

Type the Password for your DDNS account.

4.....

Type the Domain Name received from your dynamic DNS service provider here.

5.....

Click the “Save” button to log in to the DDNS service.

4.11. Routing

Choose "**Routing**" menu, and you will see the routing information in the next screen.

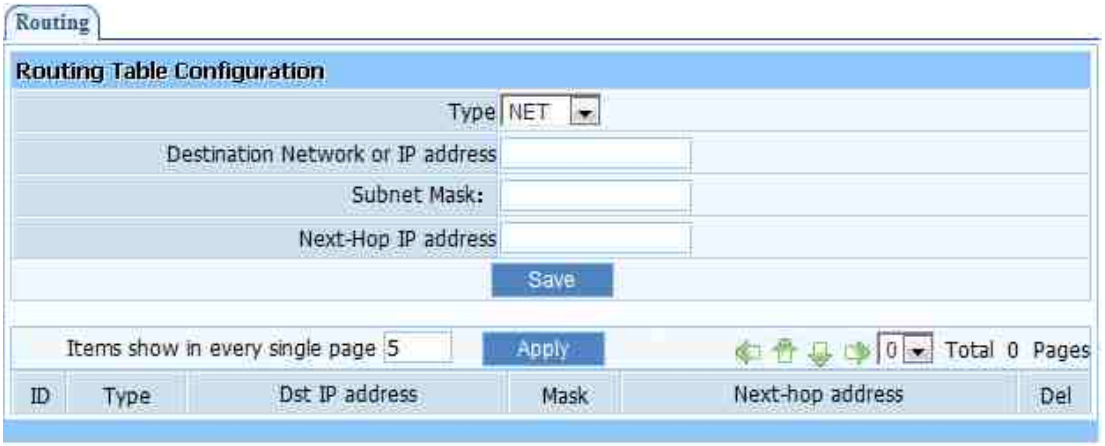


Figure 4-46

Most of broadband router and wireless router are working on NAT mode, so this feature is designed for the most common network environment.

➢ .....

Destination Network or IP Address: Specify a certain destination Network or IP address which static route forward to.

➢ .....

Subnet Mask: Subnet mask is used for distinguishing an IP address between Network portion and Host portion.

➢ .....

The Next-hop IP Address: This is an IP address of the next-hop device (and also is the gateway address for local host) that allows forwarding data between router and remote network or host.

➢ .....

Routing Table: You can check out all current route items, click "**Del**" button to delete a route item existed in routing table.

4.12. Advanced Setup

Choose "**Advanced Setup**" menu, and you will see the submenus. (Show in Figure 4-47)

Figure 4-47

4.12.1. SNMP Protocol Configuration

Choose menu "**Advanced Setup→ SNMP Protocol Configuration**" and you will see the SNMP Protocol Configuration in the next screen show in below.

Figure 4-48

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap IP address, community name, etc.

4.12.2. Remote Access

Choose menu "**Advanced Setup→ Remote Access**" and you will see the Remote Access in the next screen show in below. This feature allows you to manage your Router from a remote location via the Internet.

Figure 4-49

This page is used to enable/disable management services for the LAN and WAN. Select these services according to actual needs.

4.12.3. TR-069 Configuration

Choose menu "**Advanced Setup→ TR-069 Configuration**", you can configure the TR-069 function in the screen as shown in below.

Figure 4-50

TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server). This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

- **Status**: Select "Enable" the TR-069 function.
- **URL**: Enter the website of ACS which is provided by your ISP.
- **User Name/Password**: Enter the User Name and password to login the ACS server.
- **Periodic Inform**: Activate or deactivate the function. If Activated, the information will be informed to ACS server periodically.
- **Periodic Inform Interval**: Enter the interval time here.
- **Path**: Enter the path that connects to the ACS server.

- **Port**: Enter the port that connects to the ACS server.
- **User Name/Password**: Enter the User Name and Password that provided the ACS server to login the router.

4.13. System Management

Choose menu "**System Management**", and you will see the next submenus.

Figure 4-51

4.13.1. Password Setup

Choose menu "**System Management→ Password Setup**", you can set new password for admin in the screen.

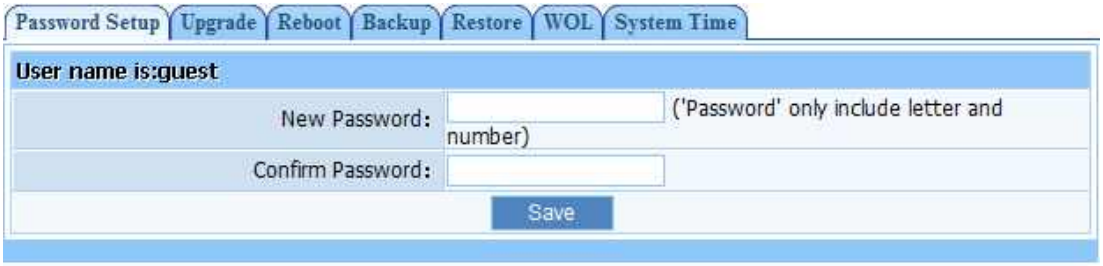


Figure 4-52

The default username/password is guest/guest. To ensure the Router's security, we strongly recommend you to change the default password. Enter a new password and confirm your new password, then click "Save" button to save settings.

4.13.2. Upgrade

Choose menu "**System Management→ Upgrade**", you can upgrade firmware in the screen.

Figure 4-53

Click "Browse..."button and select a File to upgrade. After you have selected the appropriate file, click "**Upgrade**" button to execute upgrade procedure. Do not cut off the power supply during the process of upgrading.

4.13.3. Reboot

Choose menu "**System Management→ Reboot**", click "**Restart**" button to restart the router.

Figure 4-54

4.13.4. Backup

Choose menu "**System Management→ Backup**" and you will see the next screen show in below.

Figure 4-55

This page allows you to backup current settings to a file by click the "Backup" button. Or restore the settings from the file which was saved previously.

4.13.5. Restore

Choose menu "**System Management→ Restore**" and you will see the next screen show in below.

Figure 4-56

Click "**Restore**" button, the Router will erase all of your settings and replace them with the factory defaults, make sure you have backup current settings before click this button.

4.13.6. WOL (Wake-up On LAN)

Choose menu "**System Management→ WOL**" and you will see the next screen show in below.

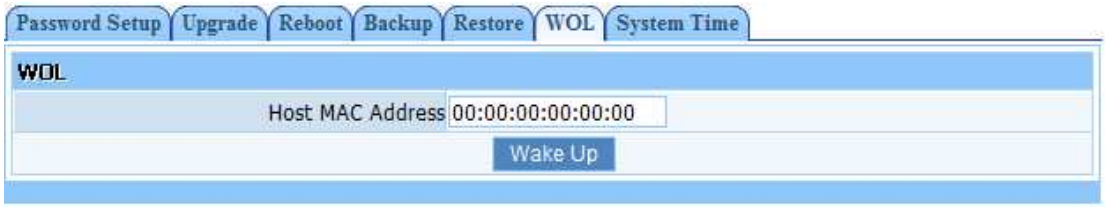


Figure 4-57

Enter host MAC address, and then click button of "**Wake up**" to wake up the target host which in the LAN.

Note:

This function in computer motherboard and NIC all have special requirements, if your PC's motherboard and NIC do not support sensei function, please don't use this function.

4.13.7. System Time

Choose menu "**System Management→ System Time**" and you will see the next screen show in below.

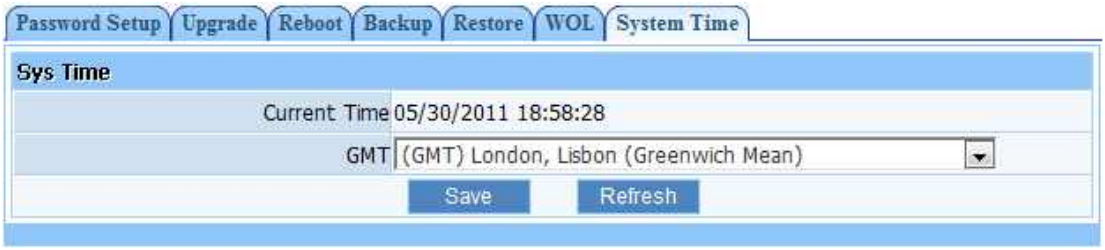


Figure 4-58

The system time is the time used by the device for scheduling services. Chose the time zone for you need.

5. Appendix

5.1. Wireless Network

To set up a wireless network between your computer and your product, please make sure the wireless adapter in your computer is available.

➢ .....

The configuration For Windows 2000 or Windows XP as below

Step 1: Click the "**Wireless Management**". Enable the wireless network as below.

Figure 5-1

Step 2: Click the "**Security**" label and select one authentication type in the drop-down menu. Set the "Encryption Type", "Key Mode", "Key" and "Key Renewal" as your wish but remember what you stetted.

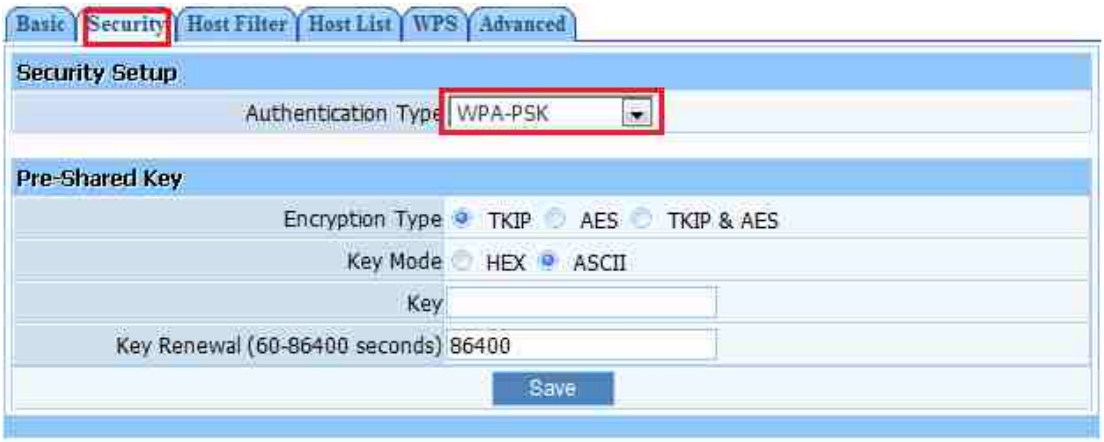


Figure 5-2

Step 3: Click "My Network Places" with the right button of your mouse. Then select "**Properties**".

Figure 5-3

Step 4: Click "**Wireless Network Connection**" with the right button of your mouse. Then select "**View Available Wireless Networks**".

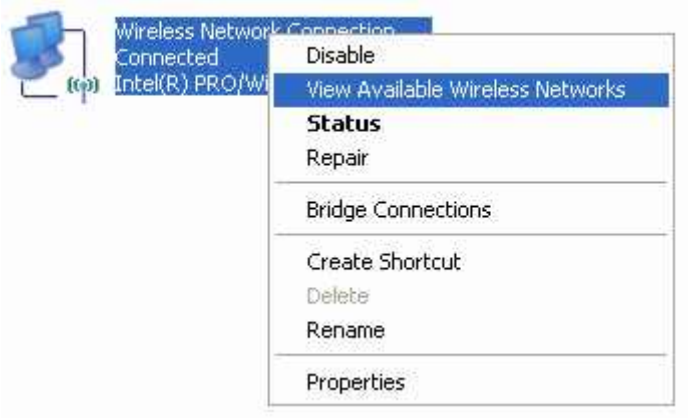


Figure 5-4

Step 5: Double click the wireless network your product provided.

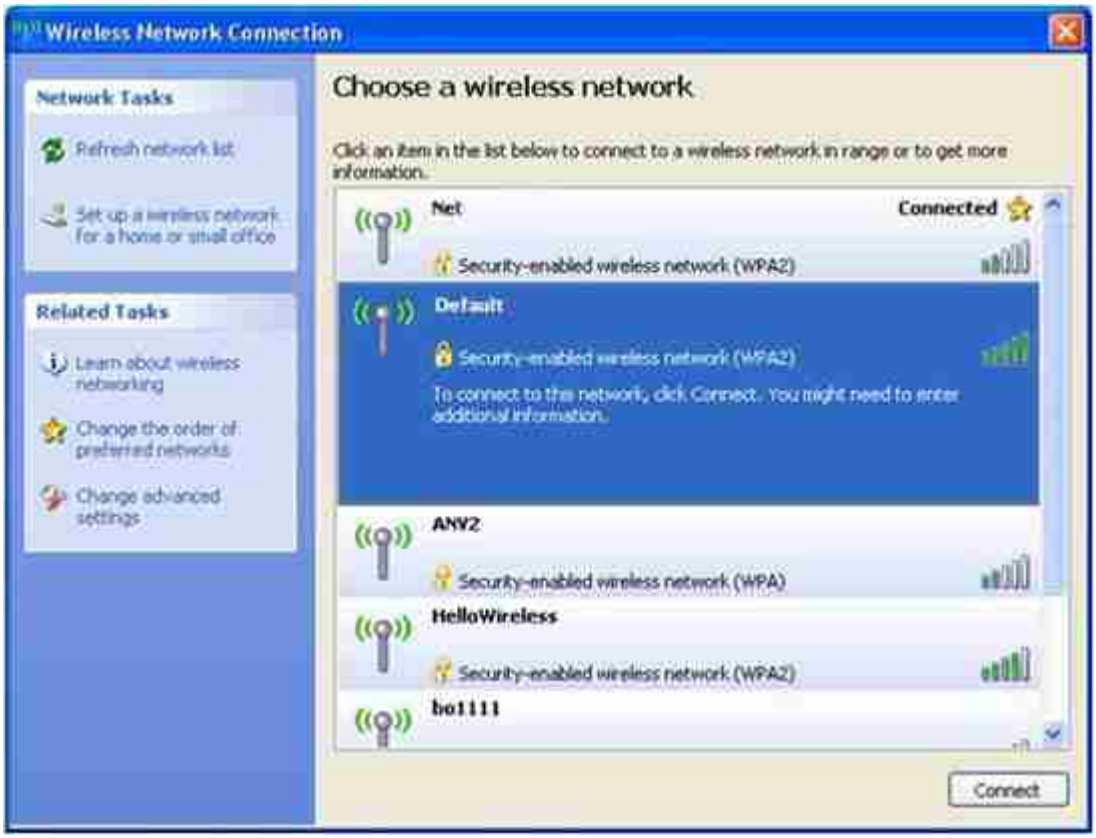


Figure 5-5

Step 6: Input the key you stetted before if the wireless network you connecting to requests password.

Figure 5-6

➢ .....

The configuration For Windows 7 or Windows Vista as below

Step 1 & **Step 2** refer to the configuration For Windows 2000 or Windows XP.

Step 3: Click  , then select the "Open Network and Sharing Center".

Figure 5-7

Step 4: Click the SSID of your wireless network and then press the "Connect" button as below.

Figure 5-8

Step 5: Input the key you stetted before if the wireless network you connecting to requests password.

Figure 5-9

5.2. WPS Detailed Configuration

5.2.1. Method A

- First, holds down the router's WPS button for 3 seconds or push the "**PBC**" button of the wireless NIC client (show in figure 5-10).

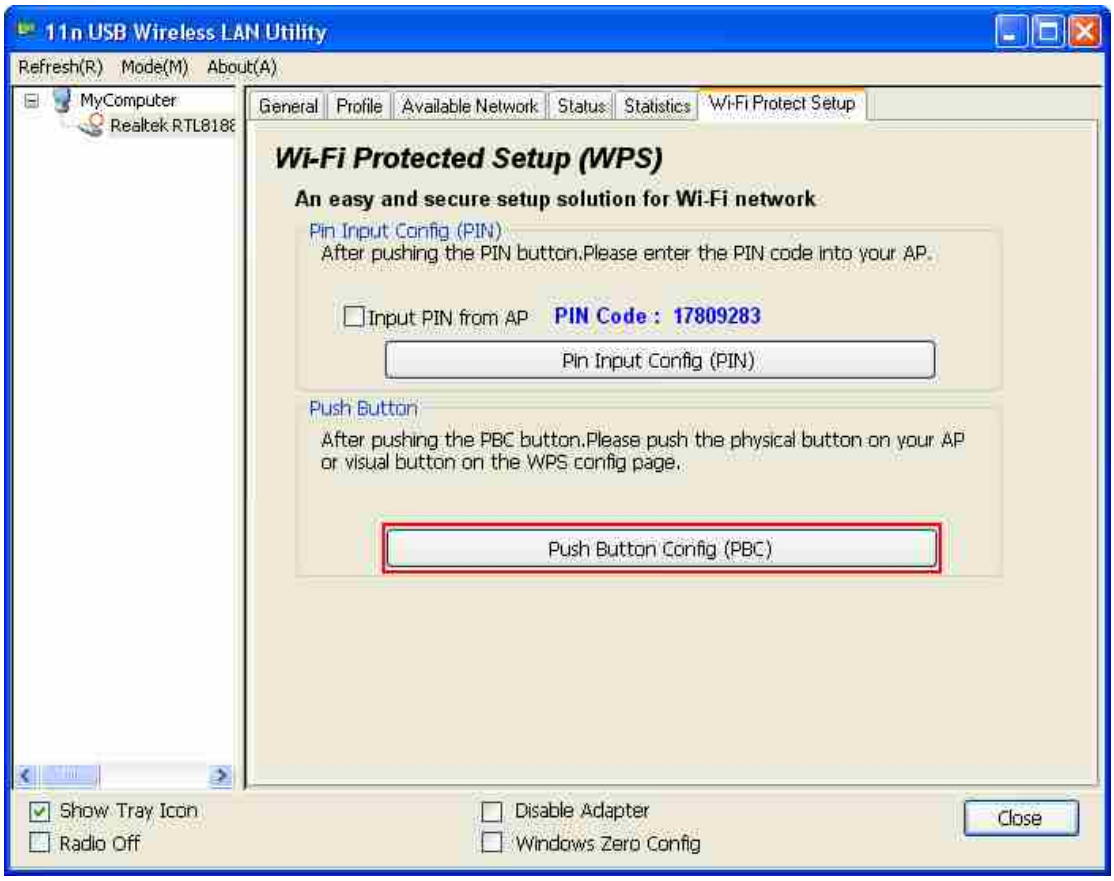


Figure 5-10

➢ .....

Then the following window will appear.

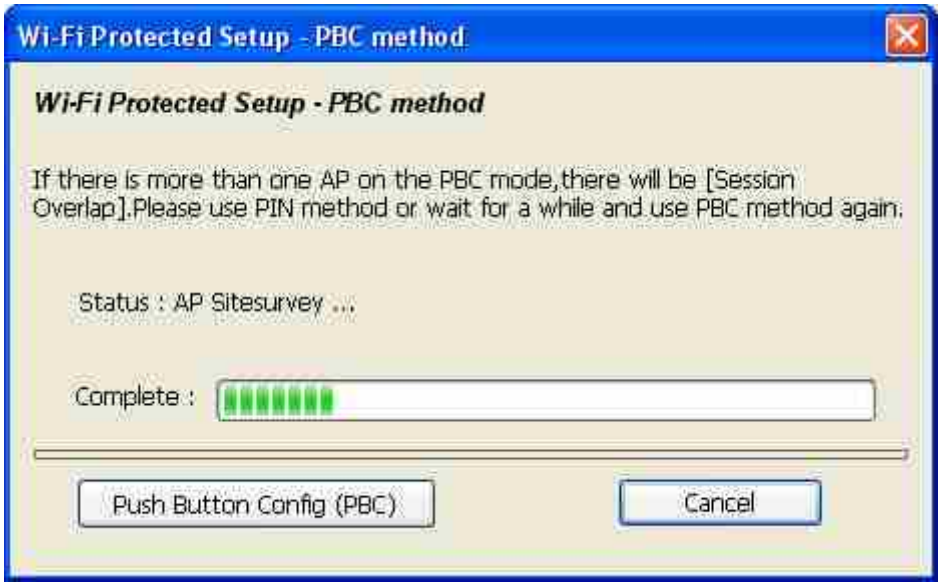


Figure 5-11

➢ Next, holds down the router's WPS button for 3 seconds or push the PBC button "**Connect**" in the webpage.

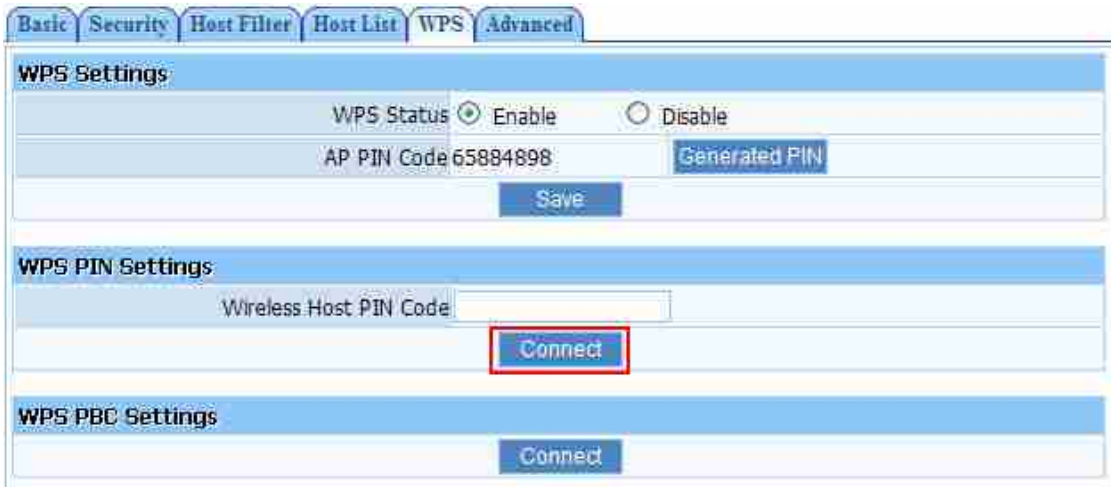


Figure 5-12

➢ Wait tens of seconds, a successful connection screen will displayed.

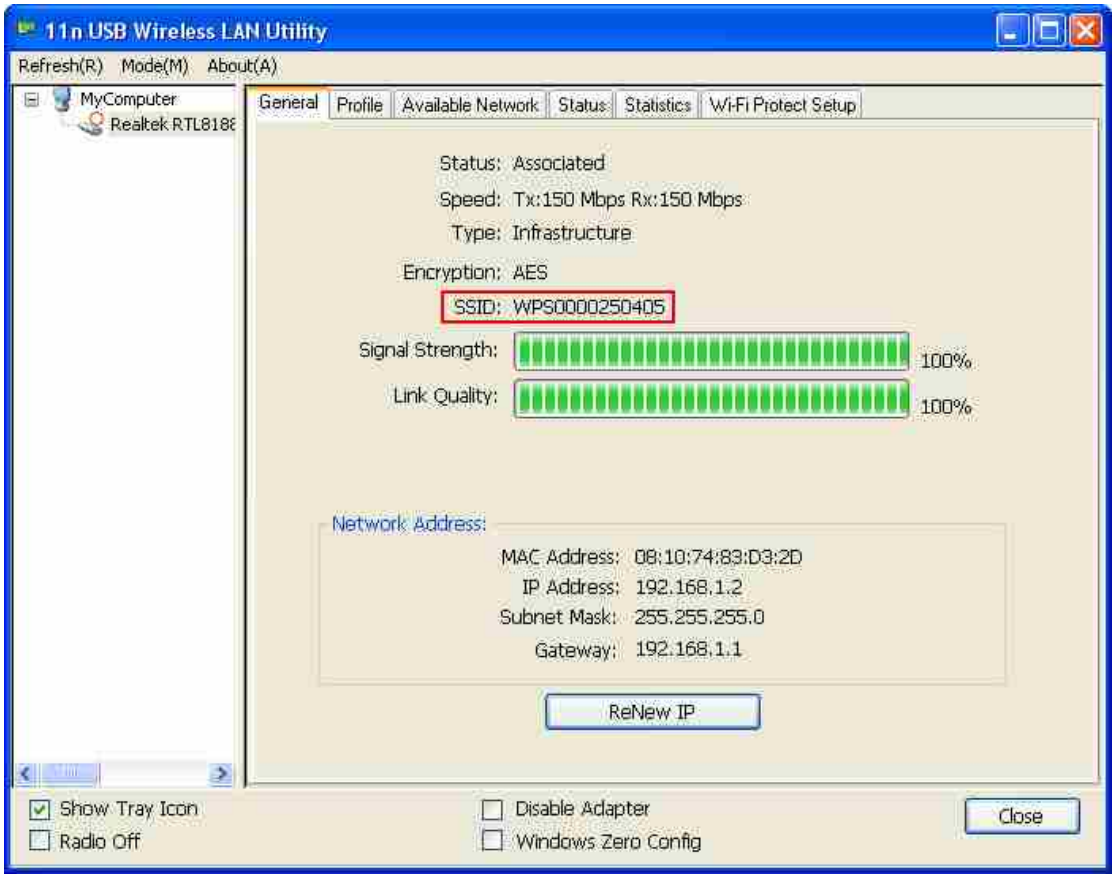


Figure 5-13

➢ .....

If the SSID in the wireless card client (show in figure 5-14) and the SSID in the webpage (show in figure 5-13) are the same. Then can determine the WPS has connected successful.

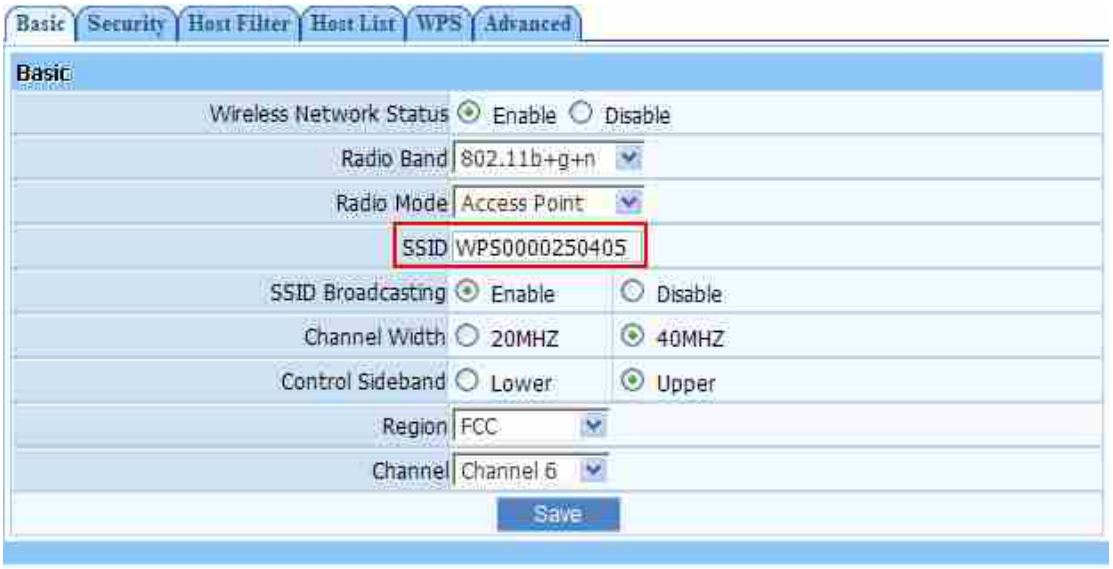


Figure 5-14

5.2.2. Method B

➢ First, click the "**Pin Input Config**" button as shown below.

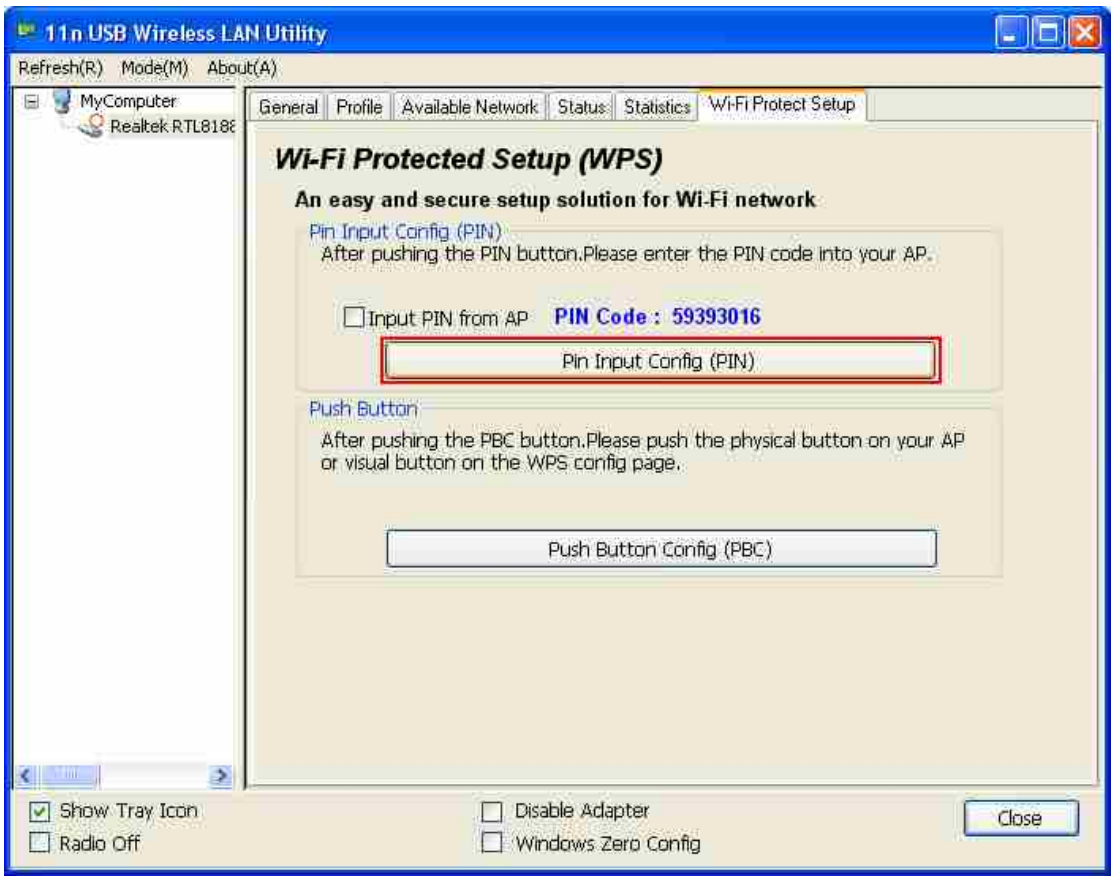


Figure 5-15

➢ Click "**Yes**" to continue.

Figure 5-16

- Then select the WPS AP Name (Here is RTL867x-ADSL).

Figure 5-17

- Then the following window will appear.

Figure 5-18

- Enter wireless NIC client auto-generated PIN Code "**59393016**", then click the "**Connect**"

button (show in Figure 5-18 and Figure 5-19).

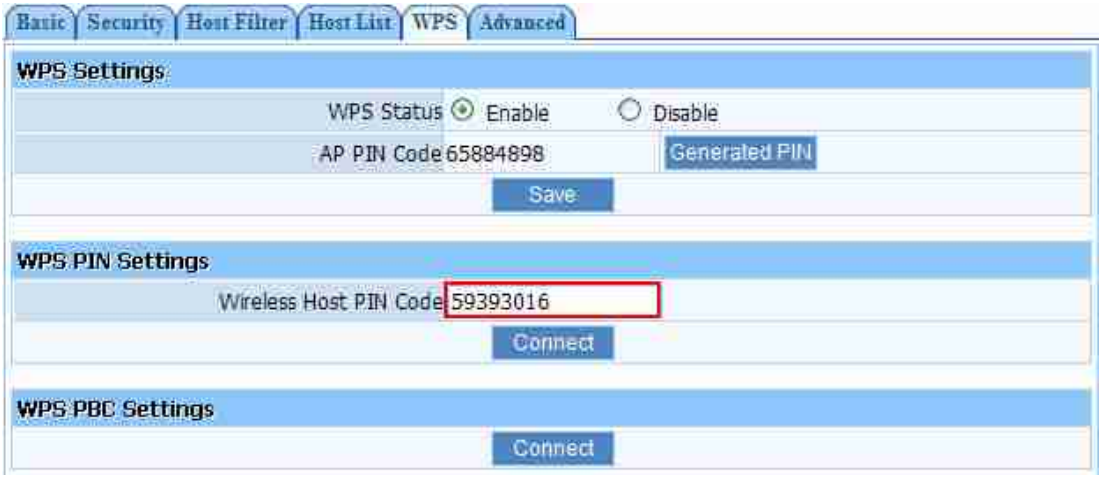


Figure 5-19

- Then will begin to automatic connection, appear as follows，the interface means connection succeeded.

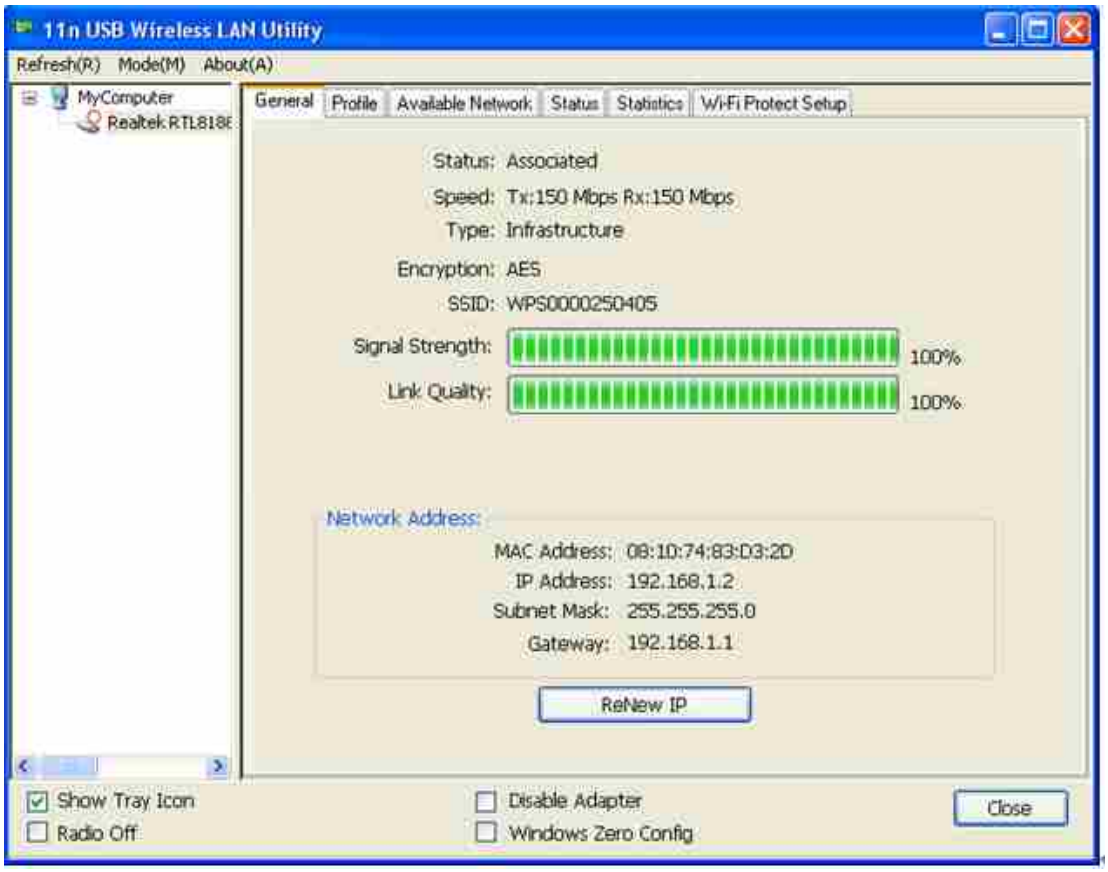


Figure 5-20

5.2.3. Method C

- Click the “**Generated PIN**” button as shown below.

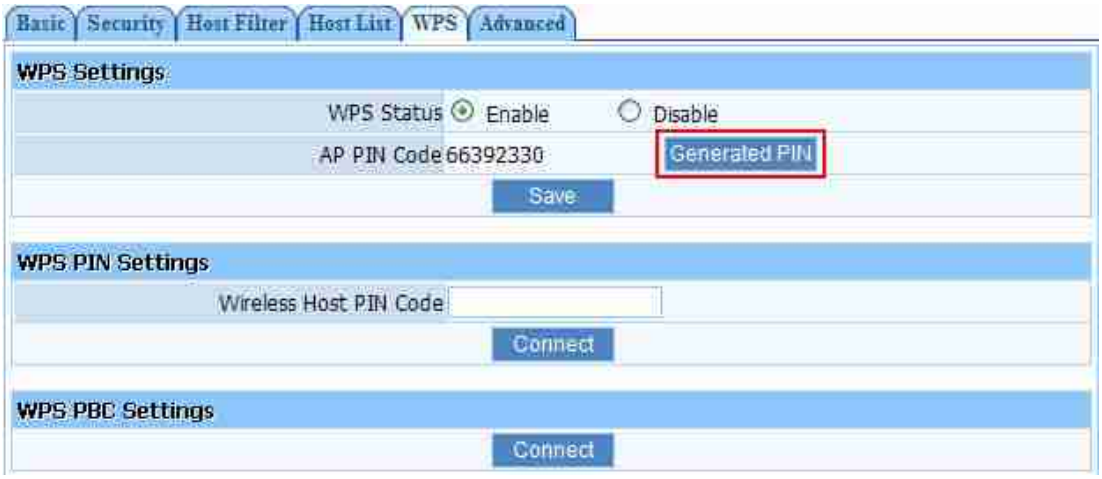


Figure 5-21

- Click "**OK**" button to make change effectively.

Figure 5-23

- Check the "**Input PIN from AP**" button, and enter the regenerate PIN: 65884898 . Then click the "**PIN Input Config**" button as shown below.

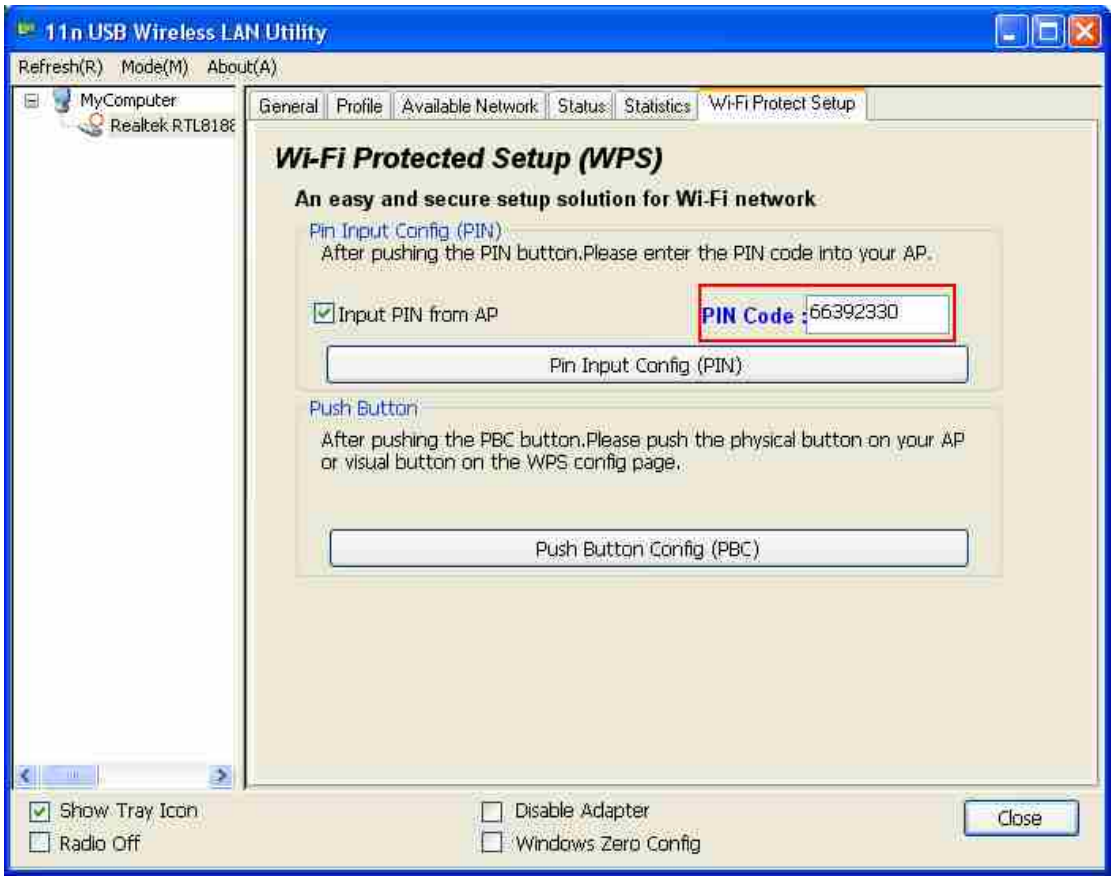


Figure 5-24

- Select the WPS AP Name (Here is RTL867x-ADSL).

Figure 5-25

- Then will begin to automatic connection, appear as follows the interface means connection succeeded.

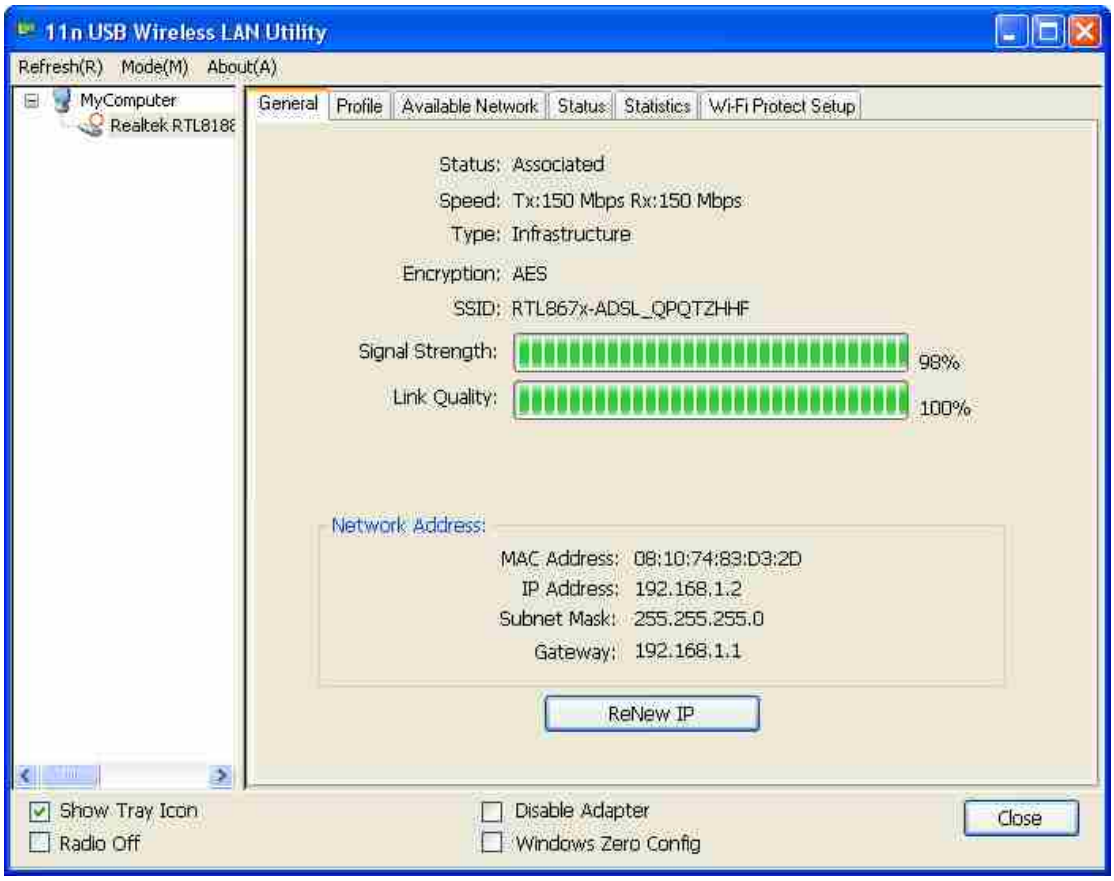


Figure 5-26

5.3. FAQ

5.3.1. How to restore the default parameter of the modem

A) Hard Reset

➢ .....

Keep the modem power on with electricity, push the default button with ball-point pen or toothpick for 10 seconds, the default parameter will be restored after about 3 minutes .But the configuration before will be lost. So you need to reset it again.

Figure 5-27

B) Soft Reset

➢ Firstly, log in the modem configuration interface, click the "**System Management Restore**" in order, then click the "**Restore**" as showed below.

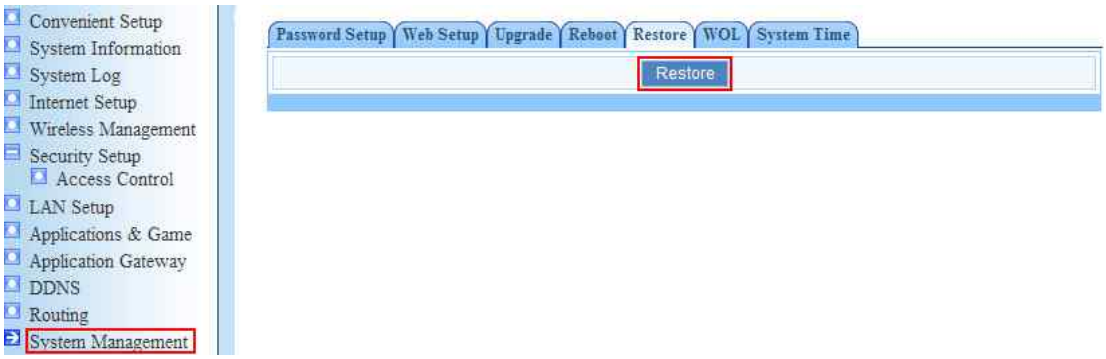


Figure 5-28

➢ .....

The interface below will appear, click "**OK**".

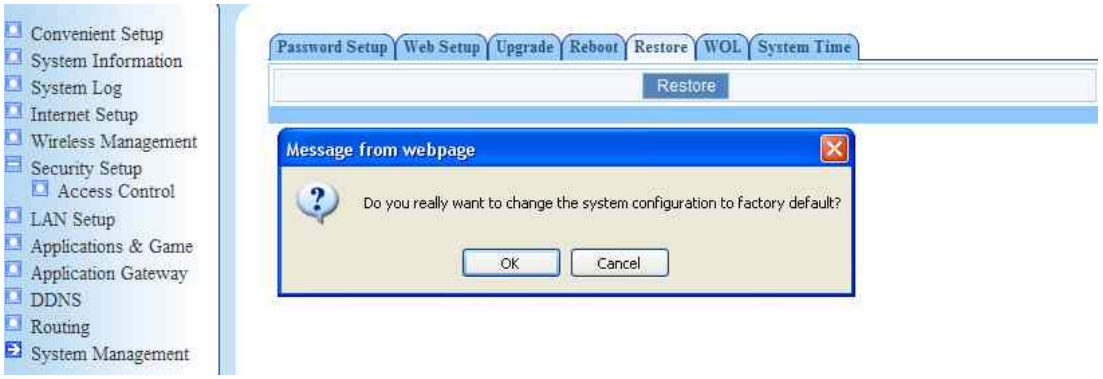


Figure 5-29

➢ .....

The interface below will appear, wait for 3 minutes, then the modem will enter the configuration interface automatically.

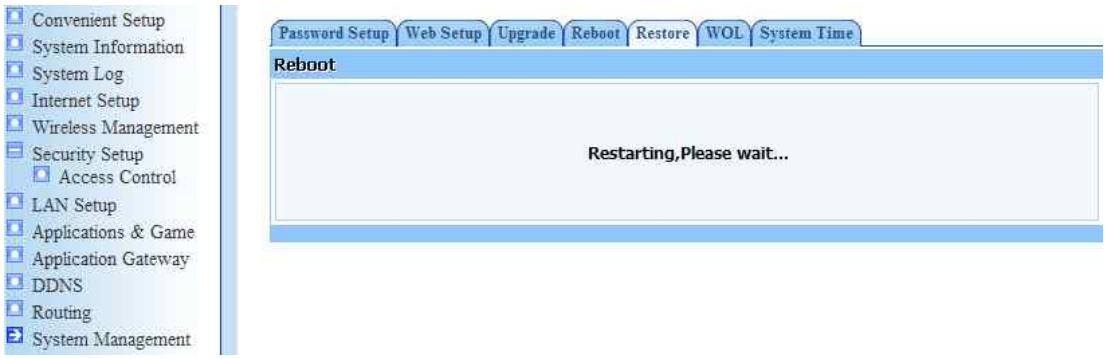


Figure 5-30

5.3.2. How to upgrade the modem

➢ .....

Firstly log in the configuration interface, then click the "**System Management Upgrade Browse**" in order as showed below.

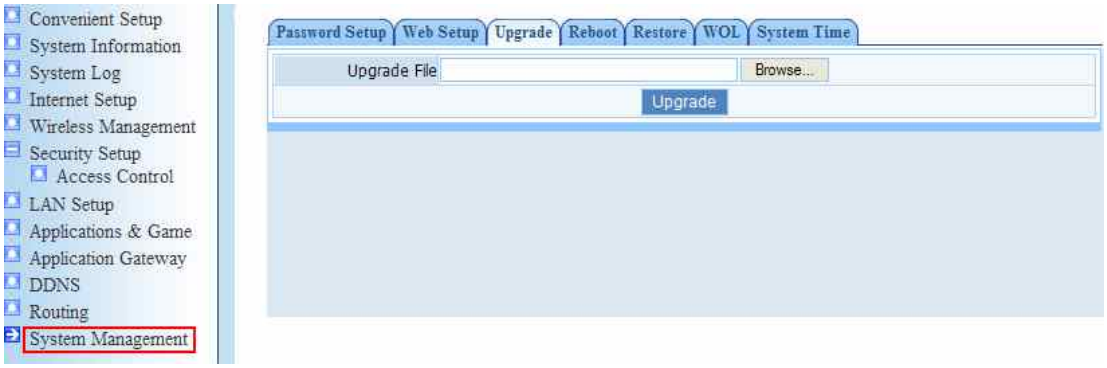


Figure 5-31

➢ .....

Select the upgrade firmware in the dialog appeared, then click the "**Open**" button to use it as showed below.

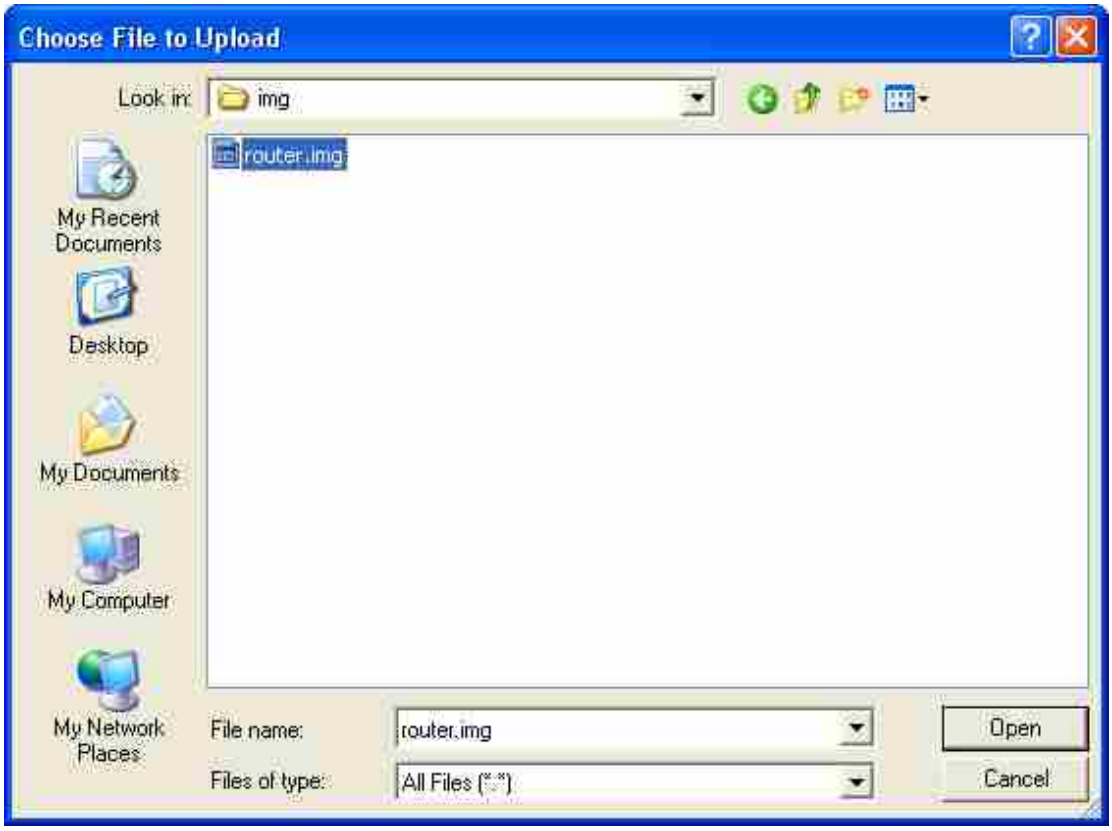


Figure 5-32

➢ .....

Then click "**Upgrade** **OK**" in order as showed below.

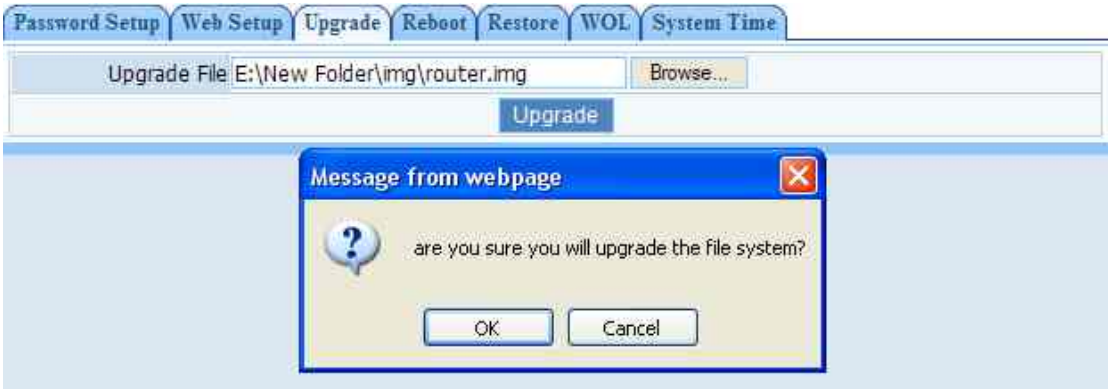


Figure 5-33

➢ .....

Then the modem begin to upgrade as showed below, wait for 3 minutes, it will enter the management interface automatically.

5.3.3. How to connect the modem after setting WLAN password

➢ .....

Firstly set password as showed below, remember to click "**Save**".

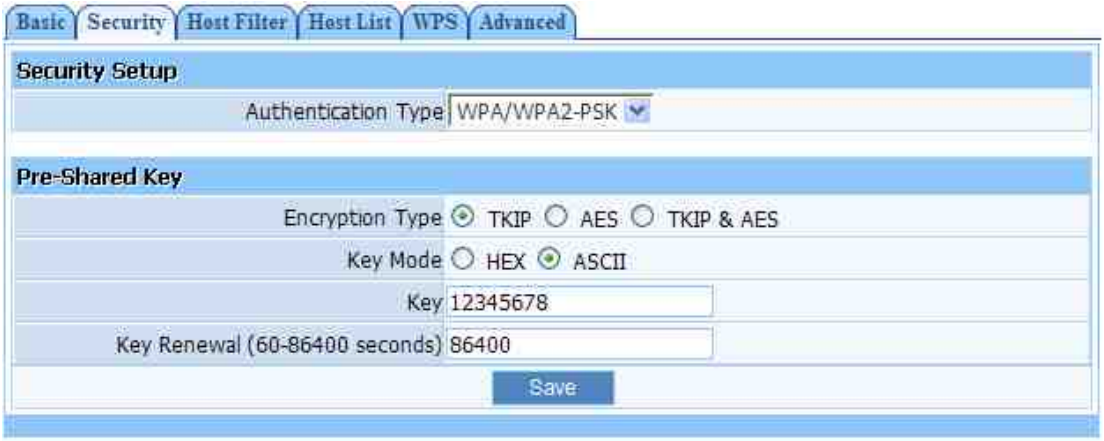


Figure 5-34

➢ .....

Then click the icon 

on desktop (here take the product WF-2403 as an example), the interface showed below will appear. Choose "**Available Network**".

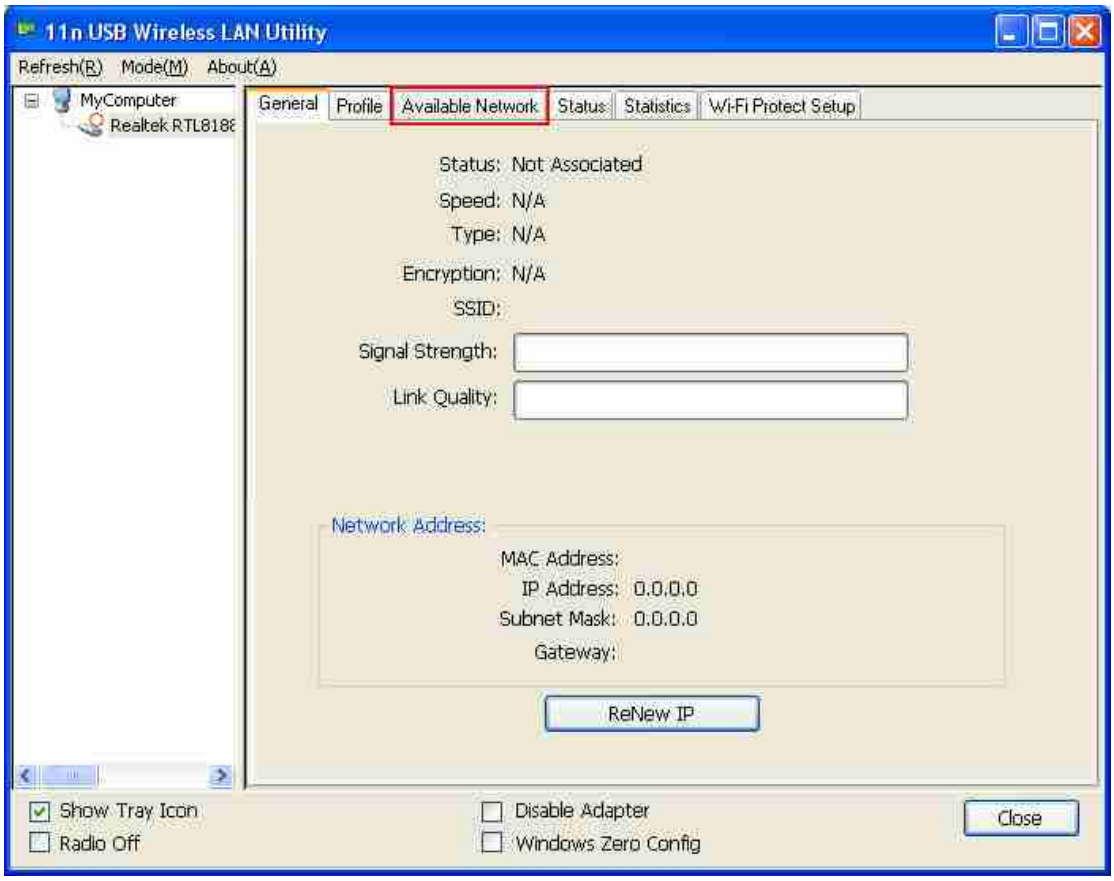


Figure 5-35

➢ .....

The interface showed below will appear. Then choose the SSID (it's "Default" here) as showed below.

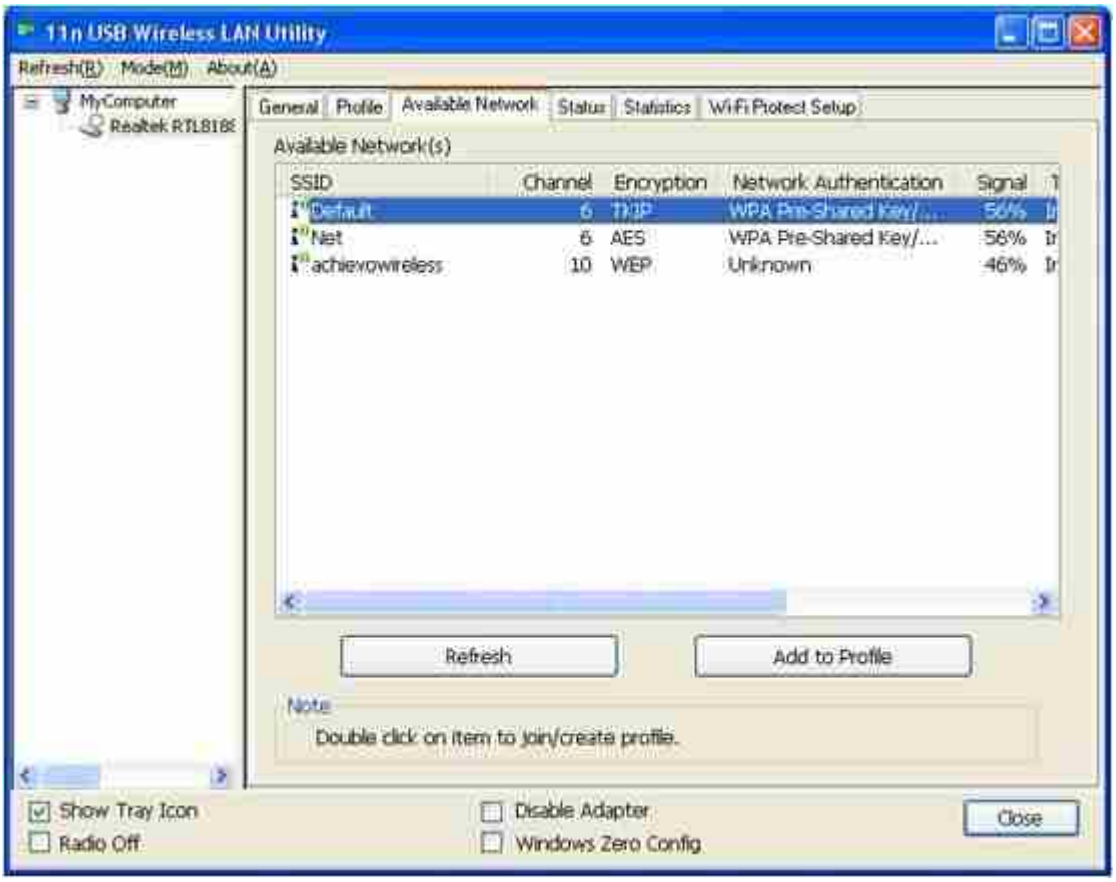


Figure 5-36

➢ .....

Double-click "**Default**", the interface showed below will appear (show in figure 5-36), then enter the WLAN password (It's 12345678 here) as showed below.

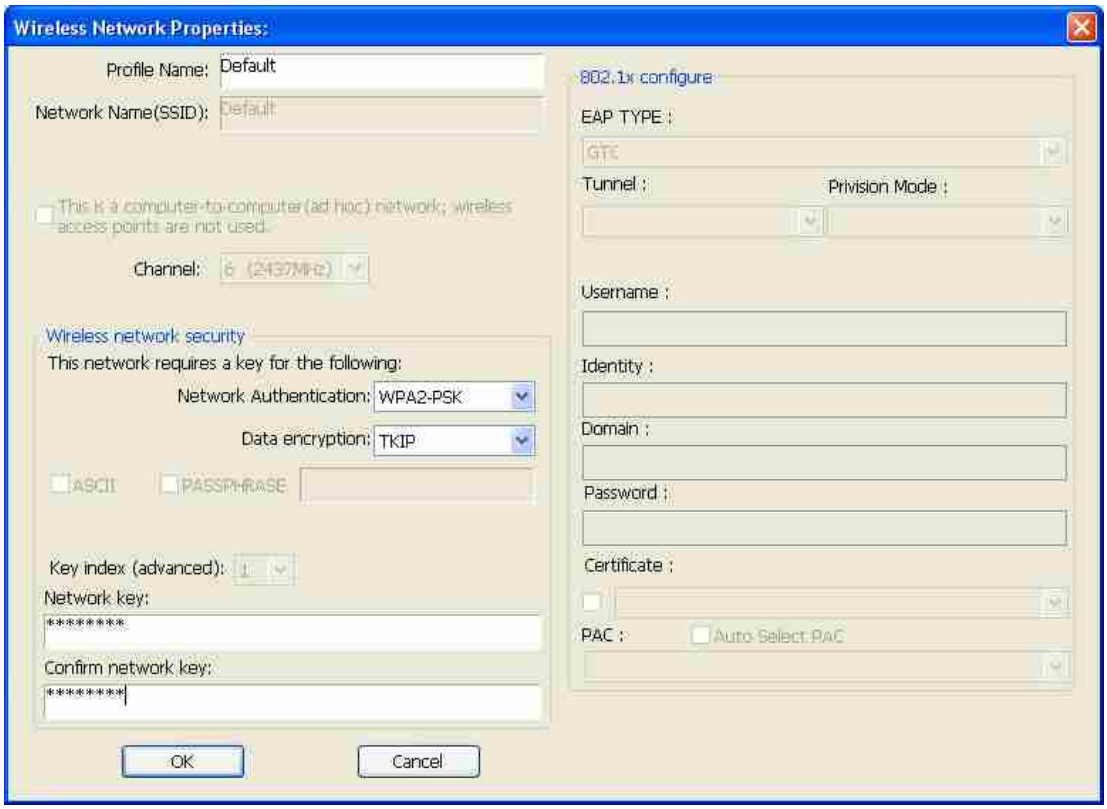


Figure 5-37

➢ Click "**OK**" and wait for several minutes (show in figure 5-37), you will see the interface showed below which means successful connection.

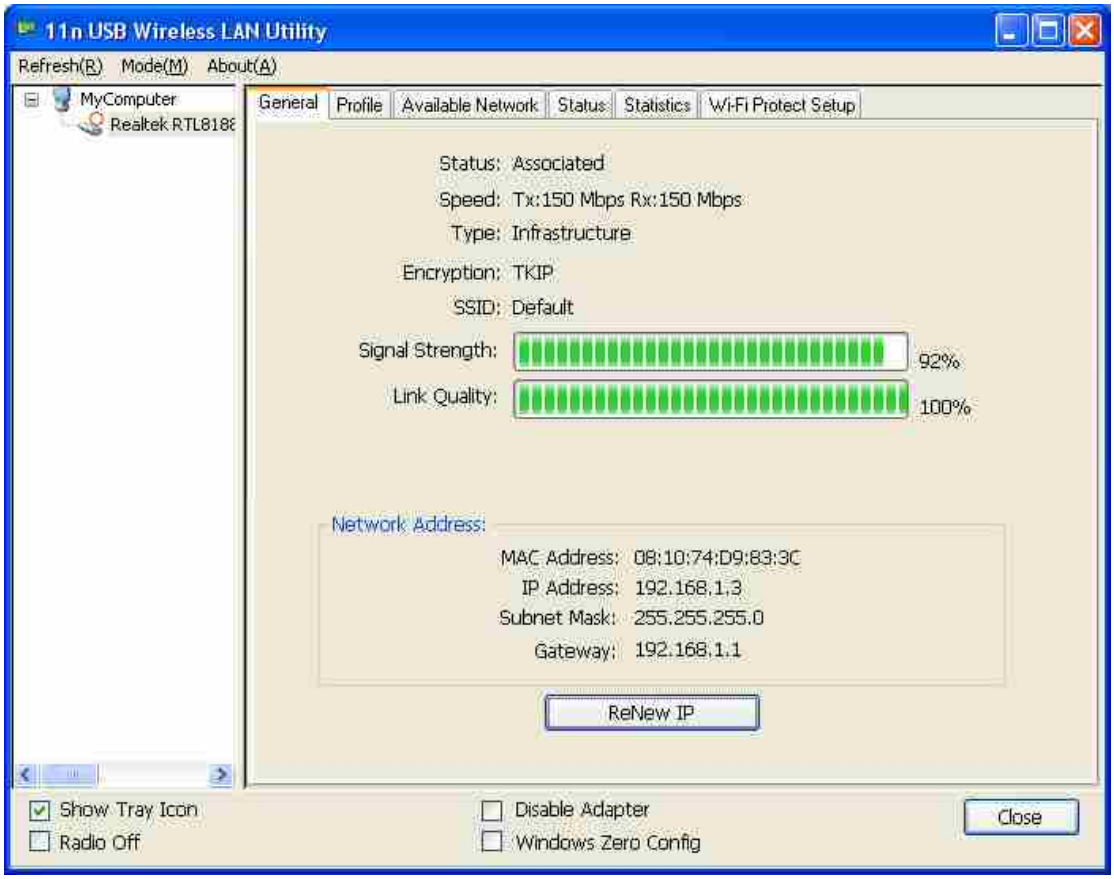


Figure 5-38

➢ .....

Note: Similarly, when use the computer's client itself to connect, just input the password when connecting.

5.4. Specifications

General	
Standards and Protocols	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.3, IEEE 802.3u, IEEE 802.1q, IGMP, SNMP, TR-069, TCP/IP, PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Safety & Emission	FCC、CE
Ports	Four 10/100M Auto-Negotiation RJ45 ports（Auto MDI/MDIX) One RJ11 port
LEDs	Power, ADSL, Internet, WLAN, 1,2,3,4(LAN), WPS
Network Medium	10Base-T: UTP category 3, 4, 5 cable 100Base-TX: UTP category-5 Max line length: 6.5Km

Data Rates	Downstream: Up to 24Mbps Upstream: Up to 1Mbps
System Requirement	Internet Explorer 5.0 or later, Win 9x/ ME/ 2000/ XP/ Vista/Windows 7
Physical and Environment	
Working Temperature	0℃ ~ 40℃
Working Humidity	10% ~ 90% RH (non-condensing)
Storage Temperature	-40℃ ~ 70℃
Storage Humidity	5% ~ 90% RH (non-condensing)