DrayTek

VigorAP 900

Concurrent Dual Band AP

Your reliable networking solutions partner

User's Guide

V1.0

VigorAP 900
Concurrent Dual Band AP
User's Guide

Version: 1.0

Firmware Version: V1.1.0_RC4a

Date: 12/08/2013

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, Hsinchu County, Taiwan 303
Product: VigorAP 900

DrayTek Corp. declares that VigorAP 900 is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC, ErP 2009/125/EC and RoHS 2011/65/EU.

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/5GHz WLAN network throughout the EC region and Switzerland with restrictions in France.

Please visit http://www.draytek.com/user/SupportDLRTTECE.php

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

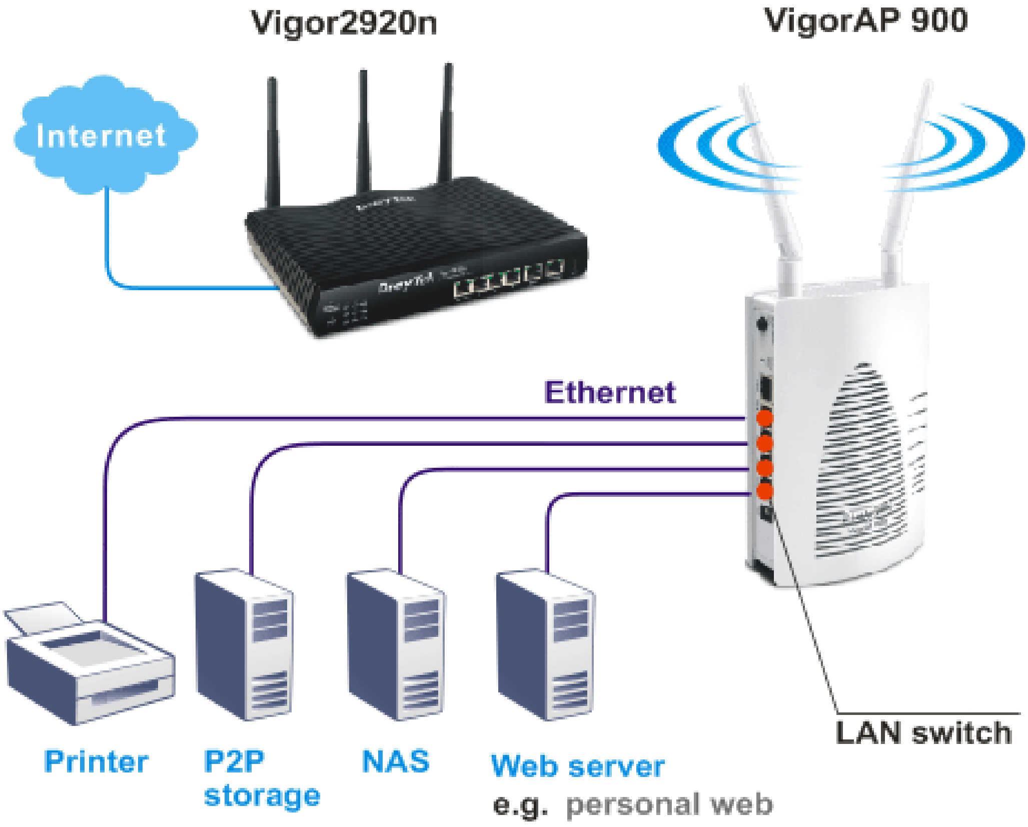
1 Preface

1.1 Introduction

Thank you for purchasing this VigorAP 900, the concurrent dual band wireless (2.4G/5G) access point offering high-speed data transmission. With this high cost-efficiency VigorAP 900, computers and wireless devices which are compatible with 802.11n/802.11a can connect to existing wired Ethernet network via this VigorAP 900, at the speed of 300Mbps.

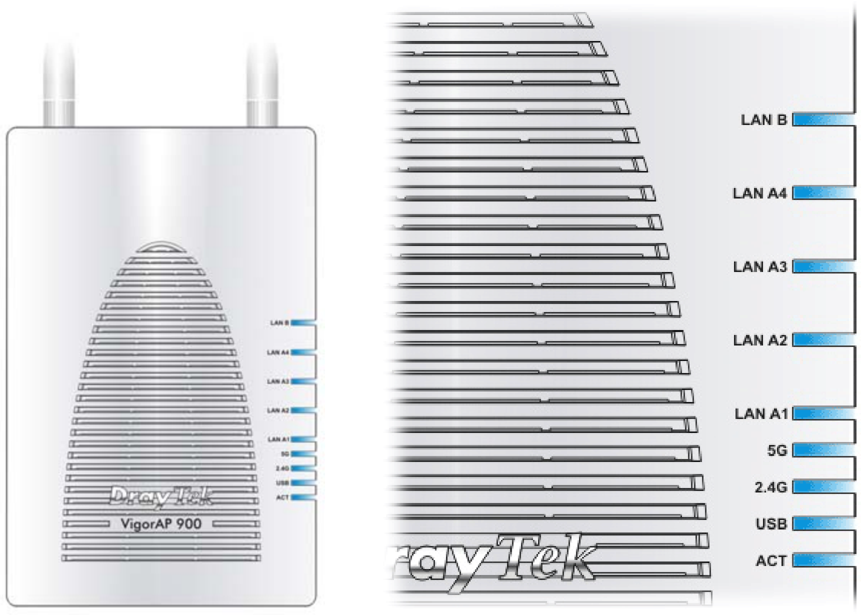
Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced users. Just follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

VigorAP 900 also is a Power over Ethernet Powered Device which adopts the technology of PoE for offering power supply and transmitting data through the Ethernet cable.

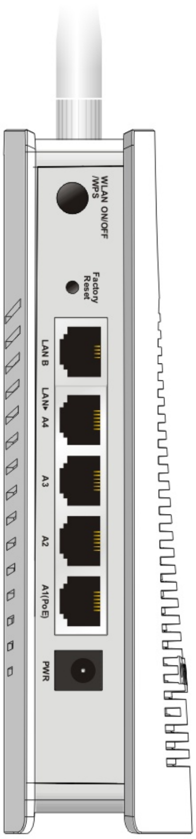
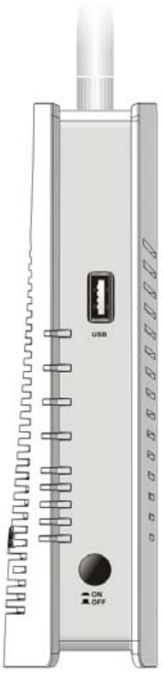
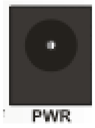


1.2 LED Indicators and Connectors

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.
2.4G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
5G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
LAN A1 - A4	On	A normal connection (rate with 100M/1000M) is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
LAN B	On	A normal connection (rate with 100M/1000M) is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).

	Interface	Description
 WLAN ON/OFF /WPS Factory Reset LAN B LAN A4 A3 A2 A1(PoE) PWR	● WPS Button	Press the button quickly (less than 2 seconds) to wait for client device making network connection (2.4G) through WPS. Press the button more than 2 seconds to turn on or turn off the wireless network connection.
		Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 6 seconds. Then the router will restart with the factory default configuration.
	LAN B	Connecter for xDSL / Cable modem (Giga level) or router.
	LAN A1 (PoE) - A4	Connecter for xDSL / Cable modem (Giga level) / computer or router.
		PWR: Connecter for a power adapter.
	USB	Connector for a printer.
		ON/OFF: Power switch.

1.3 Hardware Installation

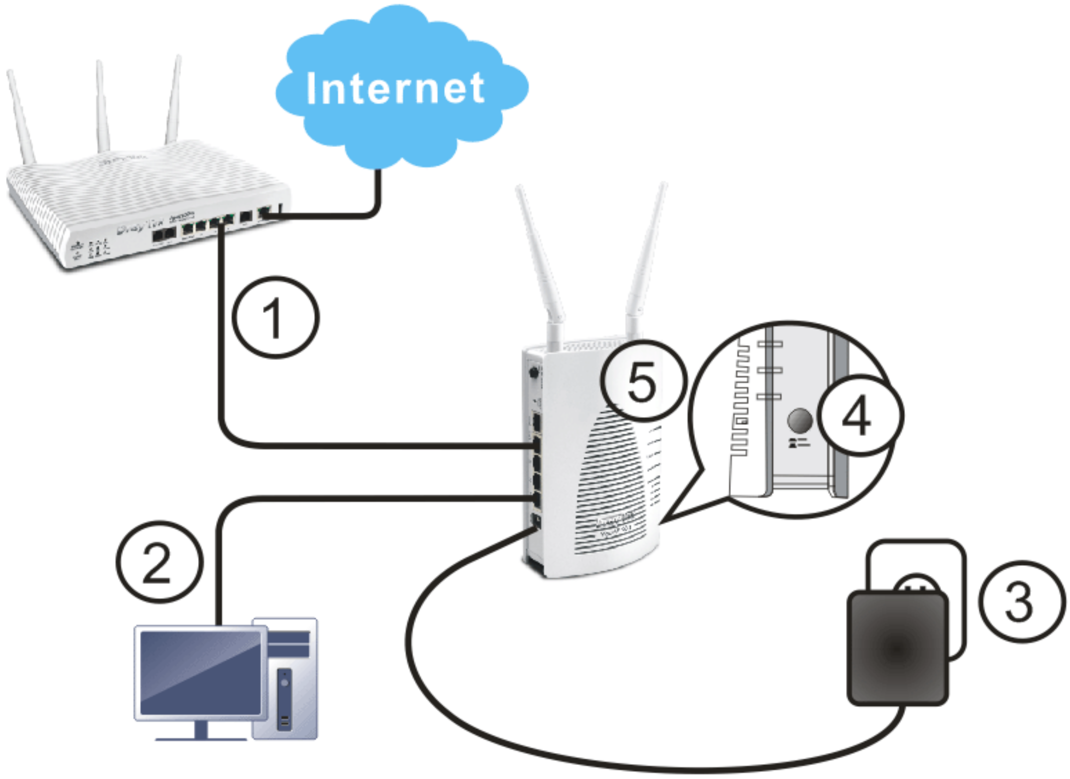
This section will guide you to install the VigorAP 900 through hardware connection and configure the device's settings through web browser.

Before starting to configure VigorAP 900, you have to connect your devices correctly.

1.3.1 Wired Connection for PC in LAN

1. Connect VigorAP 900 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 900 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 900.
5. Check all LEDs on the front panel. **ACT** LED should blink and **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem or router.

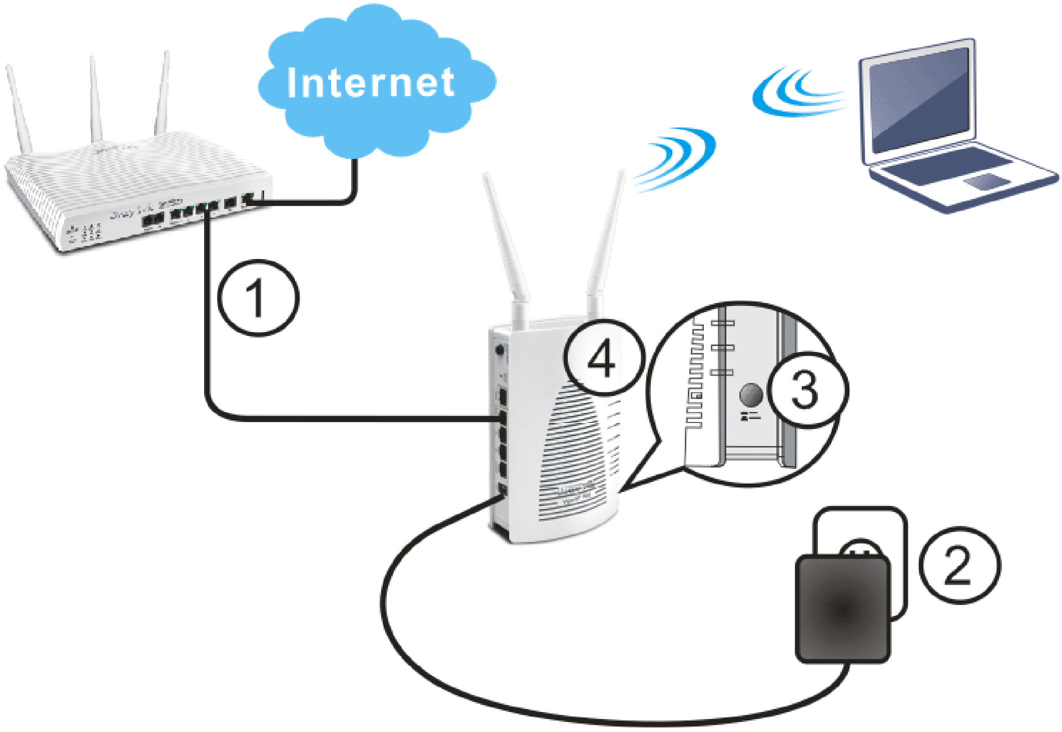
(For the detailed information of LED status, please refer to section 1.2.)



1.3.2 Wired Connection for Notebook in WLAN

1. Connect VigorAP 900 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 900.
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.)

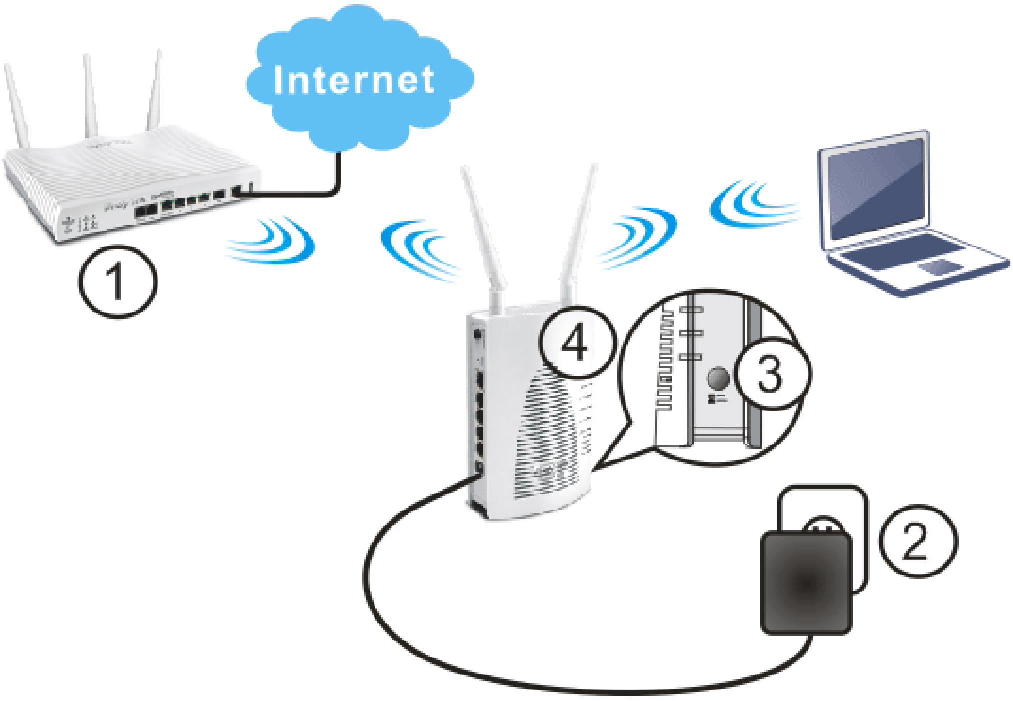


1.3.3 Wireless Connection

VigorAP 900 can access Internet via an ADSL modem, router, or switch/hub in your network through wireless connection.

1. Connect VigorAP 900 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 900.
4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if VigorAP 900 is correctly connected to the ADSL modem, router or switch/hub.

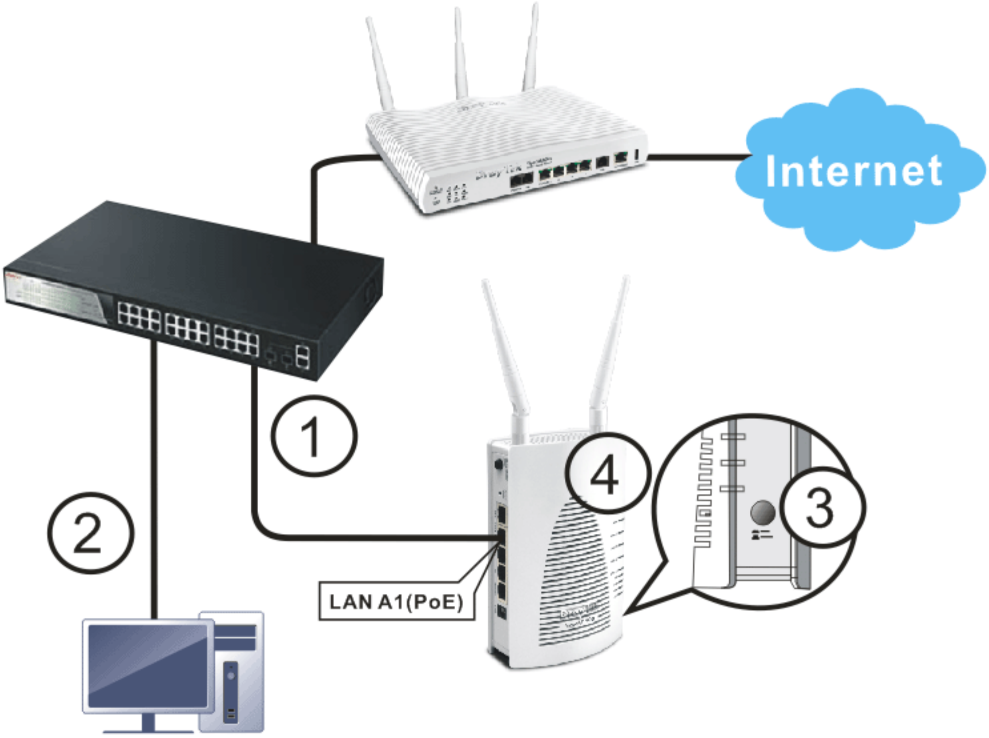
(For the detailed information of LED status, please refer to section 1.2.)



1.3.4 POE Connection

VigorAP 900 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 900 to a switch in your network through the **LAN A1 (PoE)** port of the access point by Ethernet cable.
2. Connect a computer to VigorSwitch P2260. Make sure the subnet IP address of the PC is the same as VigorAP 900 management IP, e.g., **192.168.1.X**.
3. Power on VigorAP 900.
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 900 with proper network parameters, so it can work properly in your network environment.

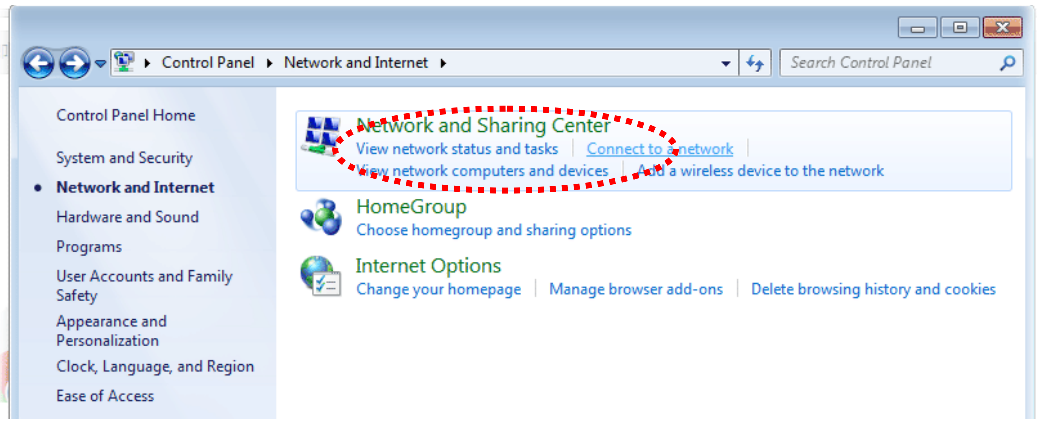
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic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

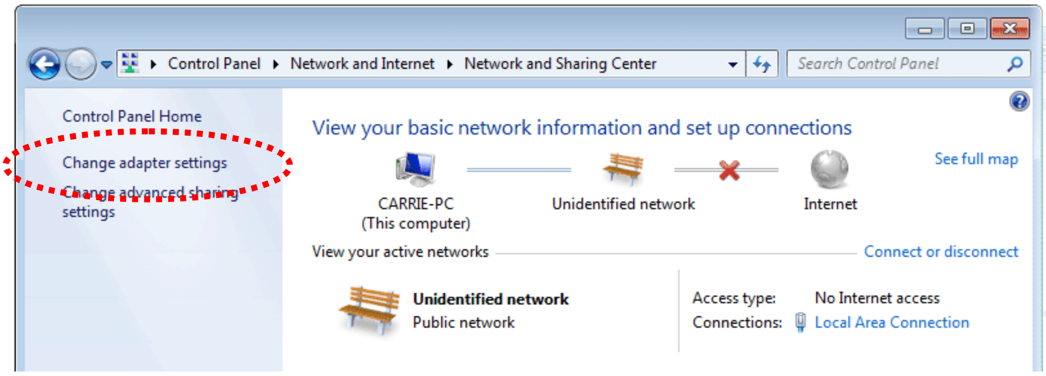
Windows 7	**- please go to section 2.1**
Windows 2000	**- please go to section 2.2**
Windows XP	**- please go to section 2.3**
Windows Vista	**- please go to section 2.4**

2.1 Windows 7 IP Address Setup

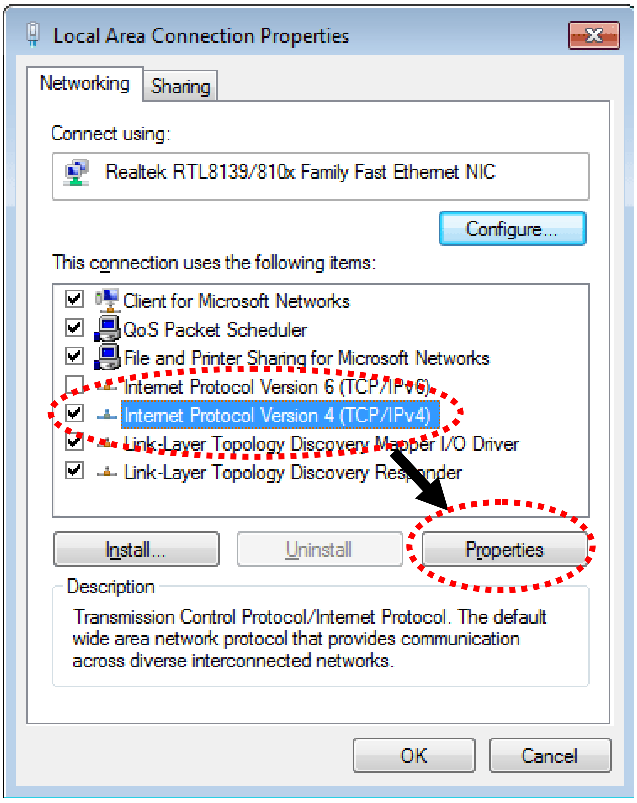
Click **Start** button (it should be located at lower-left corner of your computer), then click Control Panel. Double-click **Network and Internet**, and the following window will appear. Click **Network and Sharing Center**.


Control Panel ▸ Network and Internet ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices | Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Change your homepage | Manage browser add-ons | Delete browsing history and cookies

Next, click **Change adapter settings** and click **Local Area Connection**.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
CARRIE-PC (This computer)
Unidentified network
Internet
View your active networks
Connect or disconnect
Unidentified network
Public network
Access type: No Internet access
Connections: Local Area Connection

Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Realtek RTL8139/810x Family Fast Ethernet NIC

This connection uses the following items:

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

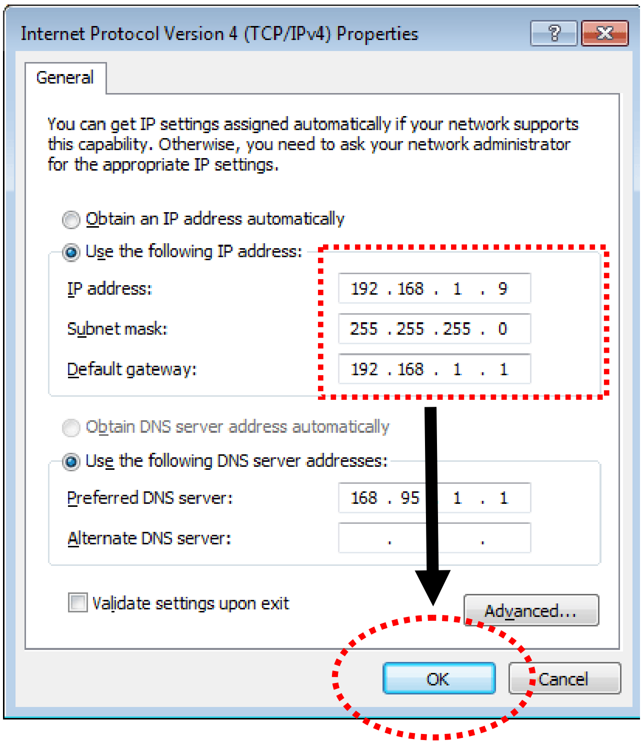
Description

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

Under the General tab, click **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**



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

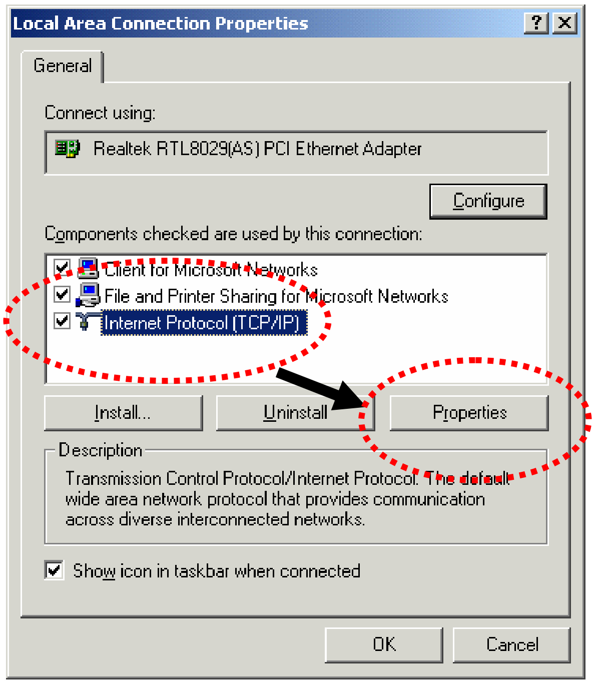
Preferred DNS server: 168 . 95 . 1 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

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**.



Local Area Connection Properties

General

Connect using:

Realtek RTL8029(AS) PCI Ethernet Adapter

Configure

Components checked are used by this connection:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

Install... Uninstall Properties

Description

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

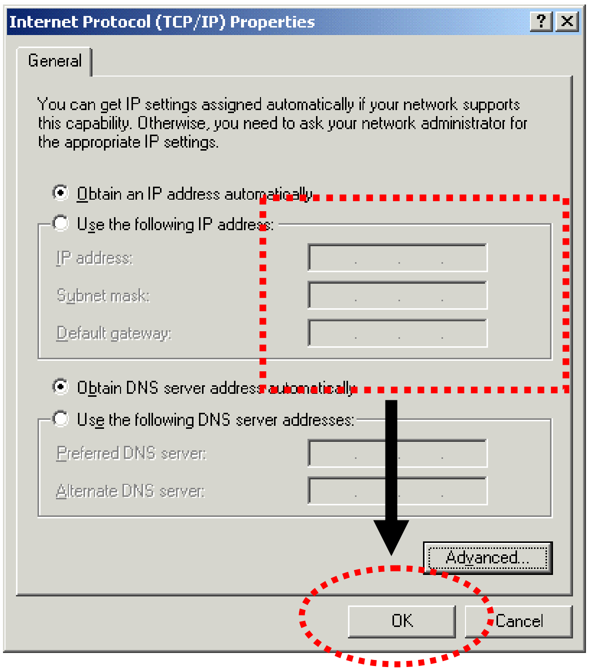
☑ Show icon in taskbar when connected

OK Cancel

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**



Internet Protocol (TCP/IP) Properties

General

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

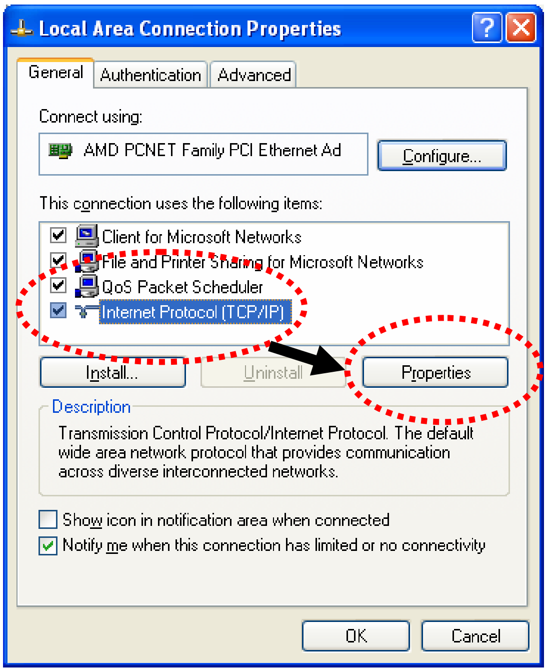
Alternate DNS server: . . .

Advanced...

OK Cancel

2.3 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**.



Connect using:

AMD PCNET Family PCI Ethernet Ad

This connection uses the following items:

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

Description

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

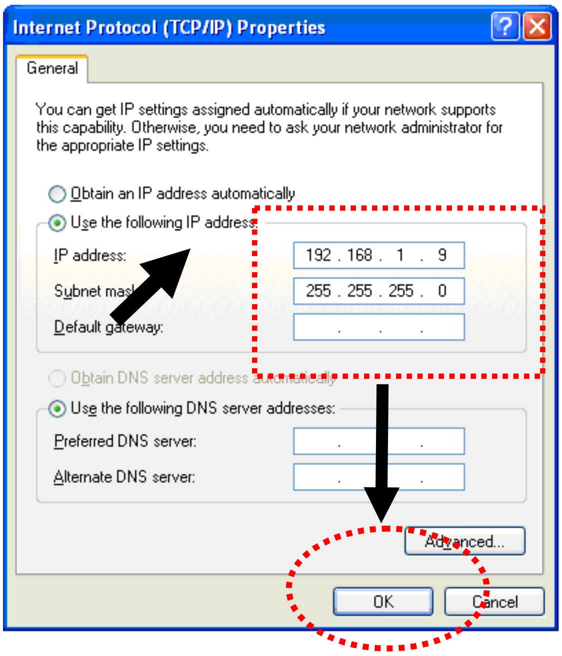
□ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

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**.



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

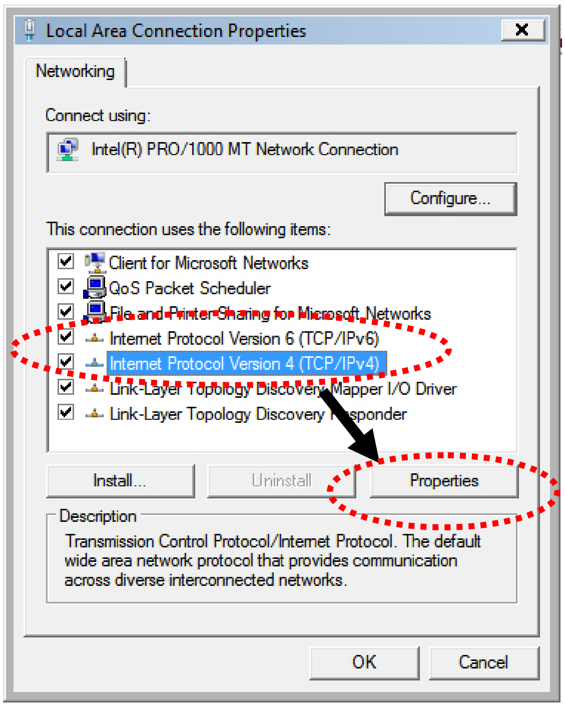
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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**.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

This connection uses the following items:

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

Install... Uninstall Properties

Description

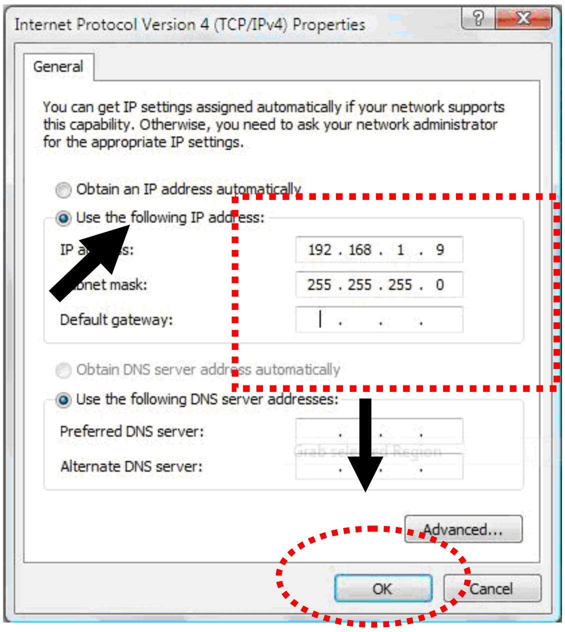
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

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**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Advanced...

OK Cancel

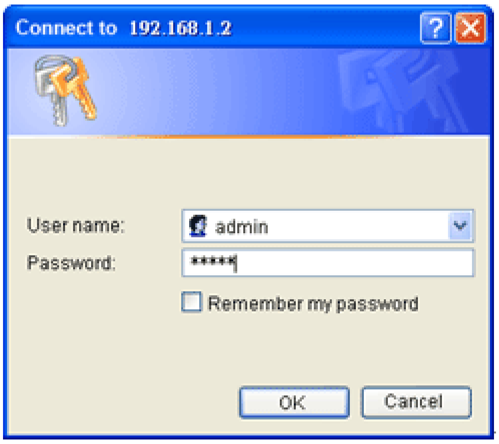
2.5 Accessing to Web User Interface

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 900 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 900 192.168.1.2**. 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**.



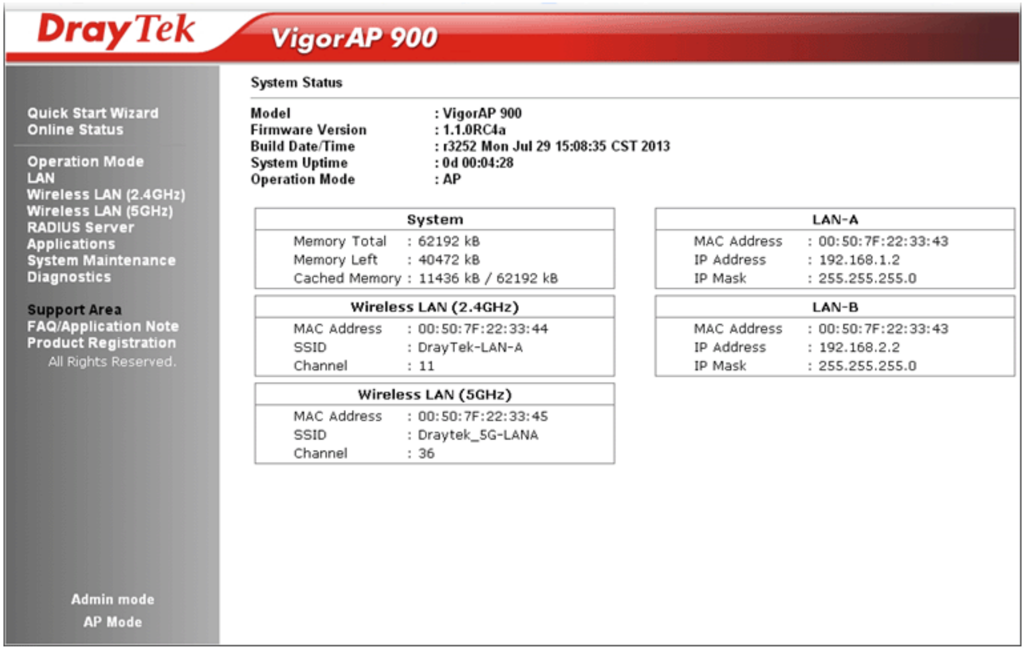
Connect to 192.168.1.2

User name: admin

Password: *****

□ Remember my password

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



System Status

```
Model              : VigorAP 900
Firmware Version   : 1.1.0RC4a
Build Date/Time    : r3252 Mon Jul 29 15:08:35 CST 2013
System Uptime      : 0d 00:04:28
Operation Mode     : AP
```

System	
Memory Total	: 62192 kB
Memory Left	: 40472 kB
Cached Memory	: 11436 kB / 62192 kB

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:22:33:44
SSID	: DrayTek-LAN-A
Channel	: 11

Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:22:33:45
SSID	: Draytek_5G-LANA
Channel	: 36

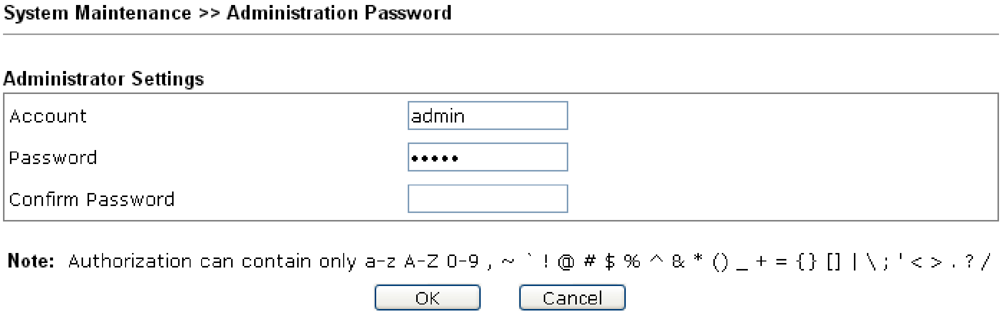
LAN-A	
MAC Address	: 00:50:7F:22:33:43
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

LAN-B	
MAC Address	: 00:50:7F:22:33:43
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

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.**



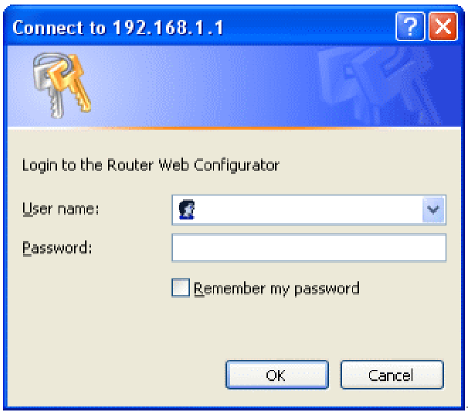
System Maintenance >> Administration Password

Administrator Settings

Account	admin
Password	•••••
Confirm Password	

Note: Authorization can contain only a-z A-Z 0-9 , ~ ` ! @ # $ % ^ & * () _ + = {} [] | \ ; ' < > . ? /

3. Enter the new login password on the field of **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.



Connect to 192.168.1.1

Login to the Router Web Configurator

User name:

Password:

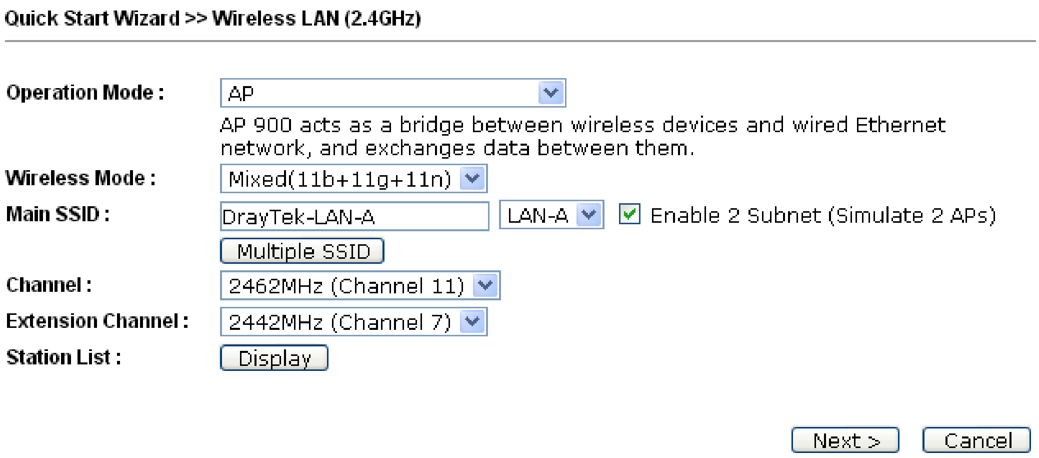
□ Remember my password

2.7 Quick Start Wizard

Quick Start Wizard will guide you to configure 2.4G wireless setting, 5G wireless setting and other corresponding settings for Vigor Access Point step by step.

2.7.1 Configuring 2.4GHz Wireless Settings – General

This page displays general settings for the operation mode selected.



Quick Start Wizard >> Wireless LAN (2.4GHz)

Operation Mode : AP

AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

Wireless Mode : Mixed(11b+11g+11n)

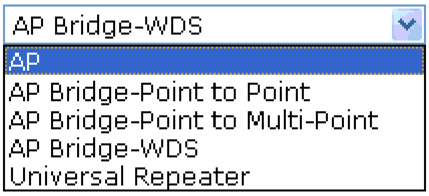
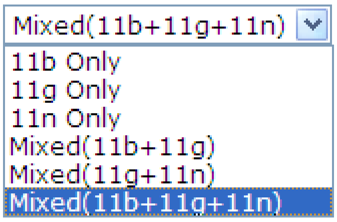
Main SSID : DrayTek-LAN-A LAN-A ☑ Enable 2 Subnet (Simulate 2 APs)

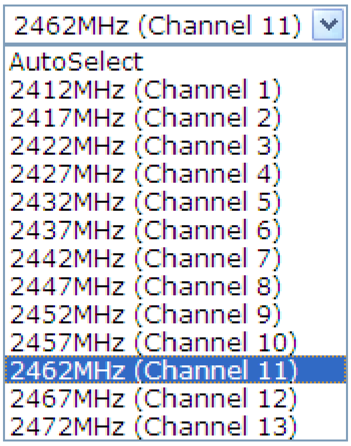
Channel : 2462MHz (Channel 11)

Extension Channel : 2442MHz (Channel 7)

Station List :

Available settings are explained as follows:

Item	Description
Operation Mode	There are six operation modes for wireless connection. Settings for each mode are different.  AP Bridge-WDS AP AP Bridge-Point to Point AP Bridge-Point to Multi-Point AP Bridge-WDS Universal Repeater
Wireless Mode	At present, VigorAP 900 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.  Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)

Main SSID	Set a name for VigorAP 900 to be identified. **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 900. 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. **Multiple SSID** - 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.
Channel	Means the channel 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.  2462MHz (Channel 11) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 9) 2457MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above.
Station List	Click the **Display** button to open the Station List dialog. It provides the knowledge of connecting wireless clients now along with its status code.
AP Discovery	Click this button to open the AP Discovery dialog. VigorAP 900 can scan all regulatory channels and find working APs in the neighborhood. This option is not available when **AP** is selected as the **Operation Mode**.

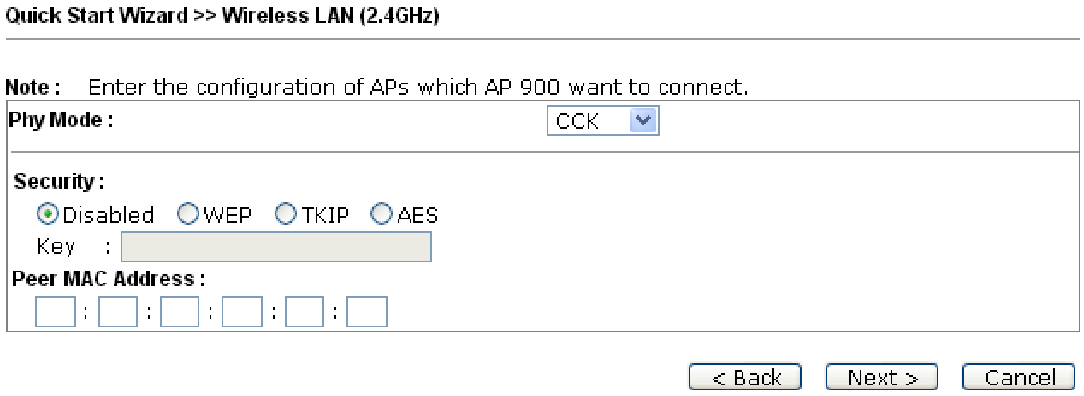
After finishing this web page configuration, please click **Next** to continue.

2.7.2 Configuring 2.4GHz Wireless Settings based on the Operation Mode

In this page, the advanced settings will vary according to the operation mode chosen on 2.7.1.

Advanced Settings for AP Bridge-Point to Point

When you choose AP Bridge-Point to Point, you will need to configure the following page.



Quick Start Wizard >> Wireless LAN (2.4GHz)

Note : Enter the configuration of APs which AP 900 want to connect.

Phy Mode : CCK

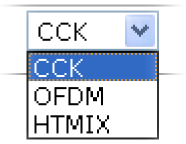
Security :

● Disabled ○ WEP ○ TKIP ○ AES

Key :

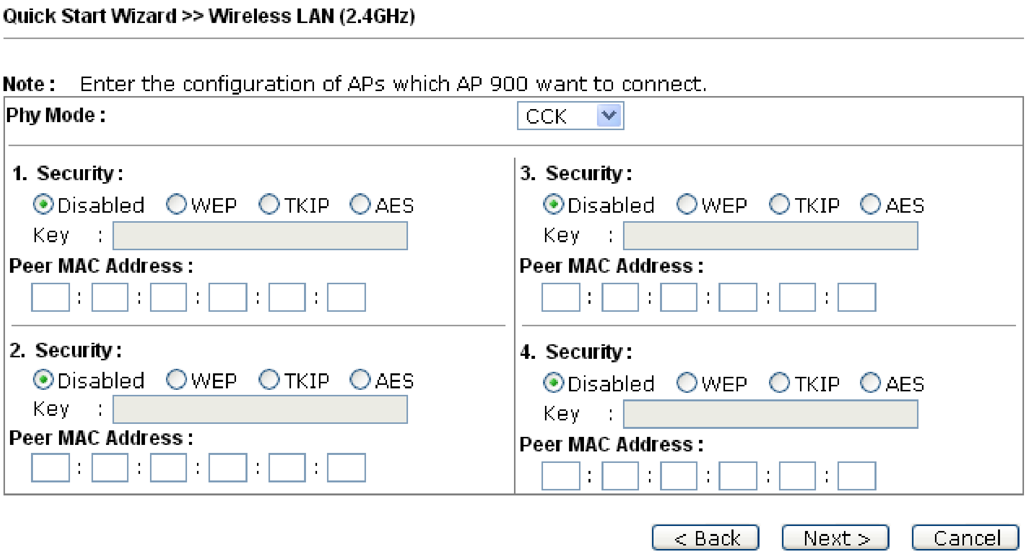
Peer MAC Address :

Available settings are explained as follows:

Item	Description
Phy Mode	There are three types of transmission rates developed by different techniques for **Phy Mode**. Data will be transmitted via communication channel.  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 900 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. Type the key number if required.
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 900 connects to.

Advanced Settings for AP Bridge-Point to Multi-Point

When you choose AP Bridge-Point to Multi-Point, you will need to configure the following page.



Quick Start Wizard >> Wireless LAN (2.4GHz)

Note : Enter the configuration of APs which AP 900 want to connect.

Phy Mode : CCK

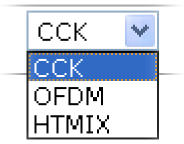
1. Security : ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address : _ : _ : _ : _ : _ : _

2. Security : ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address : _ : _ : _ : _ : _ : _

3. Security : ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address : _ : _ : _ : _ : _ : _

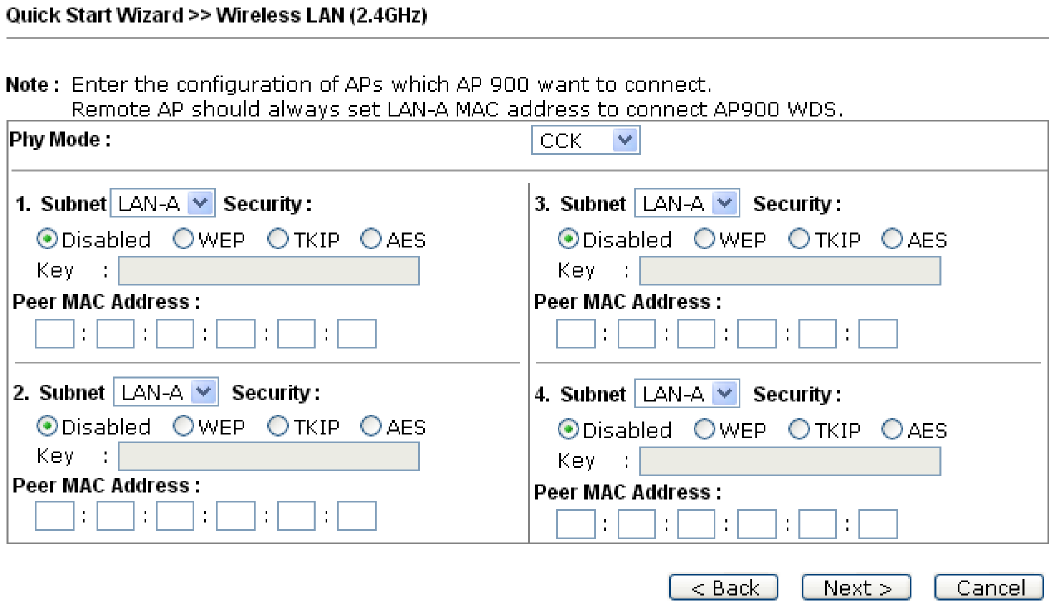
4. Security : ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address : _ : _ : _ : _ : _ : _

Available settings are explained as follows:

Item	Description
Phy Mode	There are three types of transmission rates developed by different techniques for **Phy Mode**. Data will be transmitted via communication channel.  CCK CCK OFDM HTMIX 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 900 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. Type the key number if required.
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 900 connects to.

Advanced Settings for AP Bridge-WDS

When you choose AP Bridge-WDS, you will need to configure the following page.



Quick Start Wizard >> Wireless LAN (2.4GHz)

Note : Enter the configuration of APs which AP 900 want to connect.
Remote AP should always set LAN-A MAC address to connect AP900 WDS.

Phy Mode : CCK

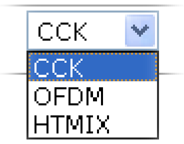
1. Subnet LAN-A **Security :**
● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

2. Subnet LAN-A **Security :**
● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

3. Subnet LAN-A **Security :**
● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

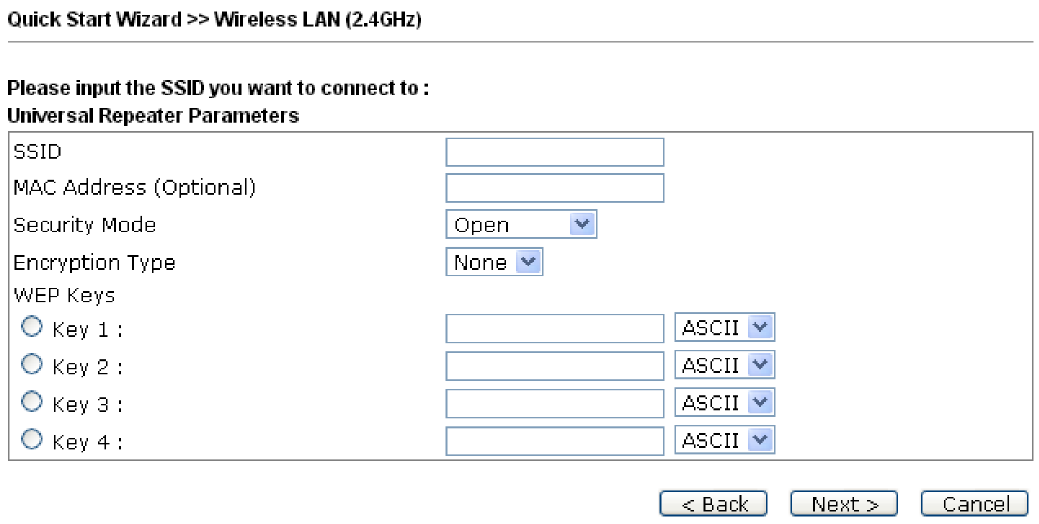
4. Subnet LAN-A **Security :**
● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

Available settings are explained as follows:

Item	Description
Phy Mode	There are three types of transmission rates developed by different techniques for **Phy Mode**. Data will be transmitted via communication channel.  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 900 wants to connect. Each access point should be setup to the same **Phy** mode for connecting with each other.
Subnet	Choose LAN-A or LAN-B for each SSID.
Security	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 900 connects to.

Advanced Settings for AP Bridge-Universal Repeater

When you choose AP Bridge-Universal Repeater you will need to configure the following page.

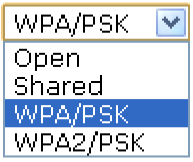
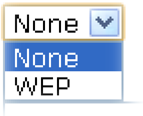


Quick Start Wizard >> Wireless LAN (2.4GHz)

Please input the SSID you want to connect to :
Universal Repeater Parameters

SSID		
MAC Address (Optional)		
Security Mode	Open	
Encryption Type	None	
WEP Keys		
○ Key 1 :		ASCII
○ Key 2 :		ASCII
○ Key 3 :		ASCII
○ Key 4 :		ASCII

Available settings are explained as follows:

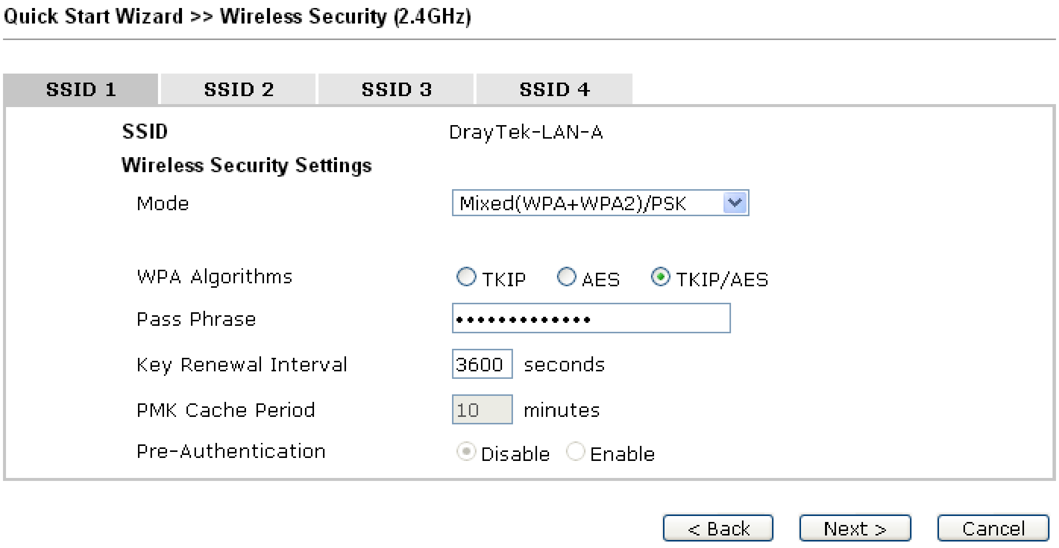
Item	Description
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
MAC Address (Optional)	Type the MAC address for the access point.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.  WPA/PSK Open Shared WPA/PSK WPA2/PSK
Encryption Type for Open/Shared	This option is available when Open/Shared is selected as Security Mode. 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**.  None None 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 ','.
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 ','.
Encryption Type for WPA/PSK and WPA2/PSK	This option is available when **WPA/PSK** or **WPA2/PSK** is selected as **Security Mode**. Select **TKIP** or **AES** as the algorithm for WPA.
Pass Phrase	It is available when WPA/PSK or WPA2/PSK is selected.

After finishing this web page configuration, please click **Next** to continue.

2.7.3 Configuring 2.4GHz Security Settings

VigorAP 900 offers 2.4GHz wireless connection capability. You can setup 2.4GHz features in Quick Start Wizard first. Once the USB 2.4GHz wireless dongle connects to VigorAP 900, it can work immediately.

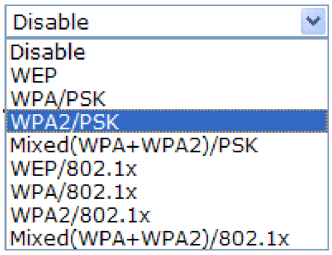


Quick Start Wizard >> Wireless Security (2.4GHz)

SSID 1 | SSID 2 | SSID 3 | SSID 4

SSID	DrayTek-LAN-A
Wireless Security Settings	
Mode	Mixed(WPA+WPA2)/PSK
WPA Algorithms	○ TKIP ○ AES ● TKIP/AES
Pass Phrase	•••••••••••••
Key Renewal Interval	3600 seconds
PMK Cache Period	10 minutes
Pre-Authentication	● Disable ○ Enable

Available settings are explained as follows:

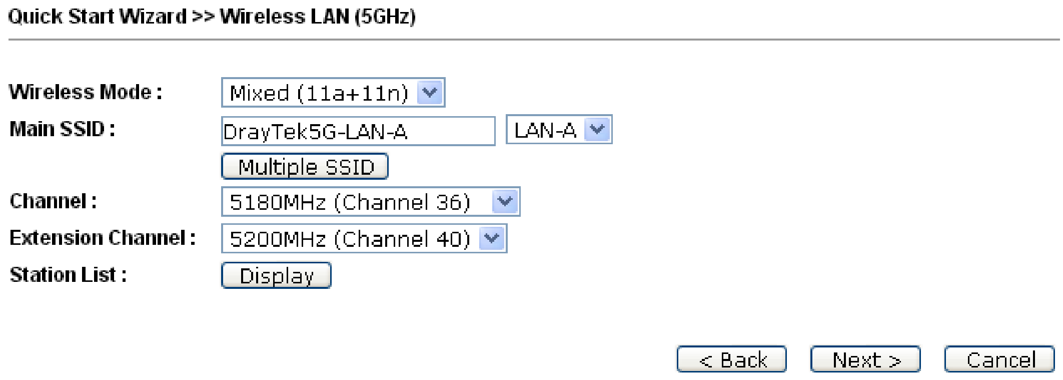
Item	Description
Mode	There are several modes provided for you to choose.  Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x **Disable -** The encryption mechanism is turned off. **WEP -** Accepts only WEP clients and the encryption key 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 900 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 Algorithm	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 Internal	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 ','.
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.

After finishing this web page configuration, please click **Next** to continue.

2.7.4 Configuring 5GHz Wireless Settings

VigorAP 900 offers 5GHz wireless connection capability. You can setup 5GHz features in Quick Start Wizard first. Once the USB 5GHz wireless dongle connects to VigorAP 900, it can work immediately.



Quick Start Wizard >> Wireless LAN (5GHz)

Wireless Mode : Mixed (11a+11n)

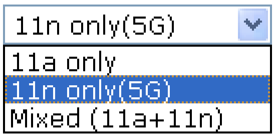
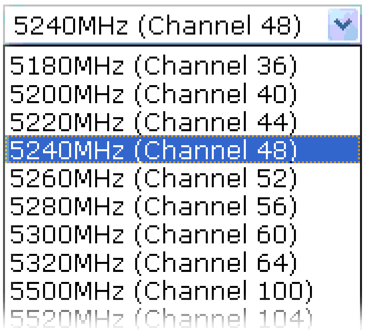
Main SSID : DrayTek5G-LAN-A LAN-A

Channel : 5180MHz (Channel 36)

Extension Channel : 5200MHz (Channel 40)

Station List :

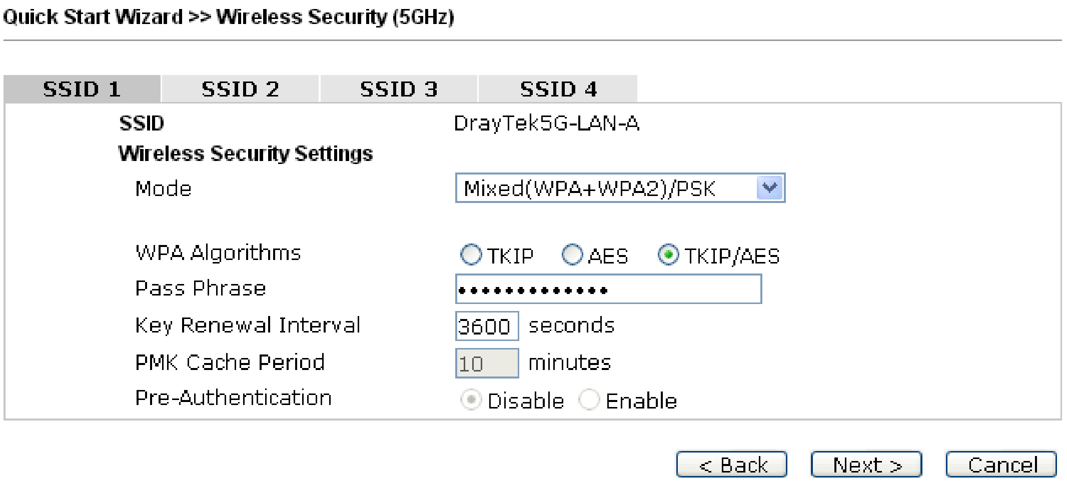
Available settings are explained as follows:

Item	Description
Wireless Mode	At present, VigorAP 900 can connect to 11a only, 11n only (5G), Mixed (11a+11n) stations simultaneously. Simply choose Mixed (11a+11n) mode. 
Main SSID	Set a name for VigorAP 900 to be identified. **Multiple SSID** – Set the SSIDs and specify subnet interface (LAN-A or LAN-B) for each SSID by click Multiple SSID.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 48. You may switch channel if the selected channel is under serious interference.  5240MHz (Channel 48) 5180MHz (Channel 36) 5200MHz (Channel 40) 5220MHz (Channel 44) 5240MHz (Channel 48) 5260MHz (Channel 52) 5280MHz (Channel 56) 5300MHz (Channel 60) 5320MHz (Channel 64) 5500MHz (Channel 100) 5520MHz (Channel 104)
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above.
Station List	Click the **Display** button to open the Station List dialog. It provides the knowledge of connecting wireless clients now along with its status code.

After finishing this web page configuration, please click **Next** to continue.

2.7.5 Configuring 5GHz Security Settings

VigorAP 900 offers 5GHz wireless connection capability. You can setup 5G features in Quick Start Wizard first. Once the USB 5GHz wireless dongle connects to VigorAP 900, it can work immediately.



Quick Start Wizard >> Wireless Security (5GHz)

SSID 1 | SSID 2 | SSID 3 | SSID 4

SSID DrayTek5G-LAN-A

Wireless Security Settings

Mode: Mixed(WPA+WPA2)/PSK

WPA Algorithms: ○ TKIP ○ AES ● TKIP/AES

Pass Phrase: •••••••••••••

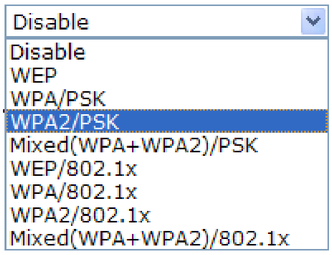
Key Renewal Interval: 3600 seconds

PMK Cache Period: 10 minutes

Pre-Authentication: ● Disable ○ Enable

< Back | Next > | Cancel

Available settings are explained as follows:

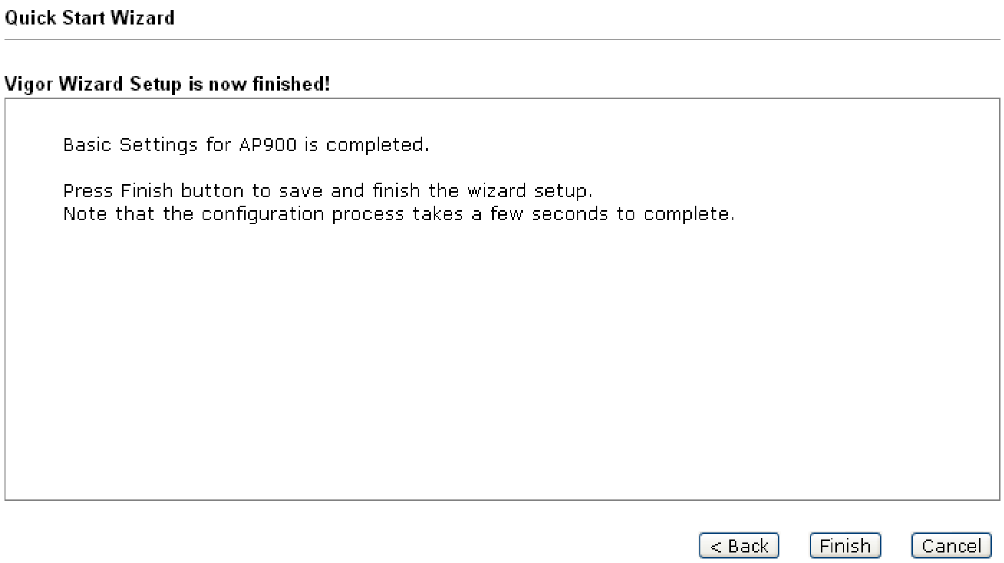
Item	Description
Mode	There are several modes provided for you to choose.  Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x **Disable** - The encryption mechanism is turned off. **WEP** - Accepts only WEP clients and the encryption key 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 900 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 Algorithm	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 Internal	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 ','.
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.

After finishing this web page configuration, please click **Next** to continue.

2.7.6 Finishing the Wireless Settings Wizard

When you see this page, it means the wireless setting wizard is almost finished. Just click **Finish** to save the settings and complete the setting procedure.



Quick Start Wizard

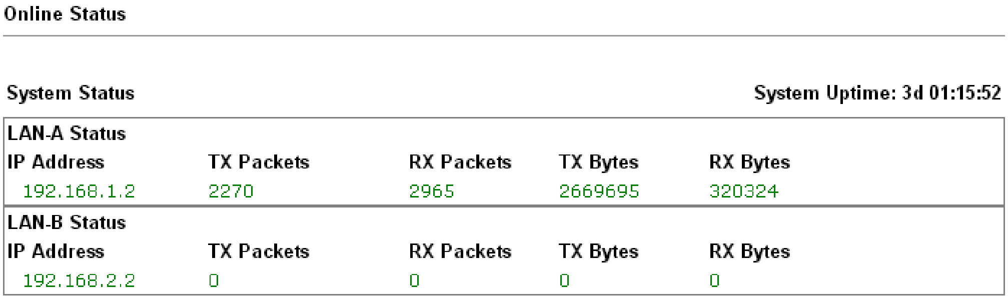
Vigor Wizard Setup is now finished!

Basic Settings for AP900 is completed.

Press Finish button to save and finish the wizard setup.
Note that the configuration process takes a few seconds to complete.

2.8 Online Status

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



Online Status

System Status — System Uptime: 3d 01:15:52

LAN-A Status

IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.1.2	2270	2965	2669695	320324

LAN-B Status

IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.2.2	0	0	0	0

Detailed explanation is shown below:

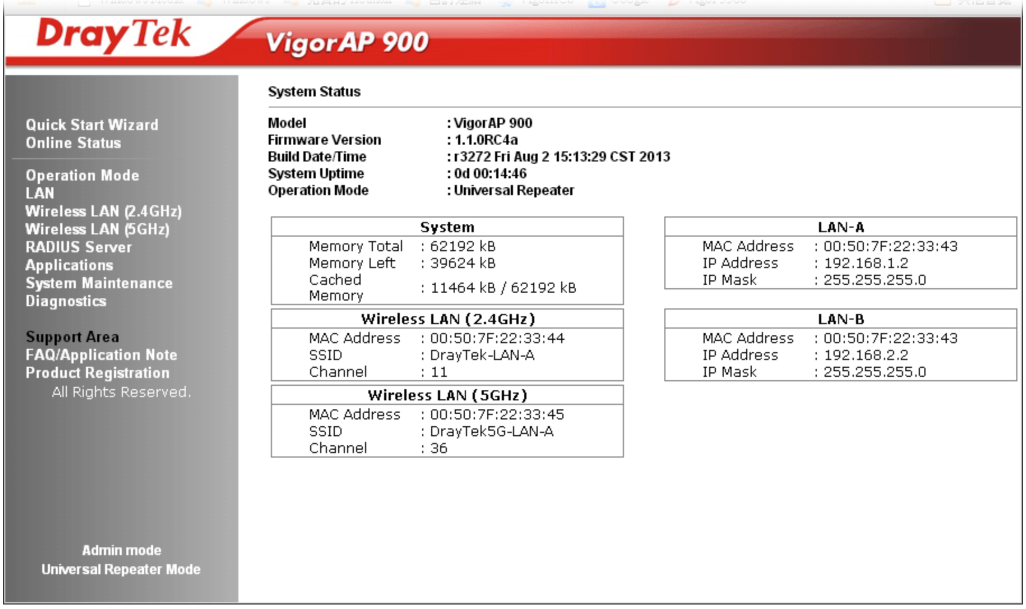
Item	Description
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
TX Bytes	Displays the total transmitted size at the LAN interface.
RX Bytes	Displays the total number of received size at the LAN interface.

3 Advanced 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.



System Status

```
Model                :VigorAP 900
Firmware Version     :1.1.0RC4a
Build Date/Time      :r3272 Fri Aug 2 15:13:29 CST 2013
System Uptime        :0d 00:14:46
Operation Mode       :Universal Repeater
```

System	
Memory Total	: 62192 kB
Memory Left	: 39624 kB
Cached Memory	: 11464 kB / 62192 kB

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:22:33:44
SSID	: DrayTek-LAN-A
Channel	: 11

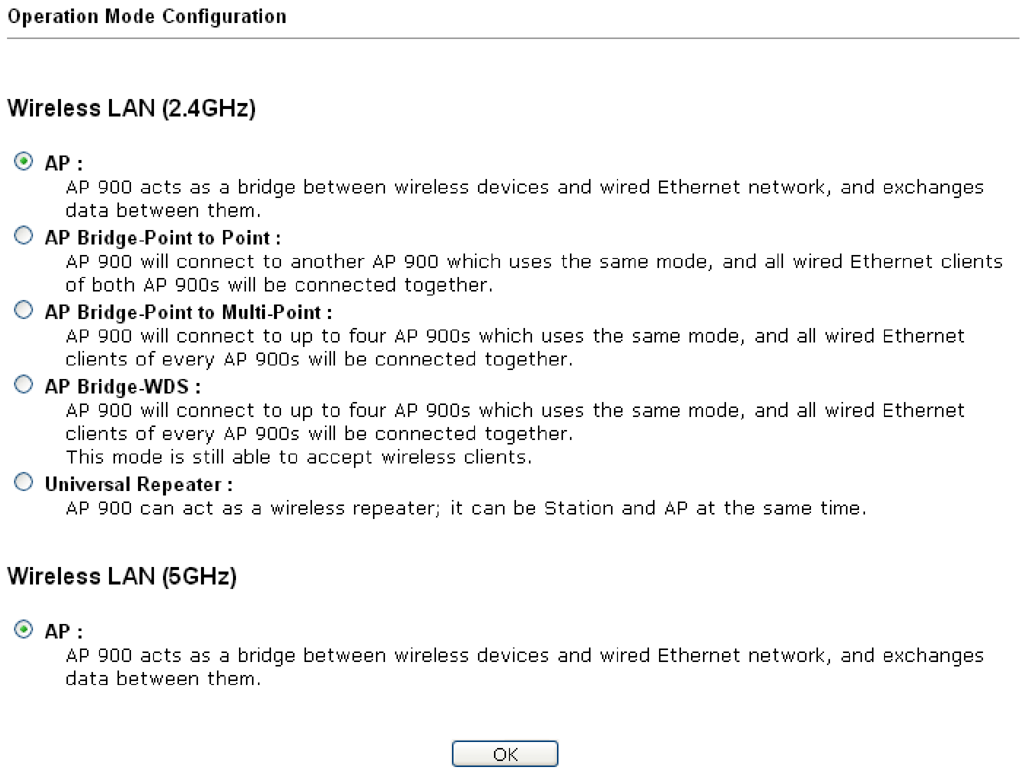
Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:22:33:45
SSID	: DrayTek5G-LAN-A
Channel	: 36

LAN-A	
MAC Address	: 00:50:7F:22:33:43
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

LAN-B	
MAC Address	: 00:50:7F:22:33:43
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

3.1 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.



Operation Mode Configuration

Wireless LAN (2.4GHz)

● **AP :**
AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

○ **AP Bridge-Point to Point :**
AP 900 will connect to another AP 900 which uses the same mode, and all wired Ethernet clients of both AP 900s will be connected together.

○ **AP Bridge-Point to Multi-Point :**
AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together.

○ **AP Bridge-WDS :**
AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together.
This mode is still able to accept wireless clients.

○ **Universal Repeater :**
AP 900 can act as a wireless repeater; it can be Station and AP at the same time.

Wireless LAN (5GHz)

● **AP :**
AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

Available settings are explained as follows:

Item	Description
Wireless LAN(2.4GHz)	
AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
AP Bridge-Point to Point	This mode can establish wireless connection with another VigorAP 900 using the same mode, and link the wired network which these two VigorAP 900s 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 900s using the same mode, and link the wired network which these VigorAP 900s 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.
Wireless LAN(5GHz)	
AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.

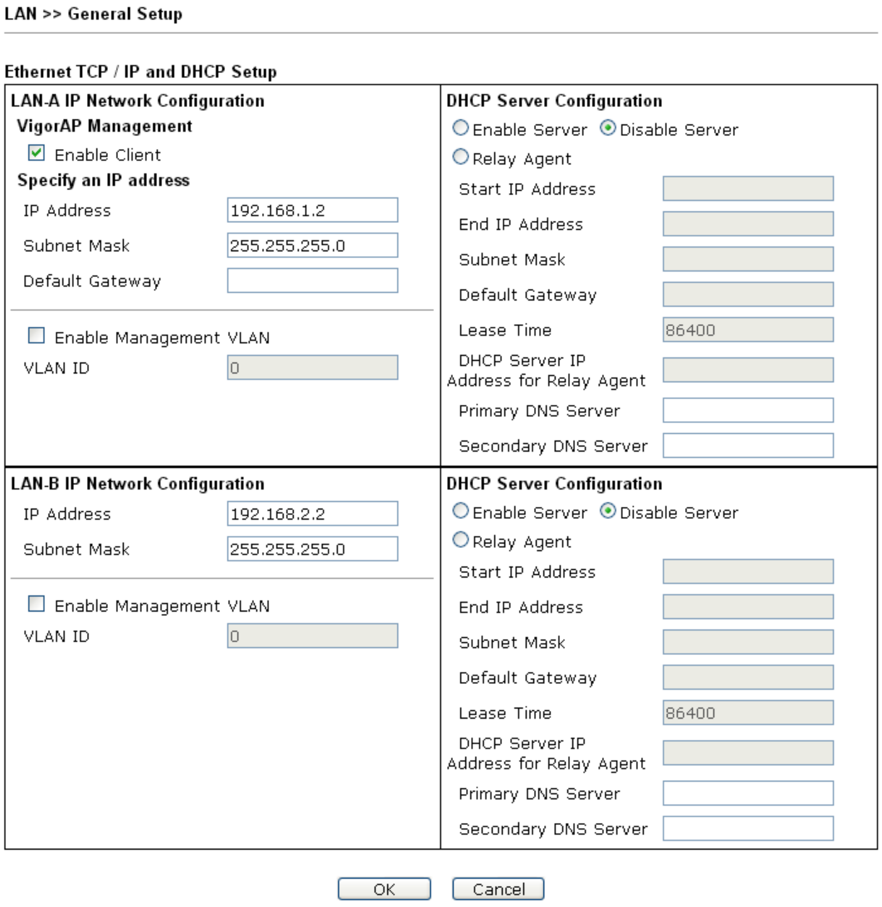
> **Note:** The **Wireless LAN** settings will be changed according to the **Operation Mode** selected here. For the detailed information, please refer to the section of **Wireless LAN**.

3.2 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.



LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN-A IP Network Configuration

VigorAP Management

☑ Enable Client

Specify an IP address

IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	

□ Enable Management VLAN

VLAN ID	0

DHCP Server Configuration

○ Enable Server ● Disable Server

○ Relay Agent

Start IP Address	
End IP Address	
Subnet Mask	
Default Gateway	
Lease Time	86400
DHCP Server IP Address for Relay Agent	
Primary DNS Server	
Secondary DNS Server	

LAN-B IP Network Configuration

IP Address	192.168.2.2
Subnet Mask	255.255.255.0

□ Enable Management VLAN

VLAN ID	0

DHCP Server Configuration

○ Enable Server ● Disable Server

○ Relay Agent

Start IP Address	
End IP Address	
Subnet Mask	
Default Gateway	
Lease Time	86400
DHCP Server IP Address for Relay Agent	
Primary DNS Server	
Secondary DNS Server	

Available settings are explained as follows:

Item	Description
Enable Client	When it is enabled, VigorAP 900 will be treated as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2860).
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)
Default Gateway	In general, it is not really necessary to specify a gateway for VigorAP 900. However, if it is required, simply type an IP address as the gateway for VigorAP 900. It will be convenient for the access point acquiring more service (e.g., accessing NTP server) from Vigor router.
Enable Management VLAN	VigorAP 900 supports tag-based VLAN for wireless clients accessing Vigor router. Only the clients with the specified VLAN ID can access into VigorAP 900. **VLAN ID -** Type the number as VLAN ID tagged on the transmitted packet. “0” means no VALN tag.
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.
Relay Agent	Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
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.
DHCP Server IP Address for Relay Agent	It is available when Enable Relay Agent is selected. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
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.

After finishing this web page configuration, please click **OK** to save the settings.

3.3 General Concepts for Wireless LAN (2.4GHz/5GHz)

The VigorAP 900 is equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the VigorAP 900 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 900 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 900. 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.

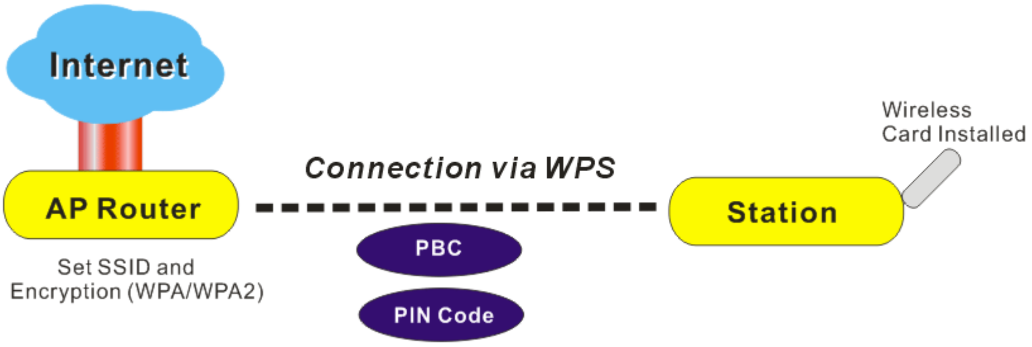
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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 900 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 900) with the encryption of WPA and WPA2.

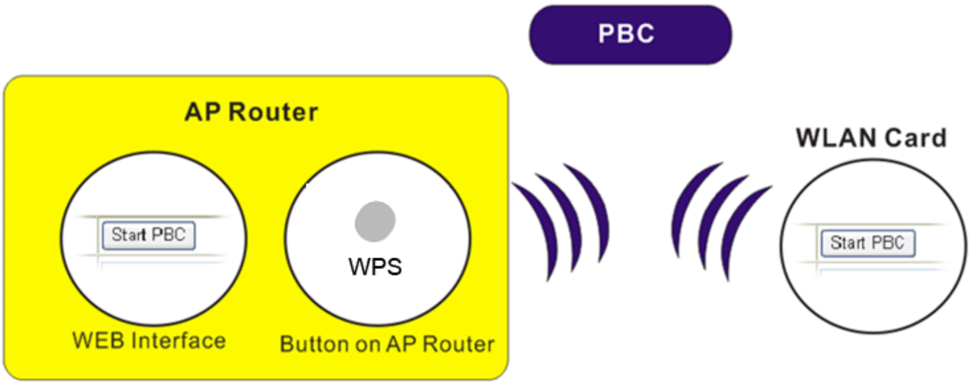
It is the simplest way to build connection between wireless network clients and VigorAP 900. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 900 automatically.



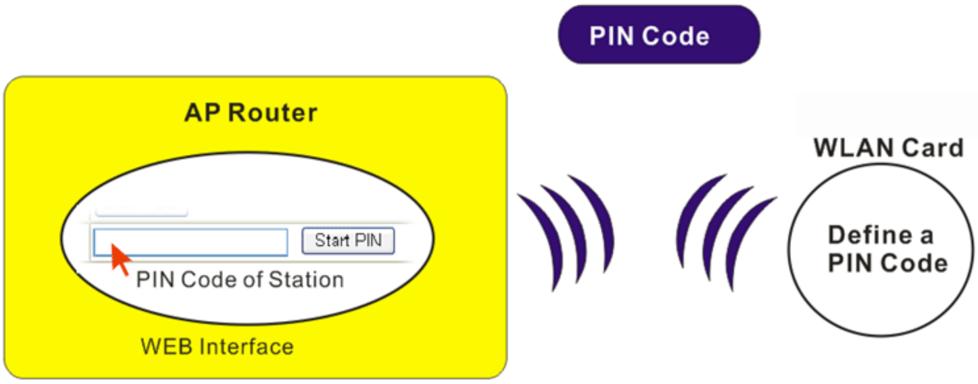
Note: Such function is available for the wireless station with WPS supported.

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 900 series which served as an AP, press **WPS** button once on the front panel of VigorAP 900 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.

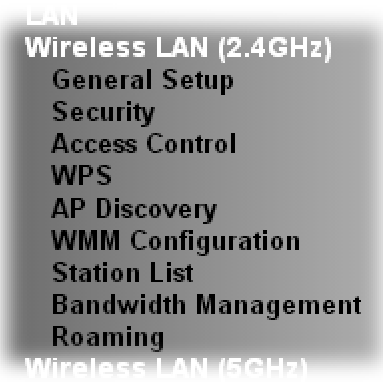


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 900.



3.4 Wireless LAN Settings for AP Mode

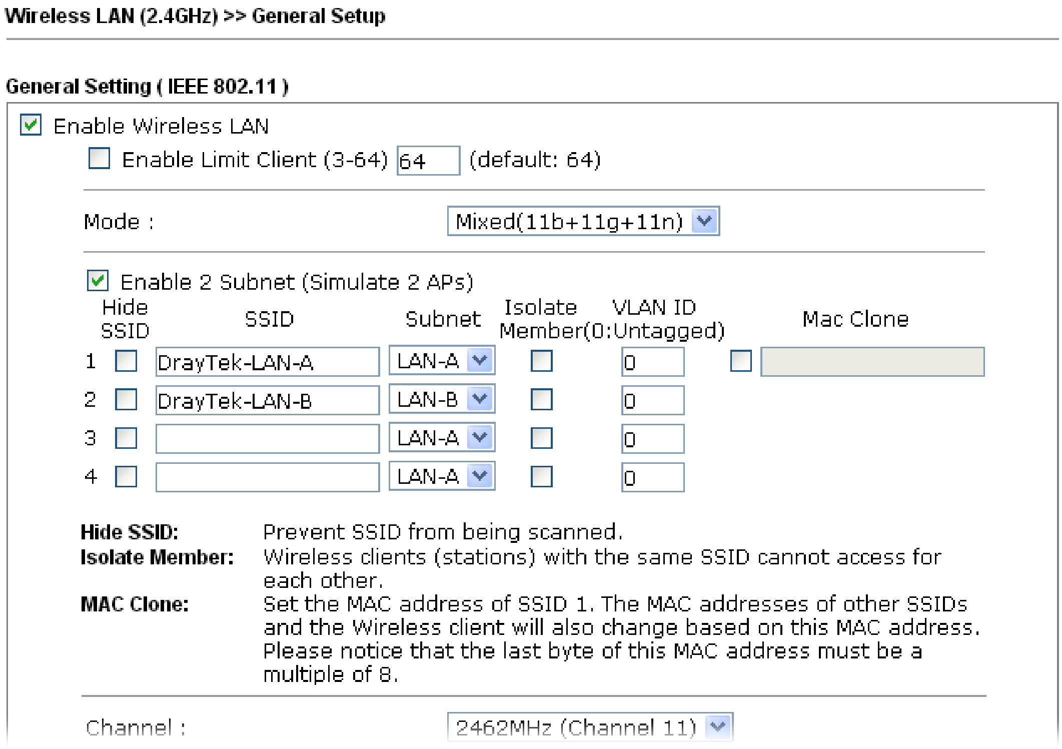
When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery and Station List.



> **Note:** The **Wireless LAN** settings will be changed according to the **Operation Mode** selected in section 3.1.

3.4.1 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.



Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

□ Enable Limit Client (3-64) 64 (default: 64)

Mode : Mixed(11b+11g+11n)

☑ Enable 2 Subnet (Simulate 2 APs)

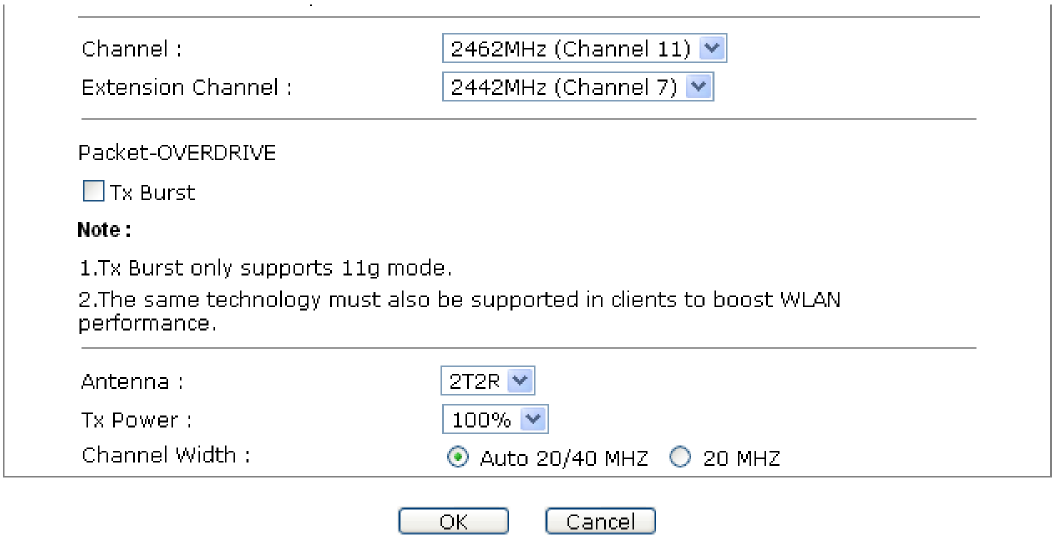
	Hide SSID	SSID	Subnet	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
1	□	DrayTek-LAN-A	LAN-A	□	0	□
2	□	DrayTek-LAN-B	LAN-B	□	0	
3	□		LAN-A	□	0	
4	□		LAN-A	□	0	

Hide SSID: Prevent SSID from being scanned.

Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

MAC Clone: Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.

Channel : 2462MHz (Channel 11)



Channel : 2462MHz (Channel 11)

Extension Channel : 2442MHz (Channel 7)

Packet-OVERDRIVE

□ Tx Burst

Note :

1.Tx Burst only supports 11g mode.

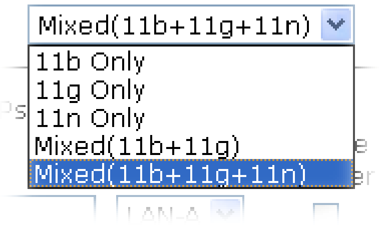
2.The same technology must also be supported in clients to boost WLAN performance.

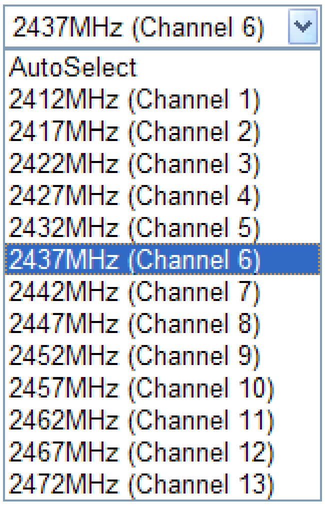
Antenna : 2T2R

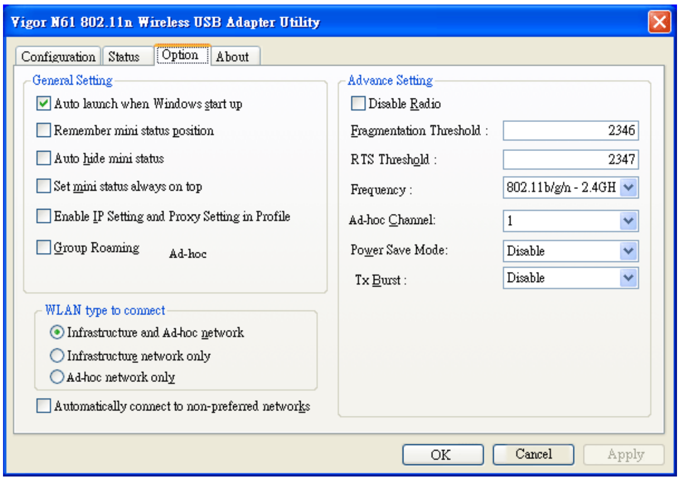
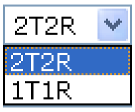
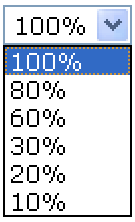
Tx Power : 100%

Channel Width : ● Auto 20/40 MHZ ○ 20 MHZ

Available settings are explained as follows:

Item	**Description**
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor router. The number you can set is from 3 to 64.
Mode	At present, VigorAP 900 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.  Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11b+11g+11n)
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 900. 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 900 while site surveying. The system allows you to set three sets of SSID for different usage.

SSID	Set a name for VigorAP 900 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.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
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. 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.  2437MHz (Channel 6) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 9) 2457MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above. Configure the extension channel you want.
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.

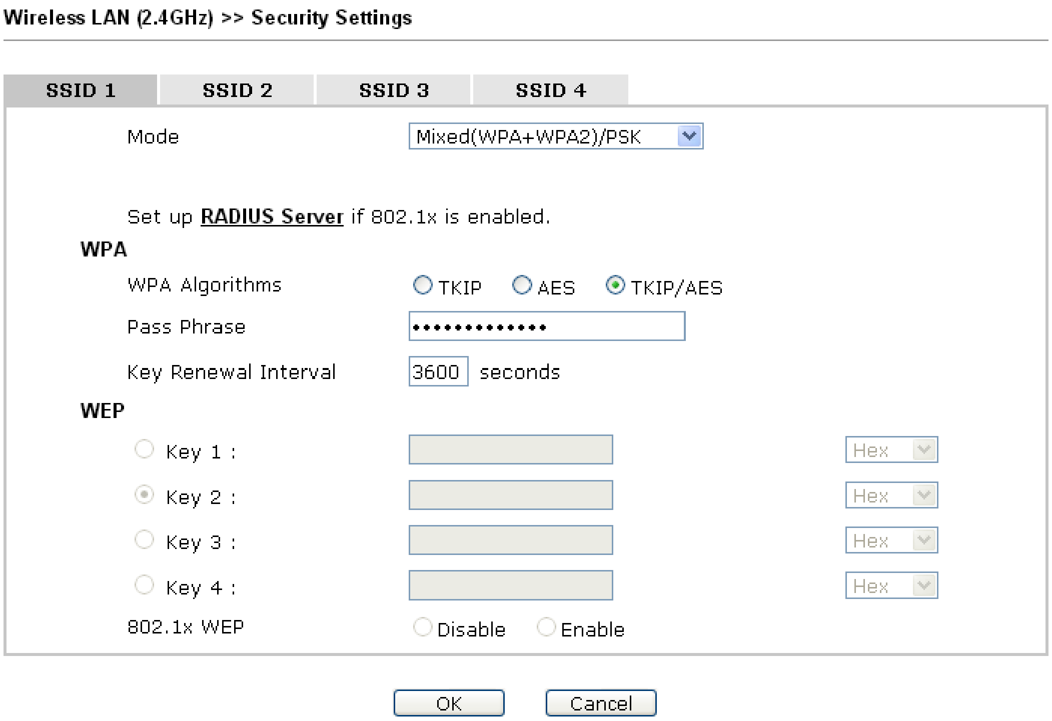
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and 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**).  Vigor N61 802.11n Wireless USB Adapter Utility Configuration | Status | Option | About General Setting ☑ Auto launch when Windows start up □ Remember mini status position □ Auto hide mini status □ Set mini status always on top □ Enable IP Setting and Proxy Setting in Profile □ Group Roaming Ad-hoc WLAN type to connect ● Infrastructure and Ad-hoc network ○ Infrastructure network only ○ Ad-hoc network only □ Automatically connect to non-preferred networks Advance Setting □ Disable Radio Fragmentation Threshold : 2346 RTS Threshold : 2347 Frequency : 802.11b/g/n - 2.4GH Ad-hoc Channel: 1 Power Save Mode: Disable Tx Burst : Disable OK Cancel Apply
Antenna	VigorAP 900 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.  2T2R 2T2R 1T1R
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.  100% 100% 80% 60% 30% 20% 10%
Channel Width	**20 MHZ-** the router will use 20Mhz for data transmission and receiving between the AP and the stations. **Auto 20/40 MHZ–** the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.

After finishing this web page configuration, please click **OK** to save the settings.

3.4.2 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.



Wireless LAN (2.4GHz) >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

Mode: Mixed(WPA+WPA2)/PSK

Set up **RADIUS Server** if 802.1x is enabled.

WPA

WPA Algorithms: ○ TKIP ○ AES ● TKIP/AES

Pass Phrase: •••••••••••••

Key Renewal Interval: 3600 seconds

WEP

○ Key 1 : Hex

● Key 2 : Hex

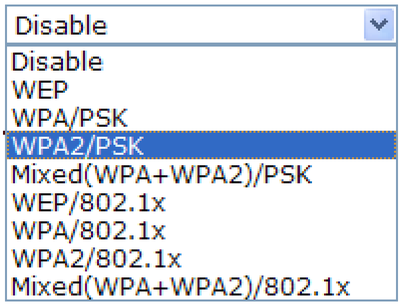
○ Key 3 : Hex

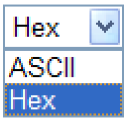
○ Key 4 : Hex

802.1x WEP: ○ Disable ○ Enable

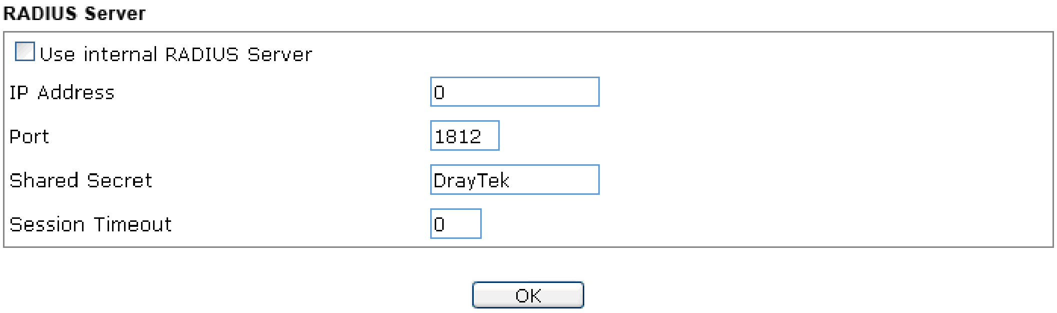
OK | Cancel

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.  Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x **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 900 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.
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.



RADIUS Server

□ Use internal RADIUS Server	
IP Address	0
Port	1812
Shared Secret	DrayTek
Session Timeout	0

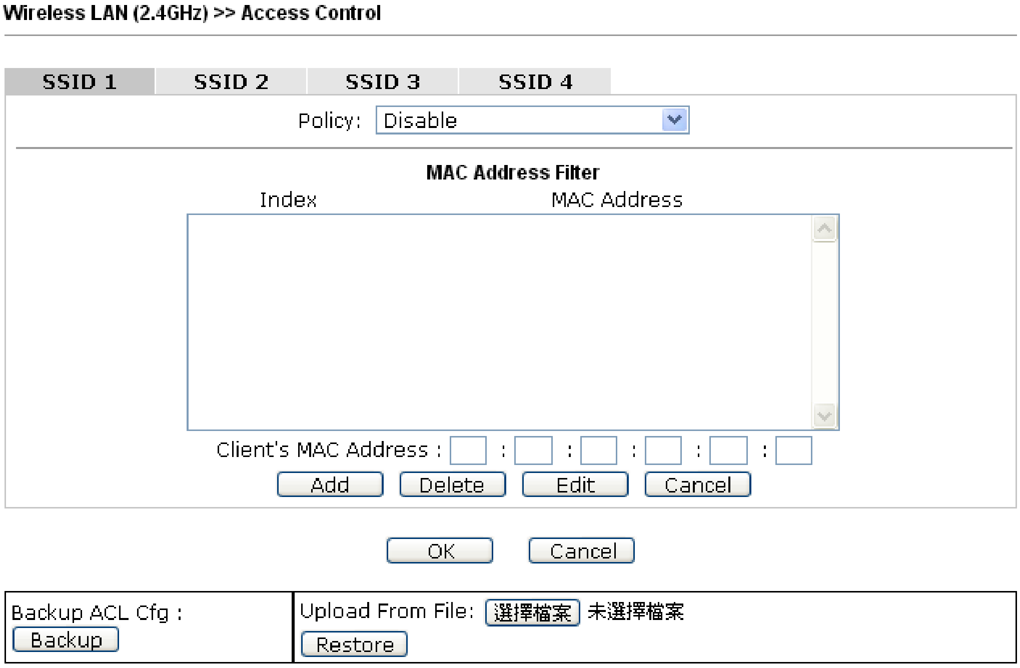
Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 900 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, **3.9 RADIUS Server** to configure settings for internal server of VigorAP 900.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external 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.)

After finishing this web page configuration, please click **OK** to save the settings.

3.4.3 Access Control

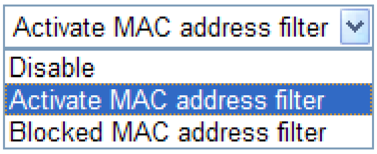
For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, 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).



Wireless LAN (2.4GHz) >> Access Control

Policy: Disable

Available settings are explained as follows:

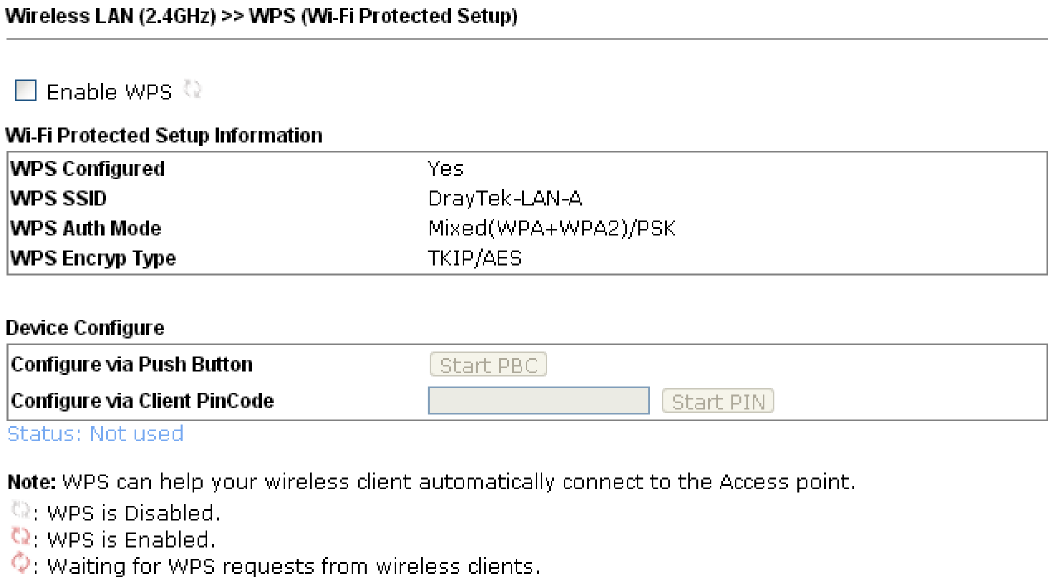
Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 900.  Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter
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.
Backup	Click it to store the settings (MAC addresses on MAC Address

	Filter table) on this page as a file.
Restore	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

3.4.4 WPS

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



Wireless LAN (2.4GHz) >> WPS (Wi-Fi Protected Setup)

□ Enable WPS

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek-LAN-A
WPS Auth Mode	Mixed(WPA+WPA2)/PSK
WPS Encryp Type	TKIP/AES

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: Not used

Note: WPS can help your wireless client automatically connect to the Access point.
: WPS is Disabled.
: WPS is Enabled.
: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

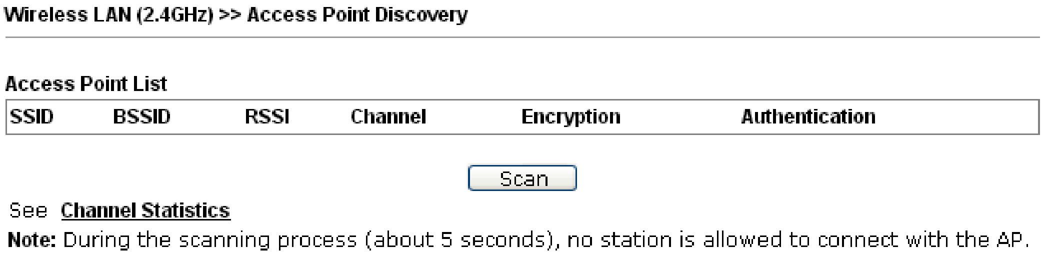
Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 900 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 900. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 900.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 900 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 900 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 900 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).

3.4.5 AP Discovery

VigorAP 900 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. Please click **Scan** to discover all the connected APs.



Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

SSID	BSSID	RSSI	Channel	Encryption	Authentication

See Channel Statistics

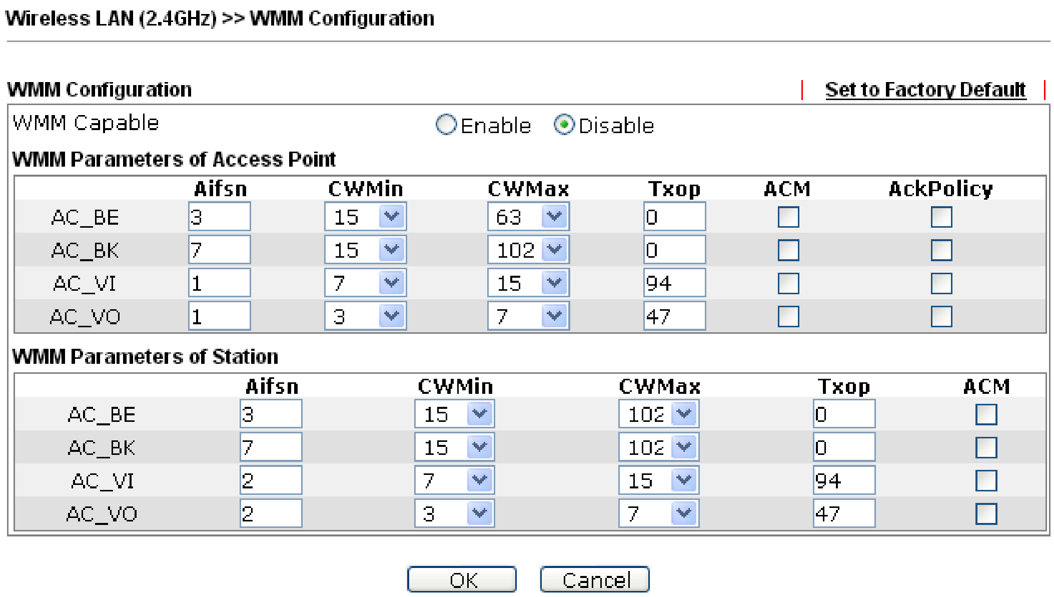
Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 900.
BSSID	Display the MAC address of the AP scanned by VigorAP 900.
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 900.
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.

3.4.6 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.



Wireless LAN (2.4GHz) >> WMM Configuration

WMM Configuration | Set to Factory Default |

WMM Capable ○Enable ●Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	102	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	□
AC_BK	7	15	102	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

Available settings are explained as follows:

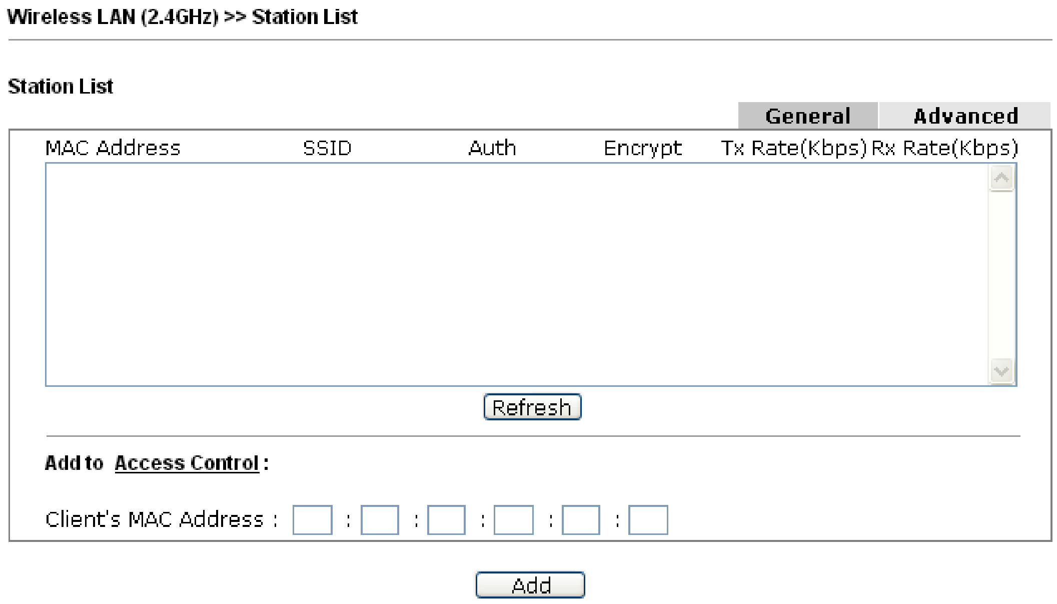
Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can

	restrict stations from using specific category class if it is checked. **Note:** VigorAP 900 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	**“**Uncheck” (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. “Check” the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

After finishing this web page configuration, please click **OK** to save the settings.

3.4.7 Station List

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



Wireless LAN (2.4GHz) >> Station List

Station List

Add to Access Control :

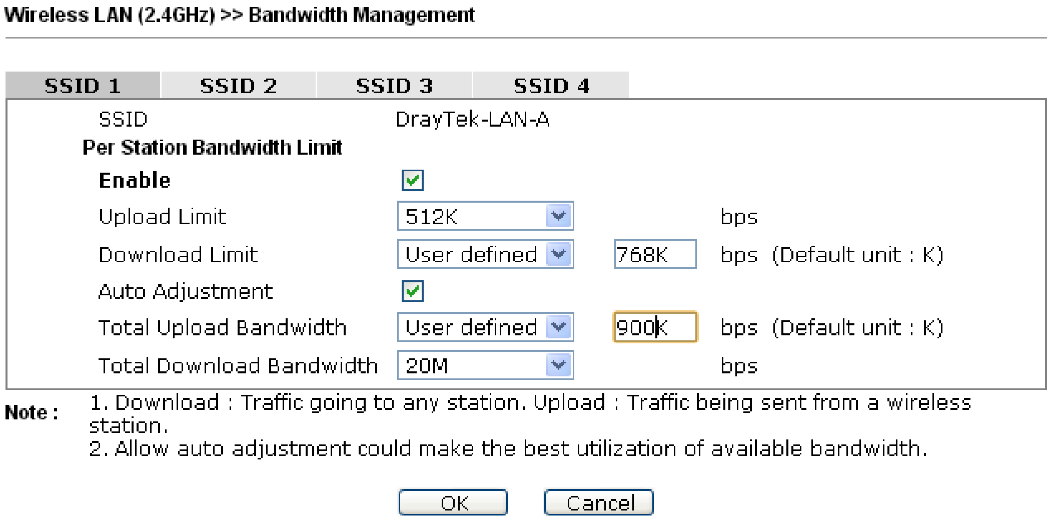
Client's MAC Address : [ ] : [ ] : [ ] : [ ] : [ ] : [ ]

Available settings are explained as follows:

Item	Description
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.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
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 Control**.
General/Advanced	**General** – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. **Advanced** – Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

3.4.8 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.



Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1 | SSID 2 | SSID 3 | SSID 4

SSID	DrayTek-LAN-A		
Per Station Bandwidth Limit			
Enable	☑		
Upload Limit	512K		bps
Download Limit	User defined	768K	bps (Default unit : K)
Auto Adjustment	☑		
Total Upload Bandwidth	User defined	900K	bps (Default unit : K)
Total Download Bandwidth	20M		bps

Note : 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.
2. Allow auto adjustment could make the best utilization of available bandwidth.

Available settings are explained as follows:

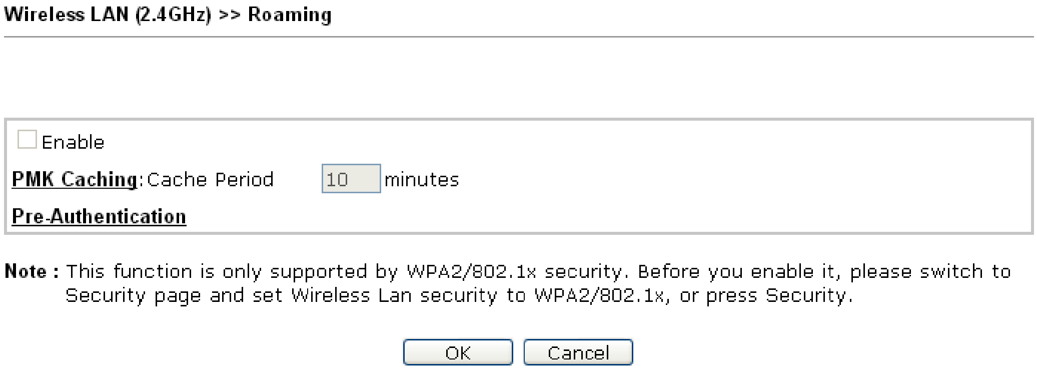
Item	Description
SSID	Display the specific SSID name of the router.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Download Limit	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Auto Adjustment	Check this box to have the bandwidth limit determined by the system automatically.
Total Upload Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data uploading.
Total Download Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data downloading.

After finishing this web page configuration, please click **OK** to save the settings.

3.4.9 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.



Wireless LAN (2.4GHz) >> Roaming

□ Enable

PMK Caching: Cache Period 10 minutes

Pre-Authentication

Note : This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

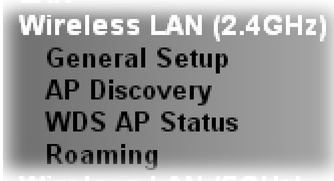
Available settings are explained as follows:

Item	Description
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.

After finishing this web page configuration, please click **OK** to save the settings.

3.5 Wireless LAN Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Mode

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

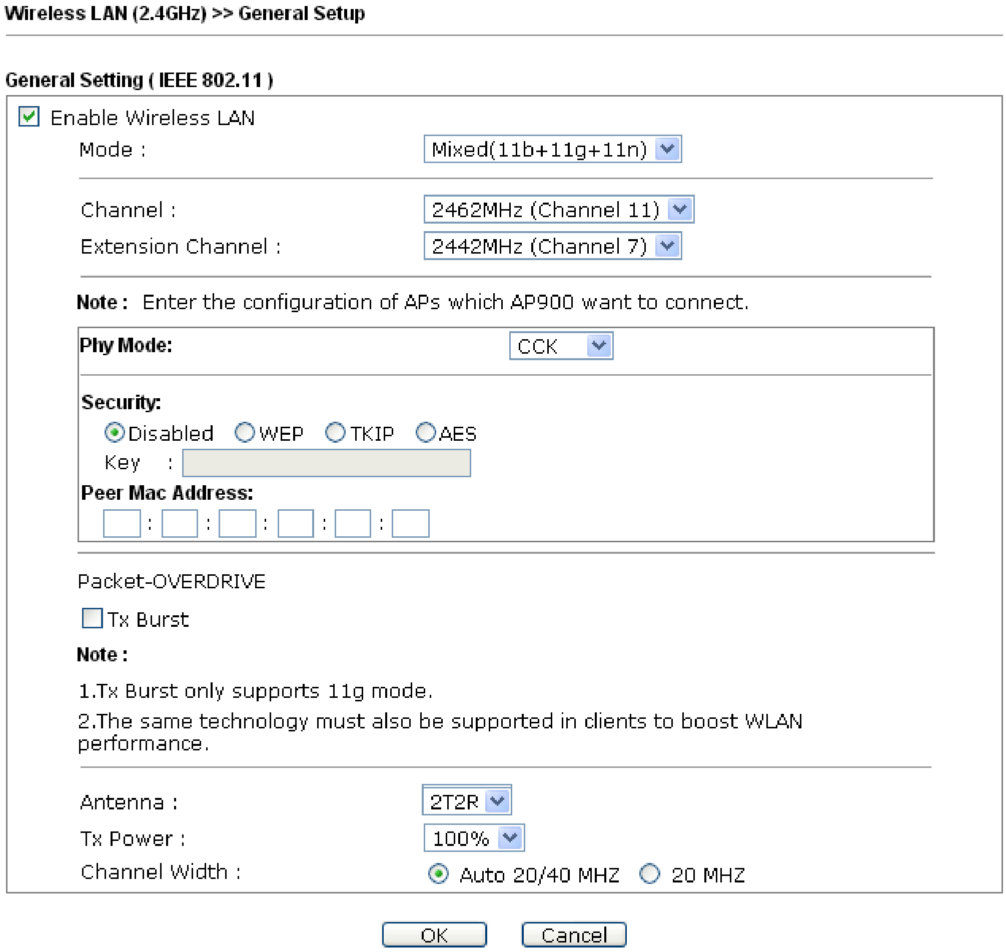


AP Bridge-Point to Point allows VigorAP 900 to connect to **another** VigorAP 900 which uses the same mode. All wired Ethernet clients of both VigorAP 900s will be connected together.

Point-to Multi-Point Mode allows AP 900 to connect up to **four** AP 900s which uses the same mode. All wired Ethernet clients of every VigorAP 900 will be connected together.

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.



Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

Mode : Mixed(11b+11g+11n)

Channel : 2462MHz (Channel 11)

Extension Channel : 2442MHz (Channel 7)

Note : Enter the configuration of APs which AP900 want to connect.

Phy Mode: CCK

Security:

● Disabled ○ WEP ○ TKIP ○ AES

Key :

Peer Mac Address:

__ : __ : __ : __ : __ : __

Packet-OVERDRIVE

□ Tx Burst

Note :

1.Tx Burst only supports 11g mode.

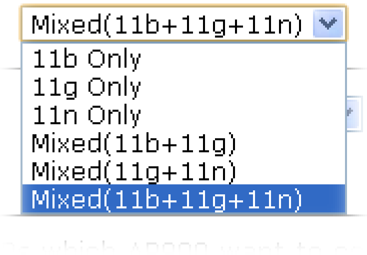
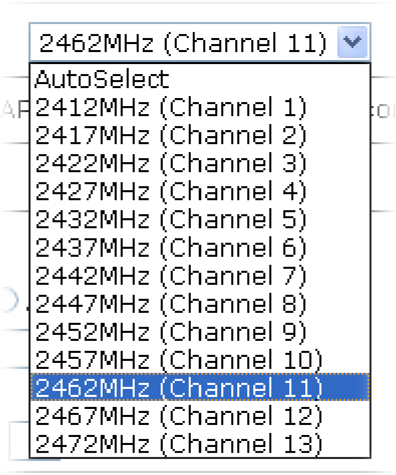
2.The same technology must also be supported in clients to boost WLAN performance.

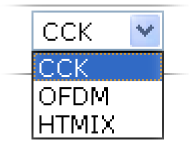
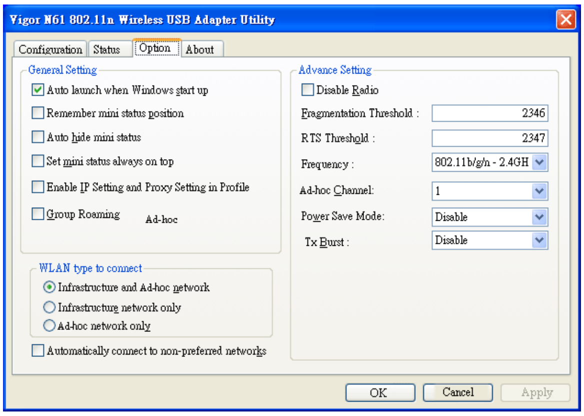
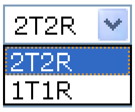
Antenna : 2T2R

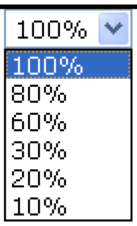
Tx Power : 100%

Channel Width : ● Auto 20/40 MHZ ○ 20 MHZ

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, VigorAP 900 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.  Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)
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.  2462MHz (Channel 11) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 9) 2457MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above.
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.

	 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 900 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. Type the key number if required.
Peer Mac Address	Type the peer MAC address for the access point that VigorAP 900 connects to.
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**).  Vigor N61 802.11n Wireless USB Adapter Utility Configuration | Status | Option | About General Setting ☑ Auto launch when Windows start up □ Remember mini status position □ Auto hide mini status □ Set mini status always on top □ Enable IP Setting and Proxy Setting in Profile □ Group Roaming Ad-hoc WLAN type to connect ● Infrastructure and Ad-hoc network ○ Infrastructure network only ○ Ad-hoc network only □ Automatically connect to non-preferred networks Advance Setting □ Disable Radio Fragmentation Threshold : 2346 RTS Threshold : 2347 Frequency : 802.11b/g/n - 2.4GH Ad-hoc Channel: 1 Power Save Mode: Disable Tx Burst : Disable OK Cancel Apply
Antenna	VigorAP 900 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R. 
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.

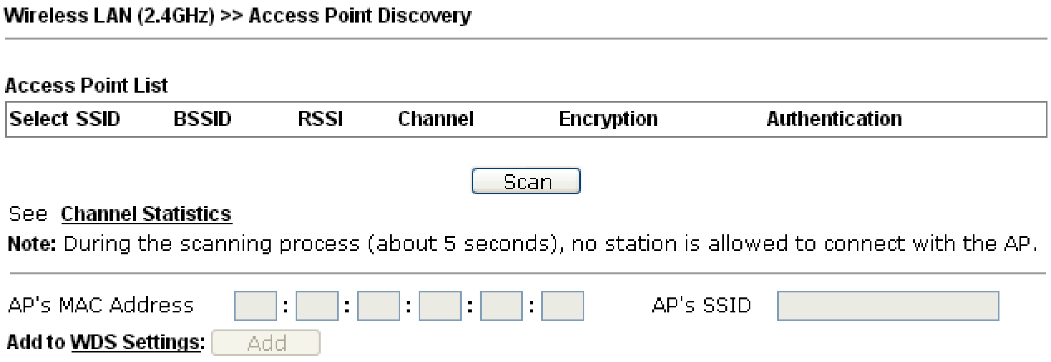
	
Channel Width	**20 MHZ-** the router will use 20Mhz for data transmission and receiving between the AP and the stations. **Auto 20/40 MHZ–** the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.

After finishing this web page configuration, please click **OK** to save the settings.

3.5.2 AP Discovery

VigorAP 900 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 900.

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 900 can be found. Please click **Scan** to discover all the connected APs.



Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Select SSID	BSSID	RSSI	Channel	Encryption	Authentication

See Channel Statistics

Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address : : : : : AP's SSID

Add to WDS Settings:

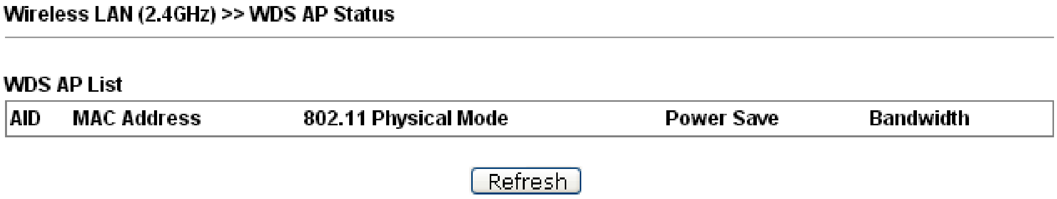
Available settings are explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 900.
BSSID	Display the MAC address of the AP scanned by VigorAP 900.
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 900.
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.
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	Type the MAC address of the AP. Click **Add**. Later, the MAC address of the AP will be added and be shown on WDS settings page.

3.5.3 WDS AP Status

VigorAP 900 can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.



Wireless LAN (2.4GHz) >> WDS AP Status

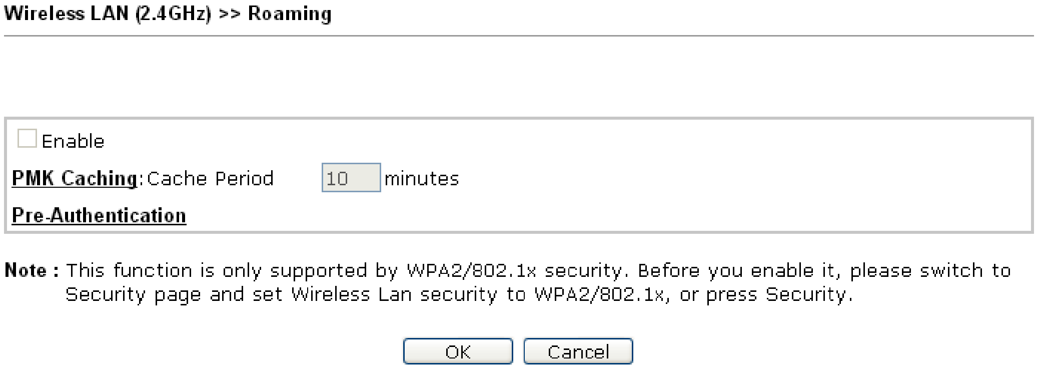
WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth

3.5.4 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.



Wireless LAN (2.4GHz) >> Roaming

□ Enable

PMK Caching: Cache Period 10 minutes

Pre-Authentication

Note : This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

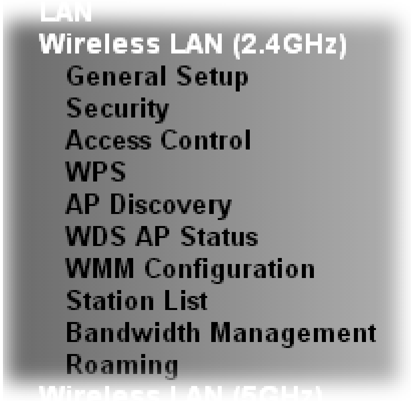
Available settings are explained as follows:

Item	Description
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.

After finishing this web page configuration, please click **OK** to save the settings.

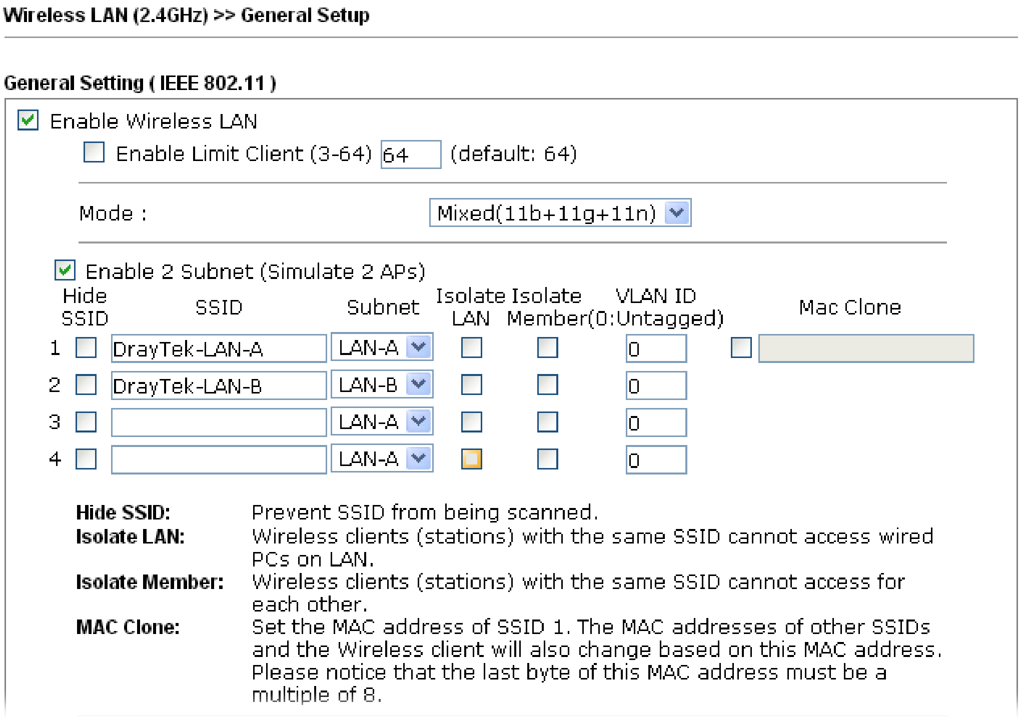
3.6 Wireless LAN Settings for AP Bridge-WDS Mode

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, Station List, Bandwidth Management and Roaming.



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.



Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

□ Enable Limit Client (3-64) 64 (default: 64)

Mode : Mixed(11b+11g+11n)

☑ Enable 2 Subnet (Simulate 2 APs)

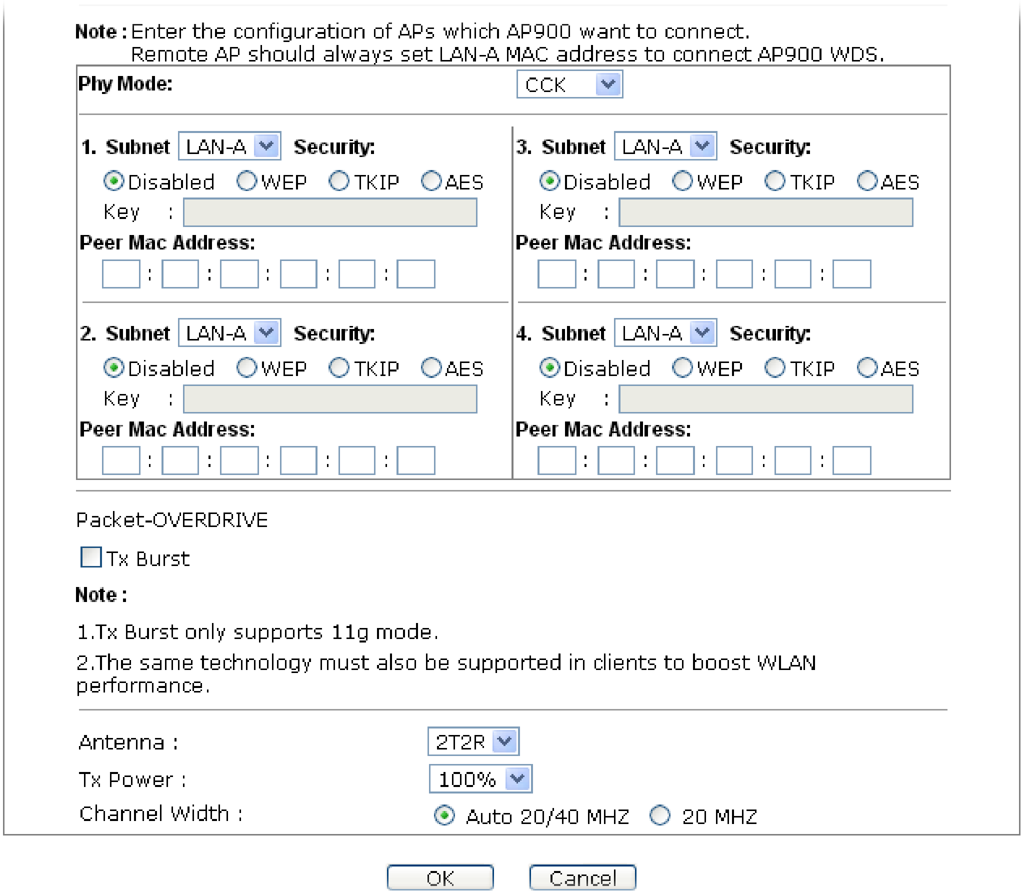
	Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)	Mac Clone
1	□	DrayTek-LAN-A	LAN-A	□	□	0	□
2	□	DrayTek-LAN-B	LAN-B	□	□	0	
3	□		LAN-A	□	□	0	
4	□		LAN-A	□	□	0	

Hide SSID: Prevent SSID from being scanned.

Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.

Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

MAC Clone: Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.



Note : Enter the configuration of APs which AP900 want to connect.
Remote AP should always set LAN-A MAC address to connect AP900 WDS.

Phy Mode: CCK

1. Subnet LAN-A **Security:** ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer Mac Address: ___ : ___ : ___ : ___ : ___ : ___

3. Subnet LAN-A **Security:** ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer Mac Address: ___ : ___ : ___ : ___ : ___ : ___

2. Subnet LAN-A **Security:** ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer Mac Address: ___ : ___ : ___ : ___ : ___ : ___

4. Subnet LAN-A **Security:** ● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer Mac Address: ___ : ___ : ___ : ___ : ___ : ___

Packet-OVERDRIVE

□ Tx Burst

Note :

1.Tx Burst only supports 11g mode.

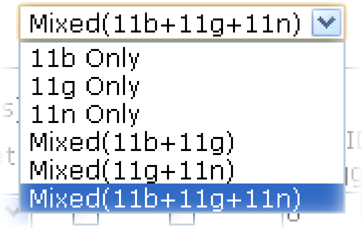
2.The same technology must also be supported in clients to boost WLAN performance.

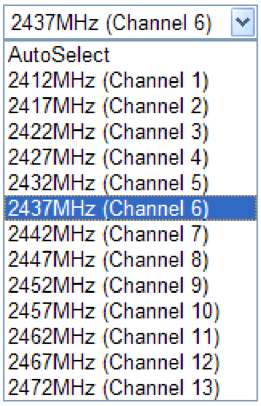
Antenna : 2T2R

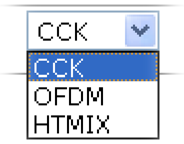
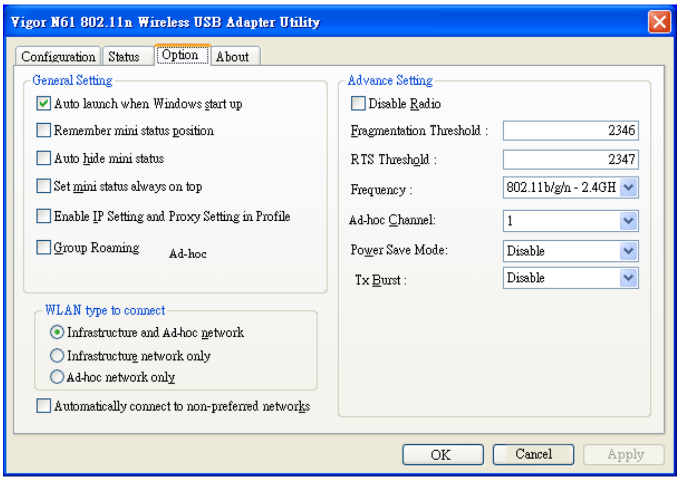
Tx Power : 100%

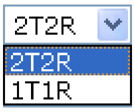
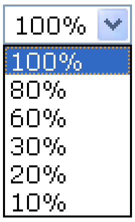
Channel Width : ● Auto 20/40 MHZ ○ 20 MHZ

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor router. The number you can set is from 3 to 64.
Mode	At present, VigorAP 900 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.  Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)
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 900. 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 900 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 900 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 LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
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. 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.  2437MHz (Channel 6) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 9) 2457MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)

Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above. Configure the extension channel you want.
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.  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 900 wants to connect. Each access point should be setup to the same **Phy** mode for connecting with each other.
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 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**).  Vigor N61 802.11n Wireless USB Adapter Utility Configuration | Status | Option | About General Setting ☑ Auto launch when Windows start up □ Remember mini status position □ Auto hide mini status □ Set mini status always on top □ Enable IP Setting and Proxy Setting in Profile □ Group Roaming Ad-hoc WLAN type to connect ● Infrastructure and Ad-hoc network ○ Infrastructure network only ○ Ad-hoc network only □ Automatically connect to non-preferred networks Advance Setting □ Disable Radio Fragmentation Threshold : 2346 RTS Threshold : 2347 Frequency : 802.11b/g/n - 2.4GH Ad-hoc Channel: 1 Power Save Mode: Disable Tx Burst : Disable OK Cancel Apply

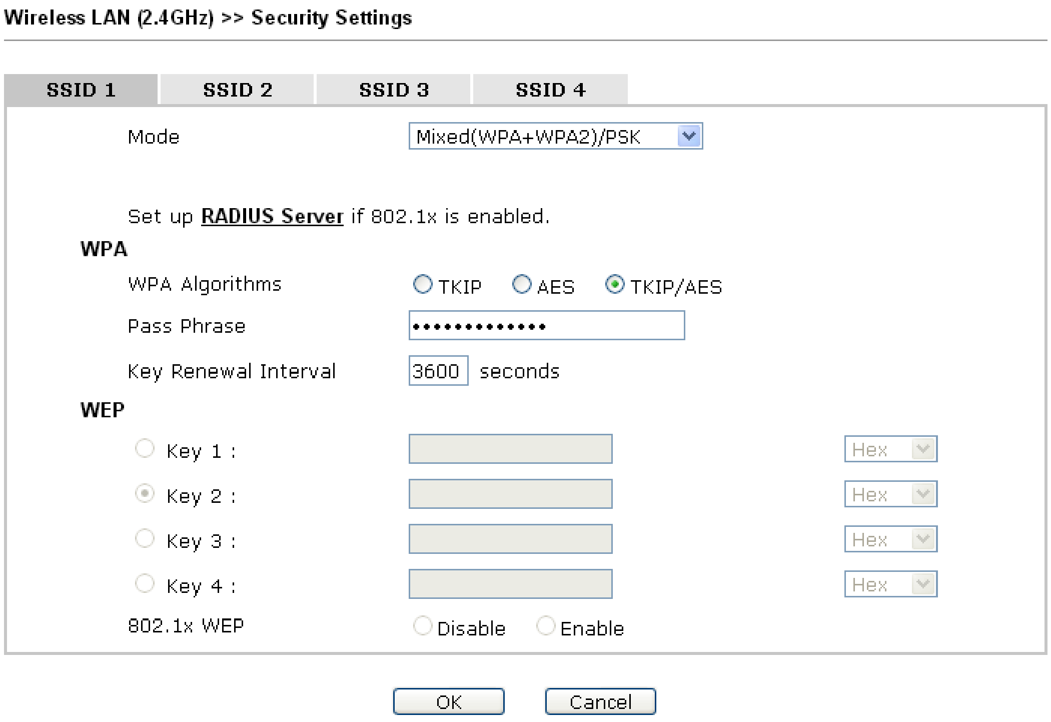
Antenna	VigorAP 900 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R. 
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless. 
Channel Width	**20 MHZ-** the router will use 20Mhz for data transmission and receiving between the AP and the stations. **Auto 20/40 MHZ–** the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.

After finishing this web page configuration, please click **OK** to save the settings.

3.6.2 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.



Wireless LAN (2.4GHz) >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

Mode: Mixed(WPA+WPA2)/PSK

Set up **RADIUS Server** if 802.1x is enabled.

WPA

WPA Algorithms: ○ TKIP ○ AES ● TKIP/AES

Pass Phrase: •••••••••••••

Key Renewal Interval: 3600 seconds

WEP

○ Key 1 : Hex

● Key 2 : Hex

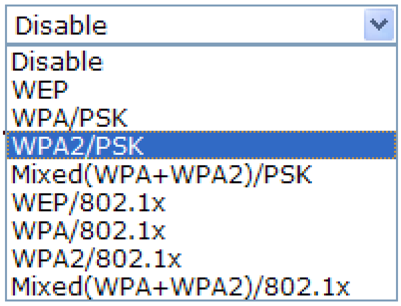
○ Key 3 : Hex

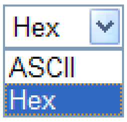
○ Key 4 : Hex

802.1x WEP: ○ Disable ○ Enable

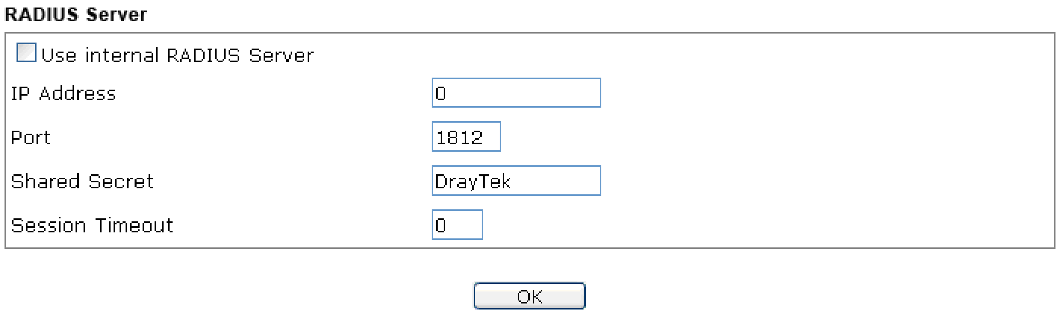
OK | Cancel

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.  Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x **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 900 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.
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.



RADIUS Server

☐ Use internal RADIUS Server

IP Address	0
Port	1812
Shared Secret	DrayTek
Session Timeout	0

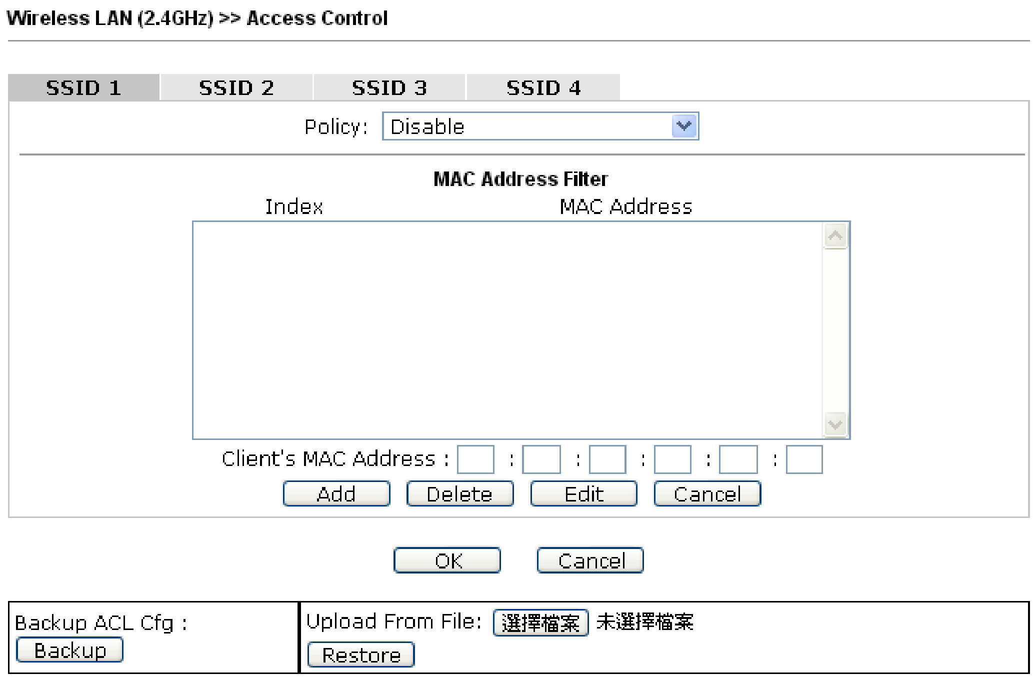
Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 900 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, **3.9 RADIUS Server** to configure settings for internal server of VigorAP 900.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external 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.)

After finishing this web page configuration, please click **OK** to save the settings.

3.6.3 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).


Wireless LAN (2.4GHz) >> Access Control

SSID 1 | SSID 2 | SSID 3 | SSID 4

Policy: Disable

MAC Address Filter

Index MAC Address

Client's MAC Address : __ : __ : __ : __ : __ : __

Add Delete Edit Cancel

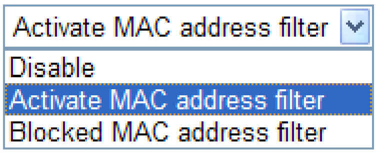
OK Cancel

Backup ACL Cfg : Backup

Upload From File: 選擇檔案 未選擇檔案

Restore

Available settings are explained as follows:

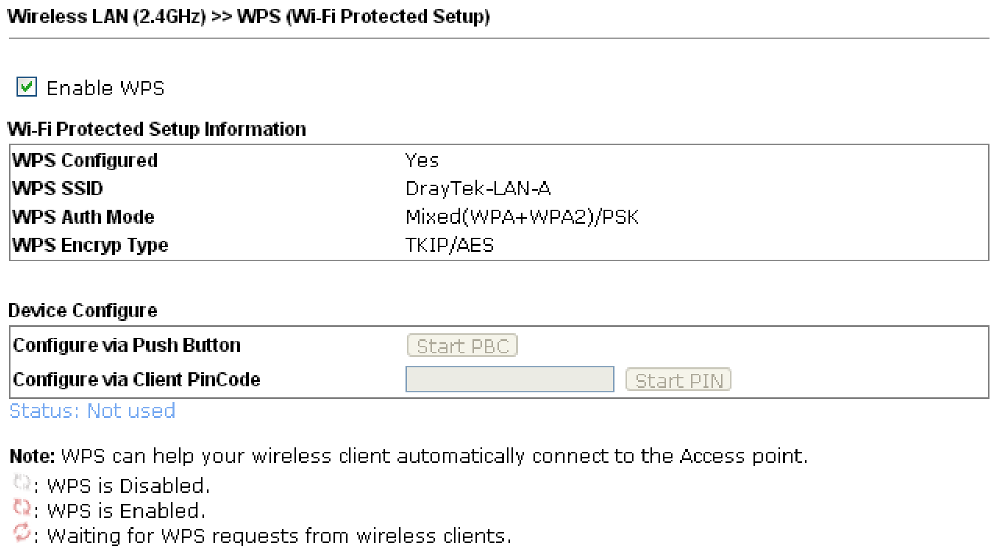
Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 900.  Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter
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.
Backup	Click it to store the settings (MAC addresses on MAC Address

	Filter table) on this page as a file.
Restore	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

3.6.4 WPS

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



Wireless LAN (2.4GHz) >> WPS (Wi-Fi Protected Setup)

☑ Enable WPS

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek-LAN-A
WPS Auth Mode	Mixed(WPA+WPA2)/PSK
WPS Encryp Type	TKIP/AES

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	▭ Start PIN

Status: Not used

Note: WPS can help your wireless client automatically connect to the Access point.

⟳: WPS is Disabled.

⟳: WPS is Enabled.

⟳: Waiting for WPS requests from wireless clients.

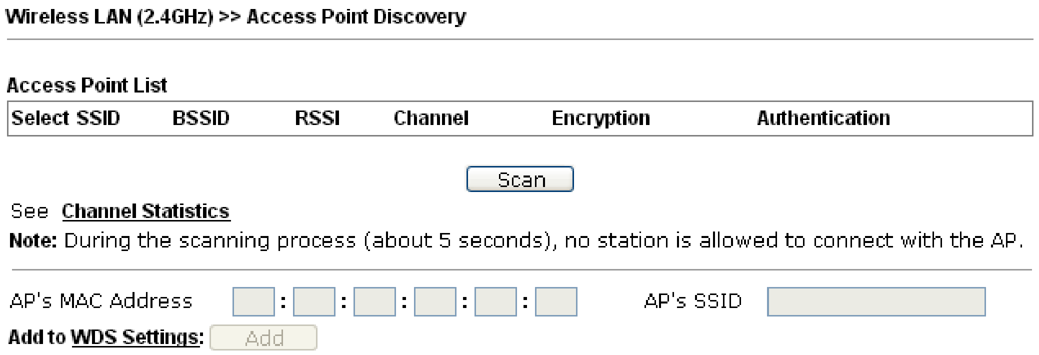
Available settings are explained as follows:

Item	Description
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 900 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 900r. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 900.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 900 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 900 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 900 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).

3.6.5 AP Discovery

VigorAP 900 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 900 can be found. Please click **Scan** to discover all the connected APs.



Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Select SSID	BSSID	RSSI	Channel	Encryption	Authentication

Scan

See **Channel Statistics**

Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address : : : : : AP's SSID

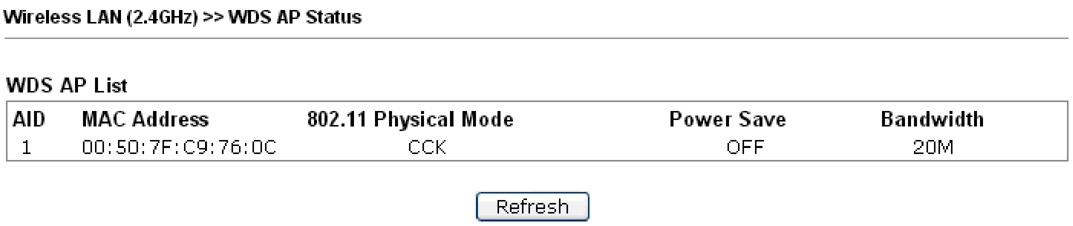
Add to WDS Settings: Add

Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 900.
BSSID	Display the MAC address of the AP scanned by VigorAP 900.
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 900.
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.
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.

3.6.6 WDS AP Status

VigorAP 900 can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.



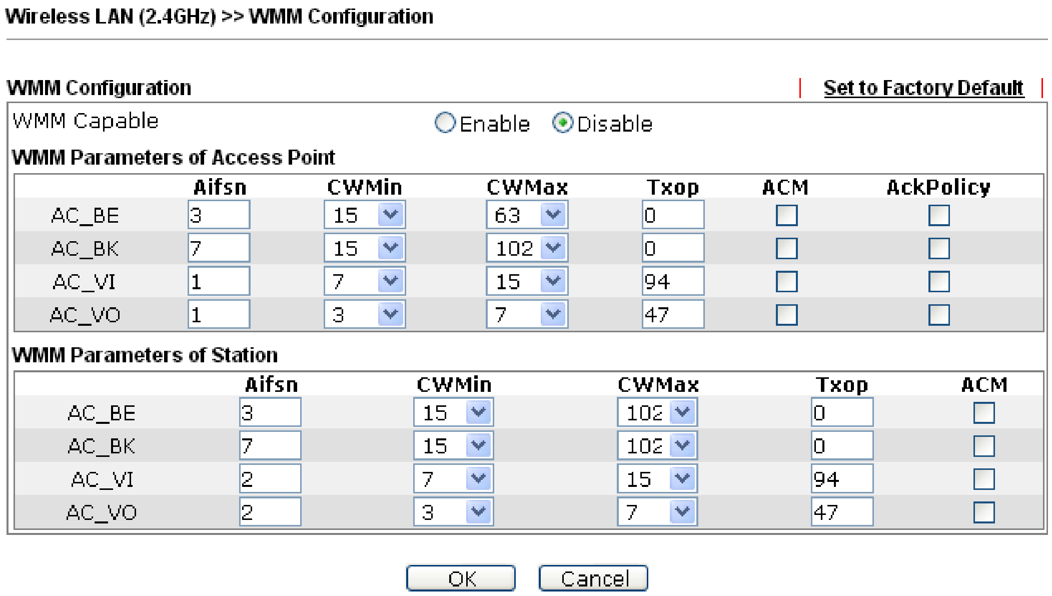
Wireless LAN (2.4GHz) >> WDS AP Status

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
1	00:50:7F:C9:76:0C	CCK	OFF	20M

3.6.7 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.



Wireless LAN (2.4GHz) >> WMM Configuration

WMM Configuration | Set to Factory Default |

WMM Capable ○ Enable ● Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	102	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	☐
AC_BK	7	15	102	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Available settings are explained as follows:

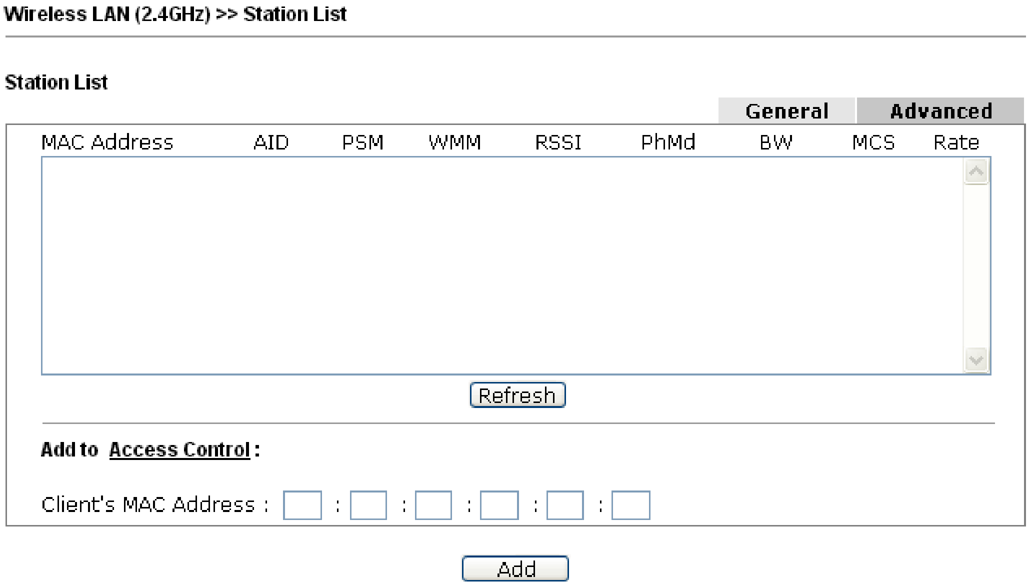
Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from

	1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. **Note:** Vigor2920 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	**"**Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

After finishing this web page configuration, please click **OK** to save the settings.

3.6.8 Station List

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



Wireless LAN (2.4GHz) >> Station List

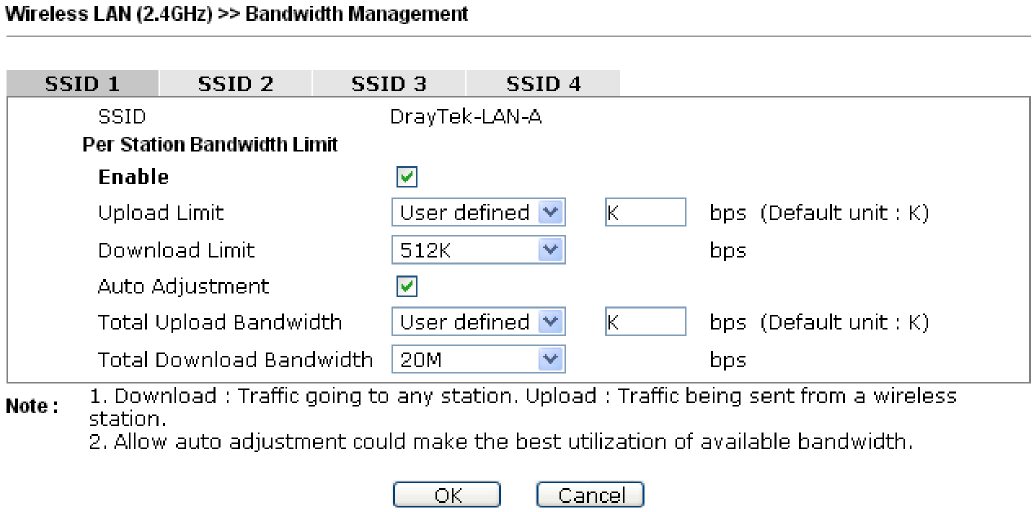
Station List

Available settings are explained as follows:

Item	Description
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.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
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.
General/Advanced	**General** – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. **Advanced** – Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

3.6.9 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.



Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1 | SSID 2 | SSID 3 | SSID 4

SSID	DrayTek-LAN-A		
Per Station Bandwidth Limit			
Enable	☑		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	512K		bps
Auto Adjustment	☑		
Total Upload Bandwidth	User defined	K	bps (Default unit : K)
Total Download Bandwidth	20M		bps

Note : 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.
2. Allow auto adjustment could make the best utilization of available bandwidth.

Available settings are explained as follows:

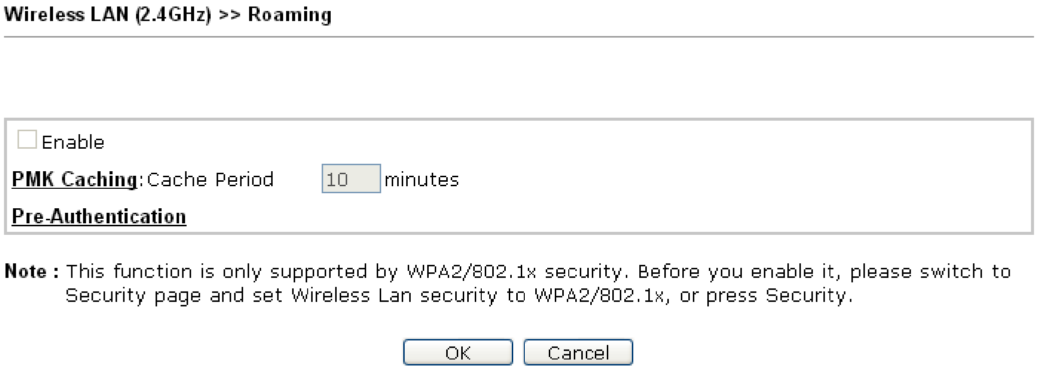
Item	Description
SSID	Display the specific SSID name of the router.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Download Limit	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Auto Adjustment	Check this box to have the bandwidth limit determined by the system automatically.
Total Upload Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data uploading.
Total Download Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data downloading.

After finishing this web page configuration, please click **OK** to save the settings.

3.6.10 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.



Wireless LAN (2.4GHz) >> Roaming

□ Enable

PMK Caching: Cache Period 10 minutes

Pre-Authentication

Note : This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

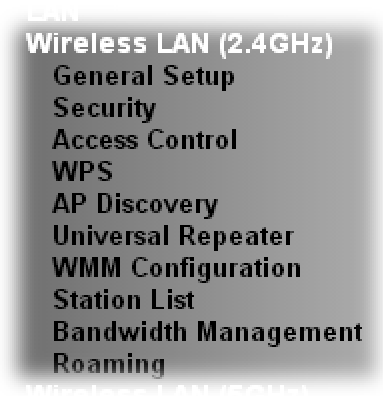
Available settings are explained as follows:

Item	Description
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.

After finishing this web page configuration, please click **OK** to save the settings.

3.7 Wireless LAN Settings for Universal Repeater Mode

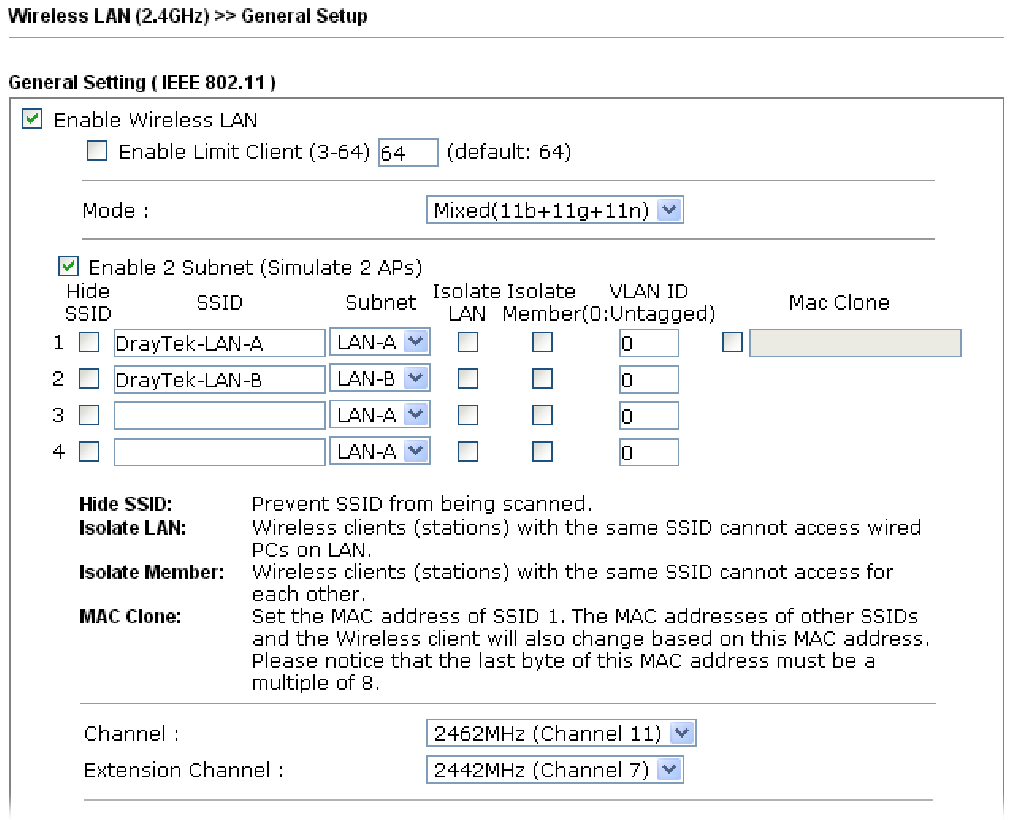
When you choose Universal Repeater as the operation mode, the Wireless LAN menu items will include General Setup, Security, WPS, AP Discovery, Universal Repeater and Station List.



3.7.1 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.



Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

□ Enable Limit Client (3-64) 64 (default: 64)

Mode : Mixed(11b+11g+11n)

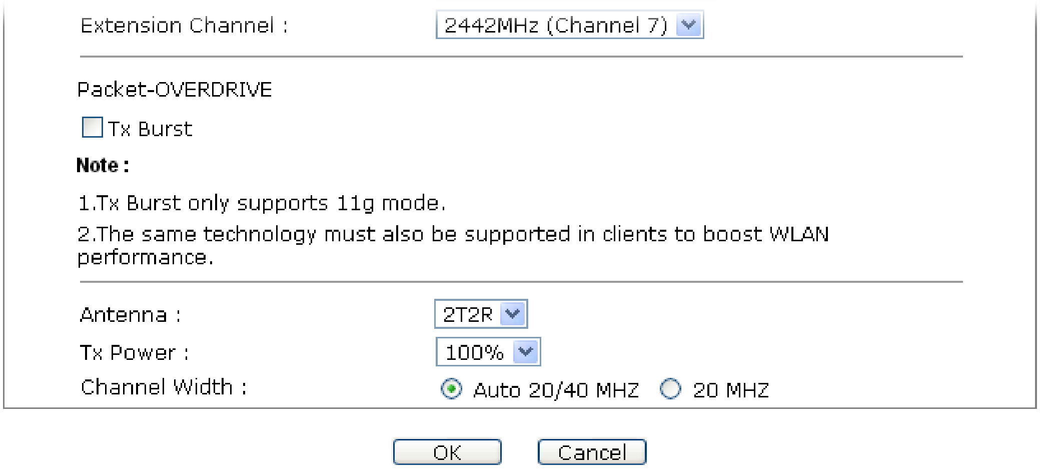
☑ Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)	Mac Clone
1	□	DrayTek-LAN-A	LAN-A	□	□	0	□
2	□	DrayTek-LAN-B	LAN-B	□	□	0	
3	□		LAN-A	□	□	0	
4	□		LAN-A	□	□	0	

Hide SSID: Prevent SSID from being scanned.
Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.
Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.
MAC Clone: Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.

Channel : 2462MHz (Channel 11)

Extension Channel : 2442MHz (Channel 7)


Extension Channel : 2442MHz (Channel 7)

Packet-OVERDRIVE

□ Tx Burst

Note :

1.Tx Burst only supports 11g mode.

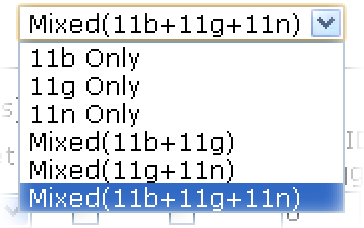
2.The same technology must also be supported in clients to boost WLAN performance.

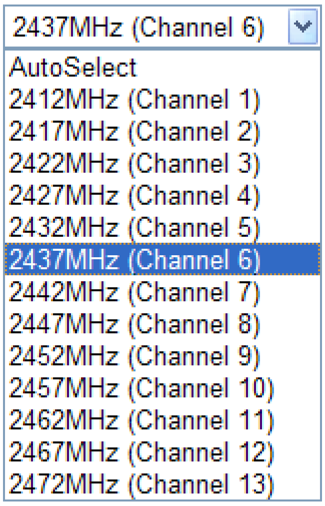
Antenna : 2T2R

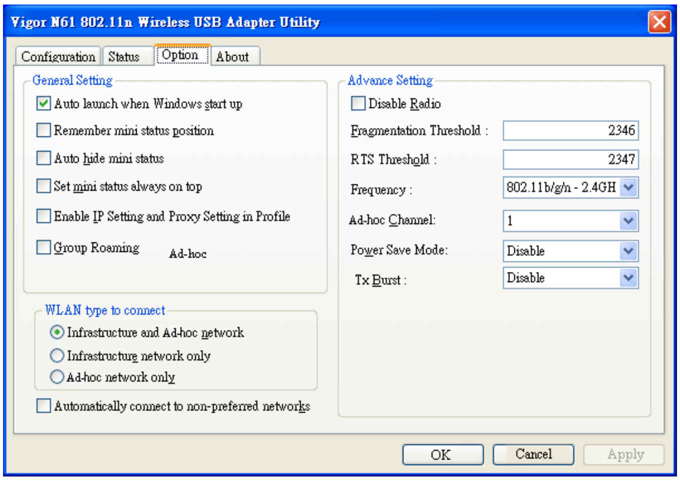
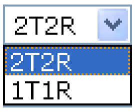
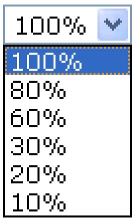
Tx Power : 100%

Channel Width : ● Auto 20/40 MHZ ○ 20 MHZ

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor router. The number you can set is from 3 to 64.
Mode	At present, VigorAP 900 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.  Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)
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 900. 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 900 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 900 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 LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
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. 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.  2437MHz (Channel 6) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 9) 2457MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above. Configure the extension channel you want.
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.

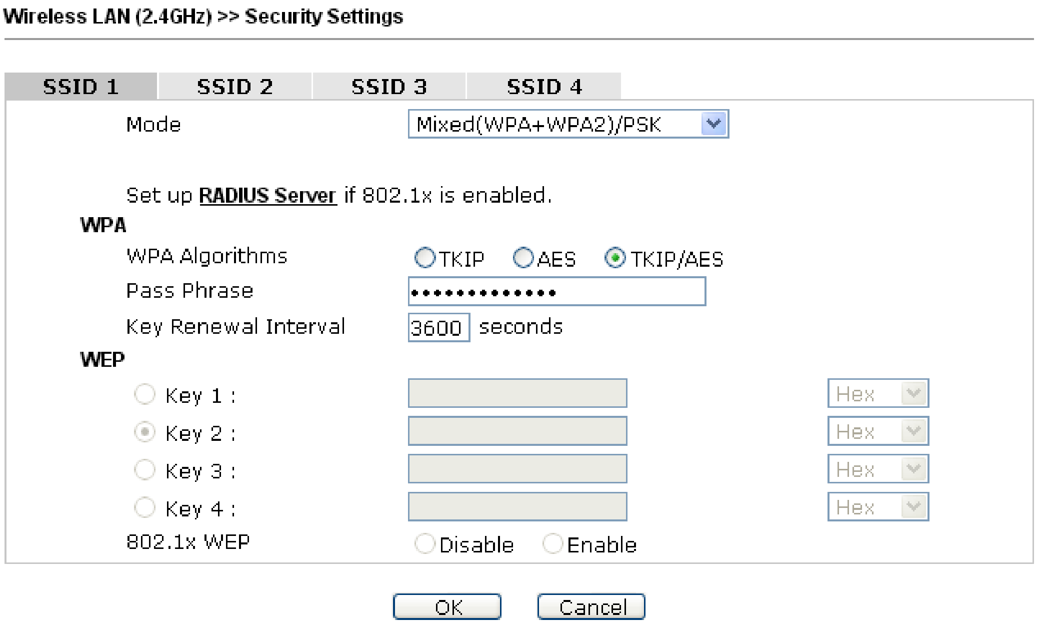
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and 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**).  Vigor N61 802.11n Wireless USB Adapter Utility Configuration | Status | Option | About General Setting ☑ Auto launch when Windows start up ☐ Remember mini status position ☐ Auto hide mini status ☐ Set mini status always on top ☐ Enable IP Setting and Proxy Setting in Profile ☐ Group Roaming Ad-hoc WLAN type to connect ● Infrastructure and Ad-hoc network ○ Infrastructure network only ○ Ad-hoc network only ☐ Automatically connect to non-preferred networks Advance Setting ☐ Disable Radio Fragmentation Threshold : 2346 RTS Threshold : 2347 Frequency : 802.11b/g/n - 2.4GH Ad-hoc Channel: 1 Power Save Mode: Disable Tx Burst : Disable OK Cancel Apply
Antenna	VigorAP 900 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.  2T2R 2T2R 1T1R
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.  100% 100% 80% 60% 30% 20% 10%
Channel Width	**20 MHZ-** the router will use 20Mhz for data transmission and receiving between the AP and the stations. **Auto 20/40 MHZ–** the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.

After finishing this web page configuration, please click **OK** to save the settings.

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.



Wireless LAN (2.4GHz) >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

Mode: Mixed(WPA+WPA2)/PSK

Set up **RADIUS Server** if 802.1x is enabled.

WPA

WPA Algorithms: ○ TKIP ○ AES ● TKIP/AES

Pass Phrase: •••••••••••••

Key Renewal Interval: 3600 seconds

WEP

○ Key 1 : Hex

● Key 2 : Hex

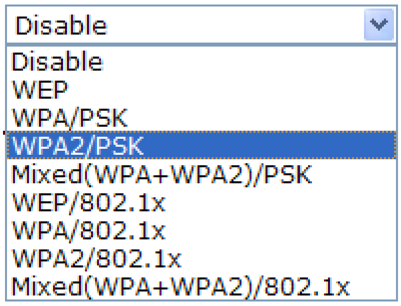
○ Key 3 : Hex

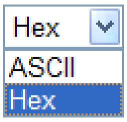
○ Key 4 : Hex

802.1x WEP: ○ Disable ○ Enable

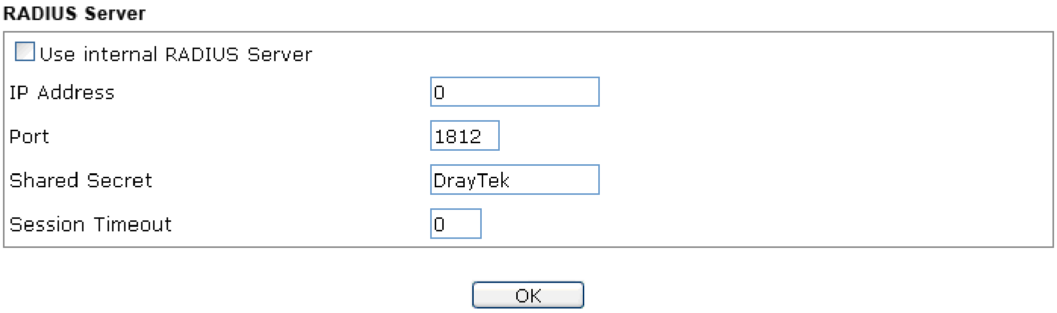
OK Cancel

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.  Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x **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 900 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.
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.



RADIUS Server

☐ Use internal RADIUS Server

IP Address	0
Port	1812
Shared Secret	DrayTek
Session Timeout	0

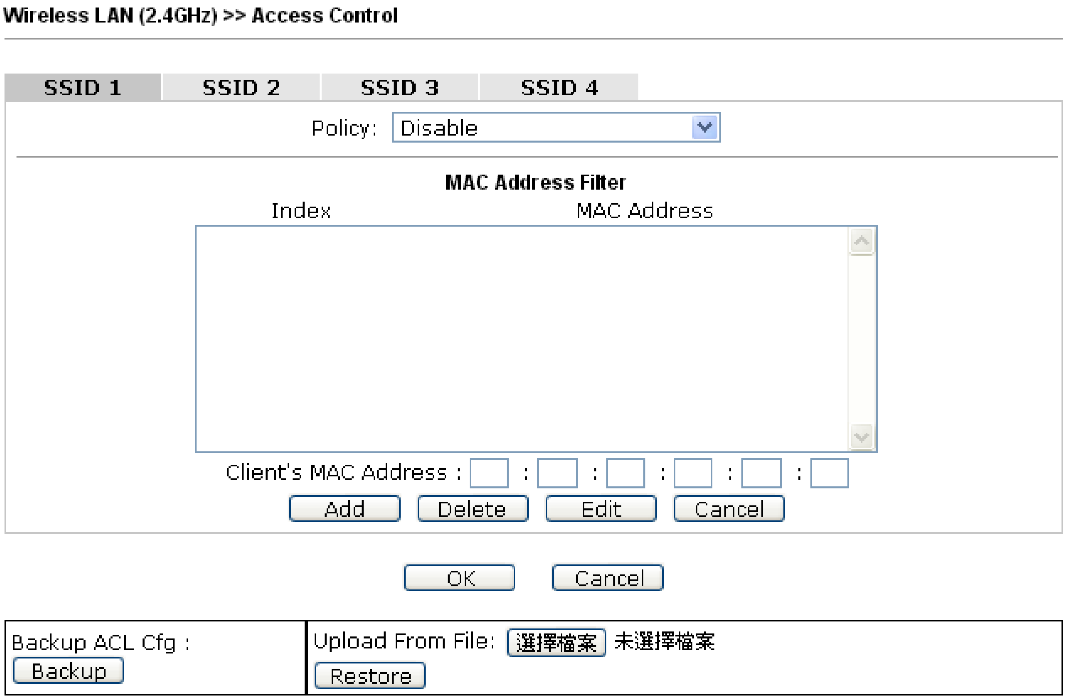
Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 900 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, **3.9 RADIUS Server** to configure settings for internal server of VigorAP 900.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external 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.)

After finishing this web page configuration, please click **OK** to save the settings.

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).



Wireless LAN (2.4GHz) >> Access Control

SSID 1 | SSID 2 | SSID 3 | SSID 4

Policy: Disable

MAC Address Filter

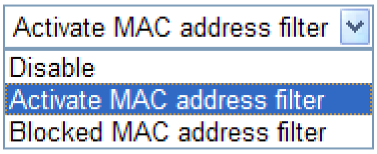
Index | MAC Address

Client's MAC Address : __ : __ : __ : __ : __ : __

Backup ACL Cfg : Backup

Upload From File: 選擇檔案 未選擇檔案

Available settings are explained as follows:

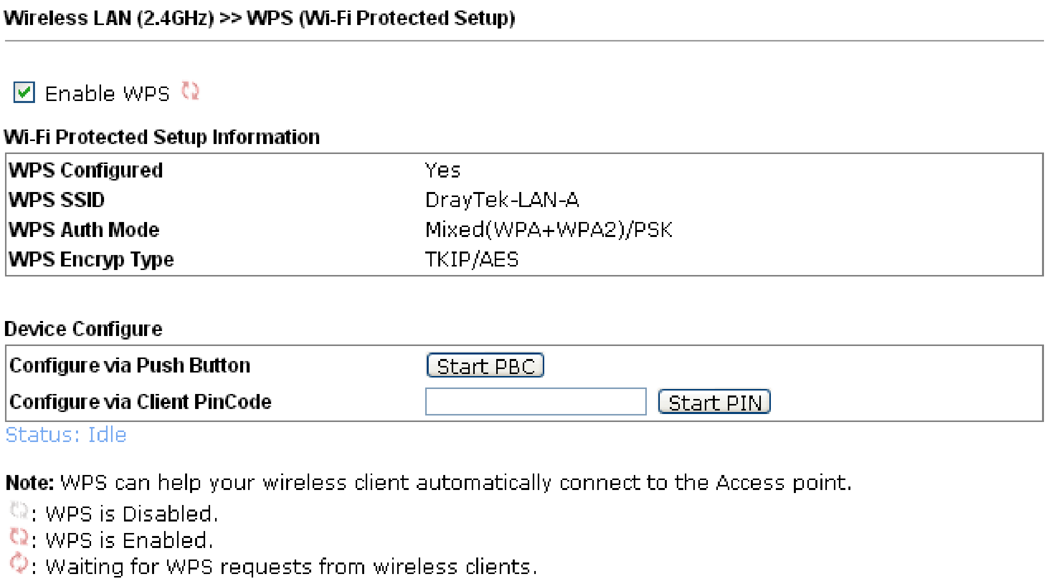
Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 900.  Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter
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.

Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

3.7.4 WPS

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



Wireless LAN (2.4GHz) >> WPS (Wi-Fi Protected Setup)

☑ Enable WPS

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek-LAN-A
WPS Auth Mode	Mixed(WPA+WPA2)/PSK
WPS Encryp Type	TKIP/AES

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: Idle

Note: WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

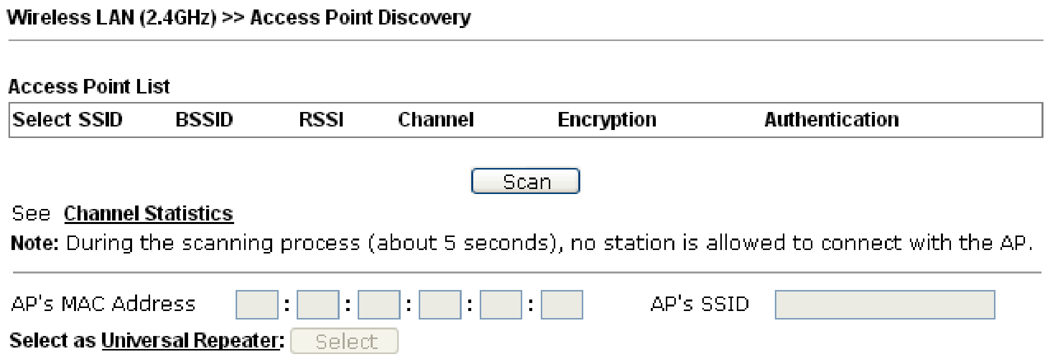
Available settings are explained as follows:

Item	Description
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 900 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 900. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 900.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 900 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 900 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 900 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).

3.7.5 AP Discovery

VigorAP 900 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 900 can be found. Please click **Scan** to discover all the connected APs.



Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Select SSID	BSSID	RSSI	Channel	Encryption	Authentication

See Channel Statistics

Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address □ : □ : □ : □ : □ : □ AP's SSID □

Select as Universal Repeater: Select

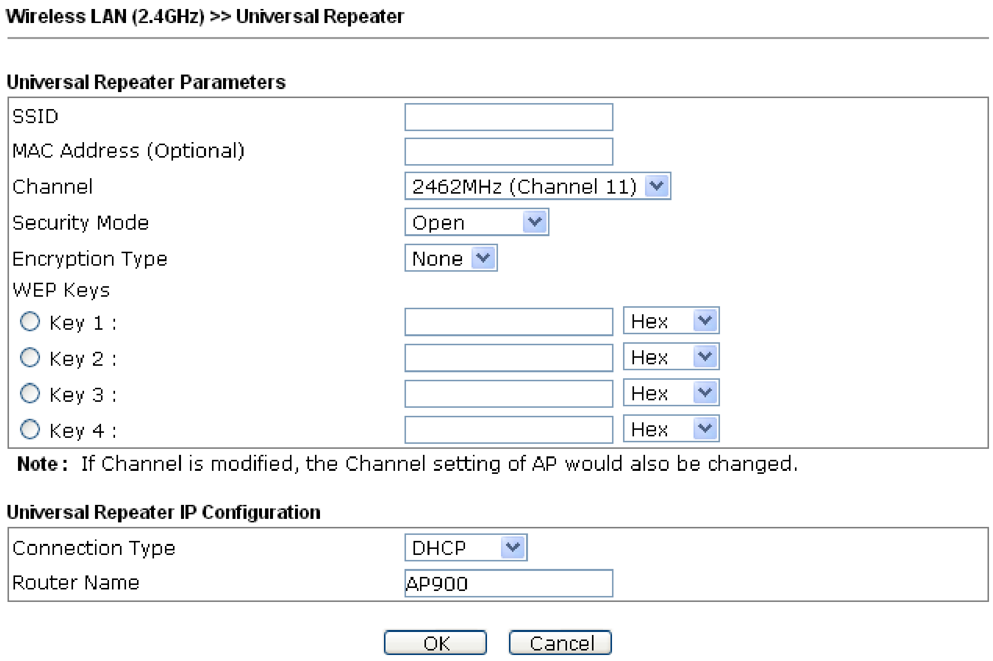
Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 900.
BSSID	Display the MAC address of the AP scanned by VigorAP 900.
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 900.
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.
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 and the wireless AP can be selected as a universal repeater. Choose one of the wireless APs from the Scan list.

3.7.6 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.



Wireless LAN (2.4GHz) >> Universal Repeater

Universal Repeater Parameters

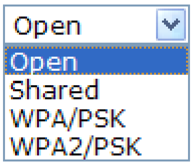
SSID		
MAC Address (Optional)		
Channel	2462MHz (Channel 11)	
Security Mode	Open	
Encryption Type	None	
WEP Keys		
○ Key 1 :		Hex
○ Key 2 :		Hex
○ Key 3 :		Hex
○ Key 4 :		Hex

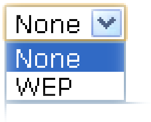
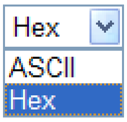
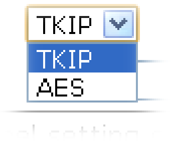
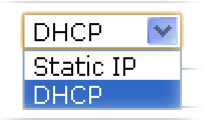
Note : If Channel is modified, the Channel setting of AP would also be changed.

Universal Repeater IP Configuration

Connection Type	DHCP
Router Name	AP900

Available settings are explained as follows:

Item	Description
SSID	Set the name of access point that VigorAP 900 wants to connect to.
MAC Address (Optional)	Type the MAC address of access point that VigorAP 900 wants to connect to.
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.
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. 
Encryption Type for	This option is available when Open/Shared is selected as

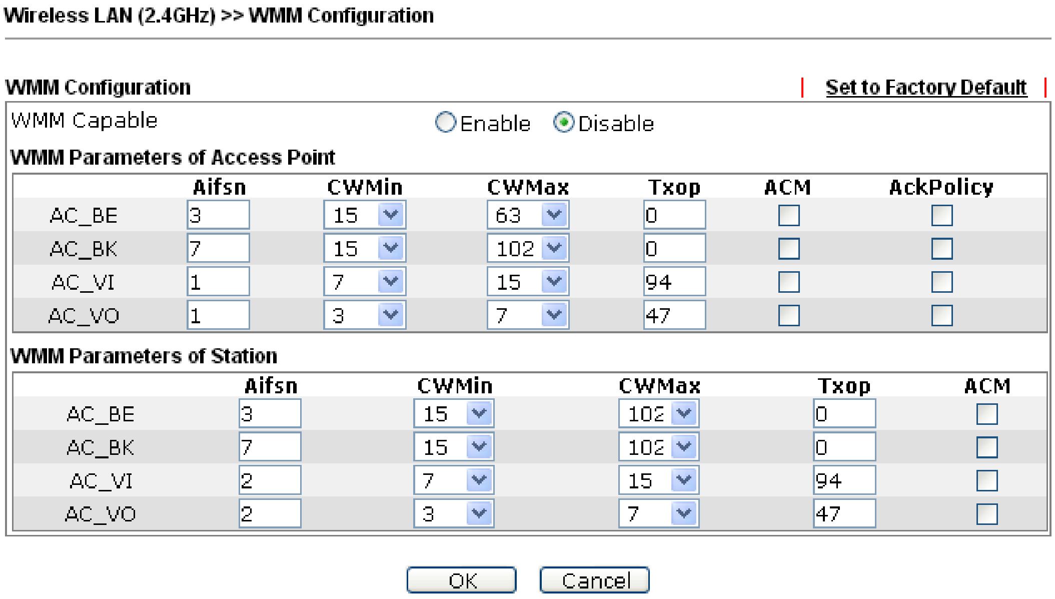
Open/Shared	Security Mode. Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose **WEP**.  **WEP Keys -** Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key 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 ','. 
Encryption Type for WPA/PSK and WPA2/PSK	This option is available when WPA/PSK or WPA2/PSK is selected as **Security Mode**. 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...").
Connection Type	Choose DHCP or Static IP as the connection mode. **DHCP** – The wireless station will be assigned with an IP from Vigor router. **Static IP** – The wireless station shall specify a static IP for connecting to Internet via Vigor router. 
Router Name	Type a name for the router as identification. Simply use the default name.
IP Address	This setting is available when **Static IP** is selected as **Connection Type**. Type an IP address with the same network segment of the LAN IP setting of the router. Such IP shall be different with any IP address in LAN.
Subnet Mask	This setting is available when **Static IP** is selected as **Connection Type**.

	Type the subnet mask setting which shall be the same as the one configured in LAN for the router.
Default Gateway	This setting is available when **Static IP** is selected as **Connection Type**. Type the gateway setting which shall be the same as the default gateway configured in LAN for the router.

After finishing this web page configuration, please click **OK** to save the settings.

3.7.7 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.



Wireless LAN (2.4GHz) >> WMM Configuration

WMM Configuration | Set to Factory Default |

WMM Capable ○ Enable ● Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	102	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	□
AC_BK	7	15	102	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

Available settings are explained as follows:

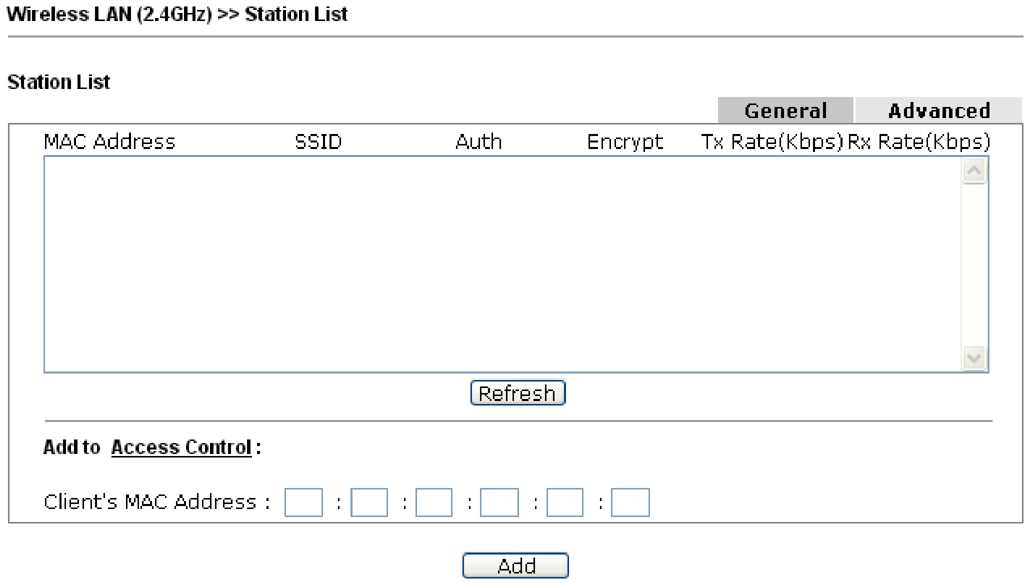
Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories

	must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. **Note:** Vigor2920 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	**"**Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

After finishing this web page configuration, please click **OK** to save the settings.

3.7.8 Station List

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



Wireless LAN (2.4GHz) >> Station List

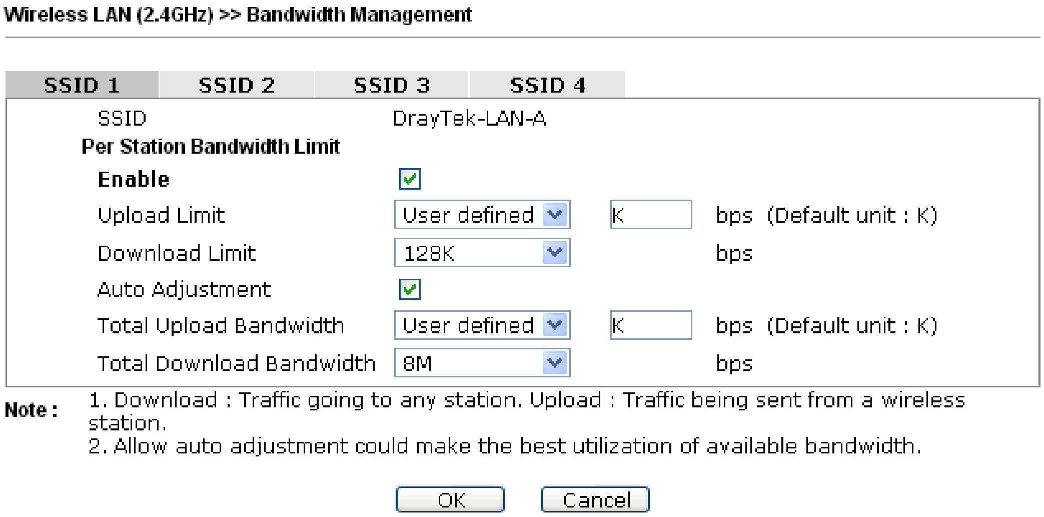
Station List

Available settings are explained as follows:

Item	Description
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.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
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.
General/Advanced	**General** – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. **Advanced** – Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

3.7.9 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.



Wireless LAN (2.4GHz) >> Bandwidth Management

SSID DrayTek-LAN-A

Per Station Bandwidth Limit

Enable ☑

Upload Limit: User defined, K bps (Default unit : K)

Download Limit: 128K bps

Auto Adjustment ☑

Total Upload Bandwidth: User defined, K bps (Default unit : K)

Total Download Bandwidth: 8M bps

Note : 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.
2. Allow auto adjustment could make the best utilization of available bandwidth.

Available settings are explained as follows:

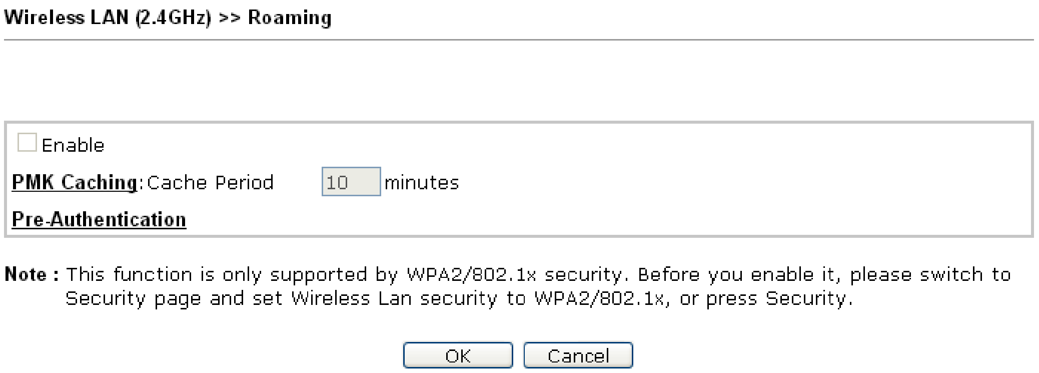
Item	Description
SSID	Display the specific SSID name of the router.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Download Limit	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Auto Adjustment	Check this box to have the bandwidth limit determined by the system automatically.
Total Upload Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data uploading.
Total Download Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data downloading.

After finishing this web page configuration, please click **OK** to save the settings.

3.7.10 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.


Wireless LAN (2.4GHz) >> Roaming

□ Enable

PMK Caching: Cache Period 10 minutes

Pre-Authentication

Note : This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

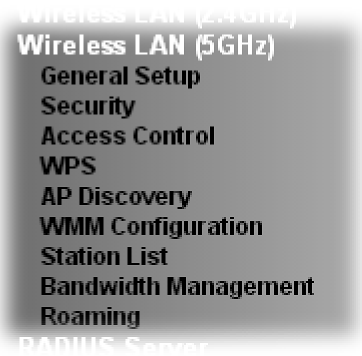
Available settings are explained as follows:

Item	Description
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.

After finishing this web page configuration, please click **OK** to save the settings.

3.8 Wireless LAN (5GHz) Settings for AP Mode

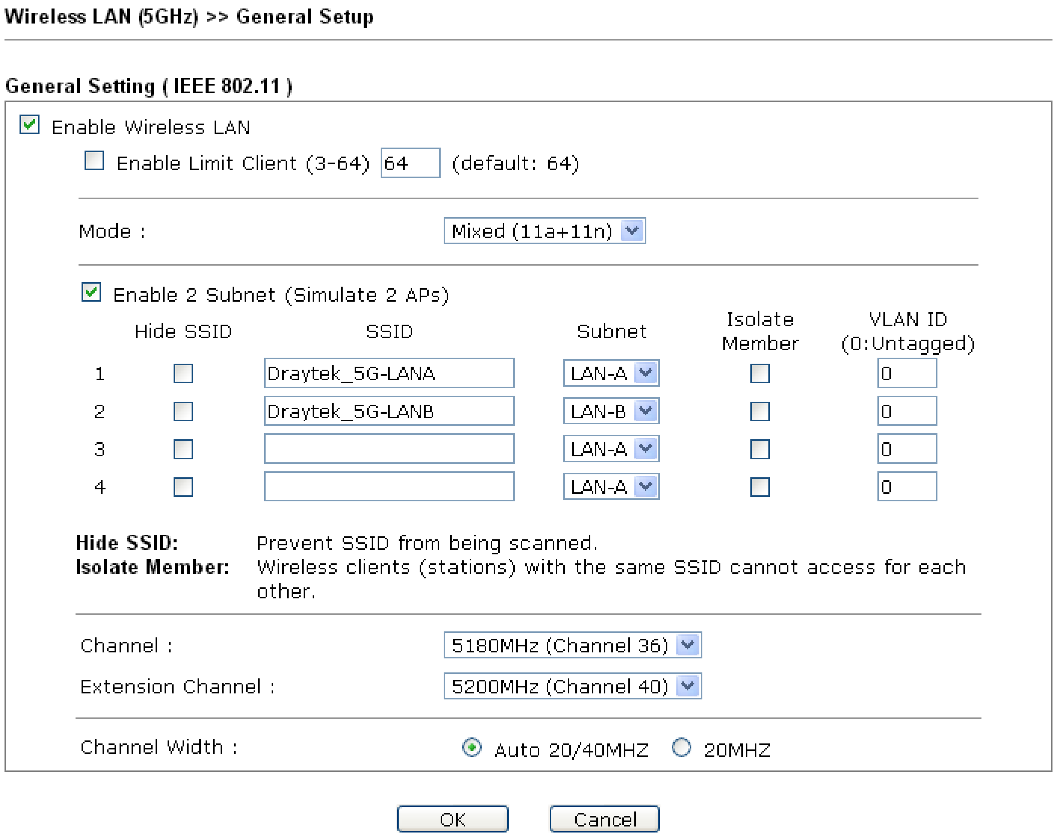
When a 5G Dongle connects to VigorAP 900, only AP mode (the operation mode) is available for configuration. The AP mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.



If no 5G dongle connected to VigorAP 900, an error message will be displayed and no function in this menu can be activated.

3.8.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the general settings for wireless connection such as specifying SSID, selecting the wireless channel, isolate LAN connection and so on.



Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

□ Enable Limit Client (3-64) 64 (default: 64)

Mode : Mixed (11a+11n)

☑ Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0:Untagged)
1	□	Draytek_5G-LANA	LAN-A	□	0
2	□	Draytek_5G-LANB	LAN-B	□	0
3	□		LAN-A	□	0
4	□		LAN-A	□	0

Hide SSID: Prevent SSID from being scanned.
Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

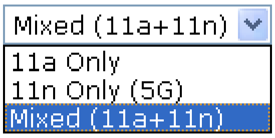
Channel : 5180MHz (Channel 36)

Extension Channel : 5200MHz (Channel 40)

Channel Width : ● Auto 20/40MHZ ○ 20MHZ

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.

Enable Limit Client	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor router. The number you can set is from 3 to 64.
Mode	At present, VigorAP 900 can be connected by 11a only, 11n only (5G), Mixed (11a+11n) stations simultaneously. Simply choose Mixed (11a+11n) mode.  Mixed (11a+11n) 11a Only 11n Only (5G) Mixed (11a+11n)
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 900. 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 900 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 900 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.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
Channel	Means the channel of frequency of the wireless LAN. The default channel is **36**. You may switch channel if the selected channel is under serious interference.
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above.

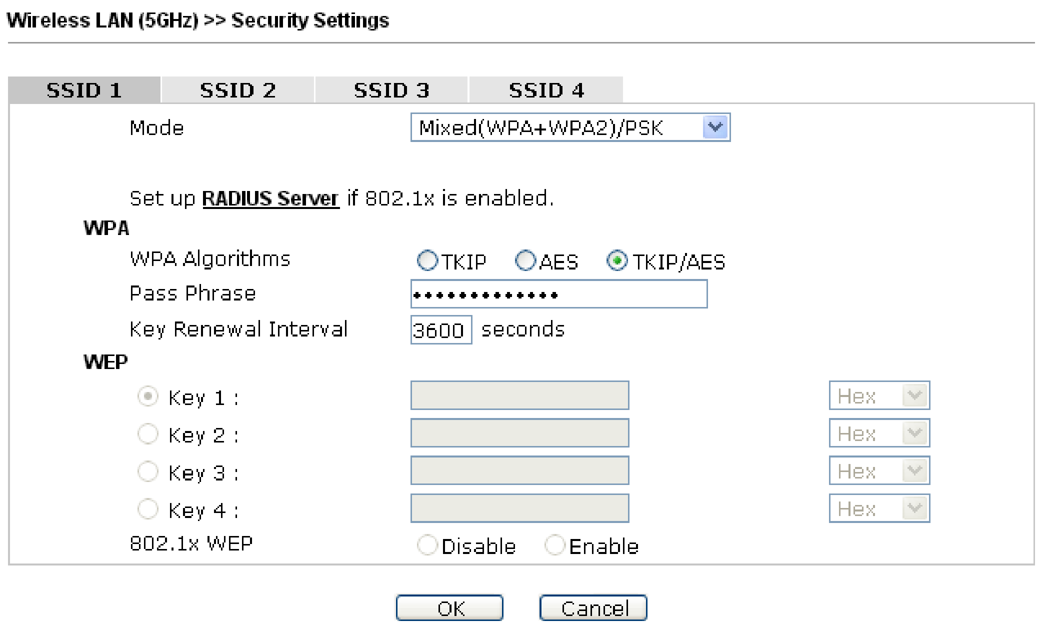
Channel Width	**20 MHZ-** the router will use 20Mhz for data transmission and receiving between the AP and the stations. **Auto 20/40 MHZ–** the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.

After finishing this web page configuration, please click **OK** to save the settings.

3.8.2 Security

This page allows you to set security with different modes for SSID 1, 2, and 3 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.



Wireless LAN (5GHz) >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

Mode: Mixed(WPA+WPA2)/PSK

Set up RADIUS Server if 802.1x is enabled.

WPA

WPA Algorithms: ○ TKIP ○ AES ● TKIP/AES

Pass Phrase: •••••••••••••

Key Renewal Interval: 3600 seconds

WEP

● Key 1 : Hex

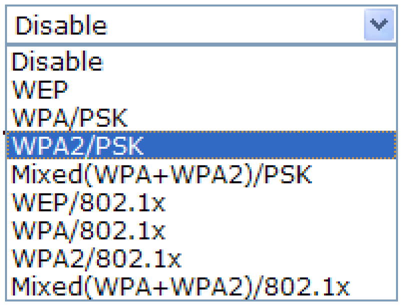
○ Key 2 : Hex

○ Key 3 : Hex

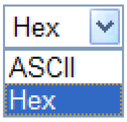
○ Key 4 : Hex

802.1x WEP: ○ Disable ○ Enable

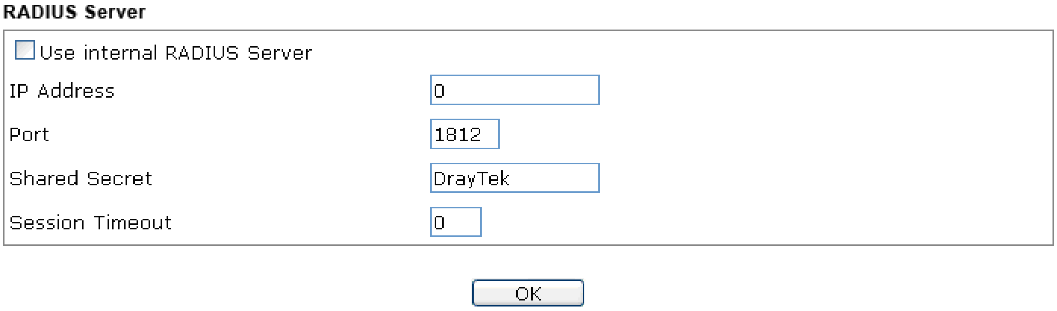
Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.  Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x **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 900 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.



RADIUS Server

☐ Use internal RADIUS Server

IP Address	0
Port	1812
Shared Secret	DrayTek
Session Timeout	0

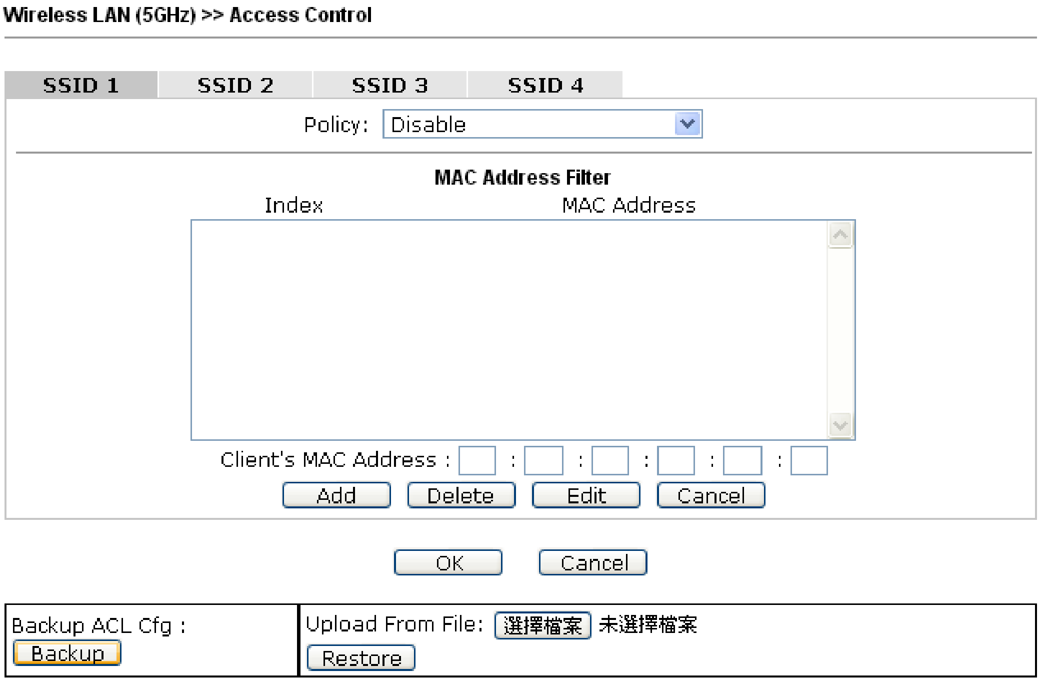
Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 900 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, **3.9 RADIUS Server** to configure settings for internal server of VigorAP 900.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external 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.)

After finishing this web page configuration, please click **OK** to save the settings.

3.8.3 Access Control

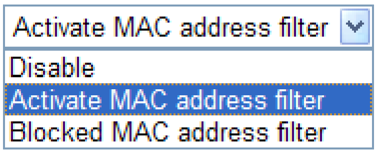
For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, 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: Disable

未選擇檔案

Available settings are explained as follows:

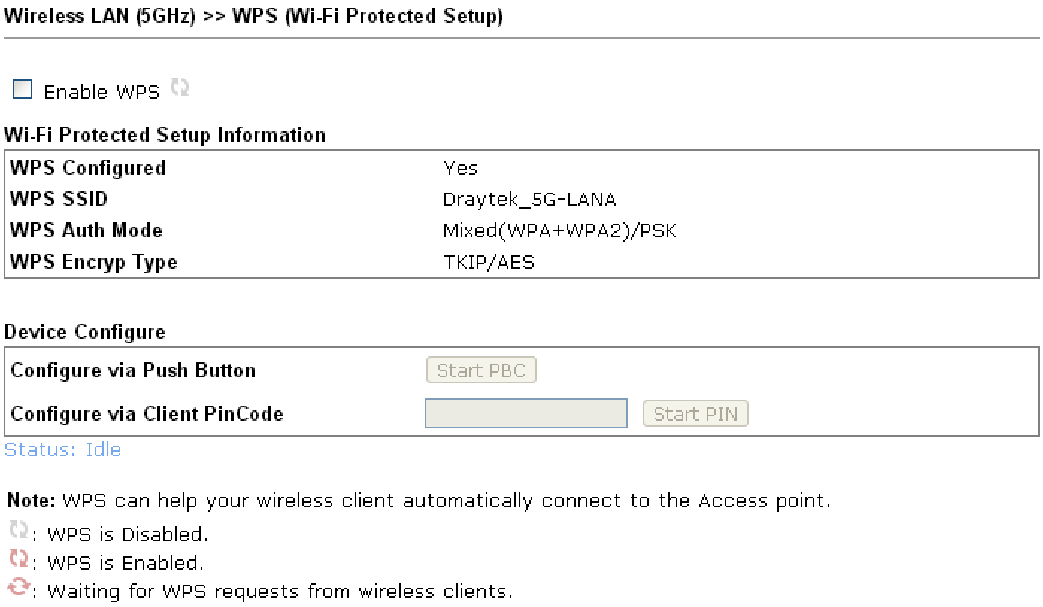
Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 900.  Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter
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.
Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

3.8.4 WPS

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



Wireless LAN (5GHz) >> WPS (Wi-Fi Protected Setup)

□ Enable WPS

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	Draytek_5G-LANA
WPS Auth Mode	Mixed(WPA+WPA2)/PSK
WPS Encryp Type	TKIP/AES

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: Idle

Note: WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

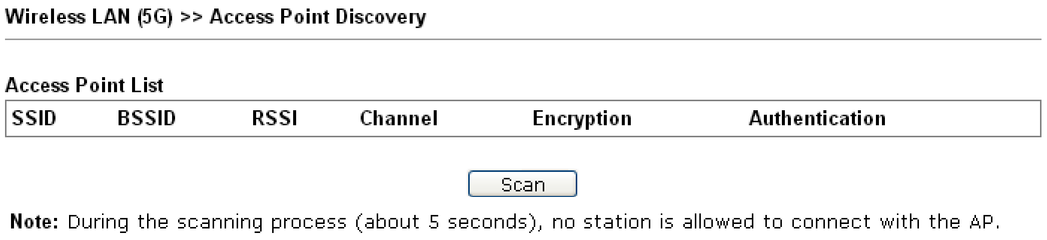
Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 900 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 900r. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 900.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 900 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 900 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	Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on

PinCode	VigorAP 900 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 900 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. Please click **Scan** to discover all the connected APs.



Wireless LAN (5G) >> Access Point Discovery

Access Point List

SSID	BSSID	RSSI	Channel	Encryption	Authentication

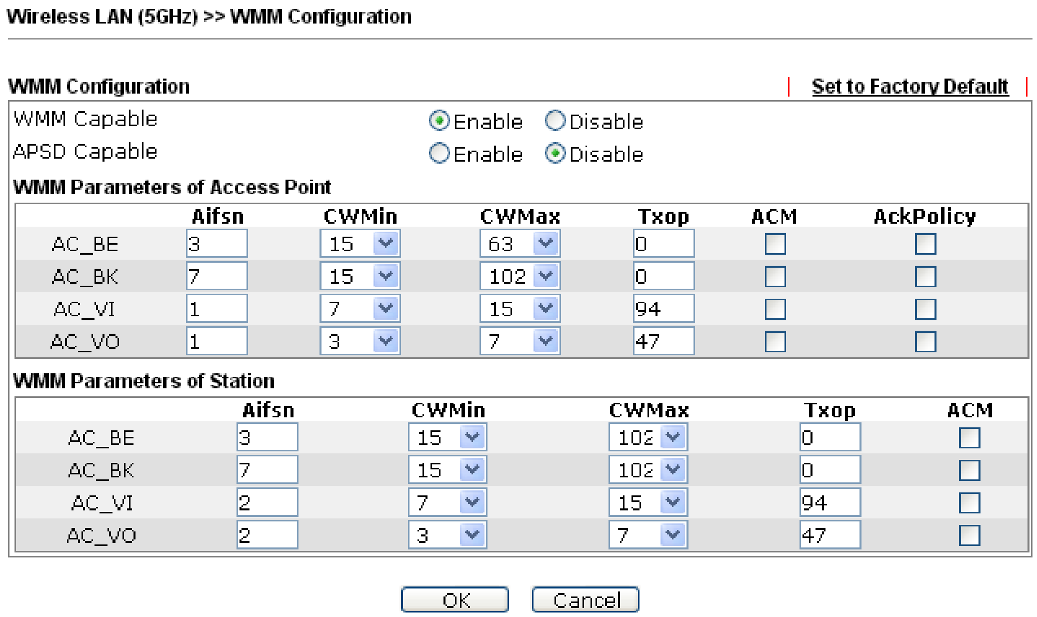
Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 900.
BSSID	Display the MAC address of the AP scanned by VigorAP 900.
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 900.
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

3.8.6 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.



Wireless LAN (5GHz) >> WMM Configuration

WMM Configuration | Set to Factory Default |

WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	102	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	□
AC_BK	7	15	102	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

Available settings are explained as follows:

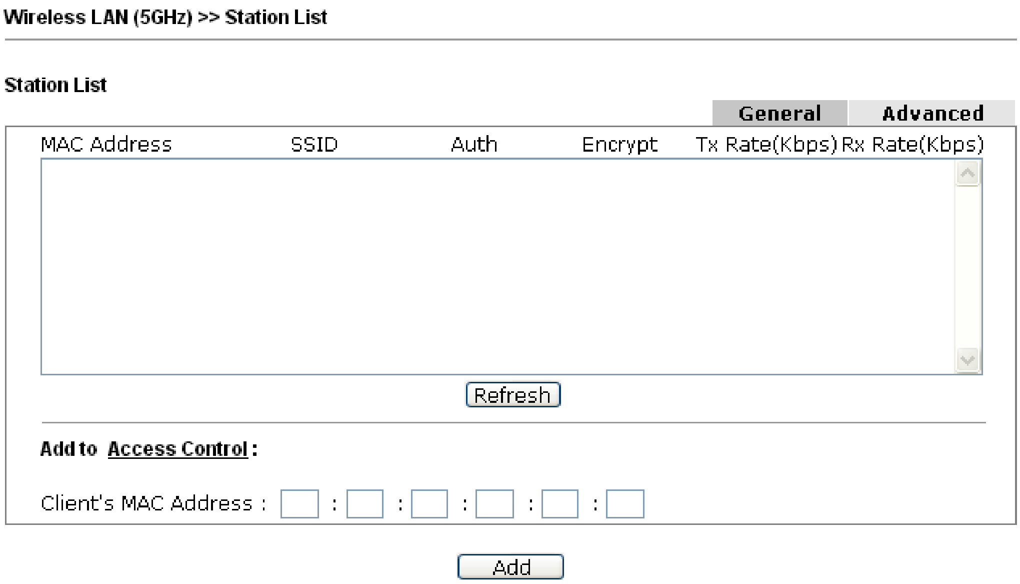
Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is

	checked. **Note:** VigorAP 900 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	"Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

After finishing this web page configuration, please click **OK** to save the settings.

3.8.7 Station List

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


Wireless LAN (5GHz) >> Station List

Station List

Add to Access Control :

Client's MAC Address : __ : __ : __ : __ : __ : __

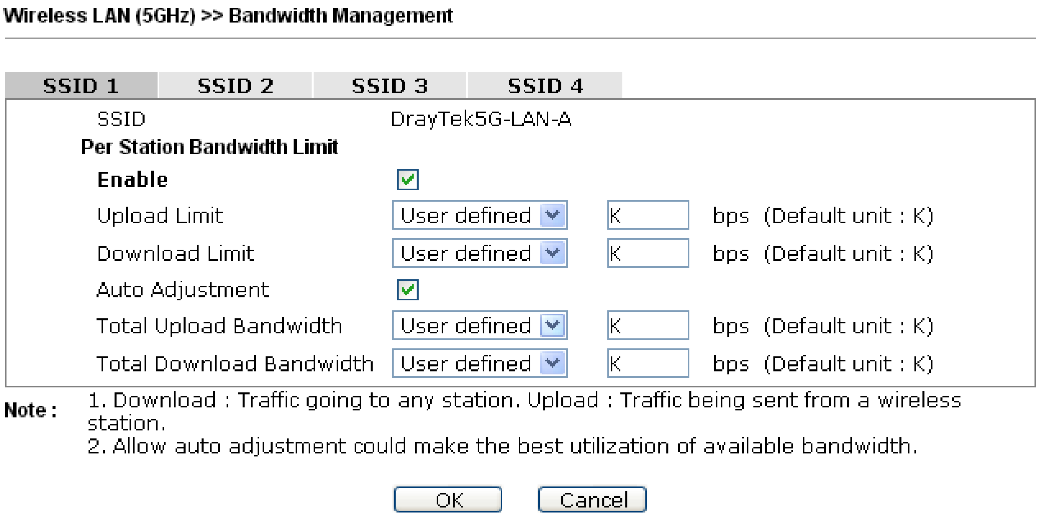
Available settings are explained as follows:

Item	Description
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.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
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.
General/Advanced	**General** – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. **Advanced** – Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

3.8.8 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.



Wireless LAN (5GHz) >> Bandwidth Management

SSID 1 | SSID 2 | SSID 3 | SSID 4

SSID	DrayTek5G-LAN-A		
Per Station Bandwidth Limit			
Enable	☑		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment	☑		
Total Upload Bandwidth	User defined	K	bps (Default unit : K)
Total Download Bandwidth	User defined	K	bps (Default unit : K)

Note : 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.
2. Allow auto adjustment could make the best utilization of available bandwidth.

Available settings are explained as follows:

Item	Description
SSID	Display the specific SSID name of the router.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Download Limit	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor router with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Auto Adjustment	Check this box to have the bandwidth limit determined by the system automatically.
Total Upload Limit	When Auto Adjustment is checked, the value defined here will

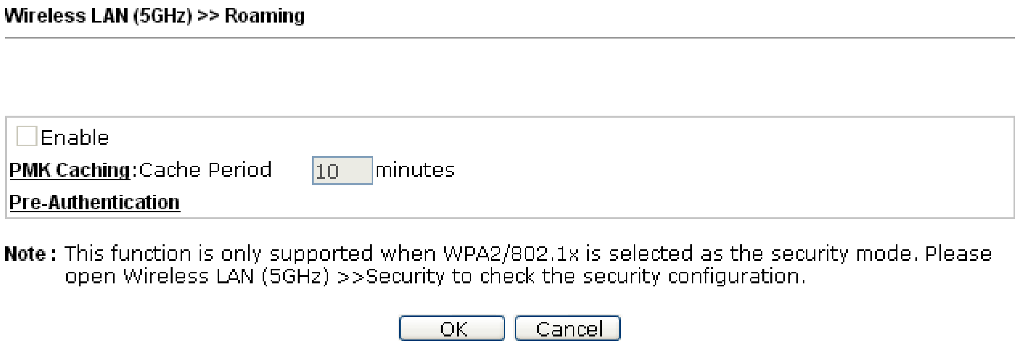
	be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data uploading.
Total Download Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data downloading.

After finishing this web page configuration, please click **OK** to save the settings.

3.8.9 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.



Wireless LAN (5GHz) >> Roaming

□ Enable

PMK Caching:Cache Period 10 minutes

Pre-Authentication

Note : This function is only supported when WPA2/802.1x is selected as the security mode. Please open Wireless LAN (5GHz) >>Security to check the security configuration.

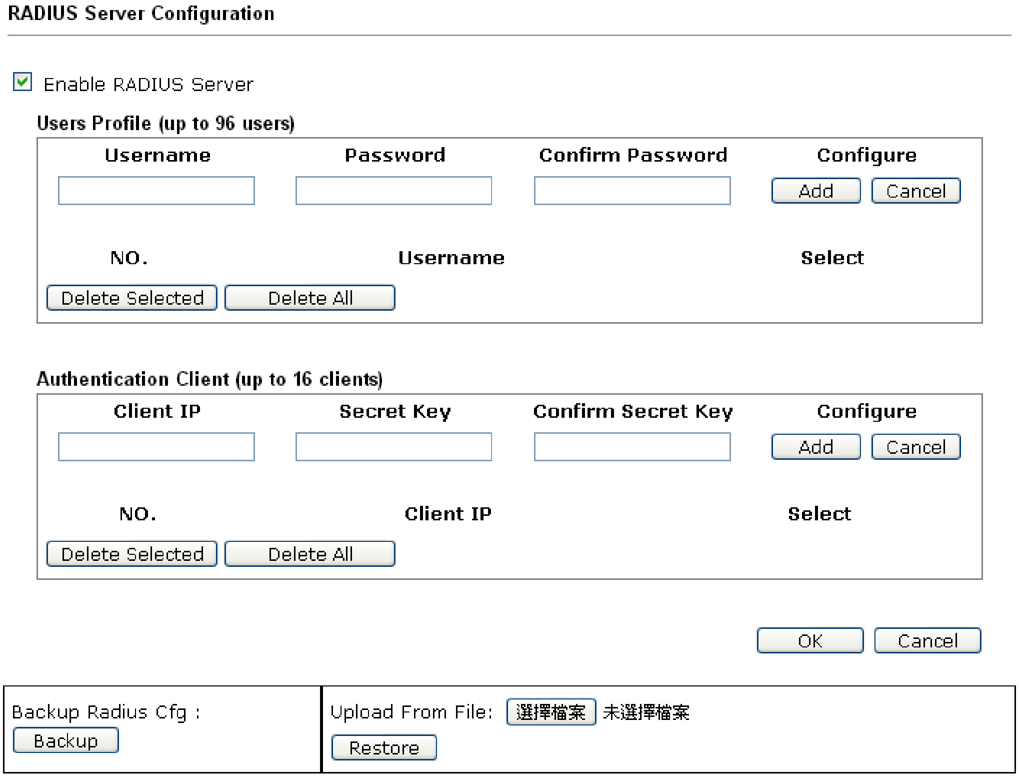
Available settings are explained as follows:

Item	Description
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.

After finishing this web page configuration, please click **OK** to save the settings.

3.9 RADIUS Server

VigorAP 900 offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 900. The AP can accept the wireless connection authentication requested by wireless clients.



RADIUS Server Configuration

☑ Enable RADIUS Server

Users Profile (up to 96 users)

Username	Password	Confirm Password	Configure
			Add Cancel
NO.	Username		Select

Delete Selected Delete All

Authentication Client (up to 16 clients)

Client IP	Secret Key	Confirm Secret Key	Configure
			Add Cancel
NO.	Client IP		Select

Delete Selected Delete All

OK Cancel

Backup Radius Cfg : Backup	Upload From File: 選擇檔案 未選擇檔案 Restore

Available settings are explained as follows:

Item	Description
Enable RADIUS Server	Check it to enable the internal RADIUS server.
Users Profile	**Username** – Type a new name for the user profile. **Password** – Type a new password for such new user profile. **Confirm Password** – Retype the password to confirm it. **Configure** ● **Add** – Make a new user profile with the name and password specified on the left boxes. ● **Cancel** – Clear current settings for user profile. **Delete Selected** – Delete the selected user profile (s). **Delete All** – Delete all of the user profiles.
Authentication Client	This internal RADIUS server of VigorAP 900 can be treated as the external RADIUS server for other users. Specify the client IP and secret key to make the wireless client choosing VigorAP 900 as its external RADUIS server. **Client IP** – Type the IP address for the user to be authenticated by VigorAP 900 when the user tries to use VigorAP 900 as the external RADIUS server.

	Secret Key – Type the password for the user to be authenticated by VigorAP 900 while the user tries to use VigorAP 900 as the external RADIUS server. **Confirm Secrete Key** – Type the password again for confirmation. **Configure** ● **Add** – Make a new client with IP and secrete key specified on the left boxes. ● **Cancel** – Clear current settings for the client. **Delete Selected** – Delete the selected client(s). **Delete All** – Delete all of the clients.
Backup	Click it to store the settings (RADIUS configuration) on this page as a file.
Restore	Click it to restore the settings (RADIUS configuration) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

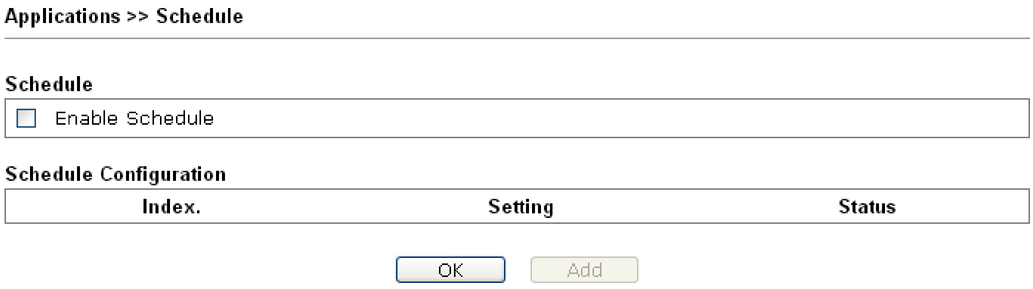
3.10 Applications

Below shows the menu items for Applications.

3.10.1 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.



Applications >> Schedule

Schedule

☐ Enable Schedule

Schedule Configuration

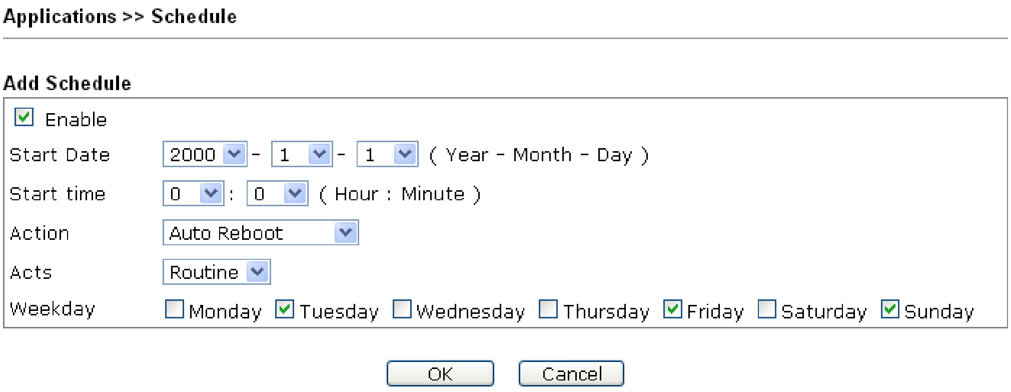
Index.	Setting	Status

Available settings are explained as follows:

Item	Description
Schedule	**Enable Schedule -** Check it to enable the function of schedule configuration.
Schedule Configuration	**Index** – Display the sort number of the schedule profile. **Setting** – Display the summary of the schedule profile. **Status** – Display if the profile is enabled (V) or not (X). **Add** – Such button is available when Enable Schedule is checked. It allows to add a new schedule profile.

You can set up to **15** schedules. To add a schedule:

1. Check the box of **Enable Schedule**.
2. Click the **Add** button to open the following web page.



Applications >> Schedule

Add Schedule

☑ Enable

Start Date 2000 - 1 - 1 (Year - Month - Day)

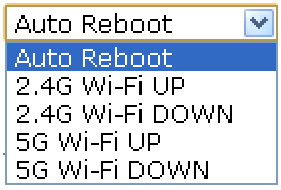
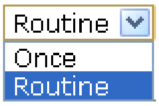
Start time 0 : 0 (Hour : Minute)

Action Auto Reboot

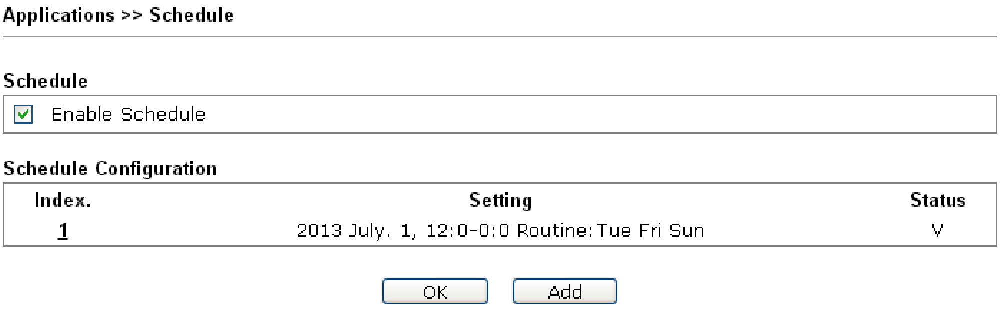
Acts Routine

Weekday ☐ Monday ☑ Tuesday ☐ Wednesday ☐ Thursday ☑ Friday ☐ Saturday ☑ Sunday

Available settings are explained as follows:

Item	Description
Enable	Check to enable such schedule profile.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
Action	Specify which action should apply the schedule.  Auto Reboot Auto Reboot 2.4G Wi-Fi UP 2.4G Wi-Fi DOWN 5G Wi-Fi UP 5G Wi-Fi DOWN
Acts	Specify how often the schedule will be applied. **Once** -The schedule will be applied just once **Routine** -Specify which days in one week should perform the schedule.  Routine Once Routine

3. After finishing this web page configuration, please click **OK** to save the settings. A new schedule profile has been created and displayed on the screen.



Applications >> Schedule

Schedule

☑ Enable Schedule

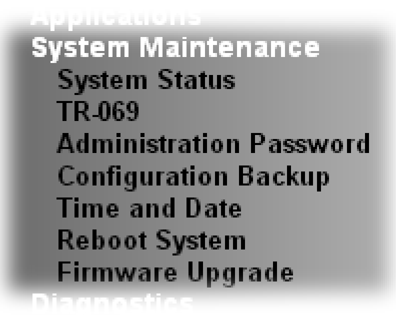
Schedule Configuration

Index.	Setting	Status
1	2013 July. 1, 12:0-0:0 Routine:Tue Fri Sun	V

3.11 System Maintenance

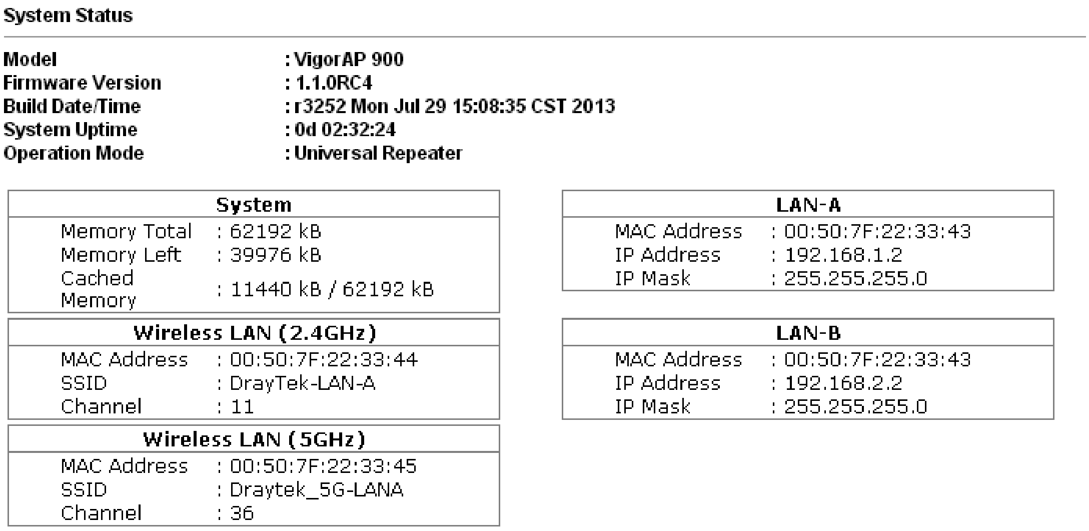
For the system setup, there are several items that you have to know the way of configuration: Status, TR-069, Administrator Password, Configuration Backup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.11.1 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.



System Status

```
Model              : VigorAP 900
Firmware Version   : 1.1.0RC4
Build Date/Time    : r3252 Mon Jul 29 15:08:35 CST 2013
System Uptime      : 0d 02:32:24
Operation Mode     : Universal Repeater
```

System	
Memory Total	: 62192 kB
Memory Left	: 39976 kB
Cached Memory	: 11440 kB / 62192 kB

LAN-A	
MAC Address	: 00:50:7F:22:33:43
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:22:33:44
SSID	: DrayTek-LAN-A
Channel	: 11

LAN-B	
MAC Address	: 00:50:7F:22:33:43
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

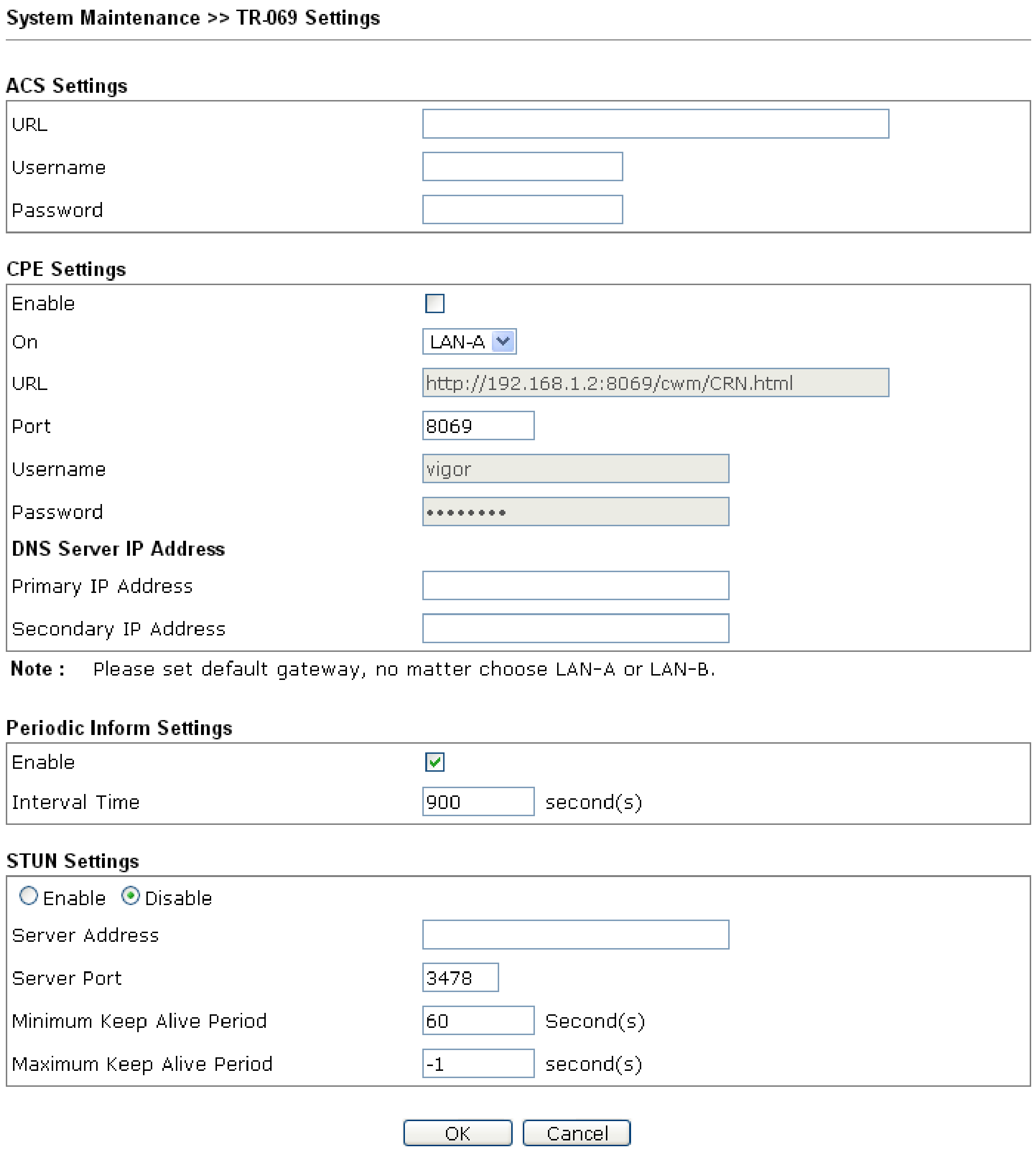
Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:22:33:45
SSID	: Draytek_5G-LANA
Channel	: 36

Each item is explained as follows:

Item	Description
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 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.

3.11.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS SI.



System Maintenance >> TR-069 Settings

ACS Settings

URL	
Username	
Password	

CPE Settings

Enable	□
On	LAN-A
URL	http://192.168.1.2:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	••••••••
DNS Server IP Address	
Primary IP Address	
Secondary IP Address	

Note : Please set default gateway, no matter choose LAN-A or LAN-B.

Periodic Inform Settings

Enable	☑
Interval Time	900 second(s)

STUN Settings

○ Enable ● Disable

Server Address	
Server Port	3478
Minimum Keep Alive Period	60 Second(s)
Maximum Keep Alive Period	-1 second(s)

Available settings are explained as follows:

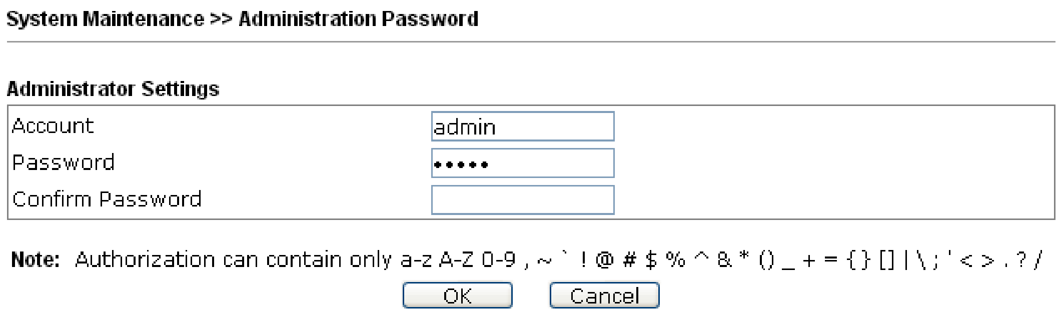
Item	Description
ACS Settings	**URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information. The setting for URL can be domain name or IP address.
CPE Settings	Such information is useful for Auto Configuration Server (ACS). **Enable**– Check the box to allow the CPE Client to connect with Auto Configuration Server.

	On – Choose the interface (LAN-A or LAN-B) for VigorAP 900 connecting to ACS server. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. **DNS Server IP Address –** Such field is to specify the IP address if a URL is configured with a domain name. ● **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.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the AP to send notification to VigorACS server. Or click **Disable** to close the mechanism of notification. **Interval Time** – Type the value for the interval time setting. The unit is “second”.
STUN Settings	The default is **Disable**. If you click **Enable**, please type the relational settings listed below: **Server Address –** Type the IP address of the STUN server. **Server Port –** Type the port number of the STUN server. **Minimum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is “60 seconds”. **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of “-1” indicates that no maximum period is specified.

After finishing this web page configuration, please click **OK** to save the settings.

3.11.3 Administrator Password

This page allows you to set new password.



System Maintenance >> Administration Password

Administrator Settings

Account	admin
Password	•••••
Confirm Password	

Note: Authorization can contain only a-z A-Z 0-9 , ~ ` ! @ # $ % ^ & * () _ + = {} [] | \ ; ' < > . ? /

Available settings are explained as follows:

Item	Description
Account	Type the name for accessing into Web User Interface.
Password	Type in new password in this filed.
Confirm Password	Type the new password again for confirmation.

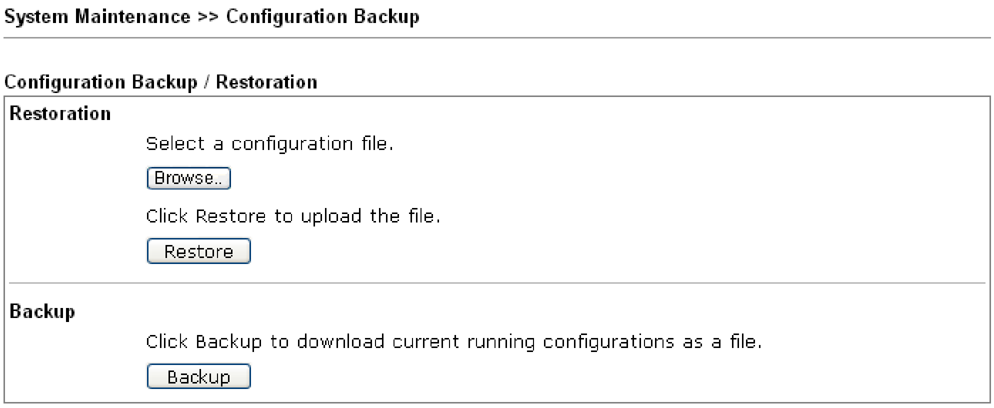
When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

3.11.4 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.



System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

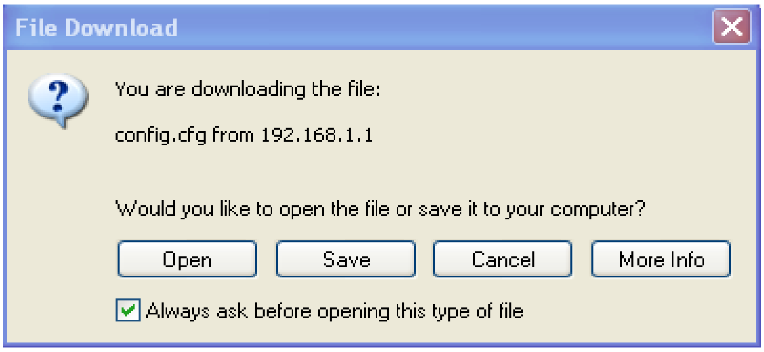
Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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



File Download

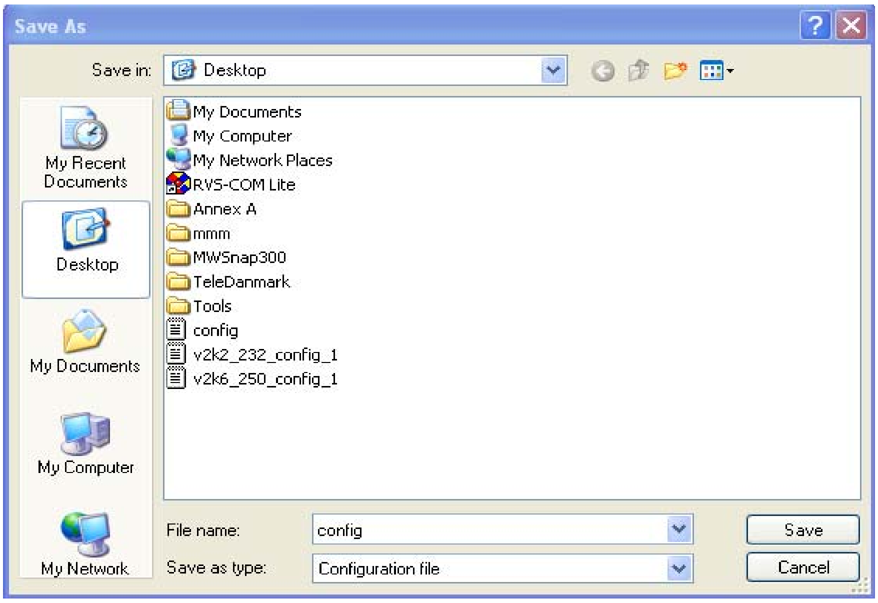
You are downloading the file:

config.cfg from 192.168.1.1

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

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



Save As

Save in: Desktop

File name: config

Save as type: Configuration file

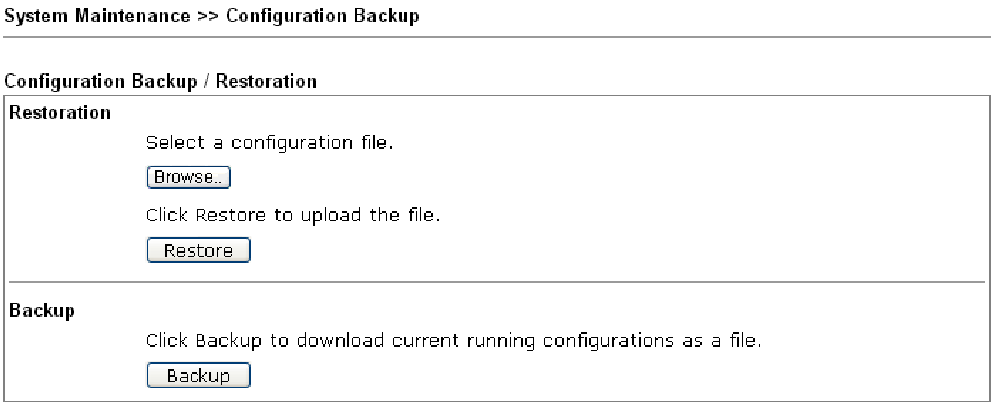
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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.



System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Browse..

Click Restore to upload the file.

Restore

Backup

Click Backup to download current running configurations as a file.

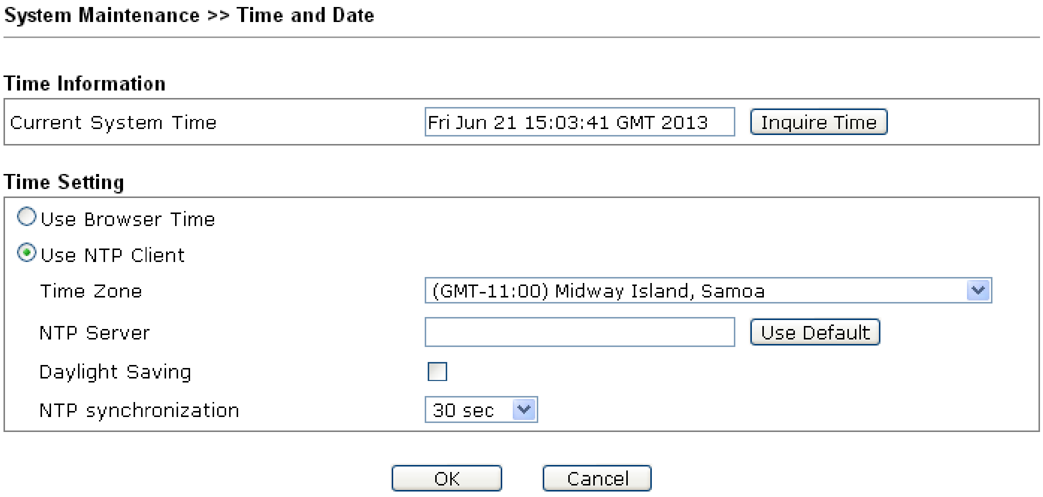
Backup

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.

3.11.5 Time and Date

It allows you to specify where the time of the router should be inquired from.



System Maintenance >> Time and Date

Time Information

Current System Time	Fri Jun 21 15:03:41 GMT 2013	Inquire Time

Time Setting

○ Use Browser Time

● Use NTP Client

Time Zone	(GMT-11:00) Midway Island, Samoa	
NTP Server		Use Default
Daylight Saving	□	
NTP synchronization	30 sec	

OK Cancel

Available parameters are explained as follows:

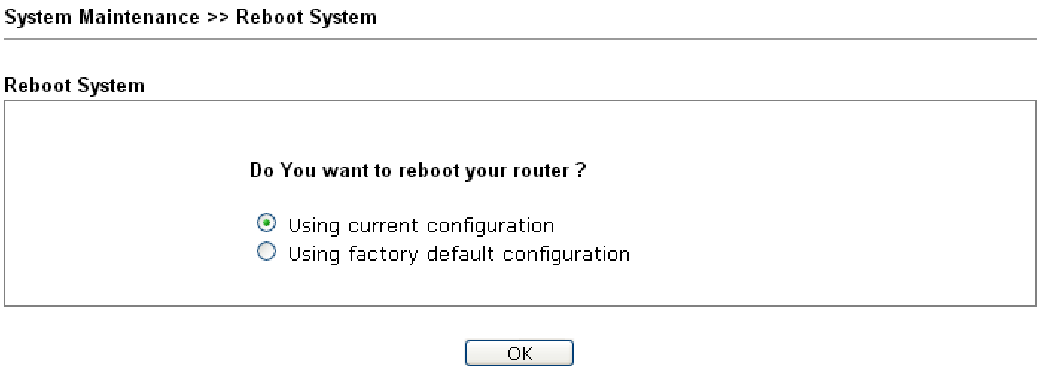
Item	Description
Current System Time	Click **Inquire Time** to get the current time.

Item	Description
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use NTP Client	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Zone	Select a time protocol.
NTP Server	Type the IP address of the time server. **Use Default** – Click it to choose the default NTP server.
Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.
NTP synchronization	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.11.6 Reboot System

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



System Maintenance >> Reboot System

Reboot System

Do You want to reboot your router ?

● Using current configuration
○ Using factory default configuration

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.

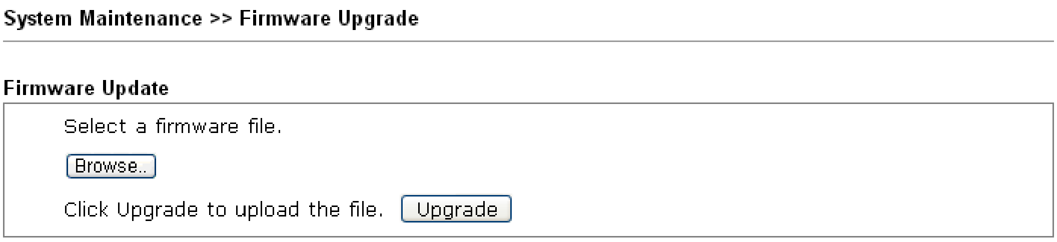
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your modem for ensuring normal operation and preventing unexpected errors of the modem in the future.

3.11.7 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.



System Maintenance >> Firmware Upgrade

Firmware Update

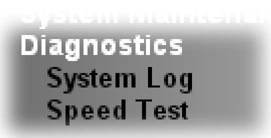
Select a firmware file.

Click Upgrade to upload the file.

Click **Browse** to locate the newest firmware from your hard disk and click **Upgrade**.

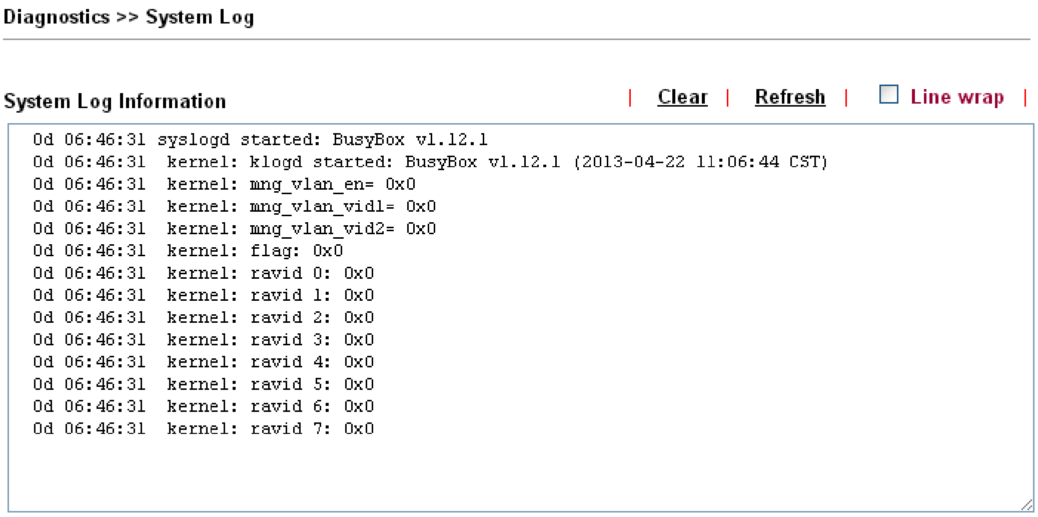
3.12 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your VigorAP 900.



3.12.1 System Log

At present, only **System Log** is offered.



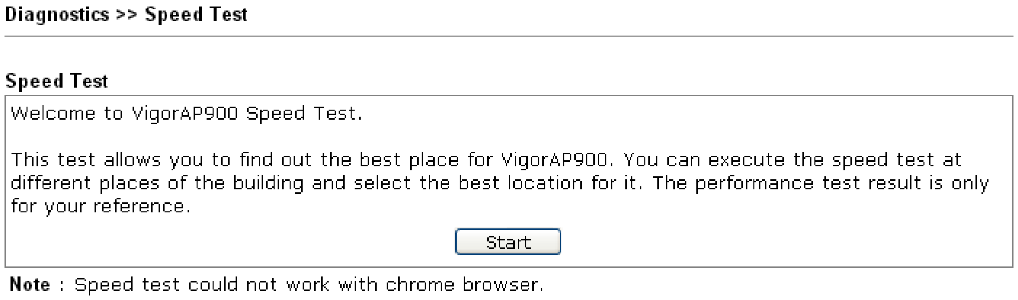
Diagnostics >> System Log

System Log Information

```
0d 06:46:31 syslogd started: BusyBox v1.12.1
0d 06:46:31  kernel: klogd started: BusyBox v1.12.1 (2013-04-22 11:06:44 CST)
0d 06:46:31  kernel: mng_vlan_en= 0x0
0d 06:46:31  kernel: mng_vlan_vid1= 0x0
0d 06:46:31  kernel: mng_vlan_vid2= 0x0
0d 06:46:31  kernel: flag: 0x0
0d 06:46:31  kernel: ravid 0: 0x0
0d 06:46:31  kernel: ravid 1: 0x0
0d 06:46:31  kernel: ravid 2: 0x0
0d 06:46:31  kernel: ravid 3: 0x0
0d 06:46:31  kernel: ravid 4: 0x0
0d 06:46:31  kernel: ravid 5: 0x0
0d 06:46:31  kernel: ravid 6: 0x0
0d 06:46:31  kernel: ravid 7: 0x0
```

3.12.2 Speed Test

Click the **Start** button on the page to test the speed. Such feature can help you to find the best installation place for Vigor AP.



Diagnostics >> Speed Test

Speed Test

Welcome to VigorAP900 Speed Test.

This test allows you to find out the best place for VigorAP900. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference.

Note : Speed test could not work with chrome browser.

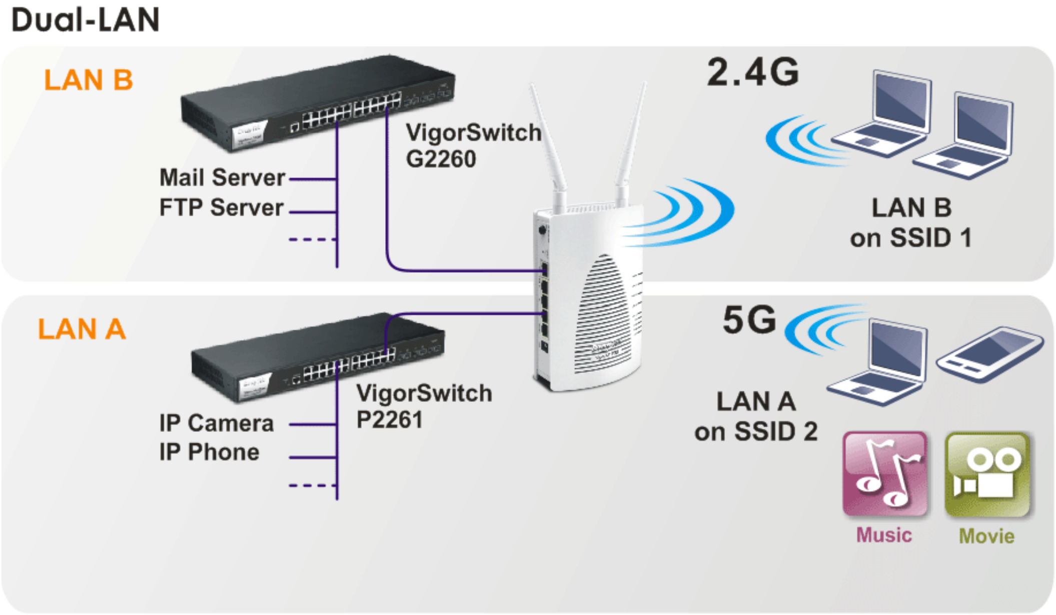
3.13 Support Area

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

4 Application and Examples

4.1 How to set different segments for different SSIDs in VigorAP 900

VigorAP 900 supports two network segments, LAN-A and LAN-B for different SSIDs. With such feature, the user can dispatch SSIDs with different network segments for reaching the target of managing wireless network. See the following figure.



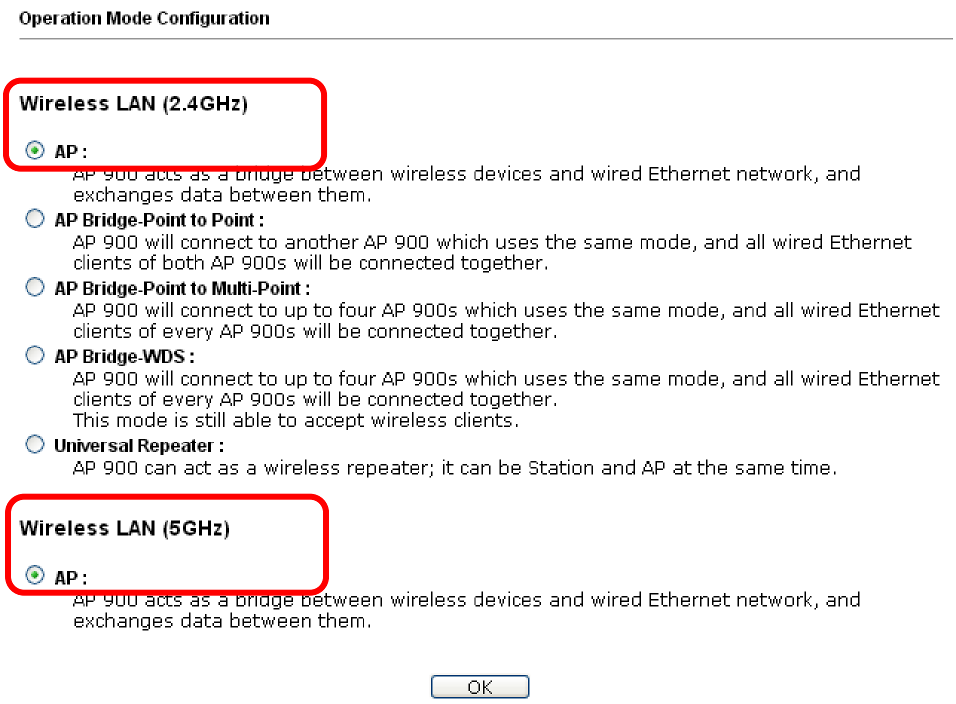
In the above figure, VigorAP 900 is used to control the wireless network connection. It can separate the wireless traffic between accessing internal server and the usage of video. Wireless station connecting to VigorAP 900 with SSID 2 can get the IP address with the network segment of 192.168.1.0/24 (LAN-A); wireless station connecting to VigorAP 900 with SSID 1 can get the IP address with the same network segment of 192.168.2.0/24 (LAN-B).

LAN-B : 192.168.2.0/24 →for internal server

LAN-A : 192.168.1.0/24 →for music, video traffic

Below shows you how to configure the web page for VigorAP 900:

1. In the page of **Operation Mode**, click **AP** mode for 2.4GHz Wireless and 5GHz Wireless.



Operation Mode Configuration

Wireless LAN (2.4GHz)

● **AP :**
AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

○ **AP Bridge-Point to Point :**
AP 900 will connect to another AP 900 which uses the same mode, and all wired Ethernet clients of both AP 900s will be connected together.

○ **AP Bridge-Point to Multi-Point :**
AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together.

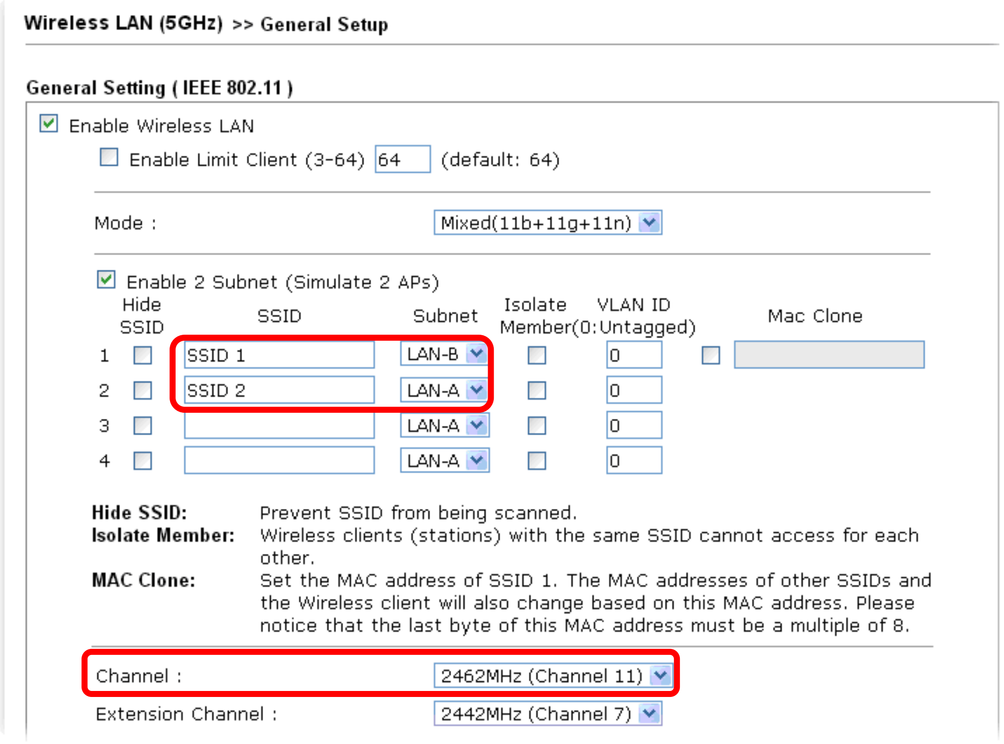
○ **AP Bridge-WDS :**
AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together.
This mode is still able to accept wireless clients.

○ **Universal Repeater :**
AP 900 can act as a wireless repeater; it can be Station and AP at the same time.

Wireless LAN (5GHz)

● **AP :**
AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

2. Open **Wireless LAN(2.4GHz) >> General Setup** and then **Wireless LAN(5GHz) >> General Setup**. Choose the subnet **LAN-B** for SSID 1 and choose **LAN-A** for SSID 2. Specify the wireless channel. Then, click **OK** to save the configuration.



Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

□ Enable Limit Client (3-64) 64 (default: 64)

Mode : Mixed(11b+11g+11n)

☑ Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0:Untagged)	Mac Clone
1	□	SSID 1	LAN-B	□	0	□
2	□	SSID 2	LAN-A	□	0	
3	□		LAN-A	□	0	
4	□		LAN-A	□	0	

Hide SSID: Prevent SSID from being scanned.

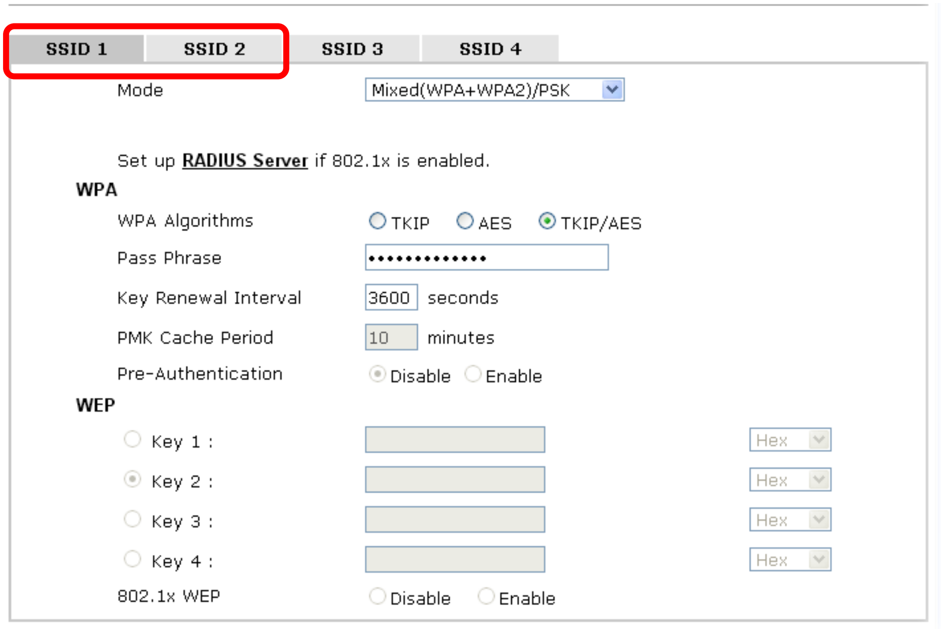
Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

MAC Clone: Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.

Channel : 2462MHz (Channel 11)

Extension Channel : 2442MHz (Channel 7)

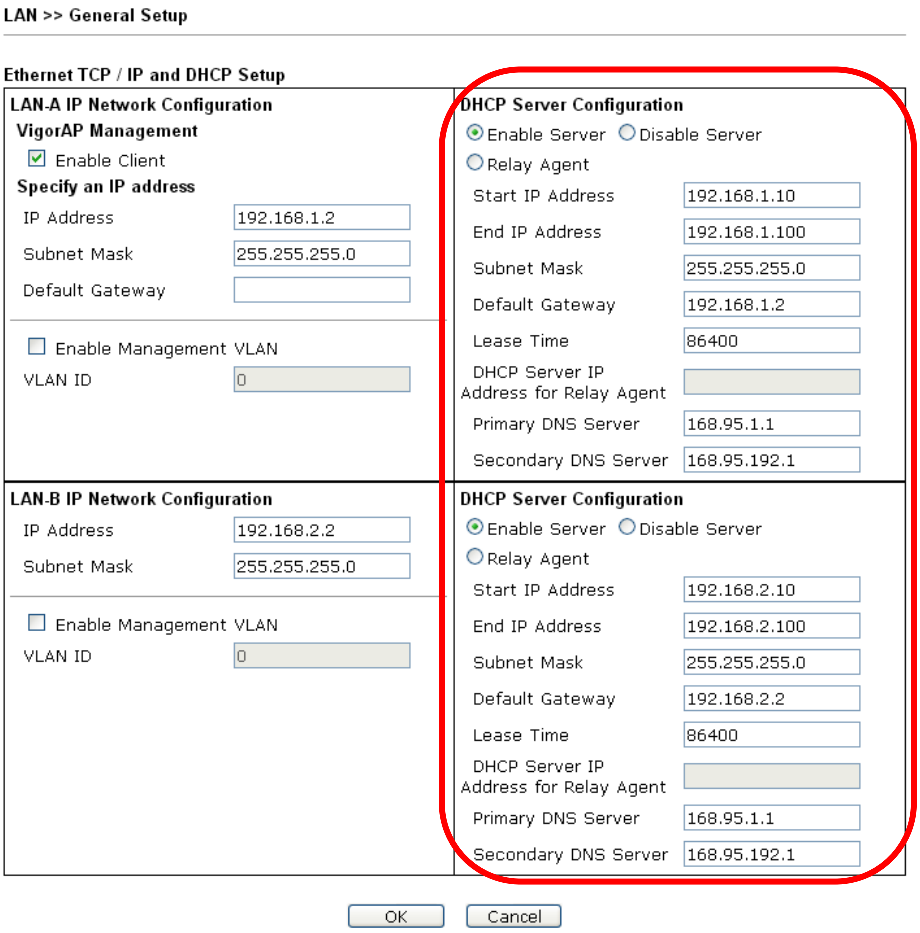
3. Open **Wireless LAN(2.4GHz) >> Security Settings** and **Wireless LAN(5GHz) >> Security Settings**. Set the encryption method and set the password for SSID 1 and SSID 2 respectively.



SSID 1 | SSID 2 | SSID 3 | SSID 4

Mode	Mixed(WPA+WPA2)/PSK	
Set up **RADIUS Server** if 802.1x is enabled.		
WPA		
WPA Algorithms	○ TKIP ○ AES ● TKIP/AES	
Pass Phrase	•••••••••••••	
Key Renewal Interval	3600 seconds	
PMK Cache Period	10 minutes	
Pre-Authentication	● Disable ○ Enable	
WEP		
○ Key 1 :		Hex
● Key 2 :		Hex
○ Key 3 :		Hex
○ Key 4 :		Hex
802.1x WEP	○ Disable ○ Enable	

4. Open **LAN>General Setup** to configure the settings for enabling DHCP server on LAN-A/LAN-B. If there is a DHCP server configured in the same network segment, skip this step.



LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN-A IP Network Configuration		**DHCP Server Configuration**	
VigorAP Management		● Enable Server ○ Disable Server	
☑ Enable Client		○ Relay Agent	
Specify an IP address		Start IP Address	192.168.1.10
IP Address	192.168.1.2	End IP Address	192.168.1.100
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway		Default Gateway	192.168.1.2
		Lease Time	86400
☐ Enable Management VLAN		DHCP Server IP Address for Relay Agent	
VLAN ID	0	Primary DNS Server	168.95.1.1
		Secondary DNS Server	168.95.192.1
LAN-B IP Network Configuration		**DHCP Server Configuration**	
IP Address	192.168.2.2	● Enable Server ○ Disable Server	
Subnet Mask	255.255.255.0	○ Relay Agent	
		Start IP Address	192.168.2.10
☐ Enable Management VLAN		End IP Address	192.168.2.100
VLAN ID	0	Subnet Mask	255.255.255.0
		Default Gateway	192.168.2.2
		Lease Time	86400
		DHCP Server IP Address for Relay Agent	
		Primary DNS Server	168.95.1.1
		Secondary DNS Server	168.95.192.1

5. After finishing the above settings, the wireless equipment connecting to VigorAP 900 with SSID 1 can get the IP address assigned by LAN-B 192.168.2.0/24 for accessing the internal server. The wireless equipment connecting to VigorAP 900 with SSID 2 can get the IP address assigned by LAN-A 192.168.1.0/24 for using the video/audio uploading and downloading services.

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.

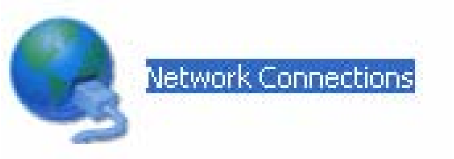
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

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.

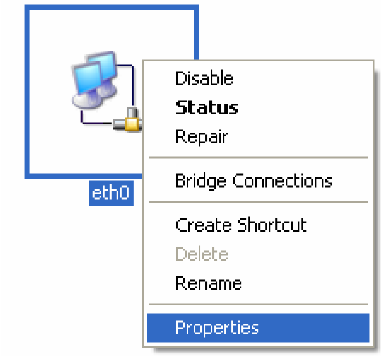
For Windows

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**.

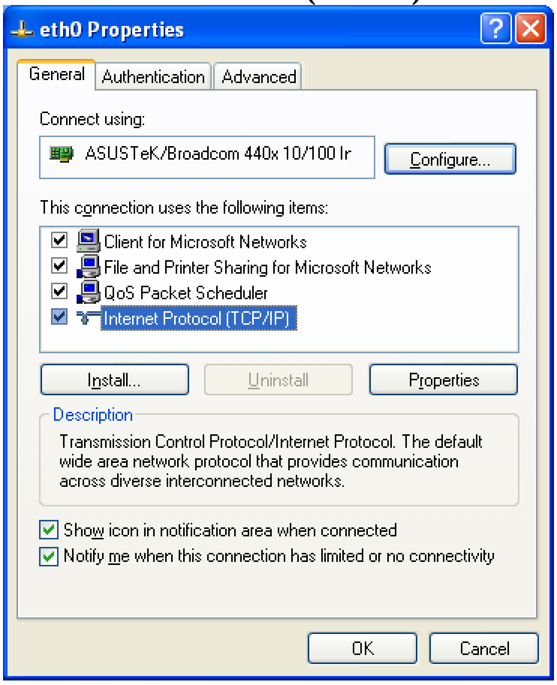
1. Go to **Control Panel** and then double-click on **Network Connections**.



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



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



eth0 Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Ir

This connection uses the following items:

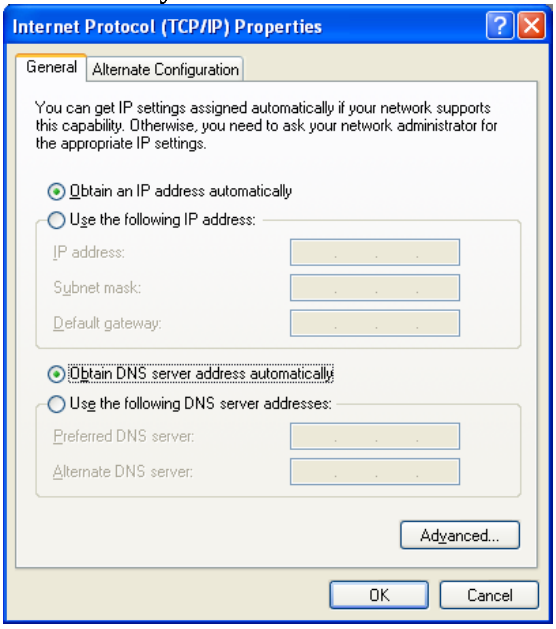
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

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

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

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



Internet Protocol (TCP/IP) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

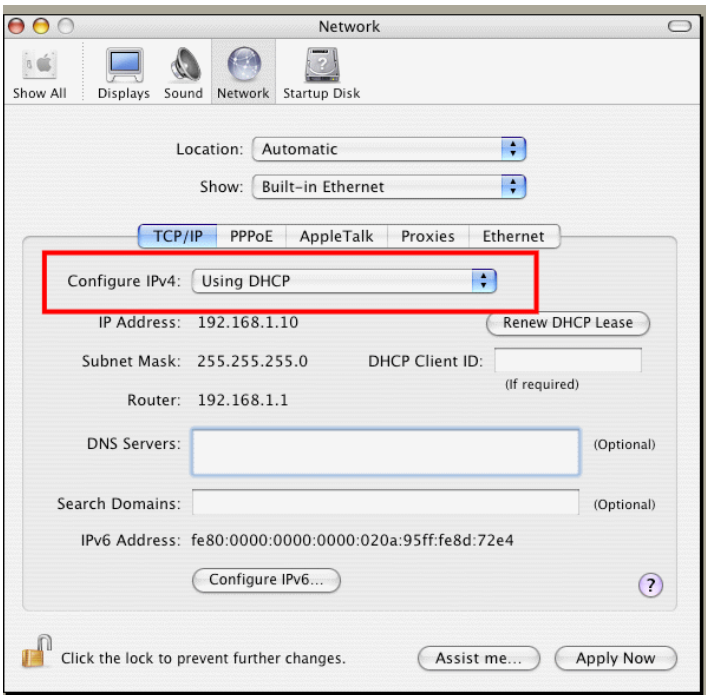
Alternate DNS server:

For Mac Os

1. Double click on the current used Mac Os 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.



Network

Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.1

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

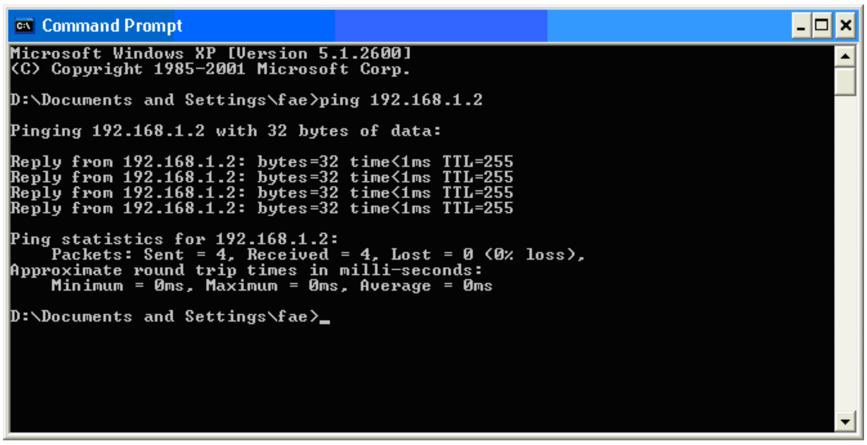
5.3 Pinging the Modem from Your Computer

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.

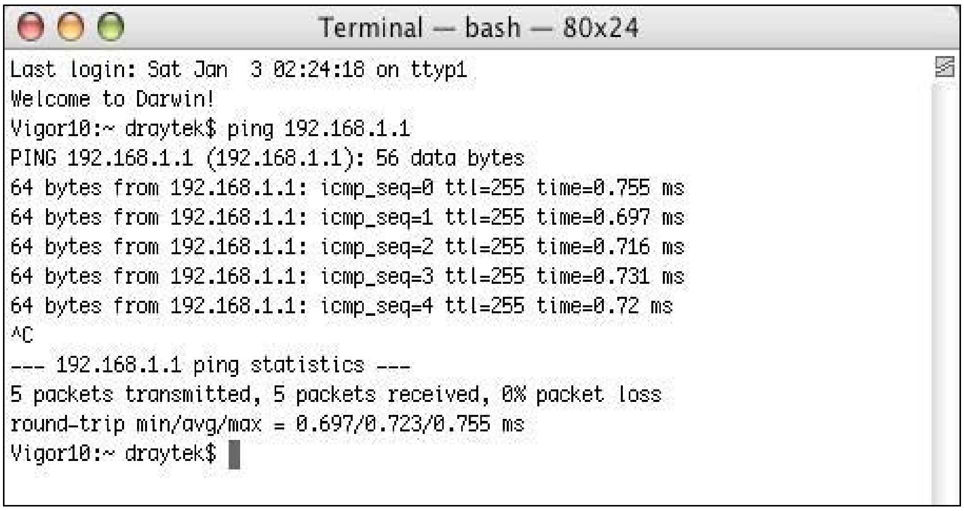


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.2 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.2: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 Mac Os (Terminal)

1. Double click on the current used Mac Os on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.2** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.



```
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

5.4 Backing to Factory Default Setting If Necessary

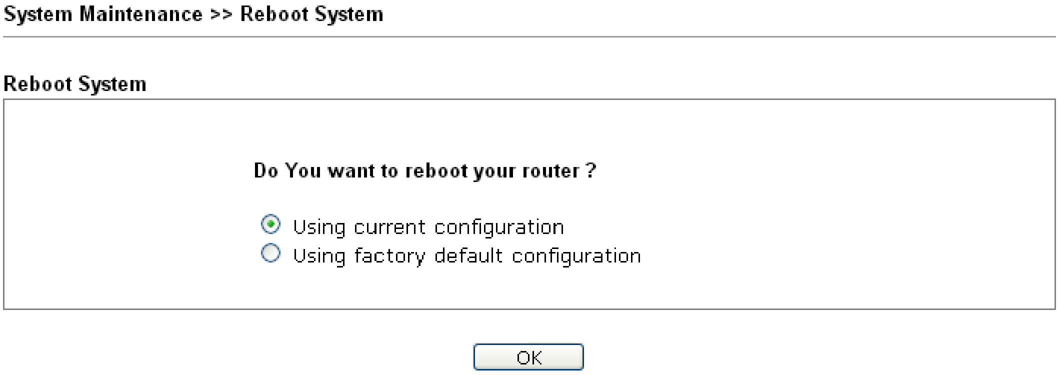
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware.

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.



System Maintenance >> Reboot System

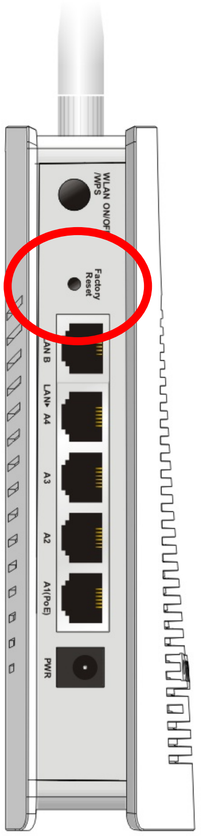
Reboot System

Do You want to reboot your router ?

● Using current configuration
○ Using factory default configuration

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.

5.5 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.