

DrayTek

VigorAP 800

802.11n Access Point



Your reliable networking solutions partner

User's Guide

V2.1

VigorAP 800

Wireless Access Point

User's Guide

Version: 2.1

Firmware Version: V1.1.6

Date: December 8, 2016

Intellectual Property Rights (IPR) Information

Copyright Declarations

All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

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 by 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 to restore 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 800

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

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

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

Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device may accept any interference received, including interference that may cause undesired operation.

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



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

FCC RF Radiation Exposure Statement

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

GPL Notice

This DrayTek product uses software partially or completely licensed under the terms of the GNU GENERAL PUBLIC LICENSE. The author of the software does not provide any warranty. A Limited Warranty is offered on DrayTek products. This Limited Warranty does not cover any software applications or programs.

To download source codes please visit:

<http://gplsource.draytek.com>

GNU GENERAL PUBLIC LICENSE:

<https://gnu.org/licenses/gpl-2.0>

Version 2, June 1991

For any question, please feel free to contact DrayTek technical support at support@draytek.com for further information.

Table of Contents

1

Preface	1
1.1 Introduction	1
1.2 LED Indicators and Connectors	2
1.3 Hardware Installation	4
1.3.1 Wired Connection for PC in LAN	4
1.3.2 Wired Connection for Notebook in WLAN	5
1.3.2 Wireless Connection.....	6
1.3.3 POE Connection	7

2

Network Configuration.....	9
2.1 Windows 7 IP Address Setup.....	9
2.2 Windows 2000 IP Address Setup.....	11
2.3 Windows XP IP Address Setup.....	12
2.4 Windows Vista IP Address Setup.....	13
2.5 Accessing to Web User Interface	14
2.6 Changing Password	15
2.7 Quick Start Wizard	16
2.7.1 Configuring 2.4G Wireless Settings – General.....	16
2.7.2 Configuring 2.4G Wireless Settings based on the Operation Mode.....	18
2.7.3 Configuring 2.4G Security Settings	25
2.7.4 Configuring 5G Wireless Settings.....	27
2.7.5 Configuring 5G Security Settings	29
2.7.6 Finishing the Wireless Settings Wizard	31
2.8 Online Status.....	32

3

Advanced Configuration	33
3.1 Operation Mode	34
3.2 LAN	35
3.3 Central AP Management.....	37
3.3.1 General Setup.....	37
3.3.2 Function Support List.....	38
3.4 General Concepts for Wireless LAN	39
3.5 Wireless LAN (2.4GHz) Settings for AP Mode.....	42
3.5.1 General Setup.....	42
3.5.2 Security	47

3.5.3 Access Control.....	50
3.5.4 WPS.....	51
3.5.5 AP Discovery	52
3.5.6 WMM Configuration	53
3.5.7 Station List	55
3.5.8 Bandwidth Management.....	56
3.6 Wireless LAN (2.4GHz) Settings for Station-Infrastructure Mode.....	57
3.6.1 General Setup.....	57
3.6.2 Site Survey	63
3.6.3 Statistics.....	64
3.6.4 WPS (Wi-Fi Protected Setup).....	64
3.7 Wireless LAN (2.4GHz) Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Mode	66
3.7.1 General Setup.....	67
3.7.2 AP Discovery	70
3.7.3 WDS AP Status	71
3.8 Wireless LAN (2.4GHz) Settings for AP Bridge-WDS Mode.....	71
3.8.1 General Setup.....	72
3.8.2 Security	76
3.8.3 Access Control.....	79
3.8.4 WPS.....	80
3.8.5 AP Discovery	81
3.8.6 WDS AP Status	82
3.8.7 WMM Configuration	82
3.8.8 Station List	84
3.8.9 Bandwidth Management.....	85
3.9 Wireless LAN (2.4GHz) Settings for Universal Repeater Mode	86
3.9.1 General Setup.....	87
3.9.2 Security	91
3.9.3 Access Control.....	94
3.9.4 WPS.....	95
3.9.5 AP Discovery	96
3.9.6 Universal Repeater	97
3.9.7 WMM Configuration	100
3.9.8 Station List	102
3.9.9 Bandwidth Management.....	103
3.10 Wireless LAN (5G) Settings for AP Mode	104
3.10.1 General Setup.....	104
3.10.2 Security	106
3.10.3 Access Control.....	109
3.10.4 AP Discovery	110
3.10.5 Station List	111
3.10.6 Bandwidth Management.....	112
3.11 RADIUS Server	113
3.12 Applications	114
3.12.1 Schedule.....	114
3.12.2 Apple iOS Keep Alive	116
3.13 System Maintenance.....	117
3.13.1 System Status.....	117
3.13.2 TR-069.....	118
3.13.3 Administrator Password.....	120
3.13.4 Configuration Backup	121

3.13.5 Time and Date	122
3.13.6 Management.....	123
3.13.7 Reboot System	124
3.13.8 Firmware Upgrade	124
3.14 Diagnostics.....	125
3.14.1 System Log.....	125
3.14.2 Speed Test	126

4

Application and Examples..... 127

4.1 How to set different segments for different SSIDs in VigorAP 800	127
--	-----

5

Trouble Shooting..... 131

5.1 Checking If the Hardware Status Is OK or Not.....	131
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	132
5.3 Pinging the Modem from Your Computer	135
5.4 Backing to Factory Default Setting If Necessary	136
5.5 Contacting DrayTek.....	137

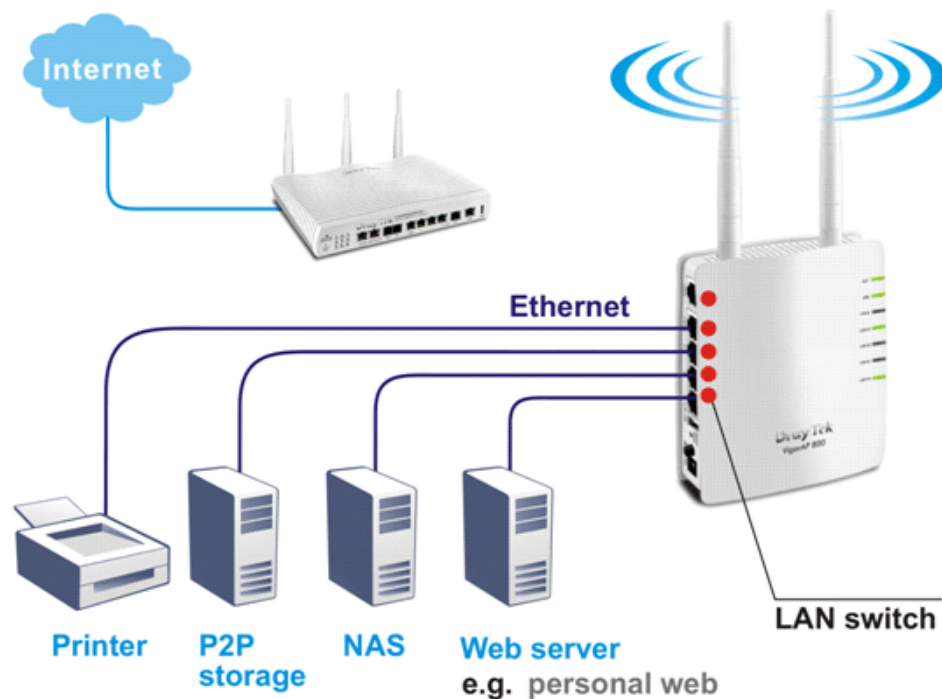
1

Preface

1.1 Introduction

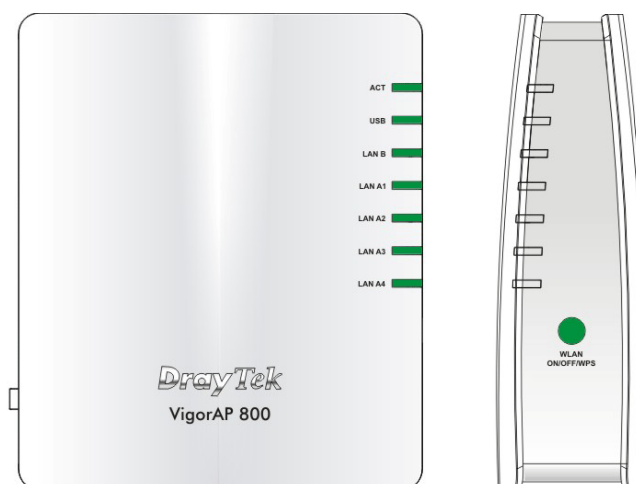
Thank you for purchasing this VigorAP 800! With this high cost-efficiency VigorAP 800, computers and wireless devices which are compatible with 802.11n can connect to existing wired Ethernet network via this VigorAP 800, at the speed of 300Mbps.

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

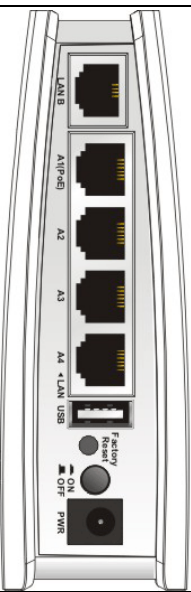

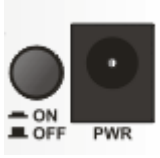


1.2 LED Indicators and Connectors

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



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

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

1.3 Hardware Installation

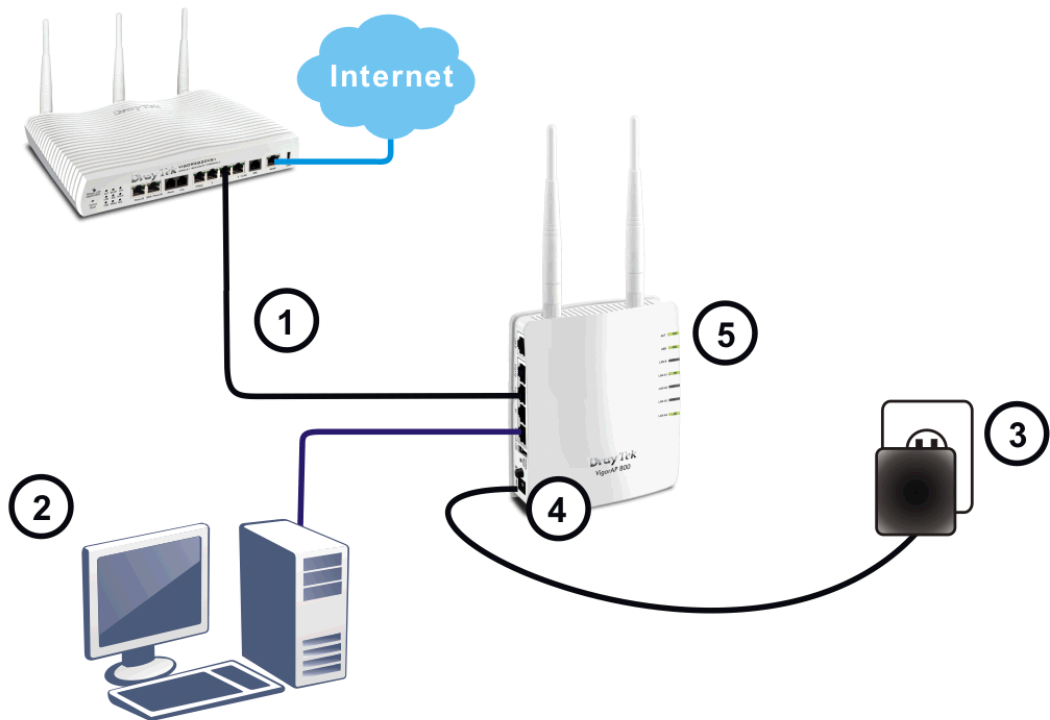
This section will guide you to install the modem through hardware connection and configure the modem's settings through web browser.

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

1.3.1 Wired Connection for PC in LAN

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

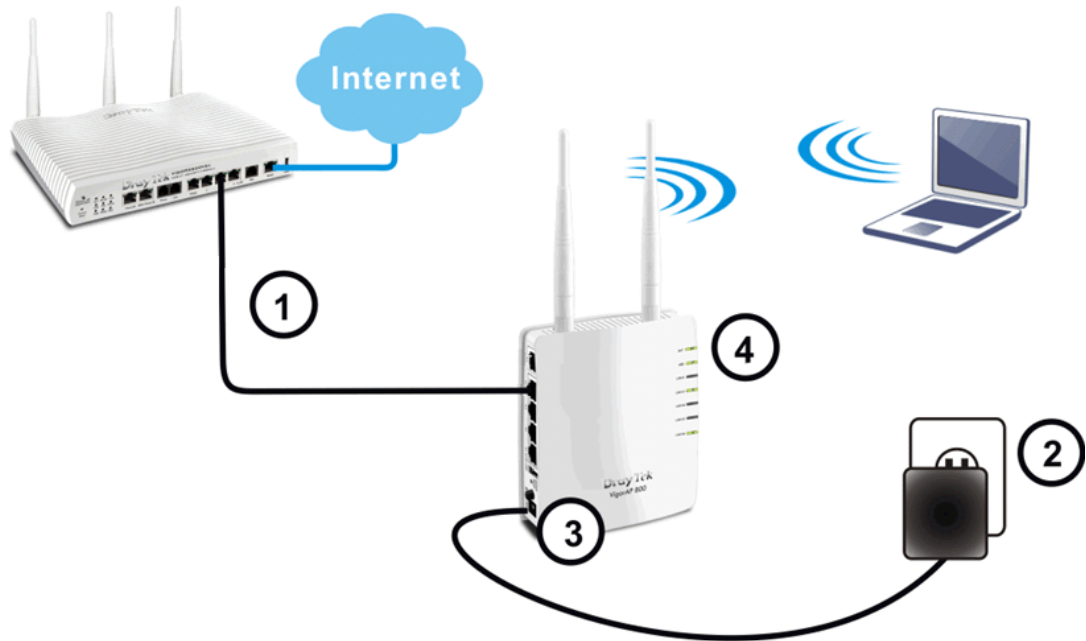
(For the detailed information of LED status, please refer to section 1.2.)



1.3.2 Wired Connection for Notebook in WLAN

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

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

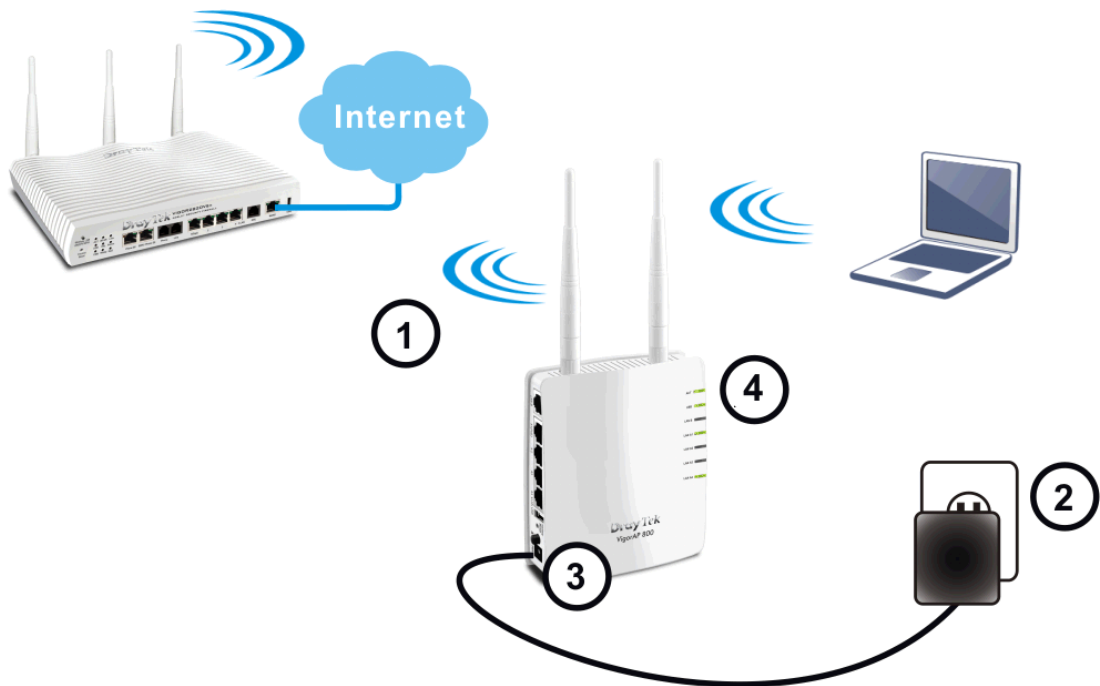


1.3.2 Wireless Connection

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

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

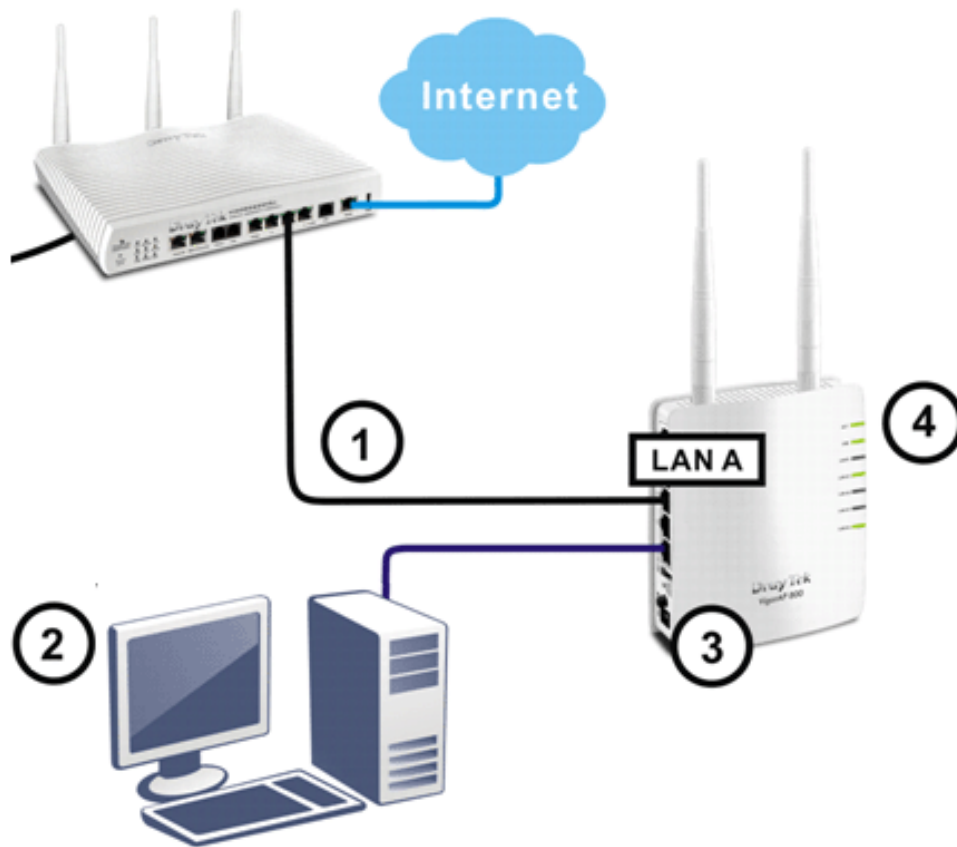
(For the detailed information of LED status, please refer to section 1.2.)



1.3.3 POE Connection

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

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



This page is left blank.

2

Network Configuration

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

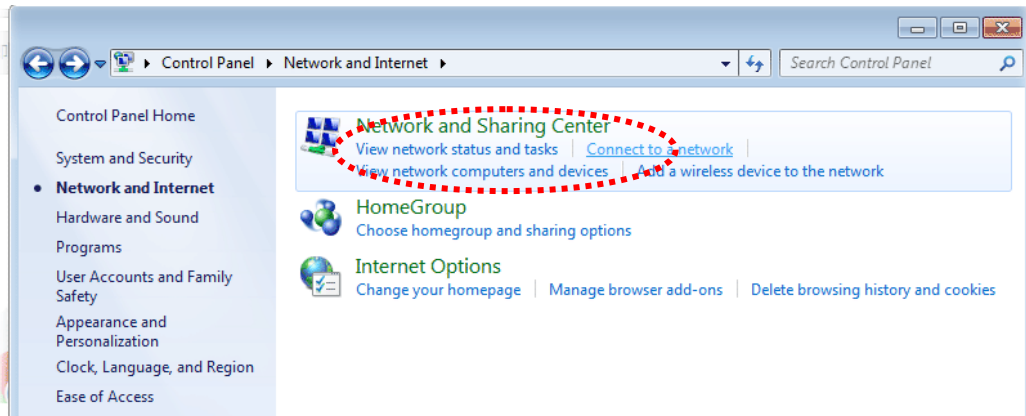
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic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

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

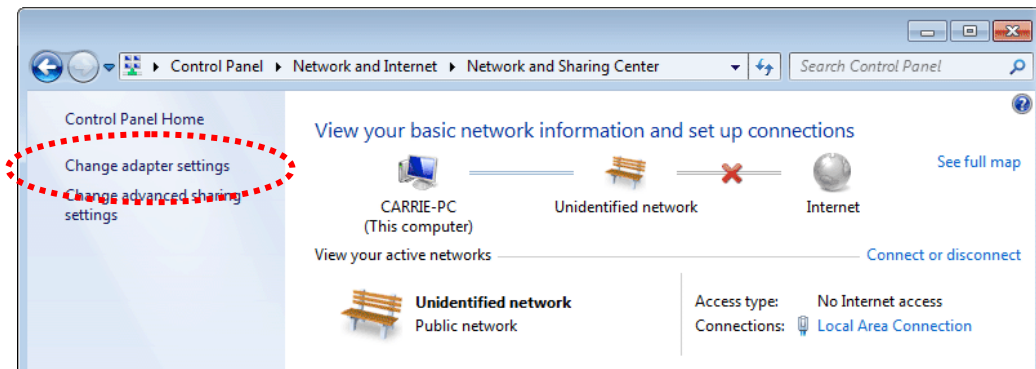
- Windows 7** - please go to section 2.1
- Windows 2000** - please go to section 2.2
- Windows XP** - please go to section 2.3
- Windows Vista** - please go to section 2.4

2.1 Windows 7 IP Address Setup

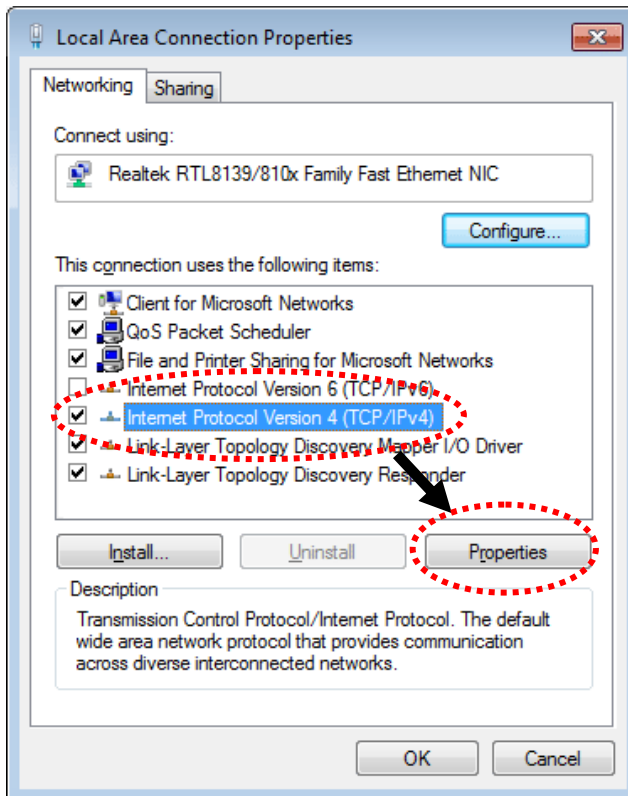
Click **Start** button (it should be located at lower-left corner of your computer), then click Control Panel. Double-click **Network and Internet**, and the following window will appear. Click **Network and Sharing Center**.



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



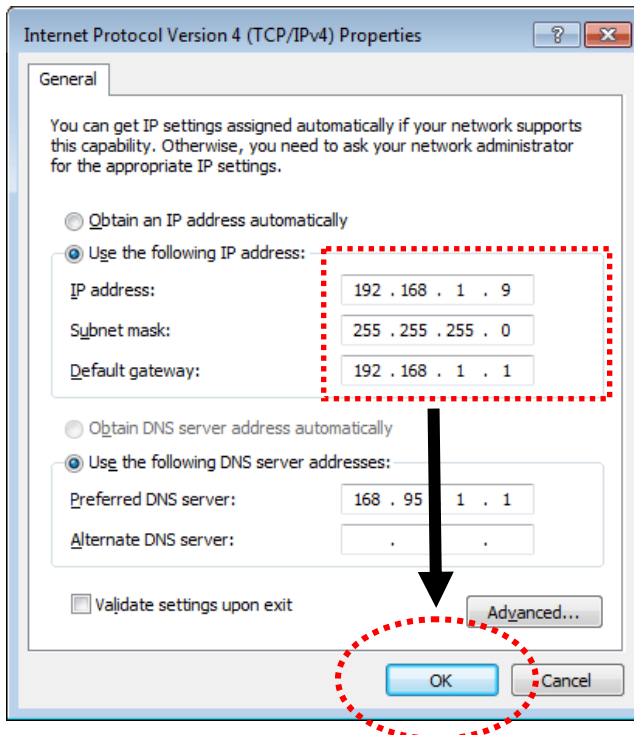
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Under the General tab, click **Use the following IP address**. Then input the following settings in respective field and click **OK** when finish.

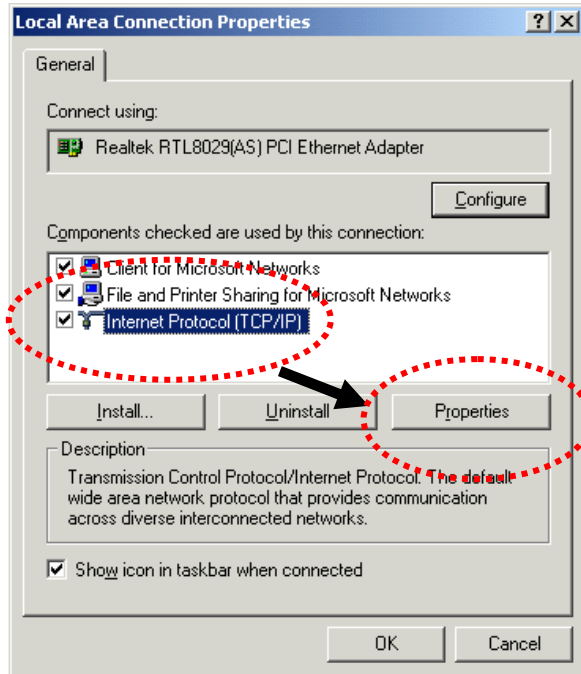
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.2 Windows 2000 IP Address Setup

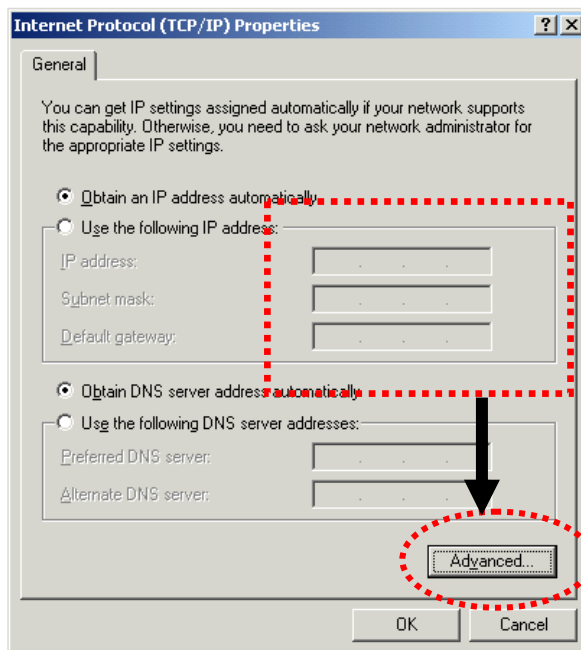
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Dial-up Connections** icon, double click **Local Area Connection**, and **Local Area Connection Properties** window will appear. Select **Internet Protocol (TCP/IP)**,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



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

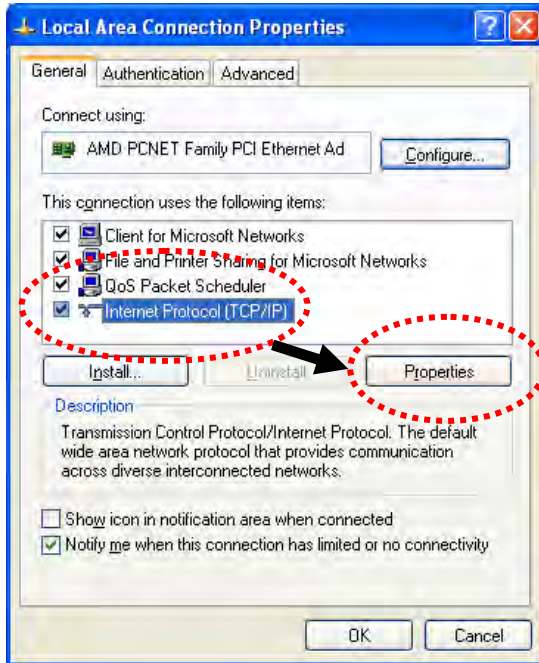
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.3 Windows XP IP Address Setup

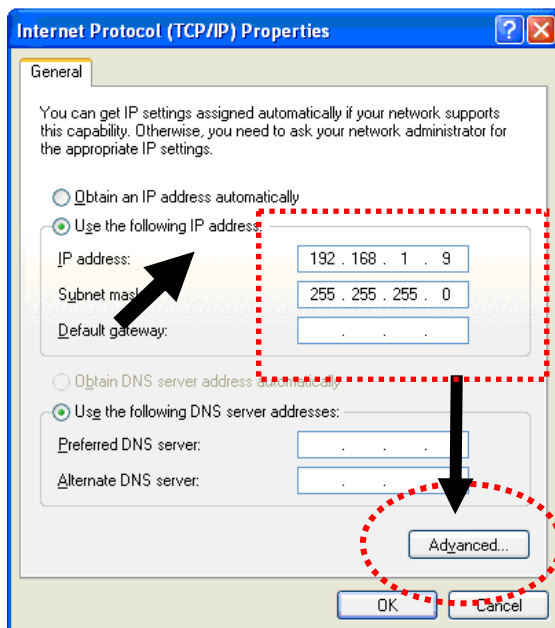
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Internet Connections** icon, click **Network Connections**, and then double-click **Local Area Connection, Local Area Connection Status** window will appear, and then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



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

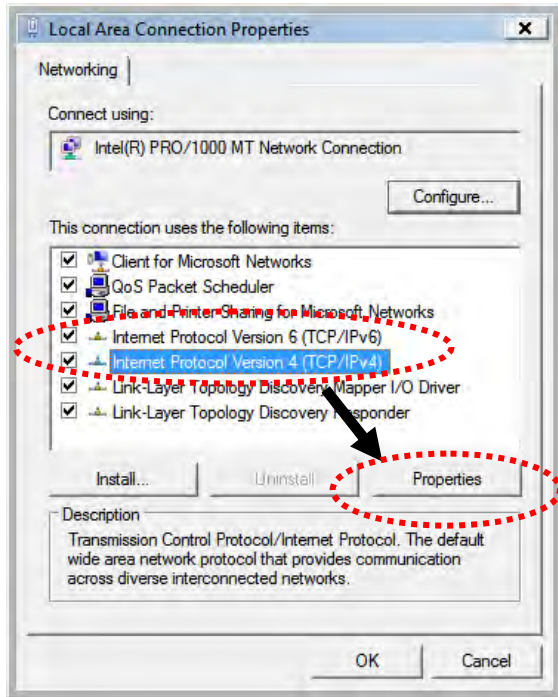
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**.



2.4 Windows Vista IP Address Setup

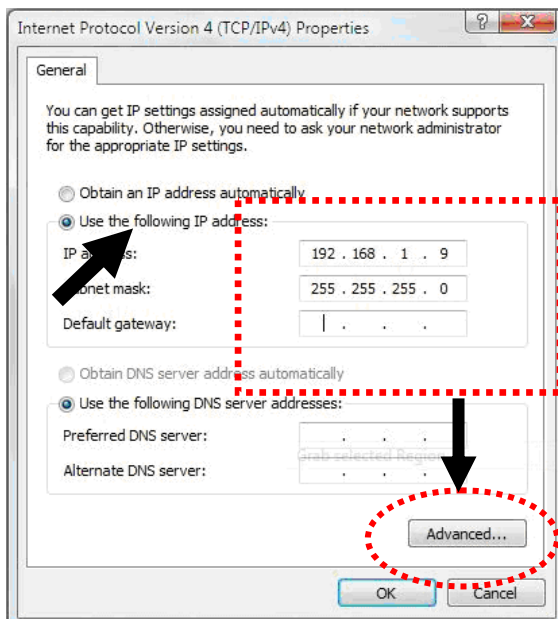
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Click **View Network Status and Tasks**, then click **Manage Network Connections**. Right-click **Local Area Network**, then select **'Properties'**. **Local Area Connection Properties** window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



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

IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.5 Accessing to Web User Interface

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

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



Notice: You may either set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as the IP address of VigorAP800. If there is no DHCP server on the network, then VigorAP800 will have an IP Address of 192.168.1.2. If DHCP is available, then VigorAP800 will receive it's IP Address via DHCP, in this case to find the VigorAP800 IP Address please check the DHCP server.

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. Please type “admin/admin” on Username/Password and click **OK**.

Authentication Required

The server http://192.168.1.2:80 requires a username and password.
The server says: VigorAP800.

User Name:

Password:

Log In **Cancel**

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

VigorAP 800
802.11n Access Point

DrayTek

System Status

Model : VigorAP 800
Device Name : VigorAP800
Firmware Version : 1.1.6
Build Date/Time : r6306 Wed Aug 17 17:01:37 CST 2016
System Uptime : 0d 00:00:54
Operation Mode : AP

System	
Memory Total	: 30252 kB
Memory Left	: 13376 kB

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:5E:AB:68
SSID	: DrayTek-LAN-A
Channel	: 11

Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:5E:AB:68
SSID	: DrayTek-5G
Channel	: 36

LAN-A	
MAC Address	: 00:50:7F:5E:AB:68
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

LAN-B	
MAC Address	: 00:50:7F:5E:AB:68
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

WARNING: Your AP is still set to default password. You should change it via System Maintenance menu.

Admin mode
AP Mode

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**.

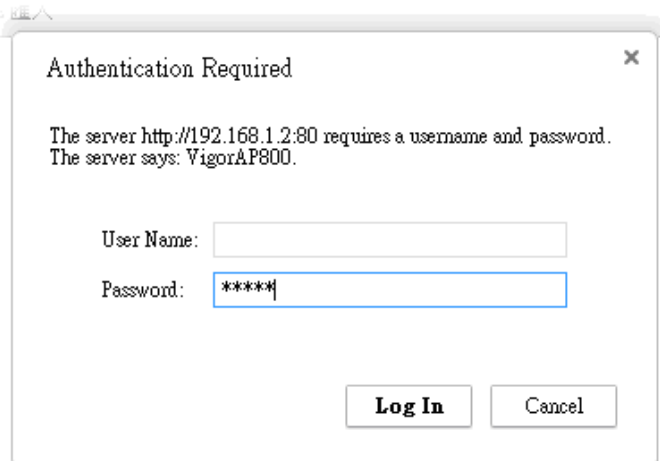
System Maintenance >> Administration Password

Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
Password Strength:	<input type="button" value="Weak"/> <input type="button" value="Medium"/> <input type="button" value="Strong"/>
Strong password requirements:	
1. Have at least one upper-case letter and one lower-case letter.	
2. Including non-alphanumeric characters is a plus.	

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

3. Enter the new login password on the field of **Password** and **Confirm 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.



The image shows a dialog box titled "Authentication Required" with a close button (X) in the top right corner. The text inside the dialog reads: "The server http://192.168.1.2:80 requires a username and password. The server says: VigorAP800." Below this text are two input fields: "User Name:" followed by an empty text box, and "Password:" followed by a password box containing "*****". At the bottom of the dialog are two buttons: "Log In" and "Cancel".

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 2.4G Wireless Settings – General

This page displays general settings for the operation mode selected.

Quick Start Wizard >> Wireless LAN (2.4GHz)

Operation Mode :
AP 800 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

Wireless Mode :

Main SSID : Enable 2 Subnet (Simulate 2 APs)

Channel :

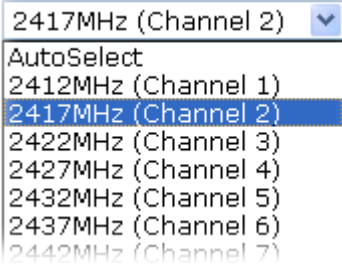
Extension Channel :

Station List :

Wireless(2.4GHz)
Security(2.4GHz)
Wireless(5GHz)
Security(5GHz)

Available settings are explained as follows:

Item	Description
Operation Mode	<p>There are six operation modes for wireless connection. Settings for each mode are different.</p> <div style="border: 1px solid black; padding: 5px;"> <input type="text" value="AP Bridge-WDS"/> <ul style="list-style-type: none"> AP Station-Infrastructure AP Bridge-Point to Point AP Bridge-Point to Multi-Point AP Bridge-WDS Universal Repeater </div>
Wireless Mode	<p>At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> <div style="border: 1px solid black; padding: 5px;"> <input type="text" value="Mixed(11b+11g+11n)"/> <ul style="list-style-type: none"> 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11b+11g+11n) </div>
Main SSID	<p>Set a name for VigorAP 800 to be identified.</p> <p>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</p>

	<p>independent AP/subnet functions in one VigorAP 800.</p> <p>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.</p> <p>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.</p>
Channel	<p>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.</p> 
Extension Channel	<p>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.</p>
Station List	<p>Click this button to open the Station List dialog. It provides the knowledge of connecting wireless clients now along with its status code.</p>
AP Discovery	<p>Click this button to open the AP Discovery dialog. VigorAP 800 can scan all regulatory channels and find working APs in the neighborhood.</p> <p>This option is available when AP-Bridge/Universal Repeater is selected as the Operation Mode.</p>
Site Survey	<p>This option is available only when Station-Infrastructure is selected as the Operation Mode.</p> <p>Click Display to pop up a window. Then, click Scan to list the access points nearby. You can select one of the access points to associate.</p>

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

2.7.2 Configuring 2.4G 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 Station-Infrastructure

When you choose Station-Infrastructure, after clicking **Next**, you will need to configure the following page to connect to one AP.

[Quick Start Wizard >> 2.4G Wireless](#)

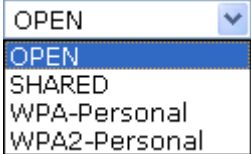
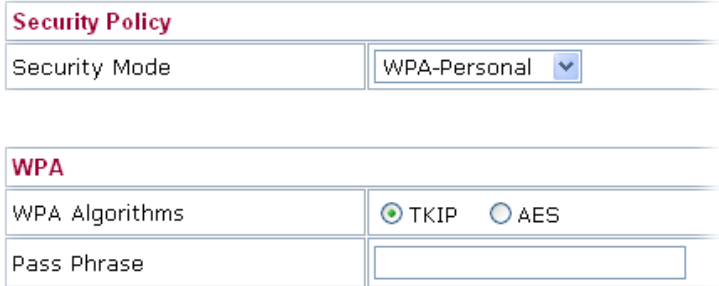
Setup Profile to connect to AP :

System Configuration	
Profile Name	PROF001
SSID	
Network Type	Infrastructure ▼
Power Saving Mode	<input checked="" type="radio"/> CAM (Constantly Awake Mode) <input type="radio"/> Power Saving Mode
RTS Threshold	<input type="checkbox"/> Used <input type="text" value="2347"/>
Fragment Threshold	<input type="checkbox"/> Used <input type="text" value="2346"/>
Security Policy	
Security Mode	OPEN ▼

WEP	
WEP Key Length	64 bit (10 hex digits / 5 ascii keys) ▼
WEP Key Entry Method	Hexadecimal ▼
WEP Keys	WEP Key 1 : <input type="text"/>
	WEP Key 2 : <input type="text"/>
	WEP Key 3 : <input type="text"/>
	WEP Key 4 : <input type="text"/>
Default Key	Key 1 ▼

Available settings are explained as follows:

Item	Description
System Configuration	<p>Profile Name -Type a name for the new profile.</p> <p>SSID - Type the name for such access point that can be used for connection by the stations.</p> <p>Network Type</p> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;"> Infrastructure ▼ 802.11 Ad Hoc Infrastructure </div> <ul style="list-style-type: none"> ● Infrastructure - In this mode, you can connect the access point to Ethernet device such as TV and Game player to enable the Ethernet device as a wireless station and join to

	<p>a wireless network through an access point or AP router.</p> <ul style="list-style-type: none"> ● 802.11 Ad Hoc – An ad-hoc network is a network where wireless stations can communicate with peer to peer (P2P). <p>Power Saving Mode - Choose the power saving mode for such device.</p> <ul style="list-style-type: none"> ● CAM – Choose this item if it is not necessary to perform power saving job. ● Power Saving Mode – Choose this item to get into the power saving status when there is no data passing through the access point. <p>RTS Threshold- Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.</p> <p>Fragment Threshold - Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.</p>
<p>Security Mode</p>	<p>802.11 standard defines two mechanisms for authentication of wireless LAN clients: Open Authentication and Shared Key Authentication.</p> <p>Choose one of the security modes from the drop down list. If you choose OPEN or SHARED, you have to type WEP information.</p> <p>OPEN – Open authentication is basically null authentication algorithm, which means that there is no verification of the user.</p> <p>SHARED – It works similar to Open authentication with only one major difference. If you choose OPEN with WEP encryption key, the WEP keys is used to encrypt and decrypt the data but not for authentication. In Shared key authentication, WEP encryption will be used for authentication.</p>  <p>If you choose WPA-Personal or WPA2-Personal, the corresponding WPA settings will be listed as follows. You have to choose the WPA algorithms and type the pass phrase for such security mode.</p>  <p>WPA Algorithms – Choose Temporal Key Integrity Protocol (TKIP) or AES for data encryption.</p>

	<p>Pass Phrase – Please type 8 to 63 alphanumerical characters here.</p>
<p>WEP</p>	<p>WEP Key Length - WEP (Wired Equivalent Privacy) is a common encryption mode. It is safe enough for home and personal use. However, if you need higher level of security, please consider using WPA encryption (see next section). Some wireless clients do not support WPA, but support WEP. Therefore WEP is still a good choice for you if you have such kind of client in your network environment.</p> <div data-bbox="639 533 1161 631" style="border: 1px solid black; padding: 2px;"> <p>64 bit (10 hex digits / 5 ascii keys) ▾ 64 bit (10 hex digits / 5 ascii keys) 128 bit (26 hex digits / 13 ascii keys)</p> </div> <p>WEP Key Entry Method - There are two types of WEP key length: 64-bit and 128-bit. Using 128-bit is safer than 64-bit, but it will reduce some data transfer performance. There are two types of key method: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select 64-bit as key length, and Hex as key format, you'll see the message at the right of Key Format is 'Hex (10 characters)' which means the length of WEP key is 10 characters.</p> <div data-bbox="639 958 853 1057" style="border: 1px solid black; padding: 2px;"> <p>Hexadecimal ▾ Hexadecimal Ascii Text</p> </div> <p>WEP Keys (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.</p> <p>Default Key – Choose one of the key settings.</p>

Advanced Settings for AP Bridge-Point to Point

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

[Quick Start Wizard >> Wireless LAN \(2.4GHz\)](#)

Note : Enter the configuration of APs which AP 800 want to connect.

Phy Mode : HTMIX
Security : <input type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input type="text"/>
Peer MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Available settings are explained as follows:

Item	Description
Phy Mode	Data will be transmitted via HTMIX communication channel. 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 800 connects to.

Advanced Settings for AP Bridge-Point to Multi-Point

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

Quick Start Wizard >> Wireless LAN (2.4GHz)

Note : Enter the configuration of APs which AP 800 want to connect.

Phy Mode : HTMIX

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

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

2. 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	Data will be transmitted via HTMIX communication channel. 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 800 connects to.

Advanced Settings for AP Bridge-WDS

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

[Quick Start Wizard >> Wireless LAN \(2.4GHz\)](#)

Note : Enter the configuration of APs which AP 800 want to connect.
Remote AP should always set LAN-A MAC address to connect AP800 WDS.

Phy Mode : HTMIX

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 :

: : : : :

< Back
Next >
Cancel

Available settings are explained as follows:

Item	Description
Phy Mode	Data will be transmitted via HTMIX communication channel. 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. Or, you can click Disable to disable the function.
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 800 connects to.

Advanced Settings for AP Bridge-Universal Repeater

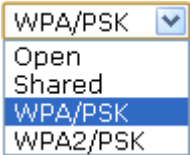
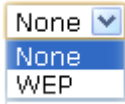
When you choose AP Bridge-Universal Repeater, after clicking **Next**, you will need to configure the following page.

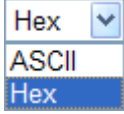
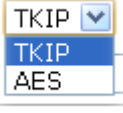
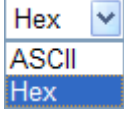
[Quick Start Wizard >> Wireless LAN \(2.4GHz\)](#)

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

SSID	<input type="text"/>
MAC Address (Optional)	<input type="text"/>
Security Mode	Open <input type="button" value="v"/>
Encryption Type	None <input type="button" value="v"/>
WEP Keys	
<input type="radio"/> Key 1 :	<input type="text"/> ASCII <input type="button" value="v"/>
<input type="radio"/> Key 2 :	<input type="text"/> ASCII <input type="button" value="v"/>
<input type="radio"/> Key 3 :	<input type="text"/> ASCII <input type="button" value="v"/>
<input type="radio"/> Key 4 :	<input type="text"/> ASCII <input type="button" value="v"/>

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	<p>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.</p> 
Encryption Type for Open/Shared	<p>This option is available when Open/Shared is selected as Security Mode.</p> <p>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.</p>  <p>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</p>

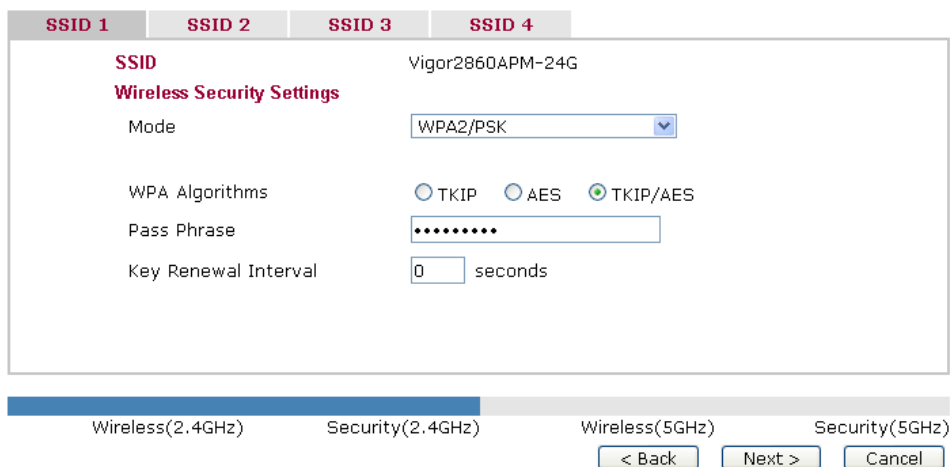
	<p>hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.</p> 
Encryption Type for WPA/PSK and WPA2/PSK	<p>This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode.</p> <p>Select TKIP or AES as the algorithm for WPA.</p> 
WEP Keys	<p>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 ','.</p> 
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 2.4G Security Settings

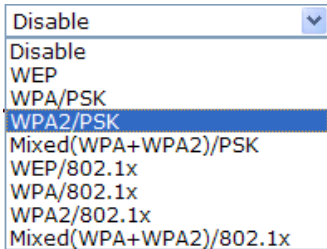
VigorAP 800 offers 2.4G wireless connection capability. You can setup 2.4G features in Quick Start Wizard first. Once the USB 2.4G wireless dongle connects to VigorAP 800, it can work immediately.

Quick Start Wizard >> Wireless Security (2.4GHz)



Available settings are explained as follows:

Item	Description
------	-------------

Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>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.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>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.</p> <p>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.</p>
WPA Algorithm	<p>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.</p>
Pass Phrase	<p>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.</p>
Key Renewal Internal	<p>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.</p>
PMK Cache Period	<p>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</p>

	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 5G Wireless Settings

VigorAP 800 offers 5G wireless connection capability. You can setup 5G features in Quick Start Wizard first. Once the USB 5G wireless dongle connects to VigorAP 800, it can work immediately.

Quick Start Wizard >> **Wireless LAN (5GHz)**

Wireless Mode :

Main SSID :

Channel :

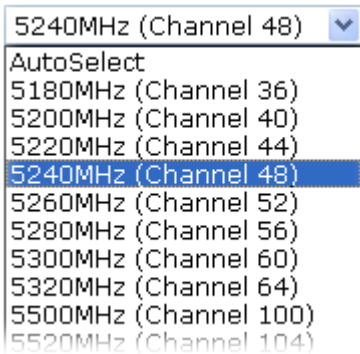
Extension Channel :

Station List :

Progress bar: Wireless(2.4GHz) | Security(2.4GHz) | **Wireless(5GHz)** | Security(5GHz)

Available settings are explained as follows:

Item	Description
Wireless Mode	At present, VigorAP 800 can connect to 11a only, 11n only (5G), Mixed (11a+11n) stations simultaneously. Simply choose Mixed (11a+11n) mode. <input type="text" value="11n only(5G)"/> 11a only 11n only(5G) Mixed (11a+11n)

Main SSID	Set a name for VigorAP 800 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. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you. 
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 5G Security Settings

VigorAP 800 offers 5G wireless connection capability. You can setup 5G features in Quick Start Wizard first. Once the USB 5G wireless dongle connects to VigorAP 800, it can work immediately.

Quick Start Wizard >> Wireless Security (5GHz)

SSID 1	SSID 2	SSID 3
SSID		
Vigor2860APM-5G		
Wireless Security Settings		
Mode	WPA2/PSK	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase	••••••••	
Key Renewal Interval	3600 seconds	

Wireless(2.4GHz) Security(2.4GHz) Wireless(5GHz) Security(5GHz)

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> Disable ▼ </div> <ul style="list-style-type: none"> Disable WEP WPA/PSK <li style="background-color: #e0e0e0;">WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x </div> <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>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.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in</p>

	<p>this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p>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.</p>
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.
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	<p>Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p>Enable - Enable the WEP Encryption.</p> <p>Such feature is available for WEP/802.1x mode.</p>

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 AP800 is completed.

Press Finish button to save and finish the wizard setup.

Note that the configuration process takes a few seconds to complete.

< Back

Finish

Cancel

2.8 Online Status

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

Online Status

System Status

System Uptime: 0d 16:32:32

LAN Status				
IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.1.2	13872	5558	9661929	502478

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.

The screenshot displays the web interface for a VigorAP 800 access point. The page title is "VigorAP 800" and "802.11n Access Point". The DrayTek logo is in the top right corner. On the left, there is a navigation menu with options like "Quick Start Wizard", "Online Status", "Operation Mode", "LAN", "Central AP Management", "Wireless LAN (2.4GHz)", "Wireless LAN (5GHz)", "RADIUS Server", "Applications", "System Maintenance", and "Diagnostics". Below the menu is a "Support Area" section with links for "FAQ/Application Note" and "Product Registration".

The main content area is titled "System Status" and contains the following information:

- Model** : VigorAP 800
- Device Name** : VigorAP800
- Firmware Version** : 1.1.6
- Build Date/Time** : r6306 Wed Aug 17 17:01:37 CST 2016
- System Uptime** : 0d 00:00:54
- Operation Mode** : AP

Below this, there are three tables showing system and network details:

System	
Memory Total	: 30252 kB
Memory Left	: 13376 kB

LAN-A	
MAC Address	: 00:50:7F:5E:AB:68
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:5E:AB:68
SSID	: DrayTek-LAN-A
Channel	: 11

LAN-B	
MAC Address	: 00:50:7F:5E:AB:68
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:5E:AB:68
SSID	: DrayTek-5G
Channel	: 36

A warning message is displayed at the bottom: **WARNING: Your AP is still set to default password. You should change it via System Maintenance menu.**

At the bottom left, there are two status indicators: "Admin mode" (highlighted in green) and "AP Mode".

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 800 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.
- Station-Infrastructure :**
Enable the Ethernet device as a wireless station and join a wireless network through an AP.
- AP Bridge-Point to Point :**
AP 800 will connect to another AP 800 which uses the same mode, and all wired Ethernet clients of both AP 800s will be connected together.
- AP Bridge-Point to Multi-Point :**
AP 800 will connect to up to four AP 800s which uses the same mode, and all wired Ethernet clients of every AP 800s will be connected together.
- AP Bridge-WDS :**
AP 800 will connect to up to four AP 800s which uses the same mode, and all wired Ethernet clients of every AP 800s will be connected together.
This mode is still able to accept wireless clients.
- Universal Repeater :**
AP 800 can act as a wireless repeater; it can be Station and AP at the same time.

Wireless LAN (5GHz)

- AP :**
AP 800 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

Available settings are explained as follows:

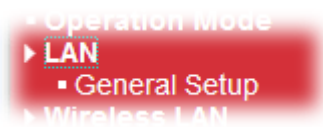
Item	Description
2.4G Wireless	
AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
Station-Infrastructure	Enable the Ethernet device such as TV and Game player connected to the VigorAP 800 to an access point.
AP Bridge-Point to Point	This mode can establish wireless connection with another VigorAP 800 using the same mode, and link the wired network which these two VigorAP 800s connected together. Only one access point can be connected in this mode.
AP Bridge-Point to Multi-Point	This mode can establish wireless connection with other VigorAP 800s using the same mode, and link the wired network which these VigorAP 800s connected together. Up to 4 access points can be connected in this mode.
AP Bridge-WDS	This mode is similar to AP Bridge to Multi-Point, but access point is not work in bridge-dedicated mode, and will be able to accept wireless clients while the access point is working as a wireless bridge.

Universal Repeater	This product can act as a wireless range extender that will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.
5G Wireless	
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

<p>LAN-A IP Network Configuration</p> <p><input checked="" type="checkbox"/> Enable DHCP Client</p> <p>IP Address: <input type="text" value="192.168.1.2"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p>Default Gateway: <input type="text"/></p> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID: <input type="text" value="0"/></p>	<p>DHCP Server Configuration</p> <p><input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>Start IP Address: <input type="text"/></p> <p>End IP Address: <input type="text"/></p> <p>Subnet Mask: <input type="text"/></p> <p>Default Gateway: <input type="text"/></p> <p>Lease Time: <input type="text" value="86400"/></p> <p>DHCP Server IP: <input type="text"/></p> <p>Address for Relay Agent: <input type="text"/></p> <p>Primary DNS Server: <input type="text"/></p> <p>Secondary DNS Server: <input type="text"/></p>
<p>LAN-B IP Network Configuration</p> <p><input type="checkbox"/> Enable DHCP Client</p> <p>IP Address: <input type="text" value="192.168.2.2"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID: <input type="text" value="0"/></p>	<p>DHCP Server Configuration</p> <p><input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>Start IP Address: <input type="text"/></p> <p>End IP Address: <input type="text"/></p> <p>Subnet Mask: <input type="text"/></p> <p>Default Gateway: <input type="text"/></p> <p>Lease Time: <input type="text" value="86400"/></p> <p>DHCP Server IP: <input type="text"/></p> <p>Address for Relay Agent: <input type="text"/></p> <p>Primary DNS Server: <input type="text"/></p> <p>Secondary DNS Server: <input type="text"/></p>

Note: Disable "DHCP Client" or "Auto Provision" for VigorAP Management only work with Vigor2860 v3.7.3.1 and newer APM Server.

Available settings are explained as follows:

Item	Description
LAN IP Network Configuration	<p>Enable DHCP Client - When it is enabled, VigorAP 800 will be treated as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2860).</p> <ul style="list-style-type: none"> ● 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 800. However, if it is required, simply type an IP address as the gateway for VigorAP 800. It will be convenient for the access point acquiring more service (e.g., accessing NTP server) from Vigor router. <p>Enable Management VLAN - VigorAP 800 supports tag-based VLAN for wireless clients accessing Vigor router. Only the clients with the specified VLAN ID can access into VigorAP 800.</p> <ul style="list-style-type: none"> ● VLAN ID - Type the number as VLAN ID tagged on the transmitted packet. "0" means no VALN tag.
DHCP Server Configuration	<p>DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client.</p> <p>Enable Server / Disable Server - Enable Server lets the modem assign IP address to every host in the LAN.</p> <p>Disable Server lets you manually or use other DHCP server to assign IP address to every host in the LAN.</p> <p>Relay Agent - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.</p> <p>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.</p> <p>End IP Address - Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>Default Gateway - Enter a value of the gateway IP address for the DHCP server.</p> <p>Lease Time - It allows you to set the leased time for the specified PC.</p> <p>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.</p> <p>Primary IP Address - You must specify a DNS server IP</p>

	<p>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.</p> <p>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.</p>
--	--

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

3.3 Central AP Management

Central AP Management allows you to configure VigorAP 800 to be managed by Vigor2860 series.



3.3.1 General Setup

Central AP Management >> General Setup

Vigor AP Managemet

<input checked="" type="checkbox"/> Enable AP Management <input checked="" type="checkbox"/> Enable Auto Provision

Available settings are explained as follows:

Item	Description
Enable AP Management	Check the box to enable the function of AP Management.
Enable Auto Provision	VigorAP can be controlled under Central AP Management in Vigor2860 series. When both Vigor2860 series and VigorAP have such feature enabled, once VigorAP is registered to Vigor2860 series, the WLAN profile pre-configured on Vigor2860 series will be applied to VigorAP immediately. Thus, it is not necessary to configure VigorAP separately.

3.3.2 Function Support List

Click the **Client** tab to list the AP management functions that the Access Points support under different firmware versions.

Central AP Management >> Function Support List

Function Name	Model Name		
	AP 800		
	1.0.5	1.1.0	1.1.1
Register			
DHCP	√	√	√
Static IP			√
Profile			
2.4GHz	√	√	√
5GHz			√
AP Mode	√	√	√
Repeater Mode			√
Client Disable Auto Provision			√
WLAN Enable/Disable			
Station List			
Station List			√

Note: DrayTek central wireless management (AP Management) lets control, efficiency, monitoring and security of your company-wide wireless access easier be managed. Inside the web user interface, we call “central wireless management” as Central AP Management which supports mobility, client monitoring/reporting and load-balancing to multiple APs. For central wireless management, you will need a Vigor2860 or Vigor2925 series router; there is no per-node licensing or subscription required. With the unified user interface of Vigor2860 Combo WAN series and Vigor2925 Triple WAN series, the multiple deployment of VigorAP can be clear at the first sight. For multiple wireless clients, to apply the AP Load Balancing to the multiple APs will manage wireless traffic with smooth flow and enhanced efficiency.

3.4 General Concepts for Wireless LAN

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

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

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

Security Overview

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

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

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

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

WPS Introduction

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

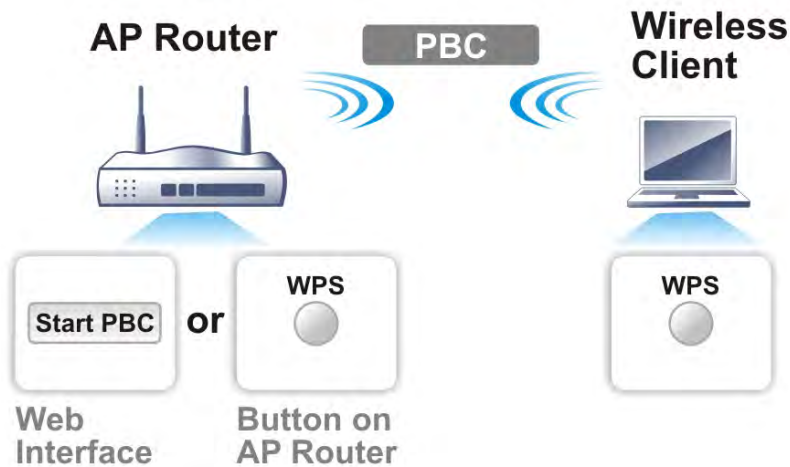
It is the simplest way to build connection between wireless network clients and VigorAP 800. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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



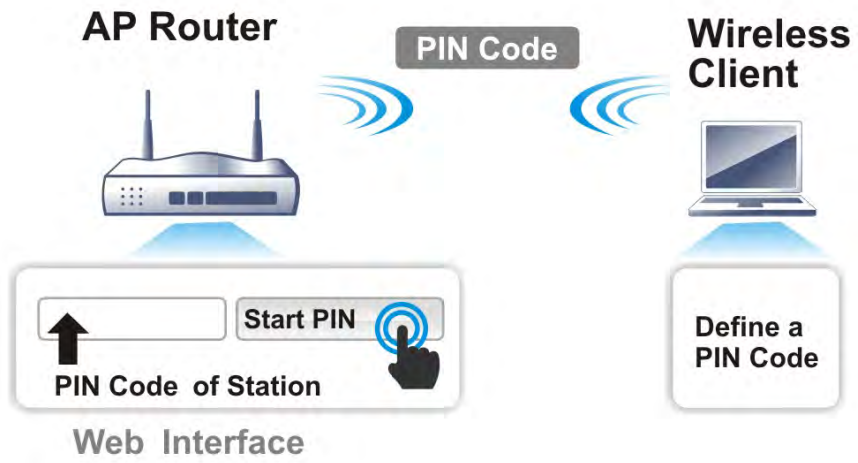
Note: Such function is available for the wireless station with WPS supported.

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

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

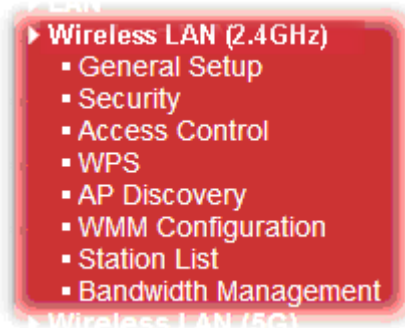


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 800.



3.5 Wireless LAN (2.4GHz) Settings for AP Mode

When you choose AP as the operation mode for Wireless LAN (2.4GHz), the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery, WMM Configuration, Station List and Bandwidth Management.



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

3.5.1 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.

General Setting (IEEE 802.11)

Enable Wireless LAN

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

Mode :

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
1	<input type="checkbox"/>	<input type="text" value="DrayTek-LAN-A"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="text" value="DrayTek-LAN-B"/>	<input type="text" value="LAN-B"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>

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 :

Extension Channel :

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.

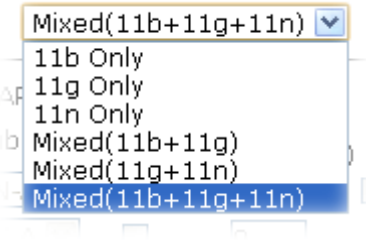
Antenna :

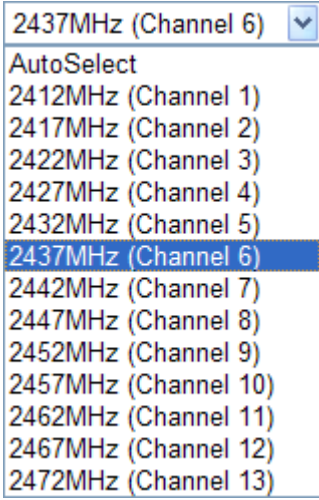

Tx Power :

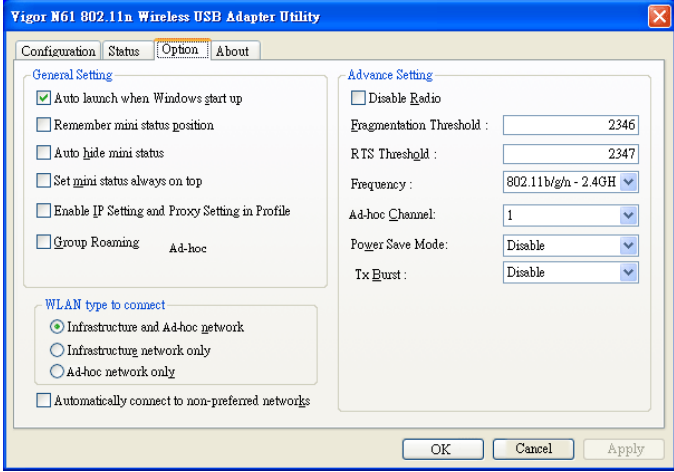

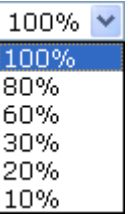
Channel Width : Auto 20/40 MHZ 20 MHZ

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 800 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.

	
<p>Enable 2 Subnet (Simulate 2 APs)</p>	<p>Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.</p> <p>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.</p>
<p>Hide SSID</p>	<p>Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 800 while site surveying. The system allows you to set three sets of SSID for different usage.</p>
<p>SSID</p>	<p>Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.</p>
<p>Subnet</p>	<p>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.</p>
<p>Isolate Member</p>	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p>
<p>VLAN ID</p>	<p>Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.</p> <p>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.</p>
<p>Mac Clone</p>	<p>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.</p>

<p>Channel</p>	<p>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.</p> 
<p>Extension Channel</p>	<p>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.</p>
<p>Rate</p>	<p>If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.</p> <p>SSID4: <small>the Wireless client will also change based on this MAC address. Reserved for Universal Repeater mode so it's not listed.</small></p>  <p>Note :</p>
<p>Packet-OVERDRIVE</p>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>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).</p>

	
<p>Antenna</p>	<p>VigorAP 800 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.</p> 
<p>Tx Power</p>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p> 
<p>Channel Width</p>	<p>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.</p>

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

3.5.2 Security

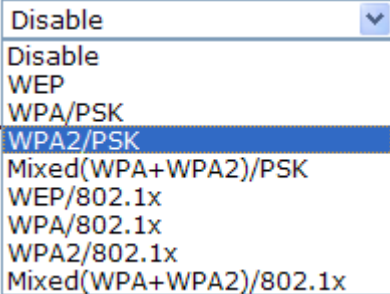
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

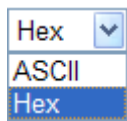
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID		Vigor2860APM-24G	
Mode		WPA2/PSK	
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms		<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase		<input type="text" value="*****"/>	
Key Renewal Interval		<input type="text" value="0"/> seconds	
WEP			
<input checked="" type="radio"/> Key 1 :		<input type="text"/>	<input type="text" value="Hex"/>
<input type="radio"/> Key 2 :		<input type="text"/>	<input type="text" value="Hex"/>
<input type="radio"/> Key 3 :		<input type="text"/>	<input type="text" value="Hex"/>
<input type="radio"/> Key 4 :		<input type="text"/>	<input type="text" value="Hex"/>
802.1x WEP		<input type="radio"/> Disable <input type="radio"/> Enable	

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>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.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access</p>

	<p>authentication for network management.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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.</p> 
802.1x WEP	<p>Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p>Enable - Enable the WEP Encryption.</p> <p>Such feature is available for WEP/802.1x mode.</p>

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

Radius Server

<input checked="" type="checkbox"/> Use internal RADIUS Server	
IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 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 800.
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.

3.5.3 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

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 800. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> Activate MAC address filter ▼ Disable Activate MAC address filter Blocked MAC address filter </div>
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.


OK	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.
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.

3.5.4 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	Vigor2860APM-24G
WPS Auth Mode	WPA2/PSK
WPS Encryp Type	TKIP/AES

Device Configure

Configure via Push Button	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="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 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 800. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 800 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on

PinCode	VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).
----------------	--

3.5.5 AP Discovery

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

This page is used to scan the existence of the APs on the wireless LAN. Please click **Scan** to discover all the connected APs.

[Wireless LAN >> Access Point Discovery](#)

Access Point List

Show List in order of RSSI values from 100% to 0%

SSID	BSSID	RSSI	Channel	Encryption	Authentication
DrayTek 5F...	00:1d:aa:2e:a5:00	100%	1	AES	WPA2/PSK
kyeh_2760_...	00:1d:aa:aa:d0:40	96%	6	NONE	
DrayTek 5F...	00:1d:aa:2e:92:a0	76%	1	AES	WPA2/PSK
DrayTek	00:1d:aa:ac:1a:40	60%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
2860 PQC t...	00:1d:aa:a8:b7:78	55%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
RD2_Johnny...	00:50:7f:94:e7:58	55%	10	TKIP/AES	Mixed(WPA+WPA2)/PSK
DrayTek 6F...	00:1d:aa:2d:ef:60	50%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK
DrayTek 5F...	00:1d:aa:2e:94:b0	44%	1	AES	WPA2/PSK
	00:1d:aa:a6:25:e8	39%	3	TKIP/AES	Mixed(WPA+WPA2)/PSK
44444	00:1d:aa:27:6f:c0	34%	3	TKIP/AES	WPA2
	00:50:7f:8f:fa:a8	24%	6	AES	WPA2/PSK
AP800-PoES...	00:1d:aa:25:68:38	15%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
DrayTek-LA...	00:1d:aa:25:68:39	10%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
DrayTek	00:1d:aa:ac:1a:08	0%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
DrayTek1	00:1d:aa:a4:23:10	0%	6	AES	WPA2/PSK
D-Link_DIR...	bc:f6:85:a8:01:fb	0%	11	NONE	

Scan

See [Channel Statistics](#)

Note: 1. During the scanning process (about 5 seconds), no station is allowed to connect with the router.
2. If you select/disselect 'Show List in order of RSSI values from 100% to 0%', you should click Scan Button again to make this function run OK.

Each item is explained as follows:

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

3.5.6 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 >> WMM Configuration

[Set to Factory Default](#)

WMM Configuration Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

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 800 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	<p>“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.</p> <p>“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.</p>

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

3.5.7 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

MAC Address	SSID	Auth	Encrypt	Tx Rate(Kbps)	Rx Rate(Kbps)

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.
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 .

3.5.8 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		Vigor2860APM-24G	
Per Station Bandwidth Limit			
Enable	<input checked="" type="checkbox"/>		
Upload Limit	User defined	100K	bps (Default unit : K)
Download Limit	User defined	100K	bps (Default unit : K)
Auto Adjustment	<input checked="" type="checkbox"/>		
Total Upload Bandwidth	User defined	200K	bps (Default unit : K)
Total Download Bandwidth	User defined	200K	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.

OK Cancel

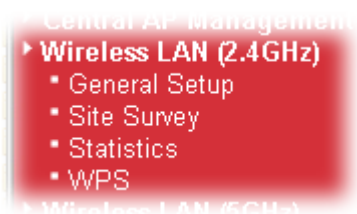
Available settings are explained as follows:

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 Wireless LAN (2.4GHz) Settings for Station-Infrastructure Mode

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



3.6.1 General Setup

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

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Mode :

Profile List

Profile	SSID	Channel	Authentication	Encryption
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Connect"/>				

Packet-OVERDRIVE

Tx Burst

Note :

- 1.Tx Burst only supports 11g mode.
- 2.The same technology must also be supported in AP to boost WLAN performance.

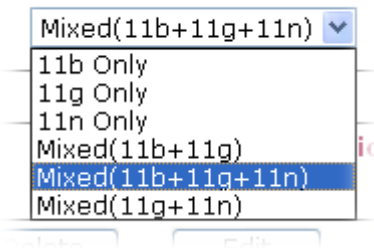
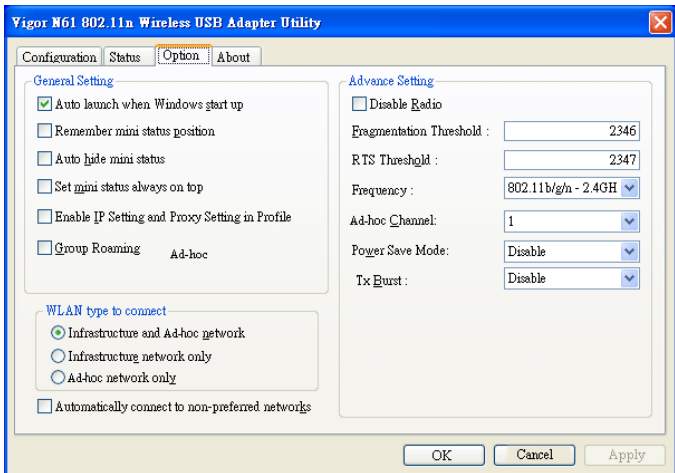
Mac Clone

Note :

1. Please notice that the last byte of this MAC address must be a multiple of 8.

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, VigorAP 800 can connect to 11 b only, 11 g only, 11 n only, Mixed (11b+11g), Mixed (11b+11g+11n) and Mixed (11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

	
Add	Click this button to add new wireless profiles.
Delete	Click this button to delete the selected wireless profile.
Edit	Click this button to modify the existing wireless profile.
Connect	Click this button to connect the wireless station to AP with the selected profile.
Packet-OVERDRIVE	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>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).</p> 
Mac Clone	Check this box and manually enter the MAC address for Station mode driver.

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

Add a New Wireless Profile

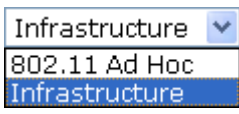
To add a new wireless profile for the stations, click **Add**. The following dialog box will appear.

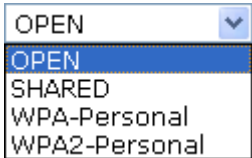
System Configuration	
Profile Name	PROF001
SSID	
Network Type	Infrastructure
Power Saving Mode	<input checked="" type="radio"/> CAM (Constantly Awake Mode) <input type="radio"/> Power Saving Mode
RTS Threshold	<input type="checkbox"/> Used 2347
Fragment Threshold	<input type="checkbox"/> Used 2346

Security Policy	
Security Mode	OPEN

WEP		
WEP Key Length	64 bit (10 hex digits / 5 ascii keys)	
WEP Key Entry Method	64 bit (10 hex digits / 5 ascii keys) 128 bit (26 hex digits / 13 ascii keys)	
WEP Keys	WEP Key 1 :	
	WEP Key 2 :	
	WEP Key 3 :	
	WEP Key 4 :	
Default Key	Key 1	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the new profile.
SSID	Type the name for such access point that can be used for connection by the stations.
Network Type	<p>Infrastructure - In this mode, you can connect the access point to Ethernet device such as TV and Game player to enable the Ethernet device as a wireless station and join to a wireless network through an access point or AP router.</p> <p>802.11 Ad Hoc – An ad-hoc network is a network where wireless stations can communicate with peer to peer (P2P).</p> 
Power Saving Mode	<p>Choose the power saving mode for such device.</p> <p>CAM – Choose this item if it is not necessary to perform power saving job.</p> <p>Power Saving Mode – Choose this item to get into the power</p>

	saving status when there is no data passing through the access point.
RTS Threshold	Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.
Fragment Threshold	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
Security Mode	<p>802.11 standard defines two mechanisms for authentication of wireless LAN clients: Open Authentication and Shared Key Authentication.</p> <p>Choose one of the security modes from the drop down list. If you choose OPEN or SHARED, you have to type WEP information.</p> <p>OPEN – Open authentication is basically null authentication algorithm, which means that there is no verification of the user.</p> <p>SHARED – It works similar to Open authentication with only one major difference. If you choose OPEN with WEP encryption key, the WEP keys is used to encrypt and decrypt the data but not for authentication. In Shared key authentication, WEP encryption will be used for authentication.</p>  <p>If you choose WPA-Personal or WPA2-Personal, the corresponding WPA settings will be listed as follows. You have to choose the WPA algorithms and type the pass phrase for such security mode.</p> <div data-bbox="646 1355 1364 1444" style="border: 1px solid #ccc; padding: 5px;"> <p>Security Policy</p> <p>Security Mode <input type="text" value="WPA-Personal"/></p> </div> <div data-bbox="646 1500 1364 1646" style="border: 1px solid #ccc; padding: 5px;"> <p>WPA</p> <p>WPA Algorithms <input checked="" type="radio"/> TKIP <input type="radio"/> AES</p> <p>Pass Phrase <input type="text"/></p> </div> <p>WPA Algorithms – Choose Temporal Key Integrity Protocol (TKIP) or AES for data encryption.</p> <p>Pass Phrase – Please type 8 to 63 alphanumerical characters here.</p>

WEP

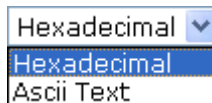
WEP Key Length - WEP (Wired Equivalent Privacy) is a common encryption mode. It is safe enough for home and personal use. However, if you need higher level of security, please consider using WPA encryption (see next section).

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



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

There are two types of key method: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select 64-bit as key length, and Hex as key format, you'll see the message at the right of Key Format is 'Hex (10 characters)' which means the length of WEP key is 10 characters.



WEP Keys (Key 1 – Key 4) - 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.

Default Key – Choose one of the key settings.

Below shows an example for a wireless profile created.

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Mode :

Profile List

	Profile	SSID	Channel	Authentication	Encryption
<input type="radio"/>	PROF001	vigor-1	Auto	OPEN	NONE

Packet-OVERDRIVE

Tx Burst

Note :

1. Tx Burst only supports 11g mode.
2. The same technology must also be supported in AP to boost WLAN performance.

Mac Clone

Note :

1. Please notice that the last byte of this MAC address must be a multiple of 8.

3.6.2 Site Survey

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

Wireless LAN (2.4GHz) >> Station Site Survey

Site Survey

	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="radio"/>	staffs_5F	00-E0-92-00-02-50	0%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	guests	00-E0-92-00-02-51	0%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	staffs	00-E0-92-00-02-52	0%	1	AES	WPA2/PSK
<input type="radio"/>	DrayTek	00-1D-AA-C6-4B-98	15%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	RD2_Kyle_2...	00-1D-AA-C3-3F-00	0%	6	NONE	
<input type="radio"/>	staffs_6F	00-1D-AA-9C-F3-C0	0%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	staffs	02-1D-AA-9C-F3-C0	0%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	guests	06-1D-AA-9C-F3-C0	0%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK

Available settings are explained as follows:

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

3.6.3 Statistics

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

Wireless LAN >> Station Statistics

Transmit Statistics

Frames Transmitted Successfully	4256
Frames Transmitted Successfully Without Retry	4256
Frames Transmitted Successfully After Retry(s)	0
Frames Fail To Receive ACK After All Retries	0
RTS Frames Successfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

Receive Statistics

Frames Received Successfully	49
Frames Received With CRC Error	11
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	0

[Reset Counters](#)

Click **Rest Counters** if required.

3.6.4 WPS (Wi-Fi Protected Setup)

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

VigorAP 800 supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch VigorAP800 to WPS mode and push a specific button on the wireless client to start WPS mode. You can push Reset/WPS button of this VigorAP 800, or click **PBC Start** button in the web configuration interface to do this; if you want to use PIN code, you have to provide the PIN code of the wireless client you wish to connect to this access point and then switch the wireless client to WPS mode.

Note: WPS function of VigorAP 800 will not work for those wireless AP/clients do not support WPS.

To use WPS function to set encrypted connection between VigorAP 800 and WPS-enabled wireless AP, please open **Wireless LAN >>WPS**. The following information will be displayed:

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

WPS AP site survey

No.	SSID	BSSID	RSSI	Ch.	Auth.	Encrypt	Ver.	Status
1	DrayTek	001DAAC64B98	20%	6	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.

Device Configure

Configure via Push Button	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="Start PIN"/> <input type="button" value="Renew PIN"/>
	<input type="button" value="Cancel"/>

Status: Idle

Available settings are explained as follows:

Item	Description
SSID	Display the SSID name of the access point.
BSSID	Display the BSSID (MAC Address) of the access point.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Ch. (Channel)	Display the channel number of the access point.
Auth. (Authentication)	Display the authentication type of the access point.
Encrypt (Encryption)	Display the encryption setting of the access points. If you have selected the access point with security setting, you have to go to 2-7 Wireless Security to set the same security with the access point you want to associate.
Ver. (Version)	Display the version of WPS.
Status	Display the status of WPS access point.
Refresh	Click this button to refresh the AP site survey.
Start PBC	Click Start PBC to make a WPS connection within 2 minutes.
PIN Start	When using PinCode method, it is required to enter PIN Code (Personal Identification Number Code, 8-digit numbers) into Registrar. When the wireless station is Enrollee, the users can use Renew PIN to re-generate a new PIN code.
Renew PIN	Click this button to re-generate a new PIN code.

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

3.7 Wireless LAN (2.4GHz) 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 800 to connect to **another** VigorAP 800 which uses the same mode. All wired Ethernet clients of both VigorAP 800s will be connected together.

Point-to Multi-Point Mode allows AP 800 to connect up to **four** VigorAP 800s which uses the same mode. All wired Ethernet clients of every VigorAP 800 will be connected together.

3.7.1 General Setup

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

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 AP 800 want to connect.

Phy Mode : HTMIX

<p>1. Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input style="width: 100%;" type="text"/> Peer Mac Address: <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p>3. Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input style="width: 100%;" type="text"/> Peer Mac Address: <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>
<p>2. Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input style="width: 100%;" type="text"/> Peer Mac Address: <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p>4. Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input style="width: 100%;" type="text"/> Peer Mac Address: <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>

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 ▼

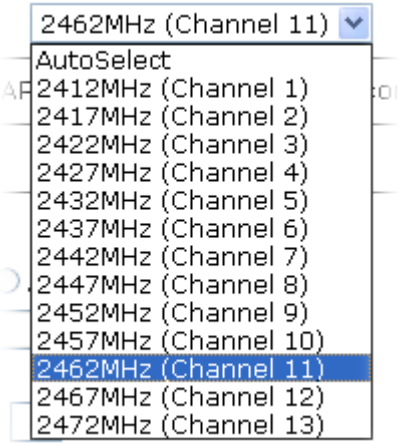
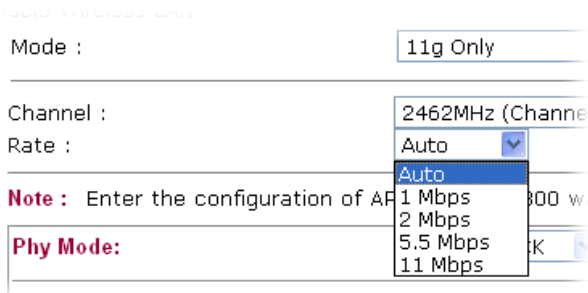
Tx Power : 100% ▼

Channel Width : Auto 20/40 MHz 20 MHz

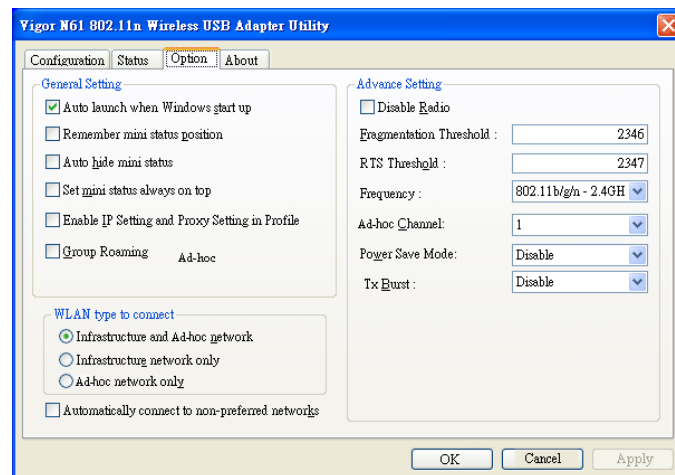
OK
Cancel

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Mixed(11b+11g+11n) ▼ 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n) </div>
Channel	Means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected

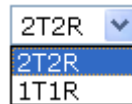
	<p>channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.</p> 
Extension Channel	<p>With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the Channel selected above.</p>
Rate	<p>If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.</p>  <p>Note: Enter the configuration of AP</p> <p>Phy Mode:</p>
PHY Mode	<p>Data will be transmitted via HTMIX communication channel.</p> <p>Each access point should be setup to the same Phy mode for connecting with each other.</p>
Security	<p>Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.</p>
Peer Mac Address	<p>Type the peer MAC address for the access point that VigorAP 800 connects to.</p>
Packet-OVERDRIVE	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>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</p>

TxBURST on the tab of Option).



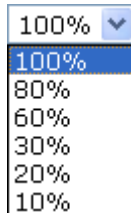
Antenna

VigorAP 800 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.

3.7.2 AP Discovery

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

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

Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Show List in order of RSSI values from 100% to 0%

Select	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="radio"/>	DrayTek	00:1d:aa:c6:4b:98	10%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	staffs	00:e0:92:00:02:52	5%	1	AES	WPA2/PSK
<input type="radio"/>	guests	00:e0:92:00:02:51	0%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	RD2_Kyle_2...	00:1d:aa:c3:3f:00	0%	6	NONE	
<input type="radio"/>	aaa_rudy_w...	00:1d:aa:c1:e6:30	0%	6	NONE	
<input type="radio"/>	staffs_6F	00:1d:aa:9c:f3:c0	0%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	staffs	02:1d:aa:9c:f3:c0	0%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK

See [Channel Statistics](#)

Note: 1. During the scanning process (about 5 seconds), no station is allowed to connect with the router.
2. If you select/deselect 'Show List in order of RSSI values from 100% to 0%', you should click Scan Button again to make this function run OK.

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

Add to [WDS Settings](#):

Available settings are explained as follows:

Item	Description
Show List....	Check the box to display the RSSI value with the order from 100% to 0.
SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 800.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Channel Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please

	type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Add	Click Bridge for the specified AP. Next, click Add . Later, the MAC address of the AP will be added and be shown on WDS settings page.

3.7.3 WDS AP Status

VigorAP 800 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 >> WDS AP Status

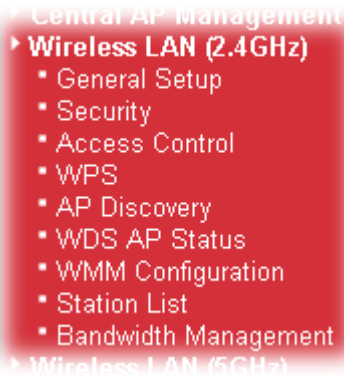
WDS AP List

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

Refresh

3.8 Wireless LAN (2.4GHz) 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, WDS AP Status, WMM Configuration, Station List and Bandwidth Management.



3.8.1 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) (default: 64)

Mode :

Enable 2 Subnet (Simulate 2 APs)

Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
<input type="checkbox"/>	DrayTek-LAN-A	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>	DrayTek-LAN-B	<input type="text" value="LAN-B"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>		<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>		<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>

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 :
 Extension Channel :

Note : Enter the configuration of APs which AP 800 want to connect.
 Remote AP should always set LAN-A MAC address to connect AP800 WDS.

Phy Mode : HTMIX

<p>1. Subnet <input type="text" value="LAN-A"/> Security:</p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p>Peer Mac Address:</p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p>3. Subnet <input type="text" value="LAN-A"/> Security:</p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p>Peer Mac Address:</p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>
<p>2. Subnet <input type="text" value="LAN-A"/> Security:</p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p>Peer Mac Address:</p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p>4. Subnet <input type="text" value="LAN-A"/> Security:</p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p>Peer Mac Address:</p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>

Packet-OVERDRIVE
 Tx Burst

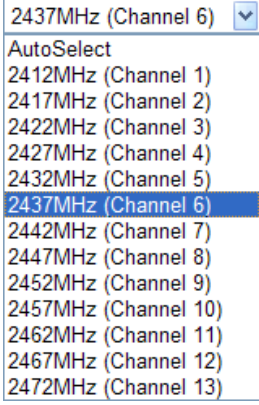
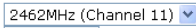


Note :
 1.Tx Burst only supports 11g mode.
 2.The same technology must also be supported in clients to boost WLAN performance.

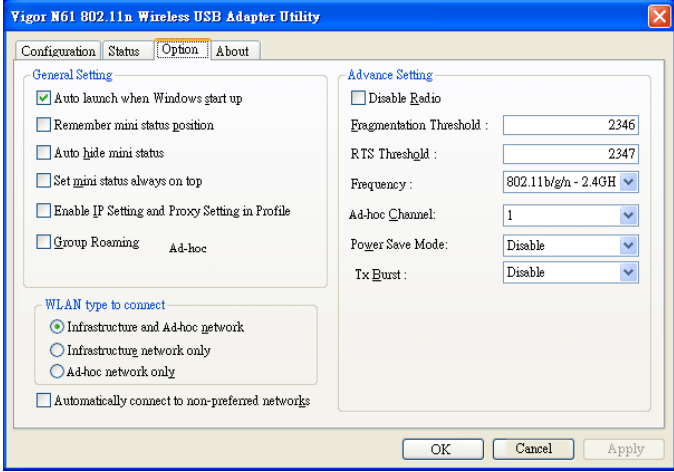
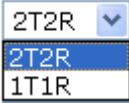
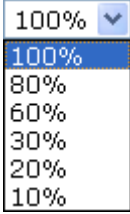
Antenna :
 Tx Power :
 Channel Width : Auto 20/40 MHZ 20 MHZ

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

	
Extension Channel	<p>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.</p>
Rate	<p>If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.</p> <p>SSID4: <small>the Wireless client will also change based on this MAC address. Reserved for Universal Repeater mode so it's not listed.</small></p> <p>Channel : </p> <p>Rate : </p> <p>Packet-OVERDRIVE </p> <p><input checked="" type="checkbox"/> Tx Burst</p> <p>Note :</p>
Phy Mode	<p>Data will be transmitted via HTMIX communication channel.</p> <p>Each access point should be setup to the same Phy mode for connecting with each other.</p>
Subnet	<p>Choose LAN-A or LAN-B for each SSID.</p>
Security	<p>Select WEP, TKIP or AES as the encryption algorithm.</p>
Peer Mac Address	<p>Four peer MAC addresses are allowed to be entered in this page at one time.</p>
Packet-OVERDRIVE	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>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).</p>

	
<p>Antenna</p>	<p>VigorAP 800 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.</p> 
<p>Tx Power</p>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p> 
<p>Channel Width</p>	<p>20 MHZ- the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p>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.</p>

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

3.8.2 Security

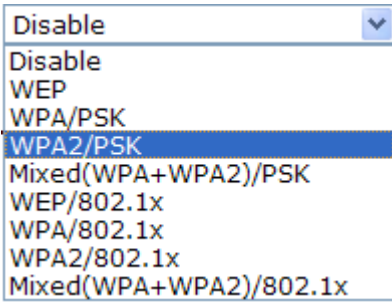
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

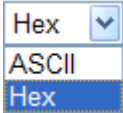
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID		Vigor2860APM-24G	
Mode		WPA2/PSK	
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms		<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase		<input type="password" value="*****"/>	
Key Renewal Interval		<input type="text" value="0"/> seconds	
WEP			
<input checked="" type="radio"/> Key 1 :		<input type="text"/>	<input type="button" value="Hex"/>
<input type="radio"/> Key 2 :		<input type="text"/>	<input type="button" value="Hex"/>
<input type="radio"/> Key 3 :		<input type="text"/>	<input type="button" value="Hex"/>
<input type="radio"/> Key 4 :		<input type="text"/>	<input type="button" value="Hex"/>
802.1x WEP		<input type="radio"/> Disable <input type="radio"/> Enable	

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>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.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access</p>

	<p>authentication for network management.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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.</p> 
802.1x WEP	<p>Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p>Enable - Enable the WEP Encryption.</p> <p>Such feature is available for WEP/802.1x mode.</p>

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

Radius Server

<input type="checkbox"/> Use internal RADIUS Server	
IP Address	<input type="text" value="0"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text" value="DrayTek"/>
Session Timeout	<input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	<p>There is a RADIUS server built in VigorAP 800 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.</p> <p>Besides, if you want to use the external RADIUS server for authentication, do not check this box.</p> <p>Please refer to the section, 3.11 RADIUS Server to configure settings for internal server of VigorAP 800.</p>
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.)

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).

Wireless LAN (2.4GHz) >> Access Control

SSID 1	SSID 2	SSID 3	SSID 4						
SSID: DrayTek-LAN-A									
Policy: <input type="button" value="Disable"/>									
MAC Address Filter									
Index		MAC Address							
<table border="1" style="width: 100%; height: 100px;"> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table>									
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>									
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/> Limit:256 entries									
<input type="button" value="OK"/> <input type="button" value="Cancel"/>									
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案							
		<input type="button" value="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 800. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <input type="button" value="Activate MAC address filter"/> <input type="button" value="Disable"/> <input type="button" value="Activate MAC address filter"/> <input type="button" value="Blocked MAC address filter"/> </div>
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.

OK	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.
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 (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	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="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 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of VigorAP 800. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
Configure via Push Button	Click Start PBC to make a WPS connection within 2 minutes.
Configure via Client PinCode	When using PinCode method, it is required to enter PIN Code (Personal Identification Number Code, 8-digit numbers) into Registrar.

3.8.5 AP Discovery

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

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

Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Show List in order of RSSI values from 100% to 0%

Select	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="radio"/>	DrayTek	00:1d:aa:c6:4b:98	15%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	RD2_Kyle_2...	00:1d:aa:c3:3f:00	0%	6	NONE	
<input type="radio"/>	staffs_6F	00:1d:aa:9c:f3:c0	0%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK

Scan

See [Channel Statistics](#)

Note: 1. During the scanning process (about 5 seconds), no station is allowed to connect with the router.
2. If you select/deselect 'Show List in order of RSSI values from 100% to 0%', you should click Scan Button again to make this function run OK.

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

Add to [WDS Settings](#):

Each item is explained as follows:

Item	Description
Show List....	Check the box to display the RSSI value with the order from 100% to 0.
SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 800.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.

Add	Click Repeater for the specified AP. Next, click Add . Later, the MAC address of the AP will be added and be shown on WDS settings page.
------------	--

3.8.6 WDS AP Status

VigorAP 800 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 >> 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

3.8.7 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 >> 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	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>

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.

3.8.8 Station List

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

Wireless LAN >> Station List

Station List

MAC Address	SSID	Auth	Encrypt	Tx Rate(Kbps)	Rx Rate(Kbps)
<input type="button" value="Refresh"/>					

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	Display the data transmission rate.
RX Rate	Display the data received rate.
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 .

3.8.9 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	<input checked="" type="checkbox"/>		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment	<input checked="" type="checkbox"/>		
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.

OK Cancel

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.

3.9 Wireless LAN (2.4GHz) 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.



3.9.1 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) (default: 64)

Mode :

Enable 2 Subnet (Simulate 2 APs)

Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
<input type="checkbox"/>	DrayTek-LAN-A	LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>	DrayTek-LAN-B	LAN-B	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>

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 :

Extension Channel :

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.

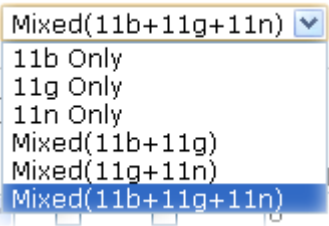
Antenna :

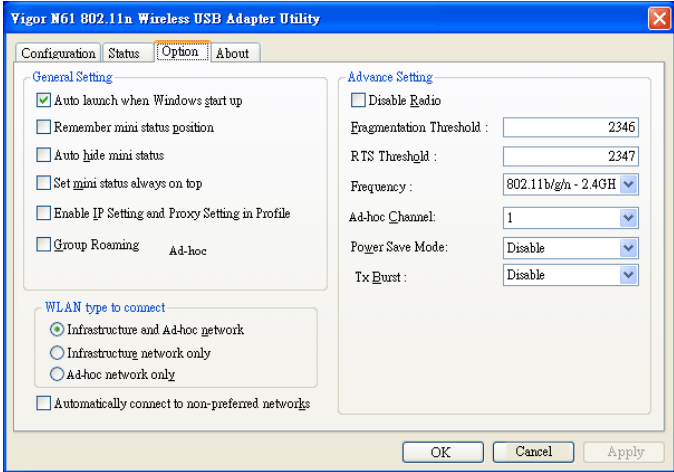
Tx Power :


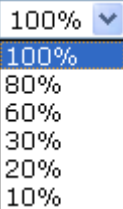
Channel Width : Auto 20/40 MHZ 20 MHZ

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 800 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.

	
<p>Enable 2 Subnet (Simulate 2 APs)</p>	<p>Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.</p> <p>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.</p>
<p>Hide SSID</p>	<p>Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 800 while site surveying. The system allows you to set three sets of SSID for different usage.</p>
<p>SSID</p>	<p>Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.</p>
<p>Subnet</p>	<p>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.</p>
<p>Isolate LAN</p>	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.</p>
<p>Isolate Member</p>	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p>
<p>VLAN ID</p>	<p>Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.</p> <p>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.</p>
<p>Mac Clone</p>	<p>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.</p>
<p>Channel</p>	<p>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.</p>

	<div style="border: 1px solid black; padding: 5px;"> 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) </div>
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	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>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).</p>  <p>The screenshot shows the 'Option' tab of the utility window. Under 'Advance Setting', the 'Tx Burst' checkbox is checked. Other settings include 'Fragmentation Threshold' at 2346, 'RTS Threshold' at 2347, 'Frequency' set to '802.11b/g/n - 2.4GH', 'Ad-hoc Channel' set to '1', 'Power Save Mode' set to 'Disable', and 'Disable Radio' unchecked. Under 'General Setting', 'Auto launch when Windows start up' is checked. Under 'WLAN type to connect', 'Infrastructure and Ad-hoc network' is selected.</p>

Antenna	<p>VigorAP 800 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.</p> 
Tx Power	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p> 
Channel Width	<p>20 MHZ- the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p>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.</p>

3.9.2 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.

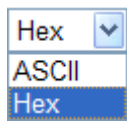
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) >> Security Settings

The screenshot shows the 'Security Settings' page for SSID 1. The SSID is 'Vigor2860APM-24G' and the Mode is 'WPA2/PSK'. Under the 'WPA' section, 'TKIP/AES' is selected as the WPA Algorithm. The 'Pass Phrase' field contains several dots. The 'Key Renewal Interval' is set to 0 seconds. Under the 'WEP' section, there are four key fields, each with a 'Hex' dropdown menu. The '802.1x WEP' section has 'Disable' selected. At the bottom, there are 'OK' and 'Cancel' buttons.

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p> <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>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.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access</p>

	<p>authentication for network management.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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.</p> 
802.1x WEP	<p>Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p>Enable - Enable the WEP Encryption.</p> <p>Such feature is available for WEP/802.1x mode.</p>

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

Radius Server

<input checked="" type="checkbox"/> Use internal RADIUS Server	
IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 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, 3.11 RADIUS Server to configure settings for internal server of VigorAP 800.
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.

3.9.3 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
SSID: DrayTek-LAN-A Policy: <input type="text" value="Disable"/>			
MAC Address Filter			
Index		MAC Address	
<div style="border: 1px solid black; height: 100px; width: 100%;"></div>			
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>			
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/> Limit:256 entries			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="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 800. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <input type="text" value="Activate MAC address filter"/> <input type="text" value="Disable"/> <input type="text" value="Activate MAC address filter"/> <input type="text" value="Blocked MAC address filter"/> </div>
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.
----------------	--

3.9.4 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	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="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 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 800. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 800 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on VigorAP 800 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

3.9.5 AP Discovery

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

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

Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Show List in order of RSSI values from 100% to 0%

Select SSID	BSSID	RSSI	Channel	Encryption	Authentication
-------------	-------	------	---------	------------	----------------

Scan

See [Channel Statistics](#)

Note: 1. During the scanning process (about 5 seconds), no station is allowed to connect with the router.
2. If you select/deselect 'Show List in order of RSSI values from 100% to 0%', you should click Scan Button again to make this function run OK.

AP's MAC Address : : : : :

AP's SSID

Select as **Universal Repeater**:

Available settings are explained as follows:

Item	Description
Show List....	Check the box to display the RSSI value with the order from 100% to 0.
SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 800.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	It displays the MAC address of the AP you selected.
AP's SSID	It displays the SSID of the AP you selected.
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.

3.9.6 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	<input type="text"/>
MAC Address (Optional)	<input type="text"/>
Channel	2462MHz (Channel 11) ▼
Security Mode	WPA/PSK ▼
Encryption Type	TKIP ▼
Pass Phrase	<input type="text"/>

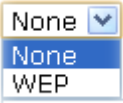
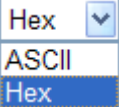
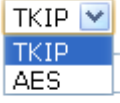
Note: If Channel is modified, the Channel setting of AP would also be changed.

Universal Repeater IP Configuration

Wan Connection Type	STATIC ▼
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>

Available settings are explained as follows:

Item	Description
SSID	Set the name of access point that VigorAP 800 wants to connect to.
MAC Address (Optional)	Type the MAC address of access point that VigorAP 800 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. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> Open ▼ Open Shared WPA/PSK WPA2/PSK </div>
Encryption Type for Open/Shared	This option is available when Open/Shared is selected as Security Mode.

	<p>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.</p>  <p>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 ','.</p> 
<p>Encryption Type for WPA/PSK and WPA2/PSK</p>	<p>This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode. Select TKIP or AES as the algorithm for WPA.</p> 
<p>Pass Phrase</p>	<p>Such option is available when WPA/PSK or WPA2/PSK is selected as Security Mode. Either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
<p>Connection Type</p>	<p>Choose DHCP or Static IP as the connection mode. DHCP – The wireless station will be assigned with an IP from Vigor router. STATIC – The wireless station shall specify a static IP for connecting to Internet via Vigor router.</p>
<p>IP Address</p>	<p>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.</p>
<p>Subnet Mask</p>	<p>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.</p>
<p>Default Gateway</p>	<p>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.</p>

Open / Shared for Security Mode

Wireless LAN (2.4GHz) >> Universal Repeater

Universal Repeater Parameters

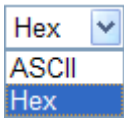
SSID	<input type="text"/>
MAC Address (Optional)	<input type="text"/>
Channel	AutoSelect <input type="button" value="v"/>
Security Mode	Open <input type="button" value="v"/>
Encryption Type	None <input type="button" value="v"/>
WEP Keys	
<input type="radio"/> Key 1 :	<input type="text"/> Hex <input type="button" value="v"/>
<input type="radio"/> Key 2 :	<input type="text"/> Hex <input type="button" value="v"/>
<input type="radio"/> Key 3 :	<input type="text"/> Hex <input type="button" value="v"/>
<input type="radio"/> Key 4 :	<input type="text"/> Hex <input type="button" value="v"/>

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

Universal Repeater IP Configuration

Connection Type	Static IP <input type="button" value="v"/>
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>

Available settings are explained as follows:

Item	Description
Encryption Type	Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP .
WEP Keys	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. 

WPA/PSK and WPA2/PSK for Security Mode

Wireless LAN (2.4GHz) >> Universal Repeater

Universal Repeater Parameters

SSID	<input type="text" value="R1"/>
MAC Address (Optional)	<input type="text"/>
Channel	2422MHz (Channel 3) ▾
Security Mode	WPA/PSK ▾
Encryption Type	TKIP ▾
Pass Phrase	<input type="password" value="••••••••"/>

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

Universal Repeater IP Configuration

Connection Type	Static IP ▾
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>

Available settings are explained as follows:

Item	Description
Encryption Type	Select TKIP or AES as the algorithm for WPA.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

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

3.9.7 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	<input type="radio"/> Enable <input checked="" type="radio"/> Disable					
WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/> ▾	<input type="text" value="63"/> ▾	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/> ▾	<input type="text" value="102"/> ▾	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/> ▾	<input type="text" value="15"/> ▾	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/> ▾	<input type="text" value="7"/> ▾	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>
WMM Parameters of Station						
	Aifsn	CWMin	CWMax	Txop	ACM	
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/> ▾	<input type="text" value="102"/> ▾	<input type="text" value="0"/>	<input type="checkbox"/>	
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/> ▾	<input type="text" value="102"/> ▾	<input type="text" value="0"/>	<input type="checkbox"/>	
AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/> ▾	<input type="text" value="15"/> ▾	<input type="text" value="94"/>	<input type="checkbox"/>	
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/> ▾	<input type="text" value="7"/> ▾	<input type="text" value="47"/>	<input type="checkbox"/>	

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.
AckPolicy	<p>“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.</p> <p>“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.</p>

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

3.9.8 Station List

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

Wireless LAN >> Station List

Station List

MAC Address	SSID	Auth	Encrypt	Tx Rate(Kbps)	Rx Rate(Kbps)

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	Display the data transmission rate.
RX Rate	Display the data received rate.
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 .

3.9.9 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 <input checked="" type="checkbox"/>			
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment <input checked="" type="checkbox"/>			
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.

OK Cancel

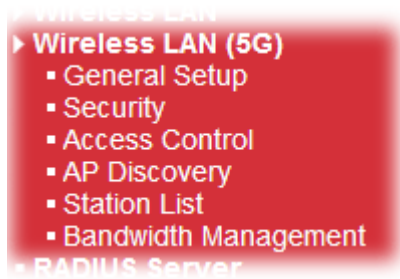
Available settings are explained as follows:

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.

3.10 Wireless LAN (5G) Settings for AP Mode

When a 5G Dongle connects to VigorAP 800, 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 800, an error message will be displayed and no function in this menu can be activated.

3.10.1 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) (default: 64)

Mode :

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="text" value="DrayTek-5G"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>

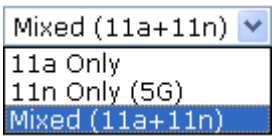
Hide SSID: Prevent SSID from being scanned.
Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

Channel :

Extension Channel :

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 800 can be connected by 11a only, 11n only (5G), Mixed (11a+11n) stations simultaneously. Simply

	<p>choose Mixed (11a+11n) mode.</p> 
Enable 2 Subnet (Simulate 2 APs)	<p>Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.</p> <p>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.</p>
Hide SSID	<p>Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 800 while site surveying. The system allows you to set three sets of SSID for different usage.</p>
SSID	<p>Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.</p>
Isolate Member	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p>
VLAN ID	<p>Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.</p> <p>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.</p>
Channel	<p>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. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.</p>
Extension Channel	<p>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.</p>

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

3.10.2 Security

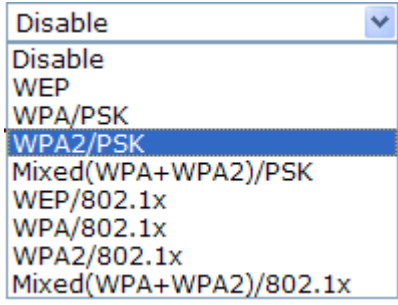
This page allows you to set security with different modes for SSID 1, 2, and 3 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

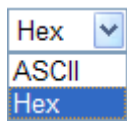
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3
SSID	Vigor2860APM-5G	
Mode	WPA2/PSK	
Set up RADIUS Server if 802.1x is enabled.		
WPA		
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase	<input type="text" value="....."/>	
Key Renewal Interval	<input type="text" value="3600"/> seconds	
WEP		
<input checked="" type="radio"/> Key 1 :	<input type="text"/>	<input type="text" value="Hex"/>
<input type="radio"/> Key 2 :	<input type="text"/>	<input type="text" value="Hex"/>
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text" value="Hex"/>
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text" value="Hex"/>
802.1x WEP	<input type="radio"/> Disable <input type="radio"/> Enable	

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>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.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 800 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access</p>

	<p>authentication for network management.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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.</p> 
802.1x WEP	<p>Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p>Enable - Enable the WEP Encryption.</p> <p>Such feature is available for WEP/802.1x mode.</p>

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

Radius Server

<input checked="" type="checkbox"/> Use internal RADIUS Server	
IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 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, 3.11 RADIUS Server to configure settings for internal server of VigorAP 800.
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.)

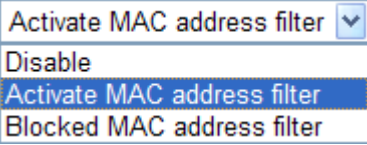
After finishing this web page configuration, please click **OK** to save the settings.

3.10.3 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 (5GHz) >> Access Control

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 800. 
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.

3.10.4 AP Discovery

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

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

Wireless LAN (5GHz) >> Access Point Discovery

Access Point List

SSID	BSSID	RSSI	Channel	Encryption	Authentication
------	-------	------	---------	------------	----------------

Note: 1. During the scanning process (about 5 seconds), no station is allowed to connect with the router.

Each item is explained as follows:

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

3.10.5 Station List

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

[Wireless LAN \(5G\) >> Station List](#)

Station List

MAC Address	SSID	Auth	Encrypt

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.
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 .

3.10.6 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 DrayTek-5G		
Per Station Bandwidth Limit		
Enable	<input checked="" type="checkbox"/>	
Upload Limit	User defined <input type="text" value="K"/> bps (Default unit : K)	
Download Limit	User defined <input type="text" value="K"/> bps (Default unit : K)	
Auto Adjustment	<input checked="" type="checkbox"/>	
Total Upload Bandwidth	User defined <input type="text" value="K"/> bps (Default unit : K)	
Total Download Bandwidth	User defined <input type="text" value="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.

3.11 RADIUS Server

VigorAP 800 offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 800. 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
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
NO.	Username	Select	
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>		

Authentication Client (up to 16 clients)

Client IP	Secret Key	Confirm Secret Key	Configure
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
NO.	Client IP	Select	
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>		

Backup Radius Cfg : <input type="button" value="Backup"/>	Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>
--	---

Available settings are explained as follows:

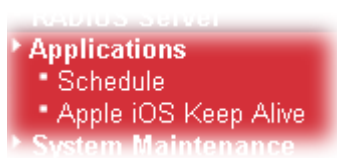
Item	Description
Enable RADIUS Server	Check it to enable the internal RADIUS server.
Users Profile	<p>Username – Type a new name for the user profile.</p> <p>Password – Type a new password for such new user profile.</p> <p>Confirm Password – Retype the password to confirm it.</p> <p>Add – Make a new user profile with the name and password specified on the left boxes.</p> <p>Cancel – Clear current settings for user profile.</p> <p>Delete Selected – Delete the selected user profile (s).</p> <p>Delete All – Delete all of the user profiles.</p>
Authentication Client	<p>This internal RADIUS server of VigorAP 800 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 800 as its external RADIUS server.</p> <p>Client IP – Type the IP address for the user to be authenticated by VigorAP 800 when the user tries to use VigorAP 800 as the external RADIUS server.</p> <p>Secret Key – Type the password for the user to be authenticated by VigorAP 800 while the user tries to use VigorAP 800 as the</p>

	<p>external RADIUS server.</p> <p>Confirm Secrete Key – Type the password again for confirmation.</p> <p>Add – Make a new client with IP and secrete key specified on the left boxes.</p> <p>Cancel – Clear current settings for the client.</p> <p>Delete Selected – Delete the selected client(s).</p> <p>Delete All – Delete all of the clients.</p>
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.

3.12 Applications

Below shows the menu items for Applications.



3.12.1 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

OK

Schedule Configuration

Index.	Setting	Status
--------	---------	--------

Add

Delete

Available settings are explained as follows:

Item	Description
Schedule	Enable Schedule - Check it to enable the function of schedule

	configuration.
Schedule Configuration	<p>Index – Display the sort number of the schedule profile.</p> <p>Setting – Display the summary of the schedule profile.</p> <p>Status – Display if the profile is enabled (V) or not (X).</p> <p>Add – Such button is available when Enable Schedule is checked. It allows to add a new schedule profile.</p>

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

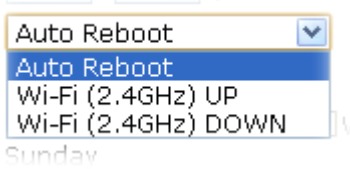
1. Check the box of **Enable Schedule**.
2. Click the **Add** button to open the following web page.

Applications >> Schedule

Add Schedule

Enable
 Start Date: 2000 - 1 - 1 (Year - Month - Day)
 Start time: 0 : 0 (Hour : Minute)
 Action: Auto Reboot
 Acts: Once
 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. 
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.

- 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

OK

Schedule Configuration

Index.	Setting	Status
1 <input type="checkbox"/>	2000 Jan. 1, 0:0-0:0 Once	V

Add

Delete

3.12.2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 800 will send the UDP packets with 5353 port to the specific IP every five seconds.

Applications >> Apple iOS Keep Alive

Enable Apple iOS Keep Alive

Apple iOS Keep Alive:

Apple iOS Keep Alive can keep Wifi connection of iOS device by sending UDP port 5353 packets every 5 seconds.

Index	Apple iOS Keep Alive IP Address	Index	Apple iOS Keep Alive IP Address
1		2	
3		4	
5		6	

OK

Cancel

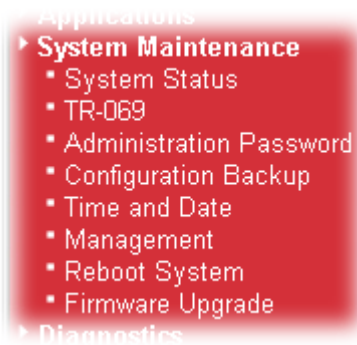
Available settings are explained as follows:

Item	Description
Enable Apple iOS Keep Alive	Check to enable the function.
Index	Display the setting link. Click the index link to open the configuration page for setting the IP address.
Apple iOS Keep Alive IP Address	Display the IP address.

3.13 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, Time and Date, Management, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.13.1 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 800
Device Name	: VigorAP800
Firmware Version	: 1.1.6
Build Date/Time	: r6306 Wed Aug 17 17:01:37 CST 2016
System Uptime	: 0d 00:15:53
Operation Mode	: AP

System	
Memory Total	: 30252 kB
Memory Left	: 12884 kB

LAN-A	
MAC Address	: 00:50:7F:5E:AB:68
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:5E:AB:68
SSID	: DrayTek-LAN-A
Channel	: 11

LAN-B	
MAC Address	: 00:50:7F:5E:AB:68
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:5E:AB:68
SSID	: DrayTek-5G
Channel	: 36

WARNING: Your AP is still set to default password. You should change it via System Maintenance menu.

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.
<i>System</i>	
Memory total	Display the total memory of your system.

Memory left	Display the remaining memory of your system.
<i>LAN</i>	
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.
<i>Wireless/Wireless LAN</i>	
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.

3.13.2 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	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>

CPE Settings

Enable	<input type="checkbox"/>
On	LAN-A <input type="button" value="v"/>
URL	<input type="text" value="http://192.168.1.2:8069/cwm/CRN.html"/>
Port	<input type="text" value="8069"/>
Username	<input type="text" value="vigor"/>
Password	<input type="password" value="....."/>
DNS Server IP Address	
Primary IP Address	<input type="text"/>
Secondary IP Address	<input type="text"/>

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

Periodic Inform Settings

Enable	<input checked="" type="checkbox"/>
Interval Time	<input type="text" value="900"/> second(s)

STUN Settings

<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Server Address	<input type="text"/>
Server Port	<input type="text" value="3478"/>
Minimum Keep Alive Period	<input type="text" value="60"/> Second(s)
Maximum Keep Alive Period	<input type="text" value="-1"/> second(s)

Available settings are explained as follows:

Item	Description
ACS Settings	<p>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.</p>
CPE Settings	<p>Such information is useful for Auto Configuration Server (ACS).</p> <p>Enable – Check the box to allow the CPE Client to connect with Auto Configuration Server.</p> <p>On – Choose the interface (LAN-A or LAN-B) for VigorAP 900 connecting to ACS server.</p> <p>Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</p> <p>DNS Server IP Address – Such field is to specify the IP address if a URL is configured with a domain name.</p> <ul style="list-style-type: none"> ● 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	<p>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.</p> <p>Interval Time – Type the value for the interval time setting. The unit is “second”.</p>
STUN Settings	<p>The default is Disable. If you click Enable, please type the relational settings listed below:</p> <p>Server Address – Type the IP address of the STUN server.</p> <p>Server Port – Type the port number of the STUN server.</p> <p>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”.</p> <p>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.</p>

3.13.3 Administrator Password

This page allows you to set new password.

[System Maintenance >> Administration Password](#)

Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password" value="••••"/>
Confirm Password	<input type="password"/>
Password Strength:	<input type="button" value="Weak"/> <input type="button" value="Medium"/> <input type="button" value="Strong"/>
Strong password requirements: 1. Have at least one upper-case letter and one lower-case letter. 2. Including non-alphanumeric characters is a plus.	

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 field.
Confirm Password	Type the new password again for confirmation.
Password Strength	The system will display the password strength (represented with the word of weak, medium or strong) of the password specified above.

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

3.13.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

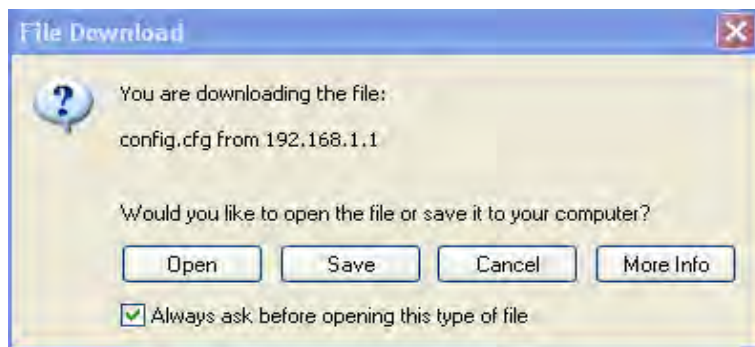
1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup

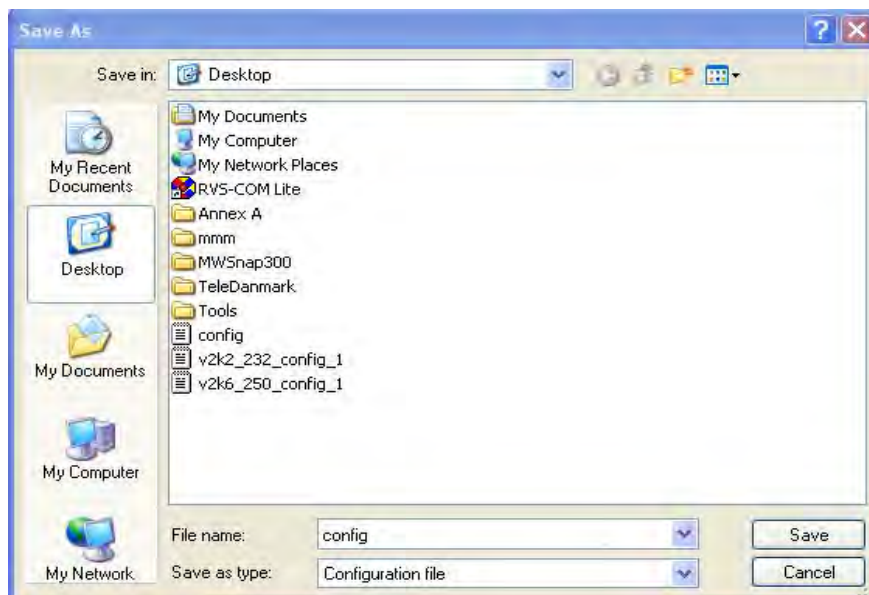
Configuration Backup / Restoration

Restoration
Select a configuration file. <input type="button" value="選擇檔案"/> 未選擇檔案 Click Restore to upload the file. <input type="button" value="Restore"/>
Backup
Click Backup to download current running configurations as a file. <input type="button" value="Backup"/>

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



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



- 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

- 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.

未選擇檔案

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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

3.13.5 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	2016 Dec 8 Thu 13:36:27	<input type="button" value="Inquire Time"/>
---------------------	-------------------------	---

Time Setting

Use Browser Time

Use NTP Client

Time Zone

NTP Server

Daylight Saving

NTP synchronization

Available parameters are explained as follows:

Item	Description
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.

Item	Description
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.

3.13.6 Management

This page allows you to manage the port settings for HTTP and HTTPS.

System Maintenance >> Management

Device Name

Name	VigorAP800
------	------------

Management Port Setup

HTTP port	80
HTTPS port	443

Available parameters are explained as follows:

Item	Description
Device Name	Name - The default setting is VigorAP800. Change the name if required.
Management Port Setup	HTTP port/HTTPS port -Specify user-defined port numbers for the HTTP and HTTPS servers.

3.13.7 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 AP ?

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.

3.13.8 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](ftp://ftp.draytek.com).

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

System Maintenance >> Firmware Upgrade

Firmware Update

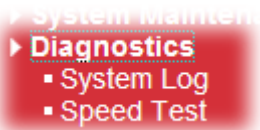
Select a firmware file.

Click Upgrade to upload the file.

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

3.14 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your VigorAP 800.



3.14.1 System Log

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

[Diagnostics >> System Log](#)

System Log Information | [Clear](#) | [Refresh](#) | Line wrap |

```
0d 02:11:12 syslogd started: BusyBox v1.12.1
0d 02:11:12 kernel: klogd started: BusyBox v1.12.1 (2011-02-25 10:27:36 CST)
0d 02:11:12 kernel: flag: 0x0
0d 02:11:12 kernel: ravid 0: 0x0
0d 02:11:12 kernel: ravid 1: 0x0
0d 02:11:12 kernel: ravid 2: 0x0
0d 02:11:12 kernel: ravid 3: 0x0
0d 02:11:12 kernel: ravid 4: 0x0
0d 02:11:12 kernel: ravid 5: 0x0
0d 02:11:12 kernel: ravid 6: 0x0
0d 02:24:19 kernel: LOG#1 40:d3:2d:a0:f7:d3 successfully associated
0d 02:24:25 kernel: LOG#2 40:d3:2d:a0:f7:d3 has disassociated
0d 02:25:25 kernel: RT305x_ESW: Link Status Changed
0d 02:28:24 kernel: LOG#3 00:1d:4f:d5:c1:39 successfully associated
0d 02:30:08 kernel: LOG#4 78:1d:ba:15:2b:13 successfully associated
0d 02:30:09 kernel: Rcv Wcid(2) AddBAREq
```

3.14.2 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 VigorAP 800.

[Diagnostics >> Speed Test](#)

Speed Test

Welcome to VigorAP800 Speed Test.

This test allows you to find out the best place for VigorAP800. 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.

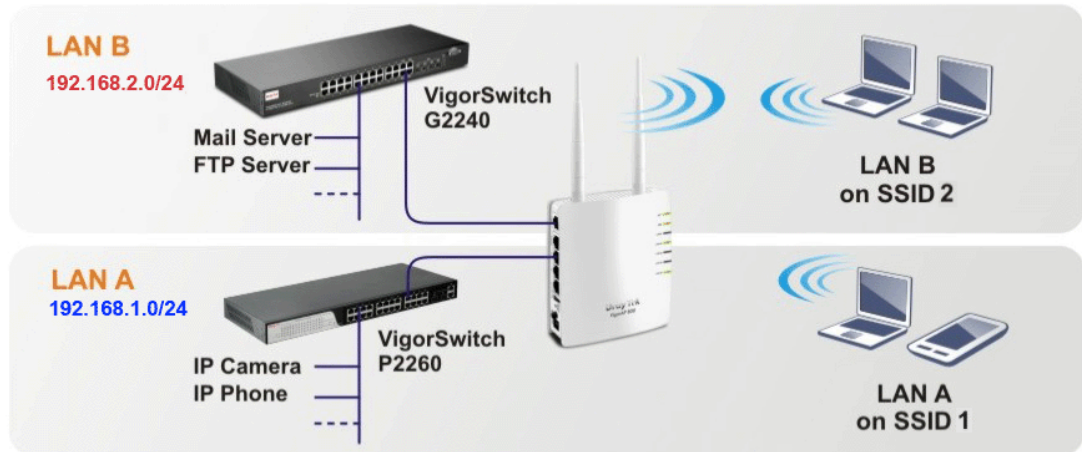
Note : Speed test could not work with chrome browser.

4

Application and Examples

4.1 How to set different segments for different SSIDs in VigorAP 800

VigorAP 800 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.



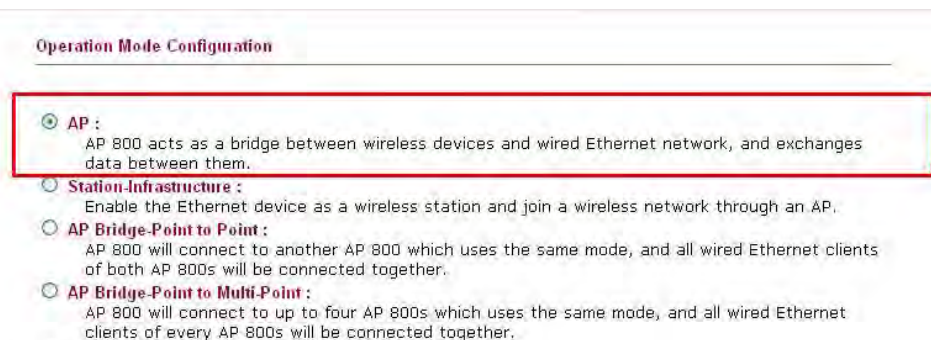
In the above figure, VigorAP 800 is used to control the wireless network connection. It can separate the wireless traffic between accessing internal server and the usage of video. Wireless station connecting to VigorAP 800 with SSID 1 can get the IP address with the network segment of 192.168.1.0/24 (LAN-A); wireless station connecting to VigorAP800 with SSID 2 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 video traffic

Below shows you how to configure the web page for VigorAP 800:

1. In the page of **Operation Mode**, click **AP mode**.



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

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN
 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
<input type="checkbox"/>	SSID 1	LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>	SSID 2	LAN-B	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>

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)

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.

WMM Capable Enable Disable

- Open **Wireless LAN >> Security Settings**. Set the encryption method and set the password for SSID 1 and SSID 2 respectively.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1 | **SSID 2** | SSID 3 | SSID 4

SSID: Vigor2860APM-24G
 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: 0 seconds

WEP
 Key 1 : Hex
 Key 2 : Hex
 Key 3 : Hex
 Key 4 : Hex

802.1x WEP Disable Enable

OK **Cancel**

- 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	
IP Address	<input type="text" value="192.168.1.2"/>	<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
Subnet Mask	<input type="text" value="255.255.255.0"/>	Start IP Address	<input type="text" value="192.168.1.10"/>
Default Gateway	<input type="text"/>	End IP Address	<input type="text" value="192.168.1.100"/>
		Subnet Mask	<input type="text" value="255.255.255.0"/>
		Default Gateway	<input type="text" value="192.168.1.2"/>
		Lease Time	<input type="text" value="86400"/>
		Primary DNS Server	<input type="text" value="168.95.1.1"/>
		Secondary DNS Server	<input type="text" value="168.95.192.1"/>
LAN-B IP Network Configuration		DHCP Server Configuration	
IP Address	<input type="text" value="192.168.2.2"/>	<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
Subnet Mask	<input type="text" value="255.255.255.0"/>	Start IP Address	<input type="text" value="192.168.2.10"/>
		End IP Address	<input type="text" value="192.168.2.100"/>
		Subnet Mask	<input type="text" value="255.255.255.0"/>
		Default Gateway	<input type="text" value="192.168.2.2"/>
		Lease Time	<input type="text" value="86400"/>
		Primary DNS Server	<input type="text" value="168.95.1.1"/>
		Secondary DNS Server	<input type="text" value="168.95.192.1"/>

- After finishing the above settings, the wireless equipment connecting to VigorAP 800 with SSID 1 can get the IP address assigned by LAN-A 192.168.1.0/24 for accessing the internal server. The wireless equipment connecting to VigorAP 800 with SSID 2 can get the IP address assigned by LAN-B 192.168.2.0/24 for using the video/audio uploading and downloading services.

This page is left blank.

5

Trouble Shooting

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

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

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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

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

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

For Windows

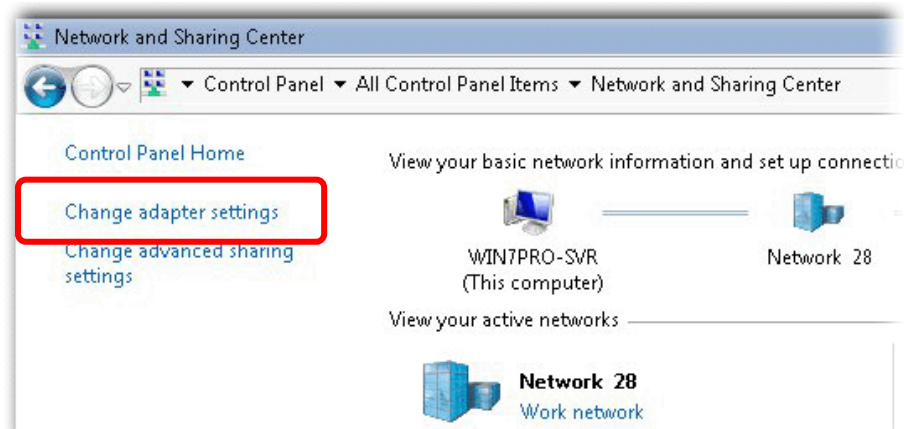


The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

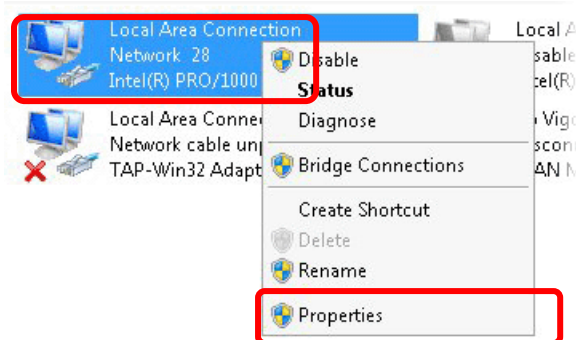
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



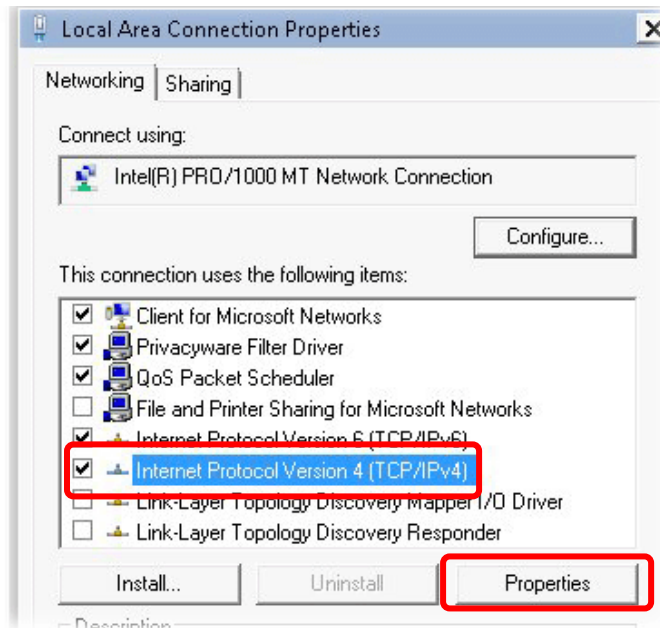
2. In the following window, click **Change adapter settings**.



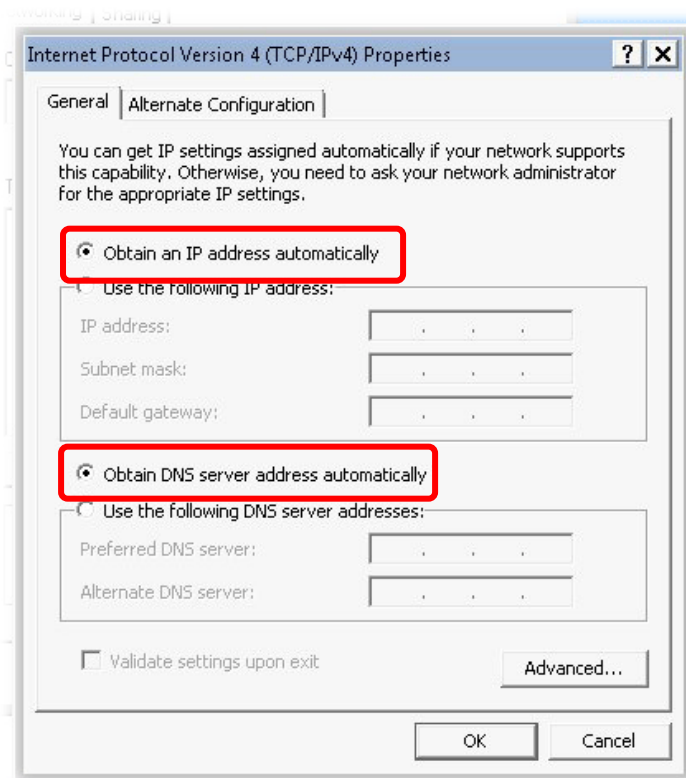
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

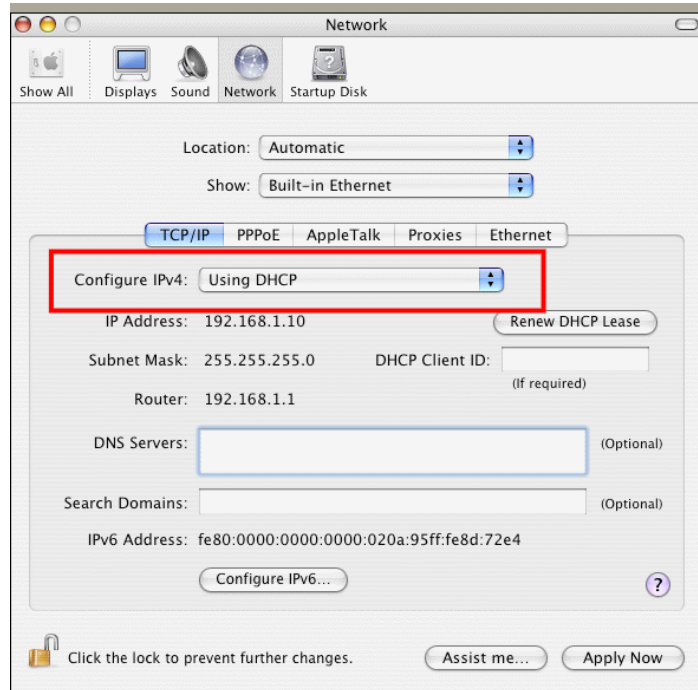


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



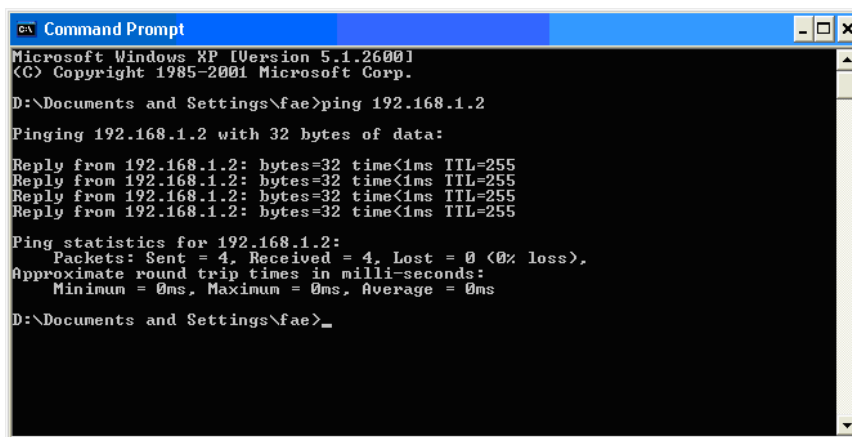
5.3 Pinging the Modem from Your Computer

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/7). The DOS command dialog will appear.



```
ex Command Prompt
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.

```
Terminal - bash - 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
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 lose 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

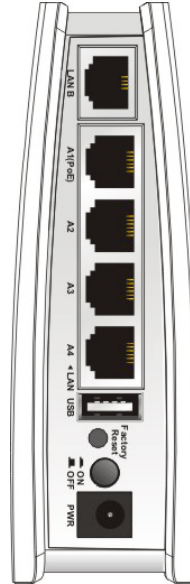
Do You want to reboot your AP ?

- Using current configuration
- Using factory default configuration

OK

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 DrayTek

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.