

DrayTek

VigorAP 920R Series

Ruggedized Outdoor AP with Extreme 802.11ac Power



Your reliable networking solutions partner

User's Guide

V1.0

VigorAP 920RP Series

Ruggedized Outdoor AP with Extreme 802.11ac

User's Guide

Version: 1.0

Firmware Version: V1.2.1

Date: June 5, 2018

Intellectual Property Rights (IPR) Information

Copyrights	© All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	The following trademarks are used in this document: <ul style="list-style-type: none">● Microsoft is a registered trademark of Microsoft Corp.● Windows, Windows 95, 98, Me, NT, 2000, XP, Vista, 7 and Explorer are trademarks of Microsoft Corp.● Apple and Mac OS are registered trademarks of Apple Inc.● Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions	<ul style="list-style-type: none">● Read the installation guide thoroughly before you set up the modem.● The modem is a complicated electronic unit that may be repaired only by authorized and qualified personnel. Do not try to open or repair the modem yourself.● Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.● Keep the package out of reach of children.● When you want to dispose of the modem, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.
Be a Registered Owner	Web registration is preferred. You can register your Vigor modem via http://www.draytek.com .
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents. http://www.draytek.com

Table of Contents

1

Introduction	1
1.1 Introduction	1
1.2 LED Indicators and Connectors	2
1.3 Mounting the Access Point.....	3
1.3.1 Antennas Installation	3
1.3.2 Connecting Ethernet Cable(s)	4
1.3.3 Access Point Installation – Pole Mount	6
1.3.4 Grounding Access Point	8
1.3.5 Powering Access Point.....	9

2

Network Configuration.....	11
2.1 Windows 7 IP Address Setup.....	11
2.2 Windows 2000 IP Address Setup.....	13
2.3 Windows XP IP Address Setup	14
2.4 Windows Vista IP Address Setup.....	15
2.5 Accessing to Web User Interface	16
2.6 Changing Password	17
2.7 Quick Start Wizard	18
2.7.1 Configuring Wireless Settings – General.....	18
2.7.2 Configuring 2.4GHz Wireless Settings Based on the Operation Mode.....	19
2.7.3 Configuring 5GHz Wireless Settings Based on the Operation Mode.....	25
2.7.4 Finishing the Wireless Settings Wizard	29
2.8 Online Status.....	30

3

Advanced Configuration	31
3.1 Operation Mode	32
3.2 LAN	33
3.2.1 General Setup.....	33
3.2.2 Port Control.....	36
3.3 Central AP Management	37
3.3.1 General Setup.....	37
3.3.2 APM Log	38
3.3.3 Function Support List.....	38
3.3.4 Overload Management	39
3.3.5 Status of Settings.....	40
3.4 General Concepts for Wireless LAN (2.4GHz/5GHz)	41

3.5 Wireless LAN (2.4GHz) Settings for AP Mode.....	44
3.5.1 General Setup.....	45
3.5.2 Security.....	47
3.5.3 Access Control.....	50
3.5.4 WPS.....	51
3.5.5 Advanced Setting.....	52
3.5.6 AP Discovery.....	54
3.5.7 WMM Configuration.....	55
3.5.8 Bandwidth Management.....	57
3.5.9 Airtime Fairness.....	58
3.5.10 Station Control.....	60
3.5.11 Roaming.....	61
3.5.12 Band Steering.....	63
3.5.13 Station List.....	68
3.6 Wireless LAN Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Mode ..	70
3.6.1 General Setup.....	70
3.6.2 Advanced Setting.....	72
3.6.3 AP Discovery.....	73
3.6.4 WDS AP Status.....	75
3.7 Wireless LAN (2.4GHz) Settings for AP Bridge-WDS Mode.....	76
3.7.1 General Setup.....	77
3.7.2 Security.....	79
3.7.3 Access Control.....	82
3.7.4 WPS.....	83
3.7.5 Advanced Setting.....	85
3.7.6 AP Discovery.....	86
3.7.7 WDS AP Status.....	88
3.7.8 WMM Configuration.....	89
3.7.9 Bandwidth Management.....	91
3.7.10 Airtime Fairness.....	92
3.7.11 Station Control.....	94
3.7.12 Roaming.....	95
3.7.13 Band Steering.....	97
3.7.14 Station List.....	102
3.8 Wireless LAN (2.4GHz) Settings for Universal Repeater Mode.....	104
3.8.1 General Setup.....	105
3.8.2 Security.....	107
3.8.3 Access Control.....	110
3.8.4 WPS.....	111
3.8.5 Advanced Setting.....	112
3.8.6 AP Discovery.....	114
3.8.7 Universal Repeater.....	115
3.8.8 WMM Configuration.....	117
3.8.9 Bandwidth Management.....	119
3.8.10 Airtime Fairness.....	120
3.8.11 Station Control.....	122
3.8.12 Roaming.....	123
3.8.13 Band Steering.....	125
3.8.14 Station List.....	130
3.9 Wireless LAN (5GHz) Settings for AP Mode.....	132
3.9.1 General Setup.....	132
3.9.2 Security.....	134
3.9.3 Access Control.....	137
3.9.4 WPS.....	138
3.9.5 Advanced Setting.....	139
3.9.6 AP Discovery.....	141

3.9.7 WMM Configuration	142
3.9.8 Bandwidth Management	143
3.9.9 Airtime Fairness	144
3.9.10 Station Control	146
3.9.11 Roaming	147
3.9.12 Station List	149
3.10 Wireless LAN (5GHz) Settings for Universal Repeater Mode	151
3.10.1 General Setup	151
3.10.2 Security	153
3.10.3 Access Control	156
3.10.4 WPS	157
3.10.5 Advanced Setting	158
3.10.6 AP Discovery	159
3.10.7 Universal Repeater	161
3.10.8 WMM Configuration	163
3.10.9 Bandwidth Management	165
3.10.10 Airtime Fairness	166
3.10.11 Station Control	168
3.10.12 Roaming	169
3.10.13 Station List	171
3.11 RADIUS Setting	173
3.11.1 RADIUS Server	173
3.11.2 Certificate Management	174
3.12 Applications	176
3.12.1 Schedule	176
3.12.2 Apple iOS Keep Alive	178
3.12.3 Wi-Fi Auto On/Off	179
3.12.4 Sensor	180
3.13 Mobile Device Management	183
3.13.1 Detection	183
3.13.2 Policies	184
3.13.3 Statistics	185
3.14 System Maintenance	185
3.14.1 System Status	186
3.14.2 TR-069	187
3.14.3 Administrator Password	189
3.14.4 Configuration Backup	190
3.14.5 Syslog/Mail Alert	192
3.14.6 Time and Date	194
3.14.7 SNMP	195
3.14.8 Management	196
3.14.9 Reboot System	197
3.14.10 Firmware Upgrade	197
3.15 Diagnostics	198
3.15.1 System Log	198
3.15.2 Speed Test	198
3.15.3 Traffic Graph	199
3.15.4 Where am I	199
3.15.5 Data Flow Monitor	200
3.15.6 WLAN (2.4GHz) Statistics	201
3.15.7 WLAN (5GHz) Statistics	202
3.15.8 Station Statistics	203
3.15.9 Interference Monitor	205
3.15.10 Station Airtime	206

3.15.11 Station Traffic Graph.....	207
3.15.12 Station Link Speed.....	208
3.16 Support Area	208

4

Trouble Shooting.....209

4.1 Checking If the Hardware Status Is OK or Not.....	209
4.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	210
4.3 Pinging the Modem from Your Computer.....	213
4.4 Backing to Factory Default Setting If Necessary	214
4.5 Contacting DrayTek.....	215

Index216

1

Introduction



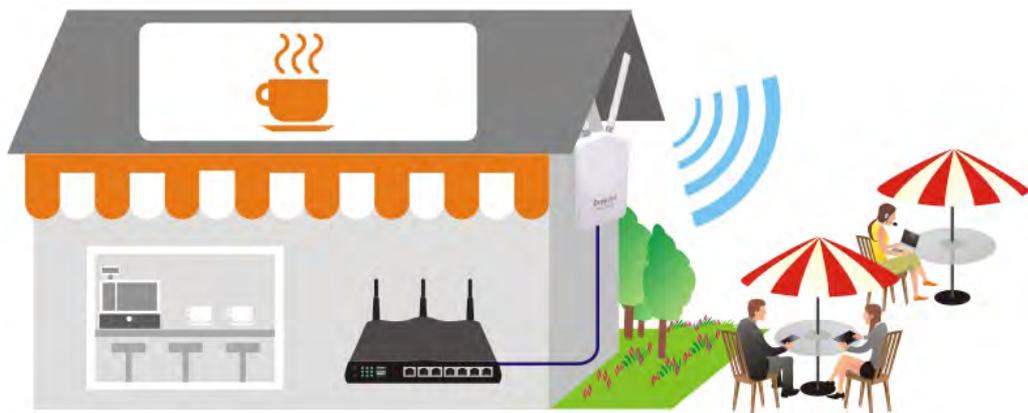
Note: This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

1.1 Introduction

Thank you for purchasing VigorAP 920R series.

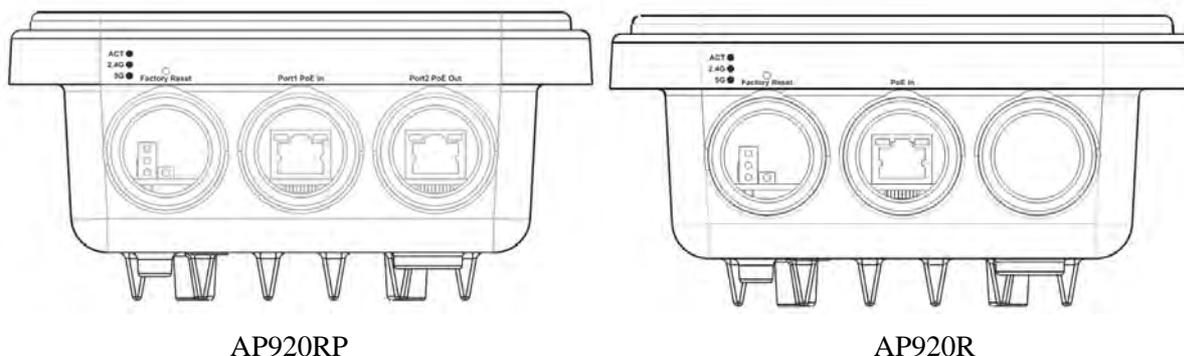
Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced users. Just follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

VigorAP 920RP also is a Power over Ethernet Powered Device which adopts the technology of PoE for offering power supply and transmitting data through the Ethernet cable.



1.2 LED Indicators and Connectors

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



LED	Status	Explanation
ACT	Off	The system is not ready or has failed.
	Blinking	The system is ready.
2.4G / 5G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is being transmitted (sending/receiving).
Interface	Description	
Factory Reset	Restore the default settings. Usage: Switch on the access point. Press and hold reset button for at least 10 seconds. The router will restart with the factory default configuration. Before pressing the button, the cover should first be removed by rotating it with a torque of 13 kgf-cm. After the access point has been reset, replace the cover and lock it with the same amount of torque.	
Port PoE In / PoE In	Connector for receiving power from another device.	
Port PoE Out (for AP920RP)	Connector for supplying power to another device.	



Note: For the sake of safety, keep the access point away from children

1.3 Mounting the Access Point

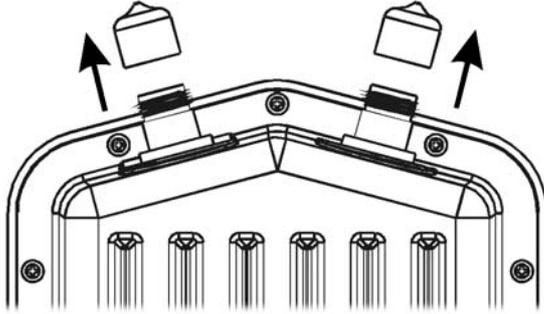
The VigorAP can be pole mounted depending on the installation environment. This section will guide you through installing the VigorAP.



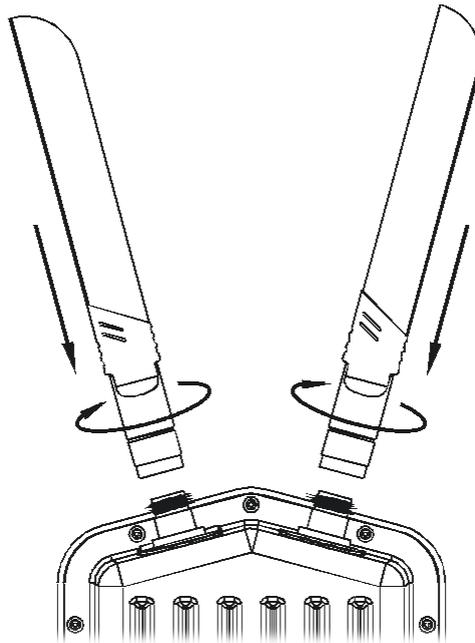
Note: For the sake of personal safety, only trained and qualified personnel should install this device.

1.3.1 Antennas Installation

1. Remove the protective cap.



2. Insert the antennas and fasten them by rotating clockwise.



Warning:
Do not open the top cover of the device.
Installation during thunderstorms could be dangerous.

1.3.2 Connecting Ethernet Cable(s)

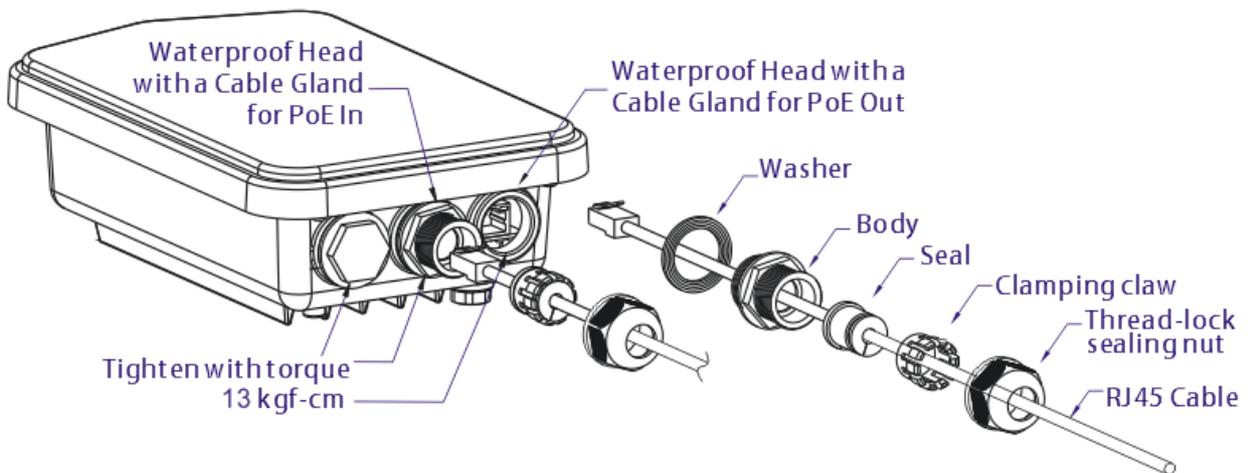
Refer to the following steps to attach the Ethernet cable and waterproof head. (Take VigorAP 920RP as an example.)

1. Remove the cable cover for Ethernet Port (e.g., **Port 1 PoE In**).
2. Before connecting, verify that the cable has a rubber seal and that it is not damaged.



Note: To prevent the enclosure from water leakage, make sure the Ethernet cable gland and the rubber gasket are present and installed properly.

3. Inserting RJ-45 connector into the port.



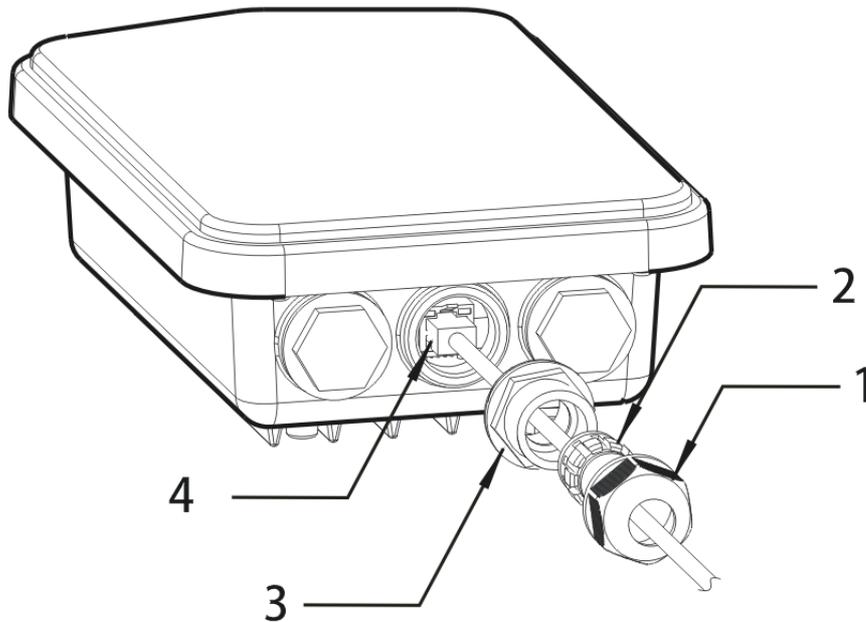
4. Use an adjustable wrench and tighten the thread-lock sealing nut with torque 10 kgf-cm.



Warning:
Do not open the top cover of the device.
Installation during thunderstorms could be dangerous.

Reconnecting Ethernet Cable

1. Loosen the thread-lock sealing nut.
2. Loosen the clamping claw and seal.
3. Loosen the body and washer.
4. Remove the cable.



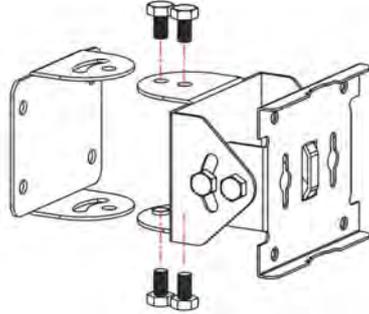
5. To reattach the cable, follow the above steps in reverse.



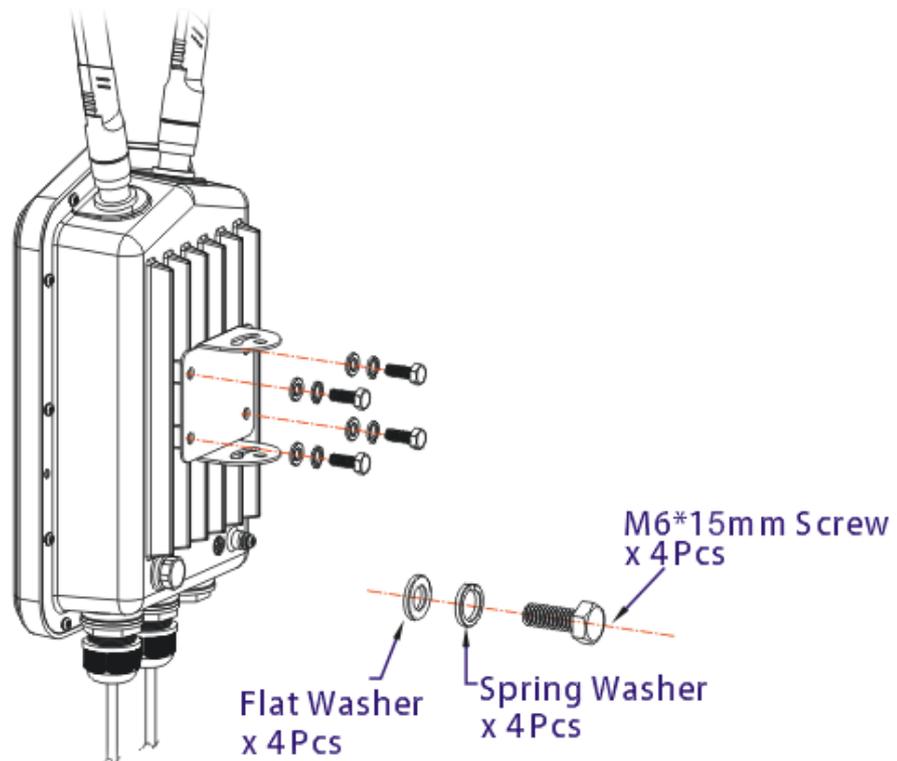
Note: The diameter for the Ethernet cable shall be limited between 4.3mm to 5.9mm.

1.3.3 Access Point Installation – Pole Mount

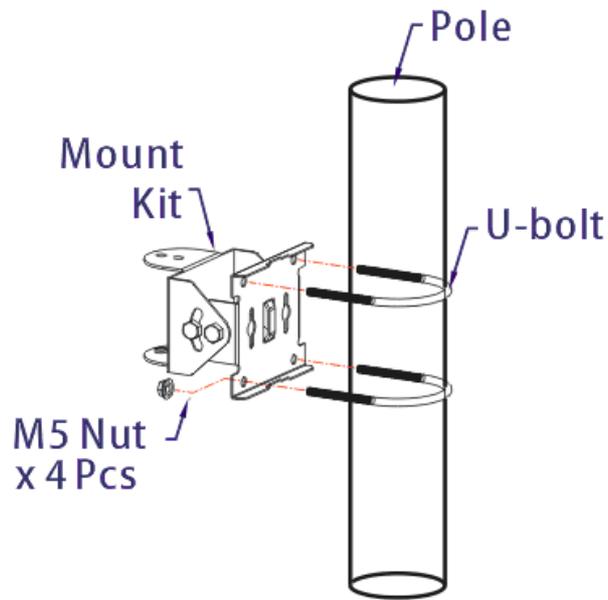
1. Find a suitable location for installing the access point.
2. Select a mounting point on a pole.
3. Remove the mounting plate from the mount kit by removing the four mounting screws.



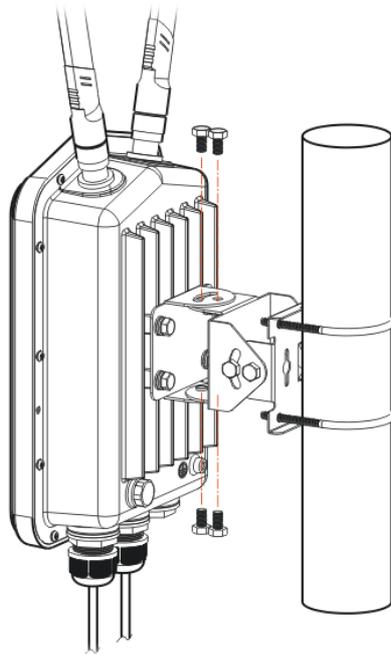
4. Attach the VigorAP920 to the mounting plate. Lock the screws with torque of 20 kgf-cm.



5. Fasten the mount kit on the pole with nut screws and with torque of 20 kgf-cm.



6. Fasten the access point to the mount kit with screws (torque of 20 kgf-cm) as shown in the following figure.

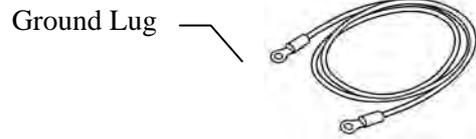


Note: Before connecting the access point to the mount kit, make sure it is oriented with the LED indicators pointing downwards.

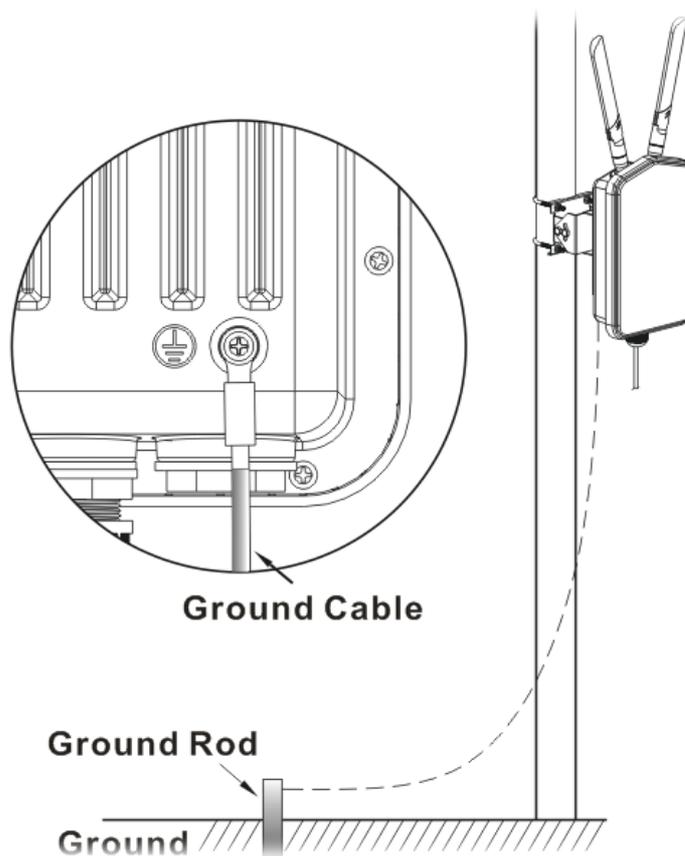
1.3.4 Grounding Access Point

In outdoor installations and before powering the access point with AC power, VigorAP must be grounded prior to wire installation.

1. Take out the ground cable from the mount kit.



2. Insert a ground rod on the ground.
3. Strip the insulation for the ground lug.
4. Use the appropriate crimping tool to crimp the ground cable to the grounding lug.
5. Connect the ground rod and the VigorAP using the ground cable.



Note: Please consult an electrician if you are uncertain about the type of grounding that is required.

1.3.5 Powering Access Point

VigorAP 920R/PR can be powered via the PoE input from an in-line power injector or a suitably powered switch port.

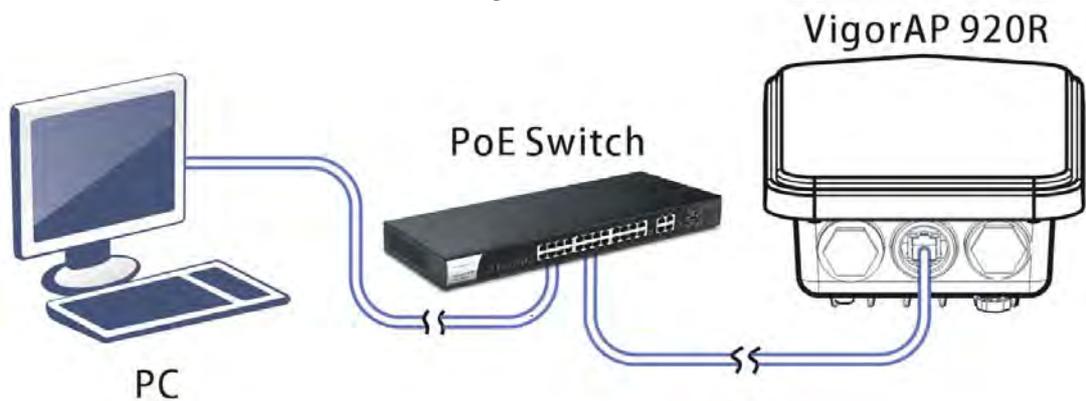


Before powering VigorAP, you should:

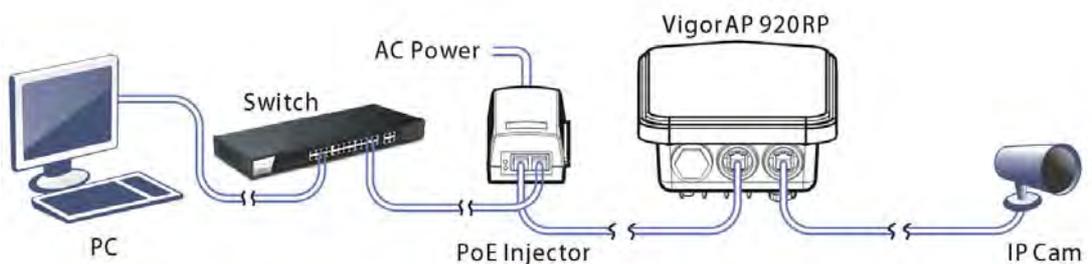
- Pay attention to local and national electrical codes.
- Not place the power injector / VigorSwitch in outdoor environment without any protection. Moisture might get into the power injector and cause a short circuit or possible fire.
- Not work on the system during periods of lightning activity to avoid the risk of electric shock, and do not connect or disconnect the Ethernet cables under bad weather.

Below shows two examples of connecting power for VigorAP 920R and VigorAP 920PR.

Example 1: AP920R



Example 2: AP920RP



This page is left blank.

2

Network Configuration

After the network connection is built, the next step you should do is setup VigorAP 920RP with proper network parameters, so it can work properly in your network environment.

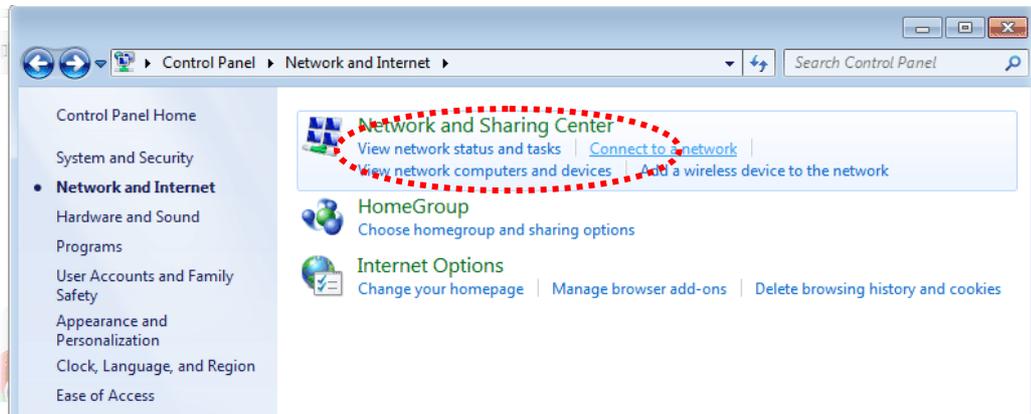
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic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

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

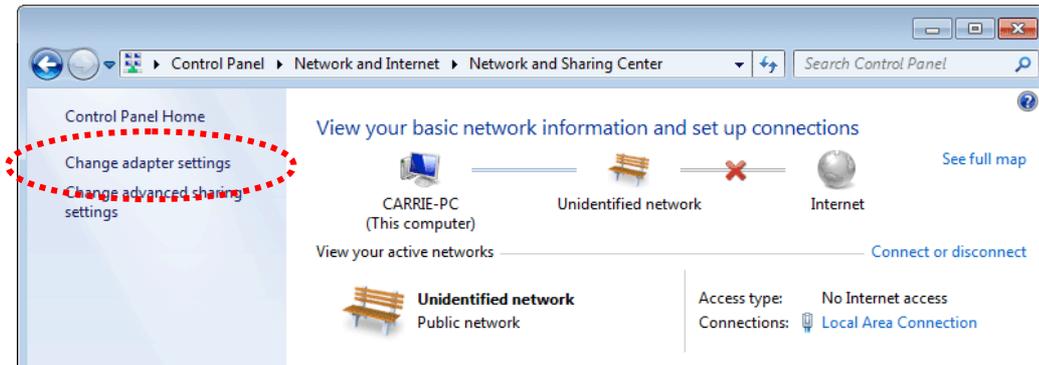
- Windows 7** - please go to section 2.1
- Windows 2000** - please go to section 2.2
- Windows XP** - please go to section 2.3
- Windows Vista** - please go to section 2.4

2.1 Windows 7 IP Address Setup

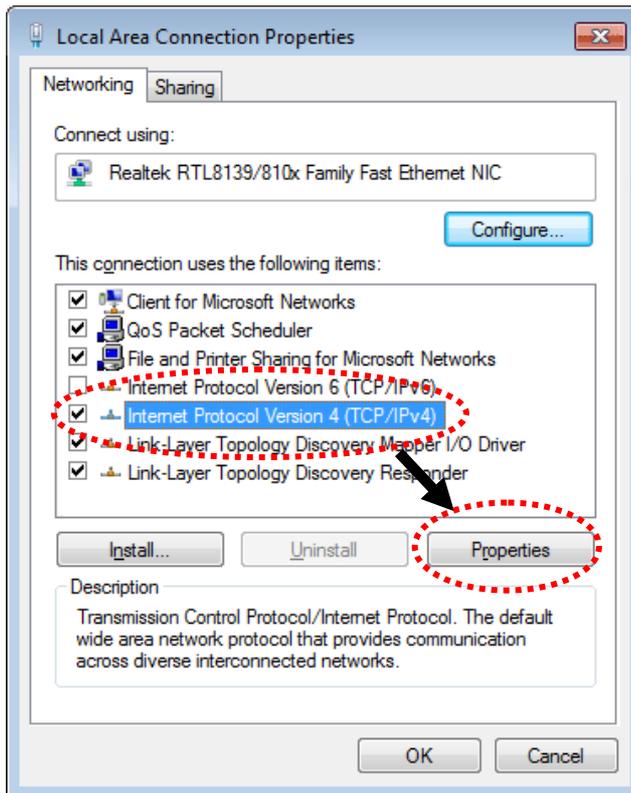
Click **Start** button (it should be located at lower-left corner of your computer), then click Control Panel. Double-click **Network and Internet**, and the following window will appear. Click **Network and Sharing Center**.



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



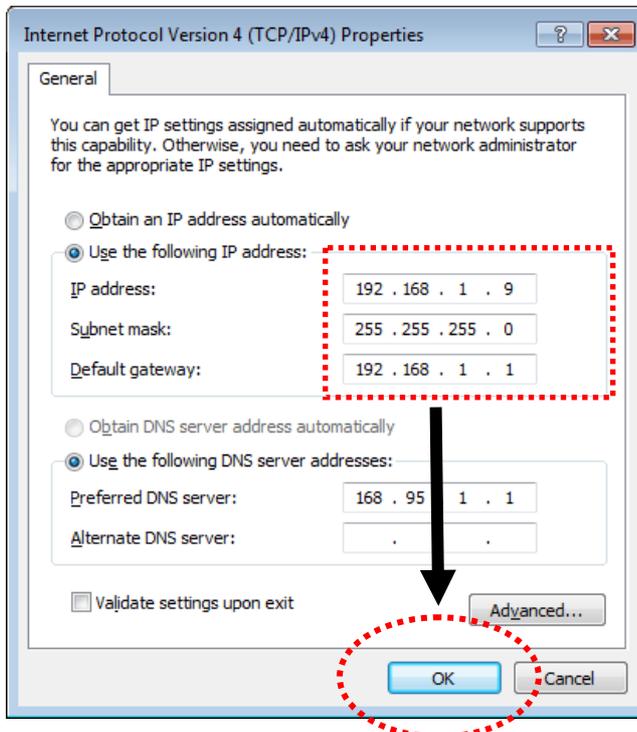
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



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

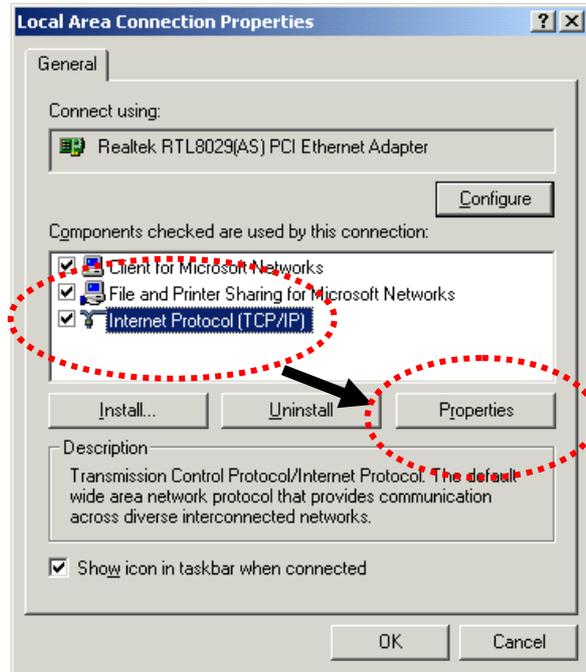
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.2 Windows 2000 IP Address Setup

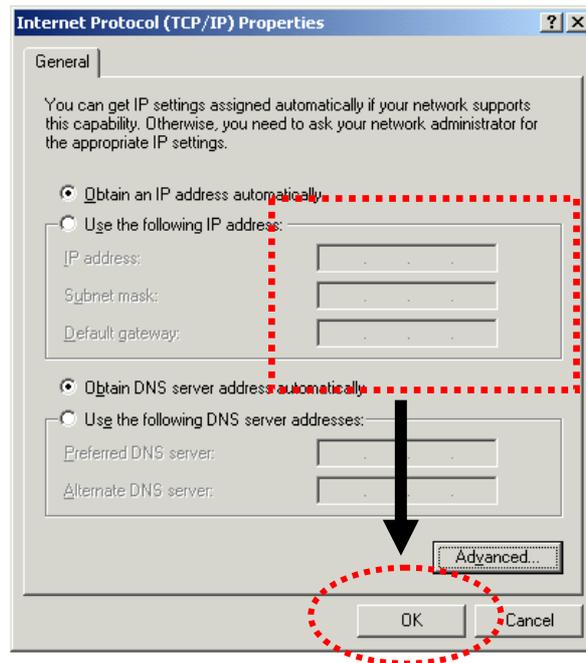
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Dial-up Connections** icon, double click **Local Area Connection**, and **Local Area Connection Properties** window will appear. Select **Internet Protocol (TCP/IP)**,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



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

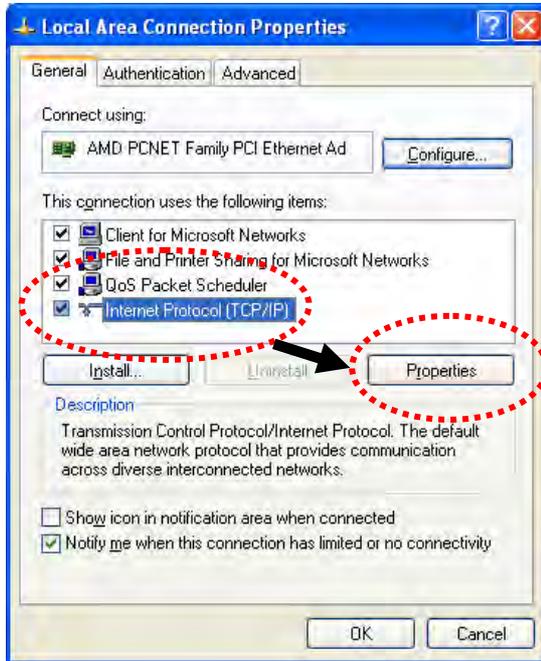
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.3 Windows XP IP Address Setup

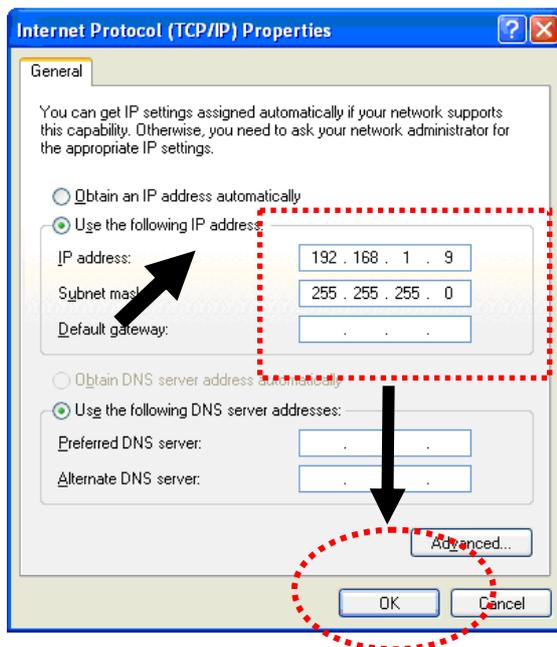
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Internet Connections** icon, click **Network Connections**, and then double-click **Local Area Connection, Local Area Connection Status** window will appear, and then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



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

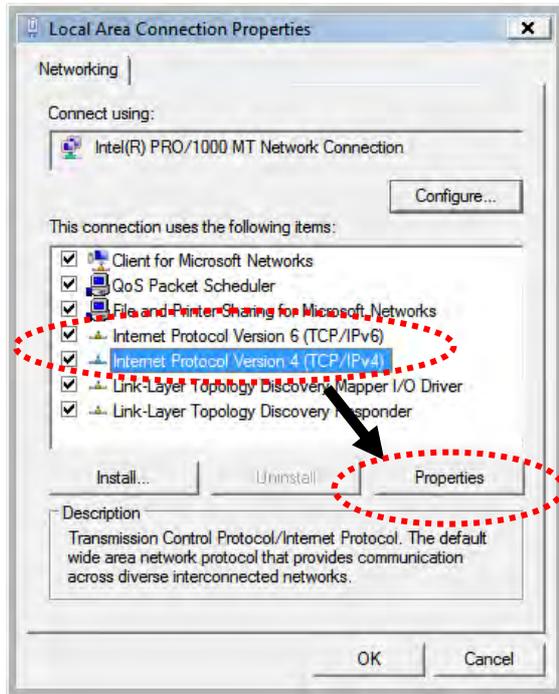
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



2.4 Windows Vista IP Address Setup

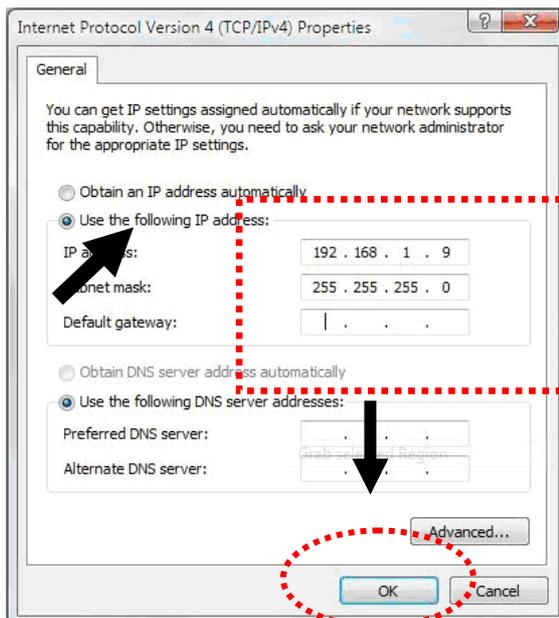
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Click **View Network Status and Tasks**, then click **Manage Network Connections**. Right-click **Local Area Network**, then select **'Properties'**. **Local Area Connection Properties** window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



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

IP address: **192.168.1.9**

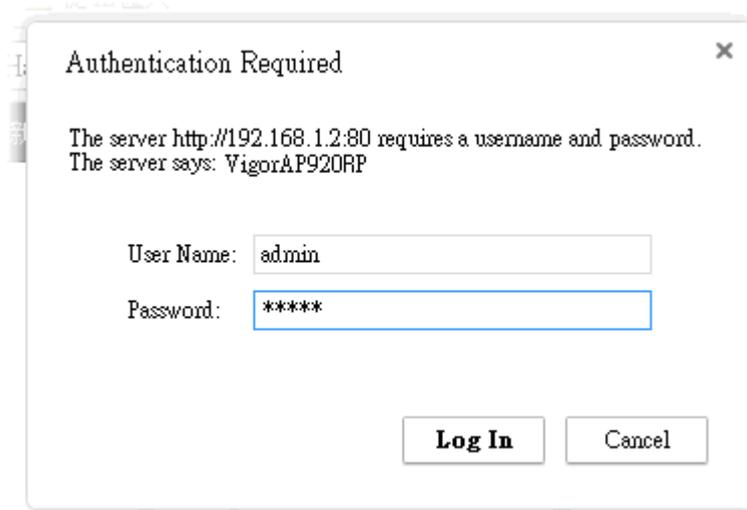
Subnet Mask: **255.255.255.0**



2.5 Accessing to Web User Interface

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

1. Make sure your PC connects to the VigorAP 920RP 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 1: 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 920RP**.

- If there is no DHCP server on the network, then VigorAP 920RP will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 920RP will receive it's 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.

2.6 Changing Password

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

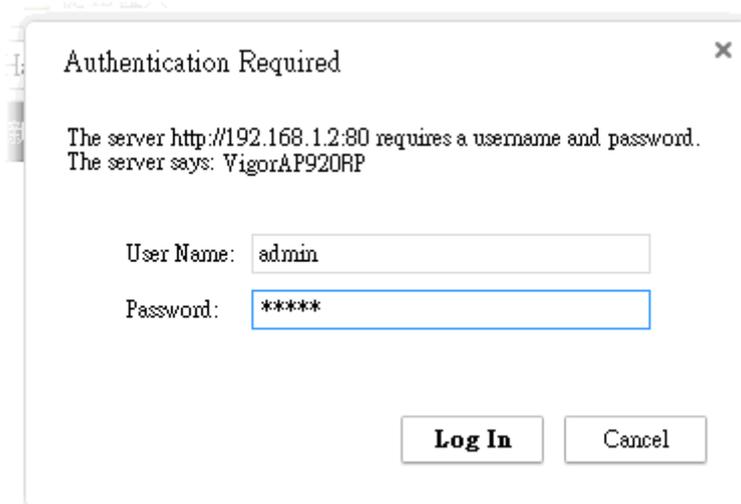
System Maintenance >> Administration Password

Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password"/>
Password Strength:	<input type="radio"/> Weak <input type="radio"/> Medium <input type="radio"/> 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.



The image shows a dialog box titled "Authentication Required" with a close button (X) in the top right corner. The text inside the dialog box reads: "The server http://192.168.1.2:80 requires a username and password. The server says: VigorAP920RP". Below this text are two input fields: "User Name:" with the value "admin" and "Password:" with the value "*****". At the bottom of the dialog box are two buttons: "Log In" and "Cancel".

2.7 Quick Start Wizard

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

2.7.1 Configuring 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 :

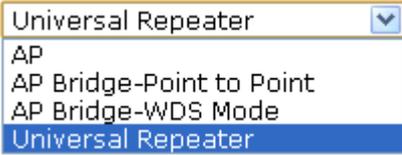
 VigorAP acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

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
Wireless LAN (2.4GHz)	Check the box to enable WLAN 2.4GHz for VigorAP. Operation Mode - There are four operation modes for wireless connection. Settings for each mode are different. 
Wireless LAN (5GHz)	Check the box to enable WLAN 5GHz for VigorAP. Operation Mode - There are three operation modes for wireless connection. Settings for each mode are different. 

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

2.7.2 Configuring 2.4GHz Wireless Settings Based on the Operation Mode

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

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)

Available settings are explained as follows:

Item	Description
Channel	Means the channel frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.
Main SSID	Set a name for VigorAP 920RP to be identified.
Security Key	Type 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Enable Guest Wireless	<p>Check the box to enable the guest 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 for one hour every day.</p> <p>SSID – Set a name for VigorAP 920RP which can be identified and connected by wireless guest.</p> <p>Security Key – Set 8~63 ASCII characters or 8~63 ASCII characters which can be used for logging into VigorAP 920RP by wireless guest.</p> <p>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.</p> <p>● Upload Limit – Scroll the radio button to choose the</p>

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

Phy Mode : HTMIX
Security :
<input checked="" type="radio"/> Disabled <input type="radio"/> TKIP <input type="radio"/> AES
Key : <input style="width: 150px;" type="text"/>
Peer Mac Address:
<input type="text"/> : <input type="text"/>

Operation Mode	Wireless(2.4GHz)	Wireless(5GHz)
	<input style="margin-right: 10px;" type="button" value=" < Back "/> <input style="margin-right: 10px;" type="button" value=" Next > "/> <input style="margin-right: 10px;" type="button" value=" Cancel "/>	

Available settings are explained as follows:

Item	Description
AP Discovery	Click this button to open the AP Discovery dialog. VigorAP 920RP can scan all regulatory channels and find working APs in the neighborhood.
Phy Mode	Data will be transmitted via HTMIX mode. Each access point should be setup to the same Phy Mode for connecting with each other.
Security	Select TKIP or AES as the encryption algorithm. Type 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 920RP connects to.

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.

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

Main SSID :

Security Key:

Operation Mode	Wireless(2.4GHz)	Wireless(5GHz)
<input style="margin-right: 10px;" type="button" value=" < Back "/> <input style="margin-right: 10px;" type="button" value=" Next > "/> <input style="margin-right: 10px;" type="button" value=" Cancel "/>		

Available settings are explained as follows:

Item	Description
AP Discovery	Click this button to open the AP Discovery dialog. VigorAP 920RP can scan all regulatory channels and find working APs in the neighborhood.
Phy Mode	Data will be transmitted via HTMIX mode. Each access point should be setup to the same Phy Mode for connecting with each other.
Security	Select TKIP or AES as the encryption algorithm. Type the key number if required.
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 920RP connects to.
Main SSID	Set a name for VigorAP 920RP to be identified.
Security Key	Type 8~63 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:

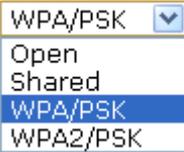
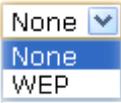
Enable Bandwidth Limit

Enable Station Control

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

Available settings are explained as follows:

Item	Description
Universal Repeater Parameters	
AP Discovery	Click this button to open the AP Discovery dialog. VigorAP 920RP can scan all regulatory channels and find working APs in the neighborhood.
SSID / MAC Address (Optional)	SSID means the identification of the wireless LAN. After choosing one of the AP from AP Discovery window and clicking OK , the settings (SSID and MAC Address) related to the selected AP will be displayed on these fields automatically. Later, VigorAP 920RP will be allowed to access Internet through the selected AP, by using SSID displayed here.
Channel	Means the channel frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.

	
Encryption Type for Open/Shared	<p>This option is available when Open/Shared is selected as Security Mode.</p> <p>Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP.</p>  <p>WEP Keys - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.</p> 
Encryption Type for WPA/PSK and WPA2/PSK	<p>This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode.</p> <p>Select TKIP or AES as the algorithm for WPA.</p> 
Security Key	<p>Type 8~63 ASCII characters, such as 012345678...(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK mode.</p>
Use the same SSID and Security Key as above	<p>In general, under the network environment, same SSID and security key can be used for the host (wireless client) and the repeater (VigorAP 920RP) in Universal Repeater mode. Check it to use the same SSID and security key configured as above.</p> <p>SSID - SSID can be any text numbers or various special characters. For VigorAP 920RP 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 920RP by using the SSID configured here.</p> <p>Security - Set 8~63 ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 920RP by other wireless client.</p>
Enable Guest	<p>Check the box to enable the guest wireless setting.</p>

Wireless

SSID – Set a name for VigorAP 920RP. Wireless guest is allowed to access into Internet via VigorAP 920RP with the SSID configured here.

Security Key – Set **8~63** ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 920RP 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.

2.7.3 Configuring 5GHz Wireless Settings Based on the Operation Mode

VigorAP 920RP offers 5GHz wireless connection capability. You can setup 5GHz features in Quick Start Wizard first. Once the USB 5GHz wireless dongle connects to VigorAP 920RP, 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)
0days 0hours 0mins

Reconnection Time Min(s)
0days 0hours 0mins

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

Available settings are explained as follows:

Item	Description
Channel	Means the channel of frequency of the wireless LAN. The default channel is 36. You may switch channel if the selected channel is under serious interference.
Main SSID	Set a name for VigorAP 920RP to be identified.
Security Key	Type 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Enable Guest Wireless	<p>Check the box to enable the guest wireless setting.</p> <p>SSID – Set a name for VigorAP 920RP which can be identified and connected by wireless guest.</p> <p>Security – Set 8~63 ASCII characters or 8~63 ASCII characters which can be used for logging into VigorAP 920RP by wireless guest.</p> <p>Enable Bandwidth Limit –Check the box to define the</p>

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.

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:

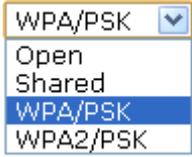
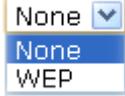
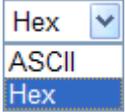
Enable Bandwidth Limit

Enable Station Control

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

Available settings are explained as follows:

Item	Description
AP Discovery	Click this button to open the AP Discovery dialog. VigorAP

	920RP can scan all regulatory channels and find working APs in the neighborhood.
SSID / MAC Address (Optional)	SSID means the identification of the wireless LAN. After choosing one of the AP from AP Discovery window and clicking OK , the settings (SSID and MAC Address) related to the selected AP will be displayed on these fields automatically. Later, VigorAP 920RP will be allowed to access Internet through the selected AP, by using SSID displayed here.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 36. You may switch channel if the selected channel is under serious interference.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure. 
Encryption Type for Open/Shared	This option is available when Open/Shared is selected as Security Mode. Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP .  WEP Keys - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. 
Encryption Type for WPA/PSK and WPA2/PSK	This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode . Select TKIP or AES as the algorithm for WPA. 
Security Key	Type 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK mode.

<p>Use the same SSID and Security Key as Above</p>	<p>In general, under the network environment, same SSID and security key can be used for the host (wireless client) and the repeater (VigorAP 920RP) in Universal Repeater mode. Check it to use the same SSID and security key configured as above.</p> <p>SSID - SSID can be any text numbers or various special characters. For VigorAP 920RP 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 VigorAP920RP by using the SSID configured here.</p> <p>Security - Set 8~63 ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 920RP by other wireless client.</p>
<p>Enable Guest Wireless</p>	<p>Check the box to enable the guest wireless setting.</p> <p>SSID – Set a name for VigorAP 920RP. Wireless guest is allowed to access into Internet via VigorAP 920RP with the SSID configured here.</p> <p>Security Key – Set 8~63 ASCII characters or 64 Hexadecimal digits which can be used for logging into VigorAP 920RP by wireless guest.</p> <p>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.</p> <ul style="list-style-type: none"> ● Upload Limit –Scroll the radio button to choose the value you want. ● Download Limit –Scroll the radio button to choose the value you want. <p>Enable Station Control – Check the box to set the duration for the guest connecting /reconnecting to Vigor device.</p> <ul style="list-style-type: none"> ● 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.

2.7.4 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 "AP920RP" is completed.

Press Finish button to save and finish the wizard setup.

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

< Back

Finish

Cancel

2.8 Online Status

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

Online Status

System Status				System Uptime: 7d 19:24:26
LAN Status				
IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.1.11	13870	54277	11117235	2831178
Universal Repeater Status				
IP	Gateway	SSID	Channel	
			11	
Remote Mac	Security Mode	TX Packets	RX Packets	
		0	0	

Detailed explanation is shown below:

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

3

Advanced Configuration

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

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

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

The screenshot displays the DrayTek VigorAP 920R Series web interface. The left sidebar contains a navigation menu with the following items: Quick Start Wizard, Online Status, Operation Mode, LAN, Central AP Management, Wireless LAN (2.4GHz), Wireless LAN (5GHz), RADIUS Setting, Applications, Mobile Device Management, System Maintenance, Diagnostics, Support Area, FAQ/Application Note, and Product Registration. The main content area is titled 'System Status' and shows the following information:

- Model**: VigorAP920RP
- Device Name**: VigorAP920RP
- Firmware Version**: 1.2.1
- Build Date/Time**: r8162 Mon, 26 Mar 2018 14:00:33
- System Uptime**: 0d 00:06:16
- Operation Mode**: Universal Repeater

Below this, there are four configuration tables:

System		LAN	
Memory Total	: 236784 kB	MAC Address	: 00:1D:AA:5C:A6:58
Memory Left	: 137064 kB	IP Address	: 192.168.1.1
Cached Memory	: 21476 kB / 236784 kB	IP Mask	: 255.255.255.0

Wireless LAN (2.4GHz)		Universal Repeater(2.4G)	
MAC Address	: 00:1D:AA:5C:A6:58	MAC Address	: 12:1D:AA:5C:A6:58
SSID	: ap920-BandSteering	SSID	:
Channel	: 11	Channel	: 11
Driver Version	: 10.4		

Wireless LAN (5GHz)	
MAC Address	: 00:1D:AA:5C:A6:59
SSID	: DrayTek5G
Channel	: Auto(44)
Driver Version	: 10.4

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

At the bottom left of the interface, the text 'Admin mode' and 'Universal Repeater Mode' is visible.

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.
- 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.
- 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
Wireless LAN(2.4GHz)	
AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
AP Bridge-Point to Point	This mode can establish wireless connection with another VigorAP 920RP using the same mode, and link the wired network which these two VigorAP 920RPs connected together. Only one access point can be connected in this mode.
AP Bridge-Point to Multi-Point	This mode can establish wireless connection with other VigorAP 920RPs using the same mode, and link the wired network which these VigorAP 920RPs connected together. Up to 4 access points can be connected in this mode.
AP Bridge-WDS	This mode is similar to AP Bridge to Multi-Point, but access point is not working in bridge-dedicated mode, and will be able to accept wireless clients while the access point is working as a wireless bridge.

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

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

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.

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

<p>LAN IP Network Configuration</p> <p><input checked="" type="checkbox"/> Enable DHCP Client</p> <p>IP Address <input type="text" value="192.168.1.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <hr/> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID <input type="text" value="0"/></p>	<p>DHCP Server Configuration</p> <p><input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>Primary DNS Server <input type="text"/></p> <p>Secondary DNS Server <input type="text"/></p> <p>Trust DHCP Server IP for WLAN <input type="text"/></p>
--	---

Available settings are explained as follows:

Item	Description
LAN IP Network	Enable DHCP Client – When it is enabled, VigorAP 920RP

<p>Configuration</p>	<p>will be treated as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2860).</p> <p>IP Address – Type in private IP address for connecting to a local private network (Default: 192.168.1.2).</p> <p>Subnet Mask – Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>Enable Management VLAN – VigorAP 920RP supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 920RP.</p> <p>VLAN ID – Type the number as VLAN ID tagged on the transmitted packet. “0” means no VALN tag.</p>
<p>DHCP Server Configuration</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>Enable Server - Enable Server lets the modem assign IP address to every host in the LAN.</p> <ul style="list-style-type: none"> ● Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254. ● End IP Address - Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses. ● Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) ● Default Gateway - Enter a value of the gateway IP address for the DHCP server. ● Lease Time - It allows you to set the leased time for the specified PC. ● Primary DNS Server - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field. ● Secondary DNS Server - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. <p>Relay Agent - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.</p> <ul style="list-style-type: none"> ● DHCP Server IP Address for Relay Agent - It is available when Enable Relay Agent is selected. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

-
- **Primary DNS Server** - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
 - **Secondary DNS Server** - 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.

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

- **Primary DNS Server** - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
- **Secondary DNS Server** - 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.

- **Trust DHCP Server IP for WLAN** –There is no right for such VigorAP to assign IP address for wireless LAN user. However, you can specify another valid DHCP server on other VigorAP to make the wireless LAN client obtaining the IP address from the designated DHCP server.

Specify a DHCP server in such field. All the IP addresses of the devices on LAN of VigorAP will be assigned via such specified server. It is used to avoid IP assignment interference due to multiple DHCP servers in one LAN.

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

3.2.2 Port Control

To avoid wrong connection due to the insertion of unsuitable Ethernet cable, the function of physical LAN ports can be disabled via web configuration.

LAN >> Port Control

Port Control

<input checked="" type="checkbox"/> Enable Port Control	Port 1	Port 2
Disable Port	<input type="checkbox"/>	<input type="checkbox"/>

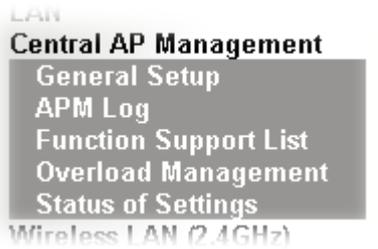
Available settings are explained as follows:

Item	Description
Enable Port Control	Check it to enable the port control. If it is enabled, you are allowed to disable the function of physical LAN port by checking the corresponding check box.
Disable Port	Choose and check the LAN port.

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

3.3 Central AP Management

Such menu allows you to configure VigorAP device to be managed by Vigor router.



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
Enable AP Management	Check the box to enable the function of AP Management (APM).
Enable Auto Provision	VigorAP 920RP can be controlled under Central AP Management in Vigor router. When both Vigor router and VigorAP 920RP have such feature enabled, once VigorAP 920RP is registered to Vigor router, the WLAN profile pre-configured on Vigor router will be applied to VigorAP 920RP immediately. Thus, it is not necessary to configure VigorAP 920RP separately.

3.3.2 APM Log

This page will display log information related to wireless stations connected to VigorAP 920RP and central AP management.

Such information also will be delivered to Vigor router (e.g., Vigor2860 or Vigor2925 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 |

```
Sep 21-18:21:42 syslog: [APM] Query AP status.
Sep 21-18:21:42 syslog: [APM] Request done.
Sep 23-06:21:44 syslog: [APM] Query AP status.
Sep 23-06:21:44 syslog: [APM] Request done.
Sep 24-18:21:44 syslog: [APM] Query AP status.
Sep 24-18:21:44 syslog: [APM] Request done.
```

3.3.3 Function Support List

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

Central AP Management >> Function Support List

Client	
Function Name	Model Name
	AP920RP
	1.1.0
Register	
DHCP	√
Static IP	√
Profile	
2.4GHz	√
5GHz	√
AP Mode	√
Repeater Mode	√
Client Disable Auto Provision	√
WLAN Enable/Disable	√
Station List	
Station List	√
Load Balance	
Load Balance	√

Note: DrayTek central wireless management (AP Management) lets control, efficiency, monitoring and security of your company-wide wireless access easier to be managed. Inside the web user interface, we call “central wireless management” as Central AP Management which supports mobility, client monitoring/reporting and load-balancing to multiple APs. For central wireless management, you will need a Vigor2860 or Vigor2925

series router; there is no per-node licensing or subscription required. With the unified user interface of Vigor2860 Combo WAN series and Vigor2925 Triple WAN series, the multiple deployment of VigorAP 920RP can be clear at the first sight. For multiple wireless clients, to apply the AP Load Balancing to the multiple APs will manage wireless traffic with smooth flow and enhanced efficiency.

3.3.4 Overload Management

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 920RP) 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 920RP 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., Vigor2860 or Vigor2925 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.

Central AP Management >> Overload Management

Overload Management

MAC Address Filter of Force Overload Disassociation

	Index	MAC Address	Comment
White List			
Black List			

Client's MAC Address : : : : : :

Apply to :

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
White List/Black List	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.
Client’s MAC	Specify the MAC Address of the remote/local client.

Address	
Apply to	White List – MAC address listed inside Client’s MAC Address will be categorized as one of members in White List. Black List - MAC address listed inside Client’s MAC Address will be categorized as one of members in Black List.
Add	Add a new MAC address into the White List/Black List.
Delete	Delete the selected MAC address in the White List/Black List.
Edit	Edit the selected MAC address in the White List/Black List.
Cancel	Give up the configuration.

3.3.5 Status of Settings

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 920RPs) registered to Vigor 2860 or Vigor2925 series. This web page displays the settings related to Load Balance for VigorAP 920RP. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor 2860 or Vigor2925 series.

Central AP Management >> Status of Settings

Function Name	Status	Value
Load Balance		
Station Number Threshold	X	
Max WLAN(2.4GHz) Station Number		128
Max WLAN(5GHz) Station Number		128
Traffic Threshold	X	
Upload Limit		None bps
Download Limit		None bps
Force Overload Disassociation	X	
Disassociate By		None
RSSI Threshold		-50 dBm
Rogue AP Detection		
Rogue AP Detection	X	

“X” means the function is not enabled or VigorAP 920RP has not registered to any Vigor router yet.

Below shows a setting example for Load Balance settings configured in Vigor 2860 or Vigor2925 series.

Central AP Management >> Load Balance

Enable:

Mode: (Overload Detected By)

 By Station Number
 Maximum Station Number:
 Wireless LAN (2.4GHz) (3-64)
 Wireless LAN (5GHz) (3-64)

By Traffic
 Upload Limit: bps (Default unit: K)
 Download Limit: bps (Default unit: K)

Force Overload Disassociation:

Note: The maximum station number of Wireless LAN (2.4GHz) will be applied to both Wireless LAN (2.4GHz) and Wireless LAN (5GHz) if the firmware version of AP900 is less than or equal to 1.1.4.1.

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

VigorAP 920RP is a highly integrated wireless local area network (WLAN) for 5 GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80 MHz at 5 GHz. VigorAP 920RP can support data rates up to 867 MBps in 802.11ac 80 MHz channels.

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 920RP 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 920RP. 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 920RP 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 920RP) with the encryption of WPA and WPA2.

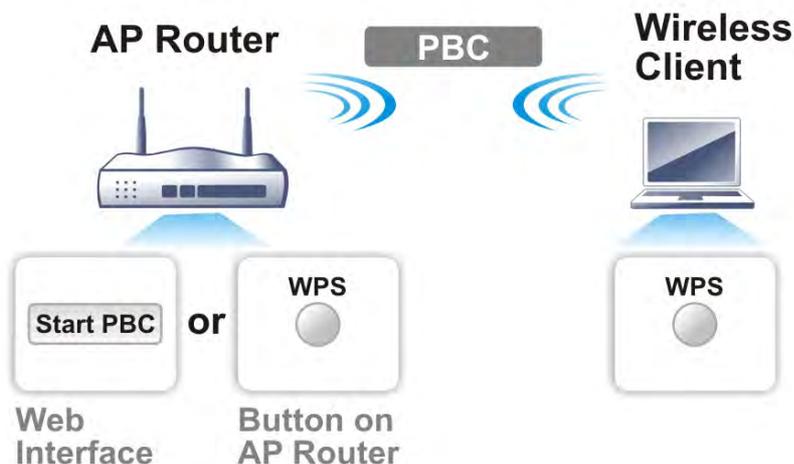


It is the simplest way to build connection between wireless network clients and VigorAP 920RP. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 920RP automatically.

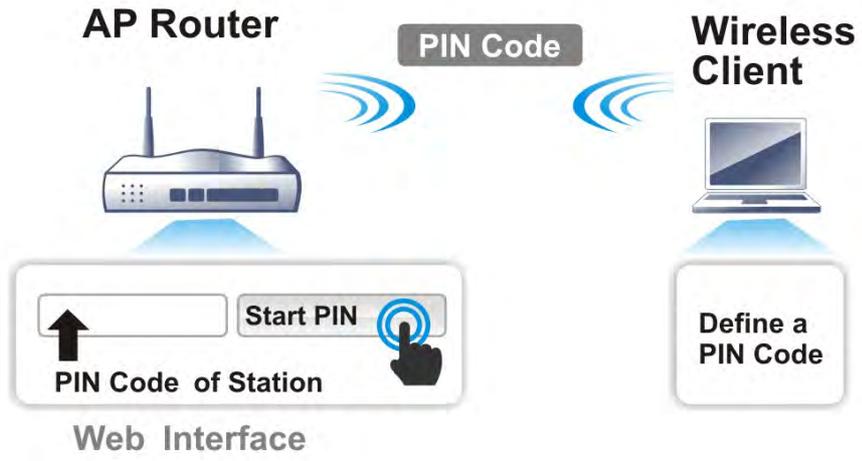
Note: Such function is available for the wireless station with WPS supported.

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 920RP series which served as an AP, press **WPS** button once on the front panel of VigorAP 920RP 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 920RP.



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, WMM Configuration, 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 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode : ▼

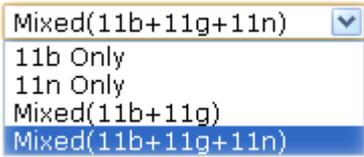
Channel : ▼

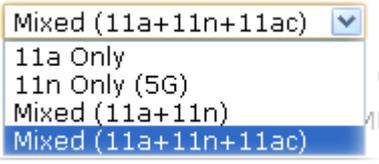
Extension Channel : ▼

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

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor device. The number you can set is from 3 to 128.
Enable Limit Client per SSID	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 128.
Mode	At present, VigorAP 920RP can connect to 11b only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode. <div style="text-align: center; margin-top: 10px;">  <p>← 2.4GHz</p> </div>

	 <p style="text-align: right;">← 5GHz</p>
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.
Extension Channel	This option is available for Wireless LAN (2.4GHz). With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the Channel selected above. Configure the extension channel you want.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 920RP while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 920RP to be identified. Default setting is DrayTek.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not access for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.

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

3.5.2 Security

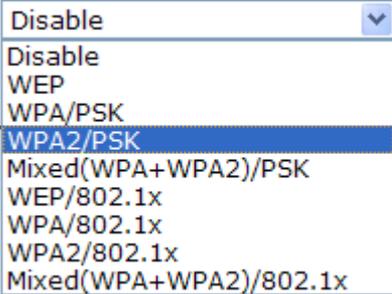
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security**, 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: ap920-BandSteering			
Mode: Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms: <input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase:			
Key Renewal Interval: 3600 seconds			
EAPOL Key Retry: <input checked="" type="radio"/> Enable <input type="radio"/> Disable			
WEP			
<input type="radio"/> Key 1 : [] Hex			
<input checked="" type="radio"/> Key 2 : [] Hex			
<input type="radio"/> Key 3 : [] Hex			
<input type="radio"/> Key 4 : [] Hex			
[OK] [Cancel]			

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables</p>

	<p>VigorAP 920RP to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p>WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Type 8-63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Enable - 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.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and '!'. Such feature is available for WEP mode. <div data-bbox="638 1848 762 1960" style="border: 1px solid black; padding: 2px; margin-top: 5px;"> Hex <input type="button" value="v"/> ASCII Hex </div>
WEP	Disable - Disable the WEP Encryption. Data sent to the AP

will not be encrypted.

Enable - Enable the WEP Encryption.

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

Radius Server

<input type="checkbox"/> Use internal RADIUS Server	
IP Address	<input type="text" value="0"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text" value="*****"/>
Session Timeout	<input type="text" value="0"/> second(s)

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 920RP which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, 3.11 RADIUS Server to configure settings for internal server of VigorAP 920RP.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

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

3.5.3 Access Control

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

Wireless LAN (2.4GHz) >> Access Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek Policy: <input type="button" value="Disable"/>			
MAC Address Filter			
Index		MAC Address	
<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>			
Client's MAC Address : <input type="text"/>			
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/> Limit: 256 entries			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>	

Available settings are explained as follows:

Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 920RP. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <input type="button" value="Activate MAC address filter"/> <input type="button" value="Disable"/> <input type="button" value="Activate MAC address filter"/> <input type="button" value="Blocked MAC address filter"/> </div>
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.

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

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

3.5.4 WPS

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

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

Enable WPS 

Wi-Fi Protected Setup Information

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

Device Configure

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

Status: Idle

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 920RP is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 920RP. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 920RP.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 920RP will wait for WPS requests from wireless clients about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. Both ACT and 2.4G WLAN LEDs on VigorAP 920RP will blink quickly when

WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

3.5.5 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 type="radio"/> Auto 20/40 MHz <input checked="" type="radio"/> 40 MHz
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
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 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
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
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
MAC Clone:	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
Channel Width	<p>20 MHz- the device will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p>Auto 20/40 MHz – 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>40 MHz- the device will use 40MHz for data transmission and receiving between the AP and the stations.</p>
Antenna	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.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold	<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>
Country Code	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.
Auto Channel Filtered Out List	The selected wireless channels will be discarded if AutoSelect is selected as Channel selection mode in Wireless LAN>>General Setup .
Isolate 2.4GHz and 5GHz bands	<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"> ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if Isolate Member (in Wireless LAN>>General Setup) is NOT enabled for such SSID. ● Yet, if the function of Isolate Member (in Wireless LAN>>General Setup) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
Isolate members with IP	<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>
MAC Clone	Click Enable 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.

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

3.5.6 AP Discovery

VigorAP 920RP can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

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

Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
1	staffs	00:1D:AA:9D:68:AC	8%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
2	guests	02:1D:AA:9D:68:AC	4%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
3	RDB_24G_wi...	00:1D:AA:5B:A0:C8	2%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
4	YRC_DrayTe...	00:1D:AA:DD:75:B0	4%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
5	DrayTek	00:1D:AA:BE:FD:68	2%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
6	RD8-910c-4	02:1D:AA:7A:5D:8C	2%	11	TKIP/AES	WPA2/PSK
7	AP920R-PQC...	00:1D:AA:63:2C:40	11%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
8	AP910C-2 P...	00:1D:AA:26:8D:68	3%	11	TKIP/AES	WPA2/PSK
9	DrayTek	00:1D:AA:80:06:B8	1%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
10	AP910C-PQC...	00:1D:AA:26:8D:30	8%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
11	RD8-910c-1	00:1D:AA:7F:5D:8C	2%	11	TKIP/AES	WPA2/PSK
12	RD8-910c-3	02:1D:AA:79:5D:8C	2%	11	TKIP/AES	WPA2/PSK
13	APM-PQC-Ta...	00:1D:AA:3D:4F:14	2%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
14	RD8-910c-2	02:1D:AA:78:5D:8C	1%	11	TKIP/AES	WPA2/PSK
15	AP910C-ssi...	02:1D:AA:79:5D:58	4%	11	NONE	
16	AP910C-ssi...	02:1D:AA:7A:5D:58	4%	11	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 920RP.
BSSID	Display the MAC address of the AP scanned by VigorAP 920RP.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 920RP.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button

3.5.7 WMM Configuration

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

Wireless LAN (2.4GHz) >> WMM Configuration

WMM Configuration | [Set to Factory Default](#) |

WMM Capable Enable Disable

APSD Capable Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input checked="" type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input checked="" type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Note: The range of setting values:

- Aifsn : 0-15, in units of slot time
- CWMin : 0-15, in units of slot time
- CWMax : 0-15, in units of slot time
- Txop : 0-256, in units of 1 us

Available settings are explained as follows:

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

	the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
AckPolicy	<p>“Uncheck” (default value) the box means the AP will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.</p> <p>“Check” the box means the AP will not answer any response request for the transmitting packets. It will have better performance with lower reliability.</p>
ACM	<p>It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.</p> <p>Note: VigorAP 920RP provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.</p>

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

3.5.8 Bandwidth Management

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

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID DrayTek			
Per Station Bandwidth Limit			
Enable <input checked="" type="checkbox"/>			
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	64K		bps
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
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor device with the same SSID. Use the drop down list to choose the rate. If you choose User defined , you have to specify the rate manually.
Download Limit	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor device with the same SSID. Use the drop down list to choose the rate. If you choose User defined , you have to specify the rate manually.
Auto Adjustment	Check this box to have the bandwidth limit determined by the system automatically.
Total Upload Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data uploading.
Total Download Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data downloading.

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

3.5.9 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.

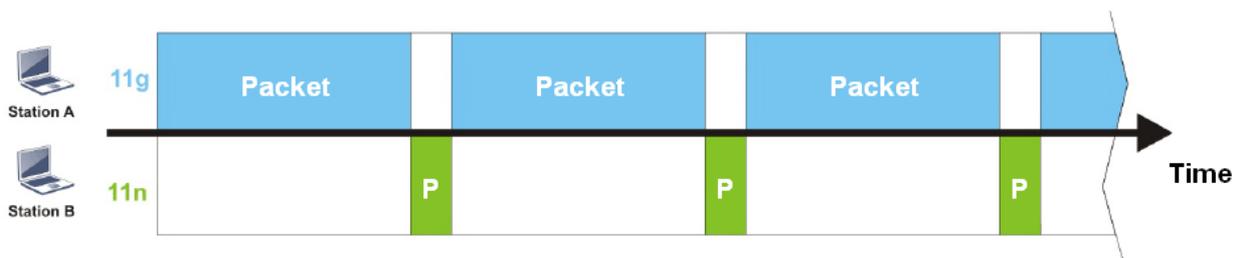
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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 920RP. 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 920RP. 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 ~ 128, Default: 2)

Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments. You could check [Diagnostics >> Station Airtime](#) Graph first.

OK

Cancel

Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p>Airtime Fairness – Click the link to display the following screen of airtime fairness note.</p> <p>Triggering Client Number – 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.

3.5.10 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.

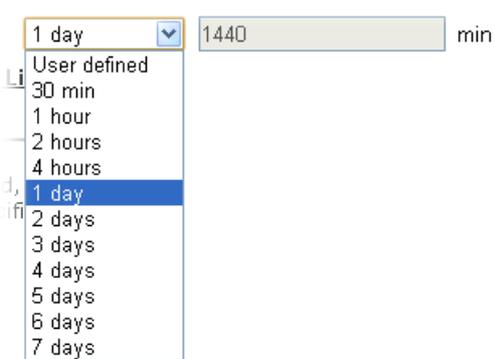
Wireless LAN (2.4GHz) >> Station Control

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

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
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor device. Or, type the duration manually when you choose User defined . 

Display All Station Control List	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.

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

Fast Roaming(WPA2/802.1x)

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

OK Cancel

Available settings are explained as follows:

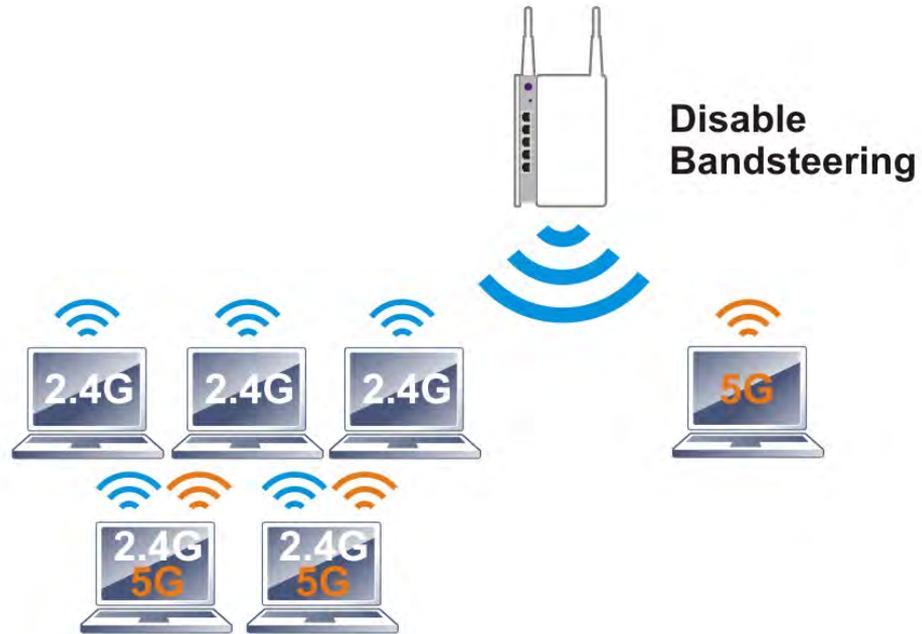
Item	Description
AP-assisted Client Roaming Parameters	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 920RP will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p>Minimum Basic Rate – Check the box to use the drop down list to specify a basic rate (Mbps). When the link rate of the wireless station is below such value, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Disable RSSI Requirement - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p>Strictly Minimum RSSI - 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 (dBm) set here, VigorAP 920RP will terminate the network connection for that wireless station.</p>

	<p>Minimum RSSI - When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of With Adjacent AP RSSI over) is detected by VigorAP 920RP, VigorAP 920RP 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"> ● With Adjacent AP RSSI over – Specify a value as a threshold.
<p>Fast Roaming (WPA2/802.1x)</p>	<p>Enable – Check the box to enable fast roaming configuration.</p> <p>PMK Caching - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode.</p> <p>Pre-Authentication - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)</p>

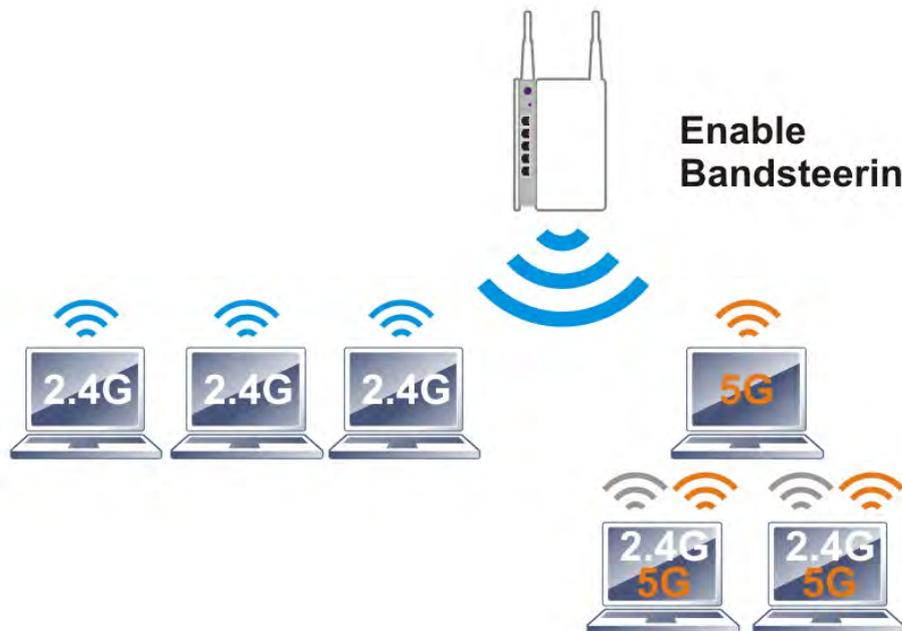
After finishing this web page configuration, please click **OK** to save the settings.

3.5.12 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)

Wait Full Time to Check 5G Capability

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

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

Overloaded

2.4GHz Utilization Overload Threshold % (Default: 70)

5GHz Utilization Overload Threshold % (Default: 70)

(Only do band steering when 2.4GHz utilization is overloaded and 5GHz utilization is not)

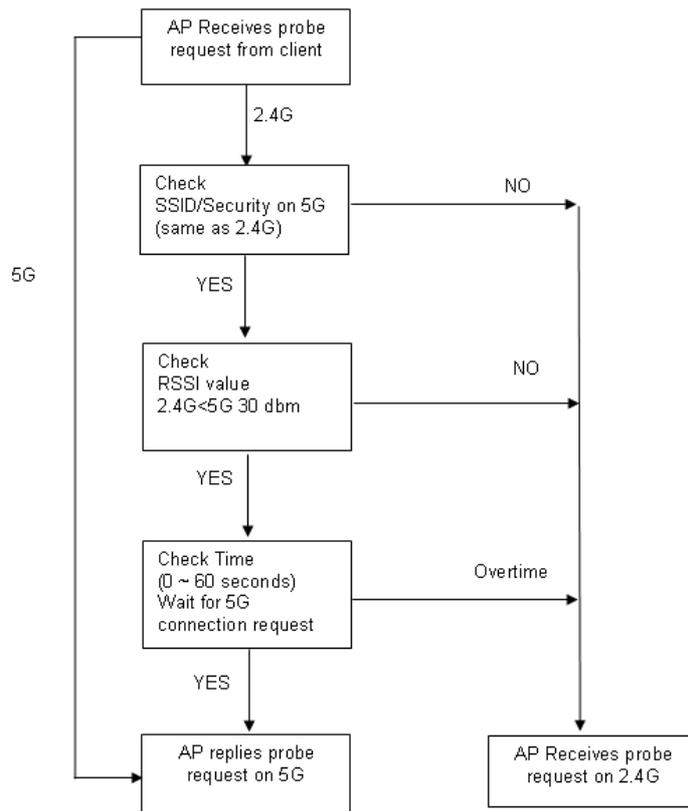
Note: Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
Enable Band Steering	<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>Check Time.... – 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>5GHz Minimum RSSI – 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 920RP, VigorAP will allow the client to connect to 2.4GHz network.</p> <p>Overloaded – If it is enabled, VigorAP will activate the band steering according to the conditions set below.</p> <ul style="list-style-type: none"> ● 2.4GHz Utilization Overload Threshold – The default setting is 70%. It can define the network congestion for 2.4GHz. ● 5GHz Utilization Overload Threshold – The default setting is 70%. It can define the network congestion for 5GHz. <p>When the utilization of 2.4GHz is higher than the specified threshold and the utilization of 5GHz is lower than the specified threshold, VigorAP will steer the client to connect to 5GHz 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

Enable **Band Steering**

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

Wait Full Time to Check 5G Capability

5GHz Minimum RSSI dBm (%) (Default: -78)
(Only do band steering when 5GHz signal is better than Minimum RSSI)

Overloaded

2.4GHz Utilization Overload Threshold % (Default: 70)

5GHz Utilization Overload Threshold % (Default: 70)
(Only do band steering when 2.4GHz utilization is overloaded and 5GHz utilization is not)

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 *ap920-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 Client Limit (3 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel :

Extension Channel :

Enable	Hide SSID	SSID	Isolate Member	VLAN ID (0: Untagged)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ap920-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>

Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Client Limit (3 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel : (Active Channel: 149) **Filtered Out List**

Details : 20/40MHz Ext Ch:153 , 80MHz Center Ch:155

Enable	Hide SSID	SSID	Isolate Member	VLAN ID (0: Untagged)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ap920-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>

Same value for 2.4GHz and 5GHz

- 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			
ap920-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
WEP			

Same value for 2.4GHz and 5GHz

Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap920-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
WEP			

- Now, VigorAP 920RP will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

3.5.13 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. Each tab (general, advanced, control, neighbor) will display different status information (including MAC address, Vendor, SSID, Auth, Encrypt, Tx/Rx Rate, Hostname, RSSI, Link Speed, BW, PSM, WMM, PHMd, MCS, Connection Time, Reconnection Time, Approx. Distance, Visit Time, and so on).

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	Control	Neighbor	
Index	MAC Address	Hostname	Vendor	SSID	Link speed (TX/RX)	RSSI	TX Rate (Kbps)	RX Rate (Kbps)
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>								
<input type="button" value="Refresh"/>								

Add to Access Control :

Client's MAC Address : : : : : :

Available settings are explained as follows:

Item	Description
MAC Address	Display the MAC Address for the connecting client.
Hostname	Display the host name of the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	Client's MAC Address - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC

	address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
Add	Click this button to add current typed MAC address into Access Control .

Control

Display connection and reconnection time of the wireless stations.

Neighbor

Display more information for the neighboring wireless stations.

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

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



AP Bridge-Point to Point allows VigorAP 920RP to connect to **another** VigorAP 920RP which uses the same mode. All wired Ethernet clients of both VigorAP 920RPs will be connected together.

Point-to Multi-Point Mode allows AP 920RP to connect up to **four** VigorAPs using the same mode. All wired Ethernet clients of every VigorAP 920RP will be connected together.

3.6.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure 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 AP920RP want to connect.

PHY Mode : HTMIX

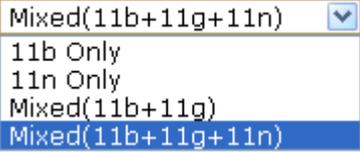
<p>Security :</p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p>	<p>Peer MAC Address :</p> <p>1. <input type="text"/> : <input type="text"/></p> <p>2. <input type="text"/> : <input type="text"/></p> <p>3. <input type="text"/> : <input type="text"/></p> <p>4. <input type="text"/> : <input type="text"/></p>
--	--

OK

Cancel

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, VigorAP 920RP can connect to 11b only, 11n only, Mixed (11b+11g), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

	
Channel	Means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.
Filtered Out List	Such link will be shown if AutoSelect is selected as Channel . Click such link to access into Wireless LAN >> Advanced Settings page.
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the Channel selected above.
Rate	If 11b Only is selected as Mode, such feature will be available to set data transmission rate.
PHY Mode	Data will be transmitted via HTMIX mode. Each access point should be setup to the same PHY Mode for connecting with each other.
Security	Select TKIP or AES as the encryption algorithm. Type the key number if required.
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 920RP connects to.

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

3.6.2 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 type="radio"/> Auto 20/40 MHz <input checked="" type="radio"/> 40 MHz
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
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 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
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
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
MAC Clone:	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.

OK

Cancel

Available settings are explained as follows:

Item	Description
Channel Width	<p>20 MHz - AP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p>Auto 20/40 MHz - 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>40 MHz - AP will use 40MHz for data transmission and receiving between the AP and the stations.</p>
Antenna	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.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold	<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>
Country Code	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.
Auto Channel Filtered Out List	The wireless channels selected in this field will be discarded if AutoSelect is selected as Channel selection mode in Wireless LAN>>General Setup .
Isolate 2.4GHz and 5GHz bands	<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"> ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if Isolate Member (in Wireless LAN>>General Setup) is NOT enabled for such SSID. ● Yet, if the function of Isolate Member (in Wireless LAN>>General Setup) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
Isolate members with IP	The default setting is “Disable”. If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).
MAC Clone	Click Enable 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.

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

3.6.3 AP Discovery

VigorAP 920RP 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 920RP.

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 920RP can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="radio"/>	1	AP910C-ssi...	02:1D:AA:7A:5D:58	3%	11	NONE	
<input type="radio"/>	2	AP910C-rd8...	00:1D:AA:7F:5D:58	0%	11	NONE	
<input type="radio"/>	3	AP910C-PQC...	00:1D:AA:26:8D:30	5%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	4	AP920R-PQC...	00:1D:AA:63:2C:40	8%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	5	RD8_24G_wi...	00:1D:AA:5B:A0:C8	2%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	6	YRC_DrayTe...	00:1D:AA:DD:75:B0	8%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	7	ycr_DrayTe...	02:1D:AA:DD:75:B0	5%	6	TKIP	WPA/PSK
<input type="radio"/>	8	staffs	00:1D:AA:9D:68:AC	4%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	9	guests	02:1D:AA:9D:68:AC	4%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK

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

AP's MAC Address AP's SSID

Add to WDS Settings:

Available settings are explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 920RP.
BSSID	Display the MAC address of the AP scanned by VigorAP 920RP.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 920RP.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Add	Type the MAC address of the AP. Click Add . Later, the MAC address of the AP will be added and be shown on WDS settings page.

3.6.4 WDS AP Status

VigorAP 920RP can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

Wireless LAN >> WDS AP Status

WDS AP List

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

Refresh

3.7 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, WMM Configuration, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering and Station List.



3.7.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure 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 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

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.

Note:Enter the configuration of APs which AP920RP want to connect.
Remote AP should always use LAN or SSID1 MAC address to connect AP920RP WDS.

PHY Mode : HTMIX

<p>Security :</p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p>	<p>Peer MAC Address :</p> <p>1. <input type="text"/> : <input type="text"/></p> <p>2. <input type="text"/> : <input type="text"/></p> <p>3. <input type="text"/> : <input type="text"/></p> <p>4. <input type="text"/> : <input type="text"/></p>
--	--

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	Check the box to set the maximum number of wireless stations which try to connect Internet through VigorAP. The number you can set is from 3 to 128.
Enable Limit Client per SSID	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 128.
Mode	At present, VigorAP 920RP can connect to 11b only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency,

	please select AutoSelect to let system determine for you.
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the Channel selected above. Configure the extension channel you want.
Rate	If 11b Only is selected as Mode, such feature will be available to set data transmission rate.
Enable	Check the box to enable the SSID configuration.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 920RP while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 920RP to be identified. Default setting is DrayTek.
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
PHY Mode	Data will be transmitted via HTMIX mode. Each access point should be setup to the same PHY Mode for connecting with each other.
Security	Select Disabled, TKIP or AES as the encryption algorithm.
Peer MAC Address	Four peer MAC addresses are allowed to be entered in this page at one time.

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

3.7.2 Security

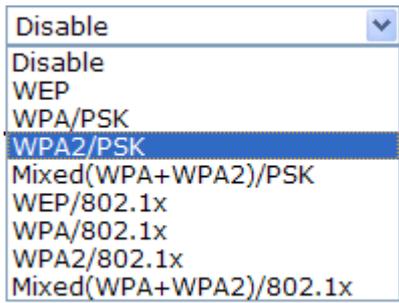
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

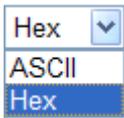
By clicking the **Security**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID: ap920-BandSteering			
Mode: Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms: <input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase:			
Key Renewal Interval: 3600 seconds			
EAPOL Key Retry: <input checked="" type="radio"/> Enable <input type="radio"/> Disable			
WEP			
<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
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>WEP/802.1x - The built-in RADIUS client feature enables</p>

	<p>VigorAP 920RP to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p>WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Enable - 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.
Key 1 – Key 4	<p>Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ';'. Such feature is available for WEP mode.</p> 

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 second(s)

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 920RP which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, 3.11 RADIUS Server to configure settings for internal server of VigorAP 920RP.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

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

3.7.3 Access Control

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

Wireless LAN (2.4GHz) >> Access Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID: ap920-BandSteering Policy: <input type="button" value="Disable"/>			
MAC Address Filter			
Index		MAC Address	
<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>			
Client's MAC Address : <input type="text"/>			
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/> Limit: 256 entries			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>	

Available settings are explained as follows:

Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 920RP. <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;"> <input type="button" value="Activate MAC address filter"/> <input type="button" value="Disable"/> <input type="button" value="Activate MAC address filter"/> <input type="button" value="Blocked MAC address filter"/> </div>
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.

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

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

3.7.4 WPS

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

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

Enable WPS 

Wi-Fi Protected Setup Information

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

Device Configure

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

Status: Idle

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 920RP is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 920RP. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, TKIP, AES, etc.) of VigorAP 920RP.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 920RP will wait for WPS requests from wireless clients about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. Both ACT and 2.4G WLAN LEDs on VigorAP 920RP will blink quickly when

	WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).
--	---

3.7.5 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 type="radio"/> Auto 20/40 MHz <input checked="" type="radio"/> 40 MHz
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
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 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
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
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
MAC Clone:	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.

OK

Cancel

Available settings are explained as follows:

Item	Description
Channel Width	<p>20 MHz- the AP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p>Auto 20/40 MHz – 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>40 MHz- the AP will use 40MHz for data transmission and receiving between the AP and the stations.</p>
Antenna	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.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold	<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>
Country Code	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.
Auto Channel Filtered Out List	The wireless channels selected in this field will be discarded if AutoSelect is selected as Channel selection mode in Wireless LAN>>General Setup .
Isolate 2.4GHz and 5GHz bands	<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"> ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if Isolate Member (in Wireless LAN>>General Setup) is NOT enabled for such SSID. ● Yet, if the function of Isolate Member (in Wireless LAN>>General Setup) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
Isolate members with IP	<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>
MAC Clone	Click Enable 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.

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

3.7.6 AP Discovery

VigorAP 920RP 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 920RP can be found. Please click **Scan** to discover all the connected APs.

Access Point List

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="radio"/>	1	AP920R-PQC...	00:1D:AA:63:2C:40	11%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	2	RD8-910c-2	02:1D:AA:78:5D:8C	1%	11	TKIP/AES	WPA2/PSK
<input type="radio"/>	3	RD8_24G_wi...	00:1D:AA:5B:A0:C8	3%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	4	YRC_DrayTe...	00:1D:AA:DD:75:B0	3%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	5	staffs	00:1D:AA:9D:68:AC	8%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	6	guests	02:1D:AA:9D:68:AC	8%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	7	AP910C-2 P...	00:1D:AA:26:8D:68	2%	11	TKIP/AES	WPA2/PSK
<input type="radio"/>	8	DrayTek	00:1D:AA:80:06:B8	1%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	9	APM-PQC-Ta...	00:1D:AA:74:DA:38	2%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	10	RD8-910c-4	02:1D:AA:7A:5D:8C	2%	11	TKIP/AES	WPA2/PSK
<input type="radio"/>	11	AP910C-ssi...	02:1D:AA:7A:5D:58	3%	11	NONE	

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
SSID	Display the SSID of the AP scanned by VigorAP 920RP.
BSSID	Display the MAC address of the AP scanned by VigorAP 920RP.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 920RP.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Add	Click Repeater for the specified AP. Next, click Add . Later, the MAC address of the AP will be added and be shown on WDS settings page.

3.7.7 WDS AP Status

VigorAP 920RP can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

Wireless LAN (2.4GHz) >> WDS AP Status

WDS AP List

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

3.7.8 WMM Configuration

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

Wireless LAN (2.4GHz) >> WMM Configuration

WMM Configuration
| [Set to Factory Default](#) |

WMM Capable Enable Disable
 APSD Capable Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input checked="" type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input checked="" type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Note: The range of setting values:
 - Aifsn : 0-15, in units of slot time
 - CWMin : 0-15, in units of slot time
 - CWMax : 0-15, in units of slot time
 - Txop : 0-256, in units of 1 us

Available settings are explained as follows:

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

	between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
AckPolicy	<p>“Uncheck” (default value) the box means the AP will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.</p> <p>“Check” the box means the AP will not answer any response request for the transmitting packets. It will have better performance with lower reliability.</p>
ACM	<p>It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.</p> <p>Note: VigorAP 920RP provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.</p>

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

3.7.9 Bandwidth Management

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

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID DrayTek			
Per Station Bandwidth Limit			
Enable	<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
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to VigorAP with the same SSID. Use the drop down list to choose the rate. If you choose User defined , you have to specify the rate manually.
Download Limit	Define the maximum speed of the data downloading which will be used for the wireless station connecting to VigorAP with the same SSID. Use the drop down list to choose the rate. If you choose User defined , you have to specify the rate manually.
Auto Adjustment	Check this box to have the bandwidth limit determined by the system automatically.
Total Upload Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data uploading.
Total Download Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data downloading.

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

3.7.10 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.

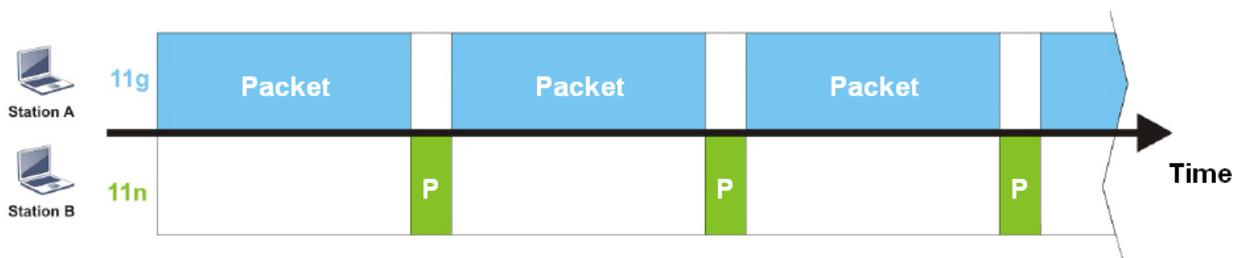
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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 920RP. 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 920RP. 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.

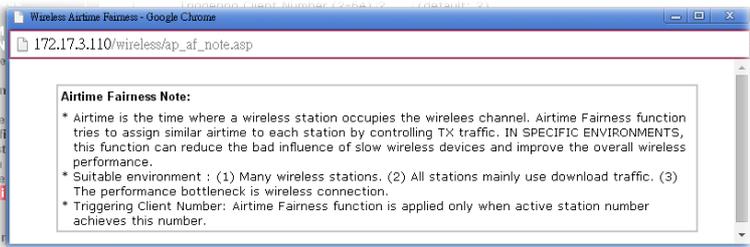
Wireless LAN (2.4GHz) >> Airtime Fairness

Enable **Airtime Fairness**

Triggering Client Number (2 ~ 128, Default: 2)

Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments. You could check [Diagnostics >> Station Airtime](#) Graph first.

Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p>Airtime Fairness – Click the link to display the following screen of airtime fairness note.</p>  <p>Triggering Client Number – 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.

3.7.11 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.

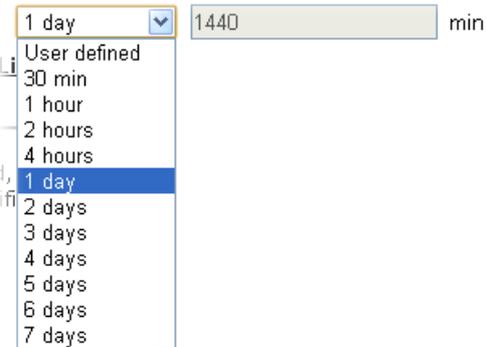
Wireless LAN (2.4GHz) >> Station Control

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

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
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	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 User defined . 
Display All Station	All the wireless stations connecting to Vigor router by using

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

3.7.12 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 (2.4GHz) >> Roaming

AP-assisted Client Roaming Parameters

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

Fast Roaming(WPA2/802.1x)

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

OK

Cancel

Available settings are explained as follows:

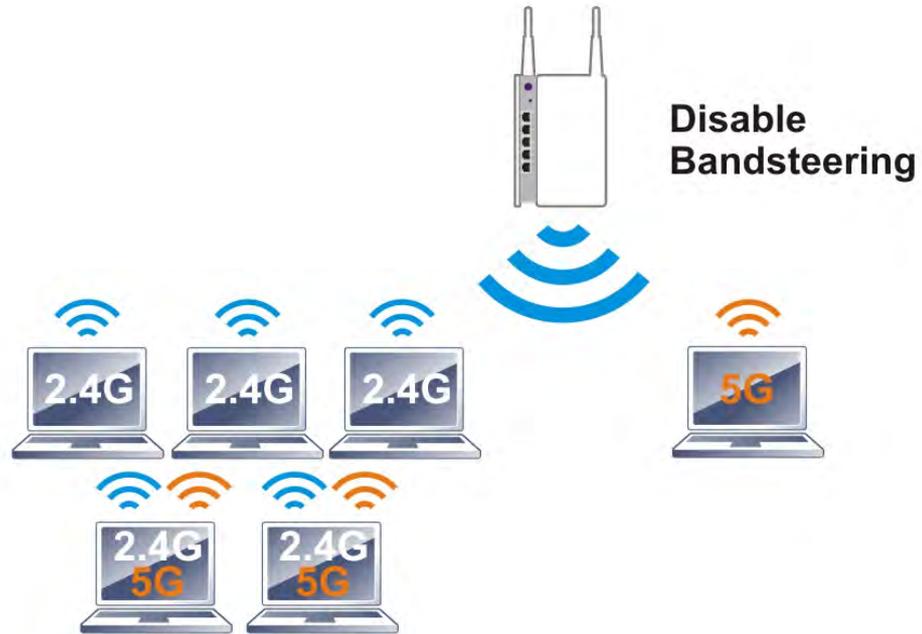
Item	Description
AP-assisted Client Roaming Parameters	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 920RP will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p>Minimum Basic Rate – Check the box to use the drop down list to specify a basic rate (Mbps). When the link rate of the wireless station is below such value, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Disable RSSI Requirement - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p>Strictly Minimum RSSI - 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 (dBm) set here, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Minimum RSSI - When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must</p>

	<p>be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of With Adjacent AP RSSI over) is detected by VigorAP 920RP, VigorAP 920RP 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"> ● With Adjacent AP RSSI over – Specify a value as a threshold.
<p>Fast Roaming (WPA2/802.1x)</p>	<p>Enable – Check the box to enable fast roaming configuration.</p> <p>PMK Caching - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1x mode.</p> <p>Pre-Authentication - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)</p>

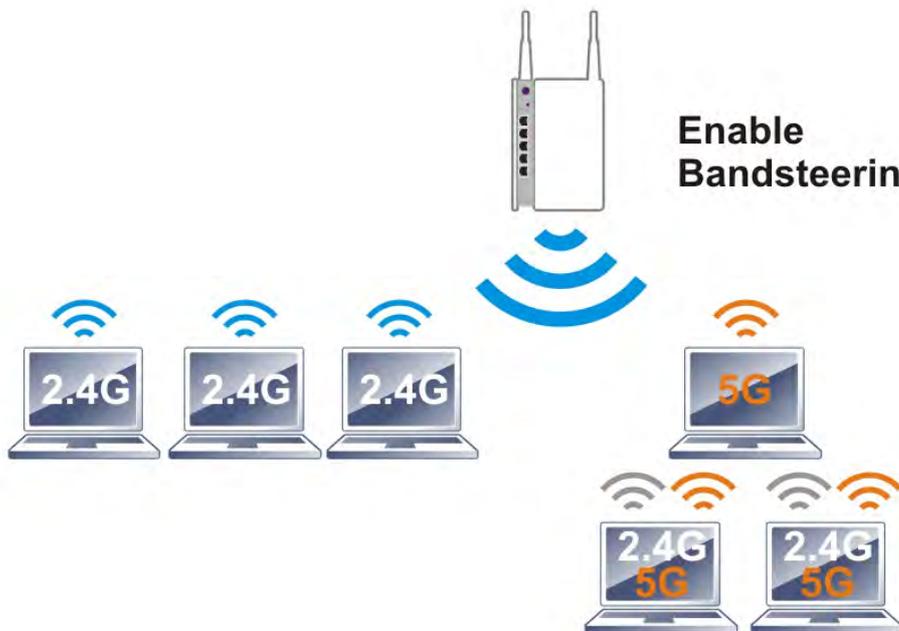
After finishing this web page configuration, please click **OK** to save the settings.

3.7.13 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)

Wait Full Time to Check 5G Capability

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

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

Overloaded

2.4GHz Utilization Overload Threshold % (Default: 70)

5GHz Utilization Overload Threshold % (Default: 70)

(Only do band steering when 2.4GHz utilization is overloaded and 5GHz utilization is not)

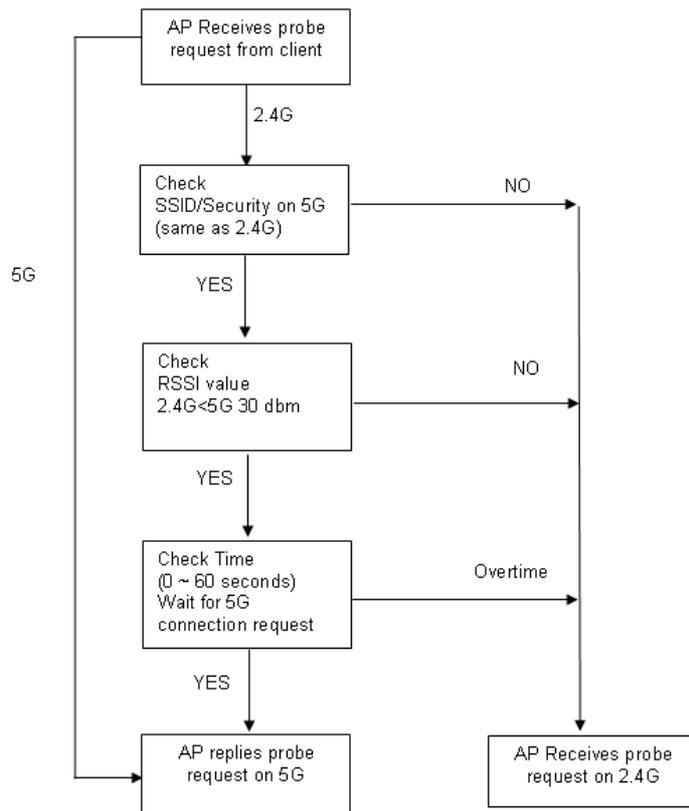
Note: Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
Enable Band Steering	<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>Check Time.... – 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>5GHz Minimum RSSI – 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 920RP, VigorAP will allow the client to connect to 2.4GHz network.</p> <p>Overloaded – If it is enabled, VigorAP will activate the band steering according to the conditions set below.</p> <ul style="list-style-type: none"> ● 2.4GHz Utilization Overload Threshold – The default setting is 70%. It can define the network congestion for 2.4GHz. ● 5GHz Utilization Overload Threshold – The default setting is 70%. It can define the network congestion for 5GHz. <p>When the utilization of 2.4GHz is higher than the specified threshold and the utilization of 5GHz is lower than the specified threshold, VigorAP will steer the client to connect to 5GHz 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

Enable **Band Steering**

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

Wait Full Time to Check 5G Capability

5GHz Minimum RSSI dBm (%) (Default: -78)
(Only do band steering when 5GHz signal is better than Minimum RSSI)

Overloaded

2.4GHz Utilization Overload Threshold % (Default: 70)

5GHz Utilization Overload Threshold % (Default: 70)
(Only do band steering when 2.4GHz utilization is overloaded and 5GHz utilization is not)

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 *ap902-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 Client Limit (3 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel :

Extension Channel :

Enable	Hide SSID	SSID	Isolate	VLAN ID Member(0:Untagged)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ap920-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>

Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Client Limit (3 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel : (Active Channel: 149) **Filtered Out List**

Details : 20/40MHz Ext Ch:153 , 80MHz Center Ch:155

Enable	Hide SSID	SSID	Isolate	VLAN ID Member (0:Untagged)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ap920-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>

Same value for 2.4GHz and 5GHz

- 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			
ap920-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
••••••••			
Key Renewal Interval			
3600 seconds			
WEP			

Same value for 2.4GHz and 5GHz

Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap920-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
••••••••			
Key Renewal Interval			
3600 seconds			
WEP			

- Now, VigorAP 920RP will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

3.7.14 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	Control	Neighbor	
Index	MAC Address	Hostname	Vendor	SSID	Link speed (TX/RX)	RSSI	TX Rate (Kbps)	RX Rate (Kbps)
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>								
<input type="button" value="Refresh"/>								

Add to Access Control :

Client's MAC Address : : : : : :

Available settings are explained as follows:

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

Control

Display connection and reconnection time of the wireless stations.

Neighbor

Display more information for the neighboring wireless stations.

3.8 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, Access Control, WPS, Advanced Setting, AP Discovery, Universal Repeater, WMM Configuration, 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 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 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel :

Extension Channel :

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	VLAN ID
1	<input type="checkbox"/>	<input type="checkbox"/>	ap920-BandSteering	<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.

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	Check the box to set the maximum number of wireless stations which try to connect Internet through VigorAP. The number you can set is from 3 to 128.
Enable Limit Client per SSID	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 128.
Mode	At present, VigorAP 920RP can connect to 11b only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.
Rate	If you choose 11b Only, such feature will be available for you to set data transmission rate.
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied

	according to the Channel selected above. Configure the extension channel you want.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 920RP while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 920RP to be identified. Default setting is DrayTek.
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.

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

3.8.2 Security

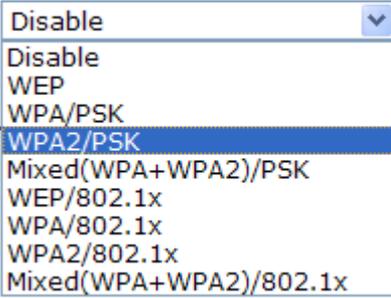
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

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

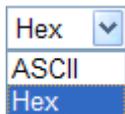
Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID		ap920-BandSteering	
Mode		Mixed(WPA+WPA2)/PSK	
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms		<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase		<input type="text" value="....."/>	
Key Renewal Interval		<input type="text" value="3600"/> seconds	
EAPOL Key Retry		<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
WEP			
<input type="radio"/> Key 1 :	<input type="text"/>	<input type="text" value="Hex"/>	
<input checked="" 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"/>	

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>

	<p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 920RP to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p>WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Type 8-63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Enable - 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.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for WEP mode.



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 second(s)

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 920RP which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, 3.11 RADIUS Server to configure settings for internal server of VigorAP 920RP.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

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

3.8.3 Access Control

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

Wireless LAN (2.4GHz) >> Access Control

SSID 1 SSID 2 SSID 3 SSID 4

SSID: DrayTek
Policy: Disable

MAC Address Filter

Index	MAC Address

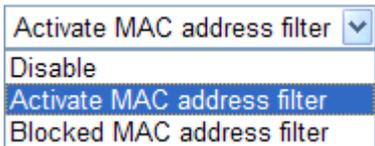
Client's MAC Address : : : : : :

Add Delete Edit Cancel Limit:256 entries

OK Cancel

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

Available settings are explained as follows:

Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 920RP. 
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.

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

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

3.8.4 WPS

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

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

Enable WPS 

Wi-Fi Protected Setup Information

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

Device Configure

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

Status: Idle

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 920RP is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 920RP. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, TKIP, AES, etc.) of VigorAP 920RP.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 920RP will wait for WPS requests from wireless clients about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. Both ACT and 2.4G WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two

minutes. (You need to setup WPS within two minutes).

3.8.5 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 type="radio"/> Auto 20/40 MHz <input checked="" type="radio"/> 40 MHz
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
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 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
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
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
MAC Clone:	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
Channel Width	<p>20 MHz - the AP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p>Auto 20/40 MHz – 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>40 MHz - the AP will use 40MHz for data transmission and receiving between the AP and the stations.</p>
Antenna	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.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold	<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>
Country Code	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.
Auto Channel Filtered Out List	The wireless channels selected in this field will be discarded if AutoSelect is selected as Channel selection mode in Wireless LAN>>General Setup .
Isolate 2.4GHz and 5GHz bands	<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"> ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if Isolate Member (in Wireless LAN>>General Setup) is NOT enabled for such SSID. ● Yet, if the function of Isolate Member (in Wireless LAN>>General Setup) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
Isolate members with IP	<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>
MAC Clone	Click Enable 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.

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

3.8.6 AP Discovery

VigorAP 920RP 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 920RP can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="radio"/>	1	staffs	00:1D:AA:9D:68:AC	4%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	2	guests	02:1D:AA:9D:68:AC	8%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	3	AP920R- PQC...	00:1D:AA:63:2C:40	15%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	4	RDB-910c-4	02:1D:AA:7A:5D:8C	1%	11	TKIP/AES	WPA2/PSK

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
SSID	Display the SSID of the AP scanned by VigorAP 920RP.
BSSID	Display the MAC address of the AP scanned by VigorAP 920RP.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 920RP.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Select as Universal Repeater	In Universal Repeater mode, WAN would work as station mode and the wireless AP can be selected as a universal repeater. Choose one of the wireless APs from the Scan list.

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

3.8.7 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	WPA2/PSK ▼
Encryption Type	AES ▼
Pass Phrase	<input type="text"/>

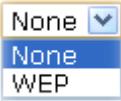
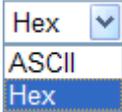
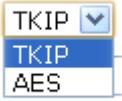
Note: If Channel is modified, the Channel setting of AP would also be changed.

Universal Repeater IP Configuration

Connection Type	DHCP ▼
Device Name	AP920RP

Available settings are explained as follows:

Item	Description
Universal Repeater Parameters	
SSID	Set the name of access point that VigorAP 920RP wants to connect to.
MAC Address (Optional)	Type the MAC address of access point that VigorAP 920RP wants to connect to.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> Open ▼ Open Shared WPA/PSK WPA2/PSK </div>
Encryption Type for	This option is available when Open/Shared is selected as

Open/Shared	<p>Security Mode.</p> <p>Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP.</p>  <p>WEP Keys - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.</p> 
Encryption Type for WPA/PSK and WPA2/PSK	<p>This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode.</p> <p>Select TKIP or AES as the algorithm for WPA.</p> 
Pass Phrase	<p>Either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
Universal Repeater IP Configuration	
Connection Type	<p>Choose DHCP or Static IP as the connection mode.</p> <p>DHCP – The wireless station will be assigned with an IP from VigorAP.</p> <p>Static IP – The wireless station shall specify a static IP for connecting to Internet via VigorAP.</p> 
Device Name	<p>This setting is available when DHCP is selected as Connection Type.</p> <p>Type a name for the router as identification. Simply use the default name.</p>
IP Address	<p>This setting is available when Static IP is selected as Connection Type.</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</p>

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

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

3.8.8 WMM Configuration

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

Wireless LAN (2.4GHz) >> WMM Configuration

WMM Configuration | [Set to Factory Default](#) |

WMM Capable Enable Disable

APSD Capable Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input checked="" type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input checked="" type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Note: The range of setting values:

- Aifsn : 0-15, in units of slot time
- CWMin : 0-15, in units of slot time
- CWMax : 0-15, in units of slot time
- Txop : 0-256, in units of 1 us

Available settings are explained as follows:

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

	<p>transmission latency.</p> <p>The default setting is Disable.</p>
Aifsn	<p>It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.</p>
CWMin/CWMax	<p>CWMin means contention Window-Min and CWMax means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.</p>
Txop	<p>It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.</p>
AckPolicy	<p>“Uncheck” (default value) the box means the AP will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.</p> <p>“Check” the box means the AP will not answer any response request for the transmitting packets. It will have better performance with lower reliability.</p>
ACM	<p>It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.</p> <p>Note: VigorAP 920RP provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.</p>

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

3.8.9 Bandwidth Management

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

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID DrayTek			
Per Station Bandwidth Limit			
Enable	<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.

Available settings are explained as follows:

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

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

3.8.10 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.

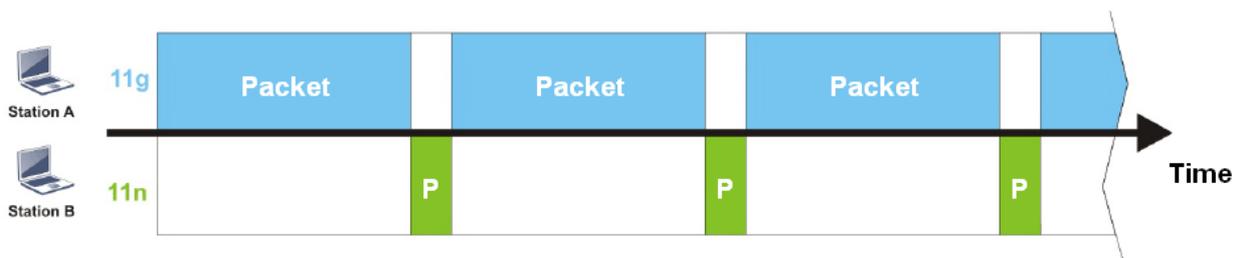
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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 920RP. 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 920RP. 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 ~ 128, Default: 2)

Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments. You could check **Diagnostics >> Station Airtime** Graph first.

Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p>Airtime Fairness – Click the link to display the following screen of airtime fairness note.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Airtime Fairness Note:</p> <ul style="list-style-type: none"> * 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. * Suitable environment : (1) Many wireless stations. (2) All stations mainly use download traffic. (3) The performance bottleneck is wireless connection. * Triggering Client Number: Airtime Fairness function is applied only when active station number achieves this number. </div> <p>Triggering Client Number –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.

3.8.11 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 (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	
Display All Station Control List			

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
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	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 User defined .
Display All Station Control List	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.

3.8.12 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 (2.4GHz) >> Roaming

AP-assisted Client Roaming Parameters

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

Fast Roaming(WPA2/802.1x)

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

OK Cancel

Available settings are explained as follows:

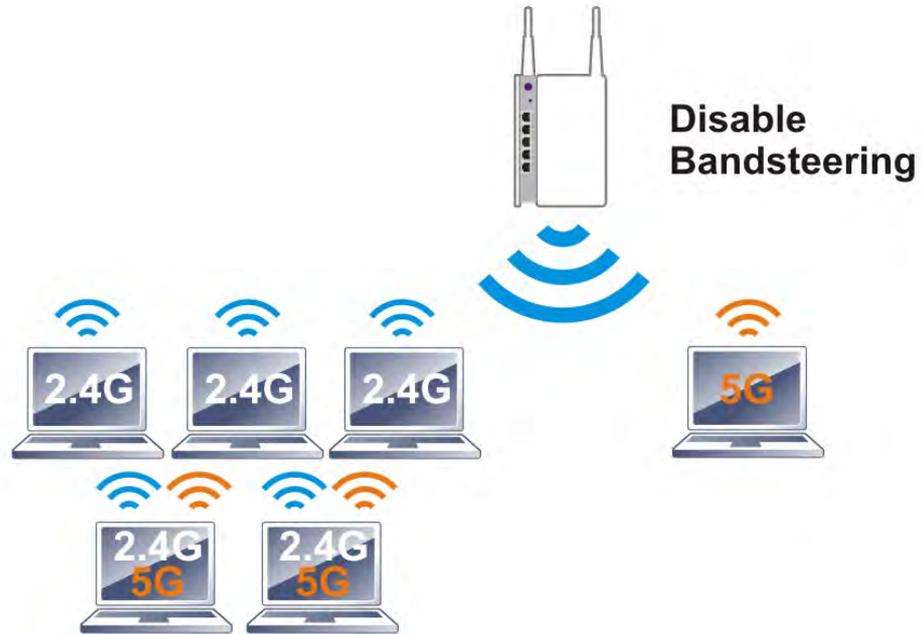
Item	Description
AP-assisted Client Roaming Parameters	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 920RP will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p>Minimum Basic Rate – Check the box to use the drop down list to specify a basic rate (Mbps). When the link rate of the wireless station is below such value, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Disable RSSI Requirement - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p>Strictly Minimum RSSI - 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 (dBm) set here, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Minimum RSSI - When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of With Adjacent AP RSSI over) is detected by VigorAP 920RP, VigorAP 920RP 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"> ● With Adjacent AP RSSI over – Specify a value as a threshold.
<p>Fast Roaming (WPA2/802.1x)</p>	<p>Enable – Check the box to enable fast roaming configuration.</p> <p>PMK Caching - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode.</p> <p>Pre-Authentication - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)</p>

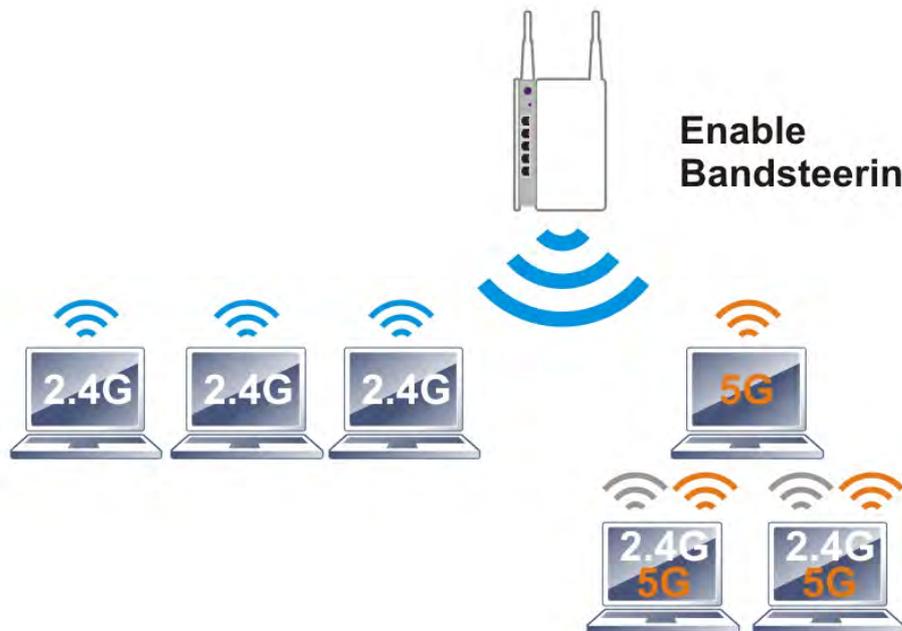
After finishing this web page configuration, please click **OK** to save the settings.

3.8.13 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)

Wait Full Time to Check 5G Capability

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

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

Overloaded

2.4GHz Utilization Overload Threshold % (Default: 70)

5GHz Utilization Overload Threshold % (Default: 70)

(Only do band steering when 2.4GHz utilization is overloaded and 5GHz utilization is not)

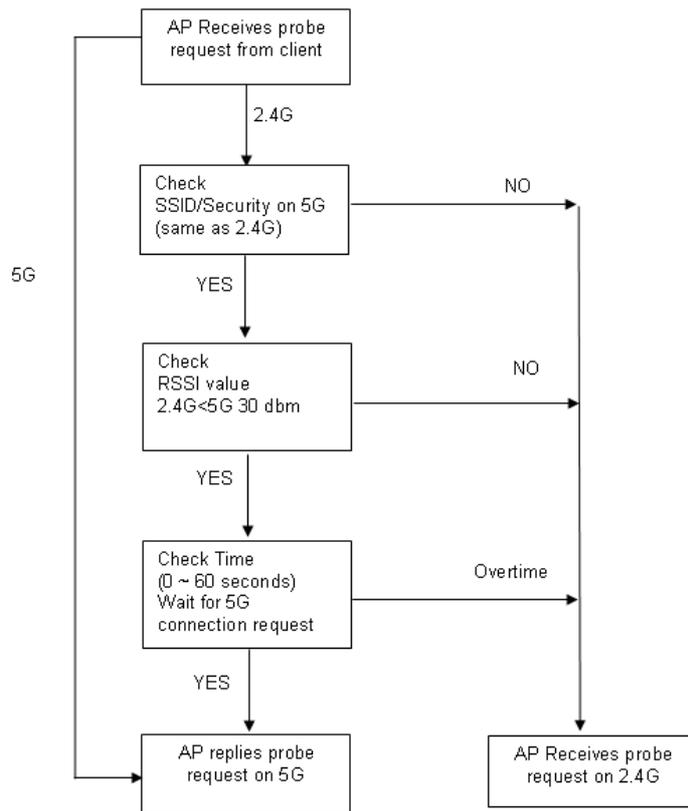
Note: Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
Enable Band Steering	<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>Check Time.... – 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>5GHz Minimum RSSI – 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 920RP, VigorAP will allow the client to connect to 2.4GHz network.</p> <p>Overloaded – If it is enabled, VigorAP will activate the band steering according to the conditions set below.</p> <ul style="list-style-type: none"> ● 2.4GHz Utilization Overload Threshold – The default setting is 70%. It can define the network congestion for 2.4GHz. ● 5GHz Utilization Overload Threshold – The default setting is 70%. It can define the network congestion for 5GHz. <p>When the utilization of 2.4GHz is higher than the specified threshold and the utilization of 5GHz is lower than the specified threshold, VigorAP will steer the client to connect to 5GHz 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

Enable **Band Steering**

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

Wait Full Time to Check 5G Capability

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

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

Overloaded

2.4GHz Utilization Overload Threshold % (Default: 70)

5GHz Utilization Overload Threshold % (Default: 70)

(Only do band steering when 2.4GHz utilization is overloaded and 5GHz utilization is not)

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 *ap902-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 Client Limit (3 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel :

Extension Channel :

Enable	Hide SSID	SSID	Isolate	VLAN ID Member(0:Untagged)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ap920-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>

Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Client Limit (3 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel : (Active Channel: 149) **Filtered Out List**

Details : 20/40MHz Ext Ch:153 , 80MHz Center Ch:155

Enable	Hide SSID	SSID	Isolate Member	VLAN ID (0:Untagged)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ap920-BandSteering	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="text" value="0"/>

Same value for 2.4GHz and 5GHz

- 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			
ap920-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
WEP			

Same value for 2.4GHz and 5GHz

Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap920-BandSteering			
Mode			
Mixed(WPA+WPA2)/PSK			
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
.....			
Key Renewal Interval			
3600 seconds			
WEP			

- Now, VigorAP 920RP will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

3.8.14 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. Each tab (general, advanced, control, neighbor) will display different status information (including MAC address, Vendor, SSID, Auth, Encrypt, Tx/Rx Rate, Hostname, RSSI, Link Speed, BW, PSM, WMM, PHMd, MCS, Connection Time, Reconnection Time, Approx. Distance, Visit Time, and so on).

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	Control	Neighbor		
Index	MAC Address	Hostname	Vendor	SSID	Link speed (TX/RX)	RSSI	TX Rate (Kbps)	RX Rate (Kbps)
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>								
<input type="button" value="Refresh"/>								

Add to Access Control :

Client's MAC Address : : : : : :

Available settings are explained as follows:

Item	Description
MAC Address	Display the MAC Address for the connecting client.
Hostname	Display the host name of the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	Client's MAC Address - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.

Add	Click this button to add current typed MAC address into Access Control .
------------	---

Control

Display connection and reconnection time of the wireless stations.

Neighbor

Display more information for the neighboring wireless stations.

3.9 Wireless LAN (5GHz) Settings for AP Mode

The AP mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.



3.9.1 General Setup

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

Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Client Limit (3 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel : (Active Channel: 149) **Filtered Out List**

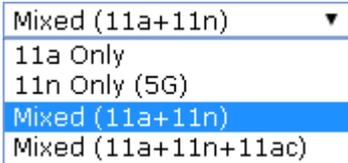
Details : 20/40MHz Ext Ch: 153 , 80MHz Center Ch: 155

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

Available settings are explained as follows:

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

	can set is from 3 to 128.
Enable Limit Client per SSID	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 128.
Mode	At present, VigorAP 920RP can be connected by 11a only, 11n only (5G), Mixed (11a+11n) and Mixed (11a+11n+ac) stations simultaneously. Simply choose Mixed (11a+11n+ac) mode. 
Channel	Means the channel of frequency of the wireless LAN. The default channel is AutoSelect . You may switch channel if the selected channel is under serious interference.
Filtered Out List	Such link will be shown if AutoSelect is selected as Channel . Click such link to access into Wireless LAN >> Advanced Settings page.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 920RP while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 920RP to be identified. Default settings are DrayTek5G.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.

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

3.9.2 Security

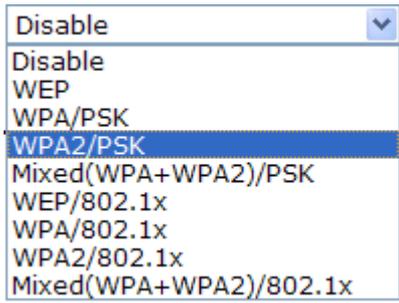
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security**, 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		Mixed(WPA+WPA2)/PSK	
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms		<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase		<input type="text" value="....."/>	
Key Renewal Interval		<input type="text" value="3600"/> seconds	
EAPOL Key Retry		<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
WEP			
<input checked="" type="radio"/> Key 1 :	<input type="text"/>	<input type="text" value="Hex"/>	
<input type="radio"/> Key 2 :	<input type="text"/>	<input type="text" value="Hex"/>	
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text" value="Hex"/>	
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text" value="Hex"/>	

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>

	<p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 920RP to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p>WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Type 8-63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Enable - 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.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for WEP mode. <div data-bbox="635 1883 762 1995" style="border: 1px solid black; padding: 2px; margin-top: 5px;"> Hex <input type="button" value="v"/> ASCII Hex </div>

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
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 920RP which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section,3.11 RADIUS Server to configure settings for internal server of VigorAP 920RP.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

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

3.9.3 Access Control

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

Wireless LAN (5GHz) >> Access Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek5G Policy: <input type="text" value="Disable"/>			
MAC Address Filter			
Index		MAC Address	
<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>			
Client's MAC Address : <input type="text"/>			
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/> Limit: 256 entries			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>	

Available settings are explained as follows:

Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 920RP. <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;"> <input type="text" value="Activate MAC address filter"/> <ul style="list-style-type: none"> Disable <li style="background-color: #e0e0e0;">Activate MAC address filter Blocked MAC address filter </div>
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.

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

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

3.9.4 WPS

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

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

Enable WPS 

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek5G
WPS Auth Mode	Mixed(WPA+WPA2)/PSK
WPS Encrypt Type	TKIP/AES

Device Configure

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

Status: Idle

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 920RP is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 920RP. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 920RP.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 920RP will wait for WPS requests from wireless clients about two minutes. Both ACT and 5G WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. Both ACT and 5G

WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

3.9.5 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
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 Filtered Out List	<input type="checkbox"/> 36 <input type="checkbox"/> 40 <input type="checkbox"/> 44 <input type="checkbox"/> 48 <input type="checkbox"/> 149 <input type="checkbox"/> 153 <input type="checkbox"/> 157 <input type="checkbox"/> 161 <input type="checkbox"/> 165
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

Note : Fragment Length take effect when mode is "11a only"

Available settings are explained as follows:

Item	Description
Channel Width	<p>20 MHz- the AP will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p>Auto 20/40 MHz – 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>
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold	<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>
Country Code	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.
Auto Channel Filtered Out List	The wireless channels selected in this field will be discarded if AutoSelect is selected as Channel selection mode in Wireless LAN>>General Setup .

<p>Isolate 2.4GHz and 5GHz bands</p>	<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"> ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if Isolate Member (in Wireless LAN>>General Setup) is NOT enabled for such SSID. ● Yet, if the function of Isolate Member (in Wireless LAN>>General Setup) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
<p>Isolate members with IP</p>	<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>

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

3.9.6 AP Discovery

VigorAP 920RP 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	AP910C-PQC...	00:1D:AA:26:8D:32	5%	149	TKIP/AES	Mixed(WPA+WPA2)/PSK
2	MK-902-mam...	00:1D:AA:3D:54:91	19%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
3	AP920RP_PQ...	00:1D:AA:63:2B:C1	4%	36	AES	WPA2/PSK
4	APMttester-...	00:1D:AA:74:DA:3A	11%	36	TKIP/AES	WPA2/PSK
5	DrayTek5G	00:1D:AA:80:06:BA	4%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
6	AP920R-PQC...	00:1D:AA:63:2C:41	28%	48	TKIP/AES	Mixed(WPA+WPA2)/PSK
7	staffs	00:1D:AA:9D:68:AE	5%	161	TKIP/AES	Mixed(WPA+WPA2)/PSK
8	910-RD8_5G	00:1D:AA:7F:5D:8E	3%	36	NONE	
9	Hotspot_5G...	00:1D:AA:CB:A3:12	70%	48	NONE	
10	Hotpost_5G...	02:1D:AA:CB:A3:12	70%	48	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 920RP.
BSSID	Display the MAC address of the AP scanned by VigorAP 920RP.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 920RP.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button

3.9.7 WMM Configuration

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

Wireless LAN (5GHz) >> WMM Configuration

WMM Configuration
[Set to Factory Default](#)

WMM Capable Enable Disable
 APSD Capable Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

Available settings are explained as follows:

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

Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
AckPolicy	<p>“Uncheck” (default value) the box means the AP will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.</p> <p>“Check” the box means the AP will not answer any response request for the transmitting packets. It will have better performance with lower reliability.</p>
ACM	<p>It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.</p> <p>Note: VigorAP 920RP provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.</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 (5GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G	
Per Station Bandwidth Limit			
Enable	<input checked="" type="checkbox"/>		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment	<input checked="" type="checkbox"/>		
Total Upload 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
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to VigorAP with the same SSID.

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

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

3.9.9 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.

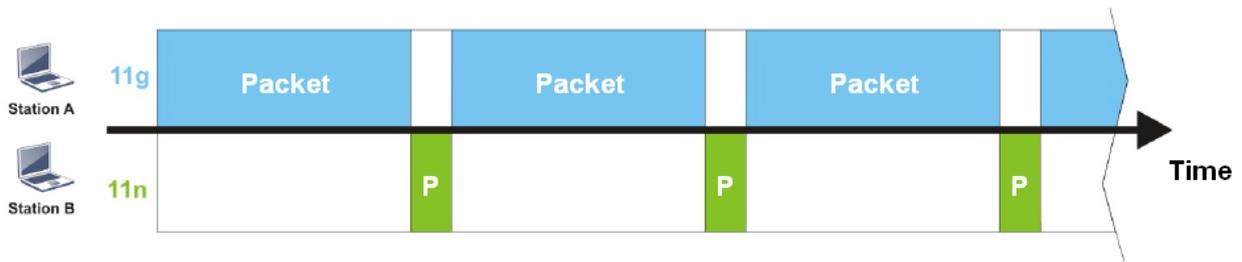
After finishing this web page configuration, please click **OK** to save the settings.

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 920RP. 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 920RP. 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

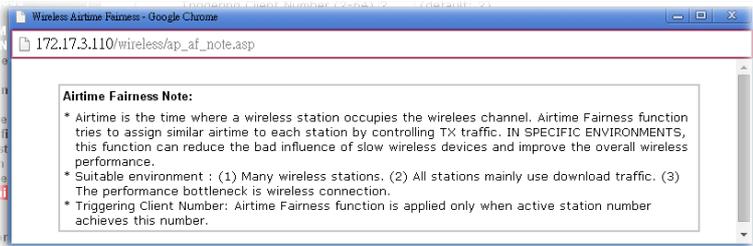
Enable **Airtime Fairness**

Triggering Client Number (2 ~ 128, Default: 2)

Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments. You could check [Diagnostics >> Station Airtime](#) Graph first.

Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. Airtime Fairness – Click the link to display the following screen of airtime fairness note.



Triggering Client Number –Airtime Fairness function is applied only when active station number achieves this number.

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 (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		
Display All Station Control List			

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
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	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 User defined .

	<div style="border: 1px solid black; padding: 5px;"> <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px; margin-right: 5px;">1 day</div> <div style="border: 1px solid black; padding: 2px; margin-right: 5px;">1440</div> <div>min</div> </div> <ul style="list-style-type: none"> User defined 30 min 1 hour 2 hours 4 hours <li style="background-color: #e0e0e0;">1 day 2 days 3 days 4 days 5 days 6 days 7 days </div>
Display All Station Control List	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.

3.9.11 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 (5GHz) >> Roaming

AP-assisted Client Roaming Parameters

Minimum Basic Rate

6

Mbps

Disable RSSI Requirement

Strictly Minimum RSSI

-73

dBm (42%) (Default: -73)

Minimum RSSI

-66

dBm (60%) (Default: -66)

with Adjacent AP RSSI over

5

dB (Default: 5)

Fast Roaming(WPA2/802.1x)

Enable

PMK Caching : Cache Period

10

minutes (10 ~ 600, Default: 10)

Pre-Authentication

Available settings are explained as follows:

Item	Description
AP-assisted Client Roaming Parameters	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 920RP 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

	<p>signal.</p> <p>Minimum Basic Rate – Check the box to use the drop down list to specify a basic rate (Mbps). When the link rate of the wireless station is below such value, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Disable RSSI Requirement - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p>Strictly Minimum RSSI - 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 (dBm) set here, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Minimum RSSI - When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of With Adjacent AP RSSI over) is detected by VigorAP 920RP, VigorAP 920RP 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"> ● With Adjacent AP RSSI over – Specify a value as a threshold.
<p>Fast Roaming (WPA2/802.1x)</p>	<p>Enable – Check the box to enable fast roaming configuration.</p> <p>PMK Caching - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode.</p> <p>Pre-Authentication - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)</p>

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

3.9.12 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. Each tab (general, advanced, control, neighbor) will display different status information (including MAC address, Vendor, SSID, Auth, Encrypt, Tx/Rx Rate, Hostname, RSSI, Link Speed, BW, PSM, WMM, PHMd, MCS, Connection Time, Reconnection Time, Approx. Distance, Visit Time, and so on).

General

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

Wireless LAN (5GHz) >> Station List

Station List

				General	Control	Neighbor		
Index	MAC Address	Hostname	Vendor	SSID	Link speed (TX/RX)	RSSI	TX Rate (Kbps)	RX Rate (Kbps)
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>								
<input type="button" value="Refresh"/>								

Add to Access Control :

Client's MAC Address : : : : : :

Available settings are explained as follows:

Item	Description
MAC Address	Display the MAC Address for the connecting client.
Hostname	Display the host name of the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	Client's MAC Address - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.

Add	Click this button to add current typed MAC address into Access Control .
------------	---

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 Universal Repeater Mode



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 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode : ▾

Channel : ▾ (Active Channel: 149) **Filtered Out List**

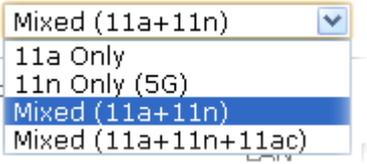
Details : 20/40MHz Ext Ch:153 , 80MHz Center Ch:155

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

Available settings are explained as follows:

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

	you can set is from 3 to 128.
Enable Limit Client per SSID	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 128.
Mode	At present, VigorAP 920RP can connect to 11a only, 11n only, Mixed (11a+11n) and Mixed (11a+11n+11ac). 
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.
Filtered Out List	Such link will be shown if AutoSelect is selected as Channel . Click such link to access into Wireless LAN >> Advanced Settings page.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 920RP while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 920RP to be identified.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.

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

3.10.2 Security

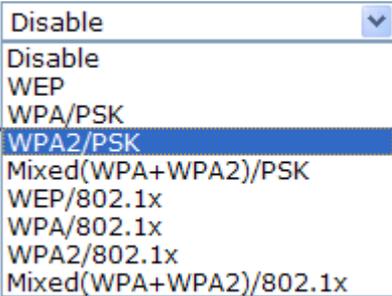
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

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

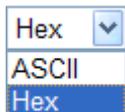
Wireless LAN (5GHz) >> Security Settings

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

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p>Disable - The encryption mechanism is turned off.</p> <p>WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>

	<p>WEP/802.1x - The built-in RADIUS client feature enables VigorAP 920RP to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p>WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Type 8-63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Enable - 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.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for WEP mode.



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

Radius Server

<input type="checkbox"/> Use internal RADIUS Server	
IP Address	<input type="text" value="0"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text" value="*****"/>
Session Timeout	<input type="text" value="0"/> second(s)

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 920RP which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section,3.11 RADIUS Server to configure settings for internal server of VigorAP 920RP.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

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

3.10.3 Access Control

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

Wireless LAN (5GHz) >> Access Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID: DrayTek5G Policy: <input type="text" value="Disable"/>			
MAC Address Filter			
Index		MAC Address	
<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>			
Client's MAC Address : <input type="text"/>			
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/> Limit: 256 entries			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>	

Available settings are explained as follows:

Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 920RP. <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"> Disable <li style="background-color: #e0e0e0;">Activate MAC address filter Blocked MAC address filter </div>
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.

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

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

3.10.4 WPS

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

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

Enable WPS 

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek5G
WPS Auth Mode	Mixed(WPA+WPA2)/PSK
WPS Encrypt Type	TKIP/AES

Device Configure

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

Status: Idle

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 920RP is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 920RP. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 920RP.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 920RP will wait for WPS requests from wireless clients about two minutes. Both ACT and 5G WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. Both ACT and 5G WLAN LEDs on VigorAP 920RP will blink quickly when WPS is in progress. It will return to normal condition after two

minutes. (You need to setup WPS within two minutes).

3.10.5 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
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 Filtered Out List	<input type="checkbox"/> 36 <input type="checkbox"/> 40 <input type="checkbox"/> 44 <input type="checkbox"/> 48 <input type="checkbox"/> 149 <input type="checkbox"/> 153 <input type="checkbox"/> 157 <input type="checkbox"/> 161 <input type="checkbox"/> 165
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

Note : Fragment Length take effect when mode is "11a only"

Available settings are explained as follows:

Item	Description
Channel Width	20 MHz- the device will use 20MHz for data transmission and receiving between the AP and the stations. Auto 20/40 MHz – 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.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold	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.
Country Code	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.
Auto Channel Filtered Out List	The wireless channels selected in this field will be discarded if AutoSelect is selected as Channel selection mode in Wireless LAN>>General Setup .
Isolate 2.4GHz and	The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless

5GHz bands	<p>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"> ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if Isolate Member (in Wireless LAN>>General Setup) is NOT enabled for such SSID. ● Yet, if the function of Isolate Member (in Wireless LAN>>General Setup) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
Isolate members with IP	<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>

3.10.6 AP Discovery

VigorAP 920RP 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 920RP 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	DrayTek5G	00:1D:AA:80:06:BA	8%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	2	APMtester-...	00:1D:AA:74:DA:3A	8%	36	TKIP/AES	WPA2/PSK
<input type="radio"/>	3	MK-902-mam...	00:1D:AA:3D:54:91	22%	36	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	4	AP920R-PQC...	00:1D:AA:63:2C:41	25%	48	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	5	AP910C-PQC...	00:1D:AA:26:8D:32	5%	149	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	6	staffs	00:1D:AA:9D:68:AE	5%	161	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	7	guests	02:1D:AA:9D:68:AE	8%	161	TKIP/AES	Mixed(WPA+WPA2)/PSK
<input type="radio"/>	8	910-RD8_5G	00:1D:AA:7F:5D:8E	3%	36	NONE	
<input type="radio"/>	9	Hotspot_5G...	00:1D:AA:CB:A3:12	70%	48	NONE	
<input type="radio"/>	10	Hotpost_5G...	02:1D:AA:CB:A3:12	73%	48	NONE	

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
------	-------------

SSID	Display the SSID of the AP scanned by VigorAP 920RP.
BSSID	Display the MAC address of the AP scanned by VigorAP 920RP.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 920RP.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Select as Universal Repeater	In Universal Repeater mode, WAN would work as station mode and the wireless AP can be selected as a universal repeater. Choose one of the wireless APs from the Scan list.

3.10.7 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	<input type="text" value="36"/> ▾
Security Mode	Open ▾
Encryption Type	None ▾
WEP Keys	
<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 ▾

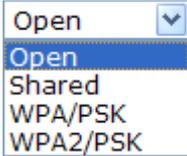
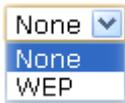
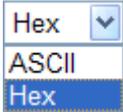
Note: If Channel is modified, the Channel setting of AP would also be changed.

Universal Repeater IP Configuration

Connection Type	DHCP ▾
Router Name	AP920RP

Available settings are explained as follows:

Item	Description
SSID	Set the name of access point that VigorAP 920RP wants to connect to.
MAC Address (Optional)	Type the MAC address of access point that VigorAP 920RP wants to connect to.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 36. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.

	
Encryption Type for Open/Shared	<p>This option is available when Open/Shared is selected as Security Mode.</p> <p>Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP.</p>  <p>WEP Keys - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.</p> 
Encryption Type for WPA/PSK and WPA2/PSK	<p>This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode.</p> <p>Select TKIP or AES as the algorithm for WPA.</p> 
Pass Phrase	<p>Type 8-63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
Connection Type	<p>Choose DHCP or Static IP as the connection mode.</p> <p>DHCP – The wireless station will be assigned with an IP from.</p> <p>Static IP – The wireless station shall specify a static IP for connecting to Internet via VigorAP.</p> 
Router Name	<p>This setting is available when DHCP is selected as Connection Type.</p> <p>Type a name for the VigorAP as identification. Simply use the default name.</p>
IP Address	<p>This setting is available when Static IP is selected as</p>

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

3.10.8 WMM Configuration

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

Wireless LAN (5GHz) >> WMM Configuration

WMM Configuration | [Set to Factory Default](#) |

WMM Capable Enable Disable

APSD Capable Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input checked="" type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input checked="" type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Note: The range of setting values:

- Aifsn : 0-15, in units of slot time
- CWMin : 0-15, in units of slot time
- CWMax : 0-15, in units of slot time
- Txop : 0-256, in units of 1 us

Available settings are explained as follows:

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable radio button.
APSD Capable	APSD (automatic power-save delivery) is an enhancement over

	<p>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 Disable.</p>
Aifsn	<p>It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.</p>
CWMin/CWMax	<p>CWMin means contention Window-Min and CWMax means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.</p>
Txop	<p>It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.</p>
AckPolicy	<p>“Uncheck” (default value) the box means the AP will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.</p> <p>“Check” the box means the AP will not answer any response request for the transmitting packets. It will have better performance with lower reliability.</p>
ACM	<p>It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.</p> <p>Note: VigorAP 920RP provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.</p>

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

3.10.9 Bandwidth Management

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

Wireless LAN (5GHz) >> Bandwidth Management

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

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

3.10.10 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.

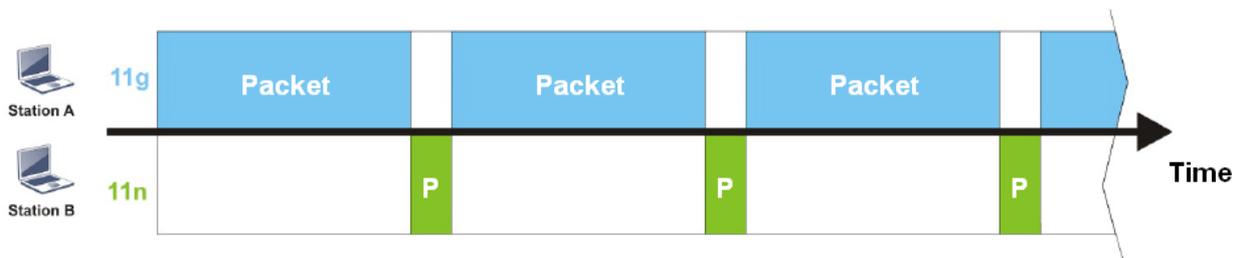
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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 920RP. 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 920RP. 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:

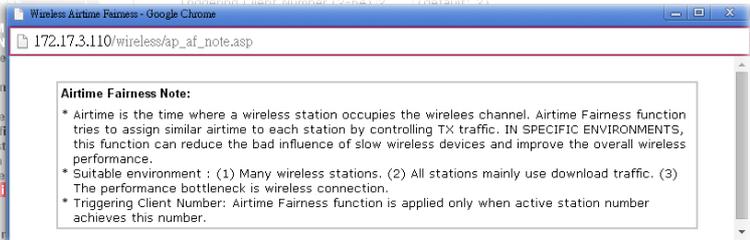
- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

Wireless LAN (5GHz) >> Airtime Fairness

Enable **Airtime Fairness**
 Triggering Client Number (2 ~ 128, Default: 2)

Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments. You could check [Diagnostics >> Station Airtime](#) Graph first.

Available settings are explained as follows:

Item	Description
<p>Enable Airtime Fairness</p>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p>Airtime Fairness – Click the link to display the following screen of airtime fairness note.</p>  <p>Triggering Client Number – 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.

3.10.11 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		
Display All Station Control List			

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
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	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 User defined . <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px;">1 day</div> <div style="margin: 0 5px;">▼</div> <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;">1440</div> <div style="margin-left: 5px;">min</div> </div> <ul style="list-style-type: none"> User defined 30 min 1 hour 2 hours 4 hours <li style="background-color: #e0e0e0;">1 day 2 days 3 days 4 days 5 days 6 days 7 days </div>
Display All Station Control List	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.

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

Fast Roaming(WPA2/802.1x)

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

OK Cancel

Available settings are explained as follows:

Item	Description
AP-assisted Client Roaming Parameters	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 920RP 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>Minimum Basic Rate – Check the box to use the drop down list to specify a basic rate (Mbps). When the link rate of the wireless station is below such value, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Disable RSSI Requirement - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p>Strictly Minimum RSSI - 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 (dBm) set here, VigorAP 920RP will terminate the network connection for that wireless station.</p> <p>Minimum RSSI - When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of With Adjacent AP RSSI over) is detected by VigorAP 920RP, VigorAP 920RP 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"> ● With Adjacent AP RSSI over – Specify a value as a threshold.
<p>Fast Roaming (WPA2/802.1x)</p>	<p>Enable – Check the box to enable fast roaming configuration.</p> <p>PMK Cache Period - Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode.</p> <p>Pre-Authentication - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)</p>

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

3.10.13 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. Each tab (general, advanced, control, neighbor) will display different status information (including MAC address, Vendor, SSID, Auth, Encrypt, Tx/Rx Rate, Hostname, RSSI, Link Speed, BW, PSM, WMM, PHMd, MCS, Connection Time, Reconnection Time, Approx. Distance, Visit Time, and so on).

General

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

Wireless LAN (5GHz) >> Station List

Station List

				General	Control	Neighbor		
Index	MAC Address	Hostname	Vendor	SSID	Link speed (TX/RX)	RSSI	TX Rate (Kbps)	RX Rate (Kbps)
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>								
<input type="button" value="Refresh"/>								

Add to **Access Control** :

Client's MAC Address : : : : : :

Available settings are explained as follows:

Item	Description
MAC Address	Display the MAC Address for the connecting client.
Hostname	Display the host name of the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	Client's MAC Address - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.

Add

Click this button to add current typed MAC address into **Access Control**.

Control

Display connection and reconnection time of the wireless stations.

Neighbor

Display more information for the neighboring wireless stations.

3.11 RADIUS Setting

3.11.1 RADIUS Server

VigorAP 920RP offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 920RP. 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 : <input type="button" value="Backup"/>	Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>
---	---

Available settings are explained as follows:

Item	Description
Enable RADIUS Server	Check it to enable the internal RADIUS server.
Authentication Type	Let the user to choose the authentication method for RADIUS server. Radius EAP Type – 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.
Users Profile	Username – Type a new name for the user profile. Password – Type a new password for such new user profile. Confirm Password – Retype the password to confirm it. Configure <ul style="list-style-type: none"> ● Add – Make a new user profile with the name and password specified on the left boxes. ● Cancel – Clear current settings for user profile. Delete Selected – Delete the selected user profile (s).

	Delete All – Delete all of the user profiles.
Authentication Client	<p>This internal RADIUS server of VigorAP 920RP 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 920RP as its external RADIUS server.</p> <p>Client IP – Type the IP address for the user to be authenticated by VigorAP 920RP when the user tries to use VigorAP 920RP as the external RADIUS server.</p> <p>Secret Key – Type the password for the user to be authenticated by VigorAP 920RP while the user tries to use VigorAP 920RP as the external RADIUS server.</p> <p>Confirm Secret Key – Type the password again for confirmation.</p> <p>Configure</p> <ul style="list-style-type: none"> ● Add – Make a new client with IP and secret key specified on the left boxes. ● Cancel – Clear current settings for the client. <p>Delete Selected – Delete the selected client(s).</p> <p>Delete All – Delete all of the clients.</p>
Backup	Click it to store the settings (RADIUS configuration) on this page as a file.
Restore	Click it to restore the settings (RADIUS configuration) from an existed file.

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

3.11.2 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 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

Certificate Name	Root CA
Subject Name	
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"/>
Key Type	RSA ▼
Key Size	1024 Bit ▼
Apply to Web HTTPS	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Subject Name	<p>Type the required information for creating a root CA.</p> <p>Country (C) – Type the country code (two characters) in this box.</p> <p>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.</p> <p>Email (E) – Type the email address for the root CA with length less than 32 characters.</p>
Key Type	At present, only RSA (an encryption algorithm) is supported by such device.
Key Size	To determine the size of a key to be authenticated, use the drop down list to specify the one you need.
Apply to Web HTTPS	<p>VigorAP needs a certificate to access into Internet via Web HTTPS.</p> <p>Check this box to use the user-defined root CA certificate which will substitute for the original certificate applied by web HTTPS.</p>

Note: “Common Name” must be configured with rotuer’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.

3.12 Applications

Below shows the menu items for Applications.



3.12.1 Schedule

The VigorAP 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 VigorAP'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

Enable Schedule

OK

Schedule Configuration

Index.	Setting	Action	Status
1 <input type="checkbox"/>	2016 Jan. 1, 08:00 Once	Auto Reboot	V

Add

Delete

Available settings are explained as follows:

Item	Description
Schedule	Enable Schedule - Check it to enable the function of schedule configuration.
Schedule Configuration	<p>Index – Display the sort number of the schedule profile.</p> <p>Setting – Display the summary of the schedule profile.</p> <p>Action – Display the action adopted by the schedule profile.</p> <p>Status – Display if the profile is enabled (V) or not (X).</p> <p>Add – Such button is available when Enable Schedule is checked. It allows to add a new schedule profile.</p> <p>Delete – Check the index box of the schedule profile and click such button to remove the profile.</p>

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

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

Applications >> Schedule

Add Schedule

Enable

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

Start Time: 0 : 0 (Hour : Minute)

Duration Time: 0 : 0 (Hour : Minute)

End Time: 0 : 0 (Hour : Minute)

Action: Auto Reboot

WiFi(2.4GHz): Radio SSID2 SSID3 SSID4

WiFi(5GHz): Radio SSID2 SSID3 SSID4

Acts: Once

Weekday: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Note: If we set WiFi schedule "Start Time" and "End Time" at exact same time, AP will execute the schedule without an end time.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Check to enable such schedule profile.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
Duration Time	Specify the duration (or period) for the schedule.
End Time	Specify the ending time of the schedule.
Action	Specify which action should apply the schedule.
WiFi(2.4GHz)/ WiFi(5GHz)	When Wi-Fi UP or Wi-Fi DOWN is selected as Action , you can check the Radio or SSID 2~4 boxes (2.4GHz and 5GHz respectively) to setup the network based on the schedule profile. Note: When Radio is selected, SSID2, SSID3 and SSID4 are not available for choosing, vice versa.
Acts	Specify how often the schedule will be applied. Once -The schedule will be applied just once Routine -Specify which days in one week should perform the schedule. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> Routine Once Routine </div>
Weekday	Choose and check the day to perform the schedule. It is available when Routine is selected as Acts .

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

Applications >> Schedule

Schedule

Enable Schedule

OK

Schedule Configuration

Index.	Setting	Action	Status
1 <input type="checkbox"/>	2000 Jan. 1, 00:00 Once	Auto Reboot	V

Add

Delete

3.12.2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 920RP will send the UDP packets with 5353 port to the specific IP every five seconds.

Applications >> Apple iOS Keep Alive

Enable Apple iOS Keep Alive

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

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

OK

Cancel

Available settings are explained as follows:

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

3.12.3 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 automatically. 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
Enable Connection Detection	Check the box to enable such function.
When the AP is unable to ping the host	<p>When VigorAP cannot ping the host, then the following actions shall be performed.</p> <p>Wi-Fi – Choose Off to disconnect the wireless connection; choose No Change to keep the Wi-Fi connection still.</p> <p>Sound Buzzer – Vigor AP will make sound according to the buzzer profile selected here. Or no sound will be made if None is specified here.</p> <p>LED – The LED on the front panel will be off if Off is selected. If No Change is selected, the LED will be on still.</p>

3.12.4 Sensor

With built-in temperature and humidity sensor, VigorAP 920 will monitor temperature around the device and send alert message to notify the system administrator by Syslog or e-mail.

Sensor Settings

Applications >> Sensor Setting

Sensor Graph
Sensor Settings

Enable "Sensor Graph"
 Alerts once via "Alert Method" when any sensor value is outside of "Alert Criteria" range

Alert Method
 Syslog Mail

Alert Criteria
inside case : -30.0 ~ 90.0 °C °F , calibration/current val: 0.0 77.0
 Humidity Sensor: 0.0 ~ 98.0 % , calibration/current val: 0.0 23.4

Note:

1. Wi-Fi temperature is only available when the selected Wi-Fi is enabled

Available settings are explained as follows:

Item	Description
Enable "Sensor Graph"	To display a graph for the connected sensor, check the box.
Alerts	It can determine the time/interval to send an alert message. Once – An alert will be sent out once when the sensor value is outside the range defined in Alert Criteria. Per min. – Alert message will be sent out per minute when the sensor value is outside the range defined in Alert Criteria.
Alert Method	Syslog - The humidity log containing the alarm message will be recorded on Syslog if it is enabled. Mail - The humidity log containing the alarm message will be sent by mail.
Alert Criteria	Alert message will be sent out according to the rules specified in this field. Inside case – The temperature reading is obtained just from the data recorded inside the chip of VigorAP. 2.4GHz Wi-Fi – The temperature reading for 2.4G Wi-Fi network operation is estimated by using 2.4GHz CPU Wi-Fi module. The built-in sensor of VigorAP contains temperature sensor and humidity sensor. Please type the upper limit and lower limit for VigorAP system to send out

temperature alert / humidity alert.

Calibration / current val- Type values used for correcting the temperature error and humidity error.

C°/F° - Choose the display unit of the temperature. There are two types for you to choose.

Sensor Graph

Below shows an example of temperature graph.

Click the circles (blue, orange, green and red) on the screen to display / close the wave charts related to “inside case”, “2.4GHz Wi-Fi”, “5GHz Wi-Fi” and “Relative Humidity”.

Applications >> Sensor Graph

Sensor Graph

Sensor Settings

Status: OK

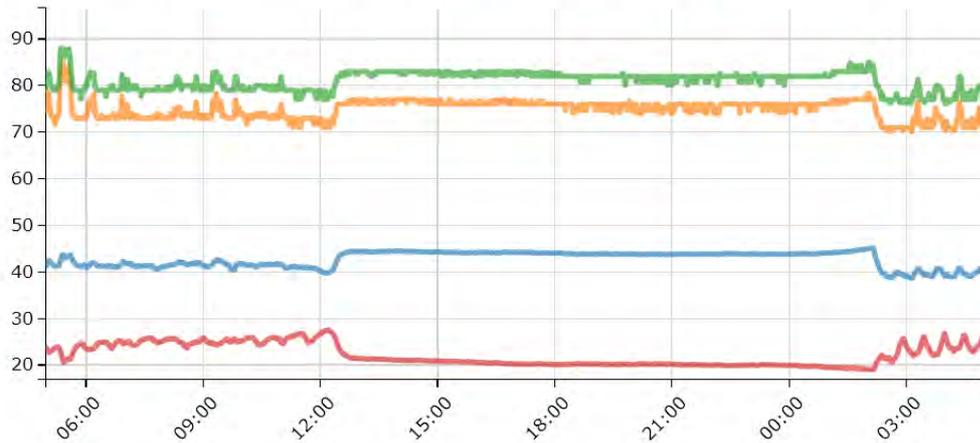
Interval: 1 days

● inside case(°C)

● 2.4GHz Wi-Fi(°C)

● 5GHz Wi-Fi(°C)

● Relative Humidity(%)



Statistics

Click **Statistics** button to get statistics data, shown as follows:

Applications >> Sensor Graph

Sensor Graph
Sensor Settings

Status: OK Interval: days

● inside case(°C)
 ● 2.4GHz Wi-Fi(°C)
 ● 5GHz Wi-Fi(°C)
 ● Relative Humidity(%)



[Hide](#)

Sensor	Max.	Min.	Avg.
inside case(°C)	45.1	38.7	42.7
2.4GHz Wi-Fi(°C)	85.0	70.0	74.9
5GHz Wi-Fi(°C)	88.0	76.0	81.0
Relative Humidity(%)	27.5	18.9	22.1

3.13 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.



3.13.1 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		F0:DB:F8:1C:E4:9F	Apple	iPad	Pass
2		F4:F1:5A:8A:E8:B9	Apple	iPhone	Pass
3		60:FA:CD:71:9B:91	Apple	Detecting	Pass
4		44:2A:60:80:15:D6	Apple	Detecting	Pass

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

 iOS  Android  Windows  Linux  Others

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
- Andorid
- WindowsPhone
- BlackBerry
- Symbian.

3.13.2 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

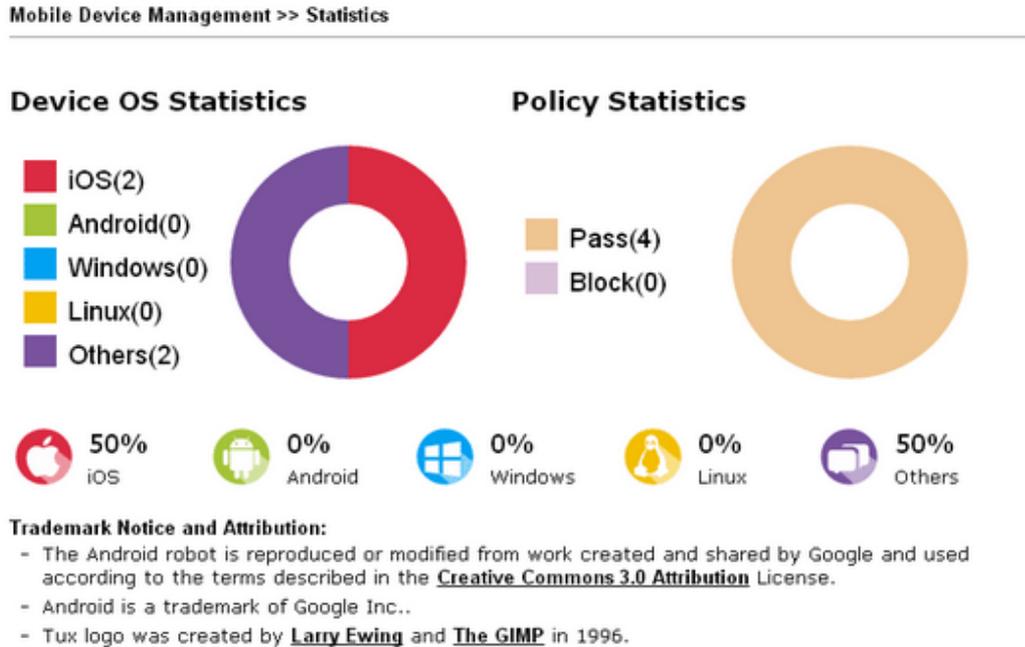
Each item is explained as follows:

Item	Description
Block Mobile Connections	All of mobile devices will be blocked and not allowed to access into Internet via VigorAP.
Block PC Connections	All of network connections based on PC, MAC or Linux platform will be blocked and terminated.
Block Unknown Connections	Only the unknown network connections (unable to be recognized by Vigor router) will be blocked and terminated.
WiFi(2.4GHz)	Specify the SSID(s) to apply such policy.
WiFi(5GHz)	Specify the SSID(s) to apply such policy.

After finished the policy selection, click **OK**. VigorAP will *reboot* to activate the new policy automatically.

3.13.3 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.



3.14 System Maintenance

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

Below shows the menu items for System Maintenance.



3.14.1 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 : VigorAP920RP
Device Name : VigorAP920RP
Firmware Version : 1.2.1
Build Date/Time : r8162 Mon, 26 Mar 2018 14:00:33
System Uptime : 0d 03:53:12
Operation Mode : Universal Repeater

System	
Memory Total	: 236784 kB
Memory Left	: 117592 kB
Cached Memory	: 23984 kB / 236784 kB

LAN	
MAC Address	: 00:1D:AA:5C:A6:58
IP Address	: 192.168.1.1
IP Mask	: 255.255.255.0

Wireless LAN (2.4GHz)	
MAC Address	: 00:1D:AA:5C:A6:58
SSID	: ap920-BandSteering
Channel	: 11
Driver Version	: 10.4

Wireless LAN (5GHz)	
MAC Address	: 00:1D:AA:5C:A6:59
SSID	: DrayTek5G
Channel	: Auto(44)
Driver Version	: 10.4

Universal Repeater(5GHz)	
MAC Address	: 12:1D:AA:5C:A6:59
SSID	:
Channel	: Auto(44)

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 /Device Name	Display the model name of the modem.
Firmware Version	Display the firmware version of the modem.
Build Date/Time	Display the date and time of the current firmware build.
System Uptime	Display the period that such device connects to Internet.
Operation Mode	Display the operation mode that the device used.
<i>System</i>	
Memory total	Display the total memory of your system.
Memory left	Display the remaining memory of your system.
<i>LAN</i>	
MAC Address	Display the MAC address of the LAN Interface.
IP Address	Display the IP address of the LAN interface.
IP Mask	Display the subnet mask address of the LAN interface.
<i>Wireless LAN (2.4GHz/5GHz)</i>	
MAC Address	Display the MAC address of the WAN Interface.
SSID	Display the SSID of the device.
Channel	Display the channel that the station used for connecting with such device.

3.14.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device (Vigor router, AP and etc.) through VigorACS (Auto Configuration Server).

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 : ●		

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="*****"/>
DNS Server IP Address	
Primary IP Address	<input type="text"/>
Secondary IP Address	<input type="text"/>

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>URL/Username/Password – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user’s manual for detailed information. The setting for URL can be domain name or IP address.</p> <p>Test With Inform – Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server.</p> <p>Event Code – Use the drop down menu to specify an event to</p>

	<p>perform the test.</p> <p>Last Inform Response Time – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.</p>
CPE Settings	<p>Such information is useful for Auto Configuration Server (ACS).</p> <p>Enable– Check the box to allow the CPE Client to connect with Auto Configuration Server.</p> <p>SSL(HTTPS) Mode - Check the box to allow the CPE client to connect with ACS through SSL.</p> <p>Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</p> <p>Username/Password – Type the username and password that VigorACS can use to access into such CPE.</p> <p>DNS Server IP Address – Such field is to specify the IP address if a URL is configured with a domain name.</p> <ul style="list-style-type: none"> ● Primary IP Address –You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field. ● Secondary IP Address –You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
Periodic Inform Settings	<p>The default setting is Enable. Please set interval time or schedule time for the AP to send notification to VigorACS server. Or click Disable to close the mechanism of notification.</p> <p>Interval Time – Type the value for the interval time setting. The unit is “second”.</p>
STUN Settings	<p>The default is Disable. If you click Enable, please type the relational settings listed below:</p> <p>Server Address – Type the IP address of the STUN server.</p> <p>Server Port – Type the port number of the STUN server.</p> <p>Minimum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is “60 seconds”.</p> <p>Maximum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of “-1” indicates that no maximum period is specified.</p>

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

3.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administration Password

Administrator Settings

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

Note : Authorization 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
Account	Type the name for accessing into Web User Interface.
Password	Type in new password in this filed.
Confirm Password	Type the new password again for confirmation.
Password Strength	The system will display the password strength (represented with the word of weak, medium or strong) of the password specified above.

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

3.14.4 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

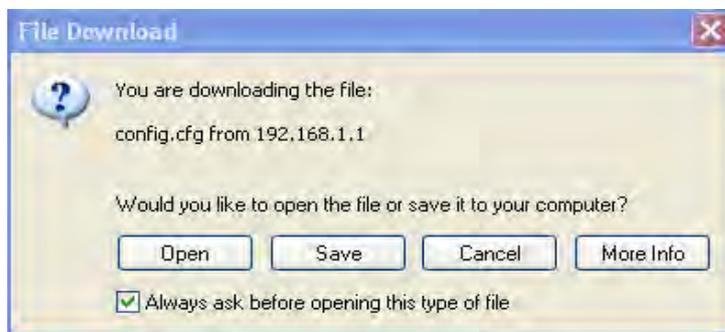
Please specify a password and click Backup to download current configuration as an encrypted file.

Protect with password

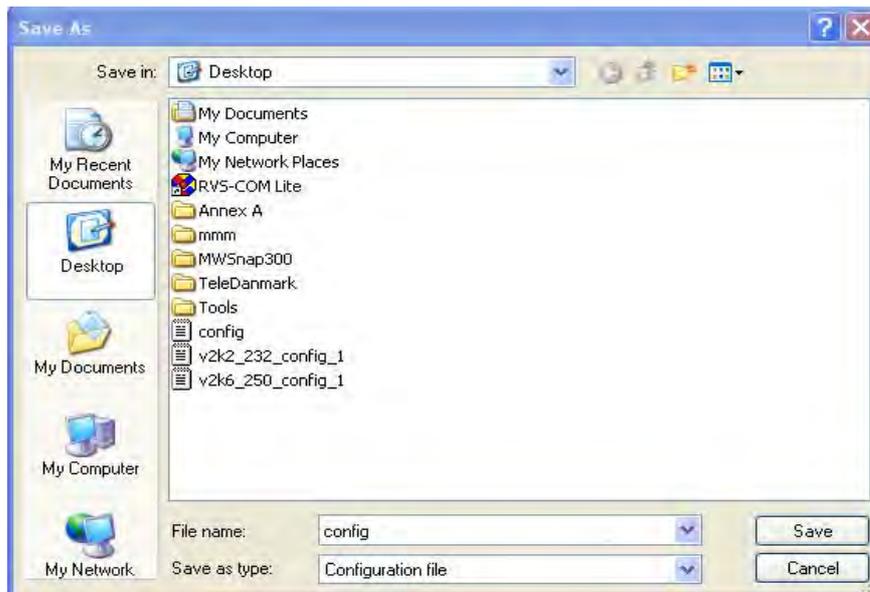
Password (Max. 23 characters allowed)

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.

3.14.5 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	<input type="button" value="All"/>

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
Syslog Access Setup	<p>Enable - Check Enable to activate function of Syslog.</p> <p>Server IP Address -The IP address of the Syslog server.</p> <p>Destination Port -Assign a port for the Syslog protocol. The default setting is 514.</p> <p>Log Level - Specify which level of the severity of the event will be recorded by Syslog.</p>
Mail Alert Setup	<p>Check Enable to activate function of mail alert.</p> <p>SMTP Server - The IP address of the SMTP server.</p> <p>Mail To - Assign a mail address for sending mails out.</p> <p>Mail From - Assign a path for receiving the mail from outside.</p> <p>User Name - Type the user name for authentication.</p> <p>Password - Type the password for authentication.</p> <p>Use TLS – 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>Enable E-Mail Alert - VigorAP will send an e-mail out when a user accesses into the user interface by using web or telnet.</p> <p>When Admin Login AP – Enable/disable the function. When it</p>

	is enabled, VigorAP will send out an e-mail to the recipient defined above when a user tries to access into VigorAP by entering login username and password.
--	--

3.14.6 Time and Date

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

System Maintenance >> Time and Date

Time Information

Current System Time	2017 Nov 2 Thu 16:48:42	Inquire Time
status	browser time synchronized	

Time Setting

<input checked="" type="radio"/> Use Browser Time	
<input type="radio"/> Use NTP Client	
Time Zone	(GMT-11:00) Midway Island, Samoa
NTP Server	Use Default
Daylight Saving	<input type="checkbox"/>
NTP synchronization	30 sec

OK Cancel

Available parameters are explained as follows:

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

Click **OK** to save these settings.

3.14.7 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than SNMP** through authentication method (support MD5) for the management needs.

System Maintenance >> SNMP

SNMP Agent

<input type="checkbox"/> Enable SNMP Agent	
<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
Enable SNMP Agent / Enable SNMPV3 Agent	Check it to enable this function.
USM User	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.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm.
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.

3.14.8 Management

This page allows you to specify the port number for HTTP and HTTPS server.

System Maintenance >> Management

Device Name

Name	VigorAP920RP
------	--------------

Management Port Setup

HTTP Port	80
HTTPS Port	443

Telnet Setup

Telnet Server	Enable
---------------	--------

LED Setup

LED Status	Original
------------	----------

OK Cancel

Available parameters are explained as follows:

Item	Description
Device Name	Name - The default setting is VigorAP 920RP. Change the name if required.
Management Port Setup	HTTP port/HTTPS port -Specify user-defined port numbers for the HTTP and HTTPS servers.
Telnet Setup	Enable – The administrator / user can access into the command line interface of VigorAP remotely for configuring settings. Disable – The administrator / user is unable to access into the command line interface of VigorAP remotely for configuring settings.
LED Setup	The LED (on or flashing) can be switched on or off to meet your favor. Original – Click it to restore the original LED display status. All on – Turn on all of the LEDs. All off – Turn off all of the LEDs.

3.14.9 Reboot System

The web user interface 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

OK

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.

3.14.10 Firmware Upgrade

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

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

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

System Maintenance >> Firmware Upgrade

Firmware Update

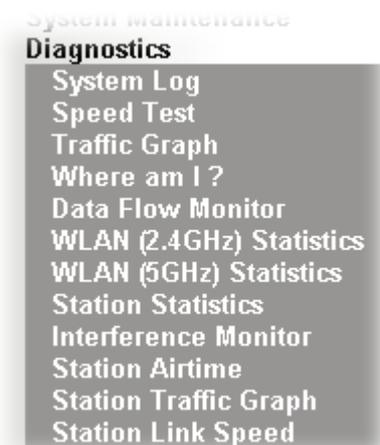
Select a firmware file.

Click Upgrade to upload the file.

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

3.15 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your VigorAP 920RP.



3.15.1 System Log

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

Diagnostics >> System Log

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

```
Sep 27 05:12:18 syslogd started: BusyBox v1.23.2
Sep 27 05:12:18 kernel: klogd started: BusyBox v1.23.2 (2017-09-20 14:07:13 CST)
Sep 27 05:12:18 kernel: [600675.070674] [syscall](9) flag: 0x0
Sep 27 05:12:18 kernel: [600675.073147] [syscall](9) ravid 0: 0x0
Sep 27 05:12:18 kernel: [600675.076878] [syscall](9) ravid 1: 0x0
Sep 27 05:12:18 kernel: [600675.080652] [syscall](9) ravid 2: 0x0
Sep 27 05:12:18 kernel: [600675.084344] [syscall](9) ravid 3: 0x0
Sep 27 05:12:18 kernel: [600675.088109] [syscall](9) ravid 4: 0x0
Sep 27 05:12:18 kernel: [600675.091811] [syscall](9) ravid 5: 0x0
Sep 27 05:12:18 kernel: [600675.095544] [syscall](9) ravid 6: 0x0
Sep 27 05:12:18 kernel: [600675.099636] [syscall](9) ravid 7: 0x0
Sep 27 05:12:18 kernel: [600675.103003] [syscall](9) ravid 8: 0x0
Sep 27 05:12:18 kernel: [600675.106731] [syscall](9) ravid 9: 0x0
Sep 27 05:12:18 kernel: [600675.110496] [syscall](9) ravid 10: 0x0
Sep 27 05:12:18 kernel: [600675.114285] [syscall](9) ravid 11: 0x0
Sep 27 05:12:18 kernel: [600675.123976] ----br_isolate_write_proc,start
```

3.15.2 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 VigorAP920RP Speed Test.

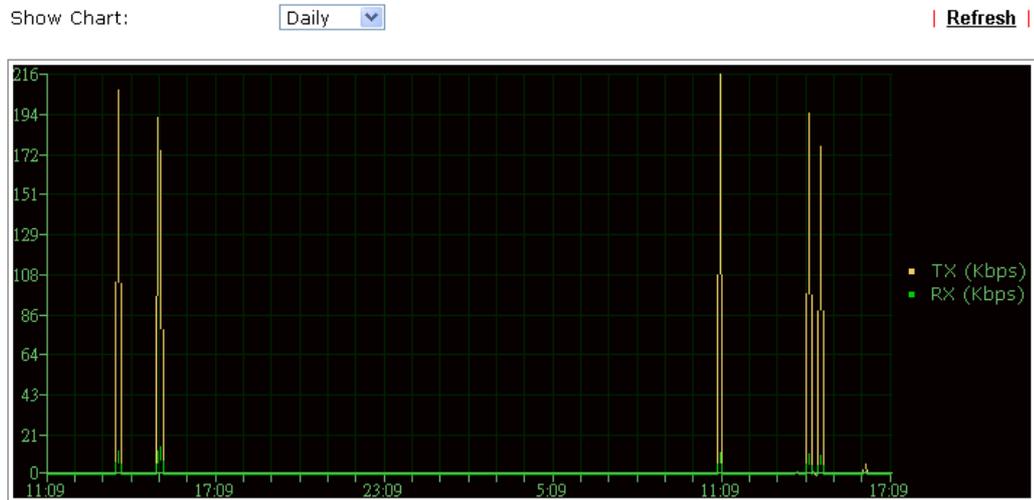
This test allows you to find out the best place for VigorAP920RP. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference.

[Start](#)

3.15.3 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, 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).

3.15.4 Where am I

Diagnostics >> Where am I ?

Where am I ?

Welcome to VigorAP920RP 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)

3.15.5 Data Flow Monitor

This page displays general information for the client connecting to VigorAP 910C.

Diagnostics >> Data Flow Monitor

Page: Auto-refresh

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	0 / 0	

Available parameters are explained as follows:

Item	Description
Auto-refresh	After checking this box, Vigor system will refresh such page periodically.
Refresh	Click this link to refresh this page immediately.
Index	Display the number of the data flow.
MAC Address	Display the MAC address of the monitored device.
Station	Display the IP address/host name of the wireless client.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
2.4G/5G	Display what wireless band (2.4G or 5G) used by the wireless client.
Action	DeAuth – Deauthenticate a wireless station.

3.15.6 WLAN (2.4GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (2.4GHz) 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	4842
Tx failures	0	Rx MIC errors	0
		Rx Decryption errors	0
		Rx errors	0

	SSID1 (ap920-BandSteering)	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	0	N/A	N/A	N/A

3.15.7 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	38910
Tx failures	0	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	0	N/A	N/A	N/A

3.15.8 Station Statistics

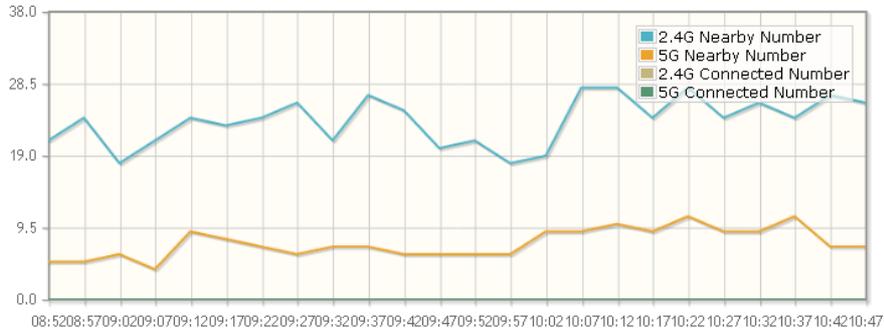
Such page is used for debug or for the user to observe network traffic and network quality.

Diagnostics >> Station Statistics

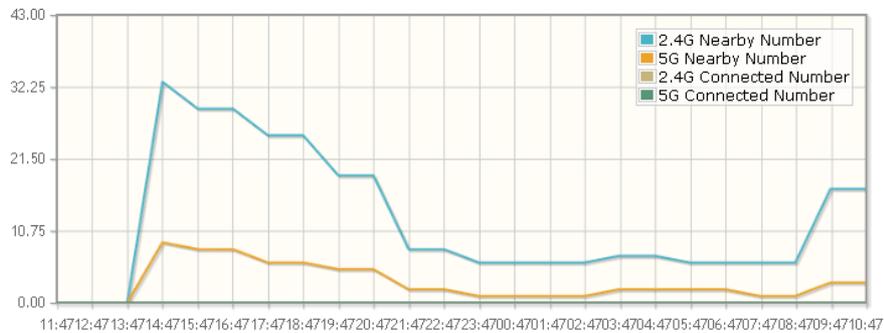
Show Chart: ▾

[Refresh](#) |

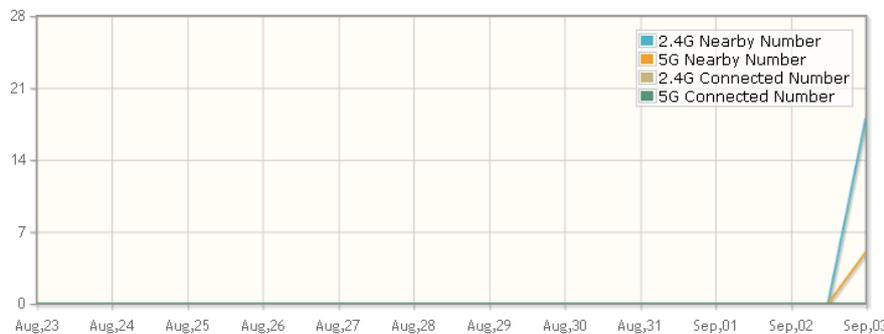
Hourly Nearby & Connected Number



Daily Nearby & Connected Number



Weekly Nearby & Connected Number



Note : Only browser supporting [HTML5](#) can display Station Statistics correctly.

Available parameters are explained as follows:

Item	Description
Show Chart	<p>Choose one of the items to display the statistics chart for wireless stations.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <p>Nearby & Connected Number ▾</p> <p>Nearby & Connected Number</p> <p>Visiting & Passing Number</p> <p>Visiting Time</p> </div> <p>Nearby & Connected Number – Choose it to have the statistics of the wireless stations which is nearby and</p>

connected to VigorAP.

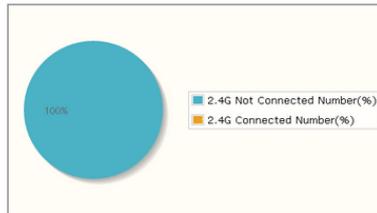
Visiting & Passing Number – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP.

Visiting Time - Choose it to have the statistics of the wireless stations which is visiting VigorAP.

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



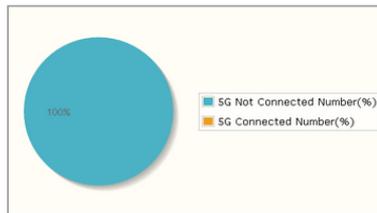
Peak of Connected Station Number:
Time: 14:58-13:58 Number: 0

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

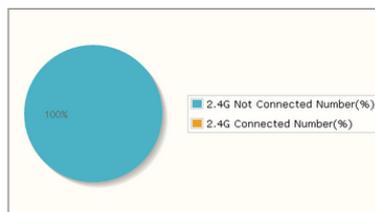
Off-peak of Nearby Station Number:
Time: 13:58 Number: 3

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



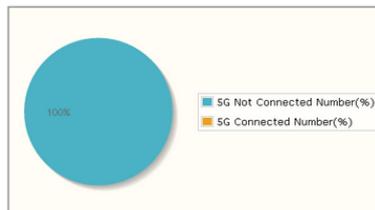
Peak of Connected Station Number:
Time: 2015-8-22(Sun)-2015-9-3(Thu) Number: 0

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

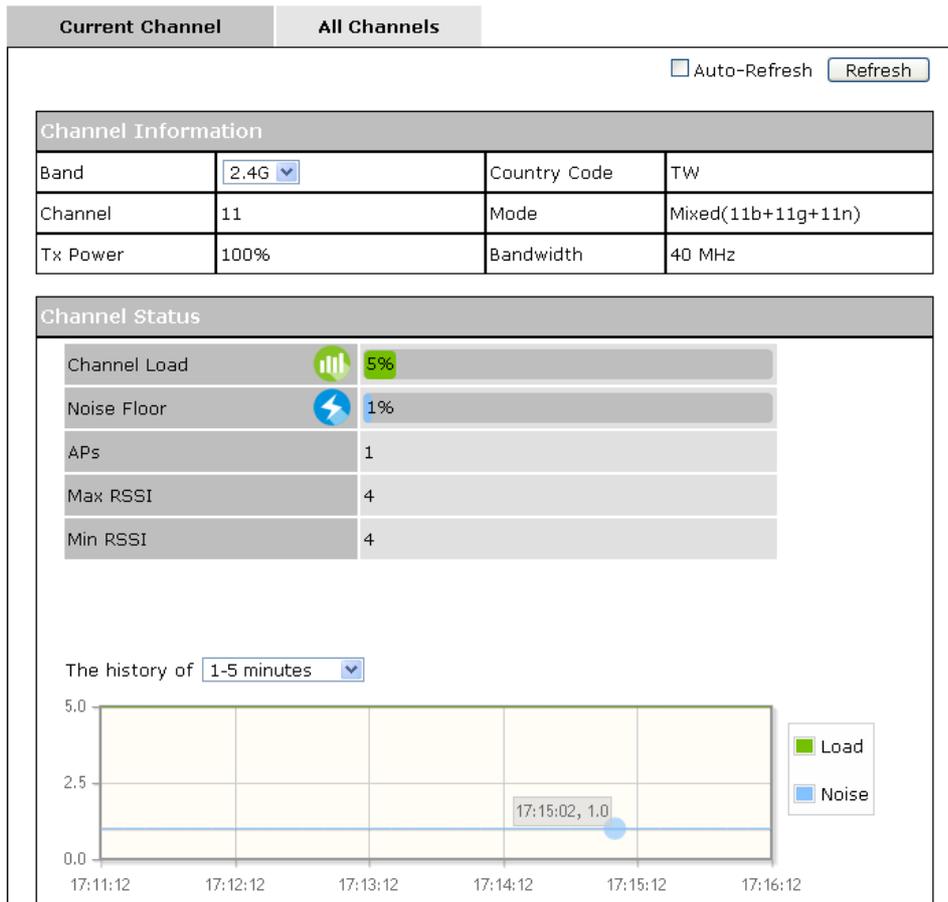
3.15.9 Interference Monitor

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	2.4G ▼		Refresh
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.

3.15.10 Station Airtime

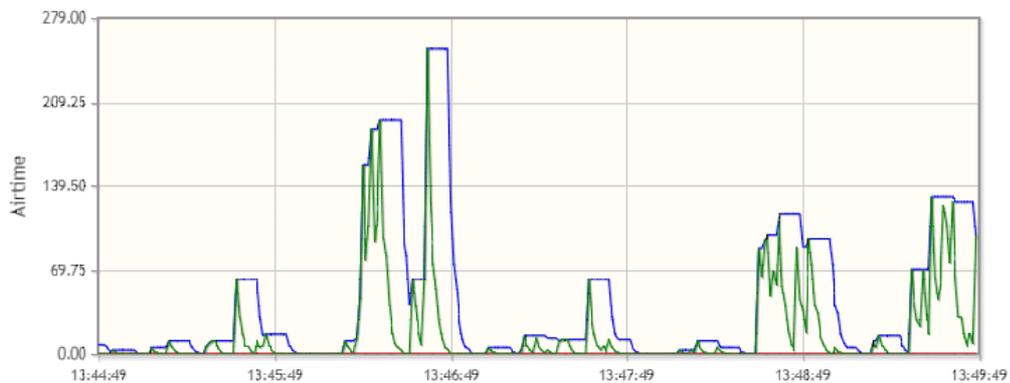
This page displays the operation status for 2.4GHz wireless stations within 30 minutes.

Diagnostics >> Station Airtime

Display: 2.4GHz ▼ Station 1-8 ▼ and the history of 1-5 minutes ▼ Airtime

| Refresh |

2.4GHz Tx Airtime



3.15.11 Station Traffic Graph

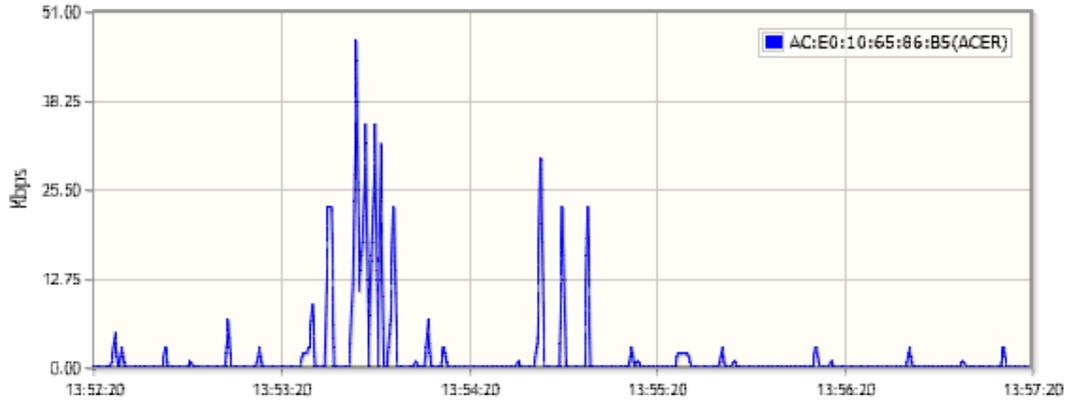
This page displays the data traffic (receiving/transmitting) status for 2.4GHz wireless stations within 30 minutes with a run chart.

Diagnostics >> Station Traffic Graph

Display: and the history of Throughput

[Refresh](#)

2.4GHz Tx Throughput



3.15.12 Station Link Speed

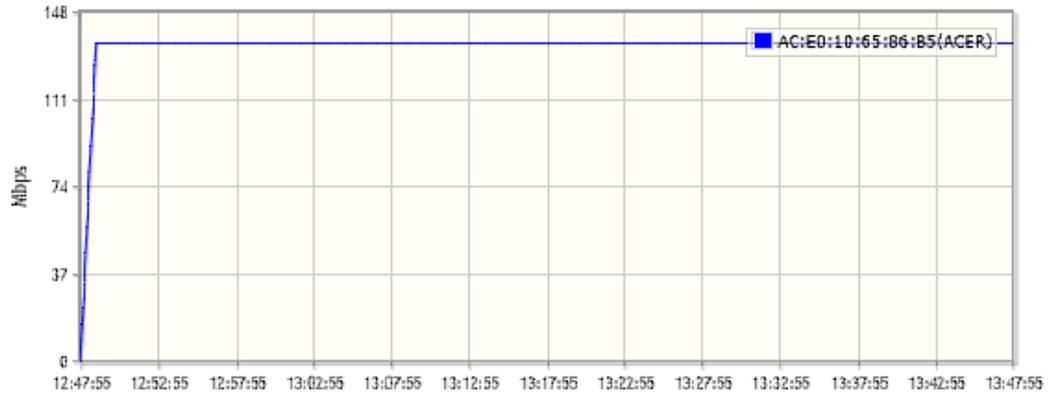
This page displays the link rate status for 2.4GHz/5GHz wireless stations within one hour with a run chart.

Diagnostics >> Station Link Speed

Display: Link rate

[Refresh](#)

2.4GHz Link Speed



3.16 Support Area

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

Support Area
FAQ/Application Note
Product Registration

All Rights Reserved

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 the modem from your computer.
- 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 Mounting the Access Point**” for details.
2. Power on the modem. Make sure the **ACT** LED and **2.4G/5G** LED are bright.
3. If not, it means that there is something wrong with the hardware status. Simply back to “**1.3 Mounting the Access Point**” 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

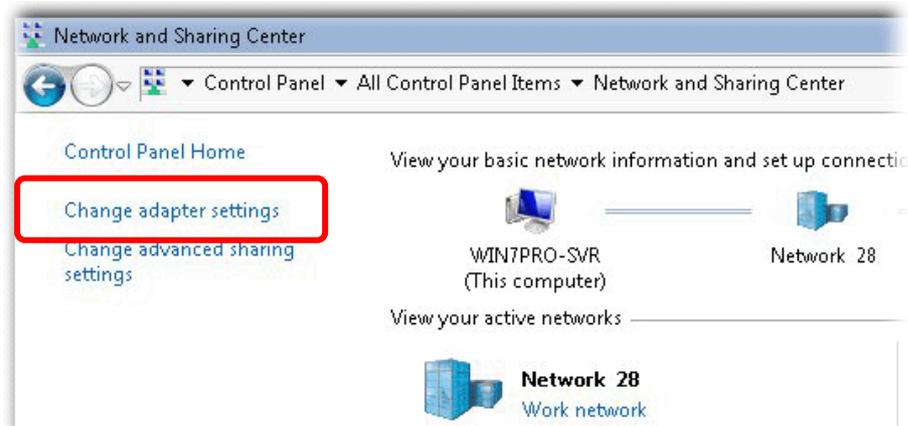


The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

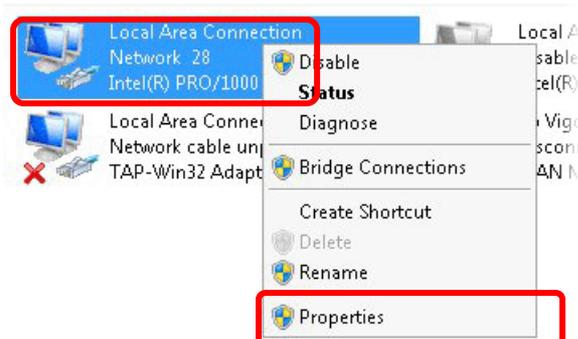
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



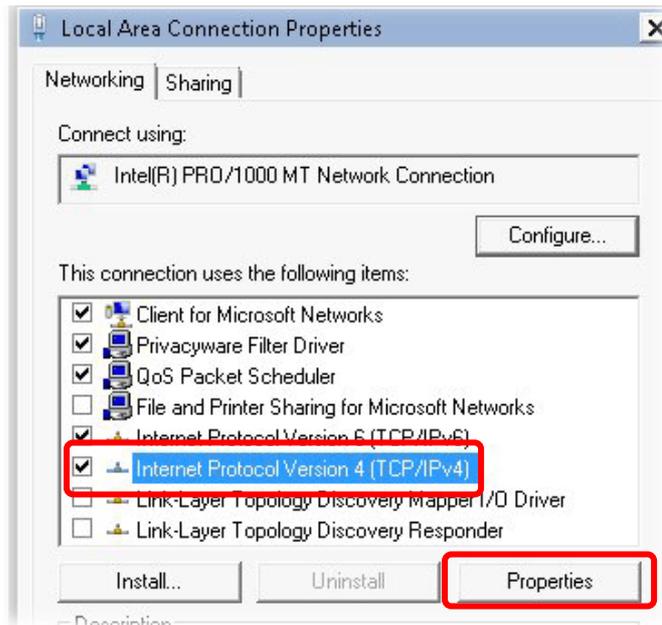
2. In the following window, click **Change adapter settings**.



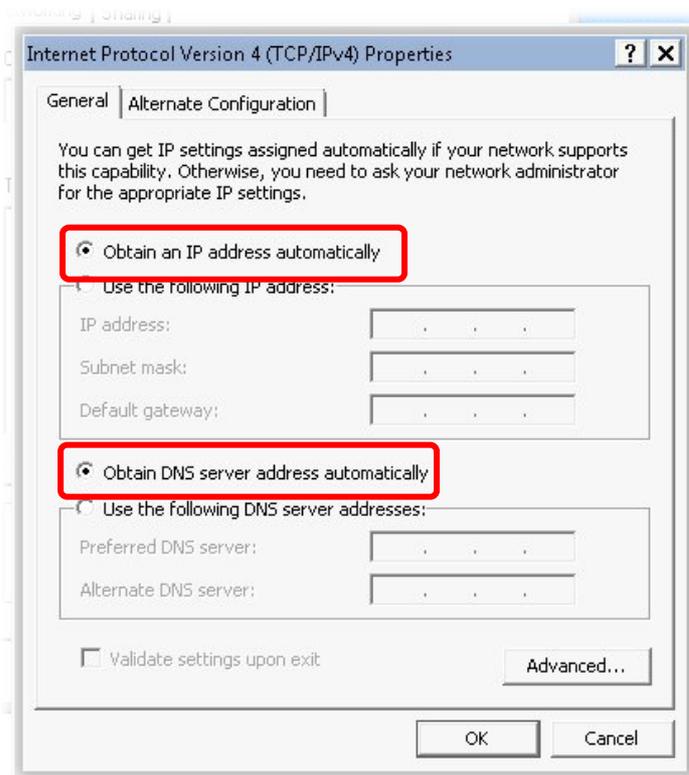
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

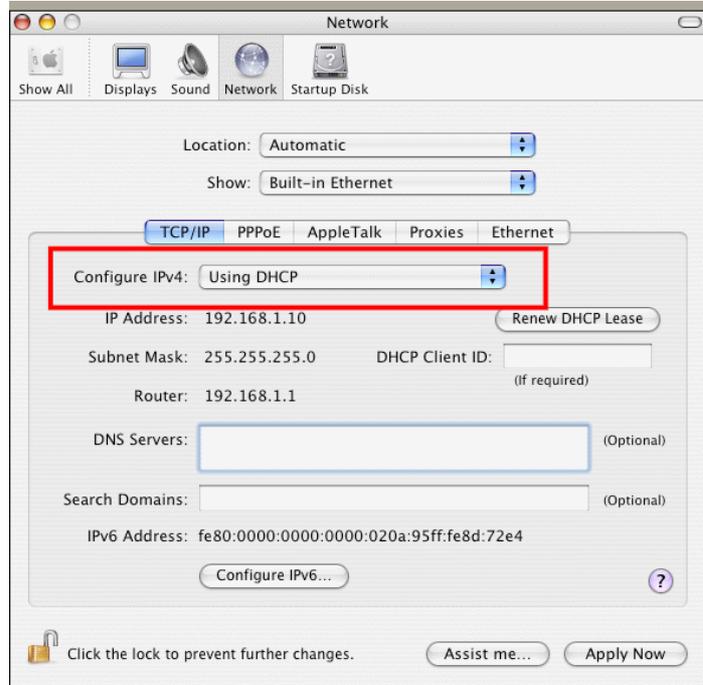


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



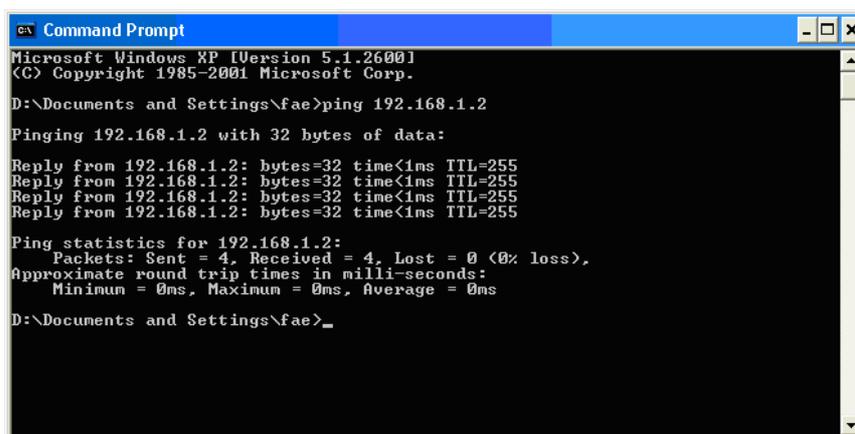
4.3 Pinging the Modem from Your Computer

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

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

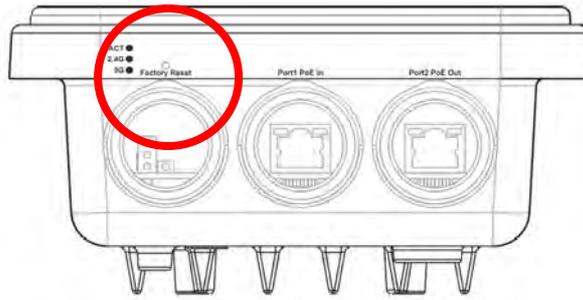
Do You want to reboot your router ?

Using current configuration
 Using factory default configuration

OK

Hardware Reset

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



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

4.5 Contacting DrayTek

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

Index

8

802.11n, 46

802.1x, 48

A

Access Control, 50, 82, 110, 137, 156

Action, 177

Activate MAC address filter, 82

Administrator Password, 189

Advanced Configuration, 31

Advanced Setting, 52, 72, 85, 112, 139, 158

AES, 23

Airtime Fairness, 58, 92, 120, 144, 166

Antenna, 52, 72, 85, 112

AP, 32

AP Bridge-Point to Multi-Point, 32

AP Bridge-Point to Multi-Point Mode, 70

AP Bridge-Point to Point, 20, 32, 70

AP Bridge-WDS, 21, 32

AP Bridge-WDS Mode, 76

AP Discovery, 20, 26, 54, 73, 86, 114, 141, 159

AP Management, 37

AP Mode, 44, 132

AP Operation Mode, 19, 25

APM Log, 38

Apple iOS Keep Alive, 178

Applications, 176

APSD Capable, 55, 142

Auth Mode, 51, 83

Authentication Client, 174

Authentication Type, 173

Auto Adjustment, 57, 91, 119, 144, 165

Auto Channel Filtered Out List, 53, 72, 85, 133, 139

Auto Provision, 37

AutoSelect, 19, 77, 115, 152, 161

B

Backup, 174

Backup the Configuration, 190

Band Steering, 63, 97, 125

Bandwidth Limit, 19

Bandwidth Management, 57, 91, 119, 143, 165

Black List, 39

Blocked MAC address filter, 82

Browser Time, 194

C

Central AP Management, 37

Certificate Management, 174

Changing Password, 17

Channel, 19, 22, 46, 71, 77, 105, 115, 133, 152, 161

Channel Width, 52, 72, 85, 112, 139, 158

Client IP, 174

Client PinCode, 51, 83

Client's MAC Address, 39, 171

Configuration Backup, 190

Connection Time, 60, 122, 146, 168

Connection Type, 116, 162

Country Code, 52, 72, 85, 112, 139, 158

D

Data Flow Monitor, 200

Daylight Saving, 194

Default Gateway, 117, 163

Detection, 183

Device Name, 116

DHCP Client, 33

DHCP server, 16

Diagnostics, 198

Download Limit, 57, 91, 119, 144, 165

E

EAP Type, 173

Encryp Type, 51, 83

End Time, 177

Event Code, 187

Extension Channel, 46, 71, 78, 105

F

Factory Default Setting, 214
Fast Roaming, 62, 96, 124, 148, 170
Firmware Upgrade, 197
Force Overload Disassociation, 39
Fragment Length, 52, 72, 85, 112, 139, 158
Function Support List, 38

G

General Setup, LAN, 33
Guest Wireless, 19

H

Hardware Reset, 214
Hide SSID, 46, 78, 106, 133, 152
HTMIX, 71
HTTP port, 196
HTTPS, 175
HTTPS port, 196

I

Interference Monitor, 205
IP Address, 33, 116, 162
Isolate LAN, 78, 106
Isolate Member, 46, 78, 106, 133, 152

K

Keep Alive Period, 188
Key Renewal Interval, 48, 80, 108, 135, 154
Key Size, 175
Key Type, 175

L

LAN, 33
LAN port, 36
Lease Time, 34
LED Indicators and Connectors, 2
LED Setup, 196
Limit Client, 45, 77, 105, 132, 151
Limit Client per SSID, 45, 77, 105, 133, 152
Load Balance, 39

M

MAC Address, 161

MAC Address Filter, 50
MAC Clone, 53, 73, 86, 113
Main Screen, 16, 31
Main SSID, 19
Management, 195, 196
Management VLAN, 33
Mobile Device Management, 183
Mode, 45, 47, 70, 77, 79, 105, 107, 133, 152, 153

N

NTP, 176
NTP Client, 194
NTP Server, 194
NTP synchronization, 194

O

Once, 177
Online Status, 30
Open/Shared, 23, 27, 115, 162
Operation Mode, 18, 32
Overload Management, 39

P

Pass Phrase, 48, 80, 108, 116, 135, 154, 162
Password, 17
Password Strength, 189
Periodic Inform Settings, 188
Phy Mode, 21
PHY Mode, 71, 78
PIN Code, 42
PMK Cache Period, 62, 96, 170
PoE Connection, 8, 9
Policy, 50, 82, 110, 137, 184
Port, 49, 136
Port Control, 36
Pre-Authentication, 62, 96, 148, 170
Primary DNS Server, 34
Primary IP Address, 188
PSK, 41
Push Button, 51, 83

Q

Quick Start Wizard, 18

R

RADIUS Server, 49, 81, 109, 136, 155, 173
RADIUS Setting, 173
Rate, 71, 78, 105
Reboot System, 197
Reconnection Time, 60, 122, 146, 168
Relay Agent, 34
Restore, 51, 174
Restore Configuration, 191
Roaming, 61, 95, 123, 147, 169
Router Name, 162
Routine, 177
RSSI, 61, 95, 123, 147, 169
RTS Threshold, 52, 72, 85, 112, 139, 158

S

Scan, 74
Schedule, 176
Secondary DNS Server, 34
Secondary IP Address, 188
Secret Key, 174
Security, 47, 71, 79, 107, 134, 153
Security Key, 19
Security Mode, 115, 161
Security Overview, 41
Security Settings, 47
Session Timeout, 49, 81, 109, 136, 155
Shared Secret, 49, 81, 109, 136, 155
Show Chart, 203
Software Reset, 214
Speed Test, 198
SSID, 78, 133, 152
SSL(HTTPS), 188
Start Date, 177
Start PBC, 42, 83, 111, 138, 157
Start PIN, 83, 111, 138, 157
Start Time, 177
Station Airtime, 206
Station Control, 19, 60, 94, 122, 146, 168
Station Link Speed, 208
Station List, 68, 102, 130, 149, 171
Station Statistics, 203
Station Traffic Graph, 207

Statistics, 185
Status of Settings, 40
STUN, 188
Subject Name, 175
Subnet Mask, 33, 117, 163
Support Area, 208
Syslog/Mail Alert, 192
System Log, 198
System Maintenance, 185
System Status, 186

T

Telnet Server, 196
Temperature High Alarm, 180
Temperature Low Alarm, 180
Temperature Sensor, 179, 180
Temperature Sensor Graph, 181
Time and Date, 194
Time Zone, 194
TKIP, 23, 41
Total Download Limit, 57, 91, 119, 144, 165
Total Upload Limit, 57, 91, 119, 144, 165
TR-069, 187
Traffic Graph, 199
traffic overload, 39
Triggering Client Number, 59, 93
Trouble Shooting, 209
Trust DHCP Server, 34

U

Universal Repeater, 22, 26, 33, 115, 161
Universal Repeater Mode, 104, 151
Upload Limit, 57, 91, 119, 143, 165
Users Profile, 173

V

VLAN ID, 33, 46, 78, 106, 133, 152

W

WDS AP Status, 75, 88
WEP, 23
WEP (Wired Equivalent Privacy), 41
White List, 39
Wi-Fi DOWN, 177

Wi-Fi UP, 177
Wired Connection, 4
Wireless Connection, 6
Wireless LAN (2.4GHz/5GHz), 41
Wireless LAN(2.4GHz), 32
Wireless LAN(5GHz), 33
WLAN (2.4GHz) Statistics, 201
WLAN (5GHz) Statistics, 202
WMM Configuration, 55, 89, 117, 142, 163
WPA (Wi-Fi Protected Access), 41
WPA Algorithms, 48, 80, 108, 135, 154
WPS, 51, 83, 111, 138, 157
WPS (Wi-Fi Protected Setup), 41