DrayTek

VigorAP 800

802.11n Access Point

Your reliable networking solutions partner

User's Guide

V1.0

VigorAP 800
Wireless Access Point
User's Guide

Version: 1.0

Firmware Version: V1.0.0RC5

Date: 15/04/2010

Copyright Information

Copyright Declarations

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the modem.
- The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself.
- Do not place the modem in a damp or humid place, e.g. a bathroom.
- The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the modem, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor modem via http://www.draytek.com.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: VigorAP 800

DrayTek Corp. declares that VigorAP 800 is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class B and EN55024/Class B.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN60950-1.

Federal Communication Commission Interference Statement

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

(1) This device may not cause harmful interference, and

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

This product is designed for 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

FCC RF Radiation Exposure Statement

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

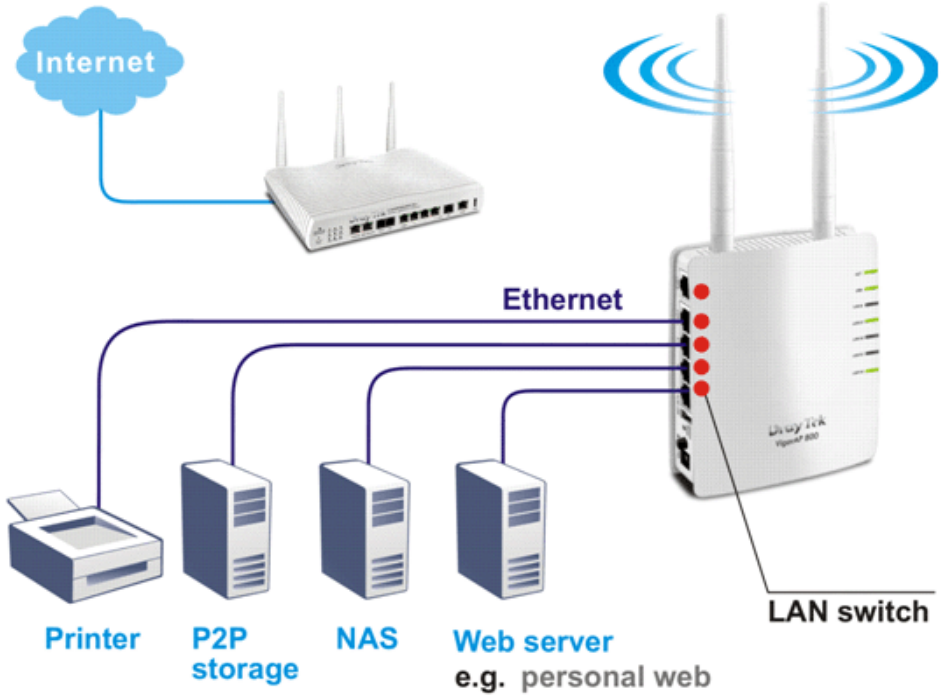
Table of Contents

1 Preface

1.1 Introduction

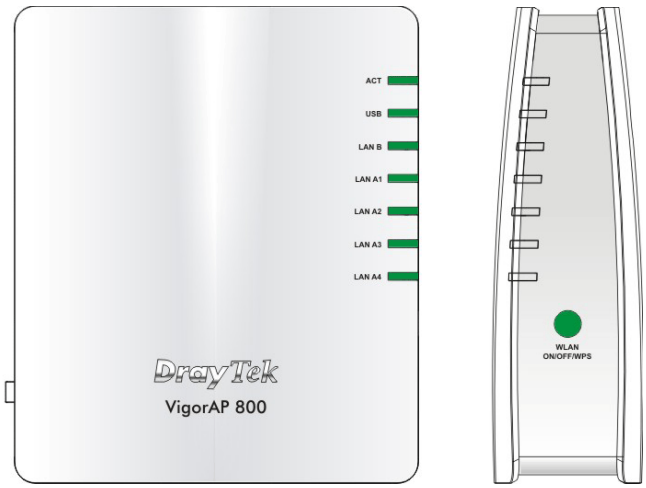
Thank you for purchasing this VigorAP 800! With this high cost-efficiency VigorAP 800, computers and wireless devices which are compatible with 802.11n can connect to existing wired Ethernet network via this VigorAP 800, at the speed of 300Mbps.

Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced users. Just follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

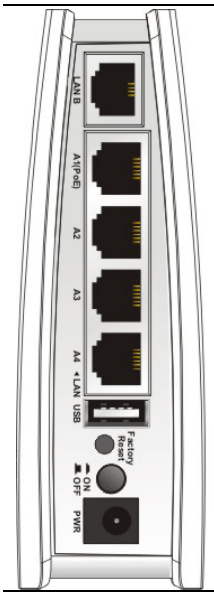


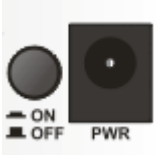
1.2 LED Indicators and Connectors

Before you use the Vigor modem, please get acquainted with the LED indicators and connectors first.



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
LAN B	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
LAN A1 - A4	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
WLAN (Green LED) on WLAN button	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
WPS (Orange LED) on WLAN button	Off	The WPS is off.
	Blinking (Orange)	Blink with 1 second cycle for 2 minutes - - WPS is enabled and waiting for wireless client to connect with it.
	Blinking (Orange)	Data is transmitting (sending/receiving).
WPS Button	Press this button for 2 seconds to wait for client device making network connection through WPS. When the orange LED lights up, the WPS will be on.	



Interface	Description
LAN B	Connecter for xDSL / Cable modem or router.
LAN A1 (PoE) - A4	Connecter for xDSL / Cable modem or router.
USB	Connector for future use.
	Restore the default settings. Usage: Turn on VigorAP 800. Press the button and keep for more than 10 seconds. Then VigorAP 800 will restart with the factory default configuration.
	ON/OFF: Power switch. PWR: Connecter for a power adapter.

1.3 Hardware Installation

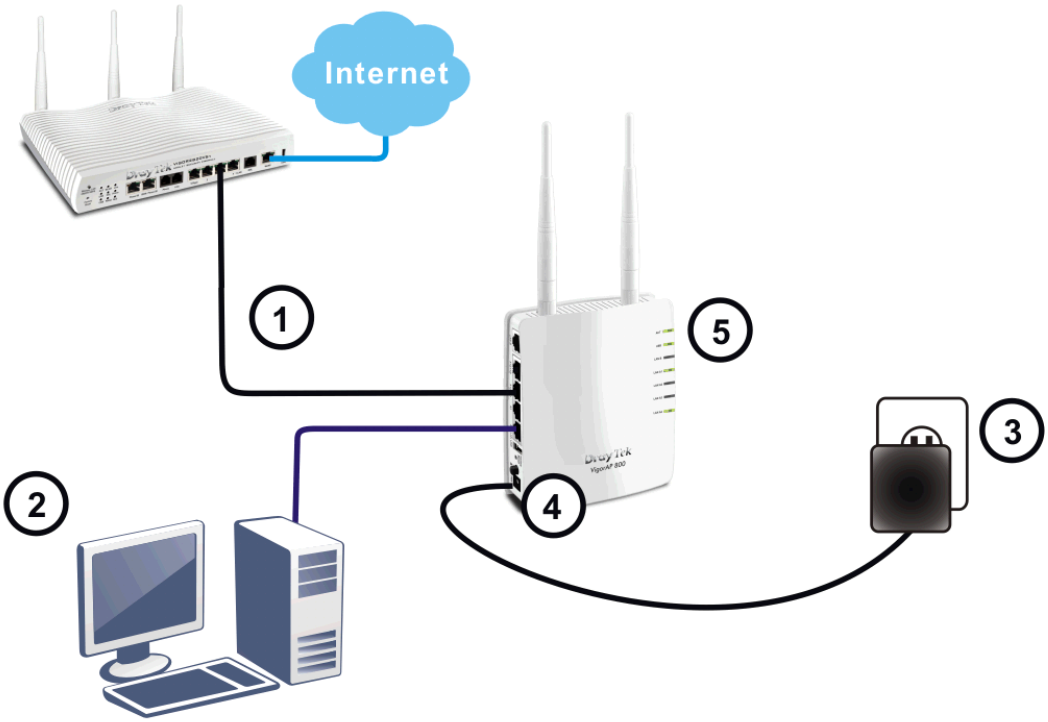
This section will guide you to install the modem through hardware connection and configure the modem's settings through web browser.

Before starting to configure the modem, you have to connect your devices correctly.

1.3.1 Wired Connection for PC in LAN

1. Connect VigorAP 800 to ADSL modem, router, or switch/hub in your network through the **LAN A** port of the access point by Ethernet cable.
2. Connect a computer to other available LAN A port. Make sure the subnet IP address of the PC is the same as VigorAP 800 management IP, e.g., **192.168.1.X**.
3. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.
4. Power on VigorAP 800.
5. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem or router.

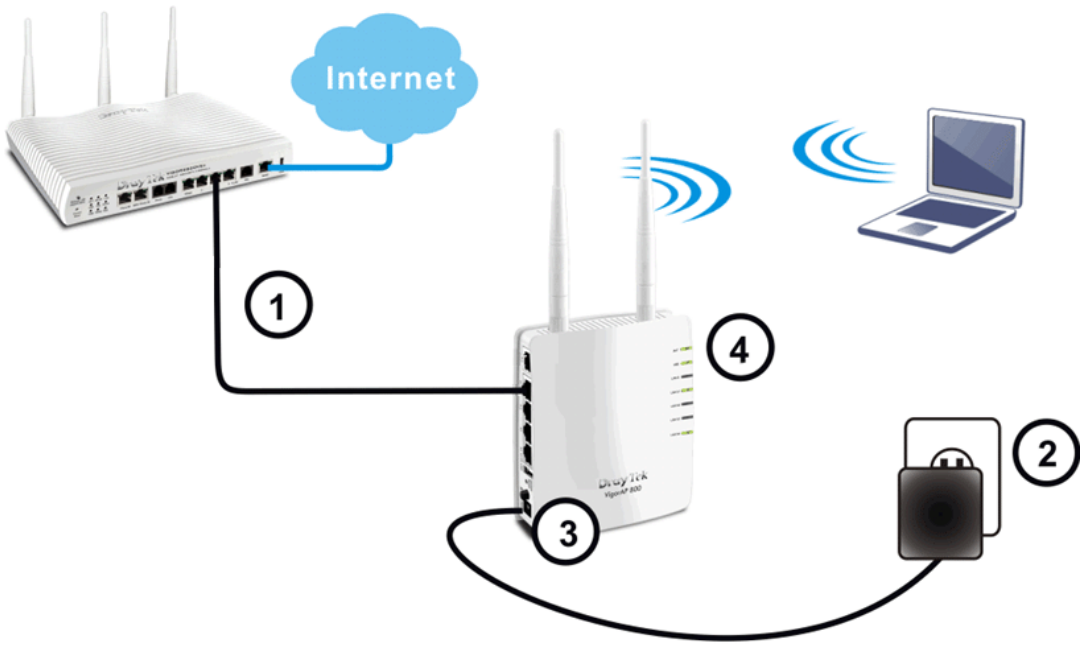
(For the detailed information of LED status, please refer to section 1.2.)



1.3.2 Wired Connection for Notebook in WLAN

1. Connect VigorAP 800 to ADSL modem or router in your network through the **LAN A** port of the access point by Ethernet cable.
2. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.
3. Power on VigorAP 800.
4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem or router.

(For the detailed information of LED status, please refer to section 1.2.)

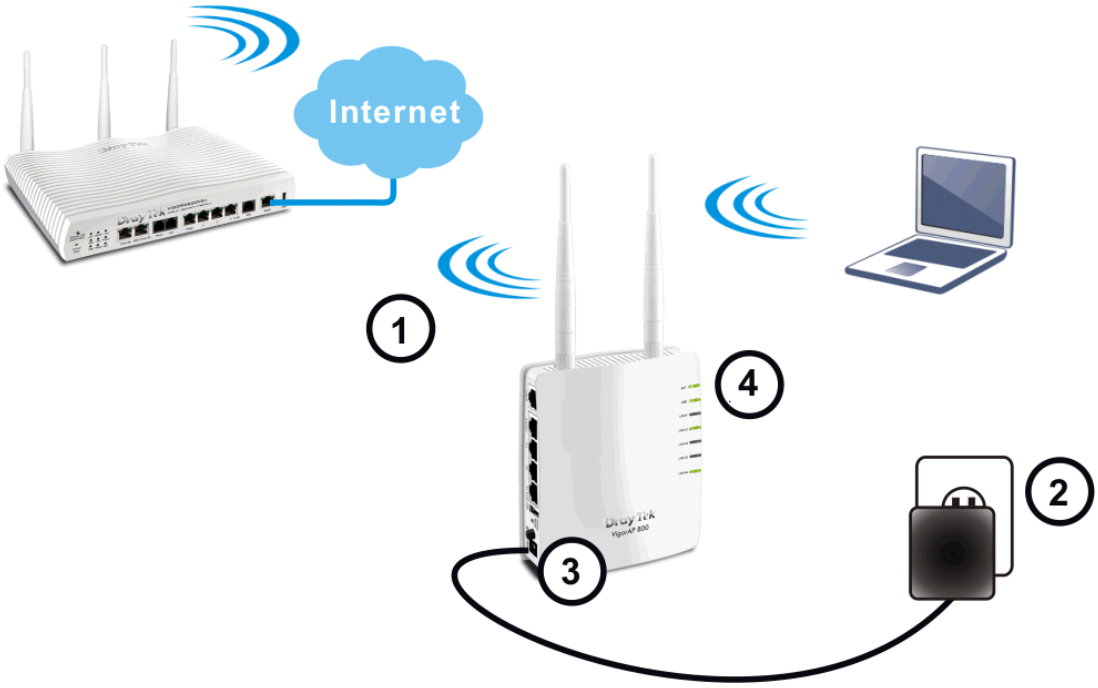


1.3.2 Wireless Connection

VigorAP 800 can access Internet via an ADSL modem, router, or switch/hub in your network through wireless connection.

1. Connect VigorAP 800 to ADSL modem or router via wireless network.
2. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.
3. Power on VigorAP 800.
4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if VigorAP 800 is correctly connected to the ADSL modem, router or switch/hub.

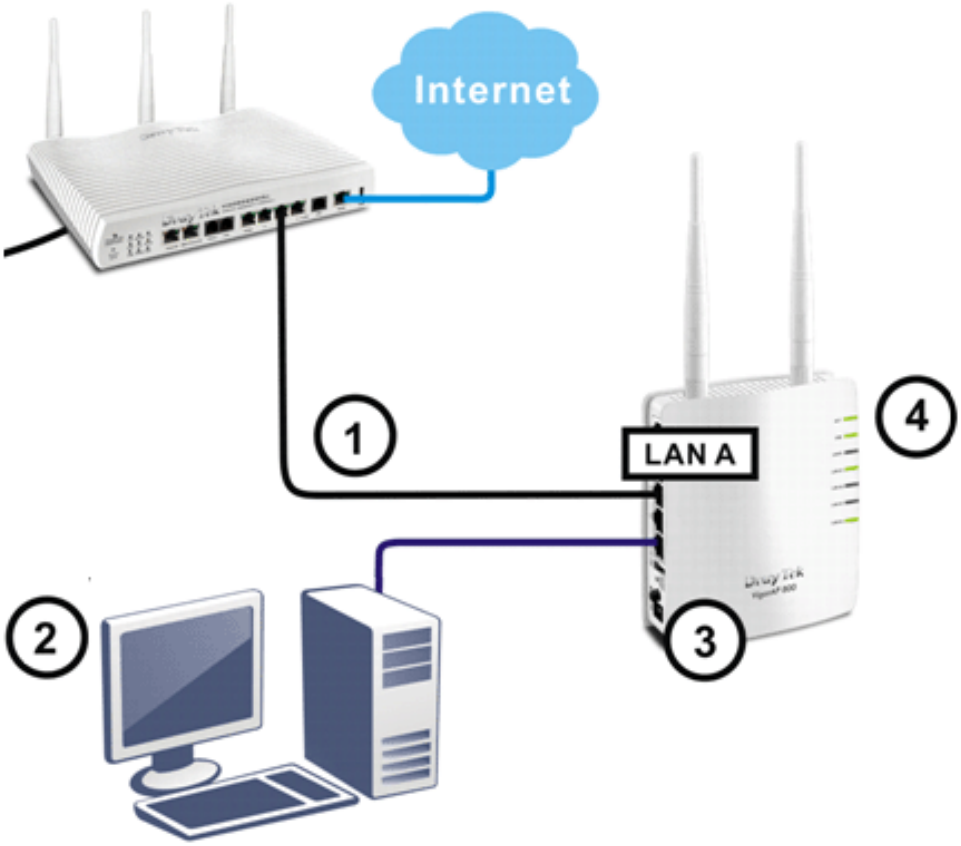
(For the detailed information of LED status, please refer to section 1.2.)



1.3.3 POE Connection

VigorAP 800 can gain the power from the connected switch, e.g., VigorSwitch P2260. PoE (Power over Ethernet) can break the install limitation caused by the fixed power supply.

1. Connect VigorAP 800 to a switch in your network through the **LAN A1** port of the access point by Ethernet cable.
2. Connect a computer to LAN A2 – A4. Make sure the subnet IP address of the PC is the same as VigorAP 800 management IP, e.g., **192.168.1.X**.
3. Power on VigorAP 800.
4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem, router or switch/hub.



This page is left blank.

2 Network Configuration

After the network connection is built, the next step you should do is setup VigorAP 800 with proper network parameters, so it can work properly in your network environment.

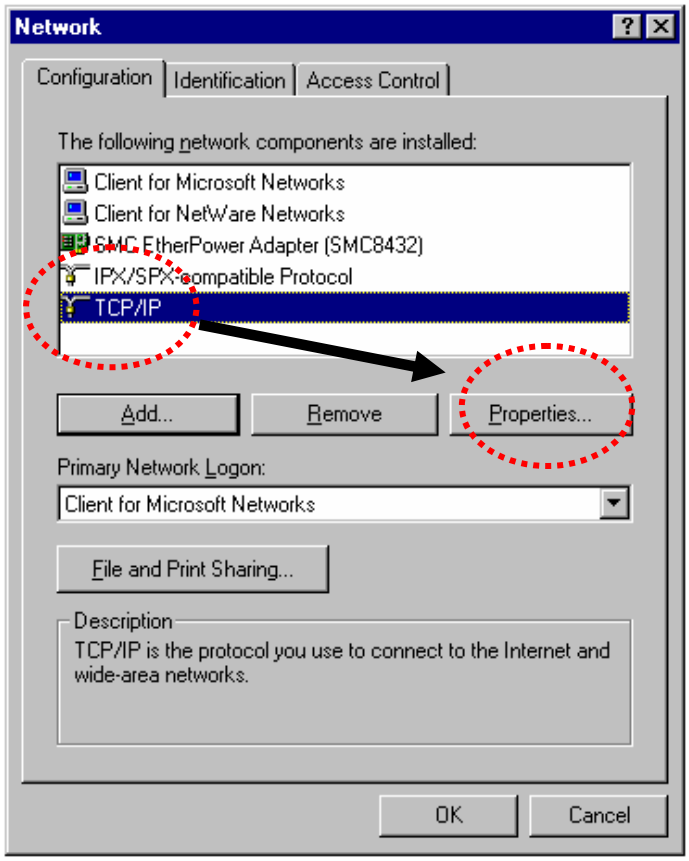
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic IP address:

For the default IP address of this AP is set "192.168.1.2", we recommend you to use "192.168.1.X (except 2)" in the field of IP address on this section for your computer.
If the operating system of your computer is…

Windows 95/98/Me	**- please go to section 2.1**
Windows 2000	**- please go to section 2.2**
Windows XP	**- please go to section 2.3**
Windows Vista	**- please go to section 2.4**

2.1 Windows 95/98/Me IP Address Setup

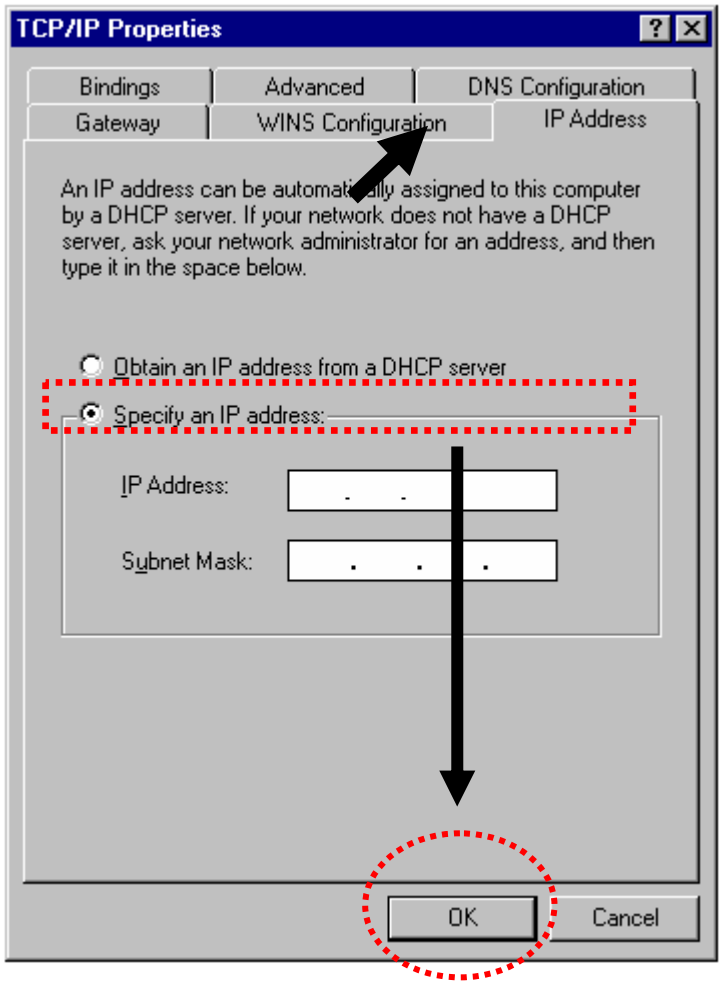
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network** icon, and the **Network** window will appear. Select **TCP/IP**, then click 'Properties'.



Select **Specify an IP address**, then input the following settings in respective field and click **OK** when finish.

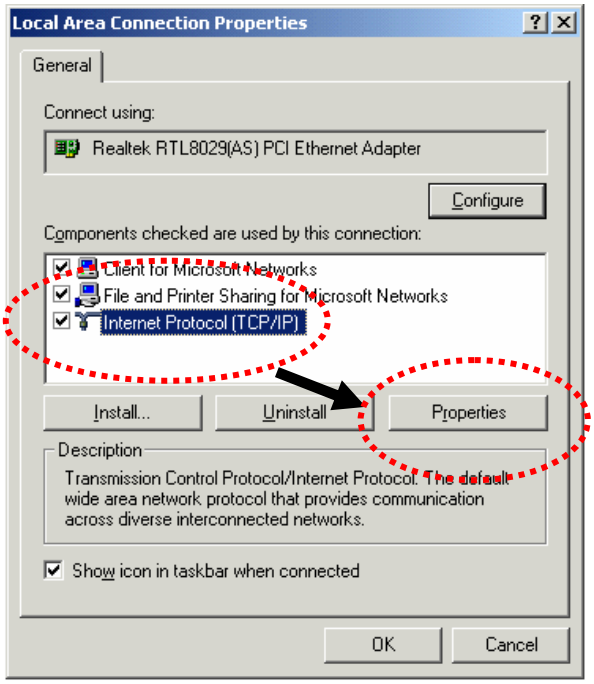
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.2 Windows 2000 IP Address Setup

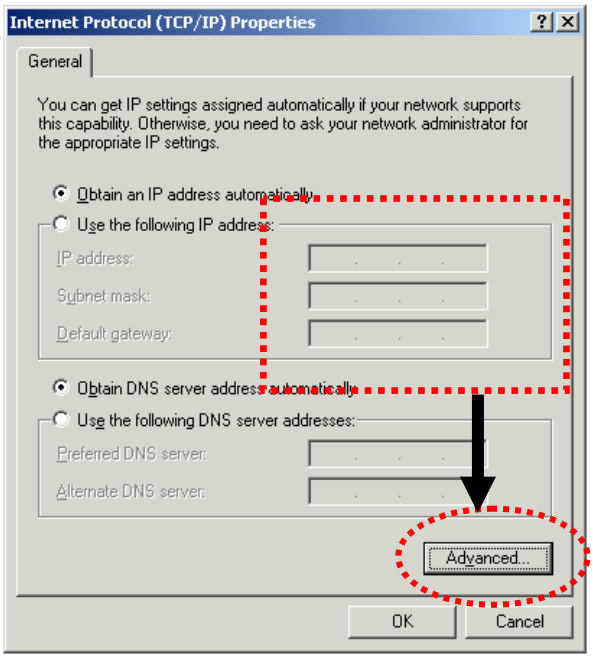
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Dial-up Connections** icon, double click **Local Area Connection,** and **Local Area Connection Properties** window will appear. Select **Internet Protocol (TCP/IP)**, then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish.

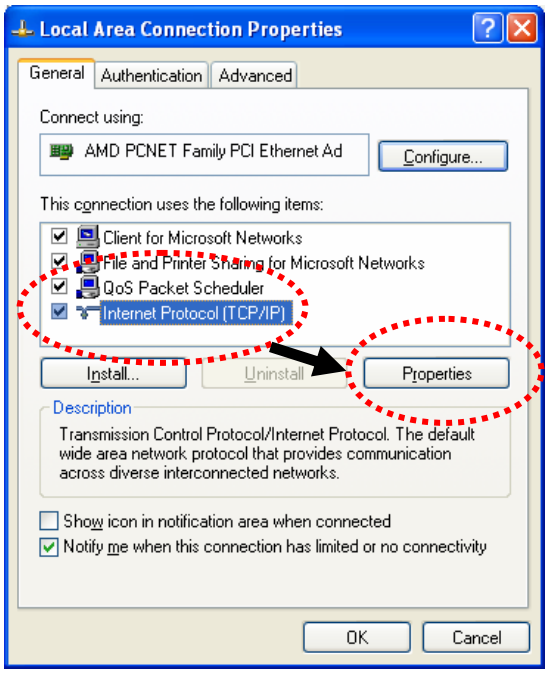
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.3 Windows XP IP Address Setup

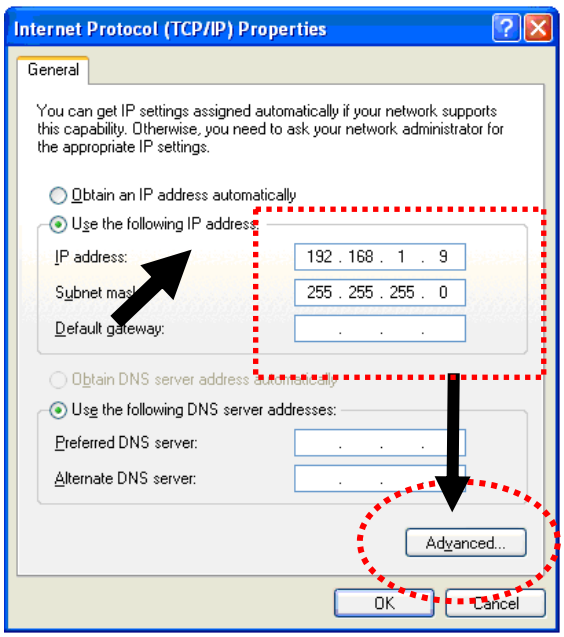
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Internet Connections** icon, click **Network Connections,** and then double-click **Local Area Connection, Local Area Connection Status** window will appear, and then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish:

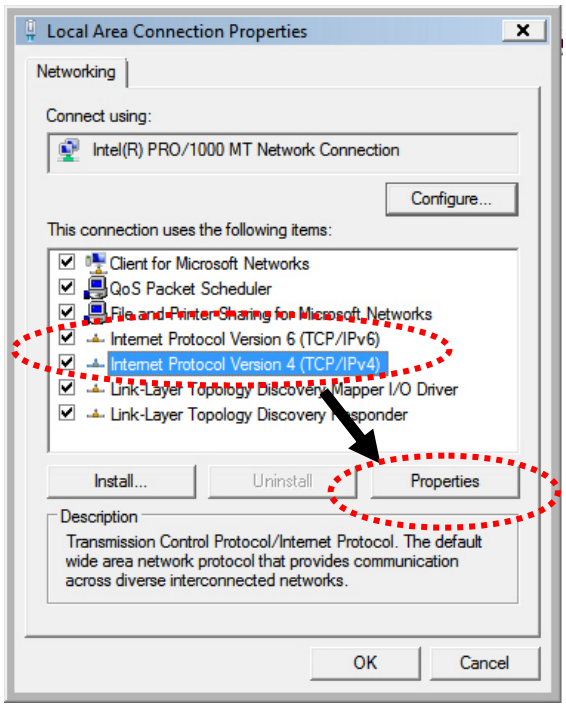
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**.



2.4 Windows Vista IP Address Setup

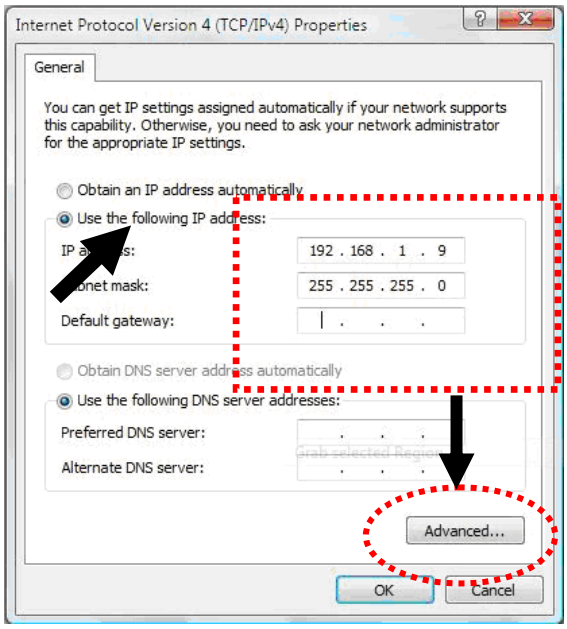
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Click **View Network Status and Tasks**, then click **Manage Network Connections.** Right-click **Local Area Netwrok, then select 'Properties'. Local Area Connection Properties** window will appear, select **Internet Protocol Version 4 (TCP / IPv4)**, and then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish:

IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**.



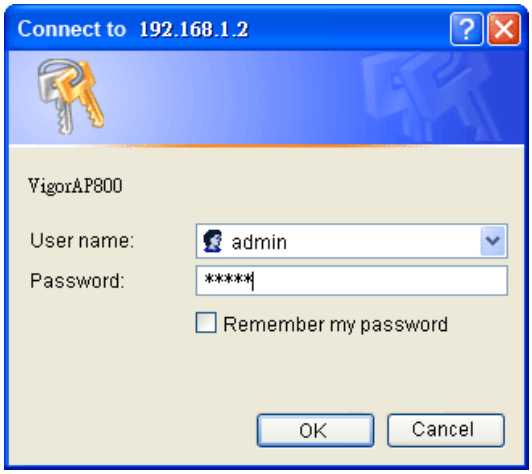
2.5 Accessing to Web User Interface

All functions and settings of this access point must be configured via web user interface. Please start your web browser (e.g., IE).

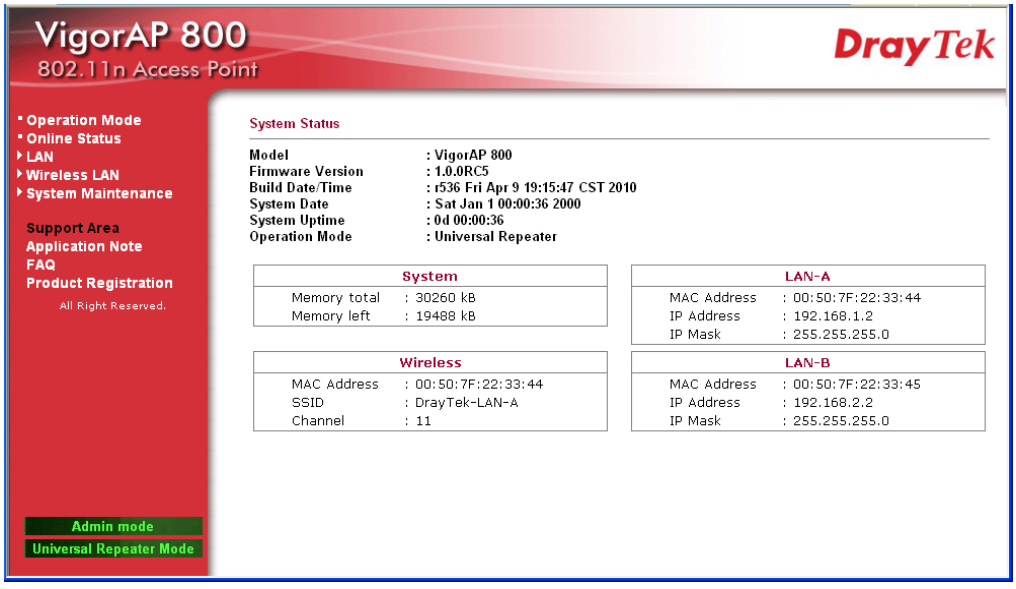
1. Make sure your PC connects to the VigorAP 800 correctly.

> **Notice:** You may either simply set up your computer to get IP dynamically from the modem or set up the IP address of the computer to be the same subnet as **the default IP address of VigorAP 800 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

2. Open a web browser on your PC and type **http://192.168.1.2.** A pop-up window will open to ask for username and password. Pease type “admin/admin” on Username/Password and click **OK**.



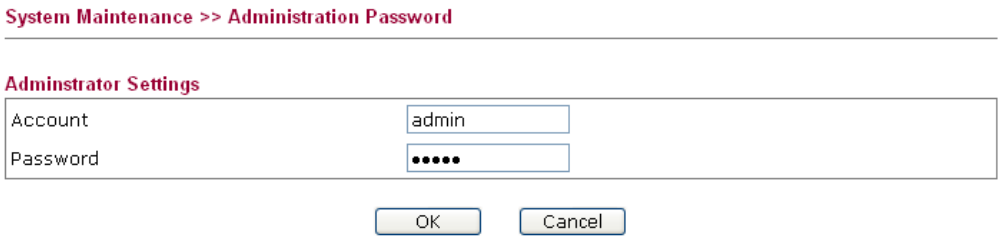
3. The **Main Screen** will pop up.



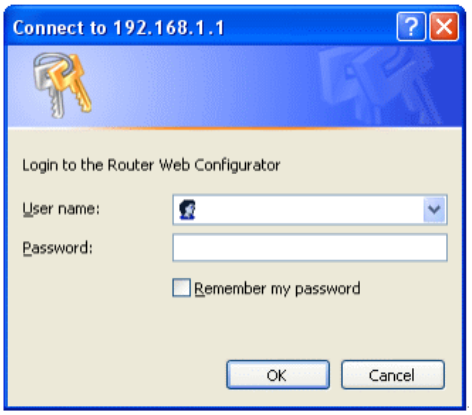
> **Note:** If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.For using the device properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

2.6 Changing Password

1. Please change the password for the original security of the modem.
2. Go to **System Maintenance** page and choose **Administrator Password.**

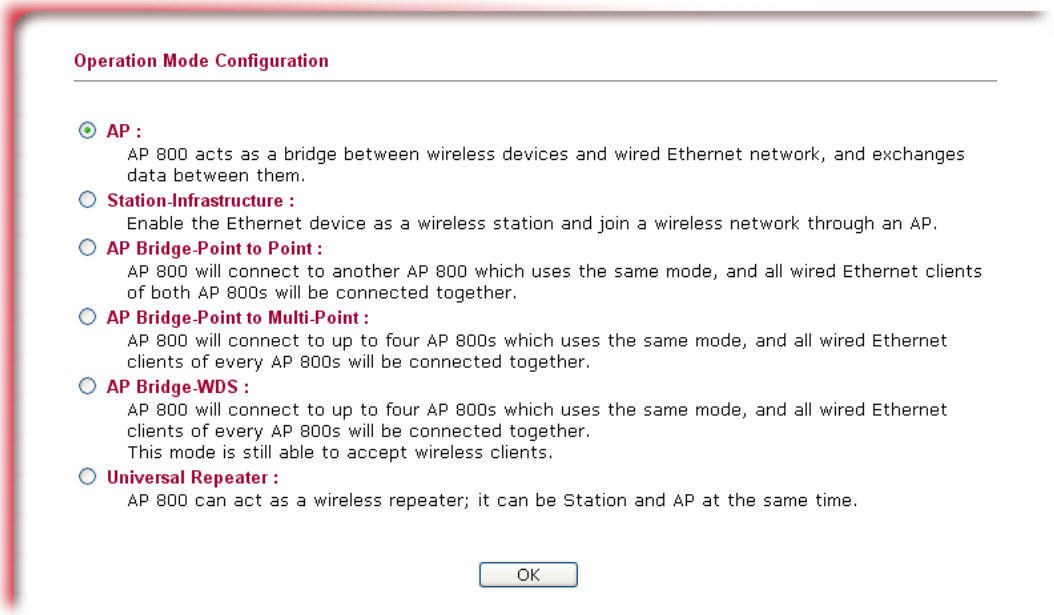


3. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this modem.



2.7 Operation Mode

This page provides several available modes for you to choose for different conditions. Click any one of them and click **OK**. The system will configure the required settings automatically.

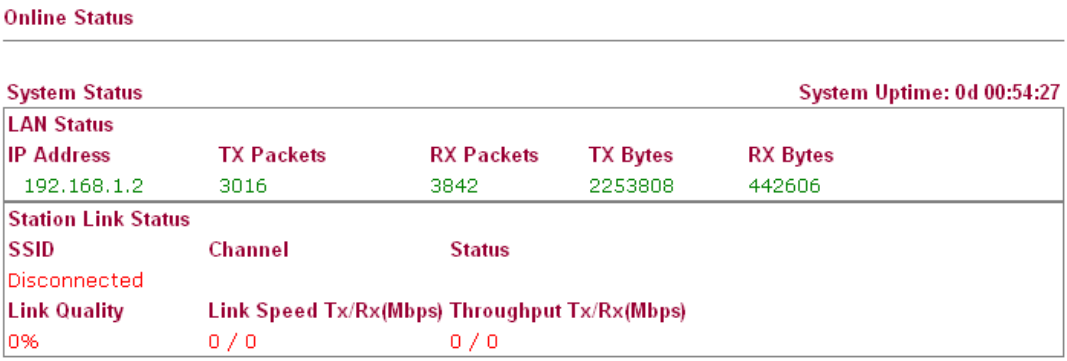


AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
Station-Infrastructure	Enable the Ethernet device such as TV and Game player connected to the VigorAP 800 to an access point.
AP Bridge-Point to Point	This mode can establish wireless connection with another VigorAP 800 using the same mode, and link the wired network which these two VigorAP 800s connected together. Only one access point can be connected in this mode.
AP Bridge-Point to Multi-Point	This mode can establish wireless connection with other VigorAP 800s using the same mode, and link the wired network which these VigorAP 800s connected together. Up to 4 access points can be connected in this mode.
AP Bridge-WDS	This mode is similar to AP Bridge to Multi-Point, but access point is not work in bridge-dedicated mode, and will be able to accept wireless clients while the access point is working as a wireless bridge.
Universal Repeater	This product can act as a wireless range extender that will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.

Note: The **Wireless LAN** settings will be changed according to the **Operation Mode** selected here. For the detailed information, please refer to the section of **Wireless LAN**.

2.8 Online Status

The online status shows the LAN status, Station Link Status for such device.



Detailed explanation is shown below:

LAN Status

IP Address Displays the IP address of the LAN interface.

TX Packets Displays the total transmitted packets at the LAN interface.

RX Packets Displays the total number of received packets at the LAN interface.

TX Bytes Displays the total transmitted size at the LAN interface.

RX Bytes Displays the total number of received size at the LAN interface.

Station Link Status

SSID Displays SSID of the station.

Channel Displays the channel that the station used.

Status Displays the connection status of the station.

Link Quality Displays the percentage of the link quality. High percentage means high quality.

Link Speed Displays transmission and receiving speed for the station.

Throughput Displays total processing size for data transmission and data receiving.

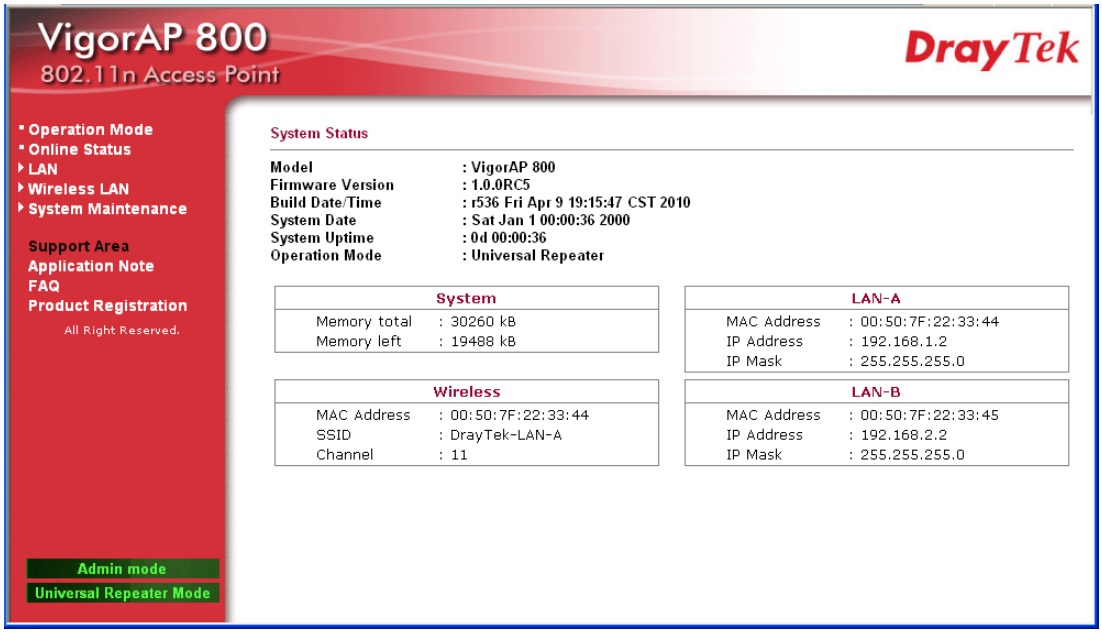
This page is left blank.

3 Web Configuration

This chapter will guide users to execute advanced (full) configuration. As for other examples of application, please refer to chapter 5.

1. Open a web browser on your PC and type **http://192.168.1.2.** The window will ask for typing username and password.
2. Please type “admin/admin” on Username/Password for administration operation.

Now, the **Main Screen** will appear. Be aware that “Admin mode” will be displayed on the bottom left side.

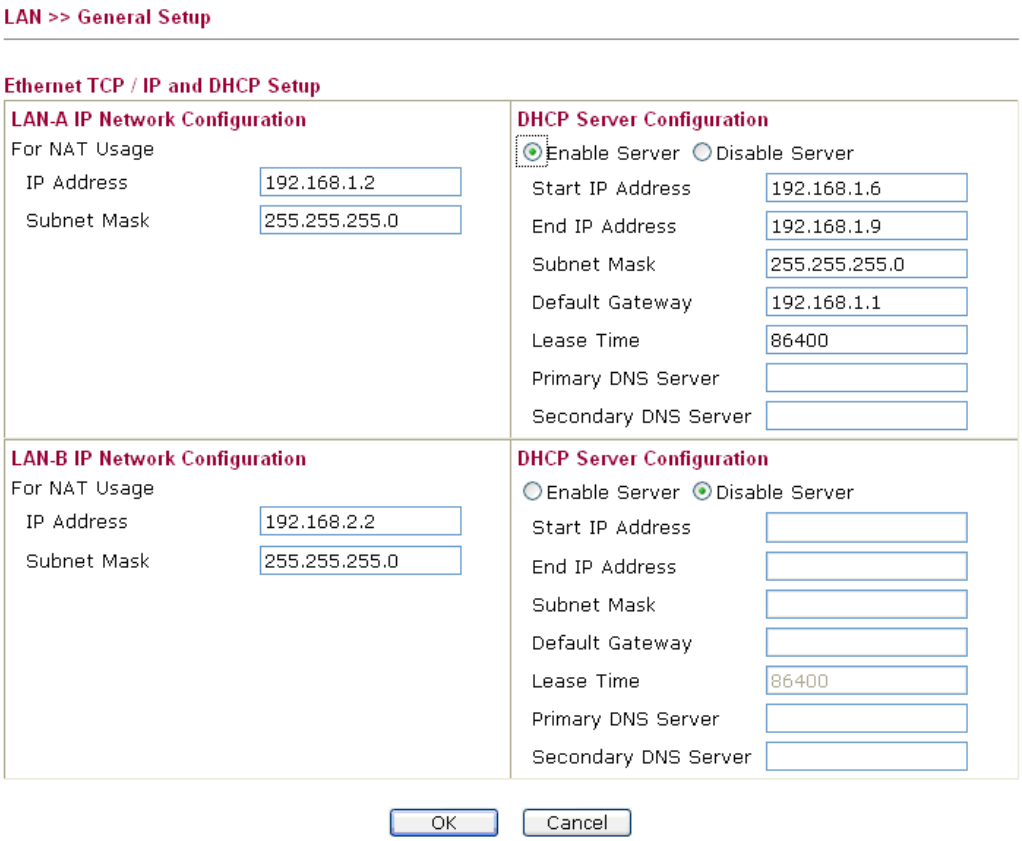


3.1 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by modem.

Click **LAN** to open the LAN settings page and choose **General Setup**.

Note: Such page will be changed according to the **Operation Mode** selected. The following screen is obtained by choosing **AP** as the operation mode.



IP Address Type in private IP address for connecting to a local private network (Default: 192.168.1.2).

Subnet Mask Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

DHCP Server Configuration DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client.

Enable Server / Disable Server Enable Server lets the modem assign IP address to every host in the LAN.

Disable Server lets you manually or use other DHCP server to assign IP address to every host in the LAN.

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254.

End IP Address Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.

Subnet Mask Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

Default Gateway Enter a value of the gateway IP address for the DHCP server.

Lease Time It allows you to set the leased time for the specified PC.

Primary IP Address You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply

	default DNS Server IP address: 194.109.6.66 to this field.
Secondary IP Address	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

3.2 General Concepts for Wireless LAN

The VigorAP 800 is equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the VigorAP 800 is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

> **Note**: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, VigorAP 800 plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via VigorAP 800. The **General Setup** will set up the information of this wireless network, including its SSID as identification, located channel etc.

Security Overview

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

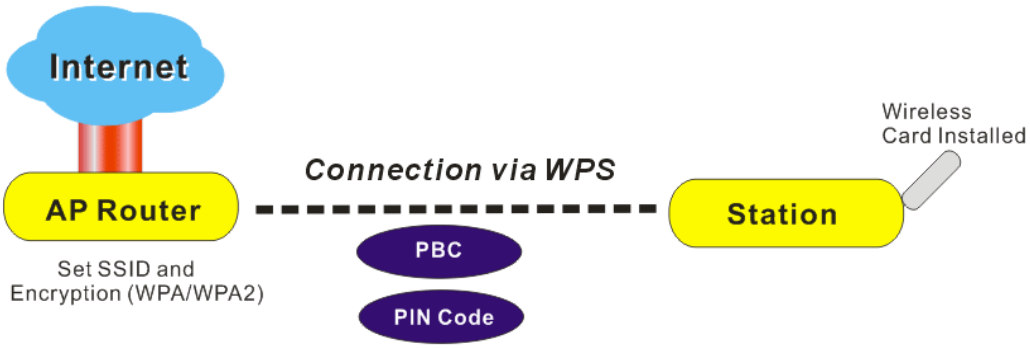
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The VigorAP 800 is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

WPS Introduction

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (VigorAP 800) with the encryption of WPA and WPA2.

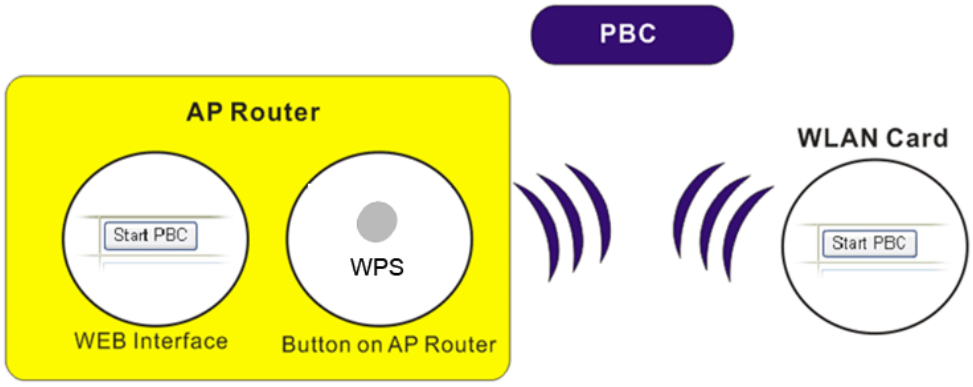
It is the simplest way to build connection between wireless network clients and VigorAP 800. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 800 automatically.



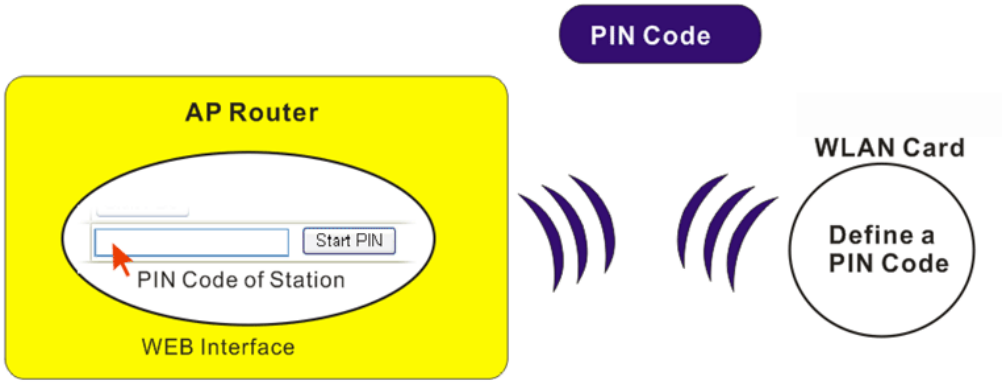
Note: Such function is available for the wireless station with WPS supported.

There are two methods to do network connection through WPS between AP and Stations: pressing the ***Start PBC*** button or using ***PIN Code***.

On the side of VigorAP 800 series which served as an AP, press **WPS** button once on the front panel of VigorAP 800 or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 800.



3.3 Wireless LAN Settings for AP Mode

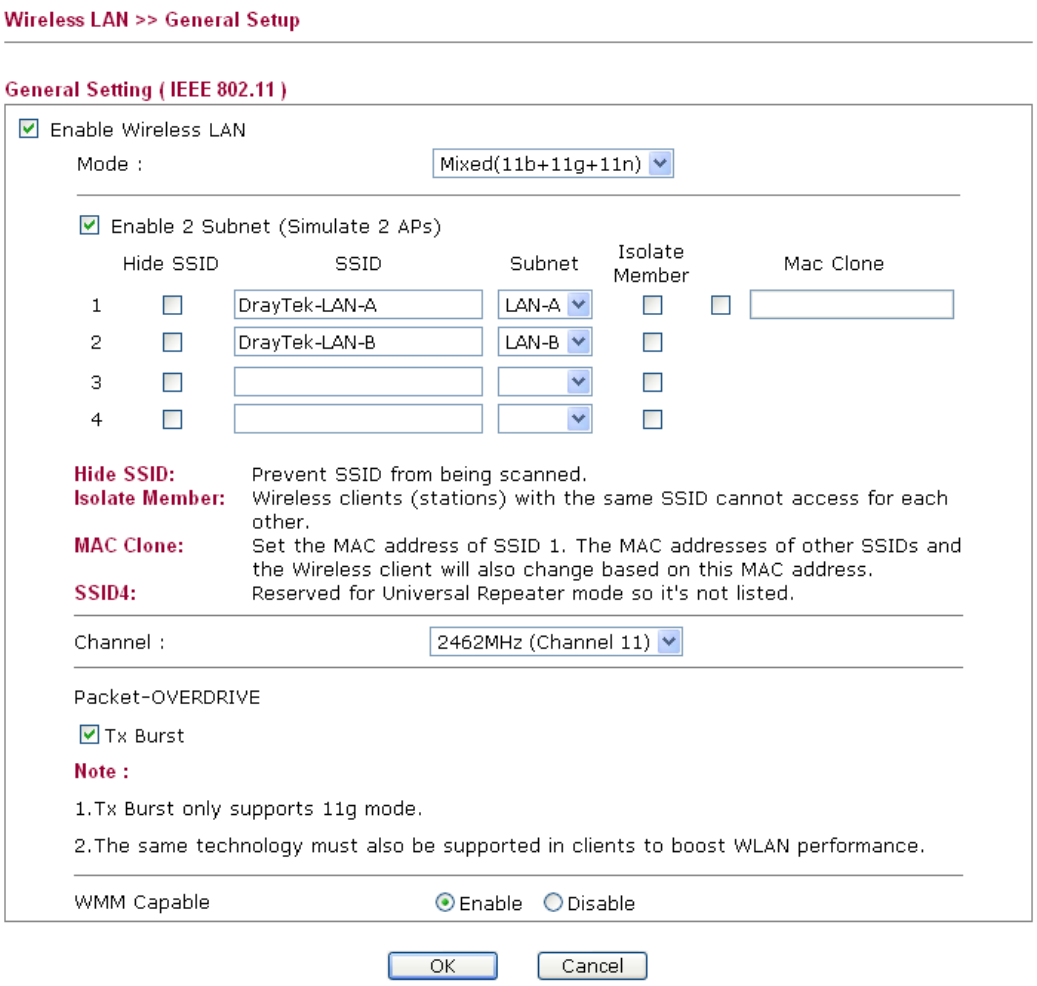
When you choose AP as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery and Station List.

Note: The **Wireless LAN** settings will be changed according to the **Operation Mode** selected here.

3.3.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

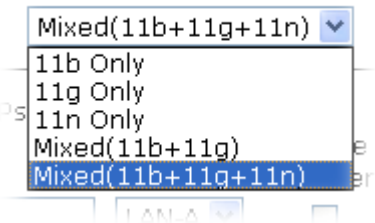
Please refer to the following figure for more information.



Enable Wireless LAN Check the box to enable wireless function.

Mode At present, VigorAP 800 can connect to 11b only, 11g only, 11n

only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.



Enable 2 Subnet (Simulate 2 APs)

Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.

If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.

Hide SSID

Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 800 while site surveying. The system allows you to set three sets of SSID for different usage.

SSID

Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When **Enable 2 Subnet** is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.

Subnet

Choose LAN-A or LAN-B for each SSID. If you choose LAN-A, the wireless clients connecting to this SSID could only communicate with LAN-A.

Isolate Member

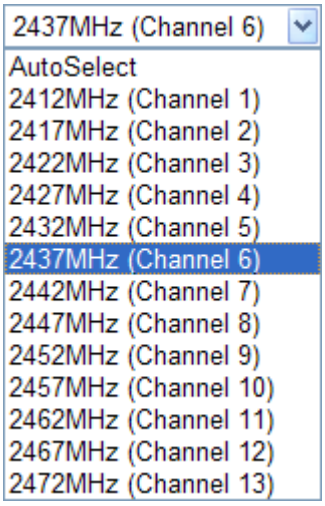
Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.

Mac Clone

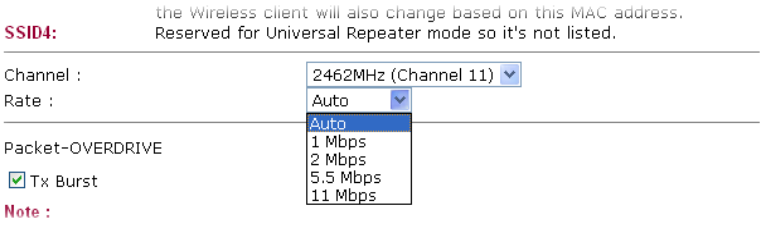
Check this box and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.

Channel

Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let system determine for you.

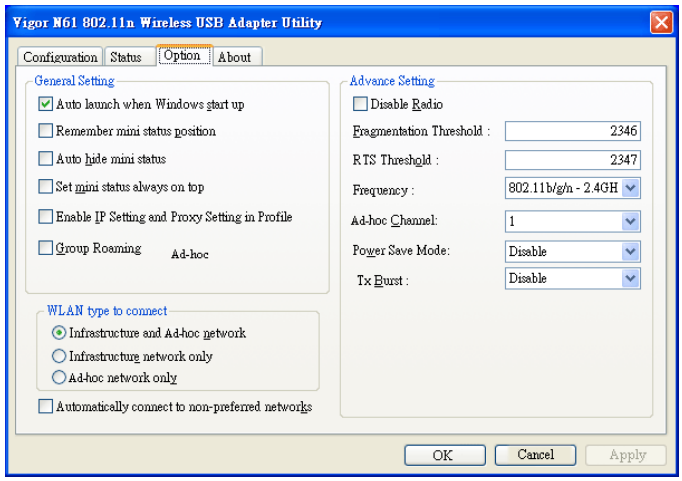


Rate If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.



Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

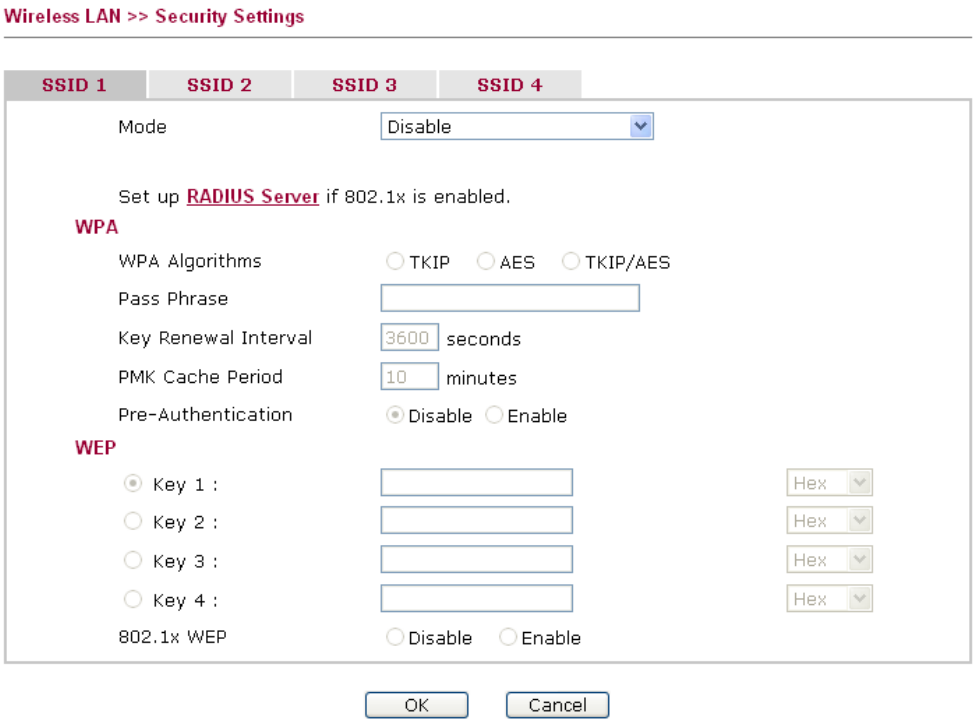


WMM Capable To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

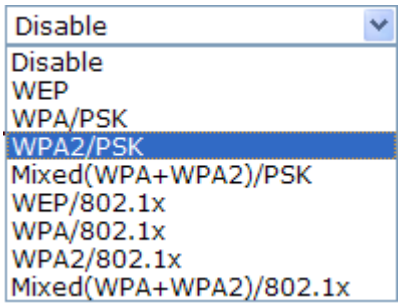
3.3.2 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.



Mode There are several modes provided for you to choose.



Disable - The encryption mechanism is turned off.

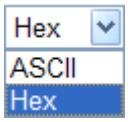
WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.

WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.

WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access

	authentication for network management. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode. **WPA/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. **WPA2/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for **WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Pass Phrase	Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for **WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for **WPA2/802.1** mode.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#'

and ','. Such feature is available for **WEP** mode.



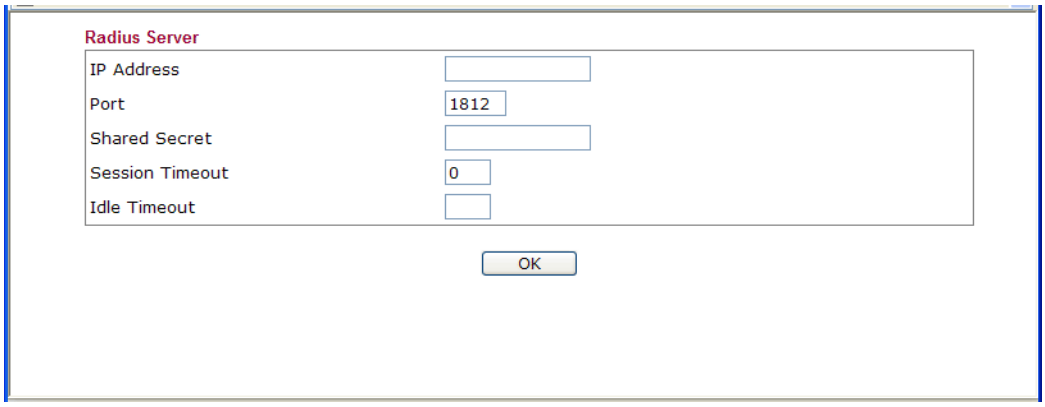
802.1x WEP

Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.

Enable - Enable the WEP Encryption.

Such feature is available for **WEP/802.1x** mode.

Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address Enter the IP address of RADIUS server.

Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

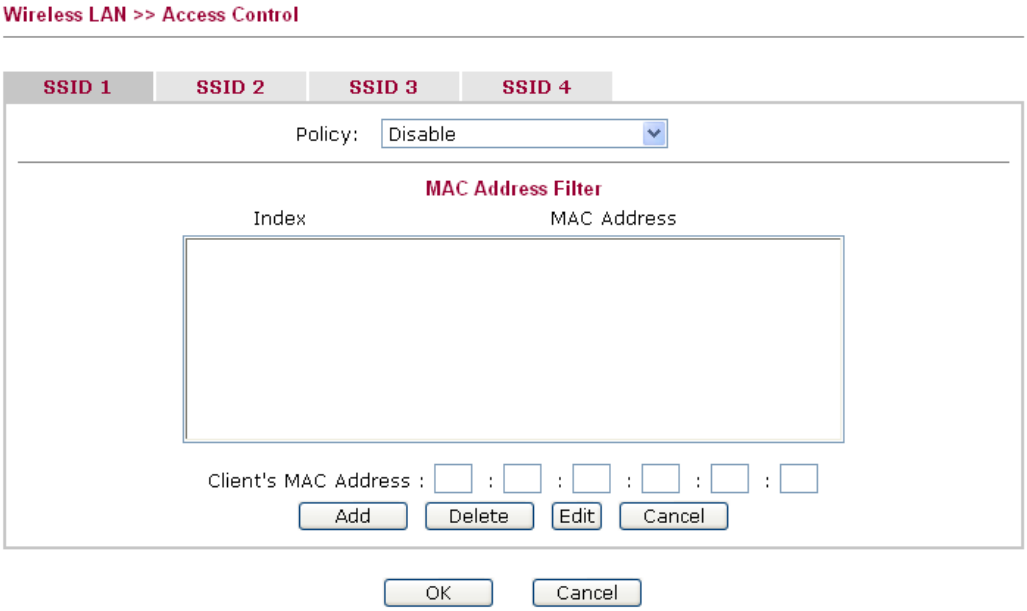
Shared Secret The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

Session Timeout Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

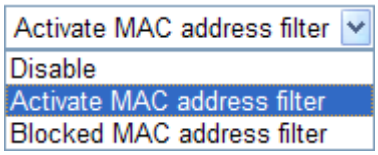
Idle Timeout Set the maximum time that a wireless device may remain idle. (The unit is second.)

3.3.3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).



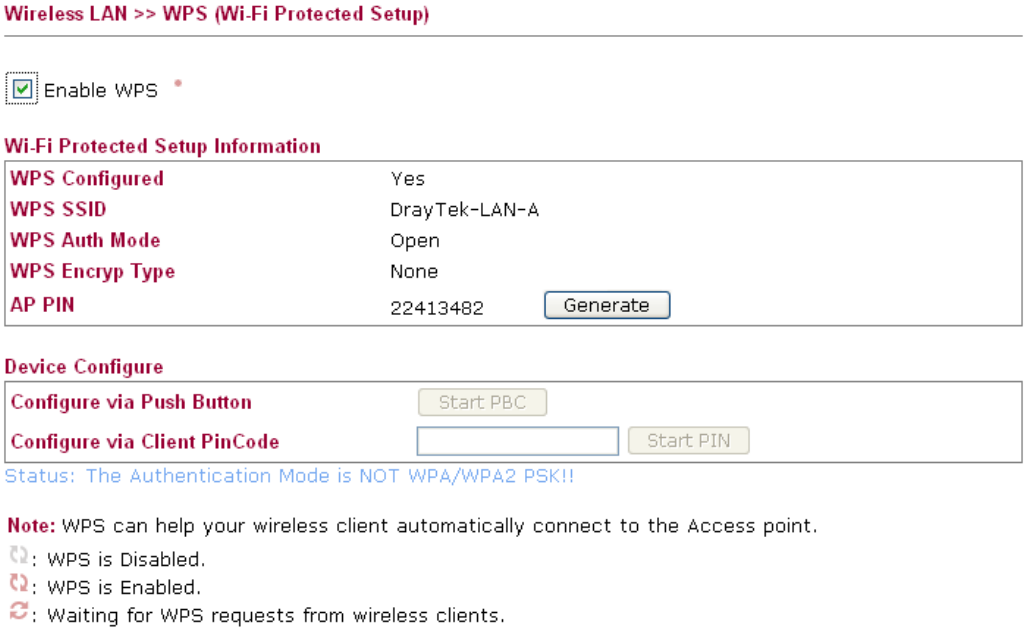
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list.



MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.

3.3.4 WPS

Open **Wireless LAN>>WPS** to configure the corresponding settings.

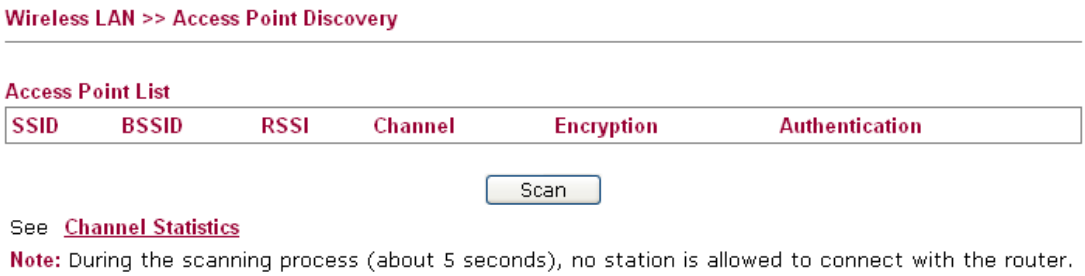


Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 800r. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
AP PIN	The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 800 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

3.3.5 AP Discovery

VigorAP 800 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

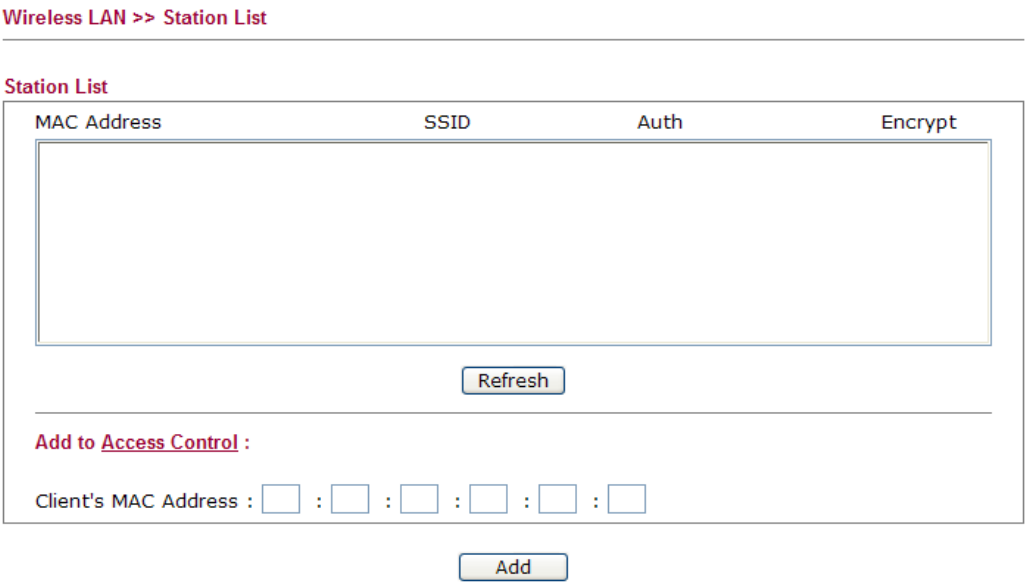
This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 800 can be found. Please click **Scan** to discover all the connected APs.



SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 800.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Channel Statistics	It displays the statistics for the channels used by APs.

3.3.6 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code.



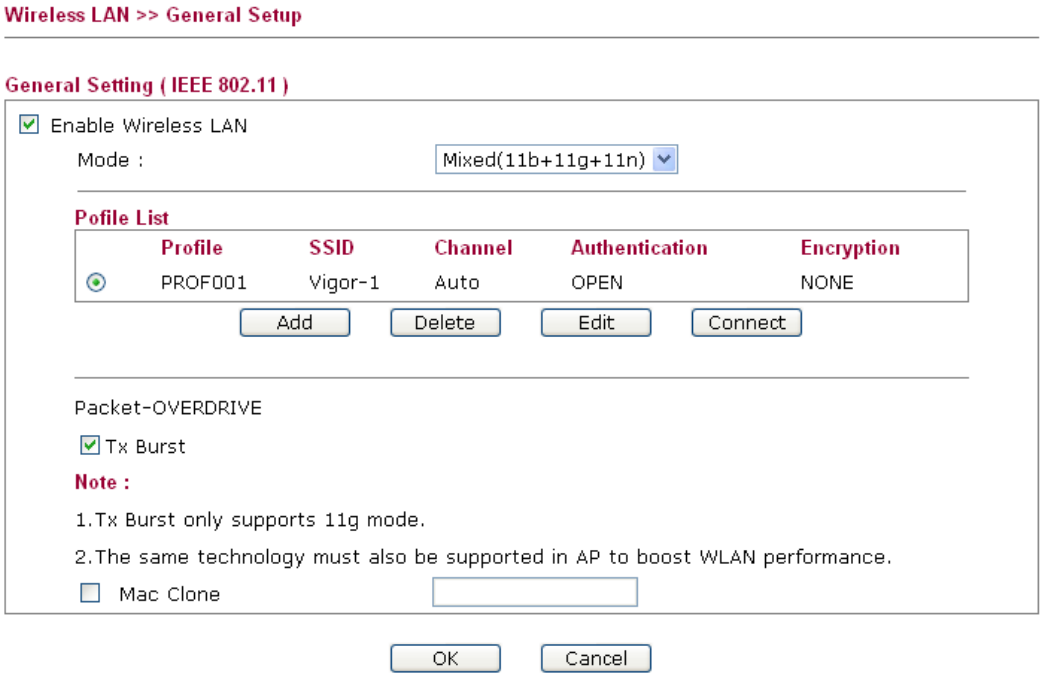
MAC Address	Display the MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	**Client's MAC Address** - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
Add	Click this button to add current typed MAC address into **Access Contro**l.

3.4 Wireless LAN Settings for Station-Infrastructure

When you choose **Station-Infrastructure** as the operation mode, the Wireless LAN menu items will include General Setup, Site Survey, Statistics and WPS.

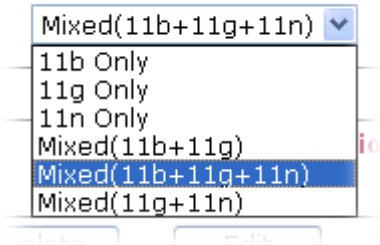
3.4.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the wireless profile and choose proper mode. Please refer to the following figure for more information.



Enable Wireless LAN Check the box to enable wireless function.

Mode At present, VigorAP 800 can connect to 11 b only, 11 g only, 11 n only, Mixed (11b+11g), Mixed (11b+11g+11n) and Mixed (11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.



Add Click this button to add new wireless profiles.

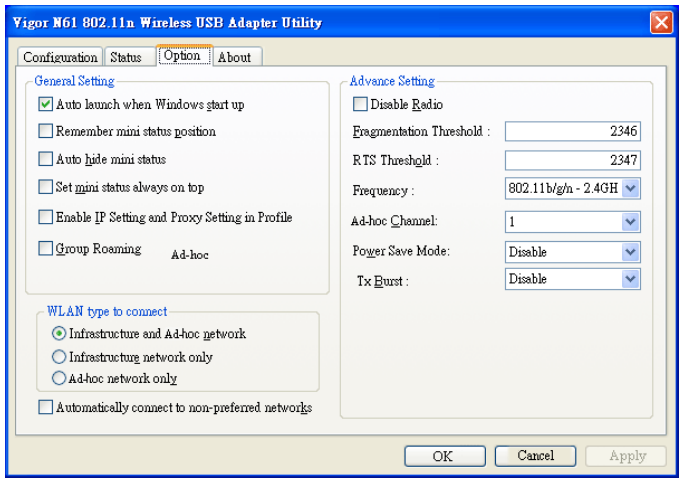
Delete Click this button to delete the selected wireless profile.

Edit Click this button to modify the existing wireless profile.

Connect Click this button to connect the wireless station to AP with the selected profile.

Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

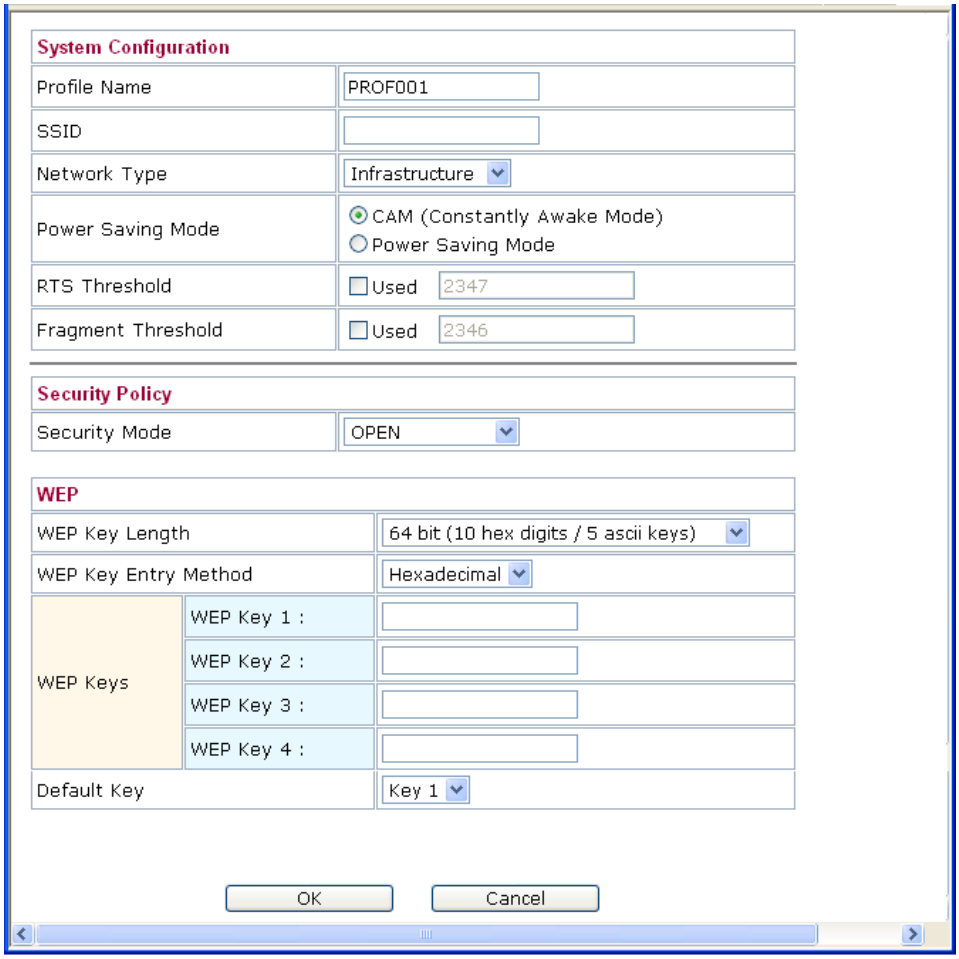
Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).



Mac Clone Check this box and manually enter the MAC address for Station mode driver.

Add a New Wireless Profile

To add a new wireless profile for the stations, click **Add.** The following dialog box will appear.

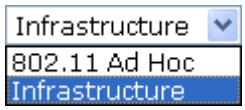


Profile Name Type a name for the new profile.

SSID Type the name for such access point that can be used for connection by the stations.

Network Type **Infrastructure** - In this mode, you can connect the access point to Ethernet device such as TV and Game player to enable the Ethernet device as a wireless station and join to a wireless network through an access point or AP router.

802.11 Ad Hoc – An ad-hoc network is a network where wireless stations can communicate with peer to peer (P2P).



Power Saving Mode Choose the power saving mode for such device.

CAM – Choose this item if it is not necessary to perform power saving job.

Power Saving Mode – Choose this item to get into the power saving status when there is no data passing through the access point.

RTS Threshold Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.

Fragment Threshold Set the Fragment threshold of wireless radio. Do not modify

default value if you don't know what it is, default value is 2346.

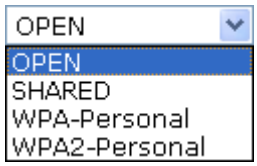
Security Mode

802.11 standard defines two mechanisms for authentication of wireless LAN clients: Open Authentication and Shared Key Authentication.

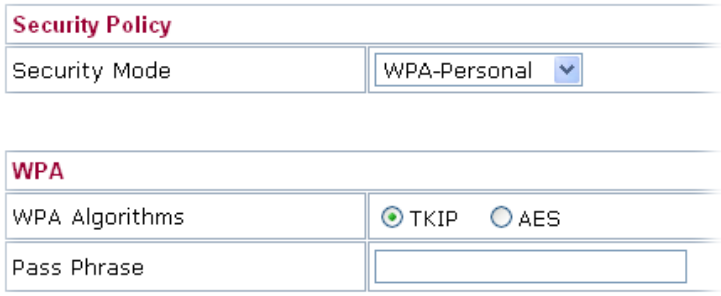
Choose one of the security modes from the drop down list. If you choose OPEN or SHARED, you have to type WEP information.

OPEN – Open authentication is basically null authentication algorithm, which means that there is no verification of the user.

SHARED – It works similar to Open authentication with only one major difference. If you choose OPEN with WEP encryption key, the WEP keys is used to encrypt and decrypt the data but not for authentication. In Shared key authentication, WEP encryption will be used for authentication.



If you choose **WPA-Personal** or **WPA2-Personal**, the corresponding WPA settings will be listed as follows. You have to choose the WPA algorithms and type the pass phrase for such security mode.



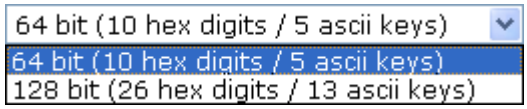
WPA Algorithms – Choose Temporal Key Integrity Protocol (TKIP) or AES for data encryption.

Pass Phrase – Please type 8 to 63 alphanumerical characters here.

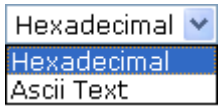
WEP Key Length

WEP (Wired Equivalent Privacy) is a common encryption mode. It is safe enough for home and personal use. However, if you need higher level of security, please consider using WPA encryption (see next section).

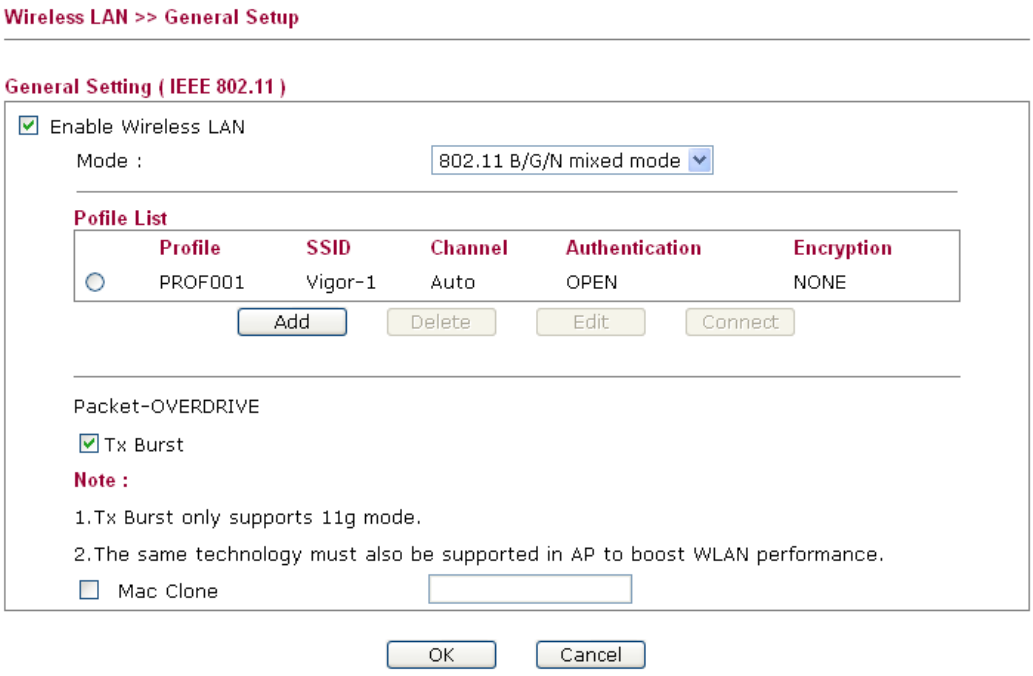
Some wireless clients do not support WPA, but support WEP. Therefore WEP is still a good choice for you if you have such kind of client in your network environment.



There are two types of WEP key length: 64-bit and 128-bit. Using 128-bit is safer than 64-bit, but it will reduce some data transfer performance.

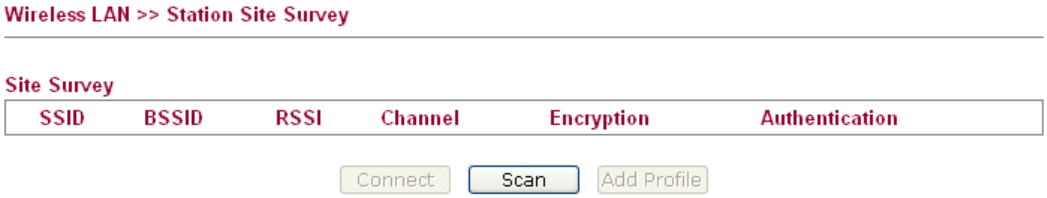
WEP Key Entry Method	There are two types of key method: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select 64-bit as key length, and Hex as key format, you'll see the message at the right of Key Format is 'Hex (10 characters) which means the length of WEP key is 10 characters. 
WEP Keys (Key 1 – Key 4)	Input WEP key characters here, the number of characters must be the same as the number displayed at Key Format field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select ASCII key format, and if you select Hex as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here. If you entered multiple WEP keys, they should not be the same with each other.
Default Key	You can set up to four sets of WEP key, and you can decide which key is being used as default here. **If you don't know which one you should use, select 'Key 1'.**

Below shows an example for a wireless profile created.



3.4.2 Site Survey

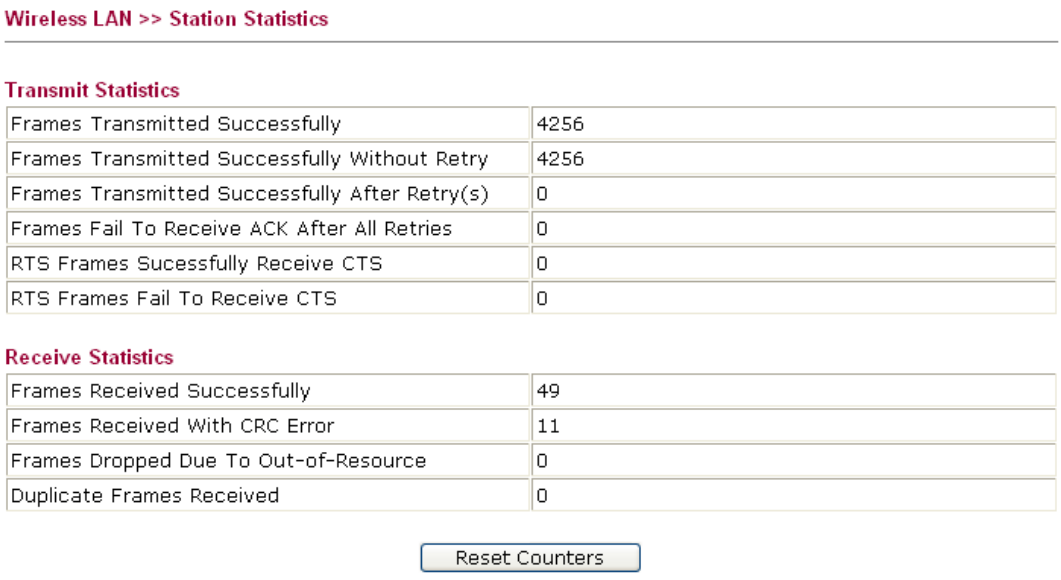
The page will list the access points nearby as VigorAP800 is set to Station mode. You can select one of the access points to associate.



SSID	Display the SSID name of the access point.
BSSID	Display the BSSID (MAC Address) of the access point.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the channel number of the access point.
Encryption	Display the encryption setting of the access points. If you have selected the access point with security setting, you have to go to 2-7 Wireless Security to set the same security with the access point you want to associate.
Authentication	Display the authentication type of the access point.
Connect	Connect to the wireless AP that you choose.
Scan	Search the stations connected to such access point.
Add Profile	The system will add a profile automatically for you to connect with the wireless AP that you choose.

3.4.3 Statistics

This page displays the statistics for data transmission and receiving between the access point and the stations.



Click **Rest Counters** if required.

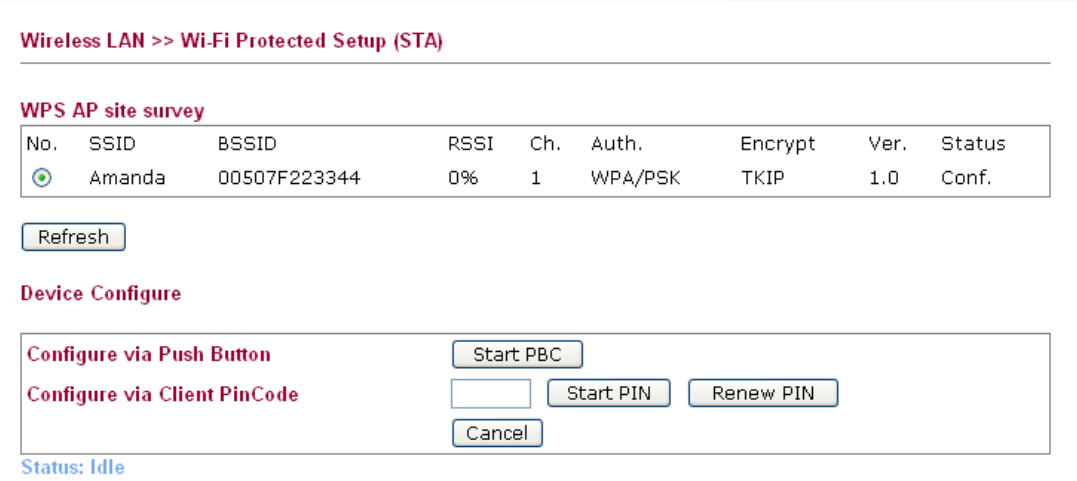
3.4.4 WPS (Wi-Fi Protected Setup)

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and the access point. You don't have to select encryption mode and input a long encryption passphrase every time when you need to setup a wireless client. You only have to press a button on wireless client and the access point, and the WPS will do the setup for you.

VigorAP800 supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch VigorAP800 to WPS mode and push a specific button on the wireless client to start WPS mode. You can push Reset/WPS button of this VigorAP800, or click **PBC Start** button in the web configuration interface to do this; if you want to use PIN code, you have to provide the PIN code of the wireless client you wish to connect to this access point and then switch the wireless client to WPS mode.

Note: WPS function of VigorAP800 will not work for those wireless AP/clients do not support WPS.

To use WPS function to set encrypted connection between VigorAP800 and WPS-enabled wireless AP, please open **Wireless LAN >>WPS**. The following information will be displayed:



SSID	Display the SSID name of the access point.
BSSID	Display the BSSID (MAC Address) of the access point.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Ch. (Channel)	Display the channel number of the access point.
Auth. (Authentication)	Display the authentication type of the access point.
Encrypt (Encryption)	Display the encryption setting of the access points. If you have selected the access point with security setting, you have to go to 2-7 Wireless Security to set the same security with the access point you want to associate.
Ver. (Version)	Display the version of WPS.

Status	Display the status of WPS access point.
Refresh	Click this button to refresh the AP site survey.
Start PBC	Click **Start PBC** to make a WPS connection within 2 minutes.
PIN Start	When using PinCode method, it is required to enter PIN Code (Personal Identification Number Code, 8-digit numbers) into Registrar. When the wireless station is Enrollee, the users can use Renew PIN to re-generate a new PIN code.
Renew PIN	Click this button to re-generate a new PIN code.

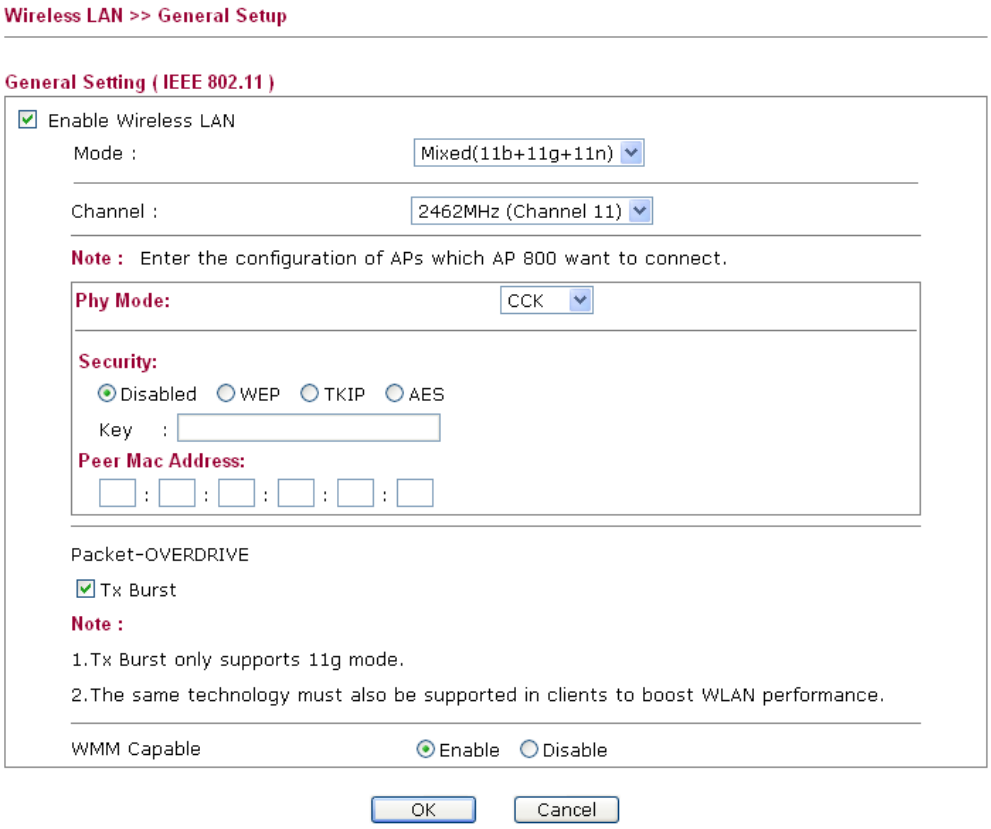
Note: When you're using PBC type WPS setup, you must press **PBC** button (hardware or software) of wireless client within 2 minutes. If you didn't press **PBC** button of wireless client within this time period, please press **PBC** button (hardware or software) of this access point again.

3.5 Wireless LAN Settings for AP Bridge-Point to Point

When you choose AP Bridge-Point to Point as the operation mode, the Wireless LAN menu items will include General Setup, and AP Discovery.

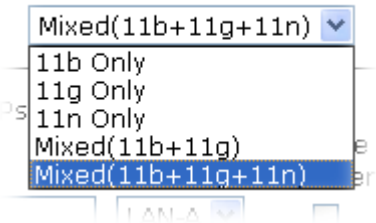
3.5.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the Phy mode, security, Tx Burst and choose proper mode. Please refer to the following figure for more information.



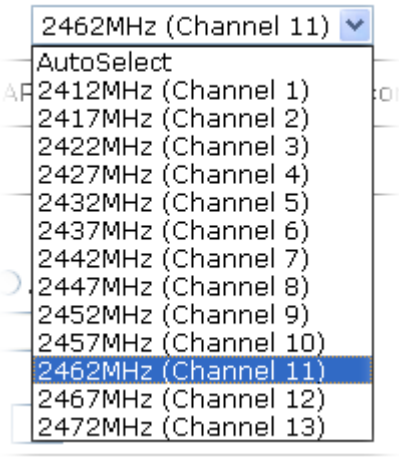
Enable Wireless LAN Check the box to enable wireless function.

Mode At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

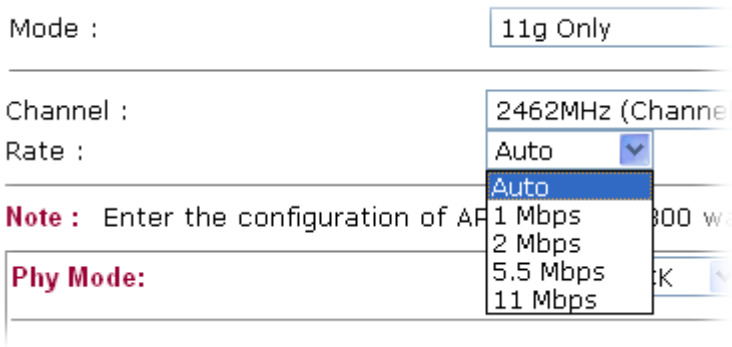


Channel Means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected channel is

under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let system determine for you.



Rate If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.



Phy Mode Select CCK (11b mode), OFDM (11g mode), or HTMIX (11b/g/n mixed mode) from the drop down menu for the access point that VigorAP 800 wants to connect. Each access point should be setup to the same **Phy** mode for connecting with each other.

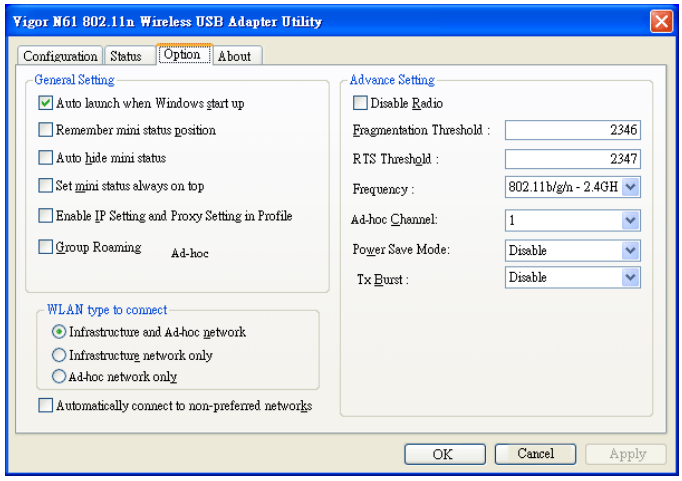
Security Select WEP, TKIP or AES as the encryption algorithm.

Peer Mac Address Type the peer MAC address for the access point that VigorAP 800 connects to.

Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching

with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

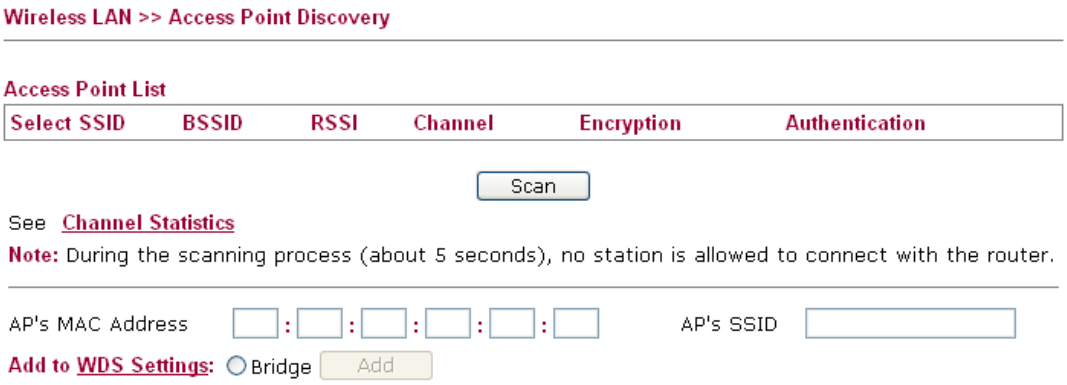


WMM Capable To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

3.5.2 AP Discovery

VigorAP 800 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to VigorAP 800.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 800 can be found. Please click **Scan** to discover all the connected APs.



SSID Display the SSID of the AP scanned by VigorAP 800r.

BSSID Display the MAC address of the AP scanned by VigorAP 800.

RSSI Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.

Channel Display the wireless channel used for the AP that is scanned by VigorAP 800.

Encryption Display the encryption mode for the scanned AP.

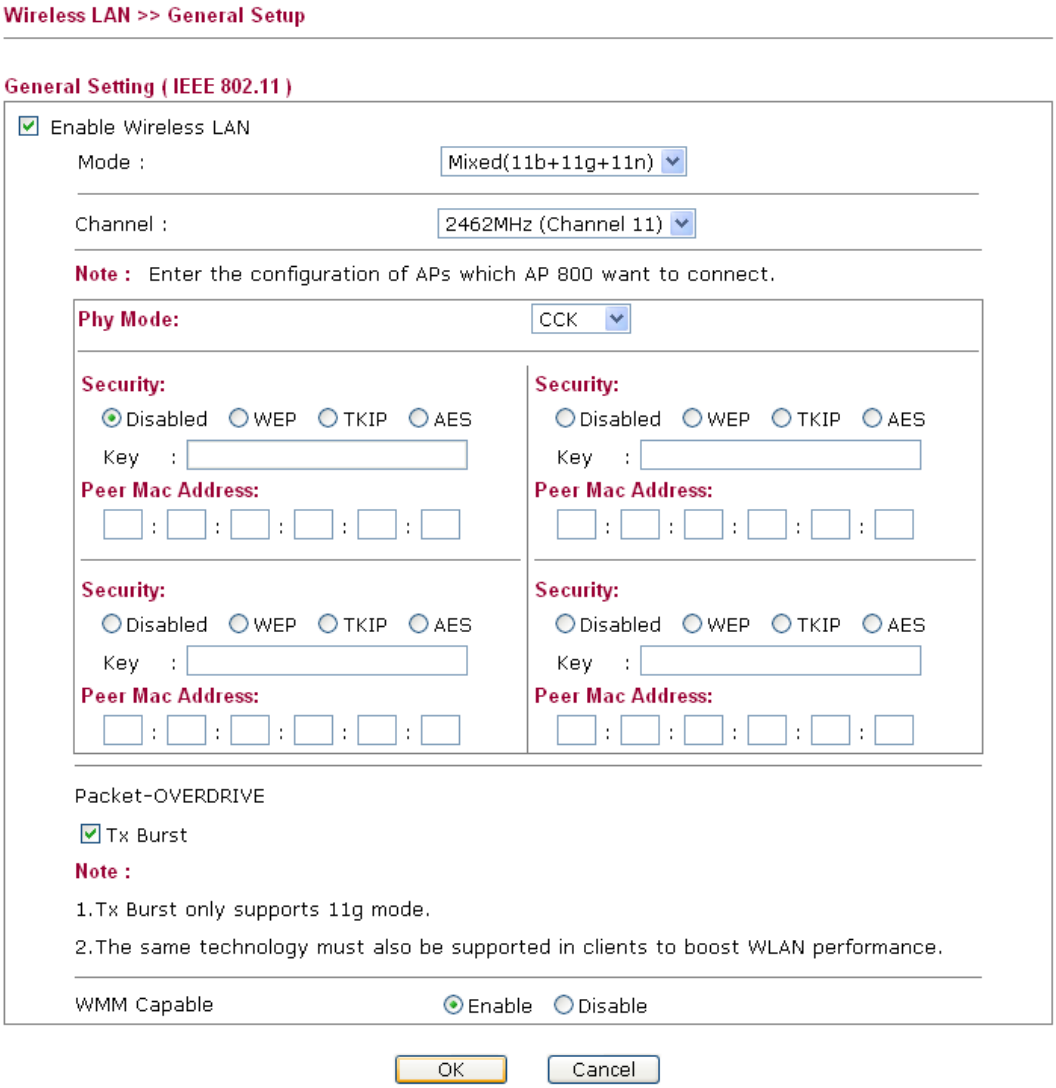
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Add	Click **Bridge** for the specified AP. Next, click **Add**. Later, the MAC address of the AP will be added and be shown on WDS settings page.

3.6 Wireless LAN Settings for AP Bridge-Point to Multi-Point

When you choose AP Bridge-Point to Multi-Point as the operation mode, the Wireless LAN menu items will include General Setup, and AP Discovery.

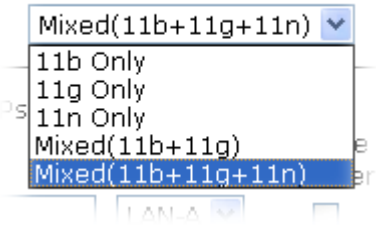
3.6.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the Phy mode, security, Tx Burst and choose proper mode. Please refer to the following figure for more information. In this page, you can set up to four groups of encryption settings (WEP, TKIP or AES) for data transmission.

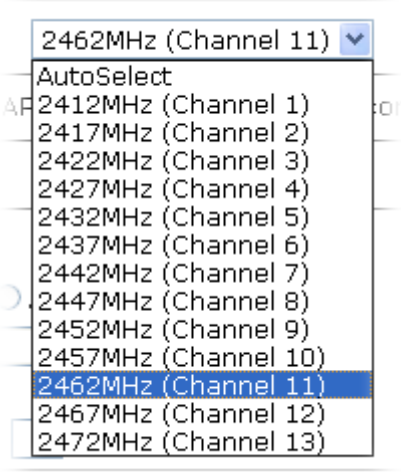


Enable Wireless LAN Check the box to enable wireless function.

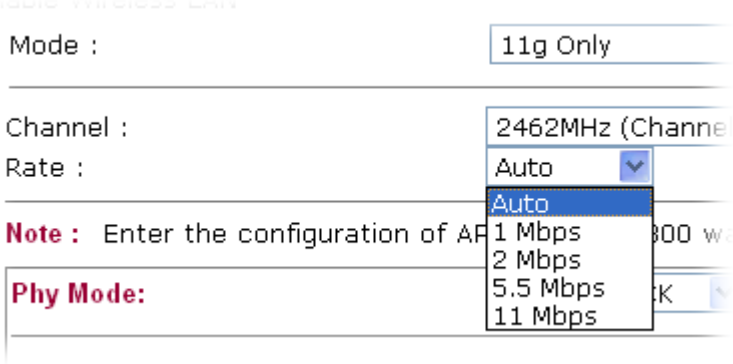
Mode At present, VigorAP 800 can connect to 11 b only, 11 g only, 11 n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.



Channel Means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let system determine for you.



Rate If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.



Phy Mode Select CCK (11b mode), OFDM (11g mode), or HTMIX (11b/g/n mixed mode) from the drop down menu for the access point that VigorAP 800 wants to connect. Each access point should be setup to the same **Phy** mode for connecting with each other.

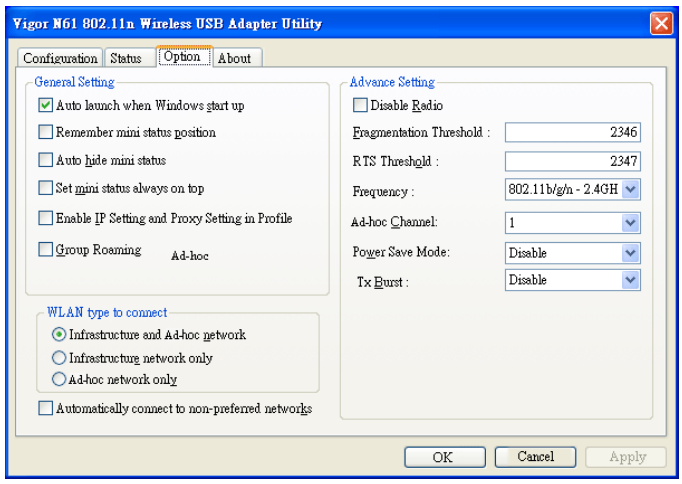
Security Select WEP, TKIP or AES as the encryption algorithm.

Peer Mac Address Type the peer MAC address for the access point that VigorAP 800 connects to. Four peer MAC addresses are allowed to be entered in this page at one time.

Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for

TxBURST on the tab of **Option**).

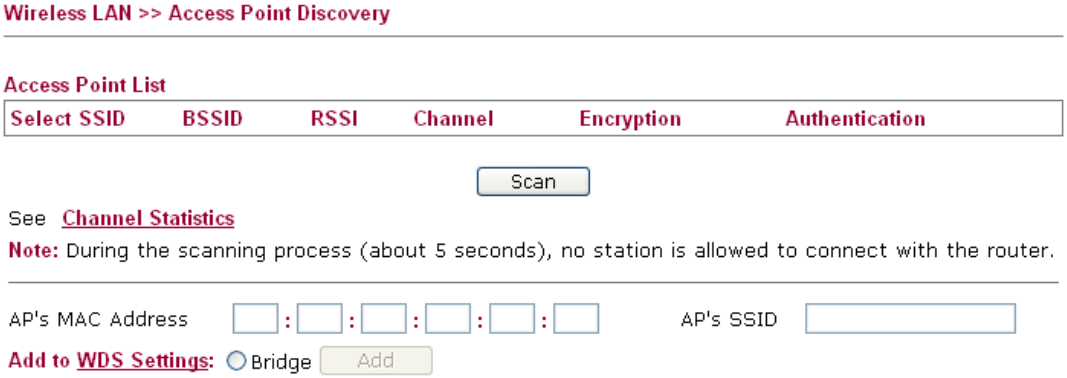


WMM Capable To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

3.6.2 AP Discovery

VigorAP 800 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 800 can be found. Please click **Scan** to discover all the connected APs.



SSID Display the SSID of the AP scanned by VigorAP 800.

BSSID Display the MAC address of the AP scanned by VigorAP 800.

RSSI Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.

Channel Display the wireless channel used for the AP that is scanned by VigorAP 800.

Encryption Display the encryption mode for the scanned AP.

Authentication Display the authentication type that the scanned AP applied.

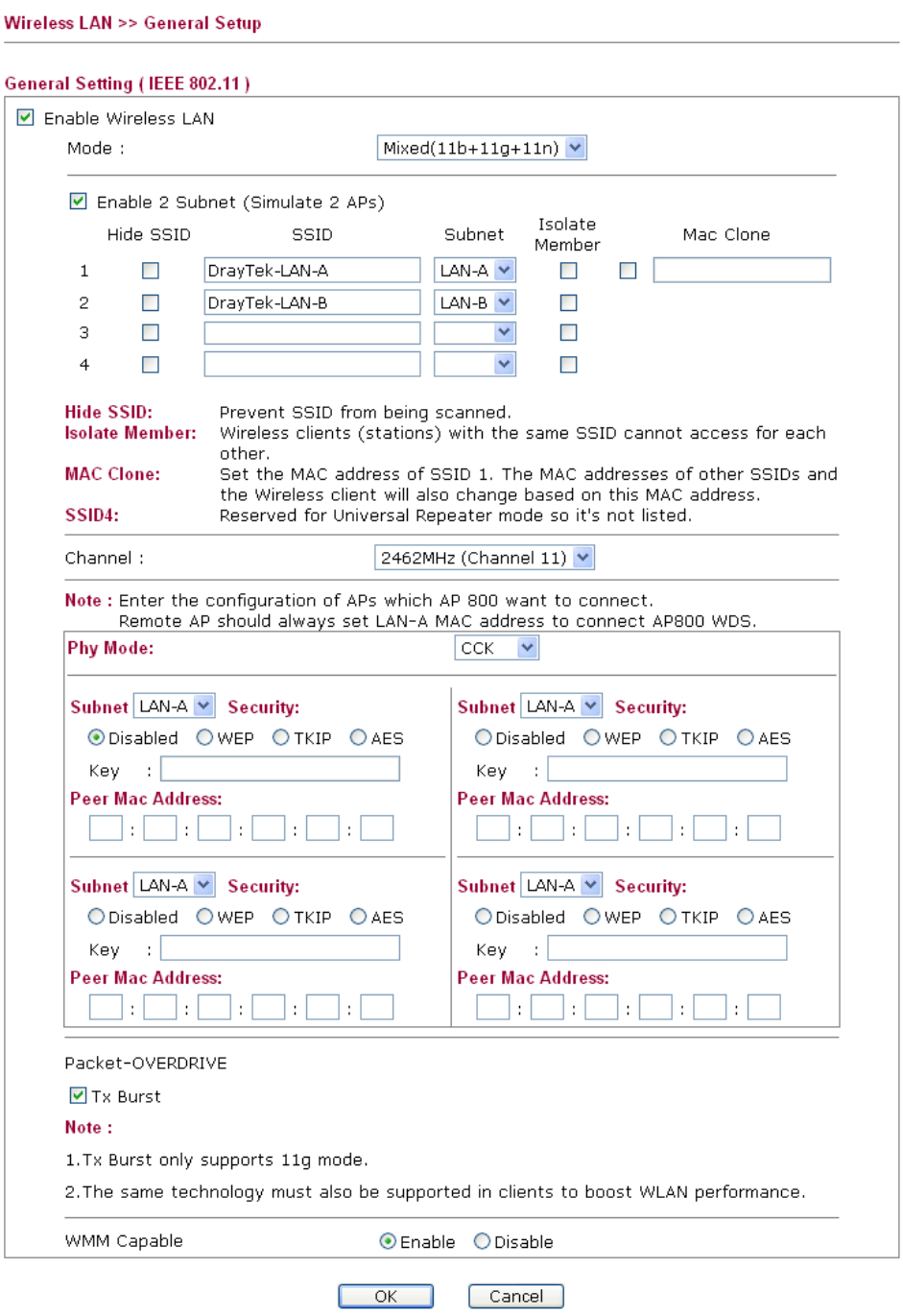
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Add	Click **Bridge** for the specified AP. Next, click **Add**. Later, the MAC address of the AP will be added and be shown on WDS settings page.

3.7 Wireless LAN Settings for AP Bridge-WDS

When you choose AP Bridge-WDS as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery and Station List.

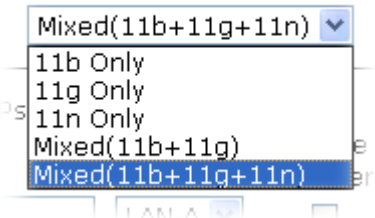
3.7.1 General Setup

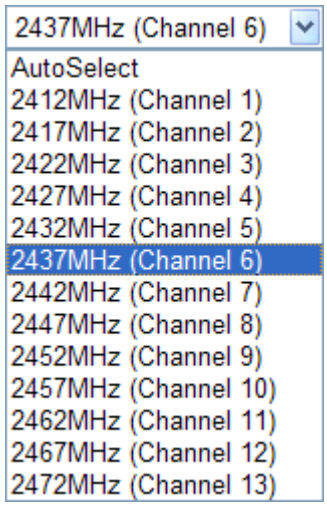
By clicking the **General Setup**, a new web page will appear so that you could configure the Phy mode, security, Tx Burst and choose proper mode. Please refer to the following figure for more information.

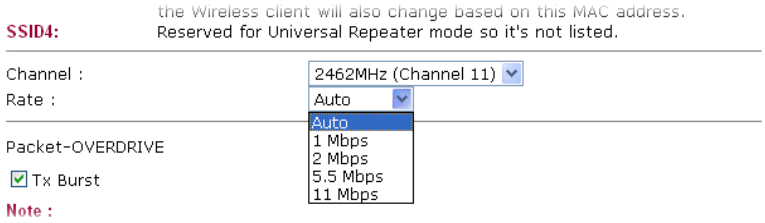


Enable Wireless LAN Check the box to enable wireless function.

Mode At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.



Enable 2 Subnet (Simulate 2 APs)	Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800. If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 800 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When **Enable 2 Subnet** is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Subnet	Choose LAN-A or LAN-B for each SSID.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
Mac Clone	Check this box and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let system determine for you. 
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.



Phy Mode There are three types of transmission rates developed by different techniques for **Phy Mode**. Data will be transmitted via communication channel.

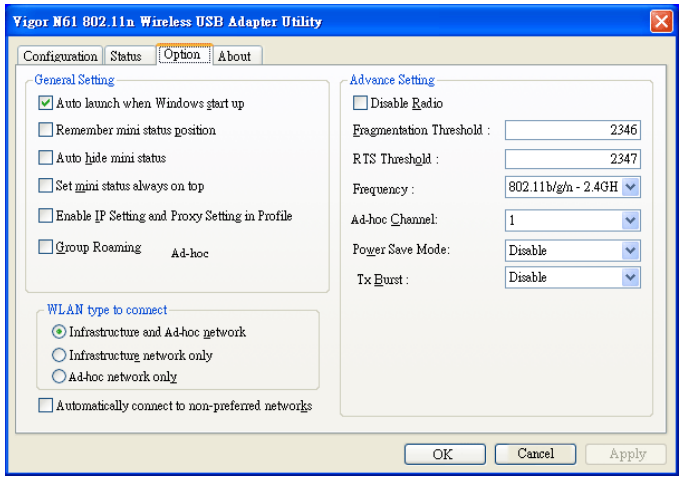
Subnet Choose LAN-A or LAN-B for each SSID.

Security Select WEP, TKIP or AES as the encryption algorithm.

Peer Mac Address Four peer MAC addresses are allowed to be entered in this page at one time.

Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

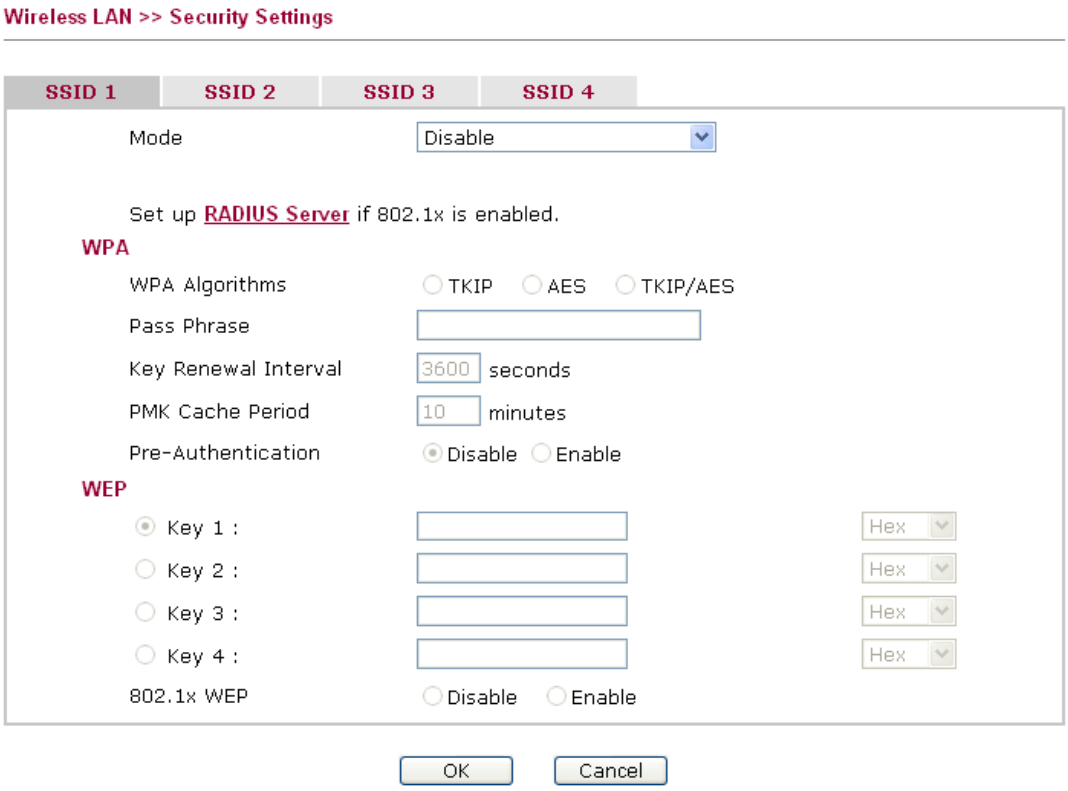


WMM Capable To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

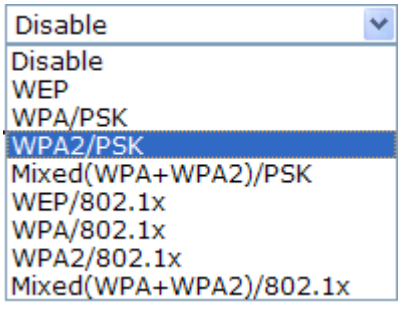
3.7.2 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.



Mode There are several modes provided for you to choose.



Disable - The encryption mechanism is turned off.

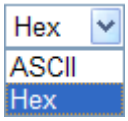
WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.

WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.

WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual

	authentication. It enables centralized remote access authentication for network management. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode. **WPA/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. **WPA2/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for **WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Pass Phrase	Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for **WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for **WPA2/802.1** mode.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed

content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for **WEP** mode.



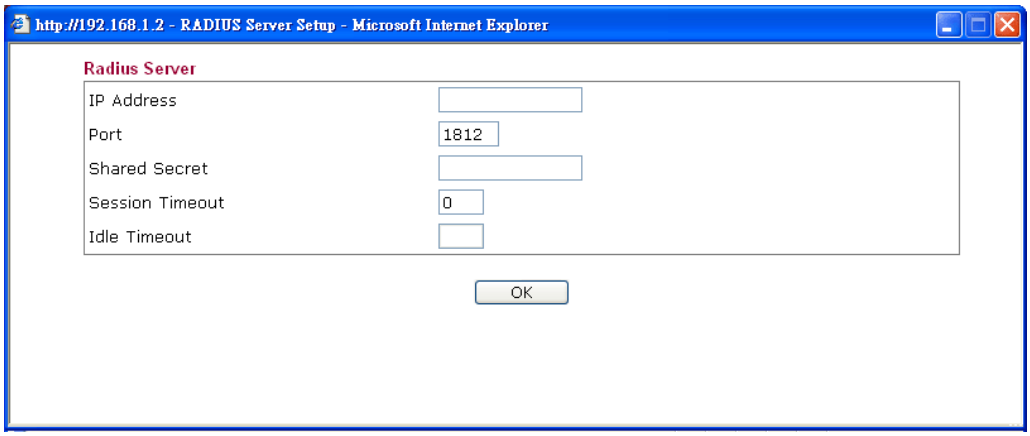
802.1x WEP

Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.

Enable - Enable the WEP Encryption.

Such feature is available for **WEP/802.1x** mode.

Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address Enter the IP address of RADIUS server.

Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

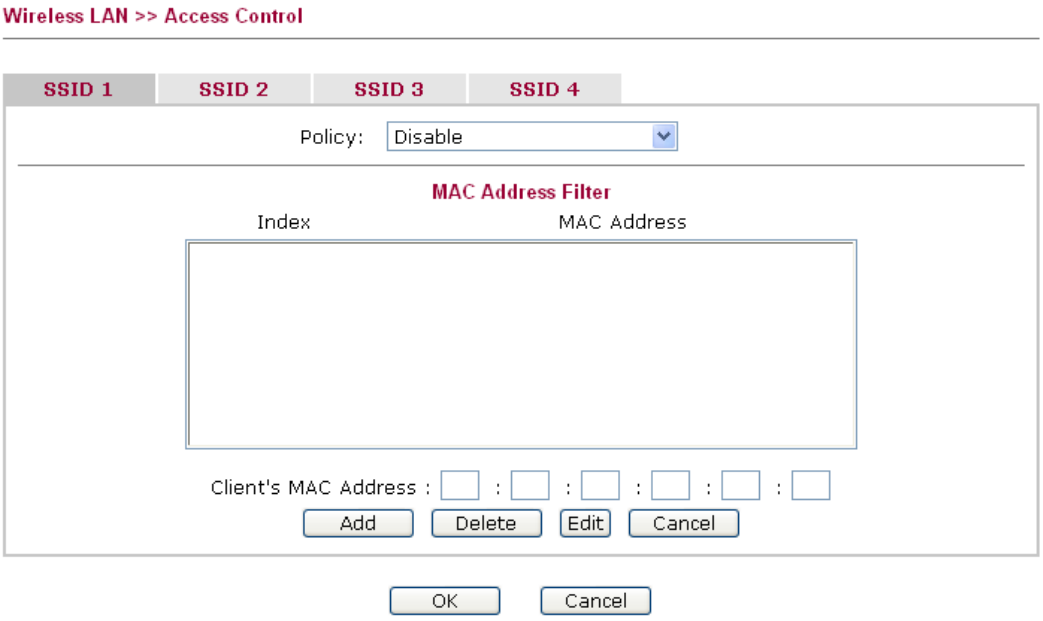
Shared Secret The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

Session Timeout Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

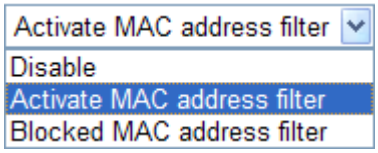
Idle Timeout Set the maximum time that a wireless device may remain idle. (The unit is second.)

3.7.3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).



Policy Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list.



MAC Address Filter Display all MAC addresses that are edited before.

Client's MAC Address Manually enter the MAC address of wireless client.

Add Add a new MAC address into the list.

Delete Delete the selected MAC address in the list.

Edit Edit the selected MAC address in the list.

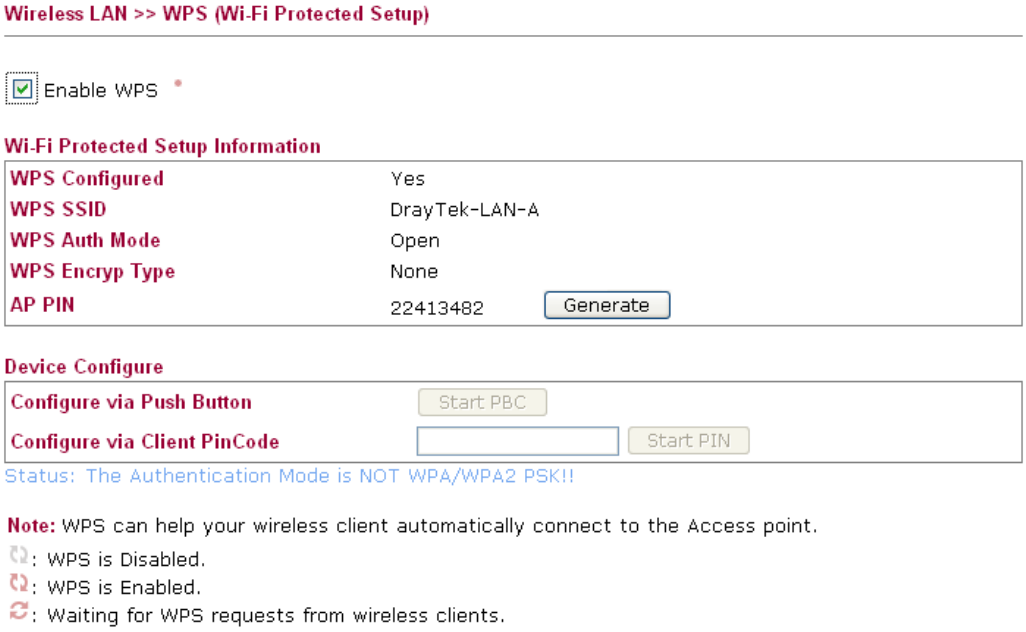
Cancel Give up the access control set up.

OK Click it to save the access control list.

Cancel Clean all entries in the MAC address list.

3.7.4 WPS

Open **Wireless LAN>>WPS** to configure the corresponding settings.

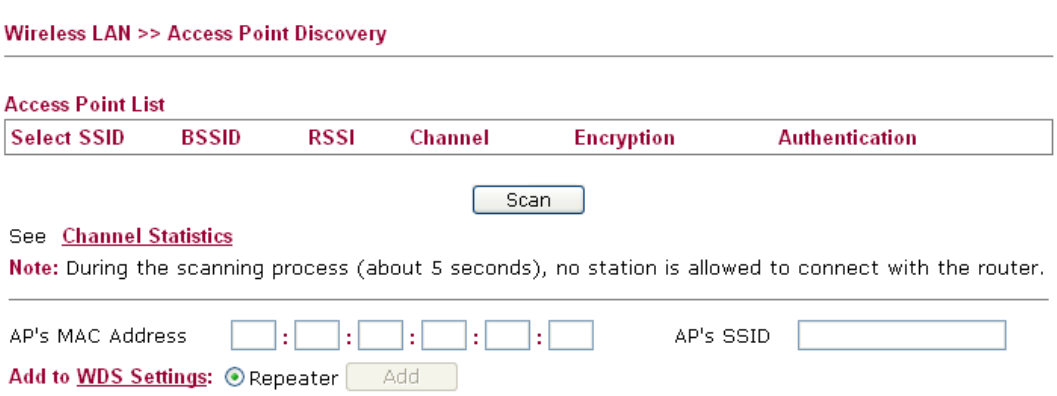


Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of VigorAP 800. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
AP PIN	The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection.
Configure via Push Button	Click **Start PBC** to make a WPS connection within 2 minutes.
Configure via Client PinCode	When using PinCode method, it is required to enter PIN Code (Personal Identification Number Code, 8-digit numbers) into Registrar.

3.7.5 AP Discovery

VigorAP 800 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

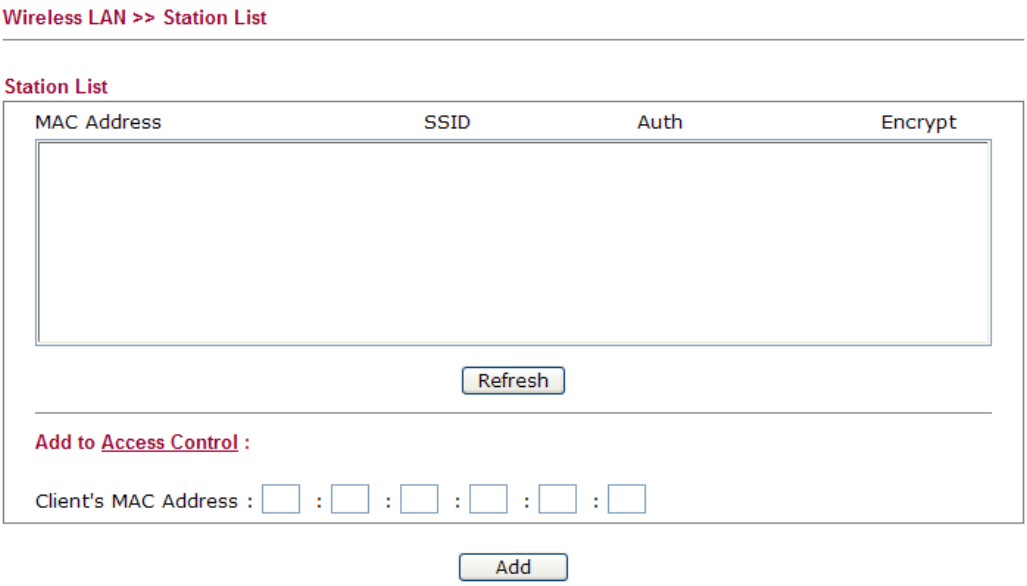
This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 800 can be found. Please click **Scan** to discover all the connected APs.



SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 800.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Add	Click **Repeater** for the specified AP. Next, click **Add**. Later, the MAC address of the AP will be added and be shown on WDS settings page.

3.7.6 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code.



MAC Address	Display the MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	**Client's MAC Address** - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
Add	Click this button to add current typed MAC address into **Access Contro**l.

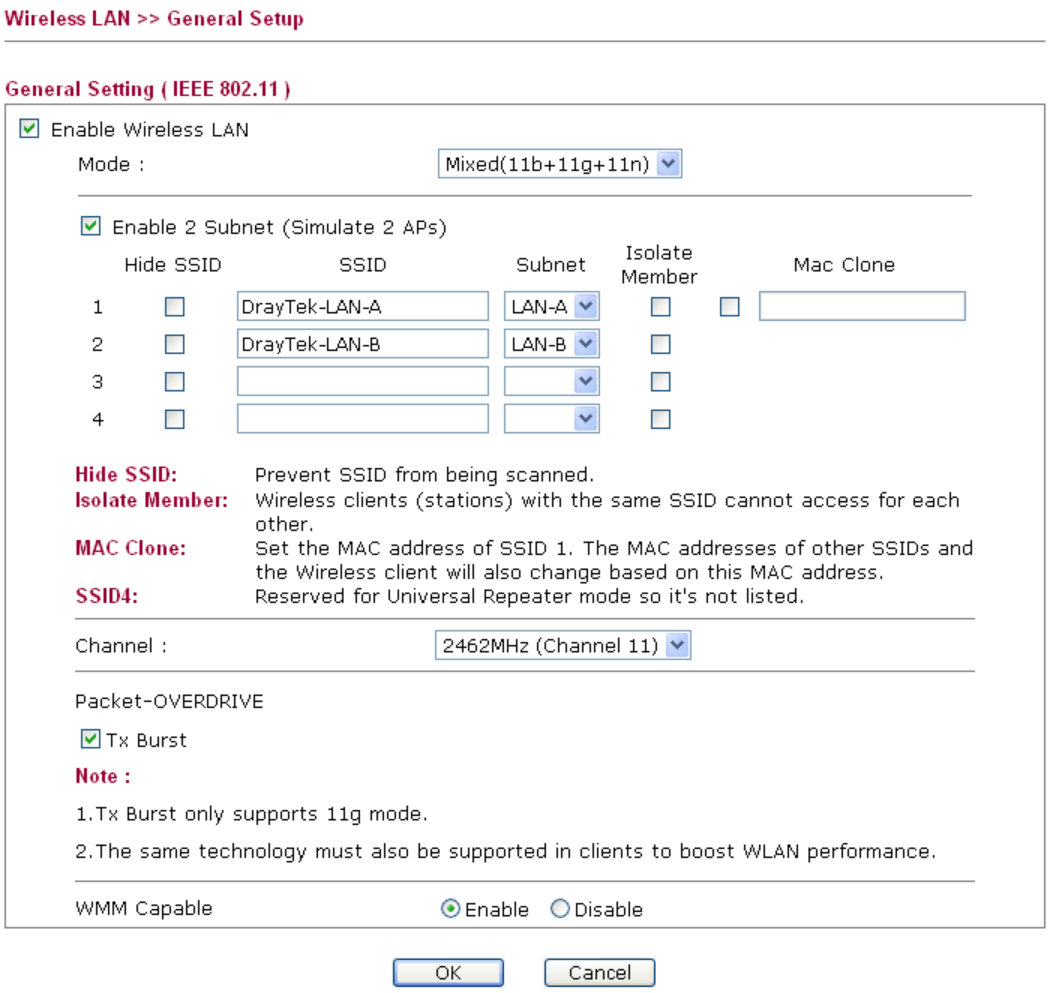
3.8 Wireless LAN Settings for Universal Repeater

When you choose Universal Repeater as the operation mode, the Wireless LAN menu items will include General Setup, Security, WPS, AP Discovery, Universal Repeater and Station List.

3.8.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

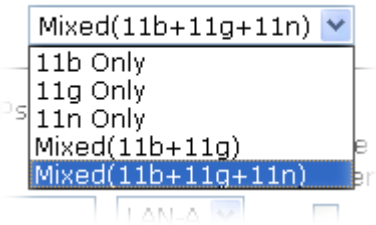
Please refer to the following figure for more information.



Enable Wireless LAN Check the box to enable wireless function.

Mode At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations

simultaneously. Simply choose Mixed (11b+11g+11n) mode.



Enable 2 Subnet (Simulate 2 APs)

Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.

If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment..

Hide SSID

Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 800 while site surveying. The system allows you to set three sets of SSID for different usage.

SSID

Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When **Enable 2 Subnet** is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.

Subnet

Choose LAN-A or LAN-B for each SSID.

Isolate Member

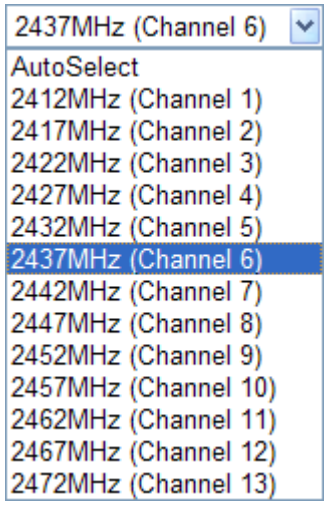
Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.

Mac Clone

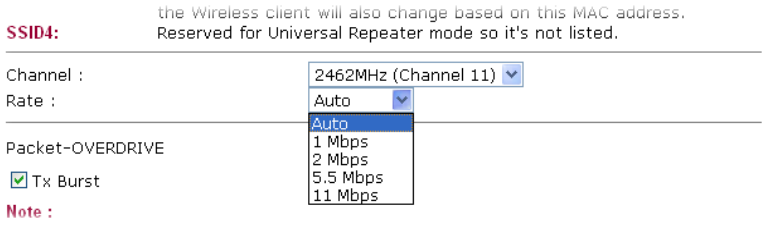
Check this box and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.

Channel

Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let system determine for you.

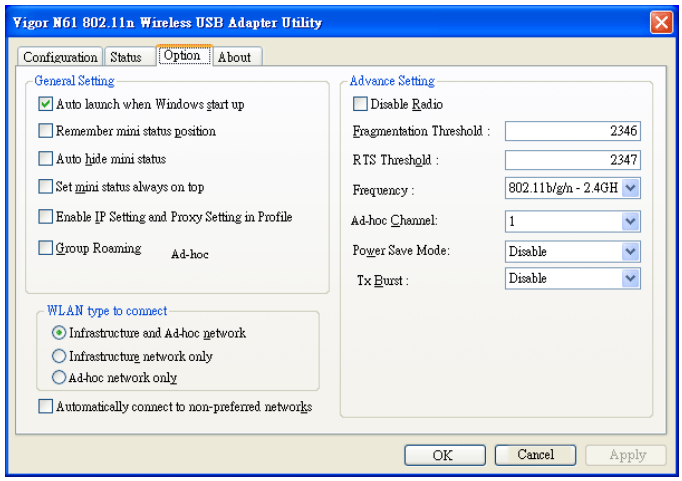


Rate If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.



Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

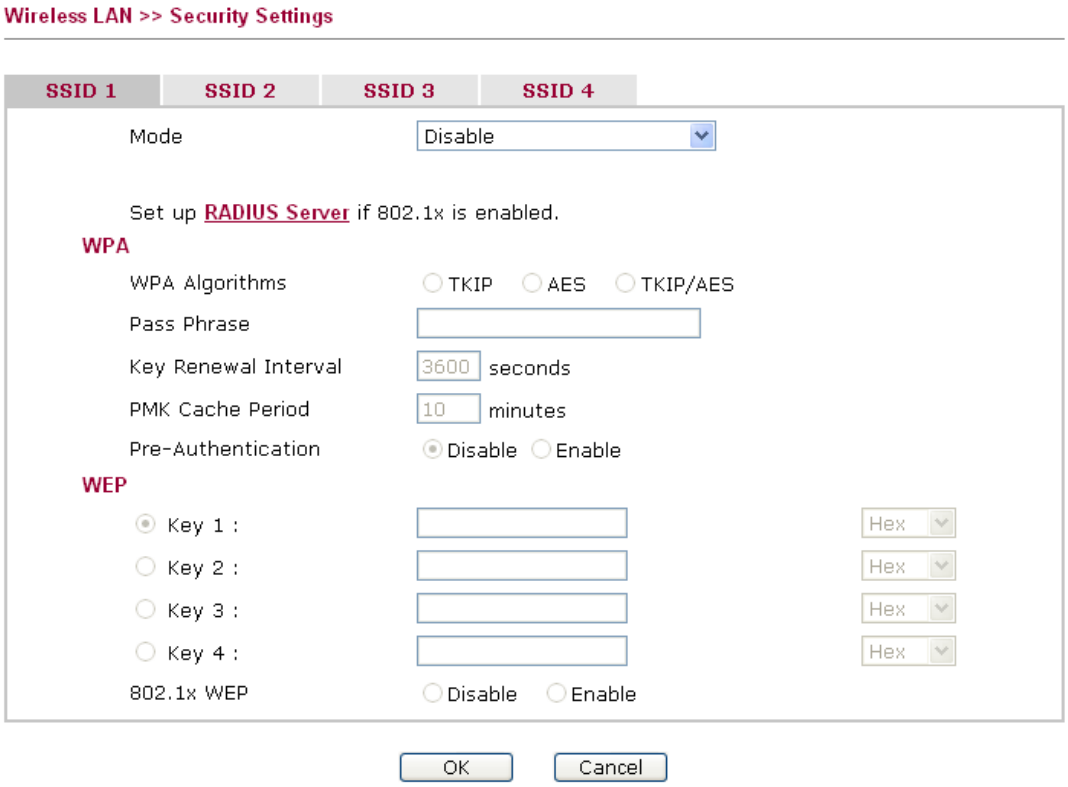


WMM Capable To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

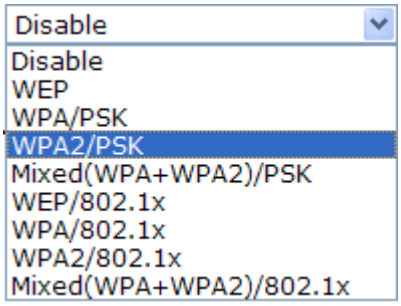
3.8.2 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.



Mode There are several modes provided for you to choose.



Disable - The encryption mechanism is turned off.

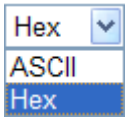
WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.

WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.

WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual

	authentication. It enables centralized remote access authentication for network management. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode. **WPA/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. **WPA2/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for **WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Pass Phrase	Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for **WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for **WPA2/802.1** mode.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed

content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for **WEP** mode.



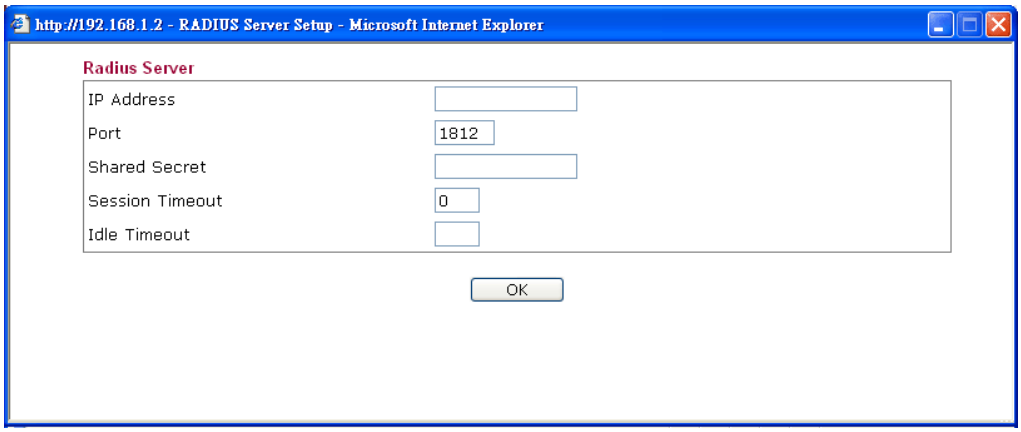
802.1x WEP

Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.

Enable - Enable the WEP Encryption.

Such feature is available for **WEP/802.1x** mode.

Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address Enter the IP address of RADIUS server.

Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

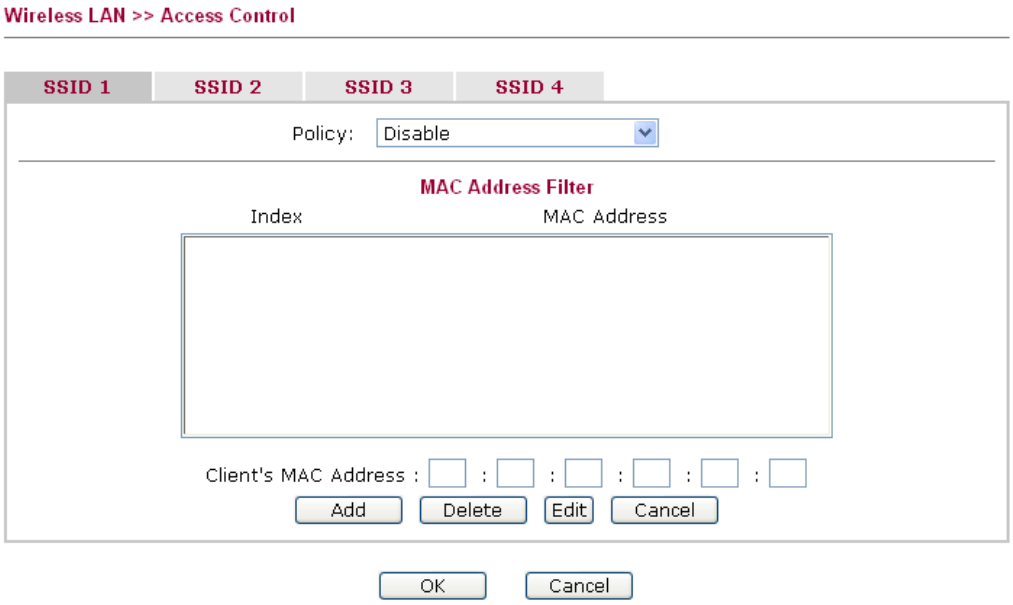
Shared Secret The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

Session Timeout Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

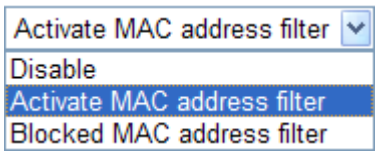
Idle Timeout Set the maximum time that a wireless device may remain idle. (The unit is second.)

3.8.3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).



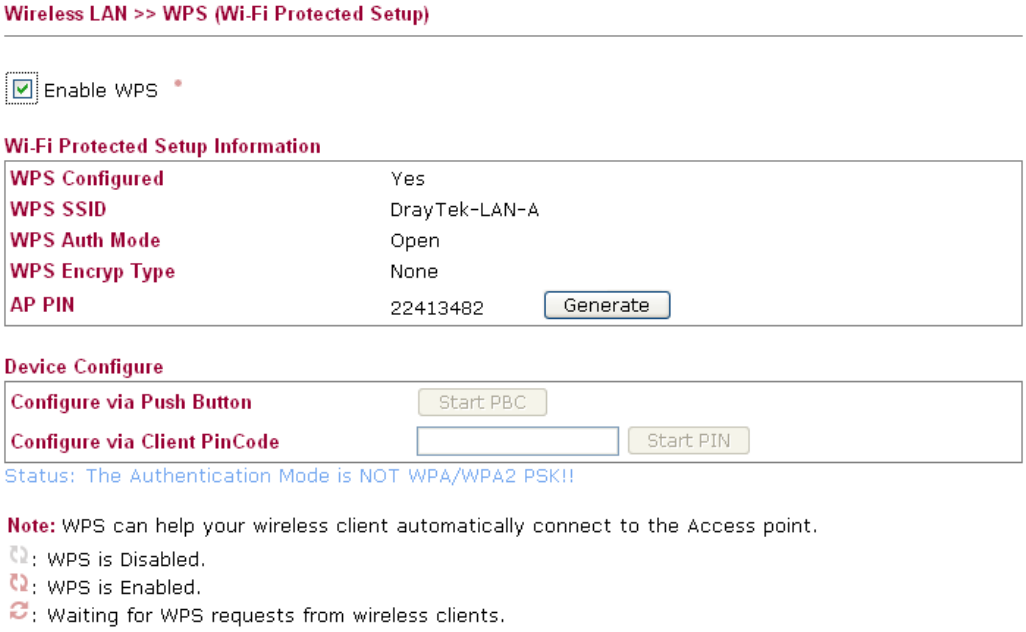
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list.



MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.

3.8.4 WPS

Open **Wireless LAN>>WPS** to configure the corresponding settings.

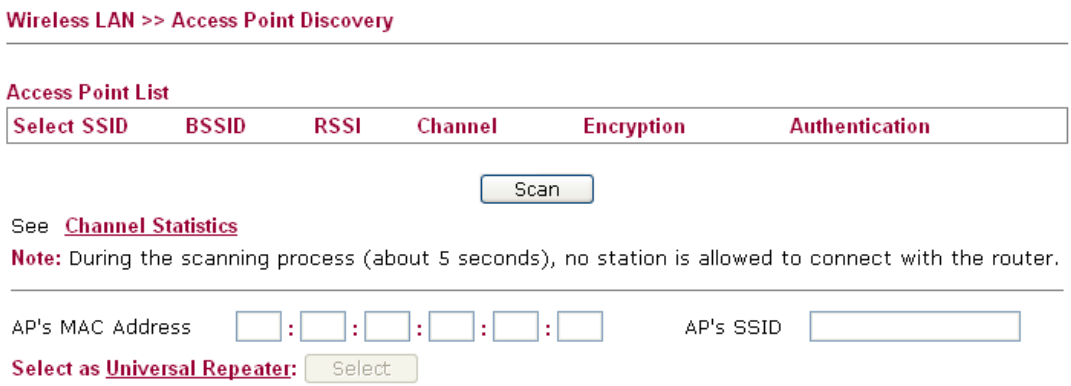


Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of VigorAP 800. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
AP PIN	The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 800 will wait for WPS requests from wireless clients about two minutes. The WPS LED on t VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

3.8.5 AP Discovery

VigorAP 800 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 800 can be found. Please click **Scan** to discover all the connected APs.

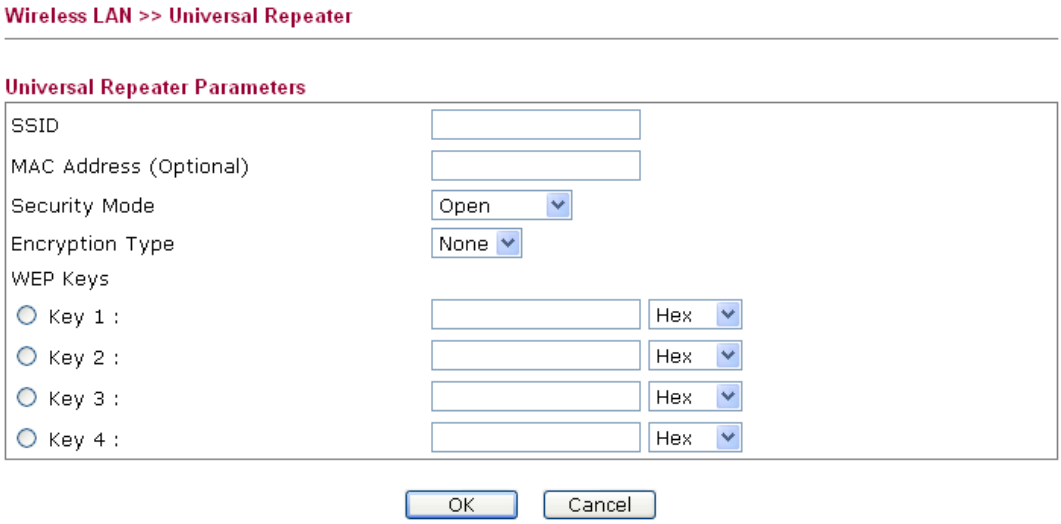


SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 800.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Select as Universal Repeater	In **Universal Repeater** mode, WAN would work as station mode. You can select on wireless AP from the Scan list to connect with it.

3.8.6 Universal Repeater

The access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to serve all wireless stations within its coverage.

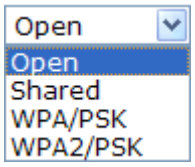
> **Note:** While using **Universal Repeater** mode, the access point will demodulate the received signal. Please check if this signal is noise for the operating network, then have the signal modulated and amplified again. The output power of this mode is the same as that of WDS and normal AP mode.



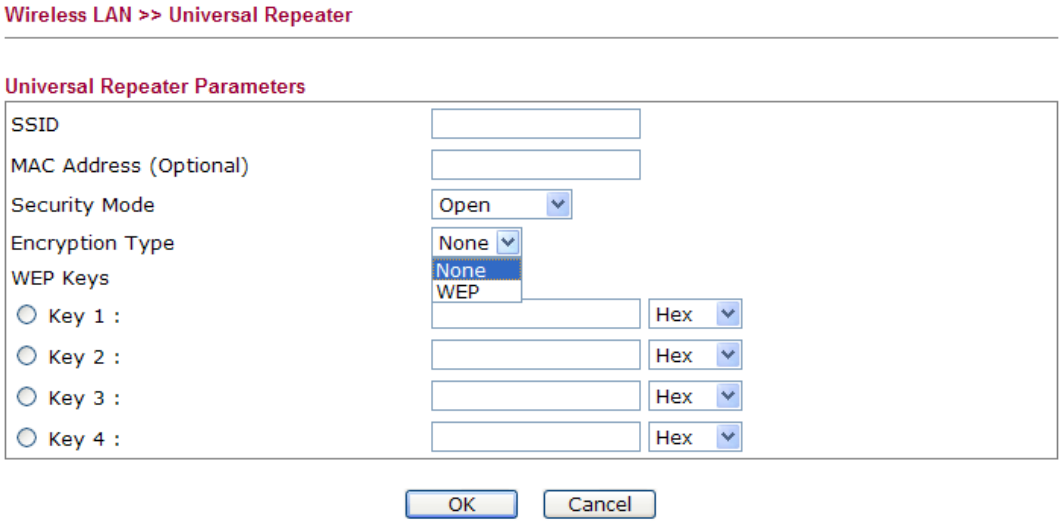
SSID — Set the name of access point that VigorAP800 wants to connect to.

MAC Address (Optional) — Type the MAC address of access point that VigorAP800 wants to connect to.

Security Mode — There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.

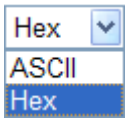


Open / Shared Mode

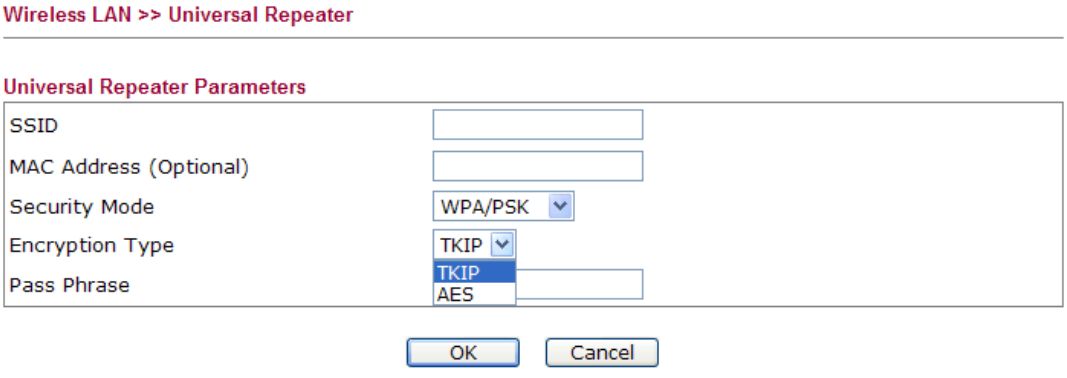


Encryption Type Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose **WEP**.

WEP Keys Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.



WPA/PSK Mode and WPA2/PSK Mode

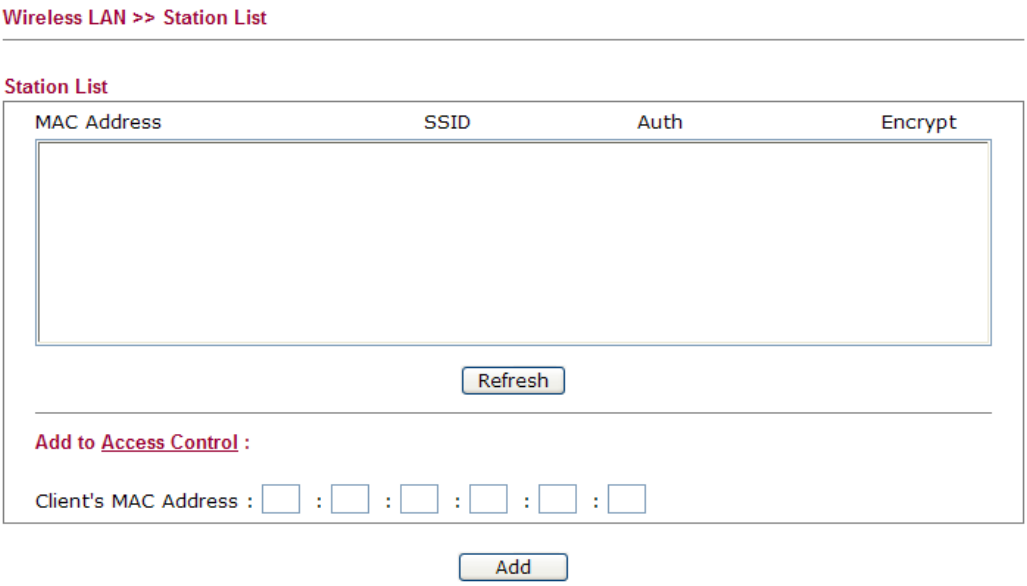


Encryption Type Select TKIP or AES as the algorithm for WPA.

Pass Phrase Either **8~63** ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

3.8.7 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code.

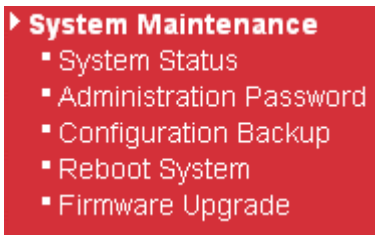


MAC Address	Display the MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	**Client's MAC Address** - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
Add	Click this button to add current typed MAC address into **Access Contro**l.

3.9 System Maintenance

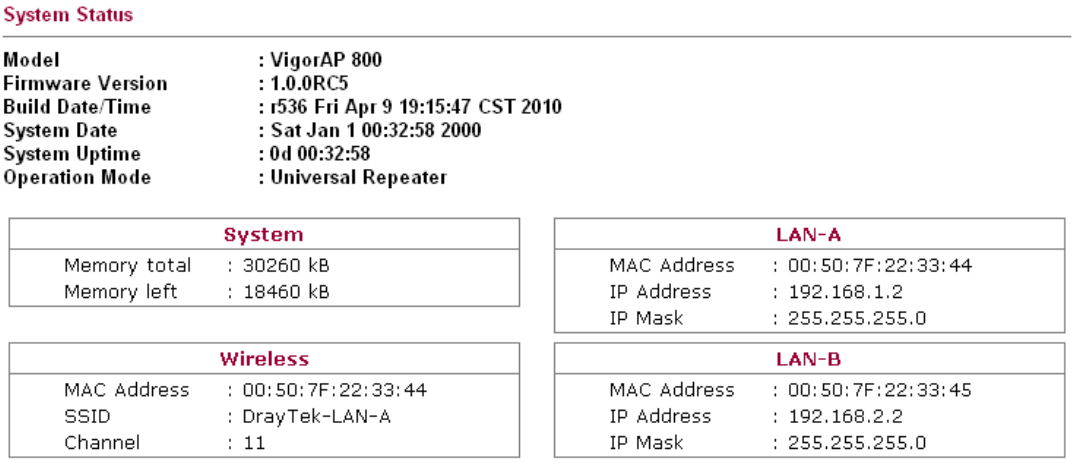
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.9.1 System Status

The **System Status** provides basic network settings of Vigor modem. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

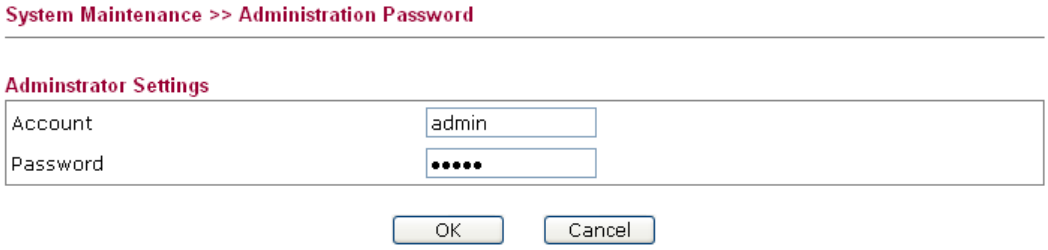


Model Name	Display the model name of the modem.
Firmware Version	Display the firmware version of the modem.
Build Date/Time	Display the date and time of the current firmware build.
System Date	Display the date and time when such device connects to Internet.
System Uptime	Display the period that such device connects to Internet.
Operation Mode	Display the operation mode that the device used.
System **-------**	
Memory total	Display the total memory of your system.
Memory left	Display the remaining memory of your system.
LAN**-------**	
MAC Address	Display the MAC address of the LAN Interface.
IP Address	Display the IP address of the LAN interface.

IP Mask	Display the subnet mask address of the LAN interface.
Wireless-------	
MAC Address	Display the MAC address of the WAN Interface.
SSID	Display the SSID of the device.
Channel	Display the channel that the station used for connecting with such device.

3.9.2 Administrator Password

This page allows you to set new password.



Account	Type the name for accessing into Web User Interface.
Password	Type in new password in this filed.

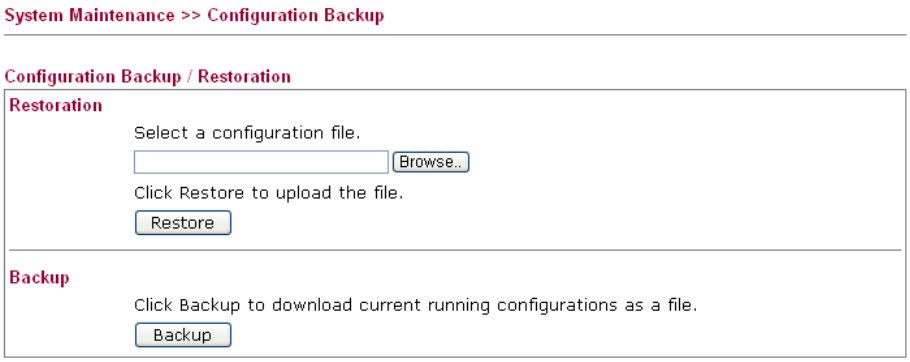
When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

3.9.3 Configuration Backup

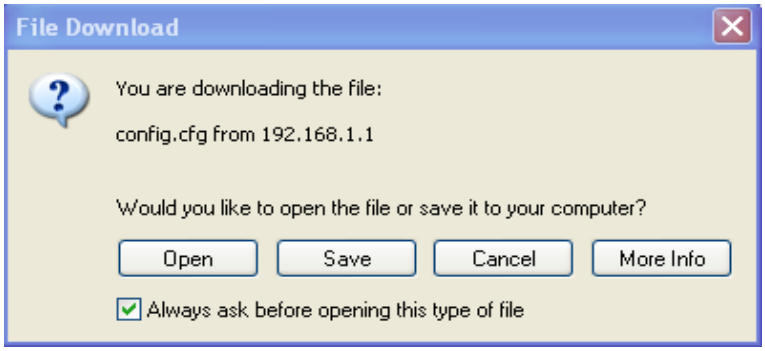
Backup the Configuration

Follow the steps below to backup your configuration.

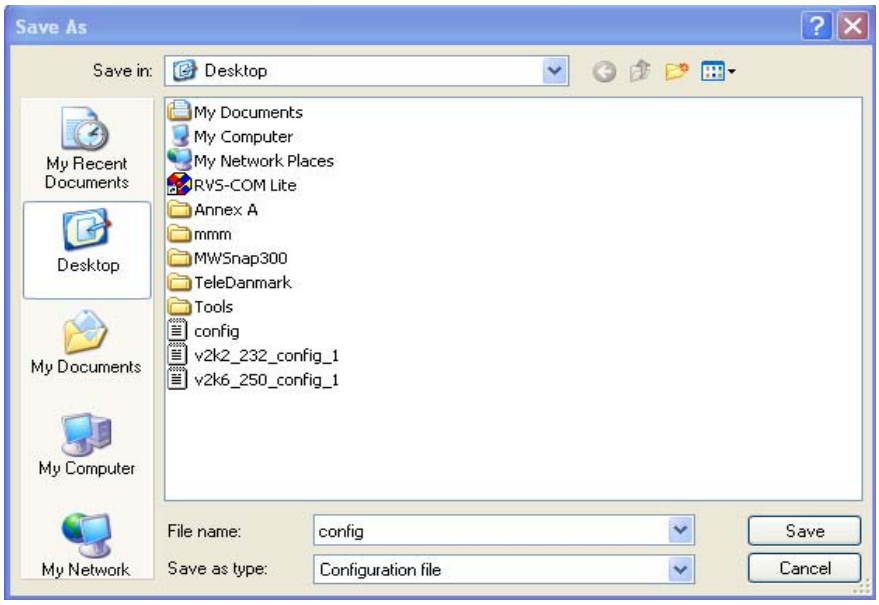
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



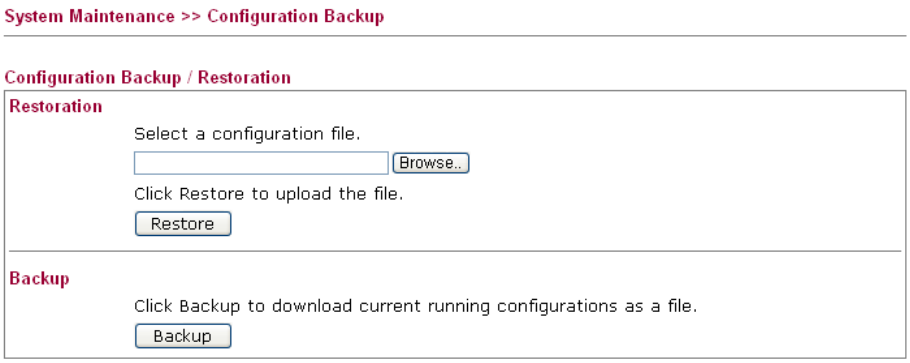
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Note: Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

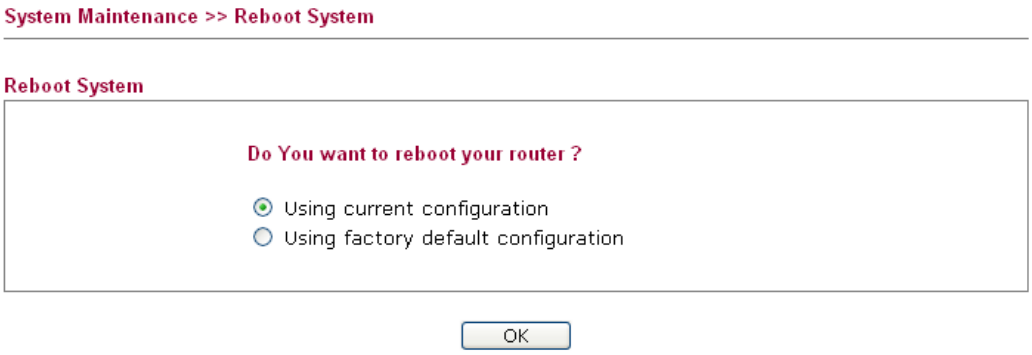
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Browse** button to choose the correct configuration file for uploading to the modem.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

3.9.4 Reboot System

The Web Configurator may be used to restart your modem. Click **Reboot System** from **System Maintenance** to open the following page.



If you want to reboot the modem using the current configuration, check **Using current configuration** and click **OK**. To reset the modem settings to default values, check **Using factory default configuration** and click **OK**. The modem will take 5 seconds to reboot the system.

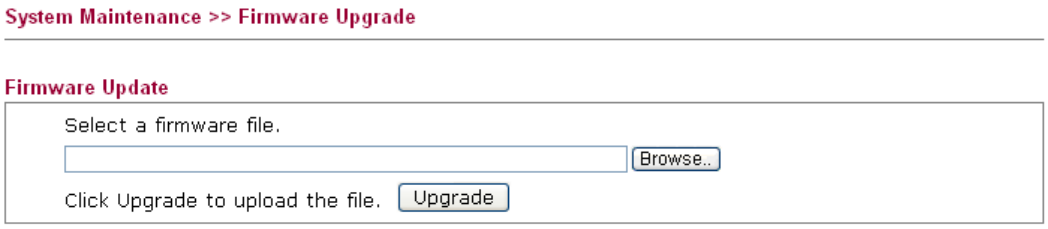
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your modem for ensuring normal operation and preventing unexpected errors of the modem in the future.

3.9.5 Firmware Upgrade

Before upgrading your modem firmware, you need to install the Modem Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

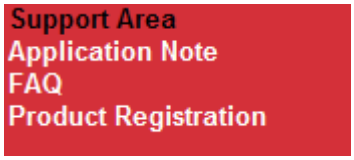
Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.



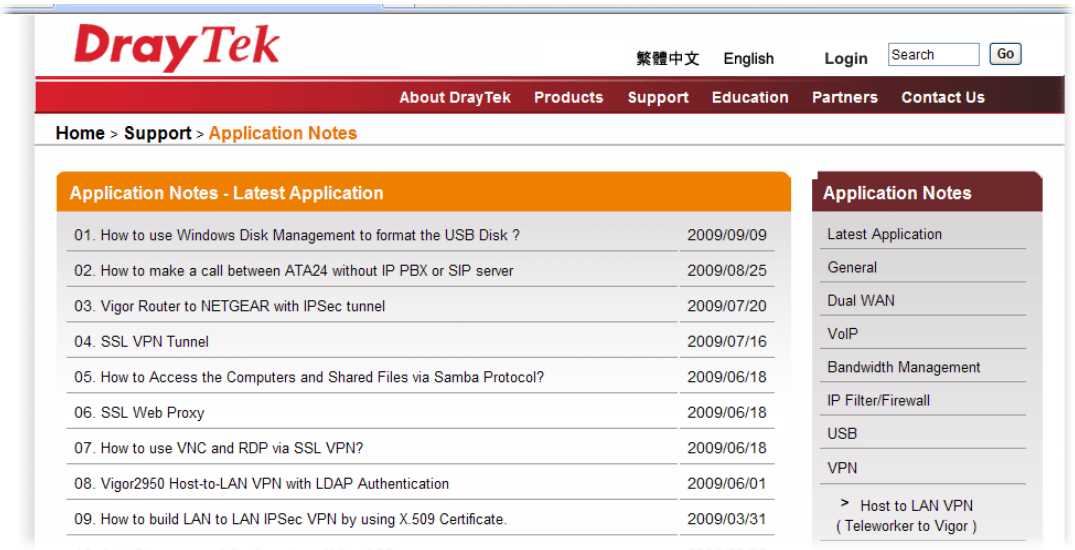
Click **Upgrade**.

3.10 Support Area

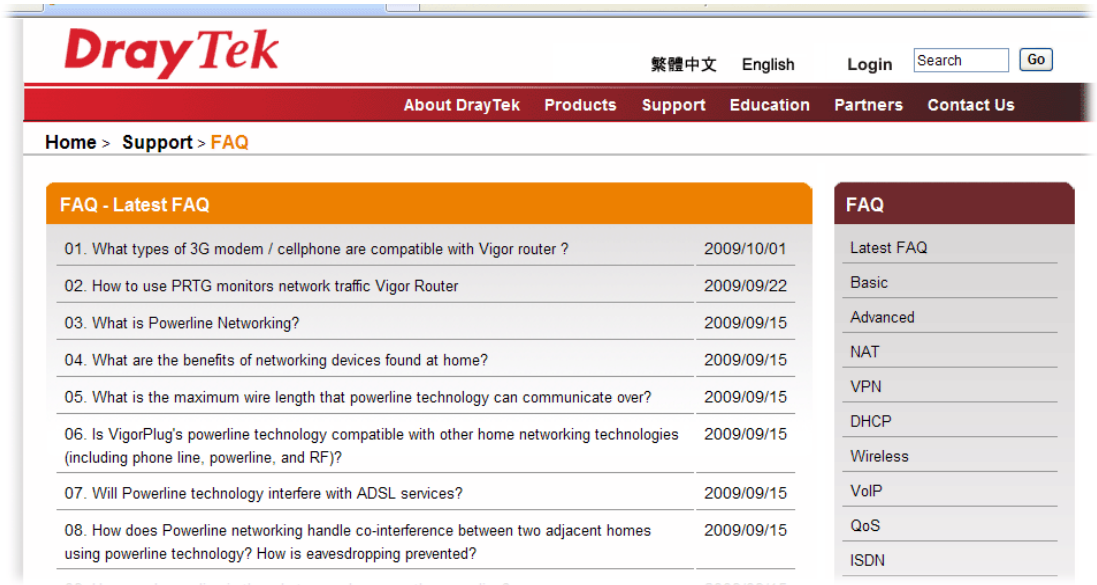
When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



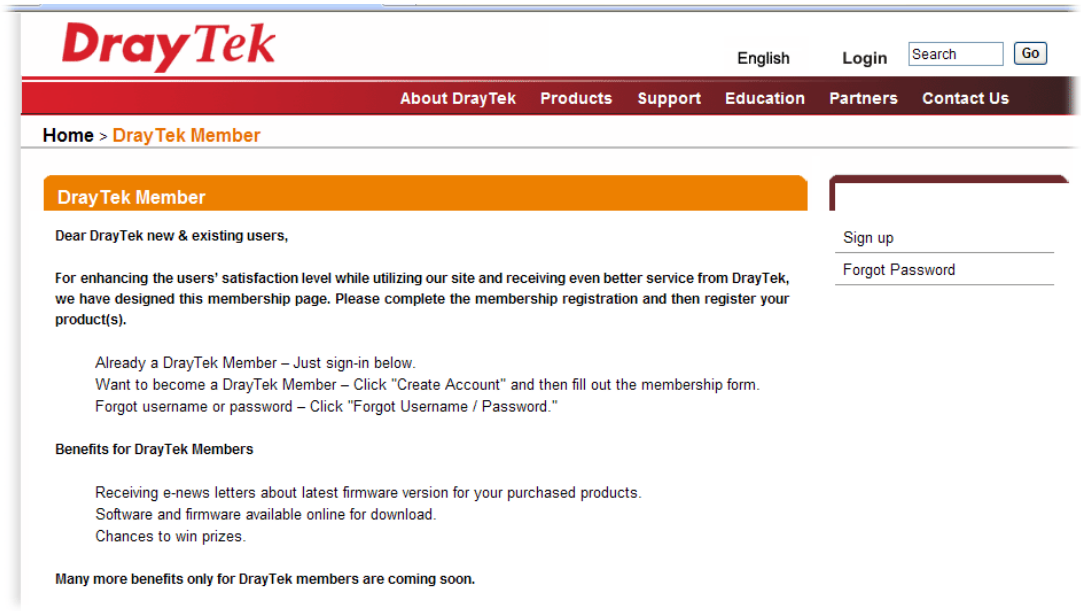
Click **Support Area>>Application Note**, the following web page will be displayed.



Click **Support Area>>FAQ**, the following web page will be displayed.



Click **Support Area>>Product Registration**, the following web page will be displayed.

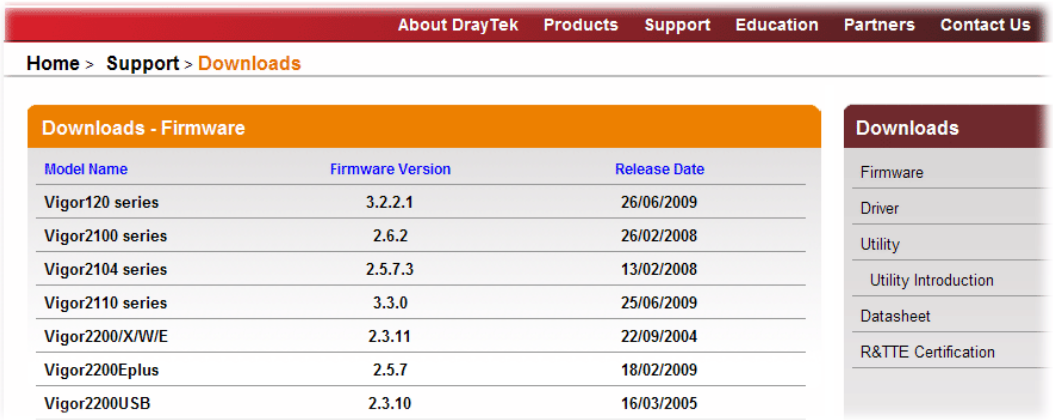


4 Application and Examples

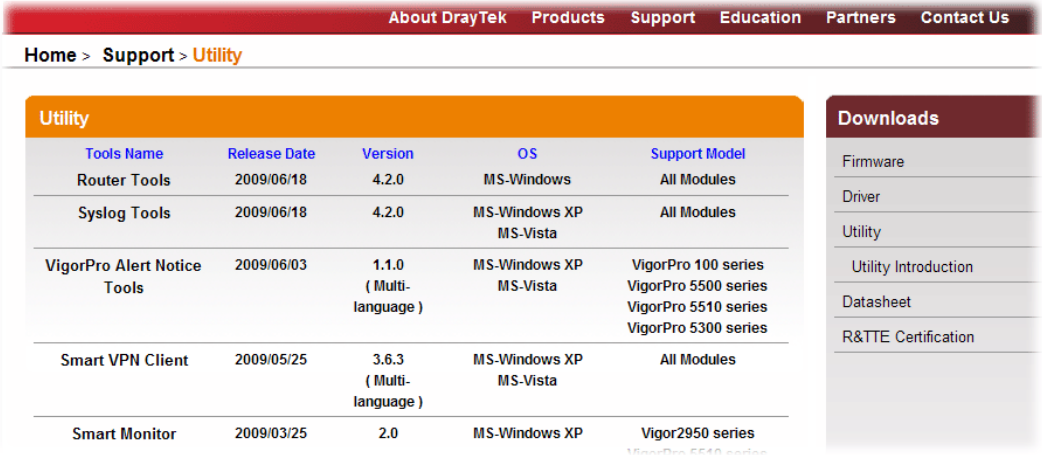
4.1 Upgrade Firmware for Your Modem

Before upgrading your router firmware, you need to install the Router Tools. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.

1. Go to **www.draytek.com.**
2. Access into **Support >> Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

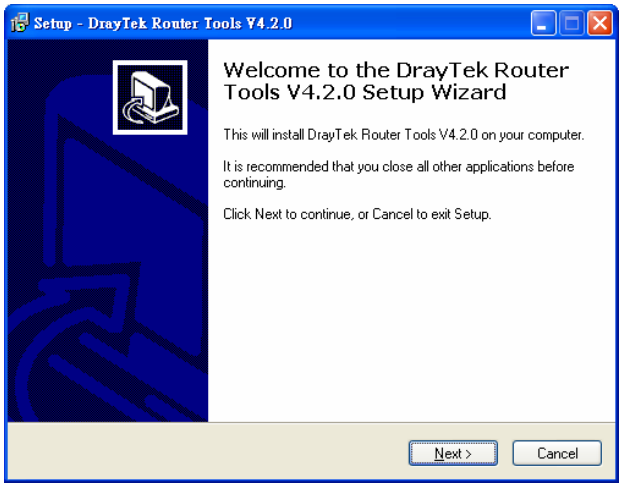


3. Access into **Support >> Downloads**. Please find out **Utility** menu and click it.



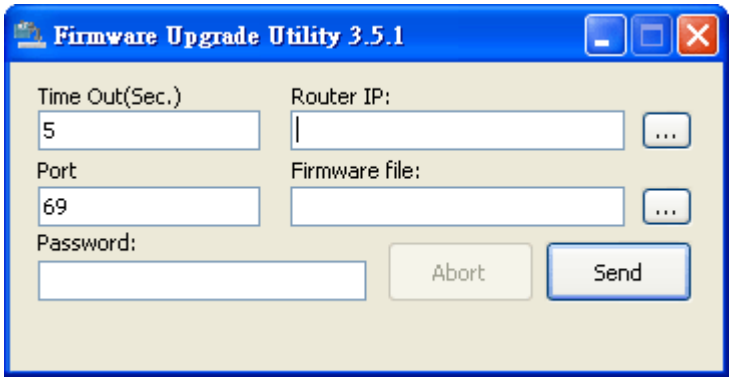
4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

5. Double click on the icon of modem tool. The setup wizard will appear.



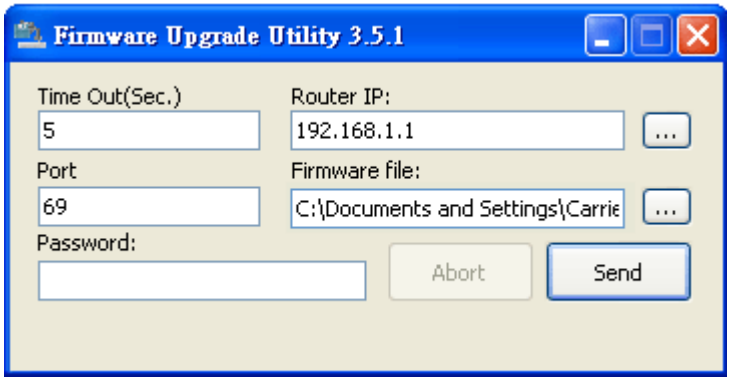
6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.

7. From the **Start** menu, open **Programs** and choose **Modem Tools XXX** >> **Firmware Upgrade Utility**.

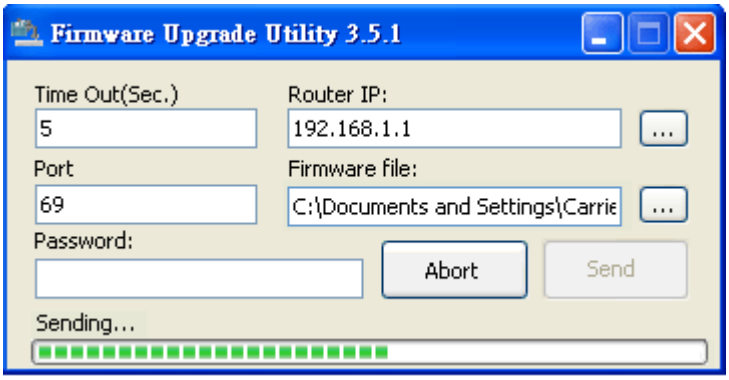


8. Type in your modem IP, usually **192.168.1.1**.

9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.



10. Click **Send**.



11. Now the firmware update is finished.

This page is left blank.

5 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the modem and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the modem from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the modem still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and cable connections.
   Refer to "**1.3 Hardware Installation"** for details.
2. Power on the modem. Make sure the **POWER** LED**, ACT** LED and **LAN** LED are bright.
3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

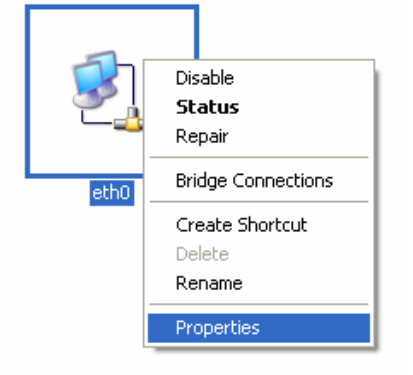
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

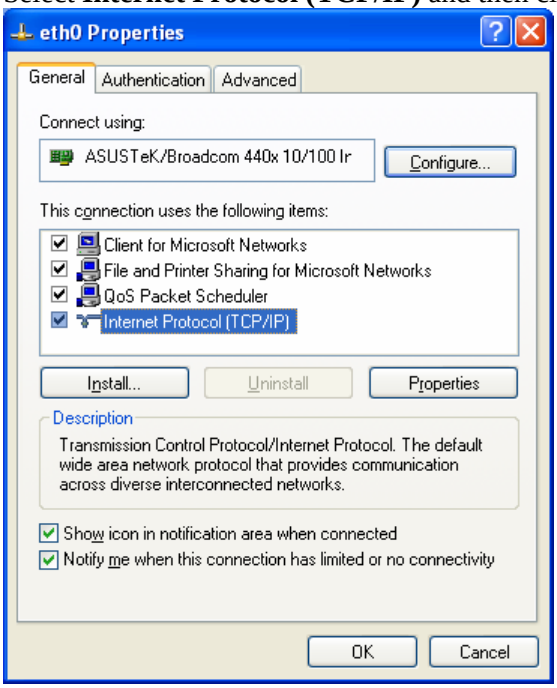
The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Go to **Control Panel** and then double-click on **Network Connections**.

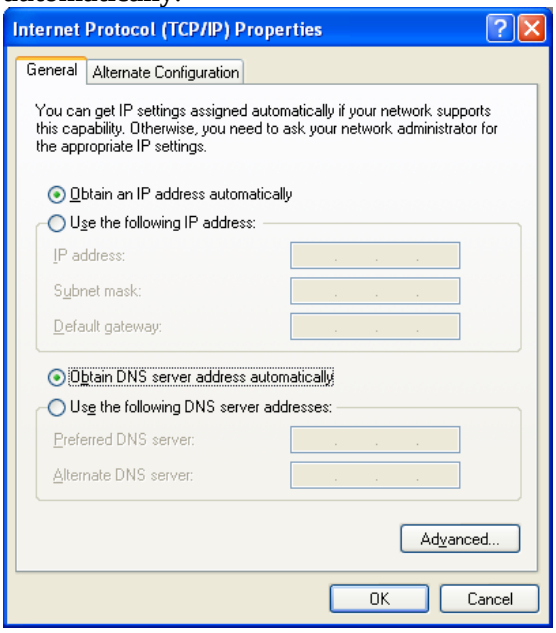
2. Right-click on **Local Area Connection** and click on **Properties**.



3. Select **Internet Protocol (TCP/IP)** and then click **Properties**.

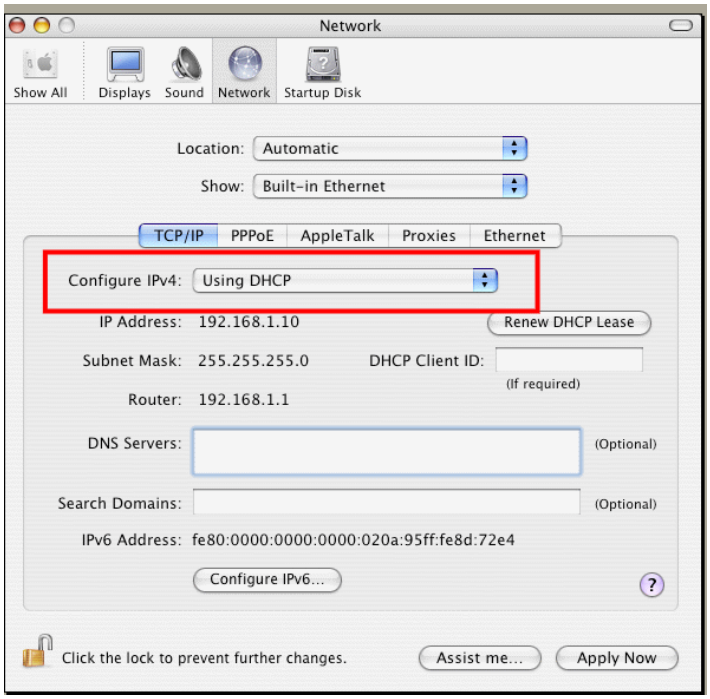


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



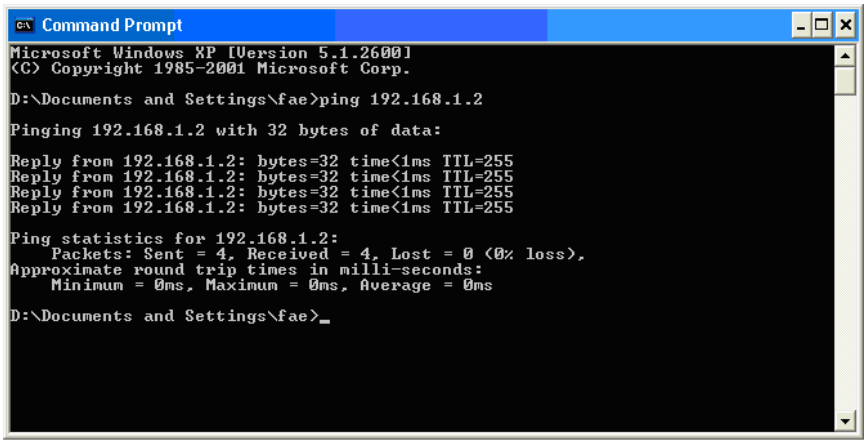
5.3 Pinging the Modem from Your Computer

The default gateway IP address of the modem is 192.168.1.2. For some reason, you might need to use "ping" command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.2.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the modem correctly.

For Windows

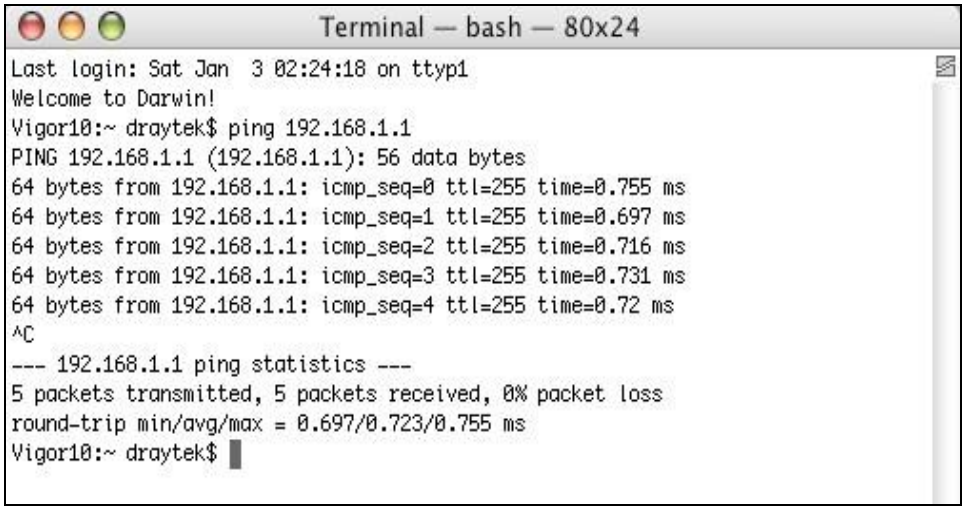
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



3. Type ping 192.168.1.2 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For MacOs (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.



5.4 Backing to Factory Default Setting If Necessary

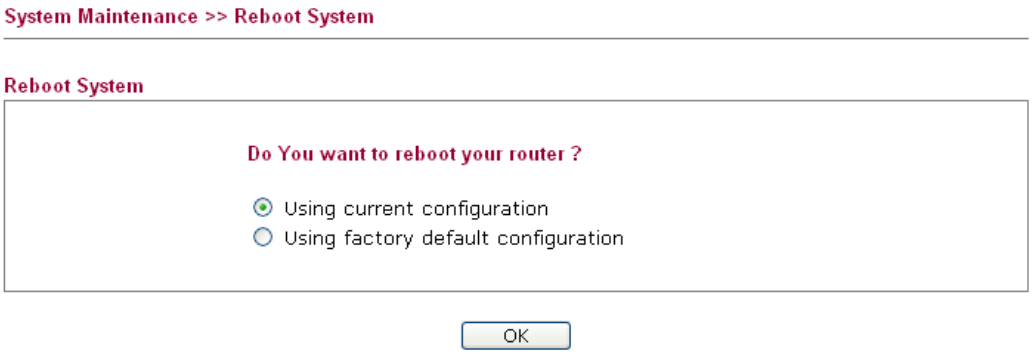
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware.

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

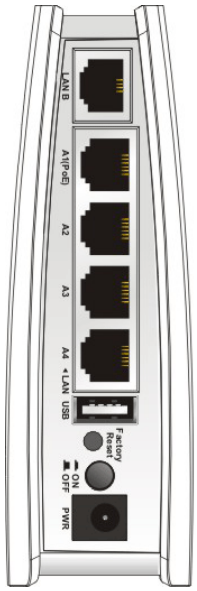
You can reset the modem to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the modem will return all the settings to the factory settings.



Hardware Reset

While the modem is running, press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the modem will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the modem again to fit your personal request.

5.6 Contacting Your Dealer

If the modem still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.