

# DrayTek

## VigorAP 910C

802.11ac Ceiling-mount Access Point



*Your reliable networking solutions partner*

# User's Guide

**V2.6**

# **VigorAP 910C**

## **802.11ac Ceiling-mount Access Point**

### **User's Guide**

**Version: 2.6**

**Firmware Version: V1.3.2**

**(For future update, please visit DrayTek web site)**

**Date: May 14, 2020**

## Intellectual Property Rights (IPR) Information

<b>Copyrights</b>	© 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.
<b>Trademarks</b>	The following trademarks are used in this document: <ul style="list-style-type: none"><li>● Microsoft is a registered trademark of Microsoft Corp.</li><li>● Windows, Windows 7,8,10 and Explorer are trademarks of Microsoft Corp.</li><li>● Apple and Mac OS are registered trademarks of Apple Inc.</li><li>● Other products may be trademarks or registered trademarks of their respective manufacturers.</li></ul>

## Safety Instructions and Approval

<b>Safety Instructions</b>	<ul style="list-style-type: none"><li>● Read the user guide thoroughly before you set up the device.</li><li>● The access point 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.</li><li>● Do not place the access point in a damp or humid place, e.g. a bathroom.</li><li>● The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.</li><li>● Do not expose the access point to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.</li><li>● Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.</li><li>● Keep the package out of reach of children.</li><li>● When you want to dispose of the access point, please follow local regulations on conservation of the environment.</li></ul>
<b>Warranty</b>	We warrant to the original end user (purchaser) that the access point 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.
<b>Be a Registered Owner</b>	Web registration is preferred. You can register your Vigor AP via <a href="http://www.draytek.com">http://www.draytek.com</a> .
<b>Firmware &amp; Tools Updates</b>	Due to the continuous evolution of DrayTek technology, all access points will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.  <a href="http://www.draytek.com">http://www.draytek.com</a>

## 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](mailto:support@draytek.com) for further information.

# Table of Contents

## 1

<b>Introduction .....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 LED Indicators and Connectors .....	3
1.3 Hardware Installation .....	4
1.3.1 Ceiling-mount Installation (Wooden Ceiling) .....	4
1.3.2 Ceiling-mount Installation (Plasterboard Ceiling) .....	5
1.3.3 Suspended Ceiling (Lightweight Steel Frame) Installation .....	6
1.3.4 Wall Mounting Installation.....	8
1.4 Notifications for Hardware Connection .....	9
1.5 Connect to a Vigor Router using AP Management .....	10
1.6 Connect to a Vigor Router without AP Management .....	11
1.7 Connect without a DrayTek Router/LAN .....	12
1.8 Connecting to PC Directly .....	13

## 2

<b>Network Configuration.....</b>	<b>15</b>
2.1 Windows 10 IP Address Setup.....	15
2.2 Accessing to Web User Interface .....	18
2.3 Changing Password .....	19
2.4 Quick Start Wizard .....	20
2.4.1 Configuring Wireless Settings – General.....	20
2.4.2 Configuring 2.4GHz Wireless Settings Based on the Operation Mode.....	21
2.4.3 Configuring 5GHz Wireless Settings Based on the Operation Mode.....	28
2.4.4 Finishing the Wireless Settings Wizard .....	33
2.5 Online Status.....	34

## 3

<b>Advanced Configuration .....</b>	<b>35</b>
3.1 Operation Mode .....	36
3.2 LAN .....	37
3.2.1 General Setup.....	37
3.2.2 Web Portal .....	41
3.3 Central AP Management .....	44
3.3.1 General Setup.....	44
3.3.2 APM Log .....	45
3.3.3 Overload Management .....	45
3.3.4 Status of Settings.....	47

3.4 General Concepts for Wireless LAN (2.4GHz/5GHz) .....	48
3.5 Wireless LAN (2.4GHz) Settings for AP Mode.....	51
3.5.1 General Setup.....	51
3.5.2 Security .....	53
3.5.3 Access Control.....	56
3.5.4 WPS.....	57
3.5.5 Advanced Setting.....	58
3.5.6 AP Discovery .....	60
3.5.7 Bandwidth Management.....	62
3.5.8 Airtime Fairness.....	63
3.5.9 Station Control .....	65
3.5.10 Roaming .....	66
3.5.11 Band Steering.....	68
3.5.12 Station List.....	73
3.6 Wireless LAN (2.4GHz) Settings for Station-Infrastructure Mode.....	75
3.6.1 General Setup.....	75
3.6.2 Site Survey .....	80
3.6.3 Statistics.....	81
3.6.4 WPS (Wi-Fi Protected Setup).....	81
3.7 Wireless LAN (2.4GHz) Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Mode .....	83
3.7.1 General Setup.....	83
3.7.2 Advanced Setting.....	86
3.7.3 AP Discovery .....	89
3.7.4 WDS AP Status .....	90
3.8 Wireless LAN (2.4GHz) Settings for AP Bridge-WDS Mode.....	91
3.8.1 General Setup.....	91
3.8.2 Security .....	93
3.8.3 Access Control.....	97
3.8.4 WPS.....	98
3.8.5 Advanced Setting.....	100
3.8.6 AP Discovery .....	103
3.8.7 WDS AP Status .....	104
3.8.8 Bandwidth Management.....	105
3.8.9 Airtime Fairness.....	106
3.8.10 Station Control.....	108
3.8.11 Roaming .....	109
3.8.12 Band Steering.....	111
3.8.13 Station List.....	116
3.9 Wireless LAN (2.4GHz) Settings for Universal Repeater Mode .....	118
3.9.1 General Setup.....	118
3.9.2 Security .....	120
3.9.3 Access Control.....	123
3.9.4 WPS.....	124
3.9.5 Advanced Setting.....	125
3.9.6 AP Discovery .....	128
3.9.7 Universal Repeater .....	129
3.9.8 Bandwidth Management.....	132
3.9.9 Airtime Fairness.....	133
3.9.10 Station Control .....	135
3.9.11 Roaming .....	136
3.9.12 Band Steering .....	138
3.9.13 Station List.....	143
3.10 Wireless LAN (5GHz) Settings for AP Mode.....	145

3.10.1	General Setup.....	145
3.10.2	Security.....	147
3.10.3	Access Control.....	150
3.10.4	WPS.....	151
3.10.5	Advanced Setting.....	152
3.10.6	AP Discovery.....	154
3.10.7	Bandwidth Management.....	156
3.10.8	Airtime Fairness.....	157
3.10.9	Station Control.....	159
3.10.10	Roaming.....	160
3.10.11	Station List.....	162
3.11	Wireless LAN (5GHz) Settings for AP Bridge-WDS Mode.....	163
3.11.1	General Setup.....	164
3.11.2	Security.....	166
3.11.3	Access Control.....	169
3.11.4	WPS.....	170
3.11.5	Advanced Setting.....	171
3.11.6	AP Discovery.....	173
3.11.7	WDS AP Status.....	174
3.11.8	Bandwidth Management.....	175
3.11.10	Airtime Fairness.....	176
3.11.11	Station Control.....	178
3.11.12	Roaming.....	179
3.11.13	Station List.....	181
3.12	Wireless LAN (5GHz) Settings for Universal Repeater Mode.....	183
3.12.1	General Setup.....	183
3.12.2	Security.....	185
3.12.3	Access Control.....	188
3.12.4	WPS.....	189
3.12.5	Advanced Setting.....	191
3.12.6	AP Discovery.....	193
3.12.7	Universal Repeater.....	195
3.12.8	Bandwidth Management.....	197
3.12.9	Airtime Fairness.....	199
3.12.10	Station Control.....	201
3.12.11	Roaming.....	202
3.12.12	Station List.....	204
3.13	RADIUS Setting.....	205
3.13.1	RADIUS Server.....	205
3.13.2	Certificate Management.....	206
3.14	Applications.....	209
3.14.1	Schedule.....	209
3.14.2	Apple iOS Keep Alive.....	211
3.14.3	Wi-Fi Auto On/Off.....	212
3.15	Mobile Device Management.....	213
3.15.1	Detection.....	213
3.15.2	Policies.....	214
3.15.3	Statistics.....	215
3.16	System Maintenance.....	216
3.16.1	System Status.....	216
3.16.2	TR-069.....	218
3.16.3	Administration Password.....	220
3.16.4	Configuration Backup.....	221
3.16.5	Syslog/Mail Alert.....	223

3.16.6 Time and Date .....	224
3.16.7 SNMP.....	225
3.16.8 Management.....	226
3.16.9 Reboot System .....	227
3.16.10 Firmware Upgrade .....	227
3.17 Diagnostics.....	228
3.17.1 System Log.....	228
3.17.2 Speed Test .....	228
3.17.3 Traffic Graph.....	229
3.17.4 Where am I .....	229
3.17.5 Data Flow Monitor.....	230
3.17.6 WLAN (2.4GHz) Statistics .....	231
3.17.7 WLAN(5GHz) Statistics .....	231
3.17.8 Station Statistics .....	232
3.17.9 Interference Monitor.....	234
3.18 Support Area .....	236

# 4

## **Trouble Shooting.....237**

4.1 Checking If the Hardware Status Is OK or Not.....	237
4.2 Checking If the Network Connection Settings on Your Computer Is OK or Not .....	238
4.3 Pinging the VigorAP from Your Computer.....	241
4.4 Backing to Factory Default Setting If Necessary .....	242
4.5 Contacting DrayTek.....	243

## **Index .....245**



# 1

# Introduction

## 1.1 Introduction

Thank you for purchasing this VigorAP 910C! With this high cost-efficiency VigorAP 910C, computers and wireless devices which are compatible with 802.11n can connect to existing wired Ethernet network via this VigorAP 910C, at the speed of 300Mbps.



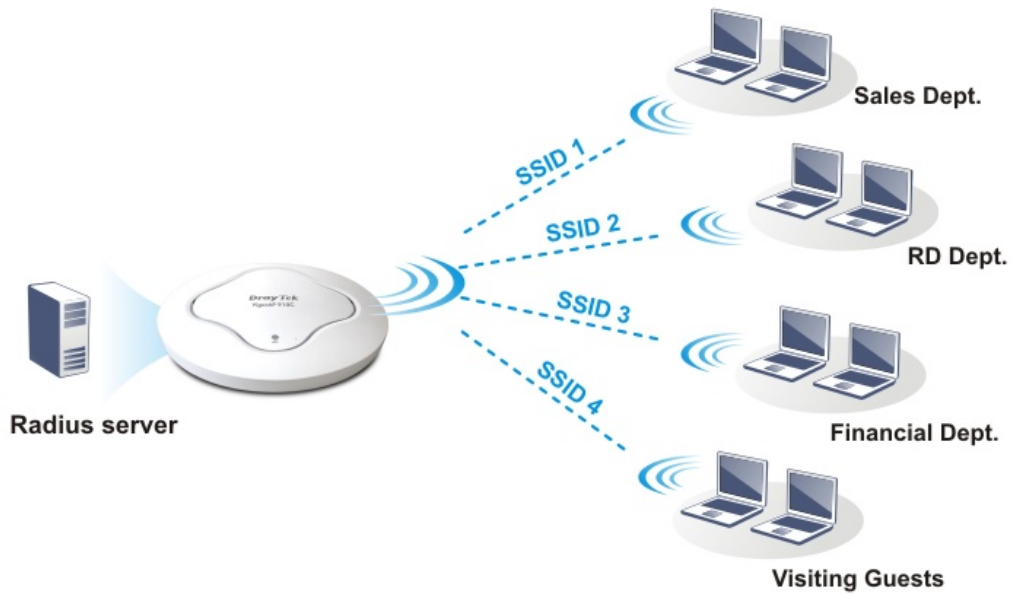
VigorAP 910C can operate in standalone mode for your office network or a classroom; connected to your LAN and offering you with wireless access.

It makes high density with quality-performance be feasible for users as it is going to be implemented with DrayTek central wireless management (AP Management) supports configuration, firmware upgrade, status, monitoring, and load-balancing.

The Power of Ethernet (PoE) on VigorAP 910C relieves the installation of power plug. The massive deployment of VigorAP 910C for hospitalities and school environment will be much easier.

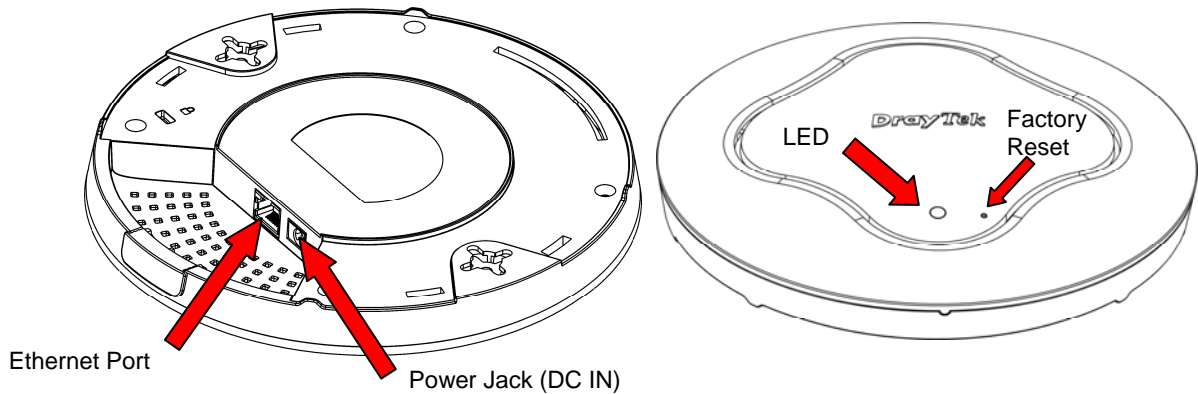
With the optimized antennas built-in, DrayTek VigorAP 910C ceiling-mount wireless access point is ideal for hospitalities, small offices and small campus.

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.



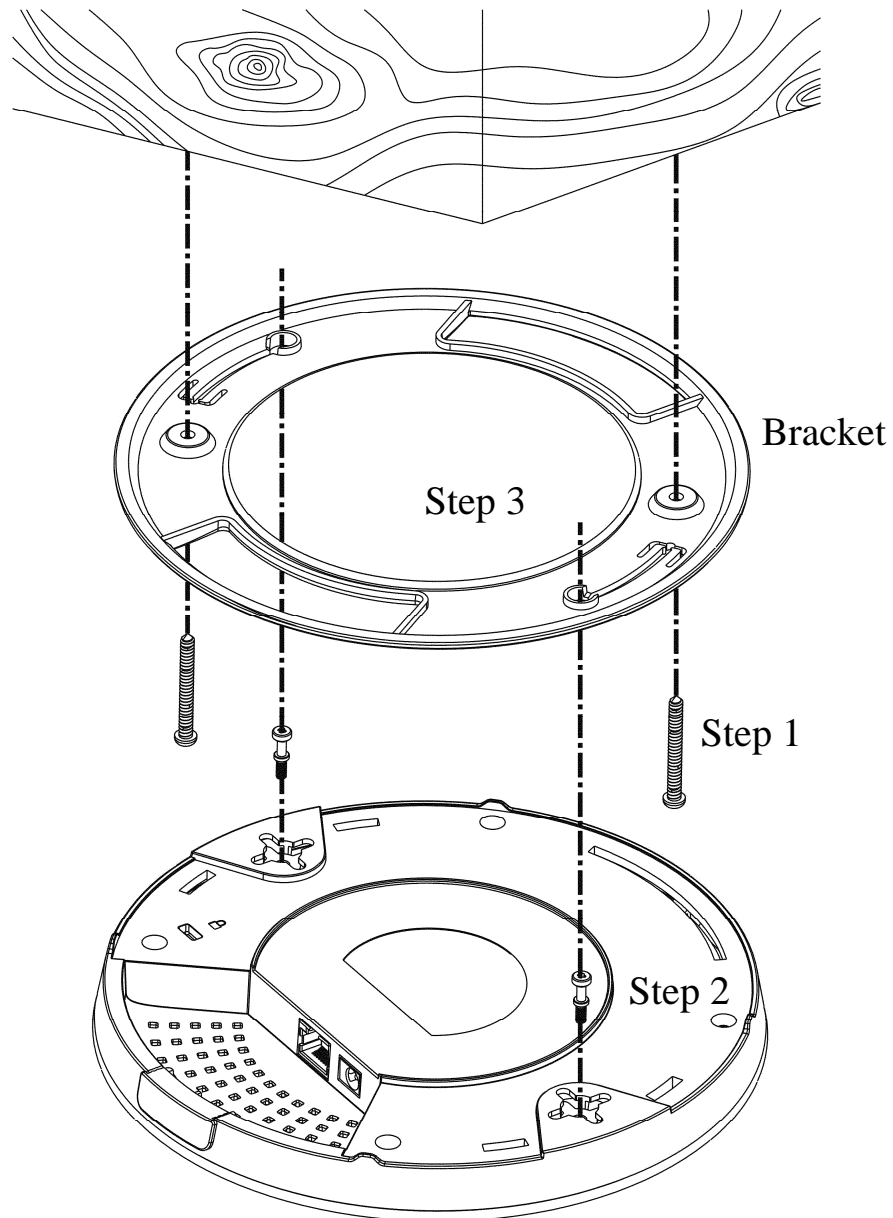
LED	Status	Explanation
Blue LED	Blinking	VigorAP is ready and can work normally.
	Off	VigorAP is not ready or fails.
Purple LED	On	Power adapter is plugged in and VigorAP is initiating.
Orange LED	Blinking	The firmware upgrade is in process.
Off	Off	VigorAP is powered off.
USB	Connector for a printer.	
Interface	Explanation	
Ethernet Port	Connector for xDSL / Cable modem (Giga level) or router.	
Power Jack (DC IN)	Connector for a power adapter.	
Hole	Explanation	
Factory Reset	Restore the default settings when any error occurs in VigorAP. Usage: Use sharp article (e.g., paperclip or pin) to insert into the hole and keep for more than 10 seconds. Then VigorAP will restart with the factory default configuration. When purple LED is On again, it means VigorAP has restarted and is ready to use.	

## 1.3 Hardware Installation

VigorAP can be installed under certain locations: wooden ceiling, plasterboard ceilings, light-weighted steel frame and wall.

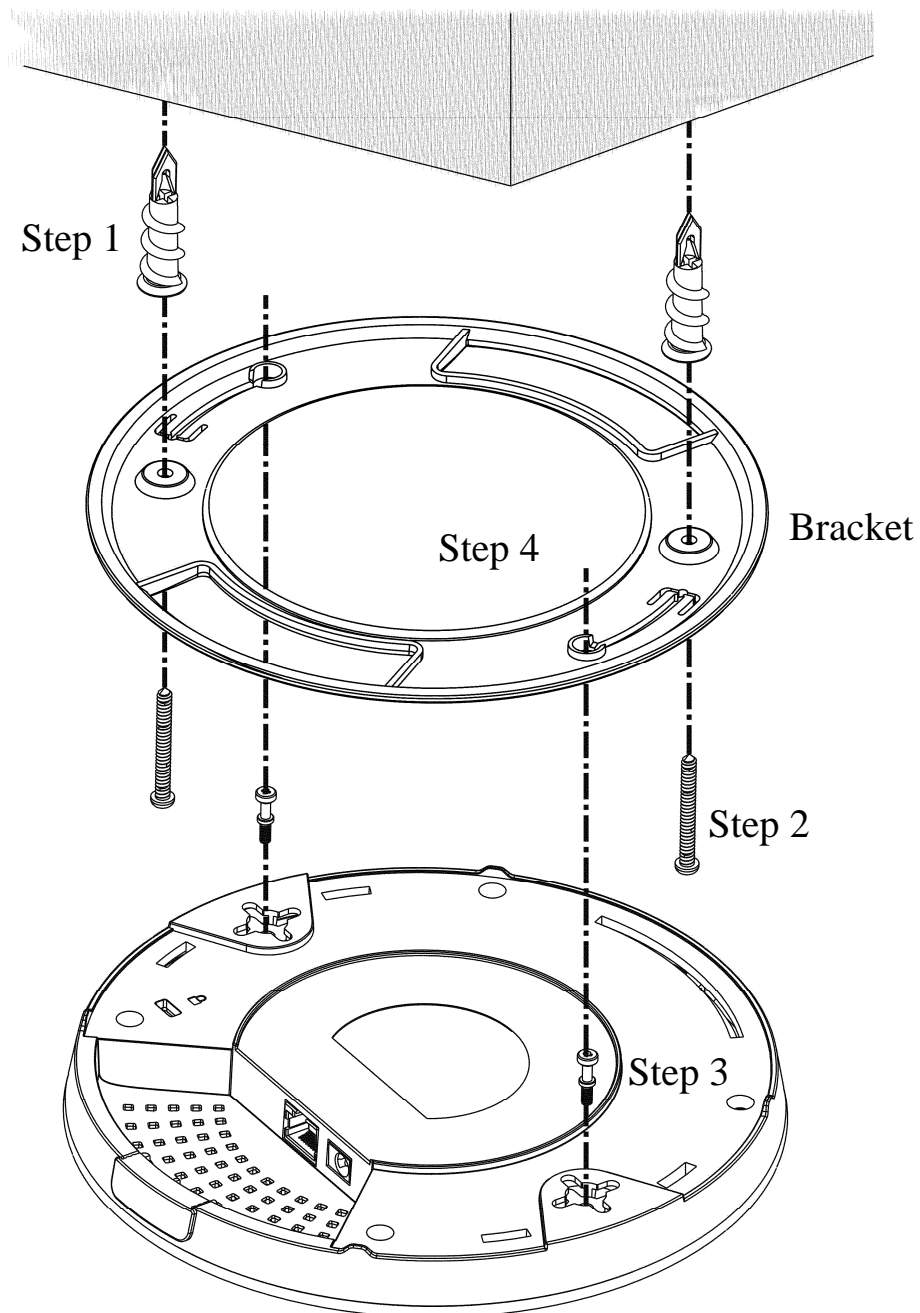
### 1.3.1 Ceiling-mount Installation (Wooden Ceiling)

1. Place the bracket under the wooden ceiling and fasten two screws firmly (as shown in Figure below, Step 1).
2. When the bracket is in place, fasten two screws firmly (as shown in Figure below, Step 2) on the bottom of VigorAP.
3. Make the device just below the bracket. Put the screws installed in Step 2 on the holes of the bracket (as shown in Figure below, Step 3).
4. Gently rotate the device to make screws slide into the notches of the bracket and move forward till it is firmly fixed.



### 1.3.2 Ceiling-mount Installation (Plasterboard Ceiling)

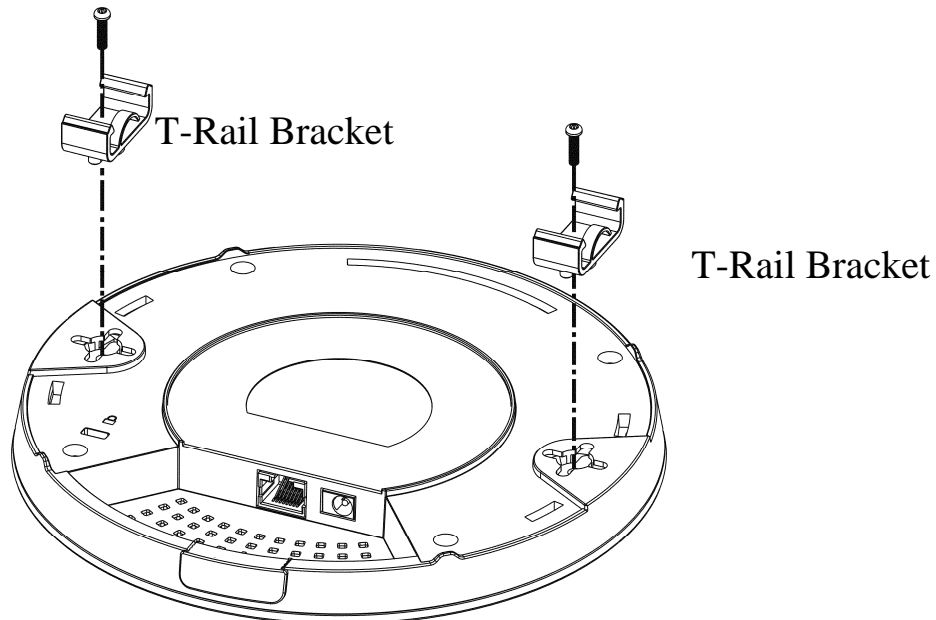
1. Place the bracket under the plasterboard ceiling and fasten two turnbuckles firmly (as shown in Figure below, Step 1).
2. Make the screws pass through the bracket and insert into the turnbuckles (as shown in Figure below, Step 2). Fasten them to offer more powerful supporting force.
3. When the bracket is in place, fasten two screws firmly (as shown in Figure below, Step 3) on the bottom of VigorAP.
4. Make the device just below the bracket. Put the screws installed in Step 3 on the screw holes of the bracket (as shown in Figure below, Step 4).
5. Gently rotate the device to make screws slide into the notches of the bracket and move forward till it is firmly fixed.



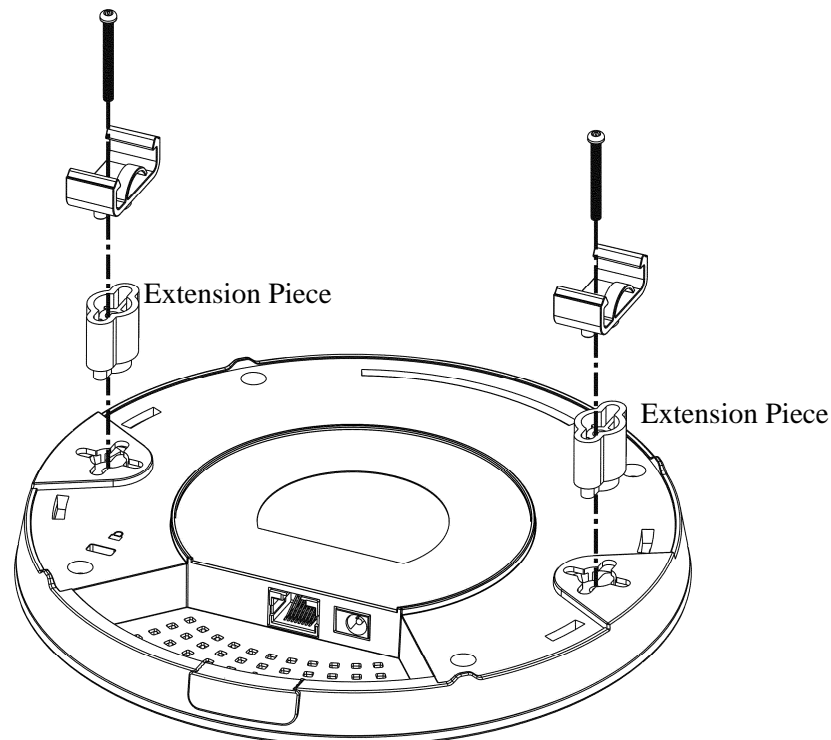
### 1.3.3 Suspended Ceiling (Lightweight Steel Frame) Installation

You cannot screw into ceiling tiles as they are weak and not suitable for bearing loads. Your VigorAP is supplied with mounts (T-Rail brackets) which attach directly to the metal grid ('T-Rail') of your suspended ceiling.

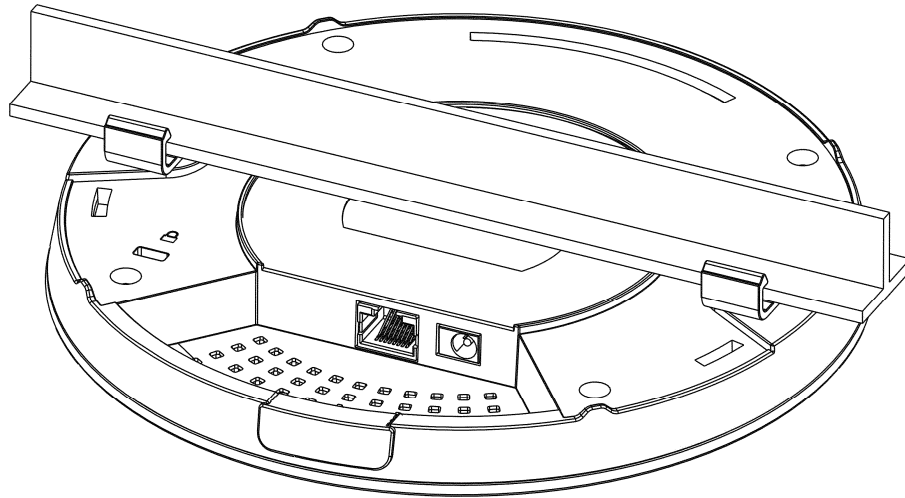
1. Choose one set of T-Rail mounting kits from the bundled package.
2. Put the T-Rail brackets on the holes of the bottom side of the device. Fasten them with suitable screws.



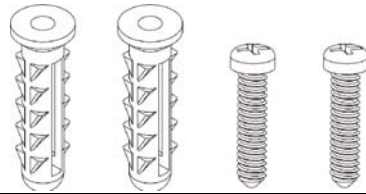
3. If a larger gap is required between the ceiling and the VigorAP, use the extension pieces to extend the height of the brackets.



4. Use the T-Rail brackets to fasten the device on Light-weighted Steel Frame.



**Warning: The screw set shown below is for wall mounting only. Do not use such set for ceiling mounting due to the danger of falling.**



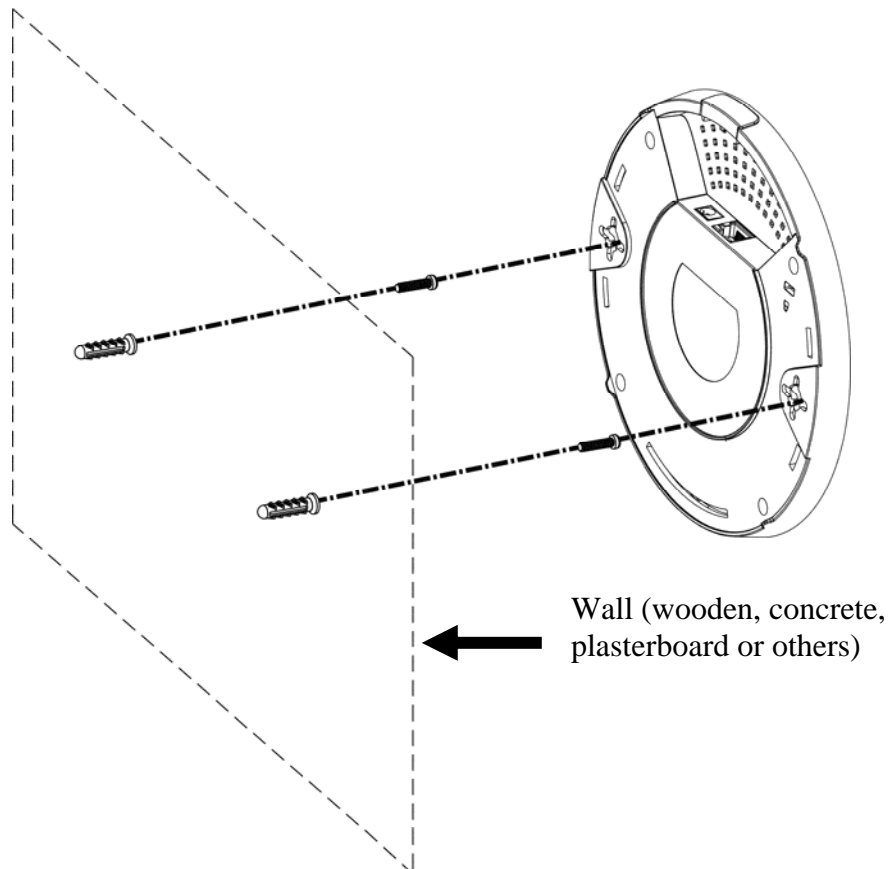
### 1.3.4 Wall Mounting Installation

For wall-mounting, the VigorAP has keyhole type mounting slots on the underside. You can fit the AP at any axis (i.e. 12, 3, 6 or 9 O’Clock) to allow for cable entry from the most convenient location if you are using side entry – note the position of the side entry cable cutout.

1. A template is provided on the VigorAP’s packaging box to enable you to space the screws correctly on the wall.



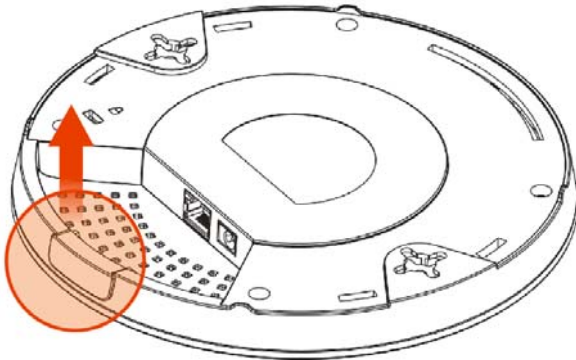
2. Place the template on the wall and drill the holes according to the recommended instruction.
3. Fit screws into the wall using the appropriate type of wall plug (as shown in the ceiling section) but do not use the ceiling bracket – the VigorAP hangs directly onto the screws.



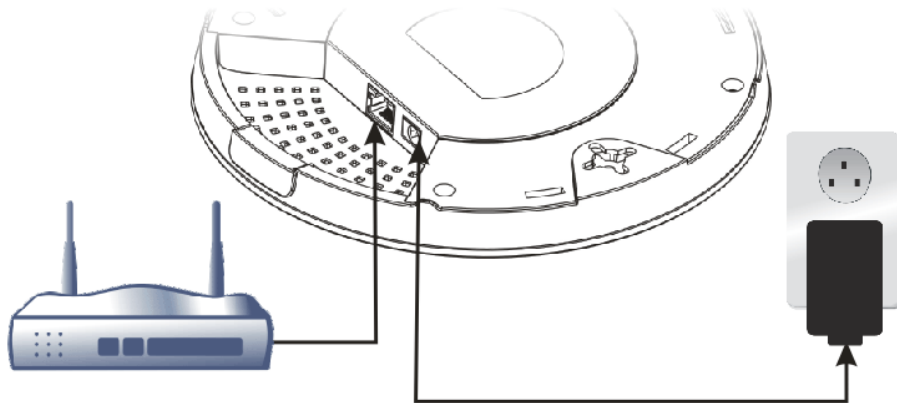


## 1.4 Notifications for Hardware Connection

- If required, remove the protective cap of VigorAP to create extra space for the cables to pass through.

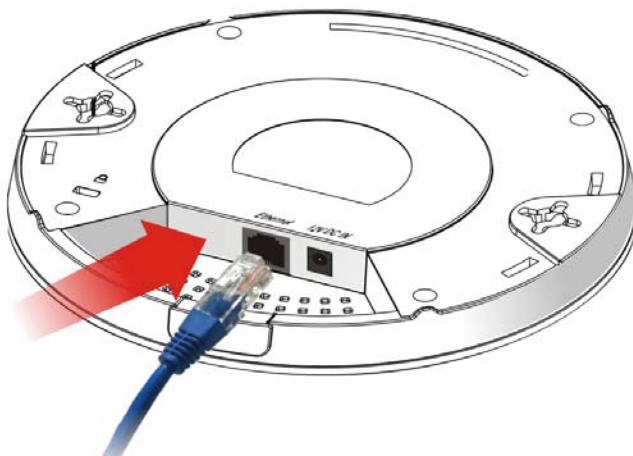


- Connect VigorAP to Vigor router (via LAN port) with Ethernet cable.



### Vigor Router

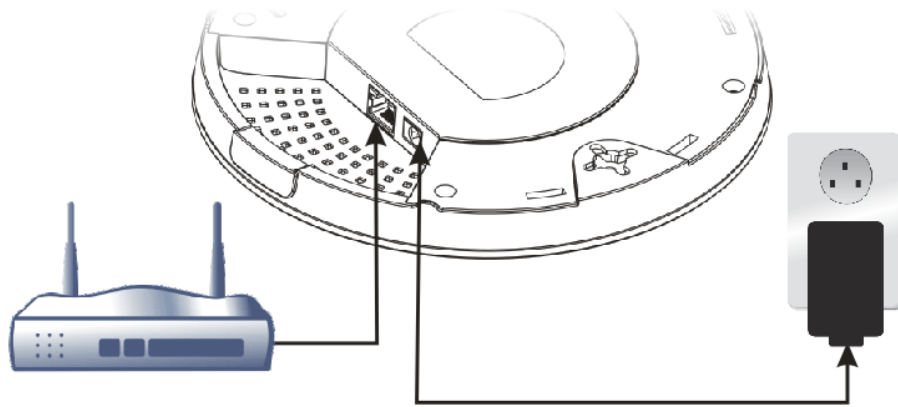
- Connect VigorAP to PoE switch (via LAN port) with Ethernet cable. For connecting with PoE switch, do not connect the power adapter. VigorAP will get the power from the switch directly.



## 1.5 Connect to a Vigor Router using AP Management

Your VigorAP can be used with Vigor routers which support AP management (such as the Vigor 2862 or Vigor 2926 series). AP Management enables you to monitor and manage multiple DrayTek APs from a single interface.

1. Connect one end of the power adapter to power port of VigorAP, and the other side into a wall outlet.




### Vigor Router

2. Access into the web user interface of Vigor router. Here we take Vigor2862 as an example. Open **Central Management >> AP >> Status**.

Central Management >> AP >> Status

Index	Device Name	IP Address	SSID	Ch.	STA List	AP List	Uptime	Ver.	Password
1	VigorAP910C	192.168.1.11	DrayTek DrayTek5G	11 36	0/6 0/6	0 0	0d 00:01	1.1.7	Password <input type="password"/>

**Note:**

 : Online    : Offline    : Hidden SSID

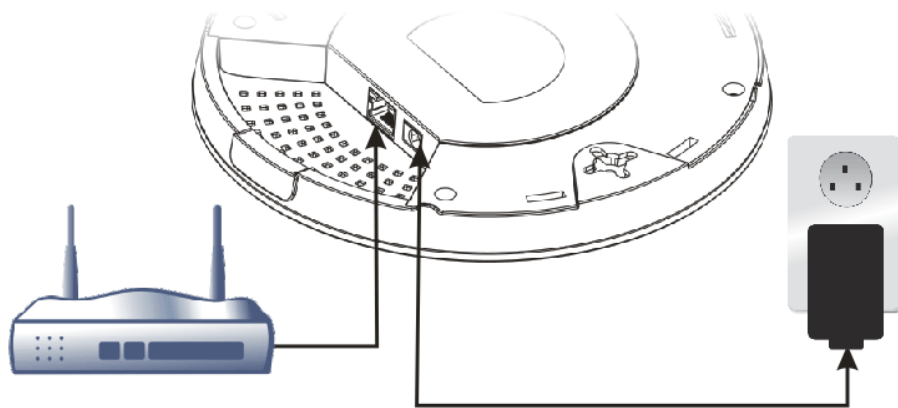
Maximum support 20 APs.

When AP Devices connect via an intermediary switch, please ensure that **UDP:4944** port and the **HTTP** port of AP Devices are not blocked so that the AP status can be retrieved.

3. Locate VigorAP 910C. Click the IP address assigned by Vigor router to access into web user interface of VigorAP 910C.
4. After typing username and password (admin/admin), the main screen will be displayed.

## 1.6 Connect to a Vigor Router without AP Management

1. Connect one end of the power adapter to power port of VigorAP, and the other side into a wall outlet.



### Vigor Router

2. Access into the web user interface of Vigor router. Here we take Vigor2830 as an example. Open **External Devices**.

#### External Devices

External Device Auto Discovery

#### External Devices Connected

Below shows available devices that connected externally:

#### For security reason:

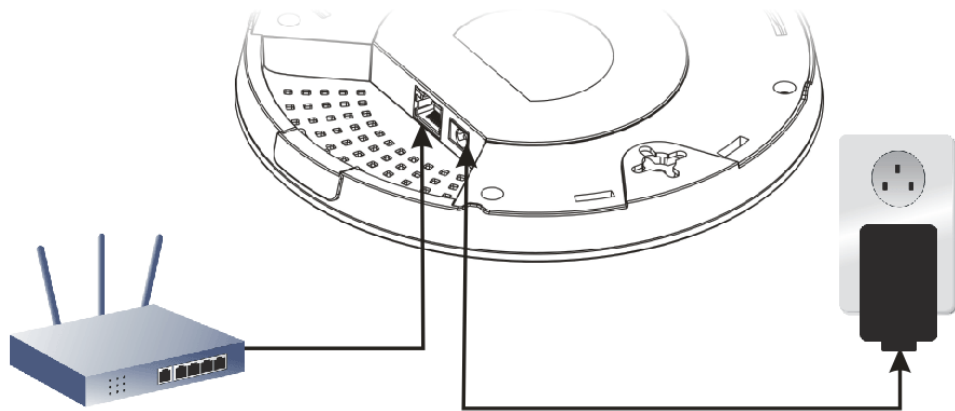
If you have changed the administrator password on External Device, please click the **Account** button to retype new username and password. Otherwise, the router will be unable to monitor the External Device properly. Click the **Clear** button to Clear the off-line information and account information.

OK

3. Check the box of **External Device Auto Discovery** and click **OK**. When the IP address assigned by Vigor router appears, click it to access into web user interface of VigorAP 910C.
4. After typing username and password (admin/admin), the main screen will be displayed.

## 1.7 Connect without a DrayTek Router/LAN

1. Connect one end of the power adapter to power port of VigorAP, and the other side into a wall outlet.



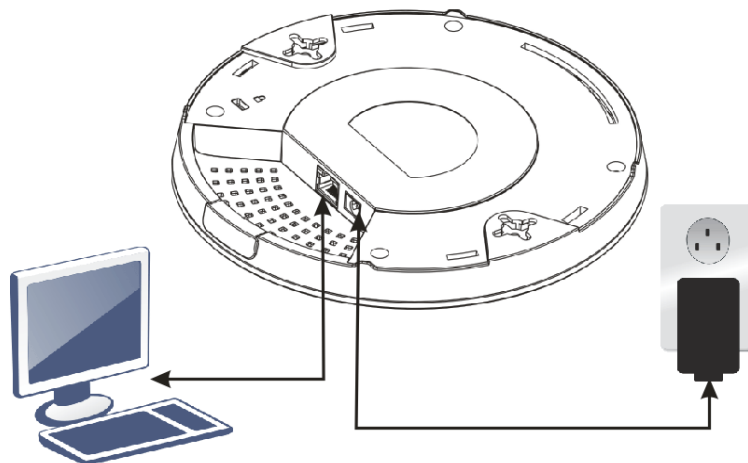
2. Access into the web user interface of the router.
3. Check that **DHCP table** to find an entry with a MAC address matching the VigorAP – the VigorAP's MAC address is printed on a label on the base. Once you have the VigorAP's IP address, you can access its own web interface, as shown in section 4.6

LAN	
MAC Address	: 00:1D:AA:74:DA:38
IP Address	: 192.168.1.10
IP Mask	: 255.255.255.0

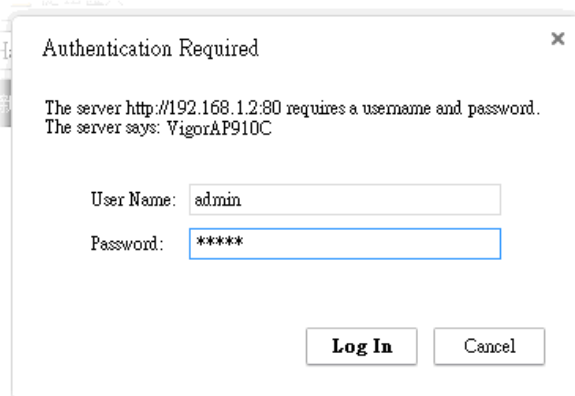
4. After getting the IP address of VigorAP 910C, access into the web user interface of VigorAP 910C through the web page of non-Vigor router.

## 1.8 Connecting to PC Directly

1. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the VigorAP and the other end of the cable (RJ-45) into the Ethernet port on your computer.
2. Connect one end of the power adapter to VigorAP's power port on the bottom of the device, and the other side into a wall outlet.
3. Wait for VigorAP initiation. When VigorAP is ready, the LED will blink in blue.



4. Set the IP address of the PC as "192.168.1.x (x means any number, ranges from 3 to 100).
5. Open a web browser on your PC and type **http://192.168.1.2**. The following window will be open to ask for username and password. Type "admin/admin" and click **Login**.



6. Main screen will be displayed.

Before using VigorAP, finish the following web configuration first.

- Configuring LAN IP address(es)
- SSID and Security setting for 2.4G and 5GHz.
- Administrator's name and password.
- Time and date.

For detailed, refer to Section 2.5 Accessing to Web User Interface.

This page is left blank.

# 2

## Network Configuration

After the network connection is built, the next step you should do is setup VigorAP 910C with proper network parameters, so it can work properly in your network environment.

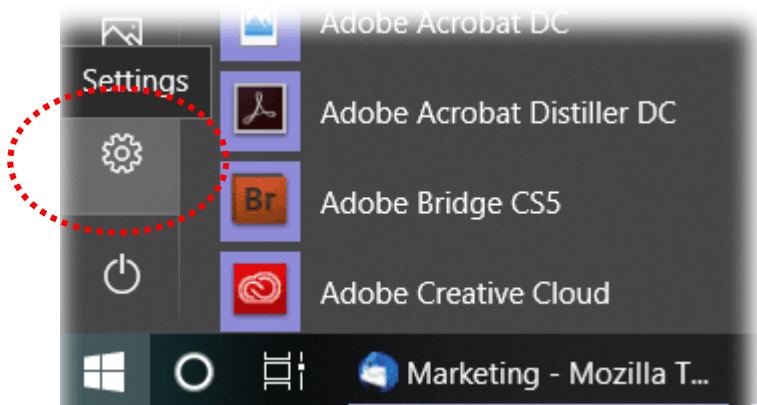
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic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

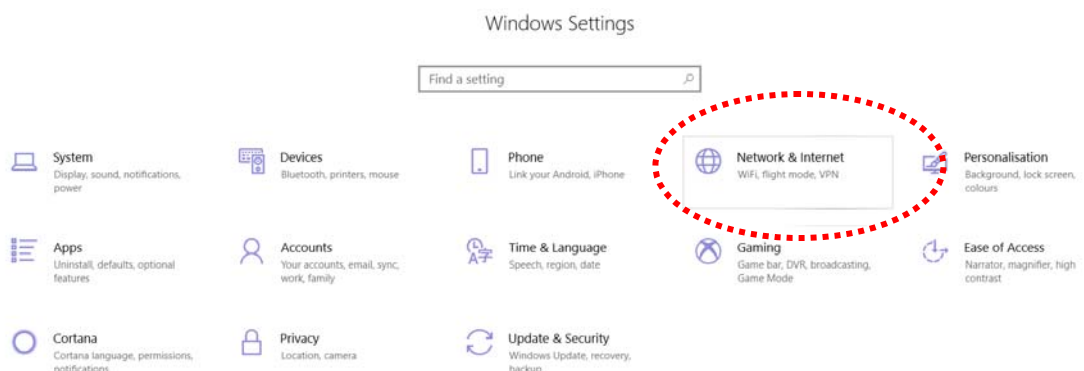
**Windows 10** - please go to section 2.1

### 2.1 Windows 10 IP Address Setup

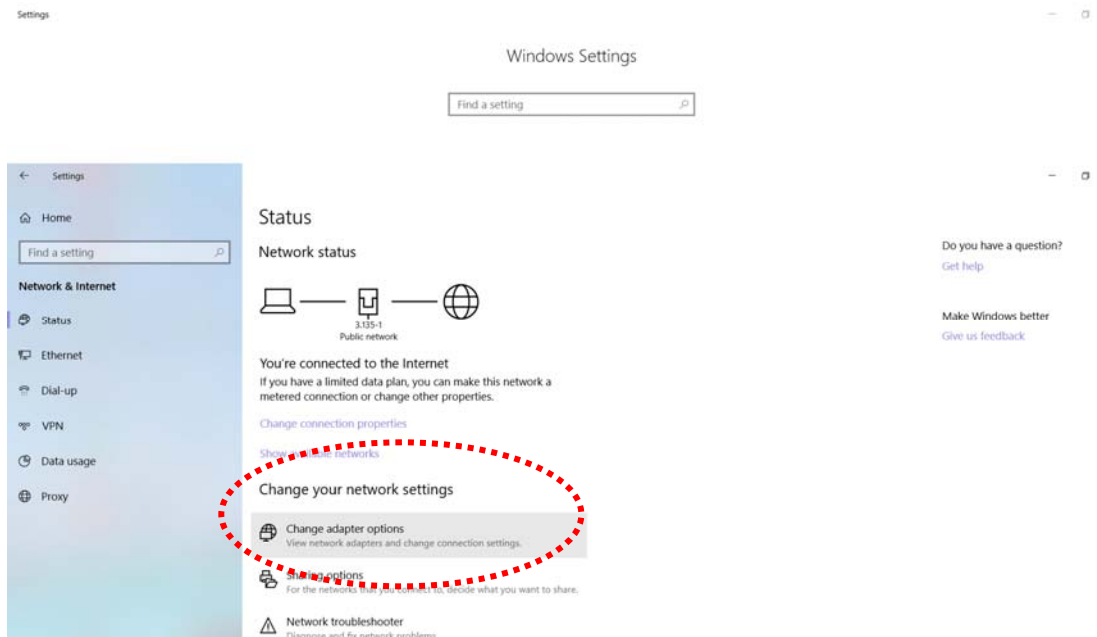
Click the **Start** button (it should be located at lower-left corner of your computer), then click the **Settings** icon.



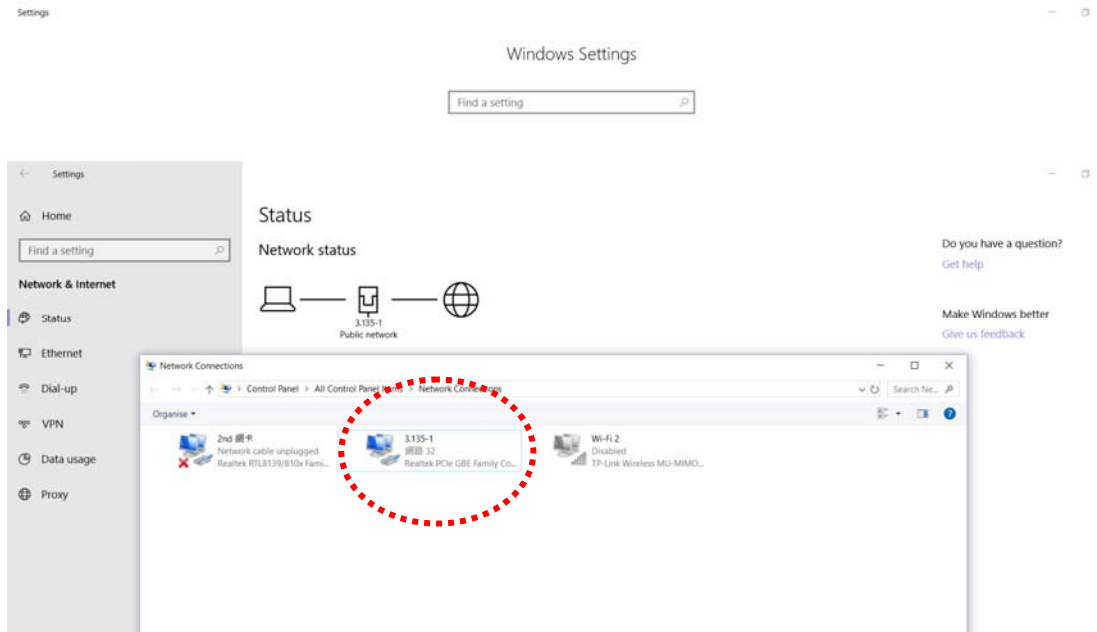
Double-click **Network & Internet**.



Next, click **Change adapter options**.

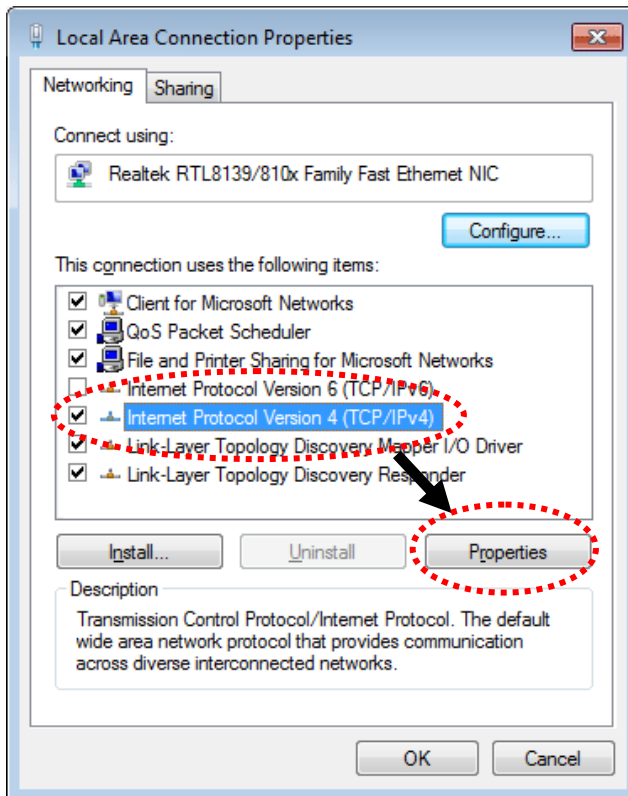


Click the local area connection.





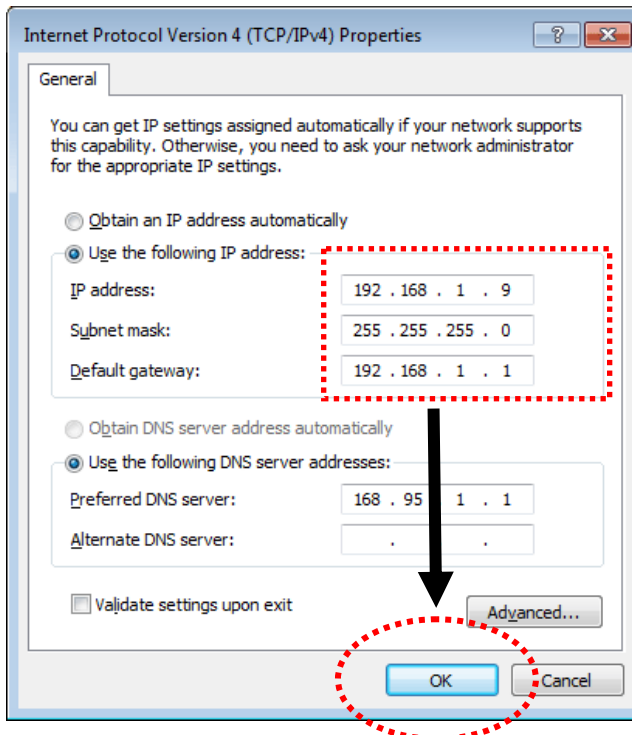
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



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**

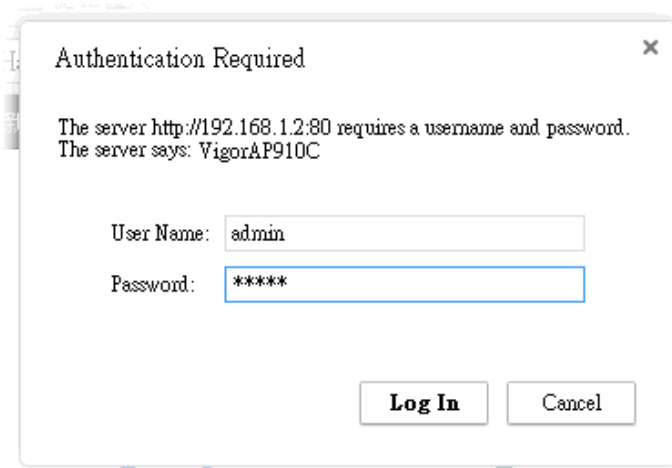
Subnet Mask: **255.255.255.0**



## 2.2 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).

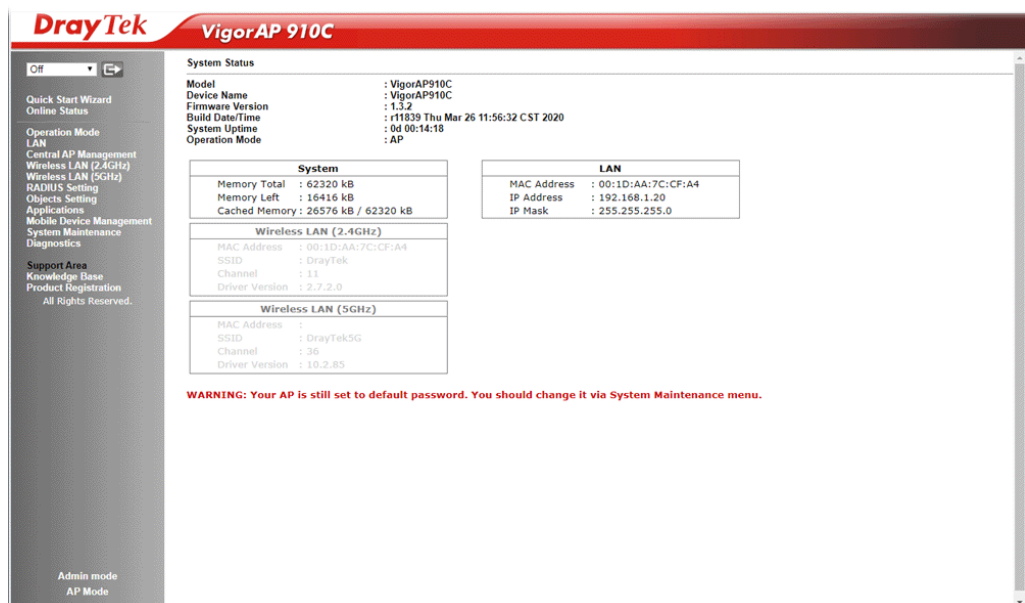
1. Make sure your PC connects to the VigorAP 910C correctly.
2. Open a web browser on your PC and type **http://192.168.1.2**. A pop-up window will open to ask for username and password. Please type “admin/admin” on Username/Password and click **OK**.



**Note:** You may either simply 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 VigorAP 910C**.

- If there is no DHCP server on the network, then VigorAP 910C will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 910C will receive its IP address via the DHCP server.

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



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

## 2.3 Changing Password

1. Please change the password for the original security of the modem.
2. Go to **System Maintenance** page and choose **Administration 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 Account can contain only a-z A-Z 0-9 , ~ ` ! @ \$ % ^ \* ( ) \_ + = { } [ ] | ; < > . ?  
Authorization Password can contain only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & \* ( ) \_ + = { } [ ] | \ ;  
< > . ? /

3. Enter the new login password on the field of **Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.

Authentication Required

The server http://192.168.1.2:80 requires a username and password.  
The server says: VigorAP910C

User Name:

Password:


## 2.4 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.

### 2.4.1 Configuring Wireless Settings – General

This page displays general settings (enable/disable wireless LAN 2.4GHz/5GHz) for the operation mode selected.

Quick Start Wizard >> wiz wireless

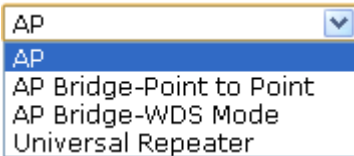
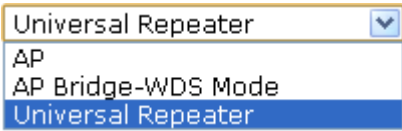
**Wireless LAN(2.4GHz)**  
**Operation Mode :**    
 VigorAP acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

**Wireless LAN(5GHz)**  
**Operation Mode:**    
 VigorAP can act as a wireless repeater; it can be Station and AP at the same time.

---

Operation Mode
Wireless(2.4GHz)
Wireless(5GHz)

Available settings are explained as follows:

Item	Description
<b>Wireless LAN (2.4GHz)</b>	Check the box to enable WLAN 2.4GHz for VigorAP. <b>Operation Mode</b> - There are four operation modes for wireless connection. Settings for each mode are different. 
<b>Wireless LAN (5GHz)</b>	Check the box to enable WLAN 5GHz for VigorAP. <b>Operation Mode</b> - There are two operation modes for wireless connection. Settings for each mode are different. 

## 2.4.2 Configuring 2.4GHz Wireless Settings Based on the Operation Mode

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

### Settings for AP

When you choose AP as the operation mode for wireless LAN (2.4GHz), you will need to configure the following page.

Quick Start Wizard >> Wireless LAN (2.4GHz)

Channel :

Main SSID :

Security Key:

Enable Guest Wireless

    SSID:

    Security Key:

Enable Bandwidth Limit

Enable Station Control

---

Operation Mode      **Wireless(2.4GHz)**      Wireless(5GHz)

Available settings are explained as follows:

Item	Description
<b>Channel</b>	<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 <b>AutoSelect</b> to let system determine for you.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>2462MHz (Channel 11) ▾</p> <p>AutoSelect</p> <p>2412MHz (Channel 1)</p> <p>2417MHz (Channel 2)</p> <p>2422MHz (Channel 3)</p> <p>2427MHz (Channel 4)</p> <p>2432MHz (Channel 5)</p> <p>2437MHz (Channel 6)</p> <p>2442MHz (Channel 7)</p> <p>2447MHz (Channel 8)</p> <p>2452MHz (Channel 9)</p> <p>2457MHz (Channel 10)</p> <p style="background-color: #e0e0e0;">2462MHz (Channel 11)</p> <p>2467MHz (Channel 12)</p> <p>2472MHz (Channel 13)</p> </div>
<b>Main SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Security Key</b>	Type <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
<b>Enable Guest Wireless</b>	<p>Check the box to enable the <b>guest</b> wireless setting.</p> <p>Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests</p>

for one hour every day.

**SSID** – Set a name for VigorAP 910C which can be identified and connected by wireless guest.

**Security Key**– Set **8~63** ASCII characters or **8~63** ASCII characters which can be used for logging into VigorAP 910C by wireless guest.

**Enable Bandwidth Limit** – Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID.

- **Upload Limit** – Scroll the radio button to choose the value you want.
- **Download Limit** – Scroll the radio button to choose the value you want.

**Enable Station Control** – Check the box to set the duration for the guest connecting /reconnecting to Vigor device.

- **Connection Time** – Scroll the radio button to choose the value you want.
- **Reconnection Time** – Scroll the radio button to choose the value you want.

## Settings for AP Bridge-Point to Point

When you choose AP Bridge-Point to Point as the operation mode for wireless LAN (2.4GHz), you will need to configure the following page.

Quick Start Wizard >> Wireless LAN (2.4GHz)

AP Discovery:

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

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

Operation Mode	Wireless(2.4GHz)	Wireless(5GHz)
<input &gt;="" &gt;<="" <input="" td="" type="button" value=" Cancel "/>		

Available settings are explained as follows:

Item	Description
AP Discovery	Click this button to open the AP Discovery dialog. VigorAP 910C can scan all regulatory channels and find working APs in the neighborhood.

<b>Phy Mode</b>	Data will be transmitted via HTMIX mode. Each access point should be setup to the same <b>Phy Mode</b> for connecting with each other.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Type <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
<b>Peer MAC Address</b>	Type the peer MAC address for the access point that VigorAP 910C connects to.

## Advanced Settings for AP Bridge-WDS

When you choose AP Bridge-WDS as the operation mode for wireless LAN (2.4GHz), you will need to configure the following page.

Quick Start Wizard >> Wireless LAN (2.4GHz)

AP Discovery:

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

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

Main SSID:   
 Security Key:

Operation Mode	Wireless(2.4GHz)	Wireless(5GHz)
<input type="button" value=" &lt; Back"/>	<input type="button" value=" Next &gt;"/>	<input type="button" value=" Cancel"/>

Available settings are explained as follows:

Item	Description
<b>AP Discovery</b>	Click this button to open the AP Discovery dialog. VigorAP 910C can scan all regulatory channels and find working APs in the neighborhood.
<b>Phy Mode</b>	Data will be transmitted via HTMIX mode.  Each access point should be setup to the same <b>Phy Mode</b> for connecting with each other.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
<b>Peer MAC Address</b>	Type the peer MAC address for the access point that VigorAP connects to.
<b>Main SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Security Key</b>	Type <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").



## Settings for Universal Repeater

When you choose Universal Repeater as the operation mode for wireless LAN (2.4GHz), you will need to configure the following page.

Quick Start Wizard >> Wireless LAN (2.4GHz)

### Universal Repeater Parameters

Please input the SSID you want to connect to :

SSID

MAC Address (Optional)

Channel  ▼

Security Mode  ▼

Encryption Type  ▼

Security Key

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

Use the same SSID and Security Key as above

SSID :

Security Key:

Enable Guest Wireless

SSID:

Security Key:

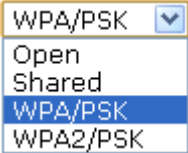
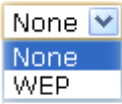
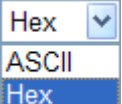
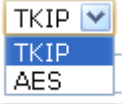
Enable Bandwidth Limit

Enable Station Control

Operation Mode  Wireless(2.4GHz)  Wireless(5GHz)

Available settings are explained as follows:

Item	Description
<b>Universal Repeater Parameters</b>	
<b>AP Discovery</b>	Click this button to open the AP Discovery dialog. VigorAP 910C can scan all regulatory channels and find working APs in the neighborhood.
<b>SSID / MAC Address (Optional)</b>	SSID means the identification of the wireless LAN. After choosing one of the AP from AP Discovery window and clicking <b>OK</b> , the settings (SSID and MAC Address) related to the selected AP will be displayed on these fields automatically. Later, VigorAP 910C will be allowed to access Internet through the selected AP, by using SSID displayed here.
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Security Mode</b>	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.

	
<b>Encryption Type for Open/Shared</b>	<p>This option is available when Open/Shared is selected as Security Mode.</p> <p>Choose <b>None</b> to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose <b>WEP</b>.</p>  <p><b>WEP Keys</b> - 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> 
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>This option is available when <b>WPA/PSK</b> or <b>WPA2/PSK</b> is selected as <b>Security Mode</b>.</p> <p>Select <b>TKIP</b> or <b>AES</b> as the algorithm for WPA.</p> 
<b>Security Key</b>	<p>Type <b>8~63</b> ASCII characters, such as 012345678...(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK</b> or <b>WPA2/PSK</b> mode.</p>
<b>Use the same SSID and Security Key as Above</b>	<p>In general, under the network environment, same SSID and security key can be used for the host (wireless client) and the repeater (VigorAP 910C) in Universal Repeater mode. Check it to use the same SSID and security key configured as above.</p> <p><b>SSID</b> - SSID can be any text numbers or various special characters. For VigorAP 910C is set as "Repeater", the purpose of the device is to extend the Wi-Fi service. Therefore, the characters set here will be regarded as "main SSID". Other wireless client can receive the wireless signal from VigorAP 910C by using the SSID configured here.</p> <p><b>Security Key</b>- Set <b>8~63</b> ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 910C by other wireless client.</p>
<b>Enable Guest</b>	<p>Check the box to enable the <b>guest</b> wireless setting.</p>

---

<b>Wireless</b>	<p><b>SSID</b> – Set a name for VigorAP 910C. Wireless guest is allowed to access into Internet via VigorAP 910C with the SSID configured here.</p> <p><b>Security</b> – Set <b>8~63</b> ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 910C by wireless guest.</p> <p><b>Enable Bandwidth Limit</b> – Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID.</p> <ul style="list-style-type: none"><li>● <b>Upload Limit</b> –Scroll the radio button to choose the value you want.</li><li>● <b>Download Limit</b> –Scroll the radio button to choose the value you want.</li></ul> <p><b>Enable Station Control</b> – Check the box to set the duration for the guest connecting /reconnecting to Vigor device.</p> <ul style="list-style-type: none"><li>● <b>Connection Time</b> –Scroll the radio button to choose the value you want.</li><li>● <b>Reconnection Time</b> –Scroll the radio button to choose the value you want.</li></ul>
-----------------	---

---

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

## 2.4.3 Configuring 5GHz Wireless Settings Based on the Operation Mode

VigorAP 910C offers 5GHz wireless connection capability. You can setup 5G features in Quick Start Wizard first. Once the USB 5GHz wireless dongle connects to VigorAP 910C, it can work immediately.

### Settings for AP

After finished the configuration for wireless LAN (2.4GHz) and click Next, you will need to configure the following page if you choose AP as the operation mode for wireless LAN (5GHz).

Quick Start Wizard >> 5G Security

Channel :

Main SSID :

Security Key :

Enable Guest Wireless

    SSID:

    Security Key:

Enable Bandwidth Limit

    Upload Limit  Kbps

    Download Limit  Kbps

Enable Station Control

    Connection Time  Min(s)

    Reconnection Time  Min(s)

Operation Mode: Wireless(2.4GHz) Wireless(5GHz)

Available settings are explained as follows:

Item	Description
<b>Channel</b>	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.
<b>Main SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Security Key</b>	Type <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
<b>Enable Guest Wireless</b>	<p>Check the box to enable the <b>guest</b> wireless setting.</p> <p><b>SSID</b> – Set a name for VigorAP 910C which can be identified and connected by wireless guest.</p> <p><b>Security Key</b>– Set <b>8~63</b> ASCII characters or <b>8~63</b> ASCII characters which can be used for logging into VigorAP 910C by wireless guest.</p> <p><b>Enable Bandwidth Limit</b> – Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID.</p> <ul style="list-style-type: none"> <li>● <b>Upload Limit</b> –Scroll the radio button to choose the value</li> </ul>

	<p>you want.</p> <ul style="list-style-type: none"> <li>● <b>Download Limit</b> –Scroll the radio button to choose the value you want.</li> </ul> <p><b>Enable Station Control</b> – Check the box to set the duration for the guest connecting /reconnecting to Vigor device.</p> <ul style="list-style-type: none"> <li>● <b>Connection Time</b> –Scroll the radio button to choose the value you want.</li> <li>● <b>Reconnection Time</b> –Scroll the radio button to choose the value you want.</li> </ul>
--	---

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

### Settings for AP Bridge-WDS Mode

After finished the configuration for wireless LAN (2.4GHz) and click Next, you will need to configure the following page if you choose AP Bridge-WDS as the operation mode for wireless LAN (5GHz).

Quick Start Wizard >> Wireless LAN (5GHz)

AP Discovery :

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

Remote AP should always set LAN-A MAC address to connect VigorAP WDS.

**Phy Mode :** HTMIX

---

**Security :**

Disabled  
 WEP  
 TKIP  
 AES

Key :

**Peer Mac Address:**

:  :  :  :  :

Main SSID :

Security Key:

Operation Mode

Wireless(2.4GHz)

Wireless(5GHz)

Available settings are explained as follows:

Item	Description
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Key – Enter a string as security key.
<b>Peer Mac Address</b>	Enter the MAC address for the peer.
<b>Main SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Security Key</b>	Type <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

## Settings for Universal Repeater

After finished the configuration for wireless LAN (2.4GHz) and click Next, you will need to configure the following page if you choose Universal Repeater as the operation mode for wireless LAN (5GHz).

Quick Start Wizard >> Wireless LAN (5GHz)

### Universal Repeater Parameters

Please input the SSID you want to connect to :

SSID

MAC Address (Optional)

Channel

Security Mode

Encryption Type

Security Key

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

Use the same SSID and Security Key as above

SSID :

Security Key:

Enable Guest Wireless

SSID:

Security Key:

Enable Bandwidth Limit

Enable Station Control

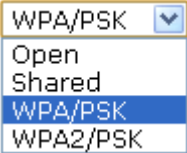
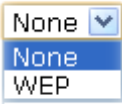
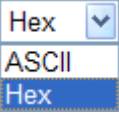
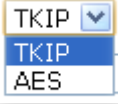
Connection Time   Min(s)

Reconnection Time   Min(s)

Operation Mode  Wireless(2.4GHz)  Wireless(5GHz)

Available settings are explained as follows:

Item	Description
<b>AP Discovery</b>	Click this button to open the AP Discovery dialog. VigorAP 910C can scan all regulatory channels and find working APs in the neighborhood.
<b>SSID / MAC Address (Optional)</b>	SSID means the identification of the wireless LAN. After choosing one of the AP from AP Discovery window and clicking <b>OK</b> , the settings (SSID and MAC Address) related to the selected AP will be displayed on these fields automatically. Later, VigorAP 910C will be allowed to access Internet through the selected AP, by using SSID displayed here.
<b>Channel</b>	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.
<b>Security Mode</b>	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.

	
<b>Encryption Type for Open/Shared</b>	<p>This option is available when Open/Shared is selected as Security Mode.</p> <p>Choose <b>None</b> to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose <b>WEP</b>.</p>  <p><b>WEP Keys</b> - 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> 
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>This option is available when <b>WPA/PSK</b> or <b>WPA2/PSK</b> is selected as <b>Security Mode</b>.</p> <p>Select <b>TKIP</b> or <b>AES</b> as the algorithm for WPA.</p> 
<b>Security Key</b>	<p>Type <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK</b> mode.</p>
<b>Use the same SSID and Security Key as Above</b>	<p>In general, under the network environment, same SSID and security key can be used for the host (wireless client) and the repeater (VigorAP 910C) in Universal Repeater mode. Check it to use the same SSID and security key configured as above.</p> <p><b>SSID</b> - SSID can be any text numbers or various special characters. For VigorAP 910C is set as "Repeater", the purpose of the device is to extend the Wi-Fi service. Therefore, the characters set here will be regarded as "main SSID". Other wireless client can receive the wireless signal from VigorAP 910C by using the SSID configured here.</p> <p><b>Security Key</b> - Set <b>8~63</b> ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 910C by other wireless client.</p>
<b>Enable Guest</b>	<p>Check the box to enable the <b>guest</b> wireless setting.</p>

---

**Wireless**

**SSID** – Set a name for VigorAP 910C Wireless guest is allowed to access into Internet via VigorAP 910C with the SSID configured here.

**Security** – Set **8~63** ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 910C by wireless guest.

**Enable Bandwidth Limit** – Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID.

- **Upload Limit** –Scroll the radio button to choose the value you want.
- **Download Limit** –Scroll the radio button to choose the value you want.

**Enable Station Control** – Check the box to set the duration for the guest connecting /reconnecting to Vigor device.

- **Connection Time** –Scroll the radio button to choose the value you want.
  - **Reconnection Time** –Scroll the radio button to choose the value you want.
- 

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



## 2.4.4 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 "AP910C" 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

## 2.5 Online Status

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

### Online Status

System Status		System Uptime: 0d 00:16:12		
<b>LAN Status</b>				
<b>IP Address</b>	<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
192.168.1.12	15923	10720	17563249	838379
<b>Universal Repeater Status</b>				
<b>IP</b>	<b>Gateway</b>	<b>SSID</b>	<b>Channel</b>	
			11	
<b>Remote Mac</b>	<b>Security Mode</b>	<b>TX Packets</b>	<b>RX Packets</b>	
		140409	4214	

Detailed explanation is shown below:

Item	Description
<b>IP Address</b>	Displays the IP address of the LAN interface.
<b>TX Packets</b>	Displays the total transmitted packets at the LAN interface.
<b>RX Packets</b>	Displays the total number of received packets at the LAN interface.
<b>TX Bytes</b>	Displays the total transmitted size at the LAN interface.
<b>RX Bytes</b>	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 DrayTek VigorAP 910C web interface. The top header shows the DrayTek logo and the device model 'VigorAP 910C'. On the left, there is a navigation menu with options like 'Quick Start Wizard', 'Online Status', 'Operation Mode', 'LAN', 'Wireless LAN (2.4GHz)', 'Wireless LAN (5GHz)', 'RADIUS Setting', 'Objects Setting', 'Applications', 'Mobile Device Management', 'System Maintenance', 'Diagnostics', and 'Support Area'. The main content area is titled 'System Status' and contains the following information:

**System Status**

Model : VigorAP910C  
Device Name : VigorAP910C  
Firmware Version : 1.3.2  
Build Date/Time : r11839 Thu Mar 26 11:56:32 CST 2020  
System Uptime : 06 00:14:18  
Operation Mode : AP

System	
Memory Total	: 62320 kB
Memory Left	: 16416 kB
Cached Memory	: 26576 kB / 62320 kB

LAN	
MAC Address	: 00:1D:AA:7C:CF:A4
IP Address	: 192.168.1.20
IP Mask	: 255.255.255.0

**Wireless LAN (2.4GHz)**

MAC Address : 00:1D:AA:7C:CF:A4  
SSID : DrayTek  
Channel : 11  
Driver Version : 2.7.2.0

**Wireless LAN (5GHz)**

MAC Address :  
SSID : DrayTek5G  
Channel : 36  
Driver Version : 10.2.85

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

At the bottom left, it indicates 'Admin mode' 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 :**  
VigorAP 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 :**  
VigorAP will connect to another VigorAP which uses the same mode, and all wired Ethernet clients of both VigorAPs will be connected together.
- AP Bridge-Point to Multi-Point :**  
VigorAP will connect to up to four VigorAPs which uses the same mode, and all wired Ethernet clients of every VigorAPs will be connected together.
- AP Bridge-WDS :**  
VigorAP will connect to up to four VigorAPs which uses the same mode, and all wired Ethernet clients of every VigorAPs will be connected together.  
This mode is still able to accept wireless clients.
- Universal Repeater :**  
VigorAP can act as a wireless repeater; it can be Station and AP at the same time.

#### Wireless LAN (5GHz)

- AP :**  
VigorAP acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.
- AP Bridge-WDS :**  
VigorAP will connect to up to four VigorAPs which uses the same mode, and all wired Ethernet clients of every VigorAPs will be connected together.  
This mode is still able to accept wireless clients.
- Universal Repeater :**  
VigorAP can act as a wireless repeater; it can be Station and AP at the same time.

OK

Available settings are explained as follows:

Item	Description
<b>Wireless LAN(2.4GHz)</b>	
<b>AP</b>	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
<b>Station-Infrastructure</b>	Enable the Ethernet device such as TV and Game player connected to the VigorAP 910C to an access point.
<b>AP Bridge-Point to Point</b>	This mode can establish wireless connection with another VigorAP 910C using the same mode, and link the wired network which these two VigorAP 910Cs connected together. Only one access point can be connected in this mode.
<b>AP Bridge-Point to Multi-Point</b>	This mode can establish wireless connection with other VigorAP 910Cs using the same mode, and link the wired network which these VigorAP 910Cs connected together. Up to 4 access points

	can be connected in this mode.
<b>AP Bridge-WDS</b>	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.
<b>Universal Repeater</b>	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.
<b>Wireless LAN(5GHz)</b>	
<b>AP</b>	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
<b>AP Bridge-WDS</b>	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.
<b>Universal Repeater</b>	This product can act as a wireless range extender that will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.

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

## 3.2 LAN

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



### 3.2.1 General Setup

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.

Ethernet TCP / IP and DHCP Setup

<p><b>LAN IP Network Configuration</b></p> <p><input checked="" type="checkbox"/> Enable DHCP Client</p> <p>IP Address: <input type="text" value="192.168.1.11"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p>Default Gateway: <input type="text" value="192.168.1.33"/></p> <hr/> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID: <input type="text" value="0"/></p>	<p><b>DHCP Server Configuration</b></p> <p><input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>For DHCP Client</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>Primary DNS Server: <input type="text"/></p> <p>Secondary DNS Server: <input type="text"/></p>
--	--

<p><b>DNS Server IP Address</b></p> <p>Primary IP Address: <input type="text"/></p> <p>Secondary IP Address: <input type="text"/></p>
---

Available settings are explained as follows:

Item	Description
<p><b>LAN IP Network Configuration</b></p>	<p><b>Enable DHCP Client</b> – When it is enabled, VigorAP 910C will be treated as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2862).</p> <p><b>IP Address</b> – Type in private IP address for connecting to a local private network (Default: 192.168.1.2).</p> <p><b>Subnet Mask</b> – Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p><b>Default Gateway</b> - In general, it is not really necessary to specify a gateway for VigorAP 902. However, if it is required, simply type an IP address as the gateway for VigorAP 902. It will be convenient for the access point to acquire more service (e.g., accessing NTP server) from Vigor router.</p> <p><b>Enable Management VLAN</b> – VigorAP 910C supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 910C.</p> <ul style="list-style-type: none"> <li>● <b>VLAN ID</b> – Type the number as VLAN ID tagged on the transmitted packet. “0” means no VALN tag.</li> </ul>
<p><b>DHCP Server Configuration</b></p>	<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><b>Enable Server</b> – When it is enabled, VigorAP will assign required information (e.g., IP address, DNS server) to every host in LAN.</p>

	<ul style="list-style-type: none"> <li>● <b>Start IP Address</b> - 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.</li> <li>● <b>End IP Address</b> - Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.</li> <li>● <b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</li> <li>● <b>Default Gateway</b> - Enter a value of the gateway IP address for the DHCP server.</li> <li>● <b>Lease Time</b> - It allows you to set the leased time for the specified PC.</li> <li>● <b>Primary DNS Server</b> - 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.</li> <li>● <b>Secondary DNS Server</b> - 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.</li> </ul> <p><b>Disable Server</b> - Disable Server lets you manually use other DHCP server to assign IP address to every host in the LAN.</p> <ul style="list-style-type: none"> <li>● <b>Trust DHCP Server IP for WLAN</b> - When the built-in DHCP server of VigorAP is disabled, the wireless client might get IP address from other DHCP server. Sometimes, it might cause wireless client obtaining wrong IP or unable to access internet. To solve this problem, simply specify a DHCP server in this field. Then, the wireless client connecting to such VigorAP will get IP address from this specified DHCP server only.</li> </ul> <p><b>Relay Agent</b> - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.</p> <ul style="list-style-type: none"> <li>● <b>DHCP Relay Agent</b> - 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.</li> </ul>
<p><b>DNS Server IP Address</b></p>	<p>Set the DNS server IP address for VigorAP.</p> <ul style="list-style-type: none"> <li>● <b>Primary IP Address</b>- 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.</li> <li>● <b>Secondary IP Address</b>- You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP</li> </ul>

	does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
--	--

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



### 3.2.2 Web Portal

This page allows you to configure a profile with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router. No matter what the purpose of the wireless/LAN client is, he/she will be forced into the URL configured here while trying to access into the Internet or the desired web page through this router. That is, a company which wants to have an advertisement for its products to users can specify the URL in this page to reach its goal.

LAN >> Web Portal

Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1	<input type="checkbox"/>		None		Preview
2	<input type="checkbox"/>		None		Preview
3	<input type="checkbox"/>		None		Preview
4	<input type="checkbox"/>		None		Preview

**Note:** The AP must connect to the Internet before webpage redirection will work.

OK Cancel

Each item is explained as follows:

Item	Description
<b>Index</b>	Display the number link which allows you to configure the profile.
<b>Enable</b>	Check the box to enable such profile.
<b>Comments</b>	Display the content (Disable, URL Redirect or Message) of the profile.
<b>Login Mode</b>	Display the login mode that a client uses to access into Internet.
<b>Interface</b>	Display the applied interfaces of the profile.
<b>Preview</b>	Open a preview window according to the configured settings.

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

To configure the profile, click any index number link to open the following page.

LAN >> Web Portal

**Web Portal**

**Enable**

**Comments**

**Welcome message**

(Max 1024 characters)

**Redirect Page**

None

URL:

**Authentication**

None

Button Click

**Applied Interfaces**

LAN  LAN (Works on universal repeater mode)

WLAN 2.4GHz  SSID1 (DrayTek)

SSID2

SSID3

SSID4

WLAN 5GHz  SSID1 (DrayTek5G)

SSID2

SSID3

SSID4

**Note:** The AP must connect to the Internet before webpage redirection will work.

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check the box to enable this function.
<b>Comments</b>	Enter a brief comment to explain such web portal profile.
<b>Welcome message</b>	Enter words or sentences here. The message will be displayed on the screen for several seconds when the wireless users access into the web page through the router. <ul style="list-style-type: none"> <li>● <b>Default</b> – Click it to restore the default content.</li> </ul>
<b>Redirect Page</b>	<b>None</b> - User can access into Internet directly. <b>URL Redirect</b> - Any user who wants to access into Internet through this router will be redirected to the URL specified here first. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit.
<b>Authentication</b>	<b>None</b> – User can access into Internet directly without authentication. <b>Button Click</b> – When a client tries to access into Internet, a welcome message page with a button named “Accept” will appear on the screen first. The client must click that button (Accept) and then he/she is allowed to access Internet.
<b>Applied Interfaces</b>	Check the box(es) representing different interfaces to be applied by such profile.

- 
- |  |
|--|
| <ul style="list-style-type: none"><li>● <b>LAN</b> – If it is selected and Universal Repeater is specified as connection mode for such AP, both LAN client and WLAN client can access into Internet via web portal. Yet, if AP mode is selected, only wireless LAN client shall access into Internet via web portal.</li><li>● <b>WLAN 2.4GHz/5GHz</b> - The advantage is that each SSID (1/2/3/4) for wireless network can be applied with different web portal separately.</li></ul> |
|--|
- 

After finishing all the settings here, please click **OK** to save the configuration.

### 3.3 Central AP Management

Central AP Management allows you to configure VigorAP 910C to be managed by Vigor2862 series.

**WLAN Setting**

SSID: S501, S502, S503, S504, 2.4G SSID

Active:  Enable  Disable

SSID: Draytek-LAN-A, LAN-A, Hide SSID

VLAN: (1-UPDg)

Include:  From Member

Security Settings

WPA-WPA2-PSK

set up: 802.1X, 802.1X is enabled.

WPA:  TKIP  AES  TKIP/AES

Pass Phrase: \_\_\_\_\_

Key Renewal Interval: 3600 Seconds

PMK Cache Period: 30 Minutes

Pre-Authentication:  Enable  Disable

WEP: Setup WEP Key if WEP is enabled. 802.1X WEP:  Enable  Disable

**Vigor Router**

**AP Status**

Index	Device Name	IP Address	SSID	Ch.	Encryption	WL Clients	Firmware	Password
1	AP800-1A2B3C	192.168.254.253	Draytek-pp	Auto(ch13)	802.1x(WPA/WPA2)	10/64	1.1.01	Password
2	AP800-5F	192.168.254.230	Draytek-hw	ch13	WPA2-AES	---	1.1.0	Password
3	AP800-1F2A	192.168.254.112	Draytek-1234567	ch6	None	2/64	1.1.0	Password

Note: Green: Online Red: Offline Gray: Hidden SSID

**Central AP Management**

- General Setup
- APM Log
- Overload Management
- Status of Settings
- Wireless LAN (2.4GHz)

#### 3.3.1 General Setup

Central AP Management >> General Setup

Vigor AP Managemet

- Enable AP Management
- Enable Auto Provision

OK

Cancel

Note: LAN-B cannot support APM feature.

Available settings are explained as follows:

Item	Description
<b>Enable AP Management</b>	Check the box to enable the function of AP Management.
<b>Enable Auto Provision</b>	VigorAP 910C can be controlled under Central AP Management in Vigor2862 series. When both Vigor2862 series and VigorAP 910C have such feature enabled, once VigorAP 910C is registered to Vigor2862 series, the <b>WLAN profile</b> pre-configured on VigorAP2862 series will be applied to VigorAP 910C immediately. Thus, it is not necessary to configure VigorAP 910C separately.

### 3.3.2 APM Log

This page will display log information related to wireless stations connected to VigorAP 910C and central AP management.

Such information also will be delivered to Vigor router (e.g., Vigor2862 or Vigor2926 series) and be shown on **Central AP Management>>Event Log** of Vigor router.

Central AP Management >> APM Log

APM Log Information

| [Clear](#) | [Refresh](#) |  Line wrap |

```
0d 00:31:52 syslog: [APM] Get the 'Query AP status' Request.
0d 00:32:53 syslog: [APM] Get the 'Query AP status' Request.
0d 00:33:53 syslog: [APM] Get the 'Query AP status' Request.
0d 00:34:53 syslog: [APM] Get the 'Query AP status' Request.
0d 00:35:53 syslog: [APM] Get the 'Query AP status' Request.
0d 00:36:53 syslog: [APM] Get the 'Query AP status' Request.
0d 00:37:53 syslog: [APM] Get the 'Query AP status' Request.
0d 00:38:54 syslog: [APM] Get the 'Query AP status' Request.
0d 00:39:54 syslog: [APM] Get the 'Query AP status' Request.
0d 00:40:54 syslog: [APM] Get the 'Query AP status' Request.
```

### 3.3.3 Overload Management

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 910C) registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

However, traffic overload might be occurred if too many wireless stations connected to VigorAP 910C for data incoming and outgoing. Therefore, “Force Overload Disassociation” is required to terminate the network connection of the client’s station to release network traffic. When the function of “Force Overload Disassociation” in web user interface of Vigor router (e.g., Vigor2862 or Vigor2926 series) is enabled, wireless clients specified in **black list** of such web page will be disassociated to solve the problem of traffic overload.

The following web page is used to configure white list and black list for wireless stations.

Overload Management

**MAC Address Filter of Force Overload Disassociation**

	Index	MAC Address	Comment
<b>White List</b>			
<b>Black List</b>			

Client's MAC Address :  :  :  :  :  :

Apply to : White List ▼

Comment :

**Note:** When force overload disassociation is enabled, clients in black list will be disassociated first. Clients in white list will not be disassociated.

Available settings are explained as follows:

Item	Description
<b>White List/Black List</b>	Display the information (such as index number, MAC address and comment) for all of the members in White List/Black List.  Wireless stations listed in Black List will be forcefully disconnected first when traffic overload occurs and “Force Overload Disassociation” is enabled.
<b>Client’s MAC Address</b>	Specify the MAC Address of the remote/local client.
<b>Apply to</b>	<b>White List</b> – MAC address listed inside Client’s MAC Address will be categorized as one of members in White List.  <b>Black List</b> - MAC address listed inside Client’s MAC Address will be categorized as one of members in Black List.
<b>Comment</b>	Type any words as notification.
<b>Add</b>	Add a new MAC address into the White List/Black List.
<b>Delete</b>	Delete the selected MAC address in the White List/Black List.
<b>Edit</b>	Edit the selected MAC address in the White List/Black List.
<b>Cancel</b>	Give up the configuration.

### 3.3.4 Status of Settings

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP910C) registered to Vigor2862 or Vigor2926 series. This web page displays the settings related to Load Balance for VigorAP 910C. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor2862 or Vigor2926 series.

Central AP Management >> Status of Settings

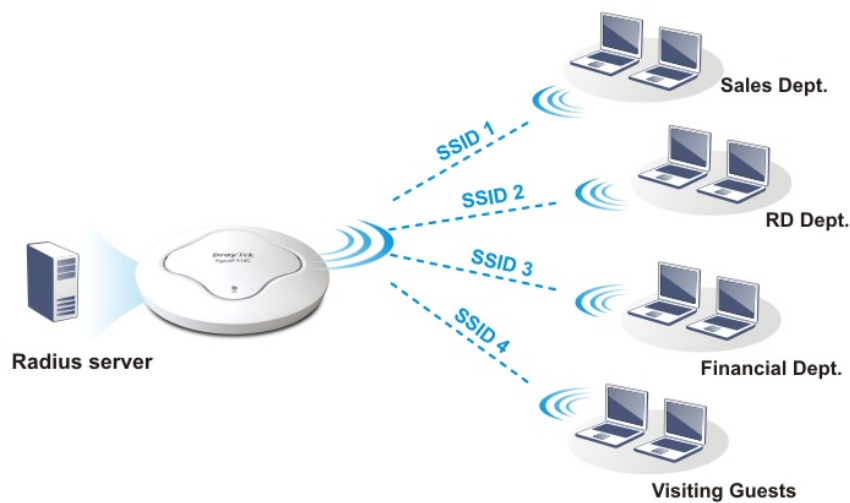
Function Name	Status	Value
<b>Load Balance</b>		
Station Number Threshold	X	
Max WLAN(2.4GHz) Station Number		64
Max WLAN(5GHz) Station Number		64
Traffic Threshold	X	
Upload Limit		None bps
Download Limit		None bps
Force Overload Disassociation	X	
Disassociate By		None
RSSI Threshold		-50 dBm
<b>Rogue AP Detection</b>		
Rogue AP Detection	X	

### 3.4 General Concepts for Wireless LAN (2.4GHz/5GHz)

VigorAP 910C is equipped with a wireless LAN interface compliant with 5GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. To boost its performance further, the VigorAP 910C 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 910C 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 910C. 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 910C 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 910C) with the encryption of WPA and WPA2.

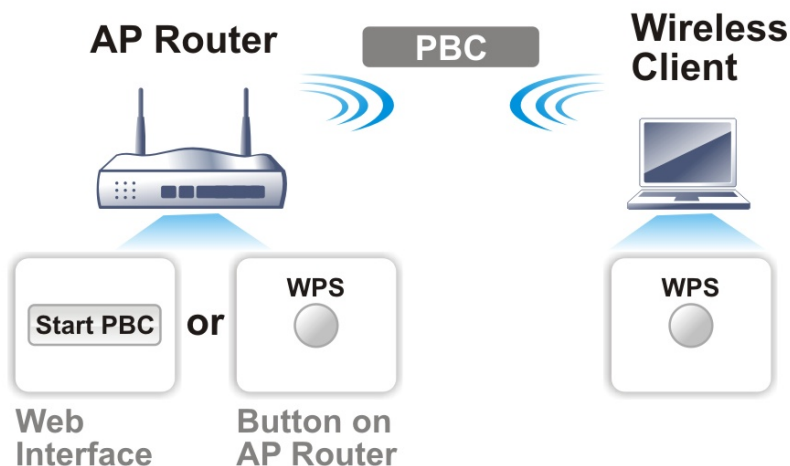
It is the simplest way to build connection between wireless network clients and VigorAP 910C. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 910C automatically.



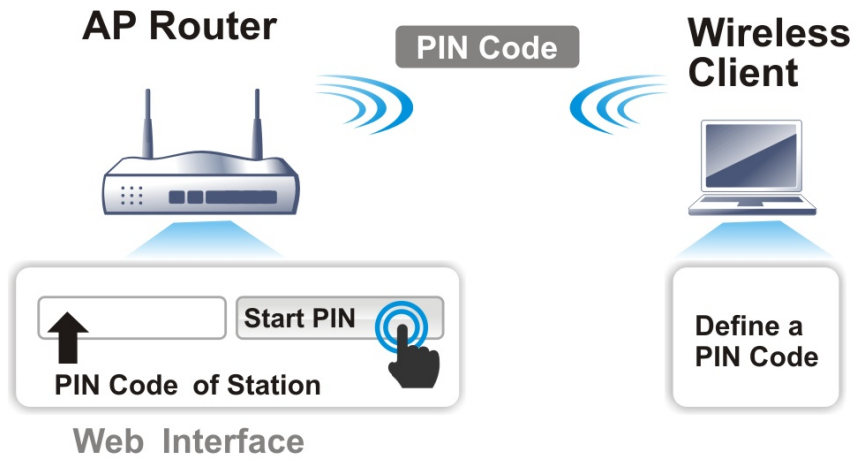
**Note:** Such function is available for the wireless station with WPS supported.

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 910C series which served as an AP, press **WPS** button once on the front panel of VigorAP 910C 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.

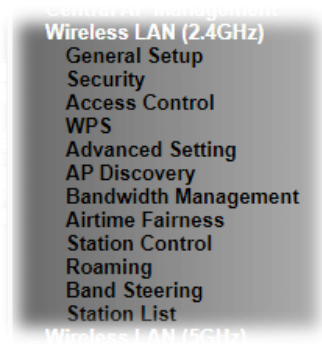


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 910C.



### 3.5 Wireless LAN (2.4GHz) Settings for AP Mode

When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering and Station List.



**Note:** The **Wireless LAN (2.4GHz)** 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.

Wireless LAN (2.4GHz) >> General Setup

---

General Setting ( IEEE 802.11 )

Enable Wireless LAN

Enable Client Limit  (3 ~ 64, default: 64)

Enable Client Limit per SSID (3 ~ 64, default: 64)

---

Mode :

Channel :

Extension Channel :

---

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	VLAN ID
1	<input type="checkbox"/>	<input type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Hide SSID: Prevent SSID from being scanned.  
 Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.  
 Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.  
 Isolate Exception: Isolate Exception can be created by adding the MAC from [Device Object](#).

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Client Limit</b>	Check the box to set the maximum number of wireless stations

	which try to connect Internet through Vigor AP. The number you can set is from 3 to 64.
<b>Enable Client Limit per SSID</b>	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
<b>Mode</b>	VigorAP 910C can connect to stations supporting 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) for 2.4GHz simultaneously.
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above. Configure the extension channel you want.
<b>Enable</b>	Check the box to enable the SSID configuration.
<b>Hide SSID</b>	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 44information except SSID or just cannot see any thing about VigorAP 910C while site surveying. The system allows you to set three sets of SSID for different usage.
<b>SSID</b>	Set a name for VigorAP 910C to be identified. Default settings are DrayTek.
<b>Isolate LAN</b>	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.  If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.

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.

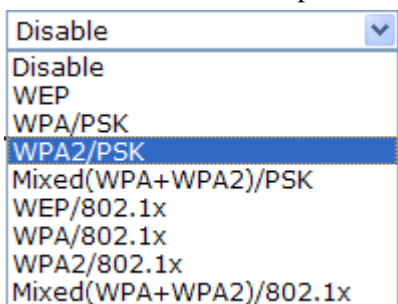
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek			
Mode: Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
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	
EAPOL Key Retry		<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
<b>WEP</b>			
<input type="radio"/> Key 1 :	<input type="text"/>	<input type="text"/>	Hex
<input checked="" type="radio"/> Key 2 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text"/>	Hex
802.1x WEP		<input type="radio"/> Disable <input type="radio"/> Enable	

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are several modes provided for you to choose.</p>  <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - 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><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 910C 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><b>WPA/802.1x</b> - 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><b>WPA2/802.1x</b> - 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>
<b>WPA Algorithms</b>	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Pass Phrase</b>	Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key Renewal Interval</b>	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 <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>EAPOL Key Retry</b>	EAPOL means Extensible Authentication Protocol over LAN. <b>Enable</b> - The default setting is "Enable". It can make sure that the key will be installed and used once in order to prevent key reinstallation attack.
<b>Key 1 – Key 4</b>	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 <b>WEP</b> mode. <div data-bbox="635 1883 762 1995" style="border: 1px solid black; padding: 2px; margin-top: 10px;"> Hex <input type="button" value="v"/>  ASCII  Hex </div>

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

<b>Item</b>	<b>Description</b>
<b>Use internal RADIUS Server</b>	<p>There is a RADIUS server built in VigorAP 910C 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, <b>3.13 RADIUS Server</b> to configure settings for internal server of VigorAP 910C.</p>
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	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.
<b>Session Timeout</b>	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

---

SSID 1	SSID 2	SSID 3	SSID 4						
SSID: DrayTek Policy: <input type="text" value="Disable"/>									
<b>MAC Address Filter</b>									
<table border="1"> <thead> <tr> <th>Index</th> <th>MAC Address</th> <th>access comment</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="height: 100px;"> </td> </tr> </tbody> </table>				Index	MAC Address	access comment			
Index	MAC Address	access comment							
<input type="radio"/> MAC <input checked="" type="radio"/> Object Device Group: <input type="text" value="None"/> or Device Object: <input type="text" value="None"/>									
<input type="button" value="Add"/> 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="text" value="選擇檔案"/> 未選擇任何檔案 <input type="button" value="Restore"/>							

Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , 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 910C. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">             Activate MAC address filter ▼              Disable              Activate MAC address filter              Blocked MAC address filter           </div>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>MAC</b>	<b>Client's MAC Address</b> - Manually enter the MAC address of wireless client. <b>Add</b> - Add a new MAC address into the list. <b>Delete</b> - Delete the selected MAC address in the list. <b>Edit</b> - Edit the selected MAC address in the list.
<b>Object</b>	In addition to enter the MAC address of the device manually, you can <b>Device Group</b> - Select one of the existed device groups and




	click <b>Add</b> . All the devices belonging to the selected group will be shown on the MAC Address Filter table. <b>Device Object</b> - Select one of the existed device object and click <b>Add</b> . The MAC address of the device will be shown on the MAC Address Filter table.
<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	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


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES


#### Device Configure

<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<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
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 910C is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 910C. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 910C.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 910C will wait for WPS requests from wireless clients about two minutes. (You need to setup WPS

	within two minutes)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. (You need to setup WPS within two minutes).

### 3.5.5 Advanced Setting

This page is to determine which algorithm will be selected for wireless transmission rate.

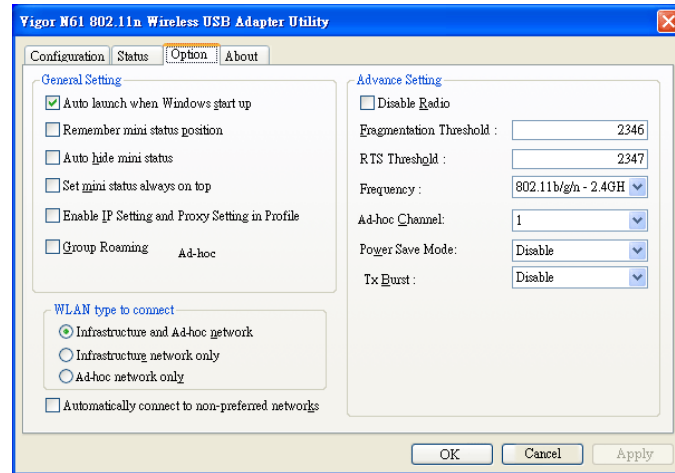
Wireless LAN (2.4GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 40 MHz
Packet-OVERDRIVE™ Tx Burst	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (For 11g mode only)
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Rate Adaptation Algorithm	<input checked="" type="radio"/> New <input type="radio"/> Old
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)
Auto Channel Reselect	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Auto Channel Filtered Out List	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
<b>MAC Clone:</b>	Set the MAC address of SSIDs and the Wireless client. Please notice that the last byte of this MAC address must be a multiple of 8.

Available settings are explained as follows:

Item	Description
<b>Channel Bandwidth</b>	<p><b>20 MHz-</b> VigorAP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHz -</b> VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz) shall be used to meet the air situation. Usually, 40MHz would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), 20MHz will be used by VigorAP automatically to ensure smooth network transmission.</p> <p><b>40 MHz -</b> VigorAP will use 40MHz for data transmission and receiving between the AP and the stations.</p>
<b>Packet-OVERDRIVE</b>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). 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><b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching</p>

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



<b>Antenna</b>	VigorAP 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.
<b>Tx Power</b>	The default setting is the maximum (100%). Lowering down the value may degrade range and throughput of wireless.
<b>Rate Adaptation Algorithm</b>	Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.
<b>Fragment Length</b>	Set the Fragment threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2346.
<b>RTS Threshold</b>	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2347.
<b>Country Code</b>	VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
<b>Auto Channel Reselect</b>	Enable – Usually, wireless channel determined by AutoSelect ( <b>Wireless LAN&gt;&gt;General Setup</b> ) means Vigor router will search for a channel with low interference automatically once the system reboots. However, when the channel utilization is more than 70% (refer to <b>Diagnostics &gt;&gt; Interference Monitor</b> ), Vigor router will search for and switch another channel with low interference to obtain better wireless signal again.
<b>Auto Channel Filtered Out List</b>	The selected wireless channels will be discarded if <b>AutoSelect</b> is selected as <b>Channel</b> selection mode in <b>Wireless LAN&gt;&gt;General Setup</b> .

<b>IGMP Snooping</b>	Check <b>Enable</b> to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
<b>Isolate 2.4GHz and 5GHz bands</b>	The default setting is “Enable”. It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.  For WLAN 2.4GHz and 5GHz set with the same SSID name: <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	The default setting is “Disable”. If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>MAC Clone</b>	Click <b>Enable</b> 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.

### 3.5.6 AP Discovery

VigorAP 910C 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.

## Access Point List

 Enable AP Monitor Mode

Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Mode	Ch. Width
1	staffs_5F	00:1d:aa:3d:af:d6	70%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
2	Michael_2G	00:1d:aa:fe:fa:58	24%	1	NONE		11b/g/n	20
3	DrayTek_CC...	00:1d:aa:f8:c9:c8	39%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
4	RD2_Kyle_2...	00:1d:aa:c3:3f:00	76%	6	NONE		11b/g/n	20
5	RD8_ACS_TE...	00:1d:aa:f7:a9:00	44%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
6	DrayTek-LA...	00:50:7f:f0:d5:c0	24%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
7	staffs_6F	00:1d:aa:55:87:38	44%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
8	staffs_4F	00:1d:aa:9d:68:ac	44%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
9	staffs	02:1d:aa:9d:68:ac	34%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
10	guests	0a:1d:aa:9d:68:ac	34%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
11	RMA Test	00:50:7f:52:2f:58	34%	11	TKIP/AES	WPA/PSK	11b/g/n	40
12	DrayTek-LA...	00:50:7f:52:2f:59	39%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
13	AP910C-PQC...	00:1d:aa:26:8d:30	29%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
14	1111111111	00:1d:aa:7f:4f:20	34%	11	NONE		11b/g/n	40
15		02:1d:aa:7c:4f:20	24%	11	NONE		11b/g/n	40
16	Draytek5G	00:1d:aa:7f:5d:58	39%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
17	RD2_Test_J...	00:1d:aa:f3:16:d0	39%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
18	AP900-PQC-...	00:1d:aa:7e:87:c8	34%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
19	AP900 PQC ...	00:1d:aa:9c:f0:58	39%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
20	AP902-PQC-...	00:1d:aa:67:05:10	39%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
21	DrayTek-LA...	02:1d:aa:7e:87:c8	34%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
22	AP910C-PQC...	00:1d:aa:7f:54:14	0%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40

See [Channel Statistics](#)**Note:** During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

Each item is explained as follows:

Item	Description
<b>Enable AP Monitor Mode</b>	This function can help to get and keep the records of APs detected by such device after clicking Scan.  In general, only the available AP will be detected by Vigor device. Once the AP is unavailable, it will be deleted from the Access Point List immediately. However, if such function is enabled, the system will keep the record of the AP (once detected by Vigor device) until it is available for Vigor device again.
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 910C.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 910C.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 910C.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Mode</b>	Display the wireless connection mode that the scanned AP used.
<b>Ch. Width</b>	Display the channel width that the scanned AP used.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.

### 3.5.7 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	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<input checked="" type="checkbox"/>		
Upload Limit	1M		bps
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment	<input checked="" type="checkbox"/>		
Total Upload Limit	User defined	K	bps (Default unit : K)
Total Download Limit	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
<b>SSID</b>	Display the specific SSID name of the AP.
<b>Enable</b>	Check this box to enable the bandwidth management for clients.
<b>Upload Limit</b>	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor AP with the same SSID. Use the drop down list to choose the rate. If you choose <b>User defined</b> , you have to specify the rate manually.
<b>Download Limit</b>	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor AP with the same SSID. Use the drop down list to choose the rate. If you choose <b>User defined</b> , you have to specify the rate manually.
<b>Auto Adjustment</b>	Check this box to have the bandwidth limit determined by the system automatically.
<b>Total Upload Limit</b>	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.
<b>Total Download Limit</b>	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.

### 3.5.8 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

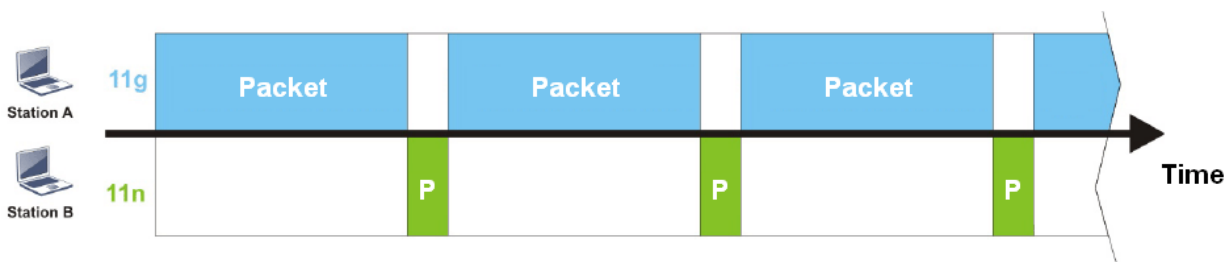
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

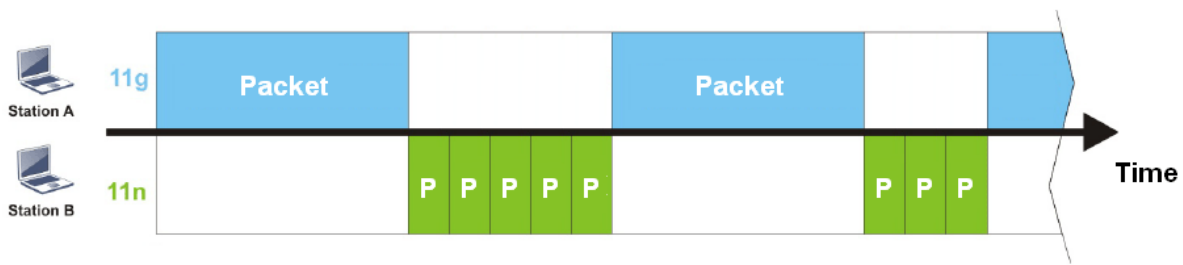
The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 910C. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 910C. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

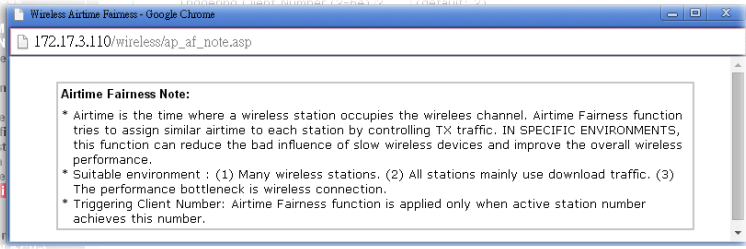
- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

**Wireless LAN (2.4GHz) >> Airtime Fairness**

Enable **Airtime Fairness**  
 Triggering Client Number  (2 ~ 64, Default: 2)

**Note:** Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Available settings are explained as follows:

Item	Description
<b>Enable Airtime Fairness</b>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p><b>Airtime Fairness</b> – Click the link to display the following screen of airtime fairness note.</p>  <p><b>Triggering Client Number</b> – Airtime Fairness function is applied only when active station number achieves this number.</p>

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



**Note:** Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

### 3.5.9 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect VigorAP. If such function is not enabled, the wireless client can connect VigorAP until it shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

**Note:** Up to 300 Wireless Station records are supported by VigorAP.

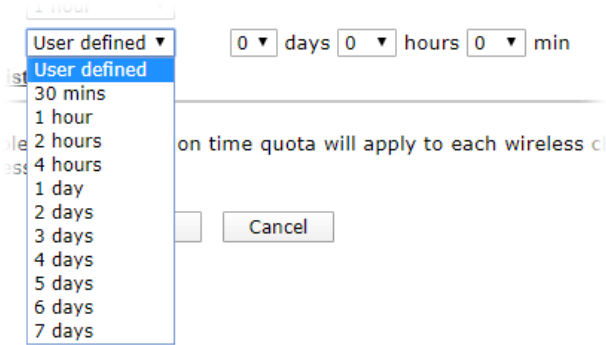
Wireless LAN (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek		
Enable	<input type="checkbox"/>		
Connection Time	1 hour		
Reconnection Time	1 day		
<a href="#">Display All Station Control List</a>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

OK Cancel

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID that the wireless station will use it to connect with Vigor router.
<b>Enable</b>	Check the box to enable the station control function.
<b>Connection Time / Reconnection Time</b>	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose <b>User defined</b> . 
<b>Display All Station Control List</b>	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.

After finishing all the settings here, please click **OK** to save the configuration.

### 3.5.10 Roaming

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

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

#### Wireless LAN (2.4GHz) >> Roaming

##### AP-assisted Client Roaming Parameters

<input type="checkbox"/> <b>Minimum Basic Rate</b>	1	Mbps
<input checked="" type="radio"/> Disable RSSI Requirement		
<input checked="" type="radio"/> <b>Strictly Minimum RSSI</b>	-73	dBm (42%) (Default: -73)
<input type="radio"/> <b>Minimum RSSI</b>	-66	dBm (60%) (Default: -66)
with Adjacent AP RSSI over	5	dBm (Default: 5)

##### Fast Roaming(WPA/802.1x)

<input type="checkbox"/> Enable	
<b>PMK Caching</b> : Cache Period	10 minute(s) (10 ~ 600) (Default: 10)
<b>Pre-Authentication</b>	

OK Cancel

Available settings are explained as follows:

Item	Description
<b>AP-assisted Client Roaming Parameters</b>	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 910C will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p><b>Minimum Basic Rate</b> – Check the box to use the drop down list to specify a basic rate (<b>Mbps</b>). When the link rate of the wireless station is below such value, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Disable RSSI Requirement</b> - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p><b>Strictly Minimum RSSI</b> - VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (<b>dBm</b>) set here, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Minimum RSSI</b> - When the signal strength of the wireless station is below the value (<b>dBm</b>) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of <b>With Adjacent AP RSSI over</b>) is detected by VigorAP 910C, VigorAP 910C will terminate the network connection for that wireless station. Later,</p>

	<p>the wireless station can connect to the adjacent AP (with better RSSI).</p> <ul style="list-style-type: none"> <li>● <b>With Adjacent AP RSSI over</b> – Specify a value as a threshold.</li> </ul>
<p><b>Fast Roaming (WPA/802.1x)</b></p>	<p><b>Enable</b> – Check the box to enable fast roaming configuration.</p> <p><b>PMK Cache Period</b> - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for <b>WPA2/802.1</b> mode.</p> <p><b>Pre-Authentication</b> - 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)</p>

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

### 3.5.11 Band Steering

Band Steering detects if the wireless clients are capable of 5GHz operation, and steers them to that frequency. It helps to leave 2.4GHz band available for legacy clients, and improves users experience by reducing channel utilization.



If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



**Note:** To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

Open **Wireless LAN (2.4GHz)>>Band Steering** to get the following web page:

**Wireless LAN (2.4GHz) >> Band Steering**

Enable **Band Steering**

Check Time for WLAN Client 5G Capability  seconds (1 ~ 60, Default: 15)

5GHz Minimum RSSI  dBm ( %) (Default: -78)

(Only do band steering when 5GHz signal is better than Minimum RSSI)

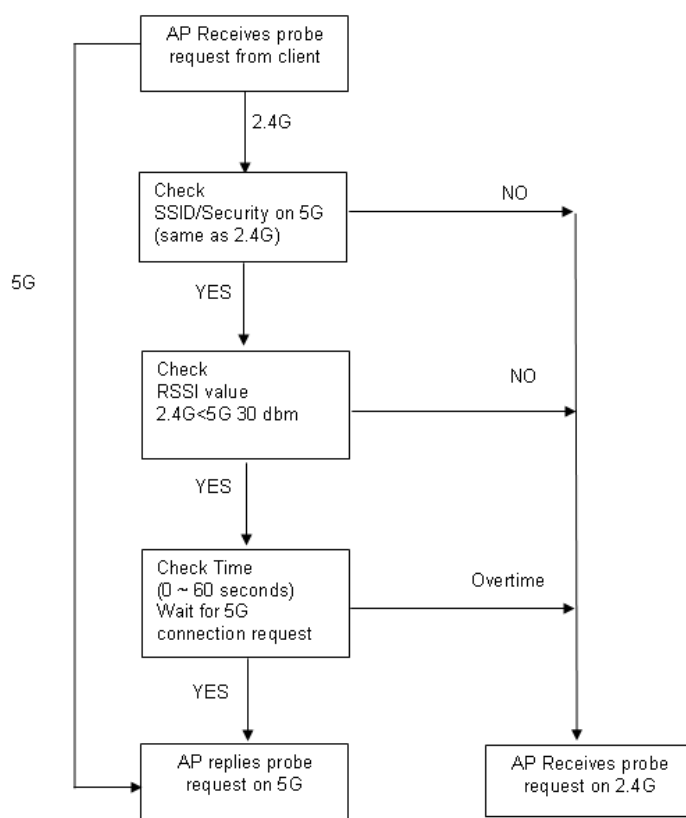
**Note:** Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
<b>Enable Band Steering</b>	<p>If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit.</p> <p><b>Check Time</b>.... – If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for VigorAP to detect the wireless client.</p> <p><b>5GHz Minimum RSSI</b> – The wireless station has the capability of 5GHz network connection, yet the signal performance might not be satisfied. Therefore, when the signal strength is below the value set here while the wireless station is connecting to VigorAP, VigorAP will allow the client to connect to 2.4GHz network.</p>

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

Below shows how Band Steering works.



## How to Use Band Steering?

1. Open **Wireless LAN(2.4GHz)>>Band Steering**.
2. Check the box of **Enable Band Steering** and use the default value (15) for check time setting.

### Wireless LAN (2.4GHz) >> Band Steering

<input checked="" type="checkbox"/> Enable <b>Band Steering</b>	
Check Time for WLAN Client 5G Capability	<input type="text" value="15"/> seconds (1 ~ 60, Default: 15)
<input type="checkbox"/> 5GHz Minimum RSSI	<input type="text" value="-78"/> dBm ( <input type="text" value="29"/> %) (Default: -78)
(Only do band steering when 5GHz signal is better than Minimum RSSI)	

**Note:** Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

3. Click **OK** to save the settings.

- Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>>General Setup**. Configure SSID as *ap910C-BandSteering* for both pages. Click **OK** to save the settings.

**Wireless LAN (2.4GHz) >> General Setup**

**General Setting ( IEEE 802.11 )**

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

Mode :

	Hide SSID	SSID	Isolate Member	VLAN ID (0:Untagged)	MAC Clone
1	<input type="checkbox"/>	<input type="text" value="ap910C-BandSteering"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text"/>

**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

Same value for 2.4GHz and 5GHz

**Wireless LAN (5GHz) >> General Setup**

**General Setting ( IEEE 802.11 )**

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

Mode :

	Hide SSID	SSID	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="text" value="ap910C-BandSteering"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="text"/>	<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 :   
 Details : 20MHz / 40MHz Ext Ch: 40 , 80MHz Center Ch: 42

- Open **Wireless LAN (2.4GHz)>>Security** and **Wireless LAN (5GHz)>>Security**. Configure Security as *12345678* for both pages. Click **OK** to save the settings.

**Wireless LAN (2.4GHz) >> Security Settings**

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap910C-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
<b>WEP</b>			
<input type="radio"/> Key 1 : <input type="text"/> Hex			
<input type="radio"/> Key 2 : <input type="text"/> Hex			
<input type="radio"/> Key 3 : <input type="text"/> Hex			
<input type="radio"/> Key 4 : <input type="text"/> Hex			
802.1x WEP			
<input type="radio"/> Disable <input type="radio"/> Enable			

Same value for 2.4GHz and 5GHz

**Wireless LAN (5GHz) >> Security Settings**

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap910C-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
PMK Cache Period			
10 minutes			
Pre-Authentication			
<input type="radio"/> Disable <input type="radio"/> Enable			
<b>WEP</b>			
<input checked="" type="radio"/> Key 1 : <input type="text"/> Hex			
<input type="radio"/> Key 2 : <input type="text"/> Hex			
<input type="radio"/> Key 3 : <input type="text"/> Hex			
<input type="radio"/> Key 4 : <input type="text"/> Hex			

- Now, VigorAP 910C will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



### 3.5.12 Station List

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

#### General

Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station.

Wireless LAN (2.4GHz) >> Station List

**Station List**

							General	Advanced	Control	Neighbor
Index	MAC Address	Vendor	RSSI	Approx. Distance	SSID	Visit Time				
1	DA:A1:19:E2:65:AD		5% (-88dBm)	141.25m	N/A	0d:0h:				
2	00:50:7F:F0:BD:2B	DrayTek	52% (-69dBm)	15.85m	N/A	0d:0h:				
3	00:50:7F:37:6D:E5	DrayTek	47% (-71dBm)	19.95m	N/A	0d:0h:				
4	1C:4B:D6:8B:9C:00	Azurewav	18% (-83dBm)	79.43m	N/A	0d:1h:				
5	00:15:AF:A5:24:A0	Azurewav	26% (-79dBm)	50.12m	N/A	0d:0h:				
6	B0:34:95:22:50:FD	Apple	47% (-71dBm)	19.95m	N/A	0d:0h:				
7	B4:52:7E:D6:68:9D	Sony	20% (-82dBm)	70.79m	N/A	0d:0h:				
8	00:1F:3C:51:9C:55	Intel	39% (-74dBm)	28.18m	N/A	0d:1h:				

Refresh

**Add to Access Control:**

Client's MAC Address :  :  :  :  :  :

- Note:**
1. Approx. Distance is calculated by actual signal strength of device detected. Inaccuracy might occur based on barrier encountered.
  2. Due to the differences in signal strength for different devices, the calculated value of approximate distance also might be different.
  3. Trademarks and brand names are the properties of their respective owners.

Add

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - 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.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

**Advanced**

Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

**Control**

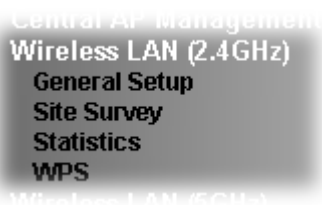
Display connection and reconnection time of the wireless stations.

**Neighbor**

Display more information for the neighboring wireless stations.

## 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 (2.4GHz) >> 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.

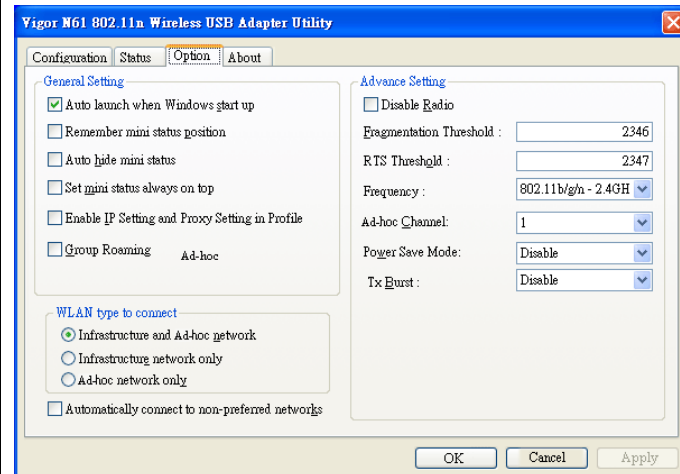
Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Mode</b>	At present, VigorAP 910C 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.
<b>Add</b>	Click this button to add new wireless profiles.
<b>Delete</b>	Click this button to delete the selected wireless profile.
<b>Edit</b>	Click this button to modify the existing wireless profile.
<b>Connect</b>	Click this button to connect the wireless station to AP with the selected profile.

## Packet-OVERDRIVE

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

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



## MAC Clone

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

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.

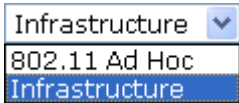
System Configuration	
Profile Name	PROF001
SSID	
Network Type	Infrastructure
Power Saving Mode	<input checked="" type="radio"/> CAM (Constantly Awake Mode) <input type="radio"/> Power Saving Mode
RTS Threshold	<input type="checkbox"/> Used 2347
Fragment Threshold	<input type="checkbox"/> Used 2346

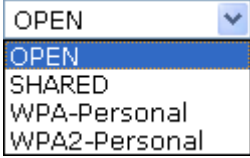

Security Policy	
Security Mode	OPEN

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

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for the new profile.
<b>SSID</b>	Type the name for such access point that can be used for connection by the stations.
<b>Network Type</b>	<p><b>Infrastructure</b> - 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><b>802.11 Ad Hoc</b> – An ad-hoc network is a network where wireless stations can communicate with peer to peer (P2P).</p> 
<b>Power Saving Mode</b>	<p>Choose the power saving mode for such device.</p> <p><b>CAM</b> – Choose this item if it is not necessary to perform</p>

	<p>power saving job.</p> <p><b>Power Saving Mode</b> – Choose this item to get into the power saving status when there is no data passing through the access point.</p>
<b>RTS Threshold</b>	Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.
<b>Fragment Threshold</b>	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
<b>Security Mode</b>	<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><b>OPEN</b> – Open authentication is basically null authentication algorithm, which means that there is no verification of the user.</p> <p><b>SHARED</b> – 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 <b>WPA-Personal</b> or <b>WPA2-Personal</b>, 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><b>WPA Algorithms</b> – Choose Temporal Key Integrity Protocol (TKIP) or AES for data encryption.</p> <p><b>Pass Phrase</b> – Please type 8 to 63 alphanumerical characters here.</p>
<b>WEP</b>	<p><b>WEP Key Length</b> - 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).</p> <p>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>  <p><b>WEP Key Entry Method</b> - There are two types of WEP key</p>



## 3.6.2 Site Survey

The page will list the access points nearby as VigorAP 910C 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	00-1D-AA-74-DA-38	91%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input checked="" type="radio"/>	willjaff	00-EE-BD-B8-C4-60	44%	1	AES	WPA2/PSK
<input type="radio"/>	guests_5F	02-1D-AA-74-DA-38	91%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	DrayTek	00-50-7F-CD-07-48	86%	6	NONE	
<input type="radio"/>	staffs_6F	00-1D-AA-9D-11-A0	65%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	guests_6F	02-1D-AA-9D-11-A0	60%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	staffs_6F8...	06-1D-AA-9D-11-A0	60%	8	TKIP/AES	WPA2
<input type="radio"/>	RD2_Test J...	00-18-E7-E9-60-48	44%	10	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	v2132ac_24...	00-1D-AA-D0-EE-78	15%	10	NONE	
<input type="radio"/>	AP800-s1	00-50-7F-52-2F-58	15%	10	WEP	
<input type="radio"/>	PQC Mark 2...	00-1D-AA-BE-9A-B0	20%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	AndroidApt...	14-A3-64-11-B6-A5	0%	4	AES	WPA2/PSK

Rescan

Connect

Add Profile

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID name of the access point.
<b>BSSID</b>	Display the BSSID (MAC Address) of the access point.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the channel number of the access point.
<b>Encryption</b>	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.
<b>Authentication</b>	Display the authentication type of the access point.
<b>Scan/Rescan</b>	Search the stations connected to such access point.
<b>Connect</b>	Connect to the wireless AP that you choose.
<b>Add Profile</b>	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 (2.4GHz) >> Station Statistics

##### Transmit Statistics

Frames Transmitted Successfully	7245
Frames Transmitted Successfully Without Retry	7245
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	49288
Frames Received With CRC Error	52511
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	2157

[Reset Counters](#)

### 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 910C supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch VigorAP 910C 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 910C, 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 910C will not work for those wireless AP/clients do not support WPS.

To use WPS function to set encrypted connection between VigorAP 910C 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
<input checked="" type="radio"/>	V2710-HW-lanxing	001DAA295D50	34%	11	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.
<input type="radio"/>	DrayTek	001DAABD64E0	60%	6	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.
<input type="radio"/>	DrayTek	001DAAAC47B0	60%	6	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.
<input type="radio"/>	PQC Mark 2830v2 Test 2.4G	001DAABE9AB0	15%	6	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.
<input type="radio"/>	DrayTek	001DAA19AA56	0%	6	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.
<input type="radio"/>	DrayTek-MKT2925	001DAABA0728	39%	6	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.
<input type="radio"/>	VigorBX2000-PQC-2.4G-0	001DAAB0BB88	34%	6	Mixed(WPA+WPA2)/PSK	TKIP/AES	1.0	Unconf.
<input type="radio"/>	RD5_TEST_GW	001DAABDE5C0	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

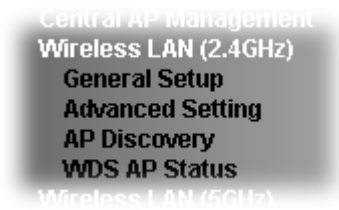
Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID name of the access point.
<b>BSSID</b>	Display the BSSID (MAC Address) of the access point.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Ch. (Channel)</b>	Display the channel number of the access point.
<b>Auth. (Authentication)</b>	Display the authentication type of the access point.
<b>Encrypt (Encryption)</b>	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.
<b>Ver. (Version)</b>	Display the version of WPS.
<b>Status</b>	Display the status of WPS access point.
<b>Refresh</b>	Click this button to refresh the AP site survey.
<b>Start PBC</b>	Click <b>Start PBC</b> to make a WPS connection within 2 minutes.
<b>Start PIN</b>	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.
<b>Renew PIN</b>	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, WDS AP Status and Roaming.



AP Bridge-Point to Point allows VigorAP 910C to connect to **another** VigorAP 910C which uses the same mode. All wired Ethernet clients of both VigorAP 910Cs will be connected together.

Point-to Multi-Point Mode allows VigorAP 910C to connect up to **four** VigorAP 910Cs which uses the same mode. All wired Ethernet clients of every VigorAP 910C 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 :

Channel :

Extension Channel :

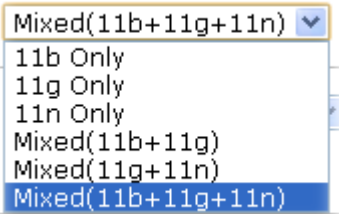
---

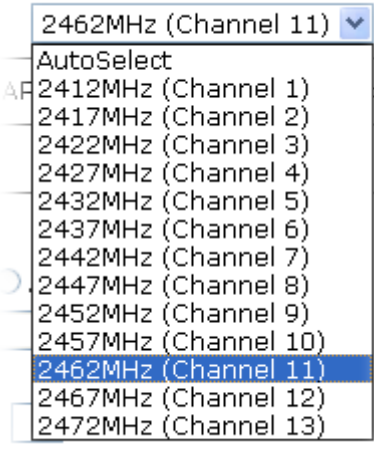
**Note:** Enter the configuration of APs which AP910C want to connect.

**PHY Mode : HTMIX**

<p><b>1. Security :</b></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><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p><b>3. Security :</b></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><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>
<p><b>2. Security :</b></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><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p><b>4. Security :</b></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><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Mode</b>	<p>At present, VigorAP 910C 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> 
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.

	
<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above.
<b>PHY Mode</b>	HTMIX (11b/g/n mixed mode) is specified VigorAP 910C.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required. Or click <b>Disabled</b> to ignore such feature.
<b>Peer Mac Address</b>	Type the peer MAC address for the access point that VigorAP 910C connects to.

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

### 3.7.2 Advanced Setting

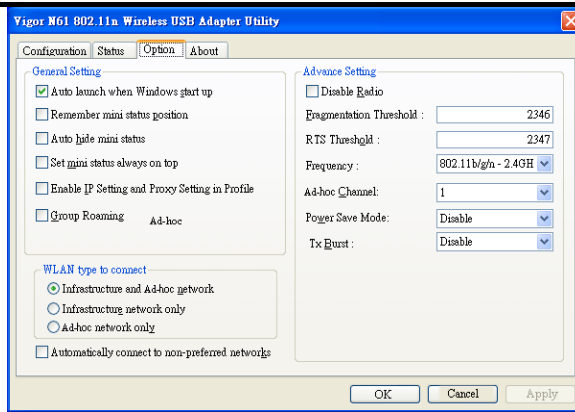
This page is to determine which algorithm will be selected for wireless transmission rate.

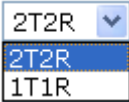
Wireless LAN (2.4GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 40 MHz
Packet-OVERDRIVE™ Tx Burst	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (For 11g mode only)
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Rate Adaptation Algorithm	<input checked="" type="radio"/> New <input type="radio"/> Old
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)
Auto Channel Reselect	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Auto Channel Filtered Out List	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
<b>MAC Clone:</b>	Set the MAC address of SSIDs and the Wireless client. Please notice that the last byte of this MAC address must be a multiple of 8.

Available settings are explained as follows:

Item	Description
<b>Channel Bandwidth</b>	<p><b>20 MHZ-</b> the device will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHZ</b> – VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz) shall be used to meet the air situation. Usually, 40MHz would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), 20MHz will be used by VigorAP automatically to ensure smooth network transmission.</p> <p><b>40 MHZ-</b> the device will use 40MHz for data transmission and receiving between the AP and the stations.</p>
<b>Packet-OVERDRIVE</b>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). 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><b>Note:</b> 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 <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b>).</p>



<p><b>Antenna</b></p>	<p>VigorAP 910C 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><b>Tx Power</b></p>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p>
<p><b>Rate Adaptation Algorithm</b></p>	<p>Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.</p>
<p><b>Fragment Length</b></p>	<p>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><b>RTS Threshold</b></p>	<p>Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. 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><b>Country Code</b></p>	<p>VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.</p>
<p><b>Auto Channel Reselect</b></p>	<p>Enable – Usually, wireless channel determined by AutoSelect (<b>Wireless LAN&gt;&gt;General Setup</b>) means Vigor router will search for a channel with low interference automatically once the system reboots. However, when the channel utilization is more than 70% (refer to <b>Diagnostics &gt;&gt; Interference Monitor</b>), Vigor router will search for and switch another channel with low interference to obtain better wireless signal again.</p>
<p><b>Auto Channel Filtered Out List</b></p>	<p>The selected wireless channels will be discarded if <b>AutoSelect</b> is selected as <b>Channel</b> selection mode in <b>Wireless LAN&gt;&gt;General Setup</b>.</p>
<p><b>IGMP Snooping</b></p>	<p>Check <b>Enable</b> to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in</p>

	the same manner as broadcast traffic.
<b>Isolate 2.4GHz and 5GHz bands</b>	<p>The default setting is “Enable”. It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.</p> <p>For WLAN 2.4GHz and 5GHz set with the same SSID name:</p> <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	<p>The default setting is “Disable”.</p> <p>If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).</p>
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>MAC Clone</b>	Click <b>Enable</b> 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.



### 3.7.3 AP Discovery

VigorAP 910C 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 910C.

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 910C can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (2.4GHz) >> Access Point Discovery

#### Access Point List

Enable AP Monitor Mode

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Mode	Ch. Width
<input type="radio"/>	1	staffs	00:1d:aa:3d:af:d6	81%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	2	guests	02:1d:aa:3c:af:d6	76%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	3	VFNL-E486C...	00:1d:aa:7e:87:bc	70%	3	TKIP/AES	WPA2/PSK	11b	20
<input type="radio"/>	4	DrayTek	00:1d:aa:f5:41:40	65%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	5	DrayTek	00:1d:aa:f7:c0:48	100%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	6	DrayTek-LA...	00:1d:aa:27:6f:c1	76%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	7	APM-PQC-Ta...	00:1d:aa:74:da:38	96%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	8	2F_WiFi	00:50:7f:c9:1e:48	65%	11	NONE		11b/g/n	20
<input type="radio"/>	9	AP920R-PQC...	00:1d:aa:63:2c:40	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	10		00:1d:aa:3d:4f:1e	100%	11	WEP		11b/g/n	20
<input type="radio"/>	11	DrayTek-LA...	02:1d:aa:3c:4f:1e	91%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	12	APM-PQC-Ta...	00:1d:aa:9f:af:00	70%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	13	DrayTek	00:1d:aa:80:06:b8	91%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	14	V2862 PQC ...	00:1d:aa:62:0f:a8	76%	11	AES	WPA2/PSK	11b/g/n	40
<input type="radio"/>	15	AP910C-PQC...	00:1d:aa:26:8d:30	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	16	RD8_24G_wi...	00:1d:aa:5b:a0:c8	96%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	17	V2710 PQC ...	00:50:7f:98:0a:38	100%	11	AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	18	APM-PQC-Ta...	00:1d:aa:3d:98:0a	70%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	19	DrayTek-LA...	00:1d:aa:27:6f:c0	81%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20

See [Channel Statistics](#)

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

AP's MAC Address

 :  :  :  :  : 

AP's SSID

Add to **WDS Settings**:

Available settings are explained as follows:

Item	Description
<b>Enable AP Monitor Mode</b>	This function can help to get and keep the records of APs detected by such device after clicking Scan. In general, only the available AP will be detected by Vigor device. Once the AP is unavailable, it will be deleted from the Access Point List immediately. However, if such function is enabled, the system will keep the record of the AP (once detected by Vigor device) until it is available for Vigor device again.
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 910C.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 910C.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 910C.

<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Mode</b>	Display the wireless connection mode that the scanned AP used.
<b>Ch. Width</b>	Display the channel width that the scanned AP used.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	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.
<b>Add</b>	Type the MAC address of the AP. Click <b>Add</b> . Later, the MAC address of the AP will be added and be shown on WDS settings page.

### 3.7.4 WDS AP Status

VigorAP 910C can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

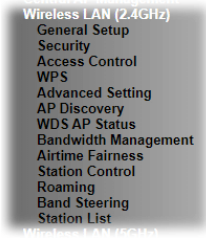
Wireless LAN (2.4GHz) >> WDS AP Status

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
-----	-------------	----------------------	------------	-----------

### 3.8 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, Advanced Setting, AP Discovery, WDS AP Status, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering and Station List.



#### 3.8.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the 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 Client Limit  (3 ~ 64, default: 64)

Enable Client Limit per SSID (3 ~ 64, default: 64)

---

Mode :

Channel :

Extension Channel :

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member(0:Untagged)	VLAN ID
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Hide SSID: Prevent SSID from being scanned.  
 Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.  
 Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.  
 Isolate Exception: Isolate Exception can be created by adding the MAC from [Device Object](#).

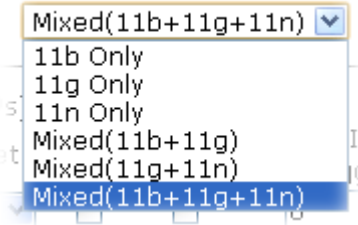
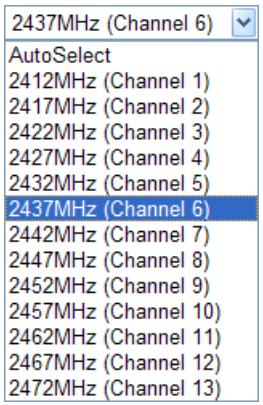
---

WDS Settings (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 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 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 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 type="text"/>            Peer MAC Address :  <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>

Note: Enter the configuration of APs which AP910C want to connect.  
 Remote AP should always use LAN or SSID1 MAC address to connect AP910C WDS.

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Client Limit</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor AP. The number you can set is from 3 to 64.
<b>Enable Client Limit per SSID</b>	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
<b>Mode</b>	<p>At present, VigorAP 910C 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> 
<b>Channel</b>	<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 <b>AutoSelect</b> to let system determine for you.</p> 
<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above. Configure the extension channel you want.
<b>Enable</b>	Check the box to enable the SSID configuration.
<b>Hide SSID</b>	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 910C while site surveying. The system allows you to set three sets of SSID for different usage.

<b>SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Isolate LAN</b>	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.  If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm.
<b>Peer MAC Address</b>	Four peer MAC addresses are allowed to be entered in this page at one time.

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 DrayTek

Mode

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

**WPA**

WPA Algorithms  TKIP  AES  TKIP/AES

Pass Phrase

Key Renewal Interval  seconds

EAPOL Key Retry  Enable  Disable

**WEP**

Key 1 :

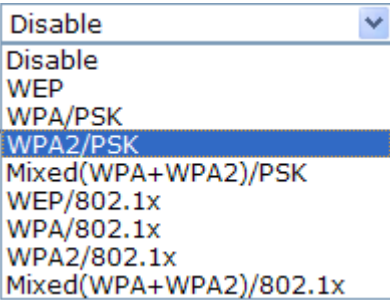
Key 2 :

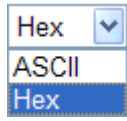
Key 3 :

Key 4 :

802.1x WEP  Disable  Enable

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are several modes provided for you to choose.</p>  <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - 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><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 910C 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><b>WPA/802.1x</b> - 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><b>WPA2/802.1x</b> - 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>
<b>WPA Algorithms</b>	<p>Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Pass Phrase</b>	<p>Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Key Renewal Interval</b>	<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</p>

	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 <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>EAPOL Key Retry</b>	EAPOL means Extensible Authentication Protocol over LAN. <b>Enable</b> - The default setting is "Enable". It can make sure that the key will be installed and used once in order to prevent key reinstallation attack.
<b>Key 1 – Key 4</b>	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 <b>WEP</b> mode. 
<b>802.1x WEP</b>	<b>Disable</b> - Disable the WEP Encryption. Data sent to the AP will not be encrypted. <b>Enable</b> - Enable the WEP Encryption. Such feature is available for <b>WEP/802.1x</b> mode.

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

#### RADIUS Server

Use internal RADIUS Server  
IP Address   
Port   
Shared Secret   
Session Timeout

Available settings are explained as follows:

Item	Description
<b>Use internal RADIUS Server</b>	There is a RADIUS server built in VigorAP 910C 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, <b>3.13 RADIUS Server</b> to configure settings for internal server of VigorAP 910C.
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.

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

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



### 3.8.3 Access Control

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

Wireless LAN (2.4GHz) >> Access Control

---

SSID 1	SSID 2	SSID 3	SSID 4						
SSID: DrayTek Policy: <input type="text" value="Disable"/>									
<b>MAC Address Filter</b>									
<table border="1"> <thead> <tr> <th>Index</th> <th>MAC Address</th> <th>access comment</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="height: 100px;"> <!-- Empty table body --> </td> </tr> </tbody> </table>				Index	MAC Address	access comment	Empty table body		
Index	MAC Address	access comment							
Empty table body									
<input type="radio"/> MAC <input checked="" type="radio"/> Object Device Group: <input type="text" value="None"/> or Device Object: <input type="text" value="None"/>									
<input type="button" value="Add"/> 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="text" value="選擇檔案"/> <input type="text" value="未選擇任何檔案"/> <input type="button" value="Restore"/>									

Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , 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 910C. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> <input type="text" value="Activate MAC address filter"/> </div> <div style="border: 1px solid black; padding: 2px; margin-top: 2px;">             Disable           </div> <div style="border: 1px solid black; padding: 2px; margin-top: 2px; background-color: #e0e0e0;">             Activate MAC address filter           </div> <div style="border: 1px solid black; padding: 2px; margin-top: 2px;">             Blocked MAC address filter           </div>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>MAC</b>	<b>Client's MAC Address</b> - Manually enter the MAC address of wireless client. <b>Add</b> - Add a new MAC address into the list. <b>Delete</b> - Delete the selected MAC address in the list. <b>Edit</b> - Edit the selected MAC address in the list.
<b>Object</b>	In addition to enter the MAC address of the device manually, you can

	<p><b>Device Group</b> - Select one of the existed device groups and click <b>Add</b>. All the devices belonging to the selected group will be shown on the MAC Address Filter table.</p> <p><b>Device Object</b> - Select one of the existed device object and click <b>Add</b>. The MAC address of the device will be shown on the MAC Address Filter table.</p>
<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	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


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES

#### Device Configure


<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<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
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 910C is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 910C. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 910C.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 910C will wait for WPS requests from

	wireless clients about two minutes. (You need to setup WPS within two minutes)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. (You need to setup WPS within two minutes).

### 3.8.5 Advanced Setting

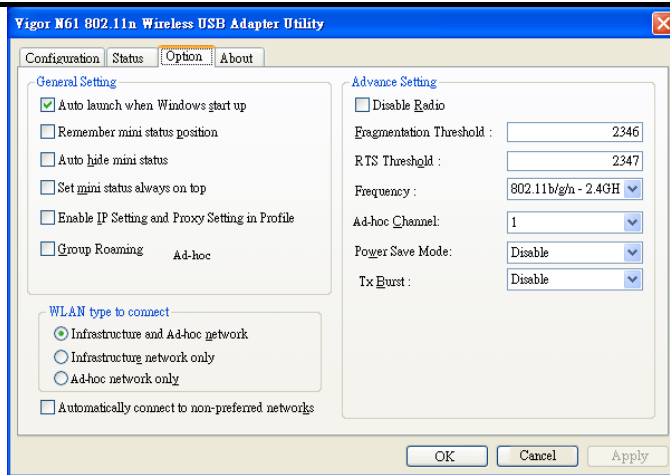
This page is to determine which algorithm will be selected for wireless transmission rate.

Wireless LAN (2.4GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 40 MHz
Packet-OVERDRIVE™ Tx Burst	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (For 11g mode only)
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Rate Adaptation Algorithm	<input checked="" type="radio"/> New <input type="radio"/> Old
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)
Auto Channel Reselect	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Auto Channel Filtered Out List	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
<b>MAC Clone:</b>	Set the MAC address of SSIDs and the Wireless client. Please notice that the last byte of this MAC address must be a multiple of 8.

Available settings are explained as follows:

Item	Description
<b>Channel Bandwidth</b>	<p><b>20 MHz-</b> the device will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHz-</b> VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz) shall be used to meet the air situation. Usually, 40MHz would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), 20MHz will be used by VigorAP automatically to ensure smooth network transmission.</p> <p><b>40 MHz-</b> the device will use 40MHz for data transmission and receiving between the AP and the stations.</p>
<b>Packet-OVERDRIVE</b>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). 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><b>Note:</b> 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 <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b>).</p>



<b>Antenna</b>	VigorAP 910C 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.
<b>Tx Power</b>	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.
<b>Rate Adaptation Algorithm</b>	Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.
<b>Fragment Length</b>	Set the Fragment threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2346.
<b>RTS Threshold</b>	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2347.
<b>Country Code</b>	VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
<b>Auto Channel Reselect</b>	<b>Enable</b> – Usually, wireless channel determined by AutoSelect ( <b>Wireless LAN&gt;&gt;General Setup</b> ) means Vigor router will search for a channel with low interference automatically once the system reboots. However, when the channel utilization is more than 70% (refer to <b>Diagnostics &gt;&gt; Interference Monitor</b> ), Vigor router will search for and switch another channel with low interference to obtain better wireless signal again.
<b>Auto Channel Filtered Out List</b>	The selected wireless channels will be discarded if <b>AutoSelect</b> is selected as <b>Channel</b> selection mode in <b>Wireless LAN&gt;&gt;General Setup</b> .
<b>IGMP Snooping</b>	Check <b>Enable</b> to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
<b>Isolate 2.4GHz and</b>	The default setting is “Enable”. It means that the wireless client

<b>5GHz bands</b>	<p>using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.</p> <p>For WLAN 2.4GHz and 5GHz set with the same SSID name:</p> <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	<p>The default setting is “Disable”.</p> <p>If it is enabled, VigorAP will isolate different wireless clients according to their IP address (es).</p>
<b>WMM Capable</b>	<p>To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.</p>
<b>MAC Clone</b>	<p>Click <b>Enable</b> 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>

### 3.8.6 AP Discovery

VigorAP 910C 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 910C can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (2.4GHz) >> Access Point Discovery

#### Access Point List

Enable AP Monitor Mode

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Mode	Ch. Width
<input type="radio"/>	1	guests	02:1d:aa:3c:af:d6	81%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	2	staffs	00:1d:aa:3d:af:d6	81%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	3	staffs	00:1d:aa:9d:68:ac	100%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	4	guests	02:1d:aa:9d:68:ac	100%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	5	DrayTek	00:1d:aa:b0:ac:90	96%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	6	DrayTek	00:1d:aa:f5:04:58	91%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	7	DrayTek	00:1d:aa:f7:c0:48	100%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	8	staffs	00:1d:aa:9c:f6:44	96%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	9	guests	02:1d:aa:9c:f6:44	55%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	10	APM-PQC-Ta...	00:1d:aa:3d:4f:14	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	11	DR8_710	00:50:7f:f1:00:16	39%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	12	AP910C-PQC...	00:1d:aa:26:8d:30	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	13	FAE-Wendy-...	00:1d:aa:f0:6d:f0	44%	11	AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	14	FAE-Wendy-...	02:1d:aa:f0:6d:f0	44%	11	AES	WPA2	11b/g/n	20
<input type="radio"/>	15	AP1000_HW...	00:1d:aa:67:d6:70	29%	11	NONE		11b/g/n	40
<input type="radio"/>	16	APM-PQC-Ta...	00:1d:aa:74:da:38	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	17	DrayTek-LA...	00:1d:aa:9c:f0:58	65%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	18	DrayTek-LA...	02:1d:aa:9c:f0:58	60%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	19	DrayTek-LA...	00:1d:aa:27:6f:c1	65%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	20	RD8-910c-1	00:1d:aa:7f:5d:8c	96%	11	TKIP/AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	21	RD8-910c-2	02:1d:aa:78:5d:8c	96%	11	TKIP/AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	22	2925 PQC k...	00:1d:aa:db:e0:88	91%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	23	DrayTek	00:50:7f:e4:8d:dc	55%	11	NONE		11b/g/n	20
<input type="radio"/>	24		00:1d:aa:3d:4f:1e	96%	11	WEP		11b/g/n	20

See [Channel Statistics](#)

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

AP's MAC Address  :  :  :  :  :

AP's SSID

Add to [WDS Settings](#):

Each item is explained as follows:

Item	Description
<b>Enable AP Monitor Mode</b>	This function can help to get and keep the records of APs detected by such device after clicking Scan. In general, only the available AP will be detected by Vigor device. Once the AP is unavailable, it will be deleted from the Access Point List immediately. However, if such function is enabled, the system will keep the record of the AP (once detected by Vigor device) until it is available for Vigor device again.
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 910C.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 910C.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by

	VigorAP 910C.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Mode</b>	Display the wireless connection mode that the scanned AP used.
<b>Ch. Width</b>	Display the channel width that the scanned AP used.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	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.
<b>Add</b>	Click <b>Repeater</b> for the specified AP. Next, click <b>Add</b> . Later, the MAC address of the AP will be added and be shown on WDS settings page.

### 3.8.7 WDS AP Status

VigorAP 910C can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

Wireless LAN (2.4GHz) >> WDS AP Status

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
-----	-------------	----------------------	------------	-----------



### 3.8.8 Bandwidth Management

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

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<input type="checkbox"/>		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	512K		bps
Auto Adjustment	<input checked="" type="checkbox"/>		
Total Upload Limit	User defined	K	bps (Default unit : K)
Total Download Limit	128K		bps

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

OK Cancel

Available settings are explained as follows:

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

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

### 3.8.9 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

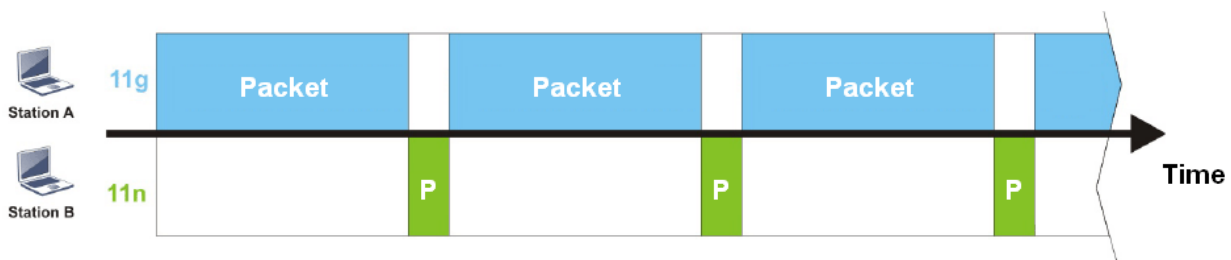
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

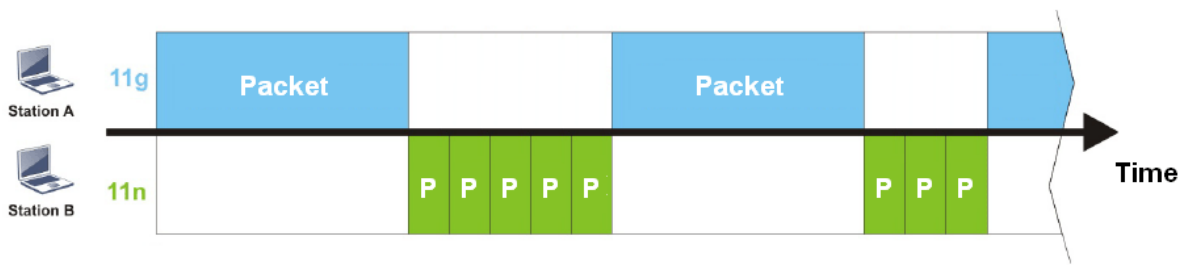
The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 910C. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 910C. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

**Wireless LAN (2.4GHz) >> Airtime Fairness**

Enable **Airtime Fairness**  
 Triggering Client Number  (2 ~ 64, Default: 2)

**Note:** Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Available settings are explained as follows:

Item	Description
<p><b>Enable Airtime Fairness</b></p>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p><b>Airtime Fairness</b> – Click the link to display the following screen of airtime fairness note.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p><b>Airtime Fairness Note:</b></p> <ul style="list-style-type: none"> <li>* Airtime is the time where a wireless station occupies the wireless channel. Airtime Fairness function tries to assign similar airtime to each station by controlling TX traffic. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.</li> <li>* Suitable environment : (1) Many wireless stations. (2) All stations mainly use download traffic. (3) The performance bottleneck is wireless connection.</li> <li>* Triggering Client Number: Airtime Fairness function is applied only when active station number achieves this number.</li> </ul> </div> <p><b>Triggering Client Number</b> –Airtime Fairness function is applied only when active station number achieves this number.</p>

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

**Note:** Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

### 3.8.10 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect VigorAP. If such function is not enabled, the wireless client can connect VigorAP until it shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

**Note:** Up to 300 Wireless Station records are supported by VigorAP.

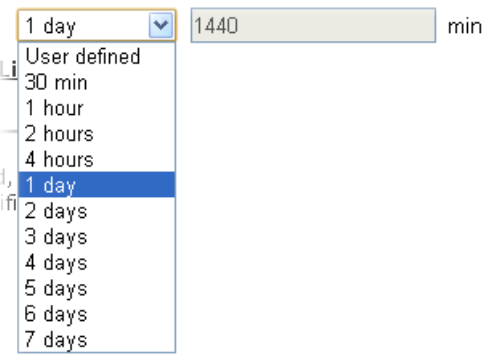
#### Wireless LAN (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek	
Enable		<input type="checkbox"/>	
Connection Time		1 hour	
Reconnection Time		1 day	
<a href="#">Display All Station Control List</a>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

OK Cancel

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID that the wireless station will use it to connect with Vigor router.
<b>Enable</b>	Check the box to enable the station control function.
<b>Connection Time / Reconnection Time</b>	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose <b>User defined</b> . 
<b>Display All Station</b>	All the wireless stations connecting to Vigor router by using

---

**Control List**such SSID will be listed on Station Control List.

---

After finishing all the settings here, please click **OK** to save the configuration.

### 3.8.11 Roaming

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

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

**Wireless LAN (2.4GHz) >> Roaming**

---

**AP-assisted Client Roaming Parameters**

<input type="checkbox"/> <b>Minimum Basic Rate</b>	1	Mbps
<input checked="" type="radio"/> Disable RSSI Requirement		
<input checked="" type="radio"/> <b>Strictly Minimum RSSI</b>	-73	dBm (42%) (Default: -73)
<input checked="" type="radio"/> <b>Minimum RSSI</b>	-66	dBm (60%) (Default: -66)
with Adjacent AP RSSI over	5	dBm (Default: 5)

**Fast Roaming(WPA/802.1x)**

<input type="checkbox"/> Enable		
<b>PMK Caching</b> : Cache Period	10	minute(s) (10 ~ 600) (Default: 10)
<b>Pre-Authentication</b>		

OK Cancel

Available settings are explained as follows:

Item	Description
<b>AP-assisted Client Roaming Parameters</b>	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 910C will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p><b>Minimum Basic Rate</b> – Check the box to use the drop down list to specify a basic rate (<b>Mbps</b>). When the link rate of the wireless station is below such value, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Disable RSSI Requirement</b> - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p><b>Strictly Minimum RSSI</b> - VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (<b>dBm</b>) set here, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Minimum RSSI</b> - When the signal strength of the wireless station is below the value (<b>dBm</b>) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of <b>With Adjacent AP RSSI</b></p>

	<p><b>over</b>) is detected by VigorAP 910C, VigorAP 910C will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI).</p> <ul style="list-style-type: none"> <li>● <b>With Adjacent AP RSSI over</b> – Specify a value as a threshold.</li> </ul>
<p><b>Fast Roaming (WPA/802.1x)</b></p>	<p><b>Enable</b> – Check the box to enable fast roaming configuration.</p> <p><b>PMK Cache Period</b> - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for <b>WPA2/802.1</b> mode.</p> <p><b>Pre-Authentication</b> - 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)</p> <p><b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.</p> <p><b>Disable</b> - Disable IEEE 802.1X Pre-Authentication.</p>

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

### 3.8.12 Band Steering

Band Steering detects if the wireless clients are capable of 5GHz operation, and steers them to that frequency. It helps to leave 2.4GHz band available for legacy clients, and improves users experience by reducing channel utilization.



If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



**Note:** To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

Open **Wireless LAN (2.4GHz)>>Band Steering** to get the following web page:

**Wireless LAN (2.4GHz) >> Band Steering**

Enable **Band Steering**

Check Time for WLAN Client 5G Capability  seconds (1 ~ 60, Default: 15)

5GHz Minimum RSSI  dBm ( %) (Default: -78)

(Only do band steering when 5GHz signal is better than Minimum RSSI)

**Note:** Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

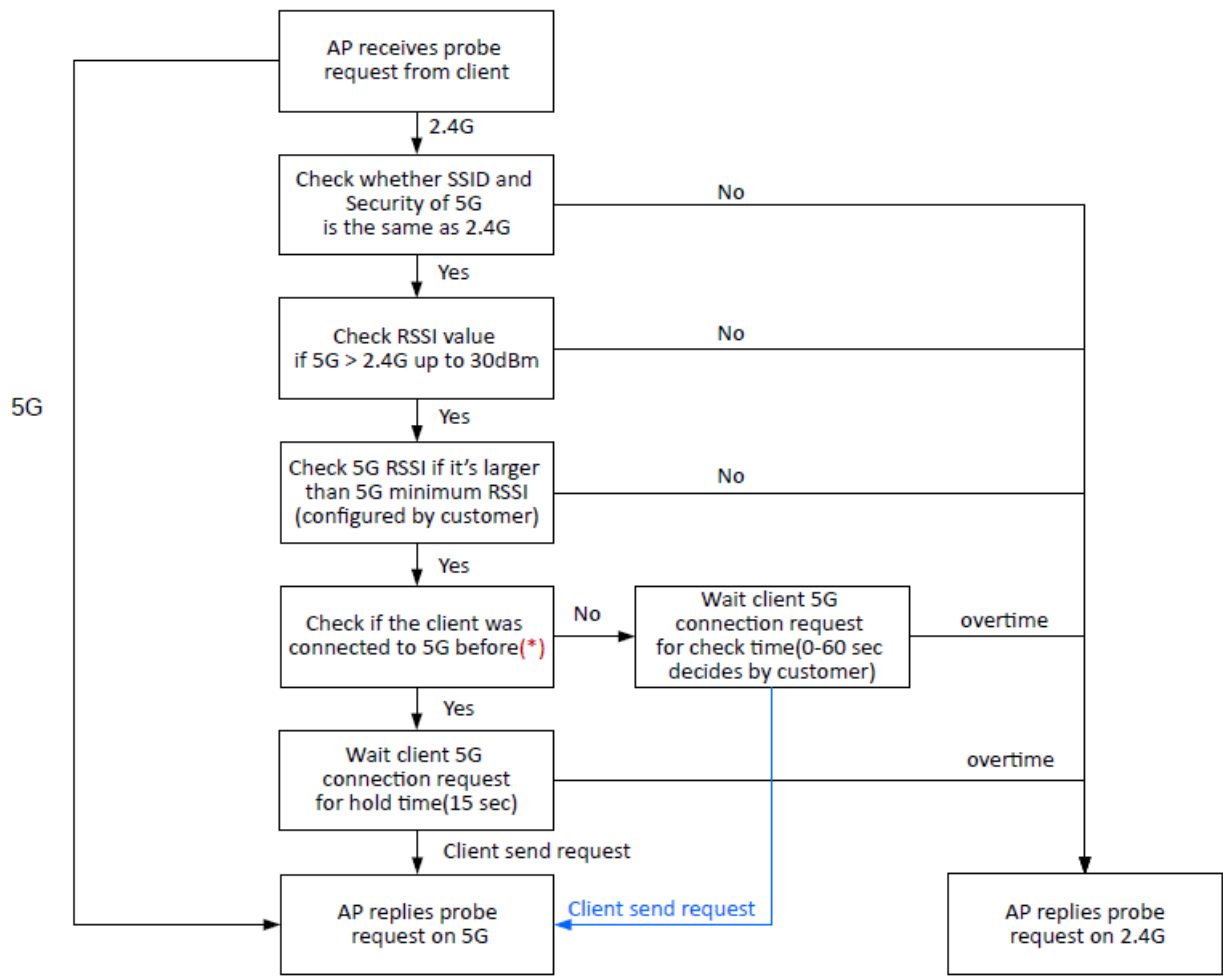
Available settings are explained as follows:

Item	Description
<b>Enable Band Steering</b>	<p>If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit.</p> <p><b>Check Time....</b> – If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for VigorAP to detect the wireless client.</p> <p><b>5GHz Minimum RSSI</b> - The wireless station has the capability of 5GHz network connection, yet the signal performance might not be satisfied. Therefore, when the signal strength is below the value set here while the wireless station connecting to VigorAP, VigorAP will allow the client to connect to 2.4GHz network.</p>

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

Below shows how Band Steering works.





\* AP will clear the 5G history station list every 2.5 mins.

## How to Use Band Steering?

1. Open **Wireless LAN(2.4GHz)>>Band Steering**.
2. Check the box of **Enable Band Steering** and use the default value (15) for check time setting.

### Wireless LAN >> Band Steering

Enable **Band Steering**  
 Check Time for WLAN Client 5G Capability  second(s) (1 ~ 60) (Default: 15)

**Note :** Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>>General Setup**. Configure SSID as *ap910C-BandSteering* for both pages. Click **OK** to save the settings.

### Wireless LAN (2.4GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

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

Mode :

	Hide SSID	SSID	Isolate Member	VLAN ID (0:Untagged)	MAC Clone
1	<input type="checkbox"/>	ap910C-BandSteerin	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
2	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
3	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
4	<input type="checkbox"/>		<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

Same value for 2.4GHz and 5GHz

### Wireless LAN (5GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

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

Mode :

	Hide SSID	SSID	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	ap910C-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>		<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 :   
 Details : 20MHz / 40MHz Ext Ch: 40 , 80MHz Center Ch: 42

- Open **Wireless LAN (2.4GHz)>>Security** and **Wireless LAN (5GHz)>>Security**. Configure Security as *12345678* for both pages. Click **OK** to save the settings.

**Wireless LAN (2.4GHz) >> Security Settings**

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap910C-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
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			
<b>WEP</b>			
<input 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			

Same value for 2.4GHz and 5GHz

**Wireless LAN (5GHz) >> Security Settings**

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap910C-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
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			
PMK Cache Period			
<input type="text" value="10"/> minutes			
Pre-Authentication			
<input type="radio"/> Disable <input type="radio"/> Enable			
<b>WEP</b>			
<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"/>			

- Now, VigorAP 910C will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

### 3.8.13 Station List

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

#### General

Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station.

Wireless LAN (2.4GHz) >> Station List

**Station List**

							General	Advanced	Control	Neighbor
Index	MAC Address	Vendor	RSSI	Approx. Distance	SSID	Visit Time				
1	DA:A1:19:E2:65:AD		5% (-88dBm)	141.25m	N/A	0d:0h:				
2	00:50:7F:F0:BD:2B	DrayTek	52% (-69dBm)	15.85m	N/A	0d:0h:				
3	00:50:7F:37:6D:E5	DrayTek	47% (-71dBm)	19.95m	N/A	0d:0h:				
4	1C:4B:D6:8B:9C:00	Azurewav	18% (-83dBm)	79.43m	N/A	0d:1h:				
5	00:15:AF:A5:24:A0	Azurewav	26% (-79dBm)	50.12m	N/A	0d:0h:				
6	B0:34:95:22:50:FD	Apple	47% (-71dBm)	19.95m	N/A	0d:0h:				
7	B4:52:7E:D6:68:9D	Sony	20% (-82dBm)	70.79m	N/A	0d:0h:				
8	00:1F:3C:51:9C:55	Intel	39% (-74dBm)	28.18m	N/A	0d:1h:				

**Add to Access Control:**

Client's MAC Address :  :  :  :  :  :

- Note:**
1. Approx. Distance is calculated by actual signal strength of device detected. Inaccuracy might occur based on barrier encountered.
  2. Due to the differences in signal strength for different devices, the calculated value of approximate distance also might be different.
  3. Trademarks and brand names are the properties of their respective owners.

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>Hostname</b>	Display the host name of the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - 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.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

**Advanced**

Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

**Control**

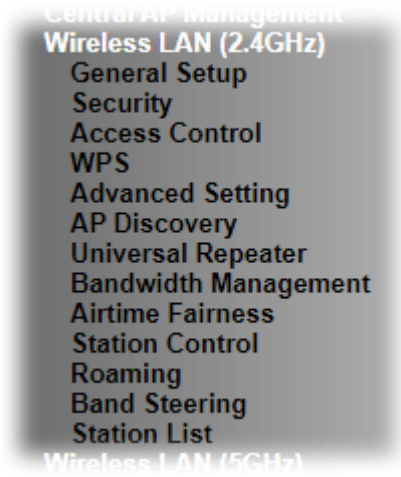
Display connection and reconnection time of the wireless stations.

**Neighbor**

Display more information for the neighboring wireless stations.

### 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, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering 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 Client Limit  (3 ~ 64, default: 64)

Enable Client Limit per SSID (3 ~ 64, default: 64)

---

Mode :  ▼

Channel :  ▼

Extension Channel :  ▼

---

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

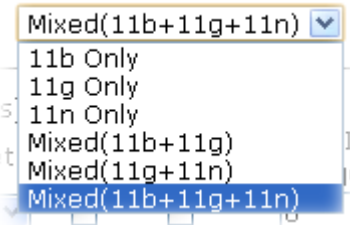
**Hide SSID:** Prevent SSID from being scanned.

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

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

**Isolate Exception:** Isolate Exception can be created by adding the MAC from [Device Object](#).

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Client Limit</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor AP. The number you can set is from 3 to 64.
<b>Enable Client Limit per SSID</b>	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
<b>Mode</b>	<p>At present, VigorAP 910C 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> 
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above. Configure the extension channel you want.
<b>Enable</b>	Check the box to enable the SSID configuration.
<b>Hide SSID</b>	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 910C while site surveying. The system allows you to set three sets of SSID for different usage.
<b>SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Isolate LAN</b>	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	<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</p>

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.

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

### 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.

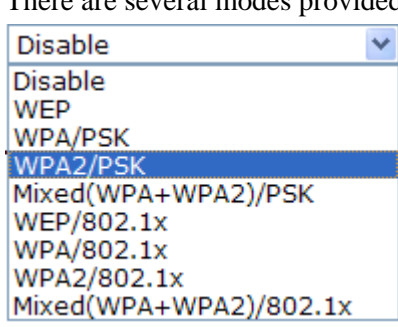
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek	
Mode		Mixed(WPA+WPA2)/PSK	
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
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="3600"/> seconds	
EAPOL Key Retry		<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
<b>WEP</b>			
<input type="radio"/> Key 1 :	<input type="text"/>	<input type="text"/>	Hex
<input checked="" type="radio"/> Key 2 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text"/>	Hex
802.1x WEP		<input type="radio"/> Disable <input type="radio"/> Enable	

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are several modes provided for you to choose.</p>  <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK -</b></p>



	<p>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><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 910C 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><b>WPA/802.1x</b> - 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><b>WPA2/802.1x</b> - 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>
<b>WPA Algorithms</b>	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Pass Phrase</b>	Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key Renewal Interval</b>	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 <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>EAPOL Key Retry</b>	EAPOL means Extensible Authentication Protocol over LAN. <b>Enable</b> - The default setting is "Enable". It can make sure that the key will be installed and used once in order to prevent key reinstallation attack.
<b>Key 1 – Key 4</b>	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 <b>WEP</b> mode.

	<div style="border: 1px solid black; padding: 2px;"> Hex ▾  ASCII  Hex </div>
<b>802.1x WEP</b>	<p><b>Disable</b> - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p><b>Enable</b> - Enable the WEP Encryption. Such feature is available for <b>WEP/802.1x</b> mode.</p>

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

**Radius Server**

Use internal RADIUS Server  
IP Address   
Port   
Shared Secret   
Session Timeout

Available settings are explained as follows:

Item	Description
<b>Use internal RADIUS Server</b>	<p>There is a RADIUS server built in VigorAP 910C 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, <b>3.13 RADIUS Server</b> to configure settings for internal server of VigorAP 910C.</p>
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	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.
<b>Session Timeout</b>	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.

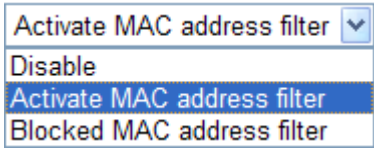
### 3.9.3 Access Control

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

The screenshot shows the 'Access Control' configuration page for SSID 1. At the top, there are tabs for SSID 1, SSID 2, SSID 3, and SSID 4. Under SSID 1, the SSID is 'DrayTek' and the Policy is set to 'Disable'. Below this is a 'MAC Address Filter' section with a table that has three columns: 'Index', 'MAC Address', and 'access comment'. The table is currently empty. Below the table, there are radio buttons for 'MAC' and 'Object', with 'Object' selected. There are also dropdown menus for 'Device Group' (set to 'None') and 'Device Object' (set to 'None'). An 'Add' button and a 'Limit:256 entries' label are also present. At the bottom of the configuration area are 'OK' and 'Cancel' buttons. Below the configuration area, there is a 'Backup ACL Cfg' section with 'Backup' and 'Restore' buttons, and an 'Upload From File' section with a file selection button and a 'Restore' button.

Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , 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 910C. 
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>MAC</b>	<b>Client's MAC Address</b> - Manually enter the MAC address of wireless client. <b>Add</b> - Add a new MAC address into the list. <b>Delete</b> - Delete the selected MAC address in the list. <b>Edit</b> - Edit the selected MAC address in the list.
<b>Object</b>	In addition to enter the MAC address of the device manually, you can


	<p><b>Device Group</b> - Select one of the existed device groups and click <b>Add</b>. All the devices belonging to the selected group will be shown on the MAC Address Filter table.</p> <p><b>Device Object</b> - Select one of the existed device object and click <b>Add</b>. The MAC address of the device will be shown on the MAC Address Filter table.</p>
<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	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.

### 3.9.4 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**




<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encrypt Type</b>	TKIP/AES

**Device Configure**

<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<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
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 910C is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 910C. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 910C.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 910C will wait for WPS requests from wireless clients about two minutes. (You need to setup WPS

	within two minutes)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. (You need to setup WPS within two minutes).

### 3.9.5 Advanced Setting

This page is to determine which algorithm will be selected for wireless transmission rate.

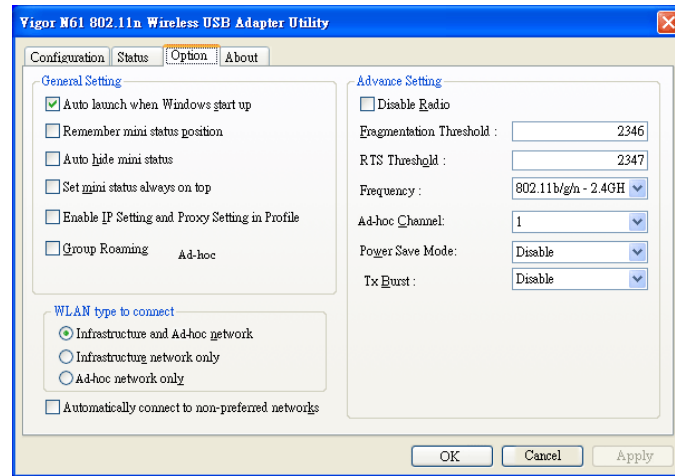
Wireless LAN (2.4GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 40 MHz
Packet-OVERDRIVE™ Tx Burst	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (For 11g mode only)
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Rate Adaptation Algorithm	<input checked="" type="radio"/> New <input type="radio"/> Old
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> ( <a href="#">Reference</a> )
Auto Channel Reselect	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Auto Channel Filtered Out List	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
<b>MAC Clone:</b>	Set the MAC address of SSIDs and the Wireless client. Please notice that the last byte of this MAC address must be a multiple of 8.

Available settings are explained as follows:

Item	Description
<b>Channel Width</b>	<p><b>20 MHz-</b> the AP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHz –</b> VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz) shall be used to meet the air situation. Usually, 40MHz would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), 20MHz will be used by VigorAP automatically to ensure smooth network transmission.</p> <p><b>40 MHz-</b> the AP will use 40MHz for data transmission and receiving between the AP and the stations.</p>
<b>Packet-OVERDRIVE</b>	This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b> ). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

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



	<p>VigorAP 910C 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><b>Tx Power</b></p>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p>
<p><b>Rate Adaptation Algorithm</b></p>	<p>Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.</p>
<p><b>Fragment Length</b></p>	<p>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><b>RTS Threshold</b></p>	<p>Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. 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><b>Country Code</b></p>	<p>VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.</p>
<p><b>Auto Channel Reselect</b></p>	<p>Enable – Usually, wireless channel determined by AutoSelect (<b>Wireless LAN&gt;&gt;General Setup</b>) means Vigor router will search for a channel with low interference automatically once the system reboots. However, when the channel utilization is more than 70% (refer to <b>Diagnostics &gt;&gt; Interference Monitor</b>), Vigor router will search for and switch another channel with low interference to obtain better wireless signal again.</p>
<p><b>Auto Channel Filtered Out List</b></p>	<p>The selected wireless channels will be discarded if <b>AutoSelect</b> is selected as <b>Channel</b> selection mode in <b>Wireless</b></p>

	<b>LAN&gt;&gt;General Setup.</b>
<b>IGMP Snooping</b>	Check <b>Enable</b> to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
<b>Isolate 2.4GHz and 5GHz bands</b>	<p>The default setting is “Enable”. It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.</p> <p>For WLAN 2.4GHz and 5GHz set with the same SSID name:</p> <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	The default setting is “Disable”. If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>MAC Clone</b>	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.

### 3.9.6 AP Discovery

VigorAP 910C 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 910C can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (2.4GHz) >> Access Point Discovery

#### Access Point List

Enable AP Monitor Mode

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Mode	Ch. Width
<input type="radio"/>	1	guests	0a:1d:aa:63:2c:38	91%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g	20
<input type="radio"/>	2	staffs_SF	00:1d:aa:63:2c:38	91%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g	20
<input type="radio"/>	3	staffs	06:1d:aa:63:2c:38	100%	1	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g	20
<input type="radio"/>	4	DIRECT-mwX...	62:f1:89:a8:09:5b	81%	1	AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	5	RD8-910c-1	00:1d:aa:7f:5d:8c	91%	3	TKIP/AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	6	RD8-910c-2	02:1d:aa:78:5d:8c	96%	3	TKIP/AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	7	RD8-910c-3	02:1d:aa:79:5d:8c	96%	3	TKIP/AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	8	RD8-910c-4	02:1d:aa:7a:5d:8c	81%	3	TKIP/AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	9	DrayTek	00:1d:aa:dd:75:b0	100%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	10	Adamchao	ba:53:ac:60:c5:d6	60%	6	AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	11	DrayTek	00:1d:aa:65:32:f0	96%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	12	staffs_6F	00:1d:aa:9c:f6:44	96%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	13	DrayTek	00:1d:aa:f7:c0:48	100%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	14	RD8_24G_wi...	00:1d:aa:5b:a0:c8	91%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	15	staffs	02:1d:aa:9c:f3:c0	60%	8	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	16	AP910C-1 P...	00:1d:aa:7f:54:5c	86%	10	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	17	DrayTek-LA...	00:1d:aa:9d:23:18	86%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	18	DrayTek-LA...	02:1d:aa:9c:23:18	86%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	19	DrayTek-LA...	00:1d:aa:3d:4f:1a	91%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	20	AP920RP-PQ...	00:1d:aa:63:2b:c0	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	21	AP920RP PQ...	06:1d:aa:5c:a7:00	100%	11	AES	WPA2/PSK	11b/g/n	40
<input type="radio"/>	22	ACS_APM_te...	00:1d:aa:3d:4f:14	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	23	DrayTek	00:1d:aa:7f:5d:58	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	24	AP1000C_PQ...	00:1d:aa:57:5d:20	81%	11	AES	WPA2	11b/g/n	40
<input type="radio"/>	25	FAE-Wendy-...	00:1d:aa:f0:6d:f0	81%	11	AES	WPA2/PSK	11b/g/n	20
<input type="radio"/>	26	FAE-Wendy-...	02:1d:aa:f0:6d:f0	76%	11	AES	WPA2	11b/g/n	20
<input type="radio"/>	27	PQC-SmartP...	00:1d:aa:67:05:10	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	28	AP920RP PQ...	00:1d:aa:5c:a7:00	96%	11	AES	WPA2/PSK	11b/g/n	40
<input type="radio"/>	29	AP910C-2 p...	00:1d:aa:26:8d:68	96%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	30	2F_WiFi	00:50:7f:c9:1e:48	39%	11	NONE		11b/g/n	20
<input type="radio"/>	31	Draytek	00:1d:aa:9f:65:3c	34%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
<input type="radio"/>	32	AP910C-PQC...	00:1d:aa:26:8d:30	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
<input type="radio"/>	33	V2860 PQC ...	00:1d:aa:d3:af:38	100%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20

See [Channel Statistics](#)

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

AP's MAC Address  AP's SSID

Select as **Universal Repeater:**

Each item is explained as follows:

Item	Description
<b>Enable AP Monitor Mode</b>	This function can help to get and keep the records of APs detected by such device after clicking Scan. In general, only the available AP will be detected by Vigor device. Once the AP is unavailable, it will be deleted from the Access Point List immediately. However, if such function is enabled, the system will keep the record of the AP (once detected by Vigor device) until it is available for Vigor device again.
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 910C.



<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 910C.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 910C.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Mode</b>	Display the wireless connection mode that the scanned AP used.
<b>Ch. Width</b>	Display the channel width that the scanned AP used.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	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.
<b>Select as Universal Repeater</b>	In <b>Universal Repeater</b> 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.

### 3.9.7 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"/>

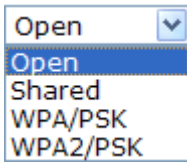
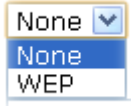
**Note :** If Channel is modified, the Channel setting of AP would also be changed.

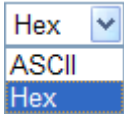
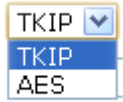
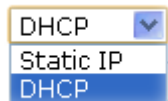
**Universal Repeater IP Configuration**

Connection Type	DHCP ▼
Device Name	AP910C

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Universal Repeater Parameters</b>	
<b>SSID</b>	Set the name of access point that VigorAP 910C wants to connect to.
<b>MAC Address (Optional)</b>	Type the MAC address of access point that VigorAP 910C wants to connect to.
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Security Mode</b>	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. 
<b>Encryption Type for Open/Shared</b>	This option is available when Open/Shared is selected as Security Mode. Choose <b>None</b> to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose <b>WEP</b> .  <b>WEP Keys</b> - 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

	<p>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> 
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>This option is available when WPA/PSK or WPA2/PSK is selected as <b>Security Mode</b>.</p> <p>Select <b>TKIP</b> or <b>AES</b> as the algorithm for WPA.</p> 
<b>Pass Phrase</b>	<p>Either <b>8~63</b> ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
<b>Universal Repeater IP Configuration</b>	
<b>Connection Type</b>	<p>Choose DHCP or Static IP as the connection mode.</p> <p><b>DHCP</b> – The wireless station will be assigned with an IP from VigorAP.</p> <p><b>Static IP</b> – The wireless station shall specify a static IP for connecting to Internet via VigorAP.</p> 
<b>Device Name</b>	<p>This setting is available when <b>DHCP</b> is selected as <b>Connection Type</b>.</p> <p>Type a name for the router as identification. Simply use the default name.</p>
<b>IP Address</b>	<p>This setting is available when <b>Static IP</b> is selected as <b>Connection Type</b>.</p> <p>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>
<b>Subnet Mask</b>	<p>This setting is available when <b>Static IP</b> is selected as <b>Connection Type</b>.</p> <p>Type the subnet mask setting which shall be the same as the one configured in LAN for the router.</p>
<b>Default Gateway</b>	<p>This setting is available when <b>Static IP</b> is selected as <b>Connection Type</b>.</p> <p>Type the gateway setting which shall be the same as the default gateway configured in LAN for the router.</p>

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

### 3.9.8 Bandwidth Management

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

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<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 Limit	User defined	K	bps (Default unit : K)
Total Download Limit	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
<b>SSID</b>	Display the specific SSID name of the AP.
<b>Enable</b>	Check this box to enable the bandwidth management for clients.
<b>Upload Limit</b>	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor AP with the same SSID. Use the drop down list to choose the rate. If you choose <b>User defined</b> , you have to specify the rate manually.
<b>Download Limit</b>	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor AP with the same SSID. Use the drop down list to choose the rate. If you choose <b>User defined</b> , you have to specify the rate manually.
<b>Auto Adjustment</b>	Check this box to have the bandwidth limit determined by the system automatically.
<b>Total Upload Limit</b>	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.
<b>Total Download Limit</b>	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.

### 3.9.9 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

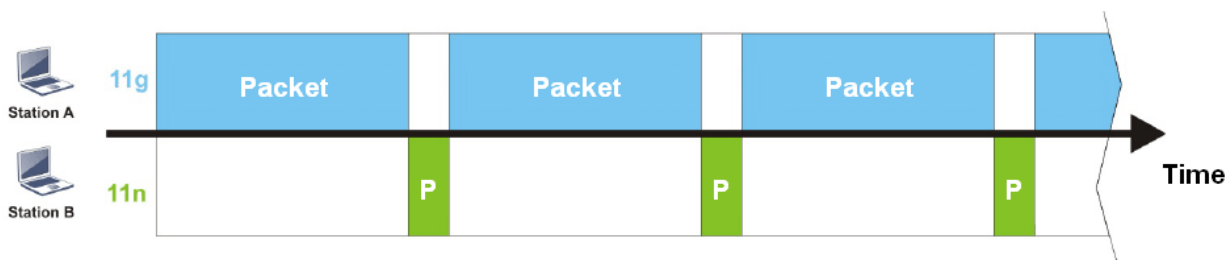
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

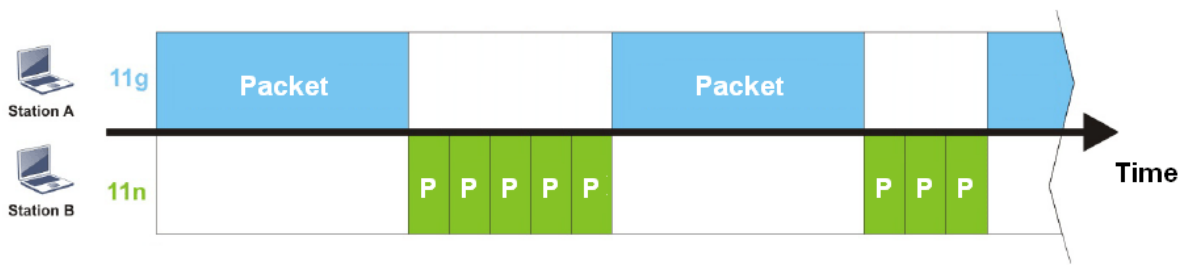
The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 910C. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 910C. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

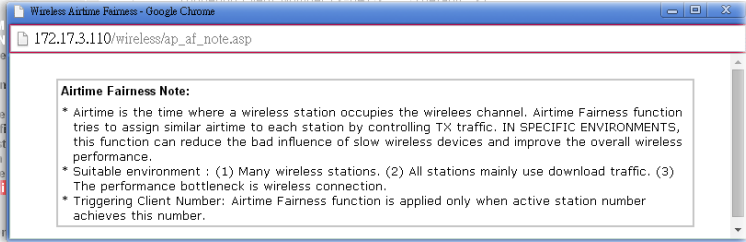
- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

**Wireless LAN (2.4GHz) >> Airtime Fairness**

Enable **Airtime Fairness**  
 Triggering Client Number  (2 ~ 64, Default: 2)

**Note:** Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Available settings are explained as follows:

Item	Description
<p><b>Enable Airtime Fairness</b></p>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p><b>Airtime Fairness</b> – Click the link to display the following screen of airtime fairness note.</p>  <p><b>Triggering Client Number</b> –Airtime Fairness function is applied only when active station number achieves this number.</p>

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

**Note:** Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

### 3.9.10 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect VigorAP. If such function is not enabled, the wireless client can connect VigorAP until it shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

**Note:** Up to 300 Wireless Station records are supported by VigorAP.

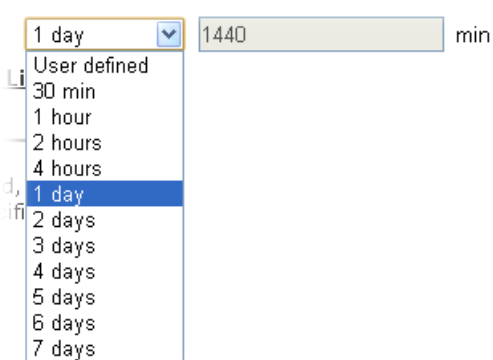
Wireless LAN (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek	
Enable		<input type="checkbox"/>	
Connection Time		1 hour	
Reconnection Time		1 day	
<a href="#">Display All Station Control List</a>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

OK Cancel

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID that the wireless station will use it to connect with Vigor router.
<b>Enable</b>	Check the box to enable the station control function.
<b>Connection Time / Reconnection Time</b>	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose <b>User defined</b> . 
<b>Display All Station</b>	All the wireless stations connecting to Vigor router by using

**Control List**

such SSID will be listed on Station Control List.

After finishing all the settings here, please click **OK** to save the configuration.

### 3.9.11 Roaming

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

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

**Wireless LAN (2.4GHz) >> Roaming**
**AP-assisted Client Roaming Parameters**

<input type="checkbox"/> <b>Minimum Basic Rate</b>	1	Mbps
<input checked="" type="radio"/> Disable RSSI Requirement		
<input checked="" type="radio"/> <b>Strictly Minimum RSSI</b>	-73	dBm (42%) (Default: -73)
<input checked="" type="radio"/> <b>Minimum RSSI</b>	-66	dBm (60%) (Default: -66)
with Adjacent AP RSSI over	5	dBm (Default: 5)

**Fast Roaming(WPA/802.1x)**

<input type="checkbox"/> Enable		
<b>PMK Caching</b> : Cache Period	10	minute(s) (10 ~ 600) (Default: 10)
<b>Pre-Authentication</b>		

OK

Cancel

Available settings are explained as follows:

Item	Description
<b>AP-assisted Client Roaming Parameters</b>	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 910C will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p><b>Minimum Basic Rate</b> – Check the box to use the drop down list to specify a basic rate (<b>Mbps</b>). When the link rate of the wireless station is below such value, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Disable RSSI Requirement</b> - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p><b>Strictly Minimum RSSI</b> - VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (<b>dBm</b>) set here, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Minimum RSSI</b> - When the signal strength of the wireless station is below the value (<b>dBm</b>) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of <b>With Adjacent AP RSSI</b></p>



	<p><b>over</b>) is detected by VigorAP 910C, VigorAP 910C will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI).</p> <ul style="list-style-type: none"> <li>● <b>With Adjacent AP RSSI over</b> – Specify a value as a threshold.</li> </ul>
<p><b>Fast Roaming (WPA/802.1x)</b></p>	<p><b>Enable</b> – Check the box to enable fast roaming configuration.</p> <p><b>PMK Cache Period</b> - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for <b>WPA2/802.1</b> mode.</p> <p><b>Pre-Authentication</b> - 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)</p> <p><b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.</p> <p><b>Disable</b> - Disable IEEE 802.1X Pre-Authentication.</p>

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

### 3.9.12 Band Steering

Band Steering detects if the wireless clients are capable of 5GHz operation, and steers them to that frequency. It helps to leave 2.4GHz band available for legacy clients, and improves users experience by reducing channel utilization.



If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



**Note:** To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

Open **Wireless LAN (2.4GHz)>>Band Steering** to get the following web page:

**Wireless LAN (2.4GHz) >> Band Steering**

Enable **Band Steering**

Check Time for WLAN Client 5G Capability  seconds (1 ~ 60, Default: 15)

5GHz Minimum RSSI  dBm ( %) (Default: -78)

(Only do band steering when 5GHz signal is better than Minimum RSSI)

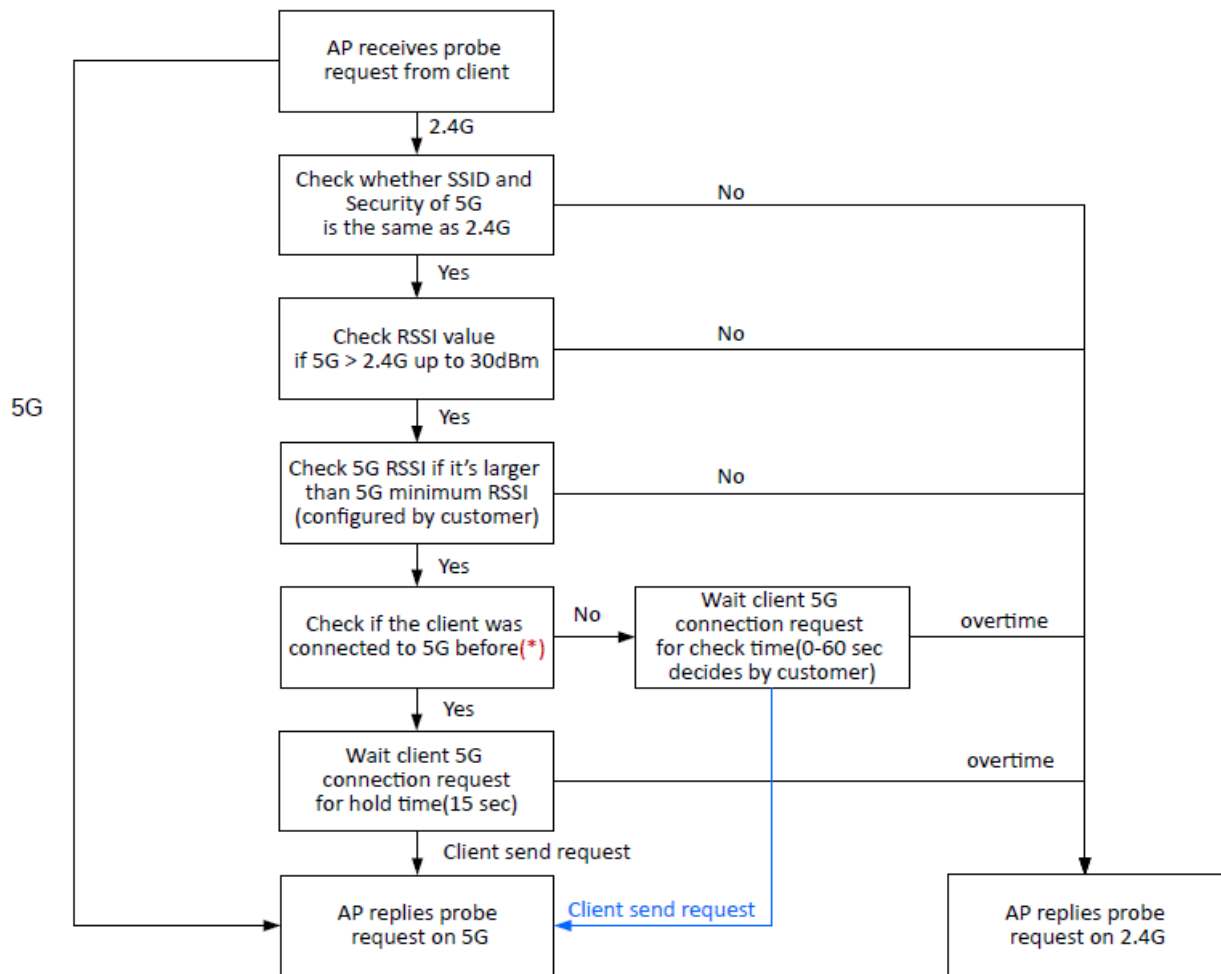
**Note:** Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
<b>Enable Band Steering</b>	<p>If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit.</p> <p><b>Check Time....</b> – If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for VigorAP to detect the wireless client.</p> <p><b>5GHz Minimum RSSI</b> - The wireless station has the capability of 5GHz network connection, yet the signal performance might not be satisfied. Therefore, when the signal strength is below the value set here while the wireless station connecting to VigorAP, VigorAP will allow the client to connect to 2.4GHz network.</p>

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

Below shows how Band Steering works.



\* AP will clear the 5G history station list every 2.5 mins.

## How to Use Band Steering?

1. Open **Wireless LAN(2.4GHz)>>Band Steering**.
2. Check the box of **Enable Band Steering** and use the default value (15) for check time setting.

### Wireless LAN >> Band Steering

Enable **Band Steering**  
Check Time for WLAN Client 5G Capability  second(s) (1 ~ 60) (Default: 15)

**Note :** Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>>General Setup**. Configure SSID as *ap910C-BandSteering* for both pages. Click **OK** to save the settings.

### Wireless LAN (2.4GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

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

Mode :

	Hide SSID	SSID	Isolate Member	VLAN ID	MAC Clone
1	<input type="checkbox"/>	ap910C-BandSteerin	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
2	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>	
3	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>	
4	<input type="checkbox"/>		<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.  
**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

Same value for 2.4GHz and 5GHz

### Wireless LAN (5GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

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

Mode :

	Hide SSID	SSID	Isolate Member	VLAN ID
1	<input type="checkbox"/>	ap910C-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>		<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 :   
Details : 20MHz / 40MHz Ext Ch: 40 , 80MHz Center Ch: 42

- Open **Wireless LAN (2.4GHz)>>Security** and **Wireless LAN (5GHz)>>Security**. Configure Security as 12345678 for both pages. Click **OK** to save the settings.

**Wireless LAN (2.4GHz) >> Security Settings**

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap910C-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
<b>WEP</b>			
<input type="radio"/> Key 1 : <input type="text"/> Hex			
<input type="radio"/> Key 2 : <input type="text"/> Hex			
<input type="radio"/> Key 3 : <input type="text"/> Hex			
<input type="radio"/> Key 4 : <input type="text"/> Hex			
802.1x WEP			
<input type="radio"/> Disable <input type="radio"/> Enable			

Same value for 2.4GHz and 5GHz

**Wireless LAN (5GHz) >> Security Settings**

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap910C-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
PMK Cache Period			
10 minutes			
Pre-Authentication			
<input type="radio"/> Disable <input type="radio"/> Enable			
<b>WEP</b>			
<input checked="" type="radio"/> Key 1 : <input type="text"/> Hex			
<input type="radio"/> Key 2 : <input type="text"/> Hex			
<input type="radio"/> Key 3 : <input type="text"/> Hex			
<input type="radio"/> Key 4 : <input type="text"/> Hex			

- Now, VigorAP 910C will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

### 3.9.13 Station List

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

#### General

Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station.

Wireless LAN (2.4GHz) >> Station List

**Station List**

							General	Advanced	Control	Neighbor
Index	MAC Address	Vendor	RSSI	Approx. Distance	SSID	Visit Time				
1	DA:A1:19:E2:65:AD		5% (-88dBm)	141.25m	N/A	0d:0h:0m:0s				
2	00:50:7F:F0:BD:2B	DrayTek	52% (-69dBm)	15.85m	N/A	0d:0h:0m:0s				
3	00:50:7F:37:6D:E5	DrayTek	47% (-71dBm)	19.95m	N/A	0d:0h:0m:0s				
4	1C:4B:D6:8B:9C:00	Azurewav	18% (-83dBm)	79.43m	N/A	0d:1h:0m:0s				
5	00:15:AF:A5:24:A0	Azurewav	26% (-79dBm)	50.12m	N/A	0d:0h:0m:0s				
6	B0:34:95:22:50:FD	Apple	47% (-71dBm)	19.95m	N/A	0d:0h:0m:0s				
7	B4:52:7E:D6:68:9D	Sony	20% (-82dBm)	70.79m	N/A	0d:0h:0m:0s				
8	00:1F:3C:51:9C:55	Intel	39% (-74dBm)	28.18m	N/A	0d:1h:0m:0s				

Refresh

**Add to Access Control:**

Client's MAC Address :  :  :  :  :  :

- Note:**
1. Approx. Distance is calculated by actual signal strength of device detected. Inaccuracy might occur based on barrier encountered.
  2. Due to the differences in signal strength for different devices, the calculated value of approximate distance also might be different.
  3. Trademarks and brand names are the properties of their respective owners.

Add

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>Hostname</b>	Display the host name of the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - 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.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

**Advanced**

Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

**Control**

Display connection and reconnection time of the wireless stations.

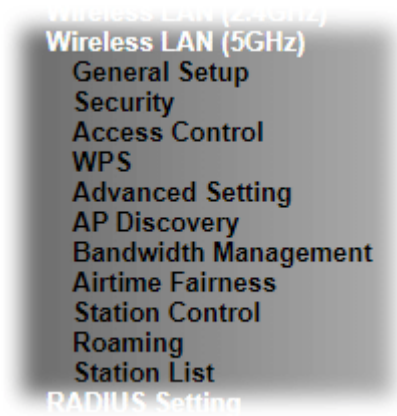
**Neighbor**

Display more information for the neighboring wireless stations.



### 3.10 Wireless LAN (5GHz) Settings for AP Mode

When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery, WMM Configuration, Bandwidth Management, Airtime Fairness, Station Control, Roaming and Station List.



#### 3.10.1 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 (5GHz) >> General Setup

---

General Setting ( IEEE 802.11 )

Enable Wireless LAN

Enable Client Limit  (3 ~ 64, default: 64)

Enable Client Limit per SSID (3 ~ 64, default: 64)

---

Mode :  ▼

Channel :  ▼ (Active Channel: 0)

Details : Wireless 5G Disabled.

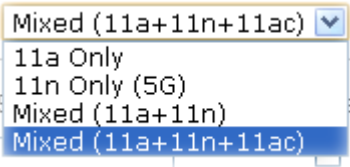
---

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek5G"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

**Hide SSID:** Prevent SSID from being scanned.  
**Isolate LAN:** Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.  
**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.  
**Isolate Exception:** Isolate Exception can be created by adding the MAC from [Device Object](#).

Available settings are explained as follows:

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

<b>Enable Client Limit</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor device. The number you can set is from 3 to 64.
<b>Enable Client Limit per SSID</b>	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
<b>Mode</b>	<p>VigorAP 910C can connect to stations supporting 11a Only, 11n Only (5G), Mixed (11a+11n) or Mixed (11a+11n+11ac).</p> 
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Hide SSID</b>	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 910C while site surveying. The system allows you to set three sets of SSID for different usage.
<b>SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Isolate LAN</b>	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	<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>

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

### 3.10.2 Security

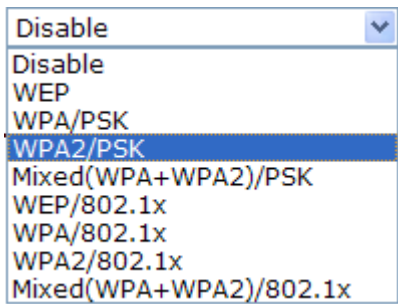
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

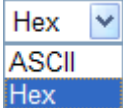
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek5G			
Mode: WPA2/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms: <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES			
Pass Phrase: .....			
Key Renewal Interval: 3600 seconds			
EAPOL Key Retry: <input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<b>WEP</b>			
<input checked="" type="radio"/> Key 1 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 2 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text"/>	Hex

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are several modes provided for you to choose.</p>  <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - 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><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 910C 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><b>WPA/802.1x</b> - 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><b>WPA2/802.1x</b> - 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>
<b>WPA Algorithms</b>	<p>Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Pass Phrase</b>	<p>Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Key Renewal Interval</b>	<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 <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>EAPOL Key Retry</b>	<p>EAPOL means Extensible Authentication Protocol over LAN. <b>Enable</b> - The default setting is "Enable". It can make sure that the key will be installed and used once in order to prevent key reinstallation attack.</p>
<b>Key 1 – Key 4</b>	<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 <b>WEP</b> mode.</p> 

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

<b>Item</b>	<b>Description</b>
<b>Use internal RADIUS Server</b>	<p>There is a RADIUS server built in VigorAP 910C 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, <b>3.13 RADIUS Server</b> to configure settings for internal server of VigorAP 910C.</p>
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	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.
<b>Session Timeout</b>	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

---

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek5G Policy: <input type="text" value="Disable"/>			
<b>MAC Address Filter</b>			
Index	MAC Address	Comment	
<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>			
<input type="radio"/> MAC <input checked="" type="radio"/> Object Device Group: <input type="text" value="None"/> or Device Object: <input type="text" value="None"/>			
<input type="button" value="Add"/> 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="text" value="選擇檔案"/> 未選擇任何檔案	
<input type="button" value="Restore"/>			

Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , 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 910C. <div style="border: 1px solid gray; 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>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>MAC</b>	<b>Client's MAC Address</b> - Manually enter the MAC address of wireless client. <b>Add</b> - Add a new MAC address into the list. <b>Delete</b> - Delete the selected MAC address in the list. <b>Edit</b> - Edit the selected MAC address in the list.
<b>Object</b>	In addition to enter the MAC address of the device manually, you can


	<p><b>Device Group</b> - Select one of the existed device groups and click <b>Add</b>. All the devices belonging to the selected group will be shown on the MAC Address Filter table.</p> <p><b>Device Object</b> - Select one of the existed device object and click <b>Add</b>. The MAC address of the device will be shown on the MAC Address Filter table.</p>
<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	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 WPS

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

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

Enable WPS 

**Wi-Fi Protected Setup Information**


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek5G
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES


**Device Configure**


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

Status: Idle

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

 : WPS is Disabled.

 : WPS is Enabled.

 : Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 910C is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 910C. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 910C.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 910C will wait for WPS requests from wireless clients about two minutes. (You need to setup WPS

	within two minutes)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. (You need to setup WPS within two minutes).

### 3.10.5 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

Wireless LAN (5GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input type="radio"/> Auto 20/40 MHz <input checked="" type="radio"/> Auto 20/40/80 MHz
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Note: Fragment Length takes effect when mode is "11a Only".

Available settings are explained as follows:

Item	Description
<b>Channel Bandwidth</b>	<p><b>20 MHz-</b> the AP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHz</b> –VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz) shall be used to meet the air situation. Usually, 40MHz would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), 20MHz will be used by VigorAP automatically to ensure smooth network transmission.</p> <p><b>Auto 20/40/80 MHz</b> –VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz or 80MHz) shall be used to meet the air situation. Usually, large bandwidth would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), small bandwidth will be used by VigorAP automatically to ensure smooth network transmission.</p>
<b>Tx Power</b>	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.
<b>Fragment Length (256 – 2346)</b>	Set the Fragment threshold. Do not modify default value if you don't know what it is, default value is 2346.



<b>RTS Threshold (1 – 2347)</b>	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold. Do not modify default value if you don't know what it is, default value is 2347.
<b>Country Code</b>	VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
<b>Auto Channel Reselect</b>	Enable – Usually, wireless channel determined by AutoSelect ( <b>Wireless LAN&gt;&gt;General Setup</b> ) means Vigor router will search for a channel with low interference automatically once the system reboots. However, when the channel utilization is more than 70% (refer to <b>Diagnostics &gt;&gt; Interference Monitor</b> ), Vigor router will search for and switch another channel with low interference to obtain better wireless signal again.
<b>Auto Channel Filtered Out List</b>	The selected wireless channels will be discarded if <b>AutoSelect</b> is selected as <b>Channel</b> selection mode in <b>Wireless LAN&gt;&gt;General Setup</b> .
<b>IGMP Snooping</b>	Check <b>Enable</b> to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
<b>Isolate 2.4GHz and 5GHz bands</b>	The default setting is “Enable”. It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa. For WLAN 2.4GHz and 5GHz set with the same SSID name: <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	The default setting is “Disable”. If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>APSD Capable</b>	APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by

minimizing transmission latency.

The default setting is **Disable**.

### 3.10.6 AP Discovery

VigorAP 910C 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 (5GHz) >> Access Point Discovery

##### Access Point List

Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
1	Draytek5G	00:1D:AA:3D:4F:17	59%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
2	AP902_5g_1...	02:1D:AA:38:4F:17	56%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
3	DrayTek_5G	00:1D:AA:F3:B9:32	59%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
4	DrayTek5G	00:1D:AA:80:06:BA	94%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
5	APMttester-...	00:1D:AA:3D:4F:15	59%	36	TKIP/AES	WPA2/PSK
6	APMttester-...	00:1D:AA:74:DA:3A	98%	36	TKIP/AES	WPA2/PSK
7	MK-2925-ma...	00:1D:AA:D4:9E:D2	100%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
8	DrayTek5G-...	00:50:7F:22:33:46	59%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
9	DrayTek5G-...	02:50:7F:22:33:46	59%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
10	DrayTek_5G	00:1D:AA:EA:38:C2	45%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
11	Joseph_wir...	00:1D:AA:D7:EC:8A	36%	36	AES	WPA2/PSK
12	DrayTek5G-...	00:1D:AA:3D:4F:1F	98%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
13	DrayTek5G-...	02:1D:AA:38:4F:1F	98%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
14	Alice2	00:1D:AA:51:28:22	19%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
15	DrayTek_5G	00:1D:AA:C6:4C:32	5%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
16	2925_RD8_m...	00:1D:AA:51:31:02	42%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
17	DrayTek_5G	00:1D:AA:C1:EF:8A	11%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
18	RD8_5G_wir...	00:1D:AA:5B:A0:CA	91%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
19	Draytek5G_...	00:1D:AA:9F:65:3E	45%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
20	DrayTek_5G	00:1D:AA:F7:C0:4A	100%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
21	APMttester-...	00:1D:AA:3D:98:0B	22%	36	TKIP/AES	WPA2/PSK
22	DrayTek_5G	00:1D:AA:DE:10:2A	28%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
23	AP920R-PQC...	00:1D:AA:63:2C:41	100%	48	TKIP/AES	Mixed(WPA+WPA2)/PSK
24	DrayTek5G	00:1D:AA:5C:A6:6A	15%	100	TKIP/AES	Mixed(WPA+WPA2)/PSK
25	FAE-Wendy-...	12:1D:AA:F0:6D:F2	62%	100	AES	WPA2/PSK
26	guests	02:1D:AA:9C:F6:46	5%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
27	910-RD8_5G	00:1D:AA:7F:5D:8E	92%	36	NONE	
28	DrayTek_5G	00:1D:AA:F7:C1:12	25%	36	NONE	
29	DrayTek_5G	00:1D:AA:5D:CB:32	32%	36	NONE	
30	DrayTek_5G	00:1D:AA:5D:CA:D2	42%	36	NONE	
31	DrayTek_5G...	02:1D:AA:EA:38:C2	45%	36	NONE	
32	Hotspot_5G...	00:1D:AA:CB:A3:12	100%	48	NONE	
33	Hotpost_5G...	02:1D:AA:CB:A3:12	100%	48	NONE	
34	V2133PQC5G...	00:1D:AA:66:E0:12	76%	36	NONE	
35	V2133PQC5G...	02:1D:AA:66:E0:12	76%	36	NONE	

Scan

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

Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 910C.
BSSID	Display the MAC address of the AP scanned by VigorAP 910C.

<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 910C.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button

### 3.10.7 Bandwidth Management

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

#### Wireless LAN (5GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>		<input type="checkbox"/>	
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
<b>Auto Adjustment</b>		<input type="checkbox"/>	

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

### 3.10.8 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

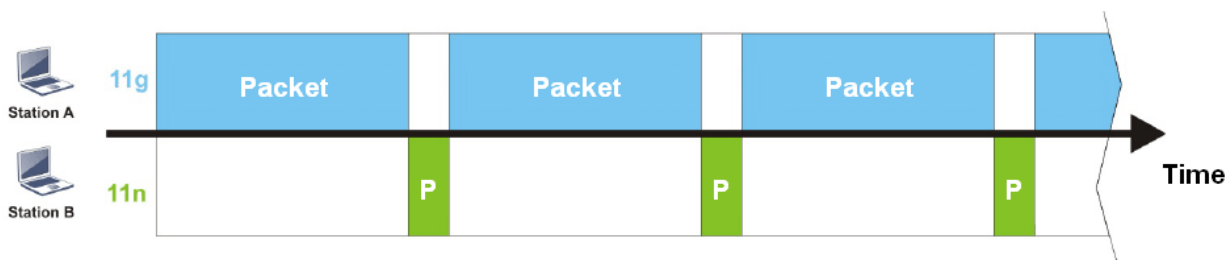
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 910C. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 910C. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

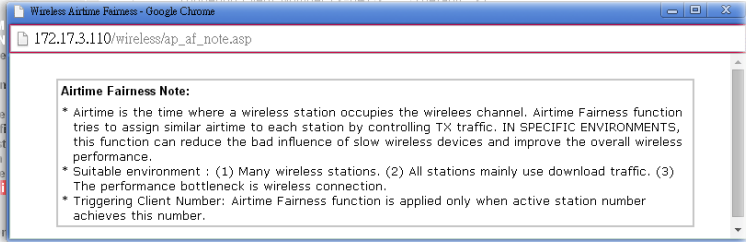
- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

**Wireless LAN (5GHz) >> Airtime Fairness**

Enable **Airtime Fairness**  
 Triggering Client Number  (2 ~ 64, Default: 2)

**Note:** Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Available settings are explained as follows:

Item	Description
<b>Enable Airtime Fairness</b>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p><b>Airtime Fairness</b> – Click the link to display the following screen of airtime fairness note.</p>  <p><b>Triggering Client Number</b> –Airtime Fairness function is applied only when active station number achieves this number.</p>

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

**Note:** Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

### 3.10.9 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect VigorAP. If such function is not enabled, the wireless client can connect VigorAP until it shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

**Note:** Up to 300 Wireless Station records are supported by VigorAP.

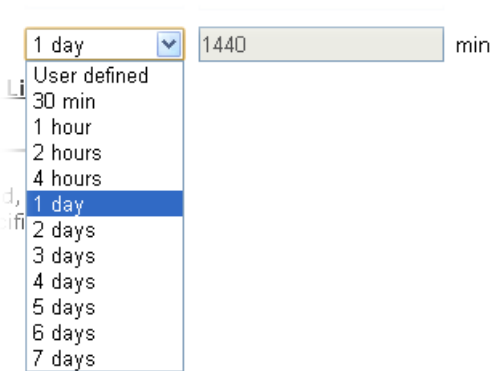
Wireless LAN (5GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G	
Enable		<input type="checkbox"/>	
Connection Time		1 hour	
Reconnection Time		User defined 0 days 0 hours 0 min	
<a href="#">Display All Station Control List</a>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

OK Cancel

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID that the wireless station will use it to connect with Vigor router.
<b>Enable</b>	Check the box to enable the station control function.
<b>Connection Time / Reconnection Time</b>	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose <b>User defined</b> . 
<b>Display All Station Control List</b>	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.

After finishing all the settings here, please click **OK** to save the configuration.

### 3.10.10 Roaming

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

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

#### Wireless LAN (5GHz) >> Roaming

##### AP-assisted Client Roaming Parameters

<input type="checkbox"/> <b>Minimum Basic Rate</b>	6 Mbps
<input checked="" type="radio"/> <b>Disable RSSI Requirement</b>	
<input type="radio"/> <b>Strictly Minimum RSSI</b>	-73 dBm (42 %) (Default: -73)
<input type="radio"/> <b>Minimum RSSI</b>	-66 dBm (60 %) (Default: -66)
with Adjacent AP RSSI over	5 dBm (Default: 5)

##### Fast Roaming(WPA2/802.1x)

<input type="checkbox"/> <b>Enable</b>	
<b>PMK Caching</b> : Cache Period	10 minute(s) (10 ~ 600) (Default: 10)
<b>Pre-Authentication</b>	

OK Cancel

Available settings are explained as follows:

Item	Description
<b>AP-assisted Client Roaming Parameters</b>	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 910C will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p><b>Minimum Basic Rate</b> – Check the box to use the drop down list to specify a basic rate (<b>Mbps</b>). When the link rate of the wireless station is below such value, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Disable RSSI Requirement</b> - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p><b>Strictly Minimum RSSI</b> - VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (<b>dBm</b>) set here, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Minimum RSSI</b> - When the signal strength of the wireless station is below the value (<b>dBm</b>) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of <b>With Adjacent AP RSSI over</b>) is detected by VigorAP 910C, VigorAP 910C will</p>



	<p>terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI).</p> <ul style="list-style-type: none"> <li>● <b>With Adjacent AP RSSI over</b> – Specify a value as a threshold.</li> </ul>
<p><b>Fast Roaming (WPA2/802.1x)</b></p>	<p><b>Enable</b> – Check the box to enable fast roaming configuration.</p> <p><b>PMK Cache Period</b> - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for <b>WPA2/802.1</b> mode.</p> <p><b>Pre-Authentication</b> - 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)</p> <p><b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.</p> <p><b>Disable</b> - Disable IEEE 802.1X Pre-Authentication.</p>

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

### 3.10.11 Station List

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

Wireless LAN (5GHz) >> Station List

Station List

Index	MAC Address	Hostname	Vendor	SSID	General	Control	Neighbor	
					Link Speed	RSSI	TxRate (Kbps)	RxRate (Kbps)
Refresh								
Add to <u>Access Control</u> :								
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>								
Add								

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>Hostname</b>	Display the host name of the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - 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.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

#### General

Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station.

#### Control

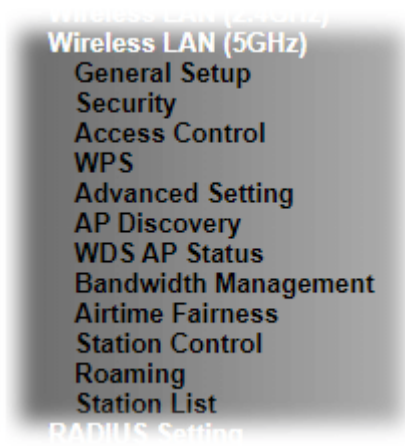
Display connection and reconnection time of the wireless stations.

#### Neighbor

Display more information for the neighboring wireless stations.

### 3.11 Wireless LAN (5GHz) 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, Advanced Setting, AP Discovery, WDS AP Status, Bandwidth Management, Airtime Fairness, Station Control, Roaming, and Station List.



### 3.11.1 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 (5GHz) >> General Setup

---

General Setting ( IEEE 802.11 )

Enable Wireless LAN

Enable Client Limit  (3 ~ 64, default: 64)

Enable Client Limit per SSID (3 ~ 64, default: 64)

---

Mode :

Channel :  (Active Channel: 0)

Details : Wireless 5G Disabled.

---

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek5G"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

**Hide SSID:** Prevent SSID from being scanned.  
**Isolate LAN:** Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.  
**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.  
**Isolate Exception:** Isolate Exception can be created by adding the MAC from [Device Object](#).

---

**WDS Settings (PHY Mode : HTMIX)**

**Security :**  
 Disabled  TKIP  AES  
 Key :

**Peer MAC Address :**

1.  :  :  :  :  :

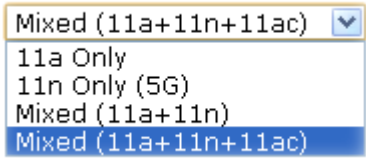
2.  :  :  :  :  :

3.  :  :  :  :  :

4.  :  :  :  :  :

Note: Enter the configuration of APs which AP910C want to connect.  
Remote AP should always use LAN or SSID1 MAC address to connect AP910C WDS.

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Client Limit</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor AP. The number you can set is from 3 to 64.
<b>Enable Client Limit per SSID</b>	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
<b>Mode</b>	At present, VigorAP 910C can connect to 11a only, 11n only (5G), Mixed (11a+11n), and Mixed (11a+11n+11ac) stations simultaneously. Simply choose Mixed (11a+11n+11ac) mode.  

<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Enable</b>	Check the box to enable the SSID configuration.
<b>Hide SSID</b>	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 910C while site surveying. The system allows you to set three sets of SSID for different usage.
<b>SSID</b>	Set a name for VigorAP 910C to be identified.
<b>Isolate LAN</b>	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.  If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
<b>PHY Mode</b>	Data will be transmitted via HTMIX mode. Each access point should be setup to the same <b>Phy Mode</b> for connecting with each other.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm.
<b>Peer MAC Address</b>	Four peer MAC addresses are allowed to be entered in this page at one time.

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

### 3.11.2 Security

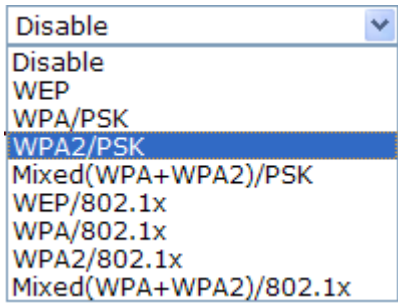
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

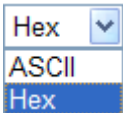
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek5G			
Mode: WPA2/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms: <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES			
Pass Phrase: .....			
Key Renewal Interval: 3600 seconds			
EAPOL Key Retry: <input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<b>WEP</b>			
<input checked="" type="radio"/> Key 1 : [ ] Hex			
<input type="radio"/> Key 2 : [ ] Hex			
<input type="radio"/> Key 3 : [ ] Hex			
<input type="radio"/> Key 4 : [ ] Hex			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are several modes provided for you to choose.</p>  <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - 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><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 910C 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><b>WPA/802.1x</b> - 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><b>WPA2/802.1x</b> - 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>
<b>WPA Algorithms</b>	<p>Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Pass Phrase</b>	<p>Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Key Renewal Interval</b>	<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 <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>EAPOL Key Retry</b>	<p>EAPOL means Extensible Authentication Protocol over LAN. <b>Enable</b> - The default setting is "Enable". It can make sure that the key will be installed and used once in order to prevent key reinstallation attack.</p>
<b>Key 1 – Key 4</b>	<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 <b>WEP</b> 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
<b>Use internal RADIUS Server</b>	There is a RADIUS server built in VigorAP 910C 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, <b>3.13 RADIUS Server</b> to configure settings for internal server of VigorAP 910C.
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	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.
<b>Session Timeout</b>	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.



### 3.11.3 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

---

SSID 1	SSID 2	SSID 3	SSID 4						
SSID: DrayTek5G Policy: <input type="text" value="Disable"/>									
<b>MAC Address Filter</b>									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Index</th> <th style="width: 60%;">MAC Address</th> <th style="width: 30%;">Comment</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="height: 100px;"> <div style="border: 1px solid gray; width: 100%; height: 100%;"></div> </td> </tr> </tbody> </table>				Index	MAC Address	Comment	<div style="border: 1px solid gray; width: 100%; height: 100%;"></div>		
Index	MAC Address	Comment							
<div style="border: 1px solid gray; width: 100%; height: 100%;"></div>									
<input type="radio"/> MAC <input checked="" type="radio"/> Object Device Group: <input type="text" value="None"/> or Device Object: <input type="text" value="None"/>									
<input type="button" value="Add"/> 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="text" value="選擇檔案"/> 未選擇任何檔案 <input type="button" value="Restore"/>									

Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , 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 910C. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <input type="text" value="Activate MAC address filter"/> <ul style="list-style-type: none"> <li>Disable</li> <li style="background-color: #e0e0e0;">Activate MAC address filter</li> <li>Blocked MAC address filter</li> </ul> </div>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>MAC</b>	<b>Client's MAC Address</b> - Manually enter the MAC address of wireless client. <b>Add</b> - Add a new MAC address into the list. <b>Delete</b> - Delete the selected MAC address in the list. <b>Edit</b> - Edit the selected MAC address in the list.
<b>Object</b>	In addition to enter the MAC address of the device manually,

	<p>you can</p> <p><b>Device Group</b> - Select one of the existed device groups and click <b>Add</b>. All the devices belonging to the selected group will be shown on the MAC Address Filter table.</p> <p><b>Device Object</b> - Select one of the existed device object and click <b>Add</b>. The MAC address of the device will be shown on the MAC Address Filter table.</p>
<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	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.

### 3.11.4 WPS

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

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

Enable WPS 

#### Wi-Fi Protected Setup Information


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek5G
<b>WPS Auth Mode</b>	WPA2/PSK
<b>WPS Encrypt Type</b>	AES


#### Device Configure


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

Status: Idle

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

 : WPS is Disabled.

 : WPS is Enabled.

 : Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 910C is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 910C. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 910C.
<b>Configure via Push</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup

<b>Button</b>	procedure. VigorAP 910C will wait for WPS requests from wireless clients about two minutes. (You need to setup WPS within two minutes)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. (You need to setup WPS within two minutes).

### 3.11.5 Advanced Setting

This page is to determine which algorithm will be selected for wireless transmission rate.

Wireless LAN (5GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input type="radio"/> Auto 20/40 MHz <input checked="" type="radio"/> Auto 20/40/80 MHz
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Note: Fragment Length takes effect when mode is "11a Only".

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Channel Bandwidth</b>	<p><b>20 MHz</b>- the device will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHz</b>– VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz) shall be used to meet the air situation. Usually, 40MHz would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), 20MHz will be used by VigorAP automatically to ensure smooth network transmission.</p> <p><b>Auto 20/40/80 MHz</b> –VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz or 80MHz) shall be used to meet the air situation. Usually, large bandwidth would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), small bandwidth will be used by VigorAP automatically to ensure smooth network transmission.</p>
<b>Tx Power</b>	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.
<b>Fragment Length</b>	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.

<b>RTS Threshold</b>	<p>Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.</p> <p>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>
<b>Country Code</b>	<p>VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.</p>
<b>IGMP Snooping</b>	<p>Click <b>Enable</b> to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group.</p> <p>Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.</p>
<b>Isolate 2.4GHz and 5GHz bands</b>	<p>The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.</p> <p>For WLAN 2.4GHz and 5GHz set with the same SSID name:</p> <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	<p>The default setting is "Disable".</p> <p>If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).</p>
<b>WMM Capable</b>	<p>To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.</p>
<b>APSD Capable</b>	<p>APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.</p> <p>The default setting is <b>Disable</b>.</p>

### 3.11.6 AP Discovery

VigorAP 910C 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 910C can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (5GHz) >> Access Point Discovery

#### Access Point List

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

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

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

Add to **WDS Settings**:

Each item is explained as follows:

Item	Description
<b>Enable AP Monitor Mode</b>	This function can help to get and keep the records of APs detected by such device after clicking Scan.  In general, only the available AP will be detected by Vigor device. Once the AP is unavailable, it will be deleted from the Access Point List immediately. However, if such function is enabled, the system will keep the record of the AP (once detected by Vigor device) until it is available for Vigor device again.
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 910C.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 910C.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 910C.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Mode</b>	Display the wireless connection mode that the scanned AP used.
<b>Ch. Width</b>	Display the channel width that the scanned AP used.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	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.
<b>Add</b>	Click <b>Repeater</b> for the specified AP. Next, click <b>Add</b> . Later, the MAC address of the AP will be added and be shown on WDS settings page.

### 3.11.7 WDS AP Status

VigorAP 910C 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 (5GHz) >> WDS AP Status

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
-----	-------------	----------------------	------------	-----------

Refresh

### 3.11.8 Bandwidth Management

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

Wireless LAN (5GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<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 Limit	User defined	K	bps (Default unit : K)
Total Download Limit	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
<b>SSID</b>	Display the specific SSID name of the AP.
<b>Enable</b>	Check this box to enable the bandwidth management for clients.
<b>Upload Limit</b>	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor AP with the same SSID. Use the drop down list to choose the rate. If you choose <b>User defined</b> , you have to specify the rate manually.
<b>Download Limit</b>	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor AP with the same SSID. Use the drop down list to choose the rate. If you choose <b>User defined</b> , you have to specify the rate manually.
<b>Auto Adjustment</b>	Check this box to have the bandwidth limit determined by the system automatically.
<b>Total Upload Limit</b>	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.
<b>Total Download Limit</b>	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.

### 3.11.10 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

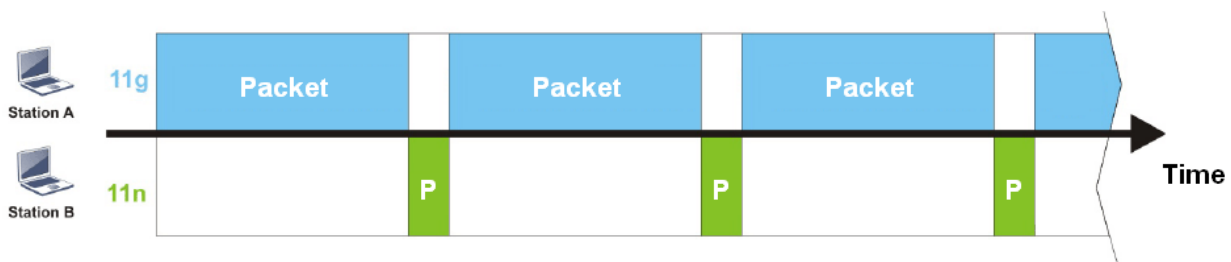
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 910C. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 910C. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).





It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

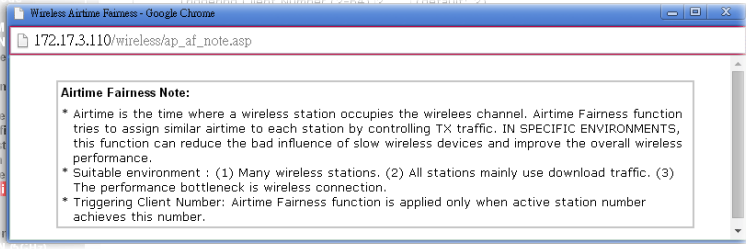
- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

#### Wireless LAN (5GHz) >> Airtime Fairness

Enable **Airtime Fairness**  
 Triggering Client Number  (2 ~ 64, Default: 2)

**Note:** Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Available settings are explained as follows:

Item	Description
<b>Enable Airtime Fairness</b>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p><b>Airtime Fairness</b> – Click the link to display the following screen of airtime fairness note.</p>  <p><b>Triggering Client Number</b> – Airtime Fairness function is applied only when active station number achieves this number.</p>

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

**Note:** Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

### 3.11.11 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect VigorAP. If such function is not enabled, the wireless client can connect VigorAP until it shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

**Note:** Up to 300 Wireless Station records are supported by VigorAP.

Wireless LAN (5GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G	
Enable		<input type="checkbox"/>	
Connection Time		1 hour	
Reconnection Time		1 day	
<a href="#">Display All Station Control List</a>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

OK Cancel

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID that the wireless station will use it to connect with Vigor router.
<b>Enable</b>	Check the box to enable the station control function.
<b>Connection Time / Reconnection Time</b>	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose <b>User defined</b> .
<b>Display All Station Control List</b>	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.

After finishing all the settings here, please click **OK** to save the configuration.

### 3.11.12 Roaming

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

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

#### Wireless LAN (5GHz) >> Roaming

##### AP-assisted Client Roaming Parameters

<input type="checkbox"/> <b>Minimum Basic Rate</b>	6 Mbps
<input checked="" type="radio"/> Disable RSSI Requirement	
<input type="radio"/> <b>Strictly Minimum RSSI</b>	-73 dBm (42%) (Default: -73)
<input type="radio"/> <b>Minimum RSSI</b>	-66 dBm (60%) (Default: -66)
with Adjacent AP RSSI over	5 dB (Default: 5)

##### Fast Roaming(WPA2/802.1x)

<input type="checkbox"/> Enable	
<b>PMK Caching</b> : Cache Period	10 minutes (10 ~ 600, Default: 10)
<b>Pre-Authentication</b>	

OK Cancel

Available settings are explained as follows:

Item	Description
<b>AP-assisted Client Roaming Parameters</b>	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 910C will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p><b>Minimum Basic Rate</b> – Check the box to use the drop down list to specify a basic rate (<b>Mbps</b>). When the link rate of the wireless station is below such value, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Disable RSSI Requirement</b> - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p><b>Strictly Minimum RSSI</b> - VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (<b>dBm</b>) set here, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Minimum RSSI</b> - When the signal strength of the wireless station is below the value (<b>dBm</b>) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of <b>With Adjacent AP RSSI over</b>) is detected by VigorAP 910C, VigorAP 910C will terminate the network connection for that wireless station. Later,</p>

	<p>the wireless station can connect to the adjacent AP (with better RSSI).</p> <ul style="list-style-type: none"> <li>● <b>With Adjacent AP RSSI over</b> – Specify a value as a threshold.</li> </ul>
<p><b>Fast Roaming (WPA/802.1x)</b></p>	<p><b>Enable</b> – Check the box to enable fast roaming configuration.</p> <p><b>PMK Cache Period</b> - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for <b>WPA2/802.1</b> mode.</p> <p><b>Pre-Authentication</b> - 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)</p> <p><b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.</p> <p><b>Disable</b> - Disable IEEE 802.1X Pre-Authentication.</p>

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

### 3.11.13 Station List

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

#### General

Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station.

Wireless LAN (5GHz) >> Station List

Station List

Index	MAC Address	Hostname	SSID	General	Control	Neighbor
				Link speed (TX/RX)	RSSI	TX Rate (Kbps)
Refresh						
<b>Add to Access Control:</b>						
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>						
Add						

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>Hostname</b>	Display the host name of the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - 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.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

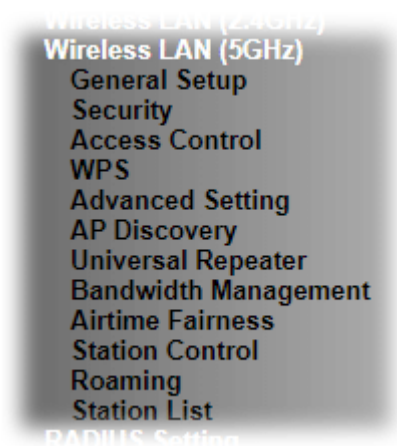
**Control**

Display connection and reconnection time of the wireless stations.

**Neighbor**

Display more information for the neighboring wireless stations.

## 3.12 Wireless LAN (5GHz) Settings for Universal Repeater Mode



### 3.12.1 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 (5GHz) >> General Setup

General Setting ( IEEE 802.11 )

Enable Wireless LAN

Enable Client Limit  (3 ~ 64, default: 64)

Enable Client Limit per SSID (3 ~ 64, default: 64)

---

Mode :  ▼

Channel :  ▼ (Active Channel: 0)

Details : Wireless 5G Disabled.

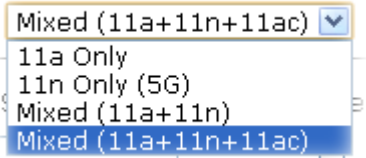
---

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek5G"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Hide SSID: Prevent SSID from being scanned.  
 Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.  
 Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.  
 Isolate Exception: Isolate Exception can be created by adding the MAC from [Device Object](#).

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Client Limit</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through VigorAP. The number

	you can set is from 3 to 64.
<b>Enable Client Limit per SSID</b>	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
<b>Mode</b>	At present, VigorAP 910C can connect to 11a only, 11n only, Mixed (11a+11n) and Mixed (11a+11n+11ac).  
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Hide SSID</b>	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 910C while site surveying. The system allows you to set four sets of SSID for different usage.
<b>SSID</b>	Set a name for VigorAP 910C to be identified. Default settings are DrayTek5G.
<b>Isolate LAN</b>	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.  If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.

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



### 3.12.2 Security

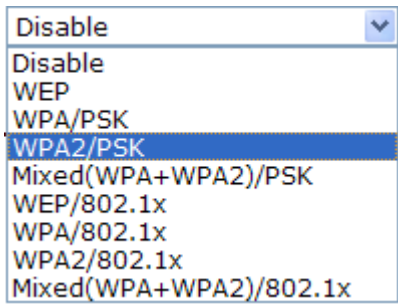
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

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

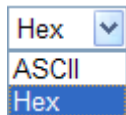
Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek5G			
Mode: WPA2/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms		<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES	
Pass Phrase		<input type="password" value="....."/>	
Key Renewal Interval		<input type="text" value="3600"/> seconds	
EAPOL Key Retry		<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
<b>WEP</b>			
<input checked="" type="radio"/> Key 1 :	<input type="text"/>	<input type="text"/>	Hex <input type="button" value="v"/>
<input type="radio"/> Key 2 :	<input type="text"/>	<input type="text"/>	Hex <input type="button" value="v"/>
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text"/>	Hex <input type="button" value="v"/>
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text"/>	Hex <input type="button" value="v"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are several modes provided for you to choose.</p>  <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - 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><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 910C 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><b>WPA/802.1x</b> - 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><b>WPA2/802.1x</b> - 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>
<b>WPA Algorithms</b>	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Pass Phrase</b>	Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key Renewal Interval</b>	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 <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>EAPOL Key Retry</b>	EAPOL means Extensible Authentication Protocol over LAN. <b>Enable</b> - The default setting is "Enable". It can make sure that the key will be installed and used once in order to prevent key reinstallation attack.
<b>Key 1 – Key 4</b>	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 <b>WEP</b> mode.



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

**RADIUS Server**

Use internal RADIUS Server

IP Address

Port

Shared Secret

Session Timeout

Available settings are explained as follows:

Item	Description
<b>Use internal RADIUS Server</b>	There is a RADIUS server built in VigorAP 910C 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, <b>3.13 RADIUS Server</b> to configure settings for internal server of VigorAP 910C.
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	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.
<b>Session Timeout</b>	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.

### 3.12.3 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

---

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek5G Policy: <input type="text" value="Disable"/>			
<b>MAC Address Filter</b>			
Index	MAC Address	Comment	
<div style="border: 1px solid black; height: 100px; width: 100%;"></div>			
<input type="radio"/> MAC <input checked="" type="radio"/> Object Device Group: <input type="text" value="None"/> or Device Object: <input type="text" value="None"/>			
<input type="button" value="Add"/> 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="text" value="選擇檔案"/> 未選擇任何檔案 <input type="button" value="Restore"/>			

Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , 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 910C. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">             Activate MAC address filter ▼              Disable              Activate MAC address filter              Blocked MAC address filter           </div>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>MAC</b>	<b>Client's MAC Address</b> - Manually enter the MAC address of wireless client. <b>Add</b> - Add a new MAC address into the list. <b>Delete</b> - Delete the selected MAC address in the list. <b>Edit</b> - Edit the selected MAC address in the list.
<b>Object</b>	In addition to enter the MAC address of the device manually, you can

	<p><b>Device Group</b> - Select one of the existed device groups and click <b>Add</b>. All the devices belonging to the selected group will be shown on the MAC Address Filter table.</p> <p><b>Device Object</b> - Select one of the existed device object and click <b>Add</b>. The MAC address of the device will be shown on the MAC Address Filter table.</p>
<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	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.

### 3.12.4 WPS

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

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

Enable WPS 

#### Wi-Fi Protected Setup Information

<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek5G
<b>WPS Auth Mode</b>	WPA2/PSK
<b>WPS Encrypt Type</b>	AES

#### Device Configure

Configure via Push Button


Start PBC


Configure via Client PinCode


Start PIN

Status: Idle

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 910C is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 910C. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 910C.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 910C will wait for WPS requests from wireless clients about two minutes. (You need to setup WPS

	within two minutes)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. (You need to setup WPS within two minutes).

### 3.12.5 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

#### Wireless LAN (5GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input type="radio"/> Auto 20/40 MHz <input checked="" type="radio"/> Auto 20/40/80 MHz
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Note: Fragment Length takes effect when mode is "11a Only".

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Channel Bandwidth</b>	<p><b>20 MHz-</b> the AP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHz-</b>VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz) shall be used to meet the air situation. Usually, 40MHz would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), 20MHz will be used by VigorAP automatically to ensure smooth network transmission.</p> <p><b>Auto 20/40/80 MHz -</b>VigorAP will scan for nearby wireless AP to determine which channel width (20MHz or 40MHz or 80MHz) shall be used to meet the air situation. Usually, large bandwidth would have better performance under the clean wireless environment (e.g., less wireless traffic / contention). When the air condition is not satisfied (e.g., dirty air), small bandwidth will be used by VigorAP automatically to ensure smooth network transmission.</p>
<b>Tx Power</b>	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.
<b>Fragment Length (256 – 2346)</b>	Set the Fragment threshold. Do not modify default value if you don't know what it is, default value is 2346.
<b>RTS Threshold (1 – 2347)</b>	<p>Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.</p> <p>Set the RTS threshold. Do not modify default value if you don't know what it is, default value is 2347.</p>

<b>Country Code</b>	VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
<b>IGMP Snooping</b>	Check <b>Enable</b> to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
<b>Isolate 2.4GHz and 5GHz bands</b>	<p>The default setting is “Enable”. It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.</p> <p>For WLAN 2.4GHz and 5GHz set with the same SSID name:</p> <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	<p>The default setting is “Disable”.</p> <p>If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).</p>
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>APSD Capable</b>	<p>APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.</p> <p>The default setting is <b>Disable</b>.</p>



### 3.12.6 AP Discovery

VigorAP 910C 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 910C can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (5GHz) >> Access Point Discovery

#### Access Point List

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="radio"/>	1	AP902_5g_1...	02:1D:AA:38:4F:17	53%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	2	APMtester-...	00:1D:AA:3D:4F:15	56%	36	TKIP/AES	WPA2/PSK
<input type="radio"/>	3	DrayTek_5G	00:1D:AA:F3:B9:32	67%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	4	RD8_5G_wir...	00:1D:AA:5B:A0:CA	92%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	5	MK-2925-ma...	00:1D:AA:D4:9E:D2	100%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	6	DrayTek_5G	00:1D:AA:F7:C0:4A	100%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	7	APMtester-...	00:1D:AA:3D:98:0B	25%	36	TKIP/AES	WPA2/PSK
<input type="radio"/>	8	DrayTek5G-...	00:1D:AA:3D:4F:1F	98%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	9	DrayTek5G-...	02:1D:AA:38:4F:1F	97%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	10	DrayTek5G-...	00:50:7F:22:33:46	62%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	11	DrayTek5G-...	02:50:7F:22:33:46	62%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	12	Draytek5G_...	00:1D:AA:9F:65:3E	56%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	13	2925_RD8_m...	00:1D:AA:51:31:02	53%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	14	Joseph_wir...	00:1D:AA:D7:EC:8A	53%	36	AES	WPA2/PSK
<input type="radio"/>	15	APMtester-...	00:1D:AA:74:DA:3A	98%	36	TKIP/AES	WPA2/PSK
<input type="radio"/>	16	DrayTek5G	00:1D:AA:80:06:BA	96%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	17	Alice2	00:1D:AA:51:28:22	15%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	18	DrayTek_5G	00:1D:AA:DE:10:2A	32%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	19	Draytek5G	00:1D:AA:3D:4F:17	53%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	20	DrayTek_5G	00:1D:AA:EA:38:C2	56%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	21	staffs	00:1D:AA:9C:F6:46	19%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	22	guests	02:1D:AA:9C:F6:46	19%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	23	DrayTek_5G	00:1D:AA:C6:4C:32	15%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	24	AP920R-PQC...	00:1D:AA:63:2C:41	100%	48	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	25	FAE-Wendy-...	12:1D:AA:F0:6D:F2	62%	100	AES	WPA2/PSK
<input type="radio"/>	26	DrayTek5G	00:1D:AA:5C:A6:6A	25%	100	TKIP/AES	Mixed(WPA+WPA2)/PSK

Scan

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

AP's MAC Address  :  :  :  :  :

AP's SSID

Select as **Universal Repeater:**

Each item is explained as follows:

Item	Description
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 910C.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 910C.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 910C.

<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	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.
<b>Select as Universal Repeater</b>	In <b>Universal Repeater</b> 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.

### 3.12.7 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 (5GHz) >> Universal Repeater

##### Universal Repeater Parameters

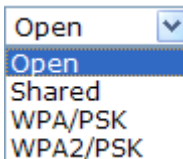
SSID	<input type="text"/>
MAC Address (Optional)	<input type="text"/>
Channel	5180MHz (Channel 36) <input type="button" value="v"/>
Security Mode	Open <input type="button" value="v"/>
Encryption Type	None <input type="button" value="v"/>
WEP Keys	
<input type="radio"/> Key 1 :	<input type="text"/> <input type="button" value="Hex"/> <input type="button" value="v"/>
<input type="radio"/> Key 2 :	<input type="text"/> <input type="button" value="Hex"/> <input type="button" value="v"/>
<input type="radio"/> Key 3 :	<input type="text"/> <input type="button" value="Hex"/> <input type="button" value="v"/>
<input type="radio"/> Key 4 :	<input type="text"/> <input type="button" value="Hex"/> <input type="button" value="v"/>

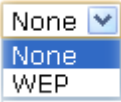
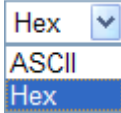


**Note:** If Channel is modified, the Channel setting of AP would also be changed.

##### Universal Repeater IP Configuration

Connection Type	DHCP <input type="button" value="v"/>
Router Name	AP910C <input type="text"/>

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Set the name of access point that VigorAP 910C wants to connect to.
<b>MAC Address (Optional)</b>	Type the MAC address of access point that VigorAP 910C wants to connect to.
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Security Mode</b>	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. 
<b>Encryption Type for</b>	This option is available when Open/Shared is selected as

<b>Open/Shared</b>	<p>Security Mode.</p> <p>Choose <b>None</b> to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose <b>WEP</b>.</p>  <p><b>WEP Keys</b> - 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> 
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>This option is available when WPA/PSK or WPA2/PSK is selected as <b>Security Mode</b>.</p> <p>Select <b>TKIP</b> or <b>AES</b> as the algorithm for WPA.</p> 
<b>Pass Phrase</b>	<p>Either <b>8~63</b> ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
<b>Connection Type</b>	<p>Choose DHCP or Static IP as the connection mode.</p> <p><b>DHCP</b> – The wireless station will be assigned with an IP from.</p> <p><b>Static IP</b> – The wireless station shall specify a static IP for connecting to Internet via VigorAP.</p> 
<b>Router Name</b>	<p>This setting is available when <b>DHCP</b> is selected as <b>Connection Type</b>.</p> <p>Type a name for the VigorAP as identification. Simply use the default name.</p>
<b>IP Address</b>	<p>This setting is available when <b>Static IP</b> is selected as <b>Connection Type</b>.</p> <p>Type an IP address with the same network segment of the LAN IP setting of VigorAP. Such IP shall be different with any IP address in LAN.</p>
<b>Subnet Mask</b>	<p>This setting is available when <b>Static IP</b> is selected as</p>

	<p><b>Connection Type.</b> Type the subnet mask setting which shall be the same as the one configured in LAN for VigorAP.</p>
<b>Default Gateway</b>	<p>This setting is available when <b>Static IP</b> is selected as <b>Connection Type.</b> Type the gateway setting which shall be the same as the default gateway configured in LAN for VigorAP.</p>

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

### 3.12.8 Bandwidth Management

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

Wireless LAN (5GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<input type="checkbox"/>		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment	<input type="checkbox"/>		

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

<b>Total Download Limit</b>	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.

### 3.12.9 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

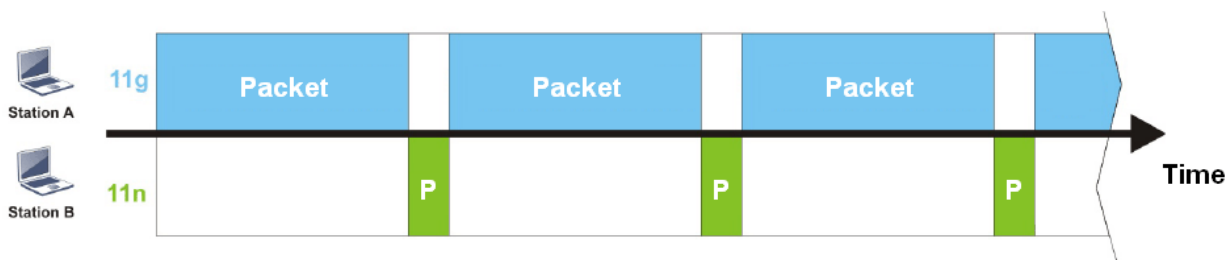
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

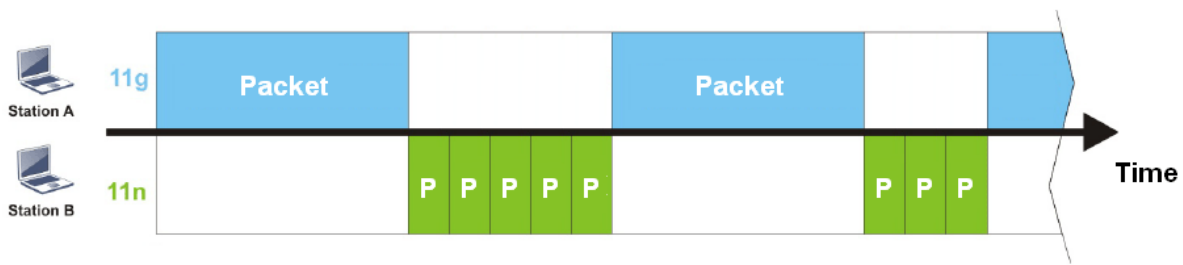
The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 910C. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 910C. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

**Wireless LAN (5GHz) >> Airtime Fairness**

Enable **Airtime Fairness**

Triggering Client Number  (2 ~ 64, Default: 2)

**Note:** Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Available settings are explained as follows:

Item	Description
<b>Enable Airtime Fairness</b>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p><b>Airtime Fairness</b> – Click the link to display the following screen of airtime fairness note.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> </div> <p><b>Triggering Client Number</b> –Airtime Fairness function is applied only when active station number achieves this number.</p>

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



**Note:** Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

### 3.12.10 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect VigorAP. If such function is not enabled, the wireless client can connect VigorAP until it shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

**Note:** Up to 300 Wireless Station records are supported by VigorAP.

Wireless LAN (5GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G	
Enable	<input type="checkbox"/>		
Connection Time		1 hour	
Reconnection Time		1 day	
<b>Display All Station Control List</b>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

OK Cancel

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID that the wireless station will use it to connect with Vigor router.
<b>Enable</b>	Check the box to enable the station control function.
<b>Connection Time / Reconnection Time</b>	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose <b>User defined</b> .
<b>Display All Station Control List</b>	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.

After finishing all the settings here, please click **OK** to save the configuration.

### 3.12.11 Roaming

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

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

#### Wireless LAN (5GHz) >> Roaming

##### AP-assisted Client Roaming Parameters

<input type="checkbox"/> <b>Minimum Basic Rate</b>	6	Mbps
<input checked="" type="radio"/> Disable RSSI Requirement		
<input type="radio"/> <b>Strictly Minimum RSSI</b>	-73	dBm (42 %) (Default: -73)
<input type="radio"/> <b>Minimum RSSI</b>	-66	dBm (60 %) (Default: -66)
with Adjacent AP RSSI over	5	dBm (Default: 5)

##### Fast Roaming(WPA2/802.1x)

<input type="checkbox"/> Enable		
<b>PMK Caching</b> : Cache Period	10	minute(s) (10 ~ 600) (Default: 10)
<b>Pre-Authentication</b>		

OK Cancel

Available settings are explained as follows:

Item	Description
<b>AP-assisted Client Roaming Parameters</b>	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 910C will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p><b>Minimum Basic Rate</b> – Check the box to use the drop down list to specify a basic rate (<b>Mbps</b>). When the link rate of the wireless station is below such value, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Disable RSSI Requirement</b> - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p><b>Strictly Minimum RSSI</b> - VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (<b>dBm</b>) set here, VigorAP 910C will terminate the network connection for that wireless station.</p> <p><b>Minimum RSSI</b> - When the signal strength of the wireless station is below the value (<b>dBm</b>) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of <b>With Adjacent AP RSSI over</b>) is detected by VigorAP 910C, VigorAP 910C will terminate the network connection for that wireless station. Later,</p>

	<p>the wireless station can connect to the adjacent AP (with better RSSI).</p> <ul style="list-style-type: none"> <li>● <b>With Adjacent AP RSSI over</b> – Specify a value as a threshold.</li> </ul>
<p><b>Fast Roaming (WPA2/802.1x)</b></p>	<p><b>Enable</b> – Check the box to enable fast roaming configuration.</p> <p><b>PMK Cache Period</b> - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for <b>WPA2/802.1</b> mode.</p> <p><b>Pre-Authentication</b> - 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)</p> <p><b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.</p> <p><b>Disable</b> - Disable IEEE 802.1X Pre-Authentication.</p>

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

### 3.12.12 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. It displays general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station.

#### General

Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station.

Wireless LAN (5GHz) >> Station List

Station List

Index	MAC Address	Hostname	SSID	General	Control	Neighbor
				Link speed (TX/RX)	RSSI	TX Rate (Kbps)
<div style="text-align: right; margin-bottom: 5px;"><input type="button" value="Refresh"/></div>						
<p>Add to <b>Access Control</b>:</p> <p>Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p> <div style="text-align: center;"><input type="button" value="Add"/></div>						

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>Hostname</b>	Display the host name of the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - 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.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

#### Control

Display connection and reconnection time of the wireless stations.

#### Neighbor

Display more information for the neighboring wireless stations.

## 3.13 RADIUS Setting

Wireless LAN (802.11)  
**RADIUS Setting**  
 RADIUS Server  
 Certificate Management  
 Applications

### 3.13.1 RADIUS Server

VigorAP 910C offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 910C. The AP can accept the wireless connection authentication requested by wireless clients.

RADIUS Setting >> RADIUS Server Configuration

Enable RADIUS Server

**Authentication Type**  
 Radius EAP Type PEAP ▼

**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 :  Upload From File:  未選擇任何檔案

Available settings are explained as follows:

Item	Description
<b>Enable RADIUS Server</b>	Check it to enable the internal RADIUS server.
<b>Authentication Type</b>	Let the user to choose the authentication method for RADIUS server.  <b>Radius EAP Type</b> – There are two types, PEAP and EAP TLS, offered for selection. If EAP TLS is selected, a certificate must be installed or must be ensured to be trusted.
<b>Users Profile</b>	<b>Username</b> – Type a new name for the user profile. <b>Password</b> – Type a new password for such new user profile. <b>Confirm Password</b> – Retype the password to confirm it.

	<p><b>Configure</b></p> <ul style="list-style-type: none"> <li>● <b>Add</b> – Make a new user profile with the name and password specified on the left boxes.</li> <li>● <b>Cancel</b> – Clear current settings for user profile.</li> </ul> <p><b>Delete Selected</b> – Delete the selected user profile (s).</p> <p><b>Delete All</b> – Delete all of the user profiles.</p>
<b>Authentication Client</b>	<p>This internal RADIUS server of VigorAP 910C 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 910C as its external RADIUS server.</p> <p><b>Client IP</b> – Type the IP address for the user to be authenticated by VigorAP 910C when the user tries to use VigorAP 910C as the external RADIUS server.</p> <p><b>Secret Key</b> – Type the password for the user to be authenticated by VigorAP 910C while the user tries to use VigorAP 910C as the external RADIUS server.</p> <p><b>Confirm Secret Key</b> – Type the password again for confirmation.</p> <p><b>Configure</b></p> <ul style="list-style-type: none"> <li>● <b>Add</b> – Make a new client with IP and secret key specified on the left boxes.</li> <li>● <b>Cancel</b> – Clear current settings for the client.</li> </ul> <p><b>Delete Selected</b> – Delete the selected client(s).</p> <p><b>Delete All</b> – Delete all of the clients.</p>
<b>Backup</b>	Click it to store the settings (RADIUS configuration) on this page as a file.
<b>Restore</b>	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.

### 3.13.2 Certificate Management

When the local client and remote server are required to make certificate authentication (e.g., Radius EAP-TLS authentication) for wireless connection and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

However, the procedure of applying digital certificate from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor AP offers a mechanism which allows you to generate root CA to save time and provide convenience for general user. Later, such root CA generated by DrayTek server can perform the issuing of local certificate.

Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.

**RADIUS Setting >> X509 Trusted CA Certificate Configuration**

Name	Subject	Status	Modify
Root CA	---	---	Create Root CA

**Note:** 1. Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA.  
2. The Time Zone MUST be setup correctly.

Click **Create Root CA** to open the following page. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name.

Click **Create Root CA** to open the following page. Type or choose all the information that the window request such as subject name, key type, key size and so on.

**RADIUS Setting >> Create Root CA**

<b>Certificate Name</b>	Root CA
<b>Subject Name</b>	
Country (C)	<input type="text"/>
State (S)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
<b>Key Type</b>	RSA ▼
<b>Key Size</b>	1024 Bit ▼
<b>Apply to Web HTTPS</b>	<input type="checkbox"/>

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Subject Name</b>	Type the required information for creating a root CA. Country (C) – Type the country code (two characters) in this box. State (S)/ Location (L)/ Organization (O)/ Organization Unit (OU) /Common Name (CN) - Type the name or information for the root CA with length less than 32 characters. Email(E) – Type the email address for the root CA with length less than 32 characters.
<b>Key Type</b>	At present, only RSA (an encryption algorithm) is supported by such device.
<b>Key Size</b>	To determine the size of a key to be authenticated, use the drop down list to specify the one you need.
<b>Apply to Web HTTPS</b>	VigorAP needs a certificate to access into Internet via Web HTTPS.

Check this box to use the user-defined root CA certificate which will substitute for the original certificate applied by web HTTPS.
---

**Note:** “Common Name” must be configured with router’s WAN IP or domain name.

After finishing this web page configuration, please click **OK** to save the settings. A new root CA will be generated.



## 3.14 Applications

Below shows the menu items for Applications.



### 3.14.1 Schedule

The Vigor AP has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the AP 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 AP's clock to current time of your PC. The clock will reset once if you power down or reset the AP. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the AP's clock. This method can only be applied when the WAN connection has been built up.

Applications >> Schedule

Schedule : Current System Time  | [System time set](#) | [Set to Factory Default](#) |

Index	Enable	Name	Action	Time	Frequency
					<input type="radio"/> Active <input type="radio"/> Finished <input type="radio"/> Not reached

Available settings are explained as follows:

Item	Description
<b>Current System Time</b>	Display current system time.
<b>System time set</b>	Click it to open Time and Date page for configuring the time setting.
<b>Set to Factory Default</b>	Click it to return to the factory default setting and remove all the schedule profiles.
<b>Index</b>	Display the sort number of the schedule profile.
<b>Enable</b>	Check it to enable the function of schedule configuration.
<b>Name</b>	Display the name of the schedule.
<b>Action</b>	Display the action adopted by the schedule profile.
<b>Time</b>	Display the time setting of the schedule.
<b>Frequency</b>	Display the frequency of the time schedule.

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

1. Check the box of **Enable Schedule**.

- Click the **Add** button to open the following web page.

Applications >> Schedule

---

**Add Schedule**

Enable

Name

Start Date  -  -  ( Year - Month - Day )

Start Time  :  ( Hour : Minute )

Duration Time  :  ( Hour : Minute )

End Time  :  ( Hour : Minute )

Action

WiFi(2.4GHz)  Radio  SSID2  SSID3  SSID4

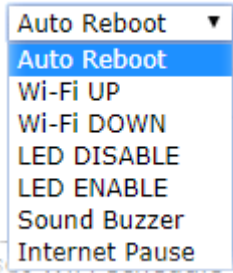
WiFi(5GHz)  Radio  SSID2  SSID3  SSID4

How Often

Weekday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

**Note:** 1. If we set WiFi schedule "Start Time" and "End Time" at exact same time, AP will execute the schedule without an end time.  
 2. "Internet Pause" will add Mac into ACL, so please make sure ACL isn't full before applying schedule.If ACL policy is "Disable", AP will change it to "Blocked".

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check to enable such schedule profile.
<b>Name</b>	Enter the name of the schedule profile.
<b>Start Date</b>	Specify the starting date of the schedule.
<b>Start Time</b>	Specify the starting time of the schedule.
<b>Duration Time</b>	Specify the duration (or period) for the schedule.
<b>End Time</b>	Specify the ending time of the schedule.
<b>Action</b>	Specify which action should apply the schedule.    In which, you have to specify the device object/device group profile for blocking certain wireless clients when <b>Internet Pause</b> is selected as the Action.
<b>WiFi(2.4GHz)/WiFi(5GHz)</b>	When <b>Wi-Fi UP</b> or <b>Wi-Fi DOWN</b> is selected as <b>Action</b> , you need to specify which channel will be used to apply the schedule.
<b>How Often</b>	Specify how often the schedule will be applied. <b>Once</b> -The schedule will be applied just once <b>Weekdays</b> - Specify which days in one week should perform

	the schedule.
<b>Weekday</b>	Choose and check the day to perform the schedule. It is available when <b>Weekdays</b> is selected as <b>How Often</b> .

- 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 : Current System Time  | [System time set](#) | [Set to Factory Default](#) |

Index	Enable	Name	Action	Time	Frequency	
1	<input checked="" type="checkbox"/>	Formkt	Auto Reboot	01:01	Once	<span style="color: green;">●</span> Active <span style="color: orange;">●</span> Finished <span style="color: gray;">●</span> Not reached

### 3.14.2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 910C 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	

Available settings are explained as follows:

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

### 3.14.3 Wi-Fi Auto On/Off

When VigorAP is able or unable to ping the specified host, the Wi-Fi function will be turned on or off. The purpose of such function is to avoid wireless station roaming to an AP which is unable to access Internet.

Applications >> Wi-Fi Auto On/Off

#### Wi-Fi Auto On/Off

Enable Connection Detection

Ping Host:

**When the AP is unable to ping the host:**

Wi-Fi:

Sound Buzzer:

LED:

OK

Available settings are explained as follows:

Item	Description
<b>Enable Connection Detection</b>	Check the box to enable such function.
<b>Ping Host</b>	Type an IP address (e.g., 8.8.8.8) or a domain name (e.g., google.com) for testing if the access point is stable or not.
<b>When the AP is unable to ping the host</b>	
<b>Wi-Fi</b>	<p><b>Off</b> - When the AP is unable to ping the host, the Wi-Fi connection will be turned off.</p> <p><b>No Change</b> - When the AP is unable to ping the host, the Wi-Fi connection will be on still.</p>
<b>Sound Buzzer</b>	Choose any sound buzzer. When the AP is unable to ping the host, VigorAP will make sound as a notification.
<b>LED</b>	<p><b>Off</b> - When the AP is unable to ping the host, the LED indicator will be turned off.</p> <p><b>No Change</b> - When the AP is unable to ping the host, the LED indicator will not be turned off.</p>

## 3.15 Mobile Device Management

Such feature can control / manage the mobile devices accessing the wireless network of VigorAP. VigorAP offers wireless LAN service for mobile device(s), PC users, MAC users or other users according to the policy selected.

Below shows the menu items for Mobile Device Management.



### 3.15.1 Detection






Such page displays mobile device(s) detected by VigorAP. Detected device(s) with Policy – **Pass** can access into the wireless LAN offered by VigorAP. Detected device(s) with Policy – **Block** are not allowed to access into Internet via VigorAP's WLAN.

#### Mobile Device Management >> Detection

Enable Mobile Device Management

Refresh Seconds: 10 Page: 1

[Refresh](#)

Index	OS	MAC	Vendor	Model	Policy
1		A4:3D:78:97:BC:A7	Guangdon	Detecting	Pass
2		00:EE:BD:B0:36:42	HTC	HTC	Pass
3		AC:3C:0B:8E:DE:30	Apple	Detecting	Pass
4		C8:6F:1D:1C:D9:F0	Apple	Detecting	Pass
5		30:5A:3A:AB:18:F2	ASUSTekC	Detecting	Pass

**Note :** Please make sure your internet access is available before enabling MDM.



iOS



Android



Windows



Linux



Others

OK

Cancel

Once you check/uncheck the box of **Enable Mobile Device Management** and click **OK**, VigorAP will reboot automatically to activate MDM.

At present, OS (for mobile device) categories supported by VigorAP include:

- Windows
- Linux
- iOS
- Android
- WindowsPhone
- BlackBerry
- Symbian.

### 3.15.2 Policies

Such page determines which devices (mobile, PC, MAC or others) allowed to make network connections via VigorAP or blocked by VigorAP.

#### Mobile Device Management >> Policy

Block Mobile Connections (OS:Android,iOS...)

Block PC Connections (OS:Windows,Linux,iMac...)

Block Unknown Connections (OS:Others)

---

WiFi(2.4GHz)       SSID1    SSID2    SSID3    SSID4

WiFi(5GHz)       SSID1    SSID2    SSID3    SSID4

Each item is explained as follows:

Item	Description
<b>Block Mobile Connections</b>	All of mobile devices will be blocked and not allowed to access into Internet via VigorAP.
<b>Block PC Connections</b>	All of network connections based on PC, MAC or Linux platform will be blocked and terminated.
<b>Block Unknown Connections</b>	Only the unknown network connections (unable to be recognized by Vigor router) will be blocked and terminated.
<b>WiFi (2.4GHz/5GHz)</b>	Choose the SSID to apply the above policy.

After finished the policy selection, click **OK**. VigorAP will *reboot* to activate the new policy automatically.

### 3.15.3 Statistics

The number of detected devices and the number of device(s) passed/blocked according to the policy specified in **Mobile Device Management>>Policy** can be illustrated as doughnut chart.

Mobile Device Management >> Statistics

#### Device OS Statistics



#### Policy Statistics



#### Trademark Notice and Attribution:

- The Android robot is reproduced or modified from work created and shared by Google and used according to the terms described in the [Creative Commons 3.0 Attribution](#) License.
- Android is a trademark of Google Inc..
- Tux logo was created by [Larry Ewing](#) and [The GIMP](#) in 1996.

## 3.16 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, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



### 3.16.1 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	: VigorAP910C
Device Name	: VigorAP910C
Firmware Version	: 1.3.2
Build Date/Time	: r11839 Thu Mar 26 11:56:32 CST 2020
System Uptime	: 0d 18:39:01
Operation Mode	: Universal Repeater

System	
Memory Total	: 62320 kB
Memory Left	: 11344 kB
Cached Memory	: 30572 kB / 62320 kB

LAN	
MAC Address	: 00:1D:AA:7C:CF:A4
IP Address	: 192.168.1.20
IP Mask	: 255.255.255.0

Wireless LAN (2.4GHz)	
MAC Address	: 00:1D:AA:7C:CF:A4
SSID	: DrayTek
Channel	: 11
Driver Version	: 2.7.2.0

Wireless LAN (5GHz)	
MAC Address	:
SSID	: DrayTek5G
Channel	: 36
Driver Version	: 10.2.85

**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	Display the model name of the modem.
Device Name	Display the name of VigorAP.
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.



<b>Operation Mode</b>	Display the operation mode that the device used.
<i>System</i>	
<b>Memory total</b>	Display the total memory of your system.
<b>Memory left</b>	Display the remaining memory of your system.
<i>LAN</i>	
<b>MAC Address</b>	Display the MAC address of the LAN Interface.
<b>IP Address</b>	Display the IP address of the LAN interface.
<b>IP Mask</b>	Display the subnet mask address of the LAN interface.
<i>Wireless</i>	
<b>MAC Address</b>	Display the MAC address of the WAN Interface.
<b>SSID</b>	Display the SSID of the device.
<b>Channel</b>	Display the channel that the station used for connecting with such device.

### 3.16.2 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"/>	<input type="button" value="Wizard"/>
Username	<input type="text"/>	
Password	<input type="text"/>	
	<input type="button" value="Test With Inform"/>	Event Code <input type="text" value="PERIODIC"/>
Last Inform Response Time : <span style="color: red;">●</span>		

##### CPE Settings

Enable	<input type="checkbox"/>
SSL(HTTPS) Mode	<input type="checkbox"/>
URL	<input type="text" value="http://192.168.1.11:8069/cwm/CRN.html"/>
Port	<input type="text" value="8069"/>
Username	<input type="text" value="vigor"/>
Password	<input type="password" value="*****"/>

**Note :** SSL(HTTPS) Mode only works when Vigor ACS SI is 1.1.6 and above version.

##### 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><b>URL/Username/Password</b> – 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> <p><b>Test With Inform</b> – Click it to send a message based on the event code selection to test if such AP is able to communicate with VigorACS SI server.</p> <p><b>Event Code</b> – Use the drop down menu to specify an event to perform the test.</p> <p><b>Last Inform Response Time</b> – Display the time that VigorACS server made a response while receiving Inform message from</p>

	AP last time.
<b>CPE Settings</b>	<p>Such information is useful for Auto Configuration Server (ACS).</p> <p><b>Enable</b>– Check the box to allow the CPE Client to connect with Auto Configuration Server.</p> <p><b>SSL(HTTPS) Mode</b> - Check the box to allow the CPE client to connect with ACS through SSL.</p> <p><b>Port</b> – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</p> <p><b>Username/Password</b> – Type the username and password that VigorACS can use to access into such CPE.</p>
<b>Periodic Inform Settings</b>	<p>The default setting is <b>Enable</b>. Please set interval time or schedule time for the AP to send notification to VigorACS server. Or click <b>Disable</b> to close the mechanism of notification.</p> <p><b>Interval Time</b> – Type the value for the interval time setting. The unit is “second”.</p>
<b>STUN Settings</b>	<p>The default is <b>Disable</b>. If you click <b>Enable</b>, please type the relational settings listed below:</p> <p><b>Server Address</b> – Type the IP address of the STUN server.</p> <p><b>Server Port</b> – Type the port number of the STUN server.</p> <p><b>Minimum Keep Alive Period</b> – 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><b>Maximum Keep Alive Period</b> – 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>

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

### 3.16.3 Administration Password

This page allows you to set new password.

System Maintenance >> Administration Password

#### Administrator Settings

Account	<input type="text" value="admin"/>
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>
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 Account can contain only a-z A-Z 0-9 , ~ ` ! @ \$ % ^ \* ( ) \_ + = { } [ ] | ; < > . ?  
 Authorization Password can contain only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & \* ( ) \_ + = { } [ ] \ ;  
 < > . ? /

Available settings are explained as follows:

Item	Description
<b>Account</b>	Type the name for accessing into Web User Interface.
<b>Old Password</b>	Type in current password.
<b>New Password</b>	Type in new password in this filed.
<b>Confirm Password</b>	Type the new password again for confirmation.
<b>Password Strength</b>	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.

## 3.16.4 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.

未選擇檔案

Please enter the password and click Restore to upload the configuration file.

Password (optional):

**Note:** 1. You will need the same password to do configuration restoration.  
2. The configuration file from the supported model list would be adopted.

---

**Backup**

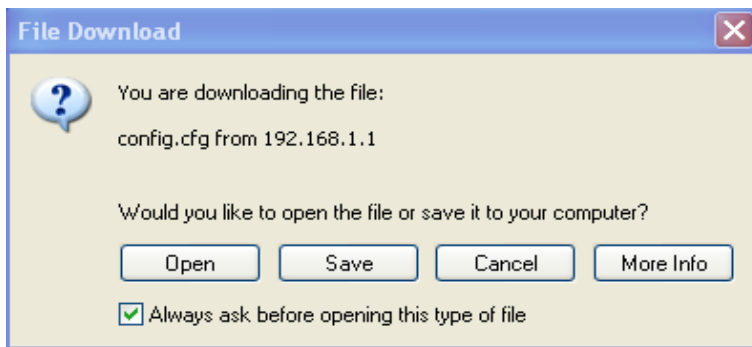
Please specify a password and click Backup to download current configuration as an encrypted file.

Protect with password

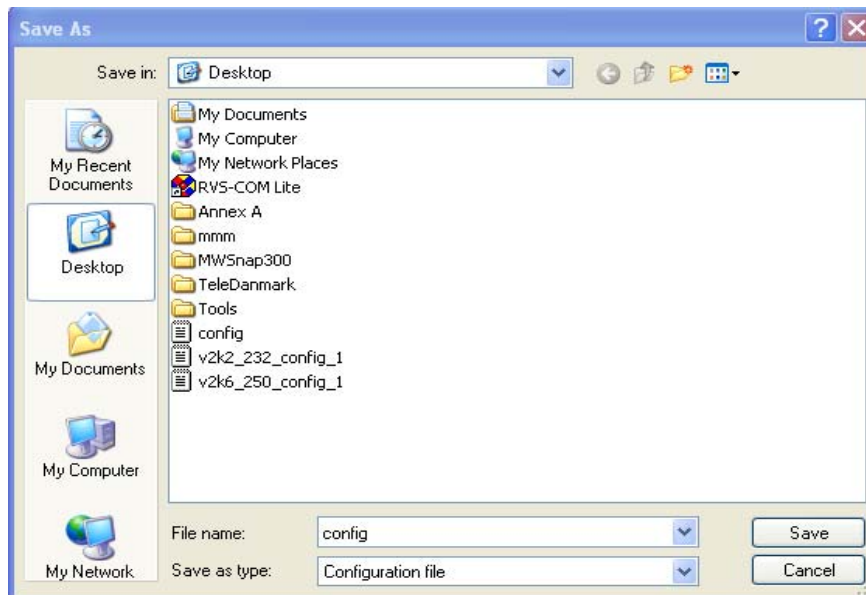
Password  (Max. 23 characters allowed)

Confirm Password

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



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



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

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

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

## Restore Configuration

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

### System Maintenance >> Configuration Backup

#### Configuration Backup / Restoration

**Restoration**

Select a configuration file.

未選擇檔案

Please enter the password and click Restore to upload the configuration file.

Password (optional):

**Note:** 1. You will need the same password to do configuration restoration.  
2. The configuration file from the supported model list would be adopted.

---

**Backup**

Please specify a password and click Backup to download current configuration as an encrypted file.

Protect with password

Password  (Max. 23 characters allowed)

Confirm Password

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

### 3.16.5 Syslog/Mail Alert

SysLog function is provided for users to monitor AP. There is no bother to directly get into the Web user interface of the AP or borrow debug equipments.

System Maintenance >> Syslog / Mail Alert Setup

#### Syslog Access Setup

Enable	<input type="checkbox"/>
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="514"/>
Log Level	All <input type="button" value="v"/>

#### Mail Alert Setup

Enable	<input type="checkbox"/>
SMTP Server	<input type="text"/>
Mail To	<input type="text"/>
Mail From	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Use TLS	<input checked="" type="checkbox"/>
Enable E-Mail Alert:	<input checked="" type="checkbox"/> When Admin Login AP

Available settings are explained as follows:

Item	Description
<b>Syslog Access Setup</b>	<p><b>Enable</b> - Check <b>Enable</b> to activate function of Syslog.</p> <p><b>Server IP Address</b> -The IP address of the Syslog server.</p> <p><b>Destination Port</b> -Assign a port for the Syslog protocol. The default setting is 514.</p> <p><b>Log Level</b> - Specify which level of the severity of the event will be recorded by Syslog.</p>
<b>Mail Alert Setup</b>	<p>Check <b>Enable</b> to activate function of mail alert.</p> <p><b>SMTP Server</b> - The IP address of the SMTP server.</p> <p><b>Mail To</b> - Assign a mail address for sending mails out.</p> <p><b>Mail From</b> - Assign a path for receiving the mail from outside.</p> <p><b>User Name</b> - Type the user name for authentication.</p> <p><b>Password</b> - Type the password for authentication.</p> <p><b>Use TLS</b> – Check this box to encrypt alert mail. However, if the SMTP server specified here does not support TLS protocol, the alert mail with encrypted data will not be received by the receiver.</p> <p><b>Enable E-Mail Alert</b> - VigorAP will send an e-mail out when a user accesses into the user interface by using web or telnet.</p>

### 3.16.6 Time and Date

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

System Maintenance >> Time and Date

#### Time Information

Current System Time	2020 May 15 Fri 10:02:01	Inquire Time
---------------------	--------------------------	--------------

#### Time Setting

<input checked="" type="checkbox"/> Enable NTP Client	
Time Zone	(GMT+08:00) China Beijing, Chongqing ▼
NTP Server	pool.ntp.org Use Default
Daylight Saving	<input type="checkbox"/>
NTP synchronization	1 day ▼

OK Cancel

Available parameters are explained as follows:

Item	Description
<b>Current System Time</b>	Click <b>Inquire Time</b> to get the current time.
<b>Enable NTP Client</b>	Select to inquire time information from Time Server on the Internet using assigned protocol.
<b>Time Zone</b>	Select a time protocol.
<b>NTP Server</b>	Type the IP address of the time server. <b>Use Default</b> – Click it to choose the default NTP server.
<b>Daylight Saving</b>	Check the box to enable the daylight saving. Such feature is available for certain area.
<b>NTP synchronization</b>	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.



### 3.16.7 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the authentication method (support MD5) for the management needs.

System Maintenance >> SNMP

#### SNMP Agent

<input type="checkbox"/> Enable SNMPv1 / SNMPv2c Agent	
Get Community	<input type="text" value="public"/>
<input type="checkbox"/> Enable SNMPv3 Agent	
USM User	<input type="text"/>
Auth Algorithm	<input type="text" value="No Auth"/>
Auth Password	<input type="text"/>

Note: SNMP V1/V2c is read-only and SNMP V3 is read-write.

Available parameters are explained as follows:

Item	Description
<b>Enable SNMPv1 / SNMPv2c Agent</b>	Check it to enable this function.
<b>Enable SNMPV3 Agent</b>	Check it to enable this function.
<b>USM User</b>	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
<b>Auth Algorithm</b>	Choose one of the encryption methods listed below as the authentication algorithm.
<b>Auth Password</b>	Type a password for authentication. The maximum length of the text is limited to 23 characters.

### 3.16.8 Management

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

System Maintenance >> Management

Device Name <input type="text" value="VigorAP910C"/>																			
<b>Access Control</b> <input checked="" type="checkbox"/> Allow management from WLAN <input checked="" type="checkbox"/> Enable Telnet Server	<b>Port Setup</b> HTTP Port <input type="text" value="80"/> ( Default:80 ) HTTPS Port <input type="text" value="443"/> ( Default:443 )																		
<b>Access List</b> <input type="checkbox"/> Enable access list <table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Mask</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td><input type="text"/></td> <td>255.255.255.255 / 32 ▼</td> </tr> <tr> <td>2.</td> <td><input type="text"/></td> <td>255.255.255.255 / 32 ▼</td> </tr> <tr> <td>3.</td> <td><input type="text"/></td> <td>255.255.255.255 / 32 ▼</td> </tr> <tr> <td>4.</td> <td><input type="text"/></td> <td>255.255.255.255 / 32 ▼</td> </tr> <tr> <td>5.</td> <td><input type="text"/></td> <td>255.255.255.255 / 32 ▼</td> </tr> </tbody> </table>	List	IP	Mask	1.	<input type="text"/>	255.255.255.255 / 32 ▼	2.	<input type="text"/>	255.255.255.255 / 32 ▼	3.	<input type="text"/>	255.255.255.255 / 32 ▼	4.	<input type="text"/>	255.255.255.255 / 32 ▼	5.	<input type="text"/>	255.255.255.255 / 32 ▼	<b>Panel Control</b> <input type="checkbox"/> Disable LED
List	IP	Mask																	
1.	<input type="text"/>	255.255.255.255 / 32 ▼																	
2.	<input type="text"/>	255.255.255.255 / 32 ▼																	
3.	<input type="text"/>	255.255.255.255 / 32 ▼																	
4.	<input type="text"/>	255.255.255.255 / 32 ▼																	
5.	<input type="text"/>	255.255.255.255 / 32 ▼																	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>																			

Available parameters are explained as follows:

Item	Description
<b>Device Name</b>	<b>Name</b> - The default setting is VigorAP910C. Change the name if required.
<b>Access Control</b>	<b>Allow management from WLAN</b> - Enable the checkbox to allow system administrators to login from wireless LAN. <b>Enable Telnet Server</b> - The administrator / user can access into the command line interface of VigorAP remotely for configuring settings.
<b>Access List</b>	<b>Enable access list</b> - Check the box to specify that the system administrator can only login from a specific host or network defined in the list. A maximum of five IPs/subnet masks is allowed.
<b>Port Setup</b>	<b>HTTP port/HTTPS port</b> - Specify user-defined port numbers for the HTTP and HTTPS servers.
<b>Panel Control</b>	<b>Disable LED</b> - The LEDs blink always since VigorAP is powered on. Some people might not like that. Therefore the function of LED is allowed to be disabled to make people feeling comfortable and undisturbed. After checking it, all the LEDs on VigorAP will light off immediately after clicking OK. <b>Enable Default Configuration Wizard</b> - Default setting is enabled. When it is enabled, you will be guided into <b>Quick Start Wizard</b> whenever clicking the DrayTek logo on the top of the web user interface. Such function will be disabled if you have configured

---

Operation Mode, WLAN>>General Setup, WLAN>>Bandwidth Management, WLAN>>Station Control or System Maintenance>>Administration Password.
--

---

### 3.16.9 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.

### 3.16.10 Firmware Upgrade

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is [www.draytek.com](http://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

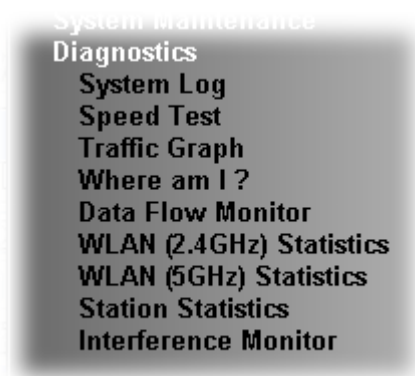
Select a firmware file.

Click Upgrade to upload the file.

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

## 3.17 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your VigorAP 910C.



### 3.17.1 System Log

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

Diagnostics >> System Log

```
System Log Information | Clear | Refresh |  Line wrap |
1d 02:05:05 syslogd started: BusyBox v1.12.1
1d 02:05:05 kernel: klogd started: BusyBox v1.12.1 (2013-11-29 14:59:53 CST)
1d 02:05:06 kernel: mng_vlan_en= 0x0
1d 02:05:06 kernel: mng_vlan_vid1= 0x0
1d 02:05:06 kernel: mng_vlan_vid2= 0x0
1d 02:05:06 kernel: flag: 0x0
1d 02:05:06 kernel: ravid 0: 0x0
1d 02:05:06 kernel: ravid 1: 0x0
1d 02:05:06 kernel: ravid 2: 0x0
1d 02:05:06 kernel: ravid 3: 0x0
1d 02:05:06 kernel: ravid 4: 0x0
1d 02:05:06 kernel: ravid 5: 0x0
1d 02:05:06 kernel: ravid 6: 0x0
1d 02:05:06 kernel: ravid 7: 0x0
1d 02:34:30 kernel: AP810 product_check ok!!!!!!^M
1d 02:34:36 kernel: AP810 product_check ok!!!!!!^M
1d 02:34:42 kernel: AP810 product_check ok!!!!!!^M
```

### 3.17.2 Speed Test

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

Diagnostics >> Speed Test

#### Speed Test

Welcome to VigorAP910C Speed Test.

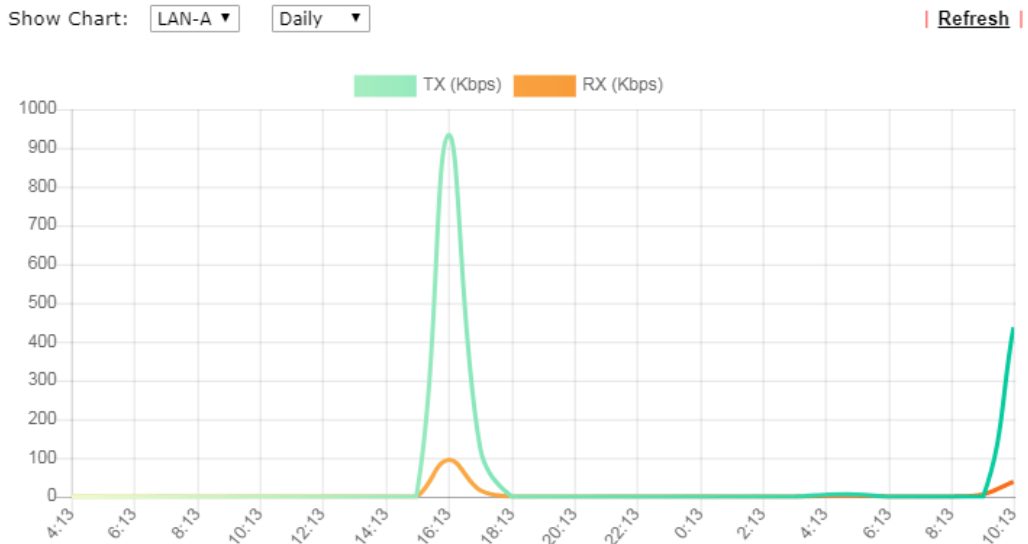
This test allows you to find out the best place for VigorAP910C. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference.

Start

### 3.17.3 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.

Diagnostics >> Traffic Graph



The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).

### 3.17.4 Where am I

This function is useful for the administrator to locate the access points to build the best signal transmitting position for multiple access points.

Diagnostics >> Where am I ?

#### Where am I ?

Welcome to VigorAP910C Where am I ?

The buzzer will sound when the "Sound" button is clicked. This is useful for network administrators to locate the access point.

Sound  ▾ for  second(s)

Available parameters are explained as follows:

Item	Description
<b>Sound</b>	Use the drop down list to specify a special sound for such access point.
<b>for XX seconds</b>	Set the duration time of the beep sound.
<b>Sound</b>	Activate the buzzer of the access point.
<b>Stop</b>	Terminate the buzzer of the access point.

### 3.17.5 Data Flow Monitor

This page displays general information for the client connecting to VigorAP 910C.

Diagnostics >> Data Flow Monitor

Index	MAC Address	Station	TX rate(Kbps)	RX rate(Kbps)	2.4G / 5G	Action
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Total			0	0		

Available parameters are explained as follows:

Item	Description
<b>Auto-refresh</b>	After checking this box, Vigor system will refresh such page periodically.
<b>Refresh</b>	Click this link to refresh this page immediately.
<b>Index</b>	Display the number of the data flow.
<b>MAC Address</b>	Display the MAC address of the monitored device.
<b>Station</b>	Display the IP address/host name of the wireless client.
<b>TX rate (kbps)</b>	Display the transmission speed of the monitored device.
<b>RX rate (kbps)</b>	Display the receiving speed of the monitored device.
<b>2.4G/5G</b>	Display what wireless band (2.4G or 5G) used by the wireless client.
<b>Action</b>	<b>DeAuth</b> – Deauthenticate a wireless station.

### 3.17.6 WLAN (2.4GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (2.4GHz) Statistics

Auto-Refresh

Tx success	18933	Rx success	642493
Tx retry count	74	Rx with CRC	1015871
Tx fail to Rcv ACK after retry	2	Rx drop due to out of resource	0
RTS Success Rcv CTS	0	Rx duplicate frame	3
RTS Fail Rcv CTS	0	False CCA (one second)	1249
TransmitCountFromOS	536	MulticastReceivedFrameCount	0
TransmittedFragmentCount	18933	RealFcsErrCount	1015871
TransmittedFrameCount	18933	WEPUndecryptableCount	0
MulticastTransmittedFrameCount	0	MultipleRetryCount	0
TransmittedAMSDUCount	0	ACKFailureCount	0
TransmittedOctetsInAMSDU	0	ReceivedAMSDUCount	0
TransmittedAMPDUCount	0	ReceivedOctetsInAMSDUCount	0
TransmittedMPDUInAMPDUCount	0	MPDUInReceivedAMPDUCount	0
TransmittedOctetsInAMPDUCount	0	fAnyStaFortyIntolerant	0

	SSID1 (DrayTek)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Packets Received	3	N/A	N/A	N/A
Packets Sent	4	N/A	N/A	N/A
Bytes Received	465	N/A	N/A	N/A
Byte Sent	396	N/A	N/A	N/A
Error Packets Received	0	N/A	N/A	N/A
Drop Received Packets	0	N/A	N/A	N/A

### 3.17.7 WLAN(5GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (5GHz) Statistics

Auto-Refresh

Tx Data Packets	0	Rx Data Packets	0
Tx Data Bytes	0	Rx Data Bytes	0
Average Tx Rate (kbps)	No Station	Average Rx Rate (kbps)	No Station
Tx Unicast Data Packets	0	Rx PHY errors	0
Tx Multi/Broadcast Data Packets	0	Rx CRC errors	52650
Tx failures	428	Rx MIC errors	0
		Rx Decryption errors	0
		Rx errors	0

	SSID1 (DrayTek5G)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Tx Data Packets	0	N/A	N/A	N/A
Tx Data Bytes	0	N/A	N/A	N/A
Tx Data BytesTx Data Payload Bytes	0	N/A	N/A	N/A
Rx Data Packets	0	N/A	N/A	N/A
Rx Data Bytes	0	N/A	N/A	N/A
Rx Data Payload Bytes	0	N/A	N/A	N/A
Tx Unicast Data Packets	0	N/A	N/A	N/A
Tx Multi/Broadcast Data Packets	0	N/A	N/A	N/A
Average Tx Rate (kbps)	No Station	N/A	N/A	N/A
Average Rx Rate (kbps)	No Station	N/A	N/A	N/A
Rx errors	0	N/A	N/A	N/A
Tx failures	428	N/A	N/A	N/A

### 3.17.8 Station Statistics

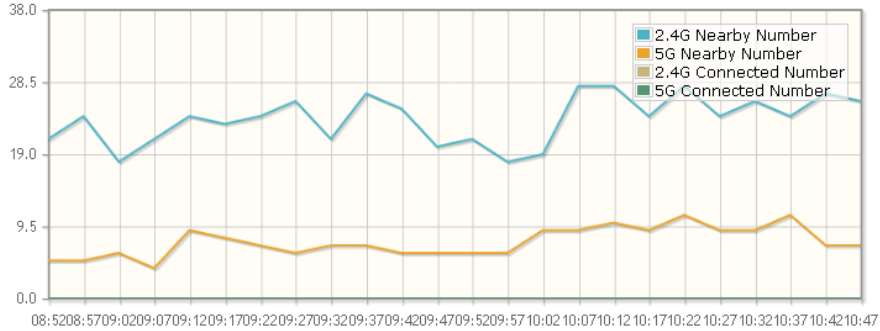
Such page is used for debug or for the user to observe network traffic and network quality.

Diagnostics >> Station Statistics

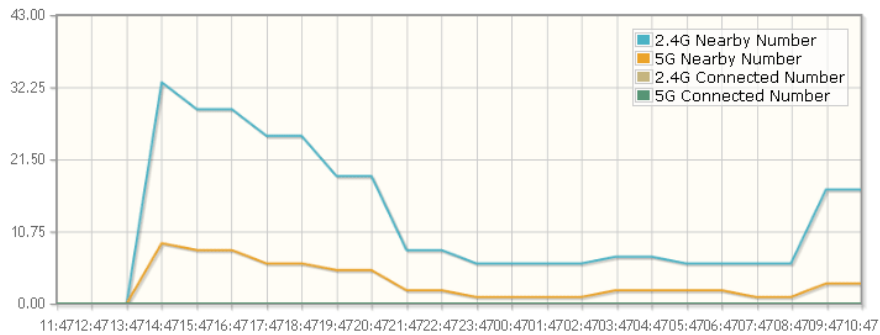
Show Chart: Nearby & Connected Number

[Refresh](#)

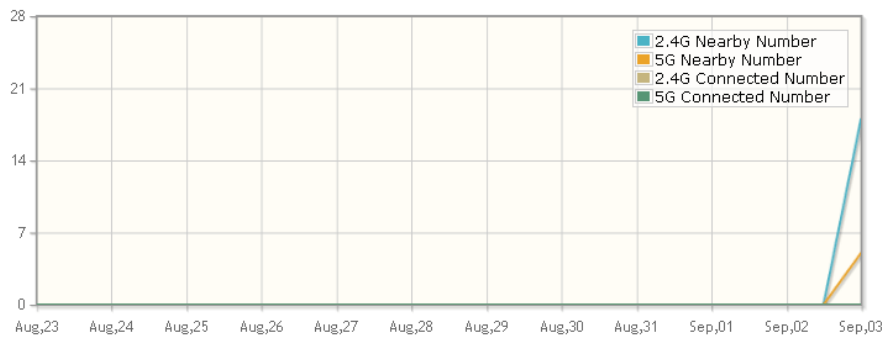
**Hourly Nearby & Connected Number**



**Daily Nearby & Connected Number** Daily Connected Number Analysis



**Weekly Nearby & Connected Number** Weekly Connected Number Analysis



Note : Only browser supporting [HTML5](#) can display Station Statistics correctly.

Available parameters are explained as follows:

Item	Description
<b>Show Chart</b>	<p>Choose one of the items to display the statistics chart for wireless stations.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <span style="border-bottom: 1px solid black; display: block; padding-bottom: 2px;">Nearby &amp; Connected Number ▾</span> <span style="border-bottom: 1px solid black; display: block; padding-bottom: 2px; background-color: #e0e0e0;">Nearby &amp; Connected Number</span> <span style="border-bottom: 1px solid black; display: block; padding-bottom: 2px;">Visiting &amp; Passing Number</span> <span style="border-bottom: 1px solid black; display: block; padding-bottom: 2px;">Visiting Time</span> </div> <p><b>Nearby &amp; Connected Number</b> – Choose it to have the</p>



statistics of the wireless stations which is nearby and connected to VigorAP 910C.

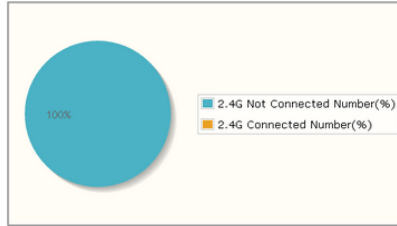
**Visiting & Passing Number** – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP 910C.

**Visiting Time** - Choose it to have the statistics of the wireless stations which is visiting VigorAP 910C.

**Daily Connected Number Analysis / Daily Visiting Number Analysis**

Click this button to get analysis pie chart for daily connected wireless stations / daily visiting wireless station.

Daily 2.4G Connected & Not Connected Number Analysis



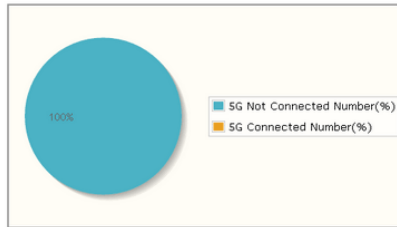
**Peak of Connected Station Number:**  
Time: 14:58-13:58 Number: 0

**Off-peak of Connected Station Number:**  
Time: 14:58-13:58 Number: 0

**Peak of Nearby Station Number:**  
Time: 19:58-20:58 Number: 12

**Off-peak of Nearby Station Number:**  
Time: 14:58-17:58 Number: 0

Daily 5G Connected & Not Connected Number Analysis



**Peak of Connected Station Number:**  
Time: 14:58-13:58 Number: 0

**Off-peak of Connected Station Number:**  
Time: 14:58-13:58 Number: 0

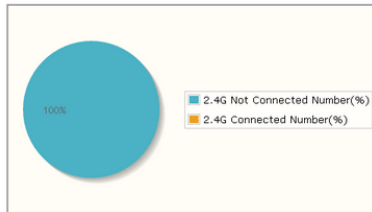
**Peak of Nearby Station Number:**  
Time: 19:58-20:58 Number: 3  
Time: 13:58 Number: 3

**Off-peak of Nearby Station Number:**  
Time: 14:58-17:58 Number: 0

**Weekly Connected Number Analysis / Weekly Visiting Number Analysis**

Click this button to get analysis pie chart for weekly connected wireless stations / weekly visiting wireless station.

Weekly 2.4G Connected & Not Connected Number Analysis



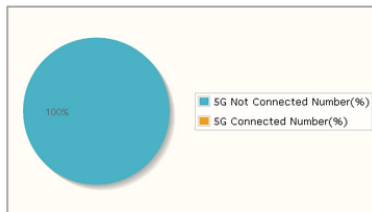
**Peak of Connected Station Number:**  
Time: 2015-8-22(Sun)-2015-9-3(Thu) Number: 0

**Off-peak of Connected Station Number:**  
Time: 2015-8-22(Sun)-2015-9-3(Thu) Number: 0

**Peak of Nearby Station Number:**  
Time: 2015-9-2(Wed) Number: 4

**Off-peak of Nearby Station Number:**  
Time: 2015-8-22(Sun)-2015-9-2(Wed) Number: 0  
Time: 2015-9-3(Thu) Number: 0

Weekly 5G Connected & Not Connected Number Analysis



**Peak of Connected Station Number:**  
Time: 2015-8-22(Sun)-2015-9-3(Thu) Number: 0

**Off-peak of Connected Station Number:**  
Time: 2015-8-22(Sun)-2015-9-3(Thu) Number: 0

**Peak of Nearby Station Number:**  
Time: 2015-9-2(Wed) Number: 1

**Off-peak of Nearby Station Number:**  
Time: 2015-8-22(Sun)-2015-9-2(Wed) Number: 0  
Time: 2015-9-3(Thu) Number: 0

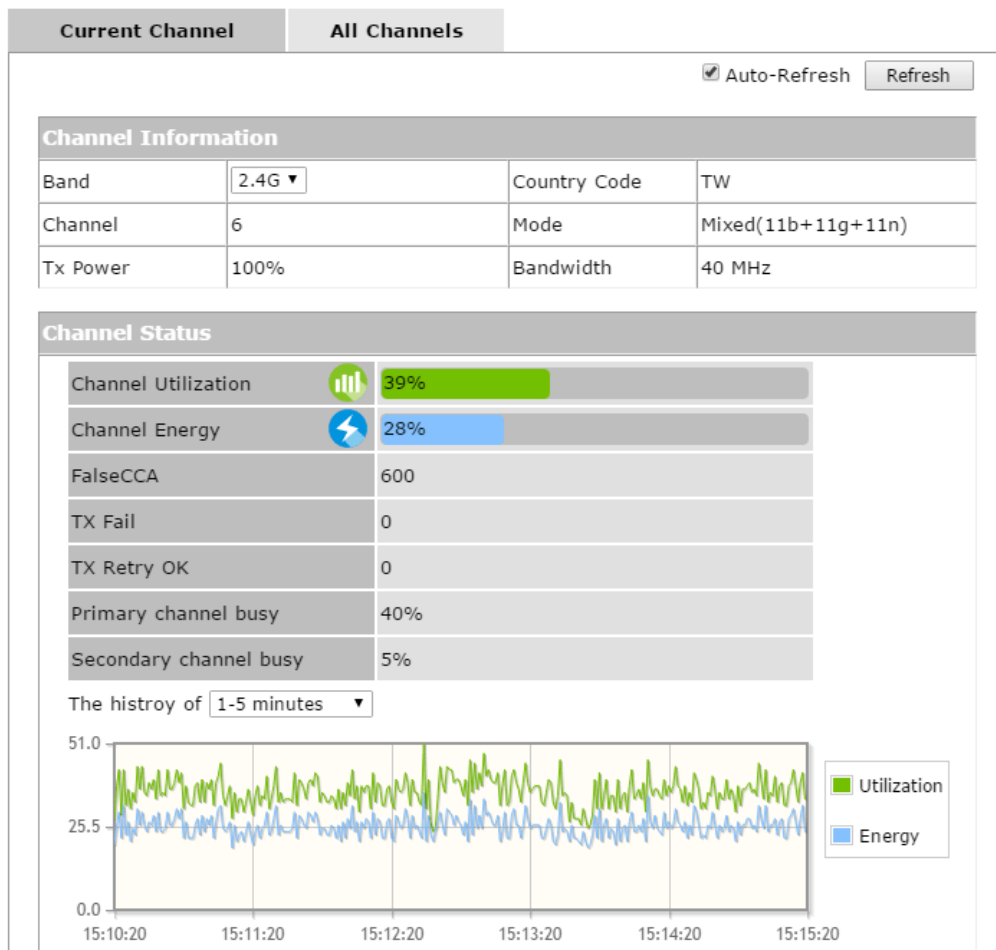
### 3.17.9 Interference Monitor

As an interference detector, VigorAP can detect all of the environmental interference factors for certain channel used or for all of the wireless channels.

#### Current Channel

The analysis page with information about wireless band, channel, transmission power, bandwidth, wireless mode, and country code chosen will be displayed on this page completely based on the wireless band (2.4G or 5G) selected. Also, channel status can be seen easily from this page.

Diagnostics >> Interference Monitor



## All Channels

This page displays the utilization and energy result for all channels based on 2.4G/5G. Click **Refresh** to get the newly update interference situation.

Diagnostics >> Interference Monitor

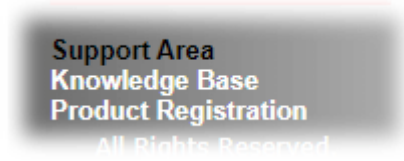
Current Channel	All Channels		
Band <span>2.4G ▾</span> <span>Refresh</span>			
Channel	Channel Utilization	Channel Energy	APs
1	43%	41%	4
2	19%	25%	0
3	9%	16%	0
4	5%	27%	0
5	7%	20%	1
6	37%	29%	11
7	7%	19%	0
8	5%	27%	0
9	9%	20%	2
10	5%	27%	0
11	48%	41%	20

Last updated: 11/04 15:15:54

**Note:** During the scanning process, no station is allowed to connect with the AP.

## 3.18 Support Area

When you click the menu item under **Support Area**, you will be guided to visit [www.draytek.com](http://www.draytek.com) and open the corresponding pages directly.



# 4

## 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 VigorAP 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.

### 4.1 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. Check the LED blinks in blue or not.
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.

## 4.2 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

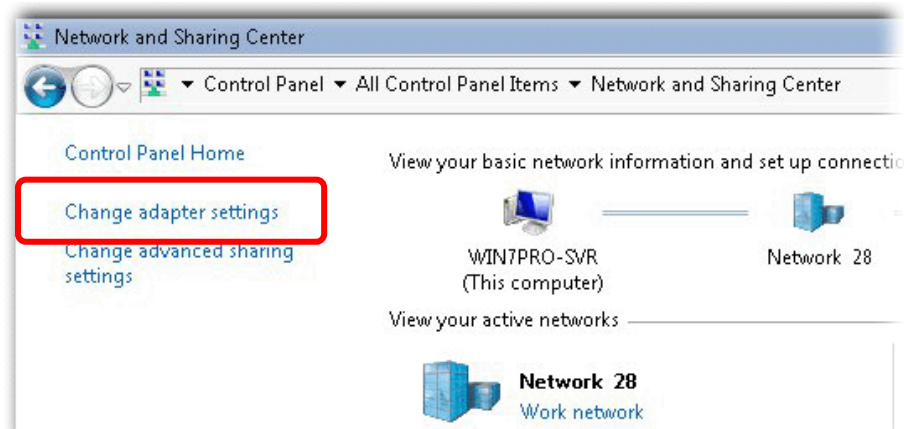


The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in [www.draytek.com](http://www.draytek.com).

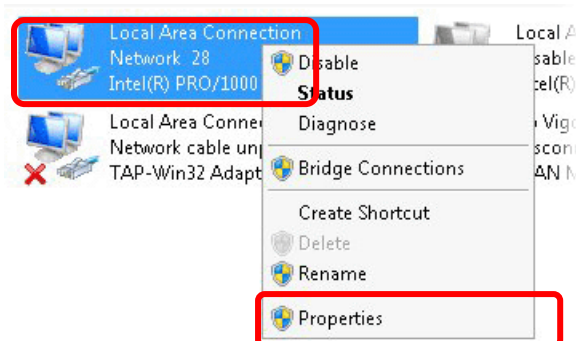
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



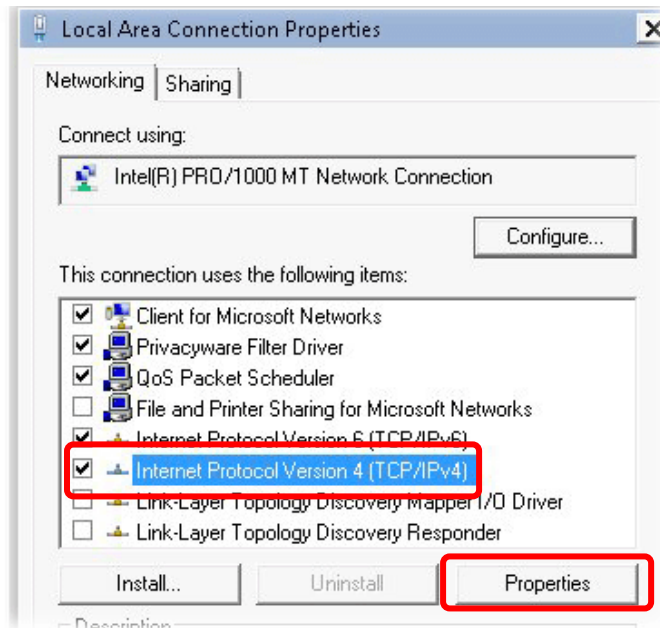
2. In the following window, click **Change adapter settings**.



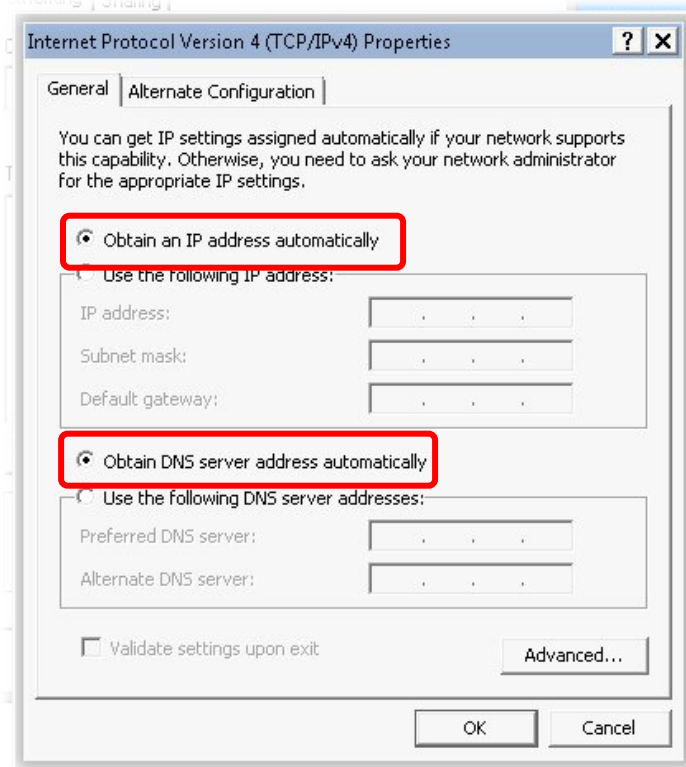
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

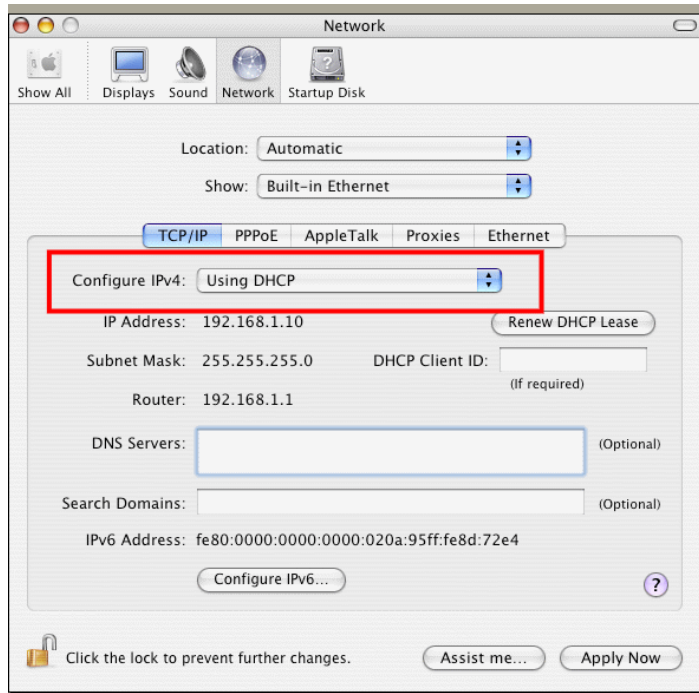


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



### 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.





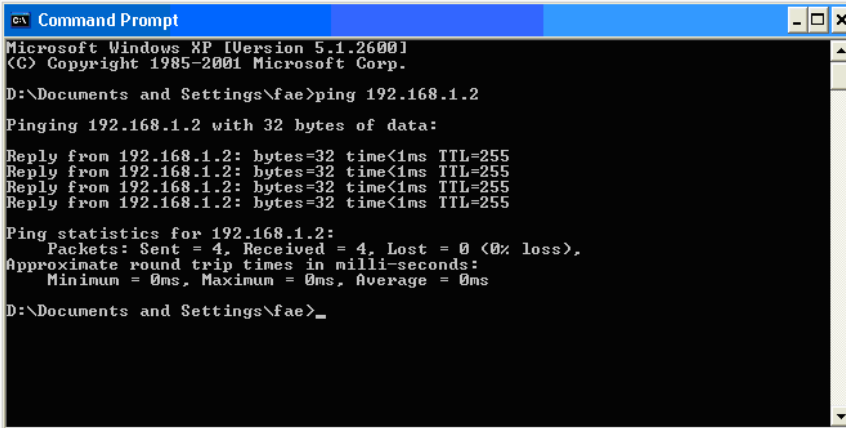
## 4.3 Pinging the VigorAP from Your Computer

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 4.2)

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$
```

## 4.4 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**

---

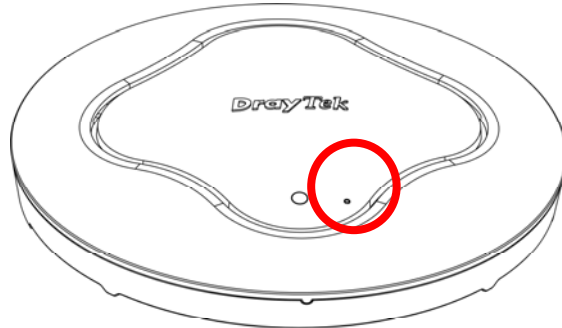
**Reboot System**

**Do You want to reboot your AP ?**

Using current configuration  
 Using factory default configuration

## Hardware Reset

While the access point 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.

## 4.5 Contacting DrayTek

If the access point 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](mailto:support@draytek.com).

This page is left blank.

# Index

## 8

802.11 Ad Hoc, 77  
802.1x WEP, 55

## A

Access Control, 56, 97, 123, 150, 169, 188  
Action, 210  
Activate MAC address filter, 97, 169  
Administrator Password, 220  
Advanced Configuration, 35  
Advanced Setting, 58, 86, 100, 125, 152, 171, 191  
AES, 26  
Airtime Fairness, 63, 106, 133, 157, 176, 199  
Antenna, 59, 87, 101, 126  
AP, 36  
AP Bridge-Point to Multi-Point, 36  
AP Bridge-Point to Multi-Point Mode, 83  
AP Bridge-Point to Point, 22, 36  
AP Bridge-Point to Point/, 83  
AP Bridge-WDS, 24, 37  
AP Bridge-WDS Mode, 91  
AP Discovery, 22, 30, 60, 89, 103, 128, 154, 173, 193  
AP Management, 44  
AP Mode, 51, 145  
AP Monitor Mode, 61, 89, 103, 128, 173  
AP Operation Mode, 21, 28  
APM Log, 45  
Apple iOS Keep Alive, 211  
Applications, 209  
Auth Mode, 57  
Authentication Client, 206  
Authentication Type, 205  
Auto Adjustment, 62, 105, 132, 156, 175, 197  
Auto Channel Filtered Out List, 59  
Auto Provision, 44  
Auto Switch, 212  
AutoSelect, 21, 130, 184

## B

Backup, 206  
Backup the Configuration, 221  
Band Steering, 68, 111, 138  
Bandwidth Limit, 21  
Bandwidth Management, 62, 105, 132, 156, 175, 197  
Black List, 46

## C

CAM, 77  
Ceiling-mount Installation, 4, 5  
Central AP Management, 44  
Certificate Management, 206  
Changing Password, 19  
Channel, 21, 52, 84, 92, 119, 130, 146, 165, 184, 195  
Channel Width, 86, 100, 125, 152, 171, 191  
Client IP, 206  
Client PinCode, 58, 99, 152, 171  
Client's MAC Address, 46, 204  
Configuration Backup, 221  
Configure via Push Button, 98, 170  
Connect to a Vigor Router, 10  
Connection Time, 65, 135, 159, 201  
Connection Type, 131, 196  
Country Code, 59, 87, 101, 126, 153, 172, 192

## D

Data Flow Monitor, 230  
Daylight Saving, 224  
Default Gateway, 131, 197  
Detection, 213  
Device Name, 131  
DHCP Client, 38  
DHCP server, 18  
DHCP Server, 38  
Diagnostics, 228  
Download Limit, 62, 105, 132, 156, 175, 197

## E

EAP Type, 205  
Encryp Type, 57  
End Time, 210  
Extension Channel, 52, 85, 92, 119

## F

Factory Default Setting, 242  
Factory Reset, 3  
Fast Roaming, 67, 110, 137, 161, 180  
Firmware Upgrade, 227  
Force Overload Disassociation, 45  
Fragment Length, 59, 87, 101, 126, 152, 171, 191  
Fragment Threshold, 78

## G

General Setup, LAN, 37  
Guest Wireless, 21

## H

Hardware Installation, 4  
Hardware Reset, 243  
Hide SSID, 52, 92, 119, 146, 165, 184  
HTMIX, 85  
HTTP port, 226  
HTTPS, 207  
HTTPS port, 226

## I

Infrastructure, 77  
Interference Monitor, 234  
Introduction, 1  
IP Address, 38, 131, 196  
Isolate Member, 52, 93, 119, 146, 165, 184

## K

Keep Alive Period, 219  
Key Renewal Interval, 54, 94, 121, 148, 167, 186  
Key Size, 207  
Key Type, 207

## L

LAN, 37  
Lease Time, 38  
LED Indicators and Connectors, 3  
Limit Client, 92, 146, 164, 183  
Limit Client per SSID, 52, 92, 119, 146, 164, 184  
Load Balance, 45  
locked MAC address filter, 97, 169

## M

MAC Address, 195  
MAC Address Filter, 56, 97  
Mac Clone, 76  
MAC Clone, 60, 127  
Main Screen, 18, 35  
Management, 226  
Management VLAN, 38  
Mobile Device Management, 213  
Mode, 52, 53, 75, 84, 92, 94, 119, 120, 146, 164, 166, 184, 185

## N

Network Configuration, 15  
Network Type, 77  
NTP, 209  
NTP Client, 224  
NTP Server, 224  
NTP synchronization, 224

## O

Once, 210  
Online Status, 34  
OPEN, 78  
Open/Shared, 26, 31, 130, 195  
Operation Mode, 20, 36  
Overload Management, 45

## P

Packet-OVERDRIVE, 58, 76, 86, 125  
Pass Phrase, 54, 78, 94, 121, 131, 148, 167, 186, 196  
Password Strength, 220  
Periodic Inform Settings, 219

Phy Mode, 24  
PHY Mode, 85  
PIN Code, 49  
Plasterboard Ceiling, 5  
PMK Cache Period, 67, 110, 161, 180, 203  
Policy, 56, 97, 123, 150, 169, 214  
Port, 55, 149, 187  
Port Control, 41  
Power Saving Mode, 77  
Pre-Authentication, 67, 110, 161, 180, 203  
Primary IP Address, 38  
PSK, 48  
Push Button, 57, 151

## Q

Quick Start Wizard, 20

## R

RADIUS Server, 55, 95, 122, 149, 168, 187, 205  
RADIUS Setting, 205  
Rate Adaptation Algorithm, 59, 87, 101, 126  
Reboot System, 227  
Reconnection Time, 65, 135, 159, 201  
Restore, 57, 206  
Restore Configuration, 222  
Roaming, 66, 109, 136, 160, 179, 202  
Router Name, 196  
Routine, 210  
RSSI, 66, 109, 136, 160, 179, 202, 203  
RTS Threshold, 59, 78, 87, 101, 126, 153, 172, 191

## S

Scan, 80, 90  
Schedule, 209  
Secret Key, 206  
Security, 53, 85, 93, 120, 147, 166, 185  
Security Key, 21  
Security Mode, 78, 130, 195  
Security Overview, 48  
Security Settings, 53  
Session Timeout, 55, 96, 122, 149, 168, 187  
SHARED, 78

Shared Secret, 55, 96, 122, 149, 168, 187  
Show Chart, 232  
Site Survey, 80  
SNMP, 225  
SNMP Agent, 225  
SNMPV3 Agent, 225  
Software Reset, 242  
Speed Test, 228  
SSID, 93, 146, 165, 184  
SSL(HTTPS), 219  
Start Date, 210  
Start PBC, 49, 57, 82, 98, 124, 151, 170, 189  
Start PIN, 58, 82, 99, 125, 152, 171, 190  
Start Time, 210  
Station Control, 21, 65, 108, 135, 159, 178, 201  
Station List, 73, 116, 143, 162, 181, 204  
Station Statistics, 232  
Station-Infrastructure, 36  
Station-Infrastructure Mode, 75  
Statistics, 81, 215  
Status of Settings, 47  
STUN, 219  
Subject Name, 207  
Subnet, 52, 93, 119, 146, 165, 184  
Subnet Mask, 38, 131, 196  
Support Area, 236  
Suspended Ceiling Installation, 6  
Syslog/Mail Alert, 223  
System Log, 228  
System Maintenance, 216  
System Status, 216

## T

Time and Date, 224  
Time Zone, 224  
TKIP, 26, 48  
TLS, 223  
Total Download Limit, 62, 105, 132, 156, 175, 198  
Total Upload Limit, 62, 105, 132, 156, 175, 197  
TR-069, 218  
Traffic Graph, 229  
traffic overload, 45

Triggering Client Number, 107, 177

Trouble Shooting, 237

Tx Power, 59, 87, 101, 126, 152, 171, 191

## U

Universal Repeater, 25, 29, 30, 37, 129, 195

Universal Repeater Mode, 118, 183

Upload Limit, 62, 105, 132, 156, 175, 197

Users Profile, 205

## V

VLAN ID, 38, 93, 119, 146, 165, 184

## W

Wall Mounting Installation, 8

WDS AP Status, 90, 104, 174

WEP, 26, 78

WEP (Wired Equivalent Privacy), 48

Where am I, 229

White List, 46

Wi-Fi DOWN, 210

Wi-Fi UP, 210

Wireless LAN(2.4GHz), 36

Wireless LAN(2.4GHz/5GHz), 48

Wireless LAN(5GHz), 37

WLAN (2.4GHz) Statistics, 231

WLAN(5GHz) Statistics, 231

Wooden Ceiling, 4

WPA (Wi-Fi Protected Access), 48

WPA Algorithms, 54, 78, 94, 121, 148, 167, 186

WPS, 57, 98, 124, 151, 170, 189

WPS (Wi-Fi Protected Setup), 49, 81

WPS Auth Mode, 98, 170

WPS Encryp Type, 98, 170