

VigorAP 918R Series 802.11ac Outdoor AP



V1.6

VigorAP 918R

802.11ac Outdoor AP

User's Guide

Version: 1.6

Firmware Version: V1.4.6

Date: July 5, 2023

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: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 7, 8, 10, 11 and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions	 Read the installation guide thoroughly before you set up the modem. The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself. Do not place the modem in a damp or humid place, e.g. a bathroom. The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius. Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources. Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards. Do not power off the device when saving configurations or firmware upgrades. It may damage the data in a flash. Please disconnect the Internet connection on the device before powering it off when a TR-069/ ACS server manages the device. 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 tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.
Be a Registered Owner	Web registration is preferred. You can register your Vigor router via https://myvigor.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. https://www.draytek.com

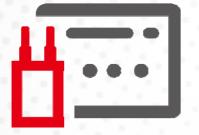
Table of Contents

	VI
I-1 Introduction	1
I-1-1 LED Indicators and Connectors	2
I-2 Mounting the Access Point	3
I-2-1 Antennas Installation	3
I-2-2 Connecting Ethernet Cable(s)	
I-2-3 Pole Mount Installation – for VigorAP 918RPD	
I-2-4 Pole Mount Installation – for VigorAP 918R	
I-2-5 Wall Mount Installation – for VigorAP 918R	
I-2-6 Grounding Access Point	
I-2-7 Powering Access Point	
I-3 Network IP Configuration	
I-3-1 Windows 10 IP Address Setup	
I-4 Accessing to Web User Interface	15
I-5 Changing Password	
I-6 Dashboard	
I-7 Quick Start Wizard	
I-7-1 Settings for Access Point	
I-7-2 Settings for Mesh Root	
I-7-3 Settings for Mesh Node	
I-7-4 Settings for Range Extender	
II Connectivity	
۔ II-1 Operation Mode	
II-2 General Concepts for Wireless LAN (2.4GHz/5GHz)	
II-3 Wireless LAN (2.4GHz/5GHz) Settings for AP Mode	
II-3-1 General Setup	
II-3-2 Security	
II-3-3 Access Control	
II-3-4 WPS	
II-3-5 Advanced Setting	
II-3-6 AP Discovery	
5	
II-3-7 WDS AP Status	
II-3-7 WDS AP Status II-3-8 Bandwidth Management	
II-3-8 Bandwidth Management	
II-3-8 Bandwidth Management II-3-9 Airtime Fairness	
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control	
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming	52 52 54 55 55 57
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control	52 52 54 55 57 57 59
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz))	52 52 54 55 57 57 59 64
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List	52 52 54 55 57 59 64 70
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode	52 52 54 55 57 59 64 70 72
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode II-4-1 Mesh Setup	52 52 54 55 55 57 59 64 70 72 77
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode II-4-1 Mesh Setup II-4-2 Mesh Status.	52 52 54 55 57 59 64 70 72 77 78
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode II-4 Mesh Settings for Mesh Mode II-4-1 Mesh Setup II-4-2 Mesh Status II-4-3 Mesh Discovery	52 52 54 55 55 57 59 64 70 72 77 77 78 79
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode II-4 Mesh Settings for Mesh Mode II-4-1 Mesh Setup II-4-2 Mesh Status II-4-3 Mesh Discovery II-4-4 Basic Configuration Sync	52 54 55 57 59 64 70 72 77 77 78 79 82
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode II-4 Mesh Settings for Mesh Mode II-4-1 Mesh Setup II-4-2 Mesh Status II-4-2 Mesh Status II-4-3 Mesh Discovery II-4-4 Basic Configuration Sync II-4-5 Advanced Config Sync	52 52 54 55 57 59 64 70 72 72 77 78 79 82 82 82
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode II-4 Mesh Settings for Mesh Mode II-4-1 Mesh Setup II-4-2 Mesh Status II-4-2 Mesh Status II-4-3 Mesh Discovery II-4-4 Basic Configuration Sync II-4-5 Advanced Config Sync II-4-6 Support List	52 52 54 55 57 59 64 70 72 77 77 78 79 82 82 83
II-3-8 Bandwidth Management II-3-9 Airtime Fairness II-3-10 Station Control II-3-11 Roaming II-3-12 Band Steering (for Wireless LAN (2.4GHz)) II-3-13 Station List II-4 Mesh Settings for Mesh Mode II-4 Mesh Settings for Mesh Mode II-4-1 Mesh Setup II-4-2 Mesh Status II-4-2 Mesh Status II-4-3 Mesh Discovery II-4-4 Basic Configuration Sync II-4-5 Advanced Config Sync II-4-6 Support List. II-4-7 Mesh Syslog	52 52 54 55 57 59 64 70 72 77 78 79 82 82 83 83

	II-6-1 General Setup	
	II-6-2 Hotspot Web Portal	
Chapter III M	lanagement	
III-1	System Maintenance	
	III-1-1 System Status	
	III-1-2 TR-069	
	III-1-3 Administrator Password	
	III-1-4 User Password	
	III-1-5 Configuration Backup	
	III-1-6 Syslog/Mail Alert	
	III-1-7 Time and Date	
	III-1-8 SNMP	
	III-1-9 Management	
	III-1-10 Reboot System	
	III-1-11 Firmware Upgrade	
III-2	e Central AP Management	
	III-2-1 General Setup	
	III-2-2 APM Log	
	III-2-3 Overload Management	
	III-2-4 Status of Settings	
III-3	Mobile Device Management	
	III-3-1 Station List	
	III-3-2 Station Statistics	
	III-3-3 Station Nearby	
	III-3-4 Policies	
	III-3-5 Station Control List	
Chapter IV Of	thers	
IV-1	RADIUS Setting	
	IV-1-1 RADIUS Server	128
	IV-1-2 Certificate Management	
1\/_2	2 Applications	
10 2		
	IV-2-1 Schedule	
	IV-2-2 Apple iOS Keep Alive	
	IV-2-3 Wi-Fi Auto On/Off	
	IV-2-4 Sensor	
IV-3	Objects Setting	
	IV-3-1 Device Object	
	IV-3-3 Device Group	
Chanter V Mo	obile APP, DrayTek Wireless	143
	Introduction of DrayTek Wireless	
	Create a New Network	
	Wizard - Mesh Root and Mesh Node	
V-4 L	Login	
		152
	V-4-1 Network	
	V-4-2 Connect	
	V-4-2 Connect V-4-2-1 Dashboard of the Device	
	V-4-2 Connect V-4-2-1 Dashboard of the Device V-4-2-2 Devices	
	V-4-2 Connect V-4-2-1 Dashboard of the Device V-4-2-2 Devices V-4-2-3 Clients / Groups	
	V-4-2 Connect V-4-2-1 Dashboard of the Device V-4-2-2 Devices	

/I-1 Diagnostics	160
VI-1-1 System Log	
VI-1-2 Speed Test	
VI-1-3 Traffic Graph	
VI-1-4 Alert Event	
VI-1-5 WLAN (2.4GHz) Statistics	
VI-1-6 WLAN (5GHz) Statistics	
VI-1-7 Interference Monitor	
VI-1-8 Support Area	
VI-2 Checking the Hardware Status	
VI-3 Checking the Network Connection Settings	
VI-3-1 For Windows	
VI-3-2 For Mac Os	
VI-4 Pinging the Device	171
VI-4-1 For Windows	
VI-4-2 For Mac Os (Terminal)	
VI-5 Backing to Factory Default Setting	
VI-5-1 Software Reset	
VI-5-2 Hardware Reset	
VI-6 Contacting DrayTek	175

Chapter I Installation

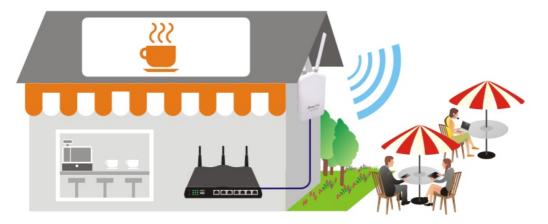


I-1 Introduction

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.

Thank you for purchasing VigorAP 918R series.

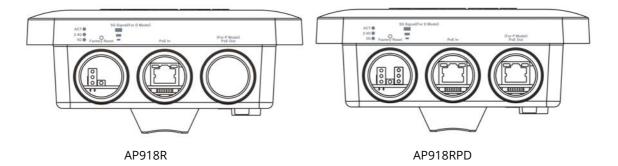
Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced users. Just follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!



VigorAP 918RPD 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.

I-1-1 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).		
5G Signal (For D Model)		The signal strength (excellent) > -50dBm.		
5G Signal (For D Model)		The signal strength (good) is between -66dBm ~ -51dBm.		
5G Signal (For D Model)		The signal strength (fair) is between -73dBm~ -67dBm.		
5G Signal (For D Model)	No signal or the signal strength is <-73dBm.			
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.			
PoE In	Connector for rece	iving power from another device.		
PoE Out (For D Model)	Connector for supplying power to another device.			

(i) Note:

For the sake of security, make the accessory kit away from children.

I-2 Mounting the Access Point

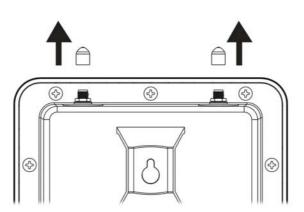
The VigorAP can be pole mounted depending on the installation environment. This section will guide you through installing the VigorAP.

(i) Note:

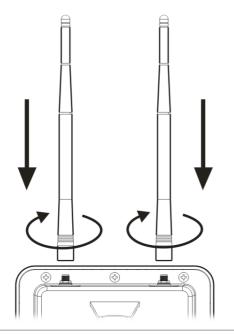
For the sake of personal safety, only trained and qualified personnel should install this device.

I-2-1 Antennas Installation

1. Remove the protective cap.



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



(i) Warning:

Do not open the top cover of the device.

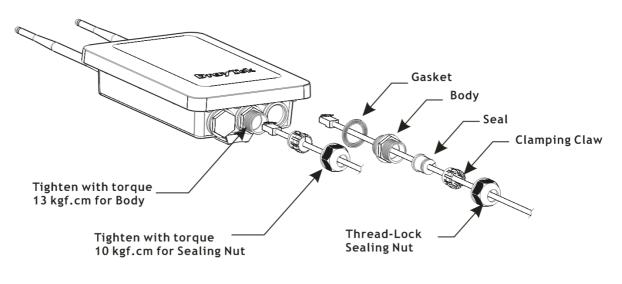
Installation during thunderstorms could be dangerous.

I-2-2 Connecting Ethernet Cable(s)

Refer to the following steps to attach the Ethernet cable and waterproof head. (Take VigorAP 918RPD 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.

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.

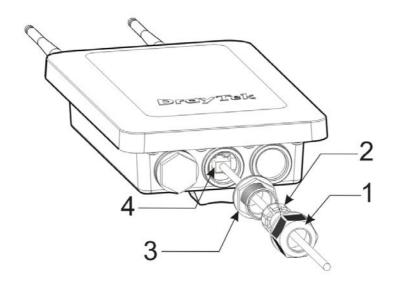
4. Use an adjustable wrench and tighten the thread-lock sealing nut with torque 10 kgf-cm.

(i) Note:

Do not pull the cable backwards; the force might break the plug.

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.



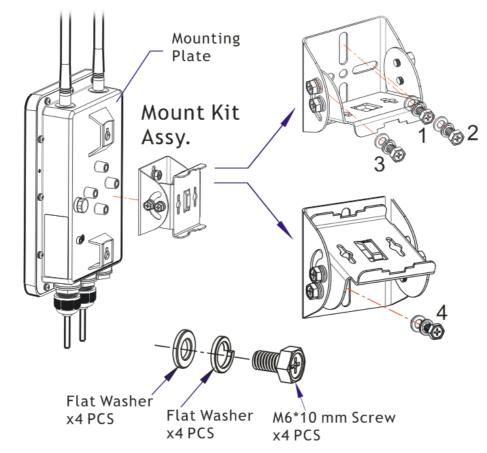
5. To reattach the cable, follow the above steps in reverse.

(i) Note:

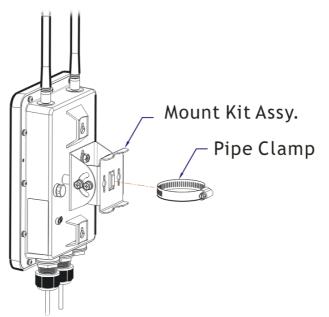
The diameter for the Ethernet cable shall be limited between 4.3mm to 5.9mm.

I-2-3 Pole Mount Installation – for VigorAP 918RPD

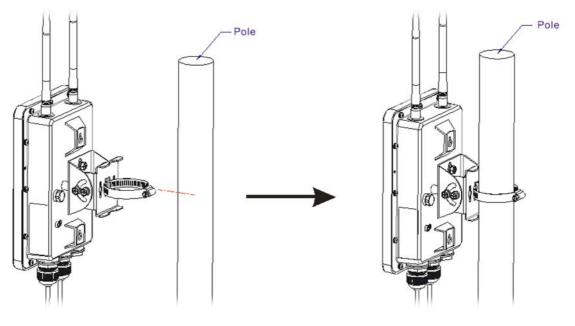
- 1. Find a suitable location for installing the access point.
- 2. Select a mounting point on a pole.
- 3. Attach the mount kit assembly to the mounting plate by locking four screws with the torque of 10 kgf-cm.



4. Insert the pipe clamp into the mount kit assembly.



5. Press the pipe clamp to open it for clamping the pole.

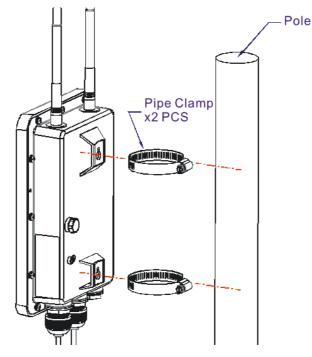


(i) Note:

The diameter for a pole shall be limited between 35mm to 60mm.

I-2-4 Pole Mount Installation – for VigorAP 918R

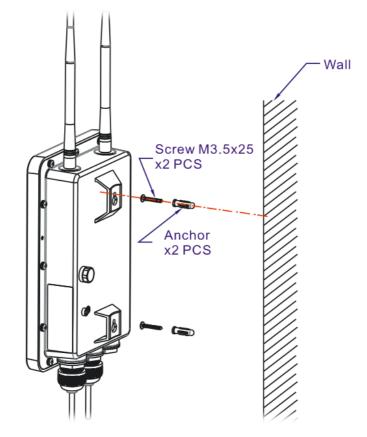
- 1. Find a suitable location for installing the access point.
- 2. Select a mounting point on a pole.
- 3. Insert the pipe clamp on the access point. Press the pipe clamp to open it for clamping the pole.



I-2-5 Wall Mount Installation – for VigorAP 918R

Refer to the following steps to mount the access point on the wall.

- 1. Find a suitable location for installing the access point.
- 2. Insert two pieces of anchor to the wall.
- 3. Lock the screws on the anchors.
- 4. Hang the access point on the anchors.



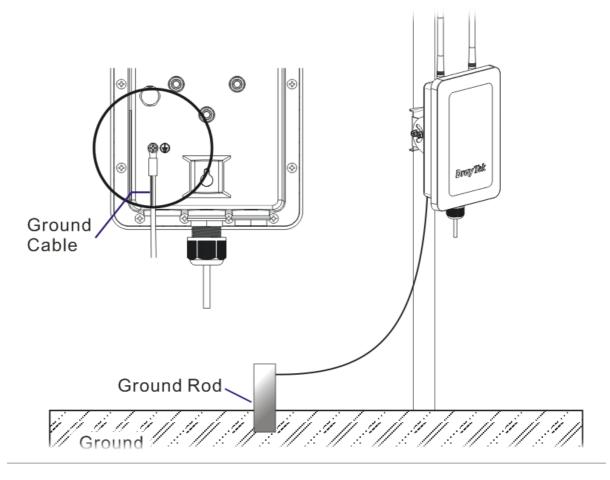
I-2-6 Grounding Access Point

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.



(i) Note:

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

I-2-7 Powering Access Point

VigorAP 918R/RPD can be powered via the PoE input from an in-line power injector or a suitably powered switch port.

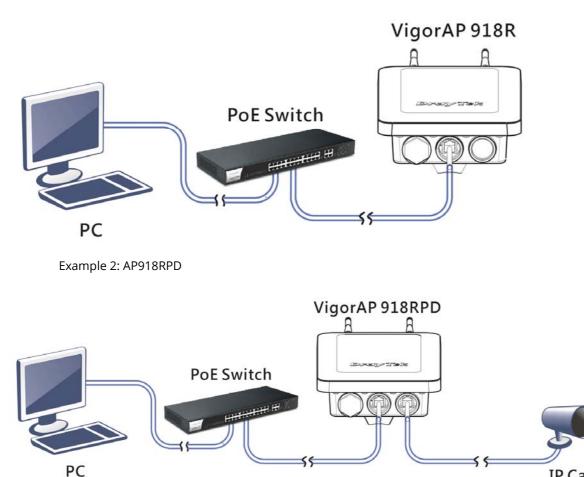


Before powering VigorAP, you should:

- 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 lighting 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 918R and VigorAP 918RPD.

Example 1: AP918R



IP Cam

I-3 Network IP Configuration

After the network connection is built, the next step you should do is setup VigorAP 1000C with proper network parameters, so it can work properly in your network environment.

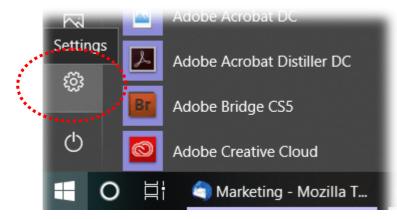
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address in the same subnet as this AP. If it's not connected to the same DHCP Server with the AP or you're unsure, please follow the following instructions to configure your computer to use the static IP address in the same subnet as default IP address of this AP.

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

Windows 10 - please go to section I-3-1

I-3-1 Windows 10 IP Address Setup

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



Double-click Network & Internet.



Next, click Change adapter options.

Settings		- 0
	Windows Settings	
	Find a setting D	
← Settings	1	- 0
⇔ Home	Status	
Find a setting	Network status	Do you have a question? Get help
Network & Internet	La Di Alss-1 Public retwork	Make Windows better Give us feedback
P Ethernet	You're connected to the Internet If you have a limited data plan, you can make this network a metered connection or change other properties.	
∞ VPN ③ Data usage	Change connection properties Show any technology is a second seco	
Proxy	Change your network settings	
1	Change adapter options View network adapters and change connection settings. Suming options for the networks that you want to share. Network troubleshooter	



Settings			
		Windows Settings	
		Find a setting	
- Settings			
		Status	
Find a setting	P	Network status	Do you have a question? Get help
Network & Internet			Make Windows better
😨 Ethernet		Public network	Give us feedback
🕾 Dial-up	Network Connections	Control Panel > All Control Panel (and) Network Contentings	×
% VPN	Organise •	B = 0	0
🕑 Data usage	2nd IB Netwo Resided	R Readive unphagoped Readive Unphagoped Rea	
Proxy	L ~	the second s	
		114444471	

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

📱 Local Area Connection Properties
Networking Sharing
Connect using:
Realtek RTL8139/810x Family Fast Ethernet NIC
Configure
This connection uses the following items:
🗹 📑 Client for Microsoft Networks
🗹 📮 QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IP♥6)
Internet Protocol Version 4 (TCP/IPv4)
Link Laver Topology Discovery Meoper I/O Driver
Link-Layer Topology Discovery Responder
Install Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK Cancel

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

IP address: 192.168.1.9

Subnet Mask: 255.255.255.0

Internet Protocol Version 4 (TCP/IPv4) Properties						
General						
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
Obtain an IP address automatica	ally					
• Use the following IP address: -						
IP address:	192.168.1.9					
Subnet mask:	255 . 255 . 255 . 0					
Default gateway:	192.168.1.1					
Obtain DNS server address automatically						
• Use the following DNS server ad	dresses:					
Preferred DNS server:	168 . 95 1 . 1					
Alternate DNS server:	• •					
Vaļidate settings upon exit	Advanced					
	OK Cancel					

I-4 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 918R 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. Pease type "admin/admin" on Username/Password and click **OK**.

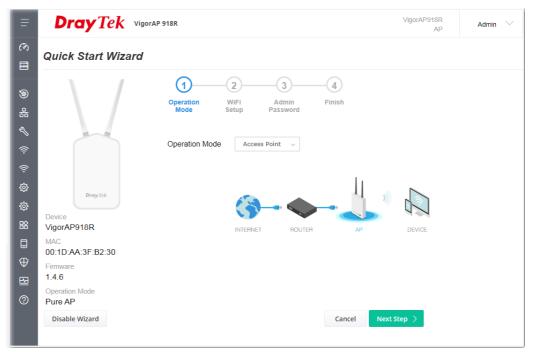
User Name admin Password VigorAP918R	
---	--

(i) Note:

You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as **the IP address of VigorAP 918R.**

- If there is no DHCP server on the network, then VigorAP 918R will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 918R will receive it's IP address via the DHCP server.
- If you connect to VigorAP by wireless LAN, you could try to access the web user interface through http://vigorap.com.

3. For the first time accessing VigorAP, the **Quick Start Wizard** for configuring wireless settings will appear as follows. Refer to *Section I-7 Quick Start Wizard for detailed information*.



4. If VigorAP has been configured previously, the Dashboard of VigorAP will appear as follows:

=	Dray Tek VigorAP 918R		VigorAP918R AP Adr	min 🗸
Image: Constraint of the start with the start withe start with the start with the start with th	0 2.4 GHz 0/128 Clients 5 GHz 0/128	CHANNEL LOAD • Ch 5 Light, 9% • Ch 44 Light, 4%	DEVICE OVERVIEW Device Name VigorAP918R IP Address 192.168.1.14 (via DHCP) Firmware 1.4.6 Uptime 1d 02:22:39 Gateway 192.168.1.1	1
 デ Wireless LAN (2.4GHz) デ Wireless LAN (5GHz) な RADIUS Setting な Objects Setting 路 Applications 	RADIO THROUGHPUT 2.4 GHz & 0 bps & 0 bps 5 GHz & 0 bps & 0 bps	PORT STATUS POE IN ACT • 2.40 • 8 • • RESET PI	MAC 00:1D:AA:3F:B2:30 Build Date g1556_2991148da Fri, 24 Feb 2023 14:32:21 ACS Server	5%
☐ Mobile Device Management > ⊕ System Maintenance > ⊡ Diagnostics > ⑦ Support >	RECENT ACTIVITES Last 24 hours 2.4 GHz • Throughput • Clients 10- 10- 10- 5PM 8PM 11PM 2AM 5 5 GHz	1.0 0.5 5 AM 8AM 11AM 2PM 0	WIRELESS OVERVIEW 2.4GHz	60%

5. The web page can be logged out by clicking Log Out on the top right of the web page. Or, logout the web user interface according to the chosen condition. The default setting is Auto Logout, which means the web configuration system will logout after 5 minutes without any operation. Change the setting of auto logout if you want.

	Auto logout	~
	Auto logout	~
	off	
	1 min	
JorAP918R Admin V	3 min	
off ~	5 min	
 A Set Password → Log Out 	10 min	

(i) Note:

If you fail to access the web configuration, please go to the section "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.

I-5 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	admin
Old Password	•••••
New Password	•••••
Confirm Password	•••••
Password Strength:	Weak Medium Strong
Strong password requirements: 1. Have at least one upper-case letter ar 2. Including non-alphanumeric character	
Note : Authorization Account can contain	only a-z A-Z 0-9 , ~ ` ! @ \$ % ^ * () + = {} [] ; < > .
Authorization Password can contain ; < > . ? /	n only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & * () + = {} [] \
	ок Cancel

- 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.

I-6 Dashboard

Dashboard shows system status including the number of client connected, throughput, gateway, physical connection status, radio (2.4GHz / 5GHz) status, backhaul network, recent activities, wireless network usage, and so on.

VigorAP918R Dray Tek VigorAP 918R Admin AP WIRELESS CLIENTS PER RADIO CHANNEL LOAD DEVICE OVERVIEW Quick Start Wizard 0 Device Name VigorAP918R IP Address 192,168,1,14 • 2.4 GHz 0/128 • Ch 5 Light, 9% 0 Operation Mode Light (via DHCP) o 5 GHz 0/128 Ch 44 Light, 4% Clients Firmware 1.4.6 몲 LAN Uptime 1d 02:22:39 🔦 Central AP Management Gateway 192.168.1.1 . 察 Wireless LAN (2.4GHz) MAC 00:1D:AA:3F:B2:30 RADIO THROUGHPUT PORT STATUS Build Date g1556_2991f48da Fri, 24 Feb 2023 14:32:21 POE IN 1 0 bps 중 RADIUS Setting 2.4 GHz 🕁 🛛 bps ACS Server . ACT 0 2.4G 0 5G 0 0 Objects Setting 1 0 bps 5 GHz 🚽 0 bps SYSTEM RESOURCE R Applications 5% CPU Usage Mobile Device Managem RECENT ACTIVITIES Last 24 hours ~ Memory Usage 60% System Maintenance Diagnostics 2.4 GHz
Throughput
Clients WIRELESS OVERVIEW ② Support 2.4GHz Clients (sdq) Radio Enable 0 MAC 00:1D:AA:3F:B2:30 0— 5PM 8PM 11PM 5AM SSID(1) DrayTek-3FB230 5GHz 5 GHz

Click **Dashboard** from the main menu on the left side of the main page.

I-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.

=	Dray Tek Vigorap 918R	VigorAP918R AP	Admin 💛
(?) 	Quick Start Wizard		
) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	0 2 3 4 Operation WiFi Admin Finish Mode Setup Password		
en (ir (ir	Operation Mode Access Point ~		
\$\$ \$\$	Device		
	VigorAP918R INTERNET ROUTER AP MAC 00:1D:AA:3F:B2:30	DEVICE	
⊕ ⊡ ©	Firmware 1.4.6 Operation Mode		
	Pure AP Disable Wizard Cancel Next	Step >	

Available operation mode includes:

- Access Point
- Mesh Root
- Mesh Node
- Range Extender

In this page, the advanced settings pages will vary according to the operation mode specified.

I-7-1 Settings for Access Point

1. Choose Access Point as the operation mode and click Next Step.

	Dray Tek VigorAP 918R	VigorAP918R AP	Admin 💛
<i>ල</i> ා ම	Quick Start Wizard		
ه ا	0 2 3 4 Operation WiFi Admin Finish Mode Setup Password Finish		
L (1: (1:	Operation Mode Access Point ~		
袋 袋 路	Device VigorAP918R INTERNET ROUTER AP	DEVICE	
□ ⊕ 2 2	MAC 00:1D:AA:3F:B2:30 Firmware 1.4.6 Operation Mode Pure AP		
	Disable Wizard Cancel Next	Step >	

2. In the following page, configure the settings for wireless LAN (for both 2.4GHz and 5GHz) and click **Next Step**.

=	Dray Tek	VigorAP 918R		VigorAP918R AP	Admin 💛
(7) 111	Quick Start Wizard				
 ○ H ◆ ○ ◇ ◇ ◇ ◇ ▲ ● H ○ ○ H ◆ □ A ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇ ◇	Device VigorAP918R MAC 00:1D:AA:3F:B2:30 Firmware 1.4.6 Operation Mode Pure AP	Operation Mode WiFi Setup Your AP is under default co WiFi Name:: WiFi Password:: Image: Image: <th>p Password infig. Please setup first. DrayTek-3FB230 int</th> <th> Next Step ></th> <th></th>	p Password infig. Please setup first. DrayTek-3FB230 int	 Next Step >	

Available settings are explained as follows:

Item Description				
WiFi Name	Set a name for VigorAP 918R to be identified.			

WiFi Password	Type 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
Enable 2nd	Check the box to enable the second wireless setting.
Wireless	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.
	2nd WiFi Name - Set a name for VigorAP 918R which can be identified and connected by wireless guest.
	2nd WiFi Password - Set 8~63 ASCII characters which can be used for logging into VigorAP 918R 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.

3. Change the default password for such device with new value. Then click **Next Step**.

Ξ	Dray Tek VigorA	P 918R				VigorAP918R AP	Admin 💛
(7) 10	Quick Start Wizard						
》 品	\setminus /	Operation Mode	2 WiFi Setup	3 Admin Password			
Ľ		Your AP is under	default c	onfig. Please setu	p first.		
((ı.		Admin Passwor		•••••			
ې چې	DrayTek	Confirm Passw	ord:	•••••			
ŵ 路	Device VigorAP918R						
	MAC 00:1D:AA:3F:B2:30						
\oplus	Firmware 1.4.6						
2 2 2 2 2	Deration Mode Pure AP						
	< Back				Cancel	Next Step >	

Available settings are explained as follows:

ltem	Description
Admin Password	Enter a new password.

Confirm	Enter the new password again for confirmation.
Password	

4. A summary of settings configuration will be shown on screen. Click **Finish**.

F	Dray Tek VigorAP	918R				VigorAP918R AP	Admin 💛
(?) []]	Quick Start Wizard						
) الله الله (Mode S	ietup Pa	3 Admin assword	Finish		
88 43 43 ~)) ~))	DrayTek Device VigorAP918R	Operation Mode WiFi Name 2nd WiFi Name Bandwidth Limit Station Control	Pure AP DrayTek-3 Disabled Disabled Disabled	FB230			
	MAC 00:1D:AA:3F:B2:30 Firmware 1.4.6 Operation Mode Pure AP Sack				Cancel	Finish	

I-7-2 Settings for Mesh Root

1. Choose **Mesh Root** as the operation mode and click **Next Step**.

I	=	Dray Tek Vigor AP S	18R	VigorAP918R AP	Admin 💛
	ල 1	Quick Start Wizard			
	 ○ 田 ⊕ □ 8 ☆ ☆ ☆ ☆ 品 □ ⊕ ⊡ 	Quick Start Wizard	$\mathbf{\circ}$	4 inish	
	Ŭ	Disable Wizard		Cancel Next Step >	

2. Configure the settings for wireless LAN (for both 2.4GHz and 5GHz) and click **Next Step**.

	Dray Tek	VigorAP 918R	VigorAP918R AP	Admin 💛
(?) 	Quick Start Wizard			
) 용 생		Operation Mode WiFi Setup Admin Password Finish Your AP is under default config. Please setup first.		
88 49 4) 4)	DrayTek Device VigorAP918R	WiFi Name:: DrayTek-3FB230 WiFi Password::		
□ ⊕	MAC 00:1D:AA:3F:B2:30 Firmware 1.4.6	Enable Bandwidth Limit Enable Station Control Note: : The WiFi settings will apply to all Wireless bands.		
	Operation Mode Pure AP Back	Cancel	Next Step >	

Available settings are explained as follows:

Item Description					
WiFi Name	Set a name for VigorAP 918R to be identified.				
WiFi Password	Type 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").				

Enable 2nd WiFi	Check the box to enable the second wireless setting.			
	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.			
	2nd WiFi Name - Set a name for VigorAP 918R which can be identified and connected by wireless guest.			
	2nd WiFi Password - Set 8~63 ASCII characters or 8~63 ASCII characters which can be used for logging into VigorAP 918R 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.			

3. Change the default password for such device with new value. Then click **Next Step**.

	Dray Tek	VigorAP 918R				VigorAP918R AP	Admin 💛
<i>(</i> ୦) ଜ୍ଞ	Quick Start Wiza	rd					
③ 品	\setminus /	Operation Mode	WiFi Setup	Admin Password			
س می (ز.		Your AP is u	nder default c	onfig. Please setu	p first.		
((i·		Admin Pas Confirm Pa		•••••			
\$} \$}	Dray Tek						
器	VigorAP918R MAC						
₽	00:1D:AA:3F:B2:30 Firmware						
5	1.4.6 Operation Mode						
0	Pure AP				Cancel	Next Step 〉	
	Dack				Cancel	Next step /	

Available settings are explained as follows:

ltem	Description
Admin Password	Enter a new password.
Confirm	Enter the new password again for confirmation.

Password

4. A summary of settings configuration will be shown on screen. Click **Finish**.

= DrayTek Vigor	AP 918R			VigorAP918R AP	Admin 💛
ØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØ<					
Image: Second state st	WiFi Name 2nd WiFi Name Bandwidth Limit	p Password	Finish button apply changes.	Finish	

5. After clicking **Finish**, the following web page appears. VigorAP will search for mesh node around the network.

Quick Start Wizard	
	Image: Constraint of the setup Image: Constraint of the setup Restart Wireless Mesh Node Finish Setup additional VigorAPs to Mesh network?
	Please power up and wait for us to find it.
DrayTek	
Device VigorAP918R	
MAC 00:1D:AA:3F:B2:30 Firmware	
1.4.6	
Operation Mode Mesh Root	
< Back	Cancel Apply

6. Available VigorAP devices will be shown on the screen. Select the device (as a mesh node) for grouping under such mesh group and enter a device name for identification.

Quick Start Wizard							
	Restart Wireless Mesh Node Setup Setup additional VigorAPs to M Please power up and wait for up						
Device VigorAP918R MAC 00:1D:AA:3F:B2:30 Firmware	Select Model	MAC 00:1D:AA:80:FE:B8	Device Nan	ne			
1.4.6 Operation Mode Mesh Root		Sending settings to mesh no	Cancel	Search Apply			

7. Click **Apply** and wait for a while.

Quick Start Wizard				
\ /	1—	2	3	
	Restart Wireless	Mesh Node Setup	Finish	
	Setup addi	tional VigorAPs to	Mesh network?	
	Please pov	ver up and wait fo	r us to find it.	
DrayTek				Device Name
Device VigorAP918R				VigorAP1060C_B8
MAC 00:1D:AA:3F:B2:30			$\sum_{i=1}^{n} \sum_{j=1}^{n}$	
Firmware 1.4.6				
Operation Mode Mesh Root				h node
< Back				Cancel Apply

8. Later, a summary page of mesh root with mesh node will be shown on the screen.

\setminus /	1 Restart Mesh N Wireless Setu			
	Setup 1 Mesh Root a	nd 1 Mesh Node completed.		
Dray Tek	ROOT	VigorAP918R VigorAP918R		2 1 Node Offline
Device VigorAP918R MAC		VigorAP1060C_B8 VigorAP1060C	-55dbm ╤	00:1D:AA:68:D6:68
00:1D:AA:3F:B2:30 Firmware 1.4.6				
Operation Mode Mesh Root			Cancel	nish
< Back				

I-7-3 Settings for Mesh Node

1. Choose **Mesh Node** as the operation mode and click **Next Step**.

Ξ	Dray Tek VigorAP 918R	VigorAP918R AP	Admin 💛
<i>(</i> ୬ ଟ୍ର	Quick Start Wizard		
) 略 《	0 2 3 4 Operation WiFi Admin Finish Mode Setup Password		
(í· (í·	Operation Mode Mesh Node ~	L.	
令 令 88	Device VigorAP918R NUTERNET ROUTER MESH ROOT	MESH NODE	
∎ ⊕	MAC 00:1D:AA:3F:B2:30 Firmware		
23 (?)	1.4.6 Operation Mode Pure AP		
	Disable Wizard Cancel Ne	xt Step >	

2. A summary of settings configuration will be shown on screen. Click **Finish**.

=	Dray Tek VigorAP 918R	,	VigorAP918R AP	Admin 💛
(?) 	Quick Start Wizard			
四 ④ 品 《 《 令 令 谷 品 印 田	Device VigorAP918R MAC 00:1D:AA:3F:B2:30 Firmware 1.4.6	PP to search this		
0	Operation Mode Pure AP < Back	Cancel Fi	inish	

I-7-4 Settings for Range Extender

1. Choose **Range Extender** as the operation mode and click **Next Step**.

Ŧ	Dray Tek VigorAP 918R	VigorAP918R AP	Admin 💛
<i>ල</i> ා ම	Quick Start Wizard		
③ 昭 ⊕ 〓 殺 췋 令 う ⊘ 昭 ⊕ 団 ⊙	Image: Constraint of the second se	Step >	

2. Configure the settings for wireless LAN (for both 2.4GHz and 5GHz) and click **Next Step**.

Ξ	Dray Tek	VigorAP 918R		VigorAP918R AP	Admin 💛
(N)	Quick Start Wizard				
) الله الله الله الله الله الله الله الله		Operation Mode Setup Pass Your AP is under default config. Pl	nin Range Finish vord Extender		
((ı- (Tek-3FB230		
49 49 	Dray Tek Device	C Enable 2nd WiFi 2nd WiFi Name:			
	VigorAP918R MAC	2nd WiFi Password::			
\oplus	00:1D:AA:3F:B2:30 Firmware	Enable Station Control			
1 (?)	1.4.6 Operation Mode Pure AP	Note: : The WiFi settings will appl	y to all Wireless bands.		
	< Back		Cancel	Next Step >	

ltem	Description
WiFi Name	Set a name for VigorAP 918R to be identified.
WiFi Password	Type 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal

	digits leading by 0x, such as "0x321253abcde").
Enable 2nd WiFi	Check the box to enable the second wireless setting.
	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.
	2nd WiFi Name - Set a name for VigorAP 918R which can be identified and connected by wireless guest.
	2nd WiFi Password - Set 8~63 ASCII characters or 8~63 ASCII characters which can be used for logging into VigorAP 918R 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.

3. Change the default password for such device with new value. Then click **Next Step**.

	Dray Tek VigorAP 918R	VigorAP918R AP	Admin 💛
(ମ) ଅଧି	Quick Start Wizard		
)) 品	0 Operation WiFi Admin Range Finish Mode Setup Password Extender Finish		
L (i:	Your AP is under default config. Please setup first.		
(به چې	Admin Password: ••••• Confirm Password: •••••		
錼	Device		
	VigorAP918R MAC		
Ð	00:1D:AA:3F:B2:30 Firmware 1.4.6		
2 (?)	Operation Mode Pure AP		
	< Back Cancel	Next Step 🗦	

ltem	Description
Admin Password	Enter a new password.

Confirm	Enter the new password again for confirmation.
Password	

4. In the following page, click **Search** to find out neighboring access point. When all the available access points appear on the page, click the one you want to connect. Corresponding settings (e.g., SSID, security key) of the selected device will be shown below. Then click **Next Step**.

()		3 4 Admin Range ssword Extender	-5 Finish			
		GHz WLAN				
	SSID	BSSID	RSSI	Channel	Encryption	Authentication
	0	12:1D:AA:52:E5:30	87%(-66dbm)	11	AES	WPA2 Personal
DrayTek	jerry-ap912c	14:49:BC:42:AF:8A	8%(-89dbm)	11	AES	WPA3/WPA2 Personal
	O DrayTek-162CA0	00:1D:AA:91:2C:15	94%(-60dbm)	11	AES	WPA3/WPA2 Personal
vice	O nancy_v2765	02:50:7F:C1:EC:87	94%(-60dbm)	11	AES	WPA3/WPA2 Personal
gorAP918R	O DrayTek-162CA0	00:1D:AA:58:69:74	94%(-60dbm)	11	AES	WPA3/WPA2 Personal
guiapator	0	22:1D:AA:58:69:74	94%(-60dbm)	11	AES	WPA2 Personal
AC	O nancy_v2765_2	06:1D:AA:04:F0:C4	100%(-44dbm)	11	AES	WPA3/WPA2 Personal
):1D:AA:3F:B2:30	O nancy_v2765	02:50:7F:C1:A2:6C	100%(-50dbm)	11	AES	WPA3/WPA2 Personal
J. TD.AA.31 .02.30	O nancy_v2765_2	02:50:7F:D1:A2:6C	100%(-51dbm)	11	AES	WPA3/WPA2 Personal
mware	0	2A:49:BC:1F:9E:C0	96%(-57dbm)	11	AES	WPA2 Personal
4.6	AP906-WDS-2.4G	2E:49:BC:1F:9E:C0	100%(-45dbm)	11	AES	WPA2 Personal
4.0	O 55554 351000 3	04.10.44.04.50.04	1000/ (4Edbm)	1 1	AEC	MDA2/MDA2 Decoral
eration Mode						Sear
esh Root	SSID	Channel		Security M	Node	Encryption Type
		2462MHz (Chanr	nel 11) 🗸	WPA2	Personal 🗸	AES ~
	Security Key					

ltem	Description
SSID/Security Key	Once the access point specified above, the name / security key of the AP will be shown automatically in these fields.
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	Available options will vary according to the selected Security Mode .
	When Open is selected:
	 Choose None to disable the WEP Encryption. Data sent to the AF will not be encrypted.
	• WEP Keys –To enable WEP encryption for data transmission, please choose WEP. 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 '.'.
	When Shared is selected:
	 WEP Keys - To enable WEP encryption for data transmission, please choose WEP. 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 ','.
When WPA Personal or WPA2 Personal is selected:
Select TKIP or AES as the algorithm for WPA.
Security Key - Select WEP, 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...").

5. A summary of settings configuration will be shown on screen. Click **Finish**.

\setminus /	0peration Mode WiFi Setup	Admin Range Password Extended	Finish	
	Basic settings are c	ompleted. Press Finish I	button apply change	S.
DrayTek Device VigorAP918R	Operation Mode Peer SSID WiFi Name 2nd WiFi Name Bandwidth Limit Station Control	Range Extender (2.4 guests DrayTek-3FB230 Disabled Disabled Disabled	GHz WLAN)	
MAC 00:1D:AA:3F:B2:30 Firmware 1.4.6 Operation Mode Mesh Root			Cancel	Finish

This page is left blank.

Chapter II Connectivity



II-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

AP: VigorAP acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them. Image: AP of the second secon

Mesh Root:

AP connects to gateway with Ethernet cable. It would be other AP's uplink

Mesh Node:

connection.

Use wireless to connect to other Mesh Root when Ethernet cable doesn't exist. A mesh network creates a set of links automatically and calculate the most optimal wireless path through the wireless network back to a wired Mesh Root.

Range Extender :

VigorAP can act as a wireless repeater; it can be Station and AP at the same time.



Available settings are explained as follows:	

ltem	Description			
АР	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.			
Mesh	Mesh Root – VigorAP must connect to a gateway with an Ethernet cable.			
	Mesh Node – VigorAP can connect to other mesh root via wireless connection. A mesh network creates one set of links automatically and calculates the most optimal wireless path through the wireless network back to a wired mesh root.			
Range Extender	VigorAP can act as a wireless repeater which 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.			

(i) 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.

II-2 General Concepts for Wireless LAN (2.4GHz/5GHz)

VigorAP 918R 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 918R can support data rates up to 867 MBps in 802.11ac 80 MHz channels.

(i) 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.

VigorAP 918R 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 918R. 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 918R 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 918R) with the encryption of WPA and WPA2.



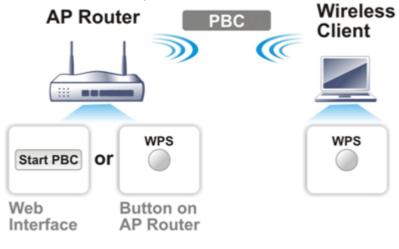
It is the simplest way to build connection between wireless network clients and VigorAP 918R. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 918R automatically.

(i) Note:

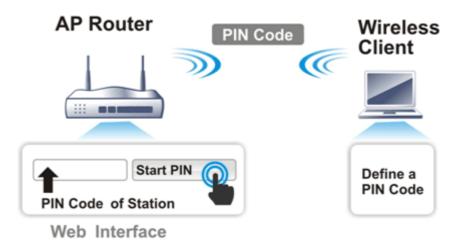
Such function is available for the wireless station with WPS supported.

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 918R series which served as an AP, press **WPS** button once on the front panel of VigorAP 918R 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.

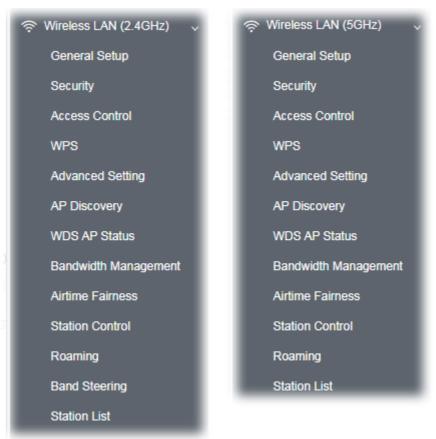


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 918R.



II-3 Wireless LAN (2.4GHz/5GHz) Settings for AP Mode

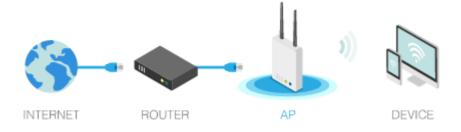
When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering and Station List.



(i) Note:

Available settings for **Wireless LAN (2.4GHz) and Wireless LAN (5GHz)** are almost the same, except for Band Steering.

The following figure shows how VigorAP runs as AP (Access Point):



II-3-1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID, the wireless channel and WDS (for 5GHz only). Please refer to the following figure for more information.

	tting (IEEE							
	Wireless							
U En	able Clien	t Limit 12	8 (3 ~ 128, defa	ault: 128)			
🗌 En	able Clien	t Limit per	SSID (3 ~ 128, de	fault: 12	(8)			
Mode	:		Mixed (11a+11n+11	ac) 🗸]			
Chan	nel :		AutoSelect 🗸 (A	ctive Ch	annel: 36) Fi	Itered Out Li	st	
Detail	ls :	2	0/40MHz Ext Ch: 40) , 80МН	z Center Ch:	42		
	Enable H	lide SSID	SSID		Isolate LAN	Isolate Member	VLAN ID (0:Untagged)	
1			DrayTek-3FB230				0	
2							0	
3							0	
4							0	— Available
Isolate Isolate Note: To allo	EAN: Member: Exception	Wireless LAN. Wireless other. Isolate B unication b	SSID from being se clients (stations) w clients (stations) w exception can be cre etween clients with bands option on Ad	vith the s vith the s eated by different	ame SSID ca adding the M t SSIDs on di	nnot access IAC from <mark>De</mark>	s for each vice Object.	5GHz Ac Point Mo
WDS S Secur	Settings (Pl	HY Mode :	HTMIX)	Deer M	AC Address :			
	isabled (AES	1.		1: []: []		
Ke								
Ke	, .			2.]:[_]:[_); []; [_]; [_]; [
				3.]:[_]:[

ltem	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Client Limit	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 Client Limit 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 918R can connect to 2.4GHz stations with 11n only, Mixed (11b+11g), and Mixed (11b+11g+11n) simultaneously, or to 5GHz stations with 11a only, 11n only(5G), Mixed (11a+11n) and Mixed (11a+11n+11ac) simultaneously. Simply choose Mixed (11b+11g+11n) / Mixed (11a+11n+11ac)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.
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 918R while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 918R to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Isolate LAN	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
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.
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 WEP, 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 918R connects to.

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

II-3-2 Security

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

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

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek-3FB	230	
Mode	WPA3/WPA	2 Personal 🗸 🗸	
Set up RADIUS	Server if 802.1x is enable	ed.	
WPA			
WPA Algorithms	🔵 TKIP [🔾	AES TKIP/AES	
Pass Phrase	••••••	•	
Key Renewal Int	terval 3600 sec	onds	
EAPOL Key Retr	y 📀 Enable 🤇	Disable	
WEP			
Key 1 :			Hex 🗸
Key 2 :			Hex 🗸
Key 3 :			Hex 🗸
Key 4 :			Hex 🗸
	ок	Cancel	

Wireless LAN (5GHz) >> Security Settings

ltem	Description		
Mode	There are several modes provided for you to choose.		
	Below shows the modes with higher security;		
WPA3/WPA2 Personal V WPA3/WPA2 Personal V WPA3/WPA2 Personal V WPA2 Personal V WPA2 Personal V	 WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal - 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. 		
WPA3 Enterprise WPA3/WPA2 Enterprise WPA2 Enterprise	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.		
WPA2/WPA Enterprise	 WPA3 Enterprise, WPA3/WPA2 Enterprise, WPA2 Enterprise WPA2/WPA Enterprise - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or 		

	automatically negotiated via 802.1x authentication.
	• WPA2 Enterprise - 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.
	• OWE - WPA3 also introduces a new open and secure connection mode; "Opportunistic Wireless Encryption" (OWE). It allows the clients to connect without a password, ideal for hotspot networks, but the connection between each individual client is uniquely encrypted behind the scenes.
	Below shows the modes with basic security;
	 WPA Personal - 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.
	 WPA Enterprise - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	• WEP Personal - Accepts only WEP clients and the encryption key should be entered in WEP Key.
	• None - The encryption mechanism is turned off.
WPA Algorithms	This feature is available for WPA3 Enterprise , WPA2 Enterprise , WPA Enterprise , WPA3 Personal , WPA2 Personal , WPA Personal , WPA3/WPA2 Personal , or WPA2/WPA Personal mode.
	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
	Note that not all modes of Vigor router supports WPA3 mode. However, if the Vigor router supports WPA3 Personal/Enterprise security mode, the WPA algorithms will be set as AES.
Pass Phrase	Type 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). This feature is available for WPA Personal or WPA2 Personal or WPA2 / WPA Personal mode, WPA3 Personal or WPA3/WPA2 Personal .
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 WPA3 Enterprise, WPA2 Enterprise, WPA Enterprise, WPA3 Personal, WPA2 Personal, WPA Personal, WPA3/WPA2 Enterprise, WPA2/WPA Enterprise, WPA3/WPA2 Personal, or WPA2/WPA Personal mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN.
	Click Enable to 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 Personal** mode.

RADIUS Server Setup - Google Chrome

③ 不安全 | 192.168.1.13/wireless/radius.asp

Radius Server

Use internal RADIUS Server

IP Address

Port

1812

Shared Secret

DrayTek

Session Timeout

O

Second(s)

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

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 918R 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, IV-1-1 RADIUS Server to configure settings for internal server of VigorAP 918R.
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.

II-3-3 Access Control

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

SSID 1	SSID 2	SSID 3	SSID 4
3310 1		k-3FB230	3310 4
Ind		ddress Filter ss Commen	its
	C Object		
Devic	e Group None	or Device Object None	+ ~
	Add	Limit:256 entries	
	ок	Cancel	
Backup ACL Cfg : Bac	kup Upload From	ile: Browse	Restore

Wireless LAN (5GHz) >> Access Control

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 918R.
MAC Address Filter	Display all MAC addresses that are edited before.
МАС	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.
Object	In addition to enter the MAC address of the device manually, you can

	Device Group - Select one of the existed device groups and click Add . All the devices belonging to the selected group will be shown on the MAC Address Filter table.
	Device Object - Select one of the existed device object and click Add . The MAC address of the device will be shown on the MAC Address Filter table.
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.

II-3-4 WPS

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

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

Wi-Fi Protected Setup Information		
WPS Configured	Yes	
WPS SSID	DrayTek-3FB230	
WPS Auth Mode	WPA3/WPA2 Personal	
WPS Encrypt Type	AES	

Configure via Push Button	Start PBC	
Configure via Client PinCode		Start PIN
Status: The Authentication Mode is N	IOT WPA2/WPA PersonalII	

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.

ltem	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 918R 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 918R. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 918R.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 918R will wait for WPS requests from wireless clients about

	two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 918R 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 918R 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).				

II-3-5 Advanced Setting

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

Wireless LAN (5GHz) >> Advanced Setting

Channel Bandwidth	○ 20 MHz ○ Auto 20/40 MHz • Auto 20/40/80 MHz
Tx Power	● 100%
Fragment Length (256 - 2346)	2346 bytes
RTS Threshold (1 - 2347)	2347 bytes
Country Code	(Reference)
Auto Channel Filtered Out List	36 40 44 48 149 153 157 161
	165
IGMP Snooping	O Enable ○ Disable
Isolate SSIDs	O Enable ○ Disable
Isolate members with IP	🔾 Enable 🝳 Disable
WMM Capable	O Enable 🔿 Disable
APSD Capable	🔾 Enable 🛛 Disable
Note: Fragment Length takes effect whe	en mode is "11a Only".

Available settings are explained as follows:

ltem	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- The AP will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not.
	40 MHz- The device will use 40MHz for data transmission and receiving between the AP and the stations. It is for wireless LAN

Cancel

	2.4GHz only.
	Auto 20/40 /80 MHz - The device will use 20/40/80 MHz channel bandwidth for data transmission and receiving between the AP and the stations.
Antenna (for 2.4GHz only)	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.
Tx Power	The default setting is the maximum (100%). Lowering down the value may degrade range and throughput of wireless.
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 selected wireless channels will be discarded if AutoSelect is selected as Channel selection mode in Wireless LAN>>General Setup .
IGMP Snooping	Click Enable to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Isolate 2.4GHz and 5GHz bands	The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.
	For WLAN 2.4GHz and 5GHz set with the same SSID name:
	 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).
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

	to improve the performance by minimizing transmission latency. The default setting is Disable .
MAC Clone	Click Enable and manually enter the MAC address of the device with
(for 2.4GHz only)	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.

II-3-6 AP Discovery

VigorAP 918R 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.

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

Select I	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
0	1	DrayTek_5G	14:49:BC:0D:8F:00	67%(-72dbm)	36	AES	WPA3/WPA2 Personal
0	2	DrayTek-04	00:50:7F:F1:92:16	15%(-87dbm)	36	TKIP/AES	WPA2/WPA Personal
0	3	DrayTek_5G	14:49:BC: DrayTek-04F06	C 3%(-76dbm)	36	AES	WPA2 Enterprise
0	4	DrayTek_5G	16:49:BC:12:37:38	50%(-77dbm)	36	TKIP	WPA Personal
\bigcirc	5	DrayTek04F	00:1D:AA:04:F0:6D	25%(-84dbm)	36	TKIP/AES	WPA2/WPA Personal
0	6	sssssss123	00:1D:AA:41:DF:18	36%(-81dbm)	36	AES	WPA2 Personal
0	7	DrayTek_5G	14:49:BC:11:7B:60	39%(-80dbm)	36	AES	WPA3/WPA2 Personal
0	8	DrayTek_5G	14:49:BC:0A:8A:B8	5%(-90dbm)	36	AES	WPA2 Personal
0	9	DrayTek-51	16:49:BC:51:B7:9C	19%(-86dbm)	36	AES	WPA3/WPA2 Personal
0	10	DrayTek_5G	14:49:BC:11:F2:90	36%(-81dbm)	36	AES	WPA2 Personal
0	11	guests_4F5	16:49:BC:71:B7:9D	92%(-62dbm)	36	AES	WPA2 Personal
0	12	DrayTek_77	06:1D:AA:04:F0:6D	25%(-84dbm)	36	TKIP/AES	WPA2/WPA Personal
\bigcirc	13	DrayTek-F1	00:50:7F:F1:91:BC	76%(-69dbm)	36	AES	WPA3/WPA2 Personal
0	14	staffs_4F5	16:49:BC:6D:68:82	53%(-76dbm)	36	AES	WPA2 Personal
\bigcirc	15	guests_4F5	16:49:BC:7D:68:82	50%(-77dbm)	36	AES	WPA2 Personal
0	16		12:1D:AA:04:F0:6D	22%(-85dbm)	36	AES	WPA2 Personal
\bigcirc	17	staffs_4F5	16:49:BC:61:B7:9D	93%(-61dbm)	36	AES	WPA2 Personal
0	18	DrayTek11	00:50:7F:67:29:0C	15%(-87dbm)	153	TKIP/AES	WPA2/WPA Personal
0	19	DrayTek22	02:50:7F:17:29:0C	15%(-87dbm)	153	TKIP/AES	WPA2/WPA Personal
0	20	DrayTek_77	06:1D:AA:04:F0:6E	32%(-82dbm)	157	TKIP/AES	WPA2/WPA Personal
0	21		12:1D:AA:04:F0:6E	32%(-82dbm)	157	AES	WPA2 Personal
0	22	DrayTek04F	00:1D:AA:04:F0:6E	32%(-82dbm)	157	TKIP/AES	WPA2/WPA Personal
0	23	Vigor2865a	14:49:BC:10:0D:68	8%(-89dbm)	165	AES	WPA3/WPA2 Personal

Wireless LAN (5GHz) >> Access Point Discovery



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

AP's MAC Address	:	:	:	:	:	AP's SSID	
Add to WDS Settings:	Add						

Each item is explained as follows:	Each it	tem is	explained	d as fo	llows:
------------------------------------	---------	--------	-----------	---------	--------

ltem	Description
SSID	Display the SSID of the AP scanned by VigorAP 918R.
BSSID	Display the MAC address of the AP scanned by VigorAP 918R.
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 918R.
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 / AP's SSID	Display the MAC address and SSID of the AP selected from the Access Point.
Add	Click it to add the AP selected from the Access Point List (with the same channel width) to the WDS Settings as peer's setting.

II-3-7 WDS AP Status

VigorAP 918R 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.

VDS	AP List			
AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth

It is available for wireless LAN (5GHz) only.

II-3-8 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		DrayTek-3	B230		
Per Stati	on Bandwidth Lim	it			
Enable	2				
Upload	Limit	User def	ined \lor	K	bps (Default unit : K)
Downlo	ad Limit	User def	ined \checkmark	K	bps (Default unit : K)
Auto A	djustment				
Total U	pload Limit	User def	ined \checkmark	K	bps (Default unit : K)
Total D	ownload Limit	User def	ined \checkmark	K	bps (Default unit : K)
					ng sent from a wireless station. ailable bandwidth.
		ОК	C	ancel	

Available settings are explained as follows:

ltem	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.

II-3-9 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.

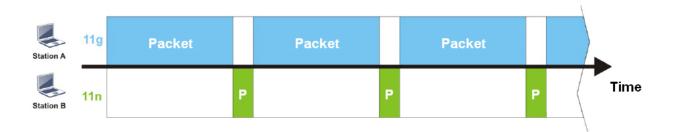
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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 918R. 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 918R. 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 (2 \sim 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.



Available settings are explained as follows:

ltem	Description
Enable Airtime Fairness	Try to assign similar airtime to each wireless station by controlling T> traffic.
	Airtime Fairness – Click the link to display the following screen of airtime fairness note.
	Wasks Attime Fainces Code Channe I 172.17.3.110/wireless/ap_af_note.asp Airtime Fainness Note: * Airtime is the time where a wireless station occupies the wirelees channel. Airtime Fairness function sites 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.

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

(i) 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.

II-3-10 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.

(i) 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		DrayTek-3FB2	230
Enable			
Connection	Time	1 hour \sim	
Reconnection	on Time	$1 day \sim$	
Display All 9	Station Control L	ist	

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



Available settings are explained as follows:

ltem	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.

II-3-11 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

Fast Transition Roaming		
Enable 802.11r		

AP-assisted Client Roaming Parameters

Minimum Basic Rate	6 v Mbps
O Disable RSSI Requirement	
O Strictly Minimum RSSI	-73 dBm (42 %) (Default: -73)
O Minimum RSSI	- 66 dBm (60 %) (Default: -66)
with Adjacent AP RSSI over	5 dB (Default: 5)
Fast Roaming(WPA2 Enterprise)	
Enable	
PMK Caching : Cache Period Pre-Authentication	10 minutes (10 ~ 600, Default: 10)
	OK Cancel

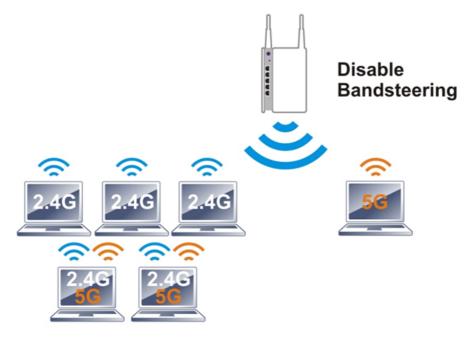
Item	Description
Fast Transition Roaming	Enable 802.11r - Check to enable the function of fast roaming to switch between the hotspots fastly and securely.
AP-assisted Client Roaming Parameters	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 918R 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.
	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 918R will terminate the network connection for that wireless station.
	Disable RSSI Requirement - If it is selected, VigorAP will not terminate the network connection based on RSSI.

	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 918R will terminate the network connection for that wireless station.
	 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 918R, VigorAP 918R will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI). With Adjacent AP RSSI over – Specify a value as a threshold.
East Roaming	Enable – Check the box to enable fast roaming configuration.
Fast Roaming (WPA2/802.1x)	 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.
	Pre-Authentication - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)
	Enable - Enable IEEE 802.1X Pre-Authentication.

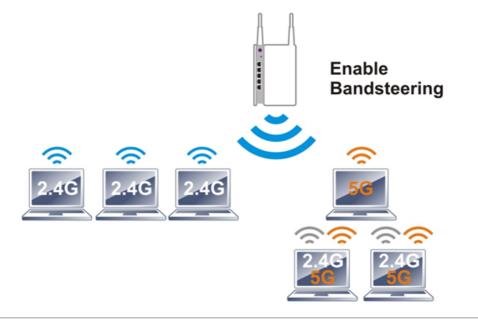
After finishing this web page configuration, please click **OK** to save the settings.

II-3-12 Band Steering (for Wireless LAN (2.4GHz))

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.



(i) 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:

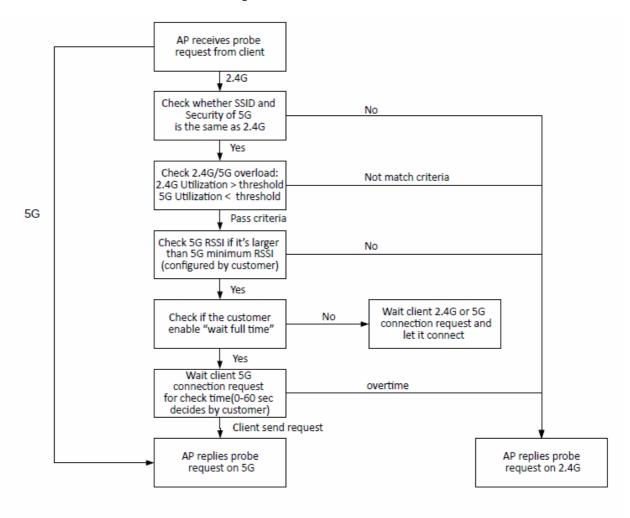
🗆 E	nable Band Steering	
	Check Time for WLAN Client 5G Capability	15 seconds (1 ~ 60, Default: 15)
	Wait Full Time to Check 5G Capability	/
	☑ 5GHz Minimum RSSI	-78 dBm (29 %) (Default: -78)
	(Only do band steering when 5GHz signal is	better than Minimum RSSI)
	Overloaded	
	2.4GHz Utilization Overload Threshold	70 % (Default: 70)
	5GHz Utilization Overload Threshold	70 % (Default: 70)
	(Only do band steering when 2.4GHz utiliza not)	tion is overloaded and 5GHz utilization is
Note:	Please setup at least one pair of 2.4GHz and security.	5GHz Wireless LAN with the same SSID and
	ОК	Cancel

Available settings are explained as follows:

ltem	Description
Enable Band Steering	If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit.
	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.
	Wait Full Time to Check 5G Capability – If enabled, the client trying to connect to wireless network 2.4G has to wait for a few seconds (defined in Check Time above) to check if the connecting device ha the 5G capability. If no 5G capability, the client will be directed to the wireless 2.4G network.
	5GHz Minimum RSSI – The wireless station has the capability of 5GH 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.
	Overloaded – If it is enabled, VigorAP will activate the band steering according to the conditions set below.
	• 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.
	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.

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

Below shows how Band Steering works.



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

How to Use Band Steering?

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

Wireless LAN (2.4GHz) >> Band Steering	
C Enable Band Steering	
Check Time for WLAN Client 5G Capability	15 seconds (1 ~ 60, Default: 15)
Wait Full Time to Check 5G Capability	

- 3. Click **OK** to save the settings.
- 4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *ap918r-BandSteering* for both pages. Click **OK** to save the settings.

	General Setting (IEEE 802.11)
	C Enable Wireless LAN
	Enable Client Limit 128 (3 ~ 128, default: 128)
	Enable Client Limit per SSID (3 ~ 128, default: 128)
	Mode: Mixed(11b+11g+11n) ~
	Channel : 2462MHz (Channel 11) \checkmark
	Extension Channel : 2442MHz (Channel 7) \checkmark
	Forthe Hide COLD Isolate Isolate VLAN ID
	Enable SSID LAN Mumber(0:Untagged)
	1 ap918r-BandSteering 0
	2 🖸 🗆 mk_carrie
/	3 ♥ Imk_carrie I0 I0 Wireless LAN (5GHz) >> General Setup
/	Wireless LAN (5GHz) >> General Setup
ame value	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11)
for 2.4GHz	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11)
	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11) Enable Wireless LAN Enable Client Limit 128 (3 ~ 128, default: 128)
ame value for 2.4GHz and 5GHz	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11)
for 2.4GHz	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11) Enable Wireless LAN Enable Client Limit 128 (3 ~ 128, default: 128)
for 2.4GHz	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11) Enable Wireless LAN Enable Client Limit 128 (3 ~ 128, default: 128) Enable Client Limit per SSID (3 ~ 128, default: 128)
for 2.4GHz	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11) Enable Wireless LAN Enable Client Limit 128 (3 ~ 128, default: 128) Enable Client Limit per SSID (3 ~ 128, default: 128) Mode : Mixed (11a+11n+11ac) ~
for 2.4GHz	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11)
for 2.4GHz	Wireless LAN (5GHz) >> General Setup General Setting (IEEE 802.11) Enable Wireless LAN Enable Client Limit 128 (3 ~ 128, default: 128) Enable Client Limit per SSID (3 ~ 128, default: 128) Mode : Mixed (11a+11n+11ac) ~ Channel : AutoSelect ~ (Active Channel: 36) Filtered Out List Details : 20/40MHz Ext Ch: 40, 80MHz Center Ch: 42

5. 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

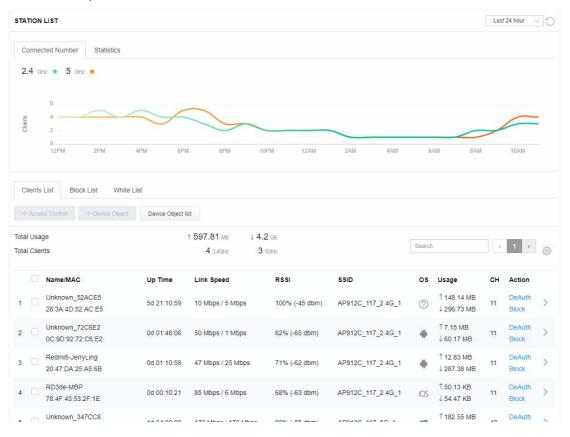
6. Now, VigorAP 918R will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

II-3-13 Station List

Station List provides the information related to the number of clients connecting to VigorAP, used bandwidth and the statistics of the AP device OS. Besides, users can create access control policies, device objects and set black & white list for

II-3-13-1 Connected Number

This page lists the graph for the number of wireless stations connected to this Access Point with different time phases.



II-3-13-2 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.

ON L	IST 🕕							L	ast 24 hour	C
necte	ed Number Statistics									
ſ	0% 0% 0% 0% 0%	 Android 0 iOS 0 Windows 0 Linux 0 Others 58 		Policy		100% 0%	Pass 58Block 0		C	ъ̀
nts Li	ist Block List White L	_ist								
ccess	Control + Device Object	Device Object I	ist							
Jsage Clients				5g	¢	1	2 3 4	5	6 7 >	
	Name/MAC	Up Time	Link Speed	RSSI	SSID	os	Usage	сн	Action	
	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
	Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:41:17	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1̂ 867 В ↓717 В	36	DeAuth Block	>
	Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1867 B ↓717 B	36	DeAuth Block	>
	Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:41:16	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	1̂ 867 В ↓717 В	36	DeAuth Block	>
	Unknown_607C8F 00:BC:DA:60:7C:8F	0d 03:41:16	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1867 B ↓717 B	36	DeAuth Block	>
	Unknown_9D28C0 00:BC:DA:9D:28:C0	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1867 B ↓717 B	36	DeAuth Block	>
	Unknown_79E9C2 00:BC:DA:79:E9:C2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1867 B ↓717 B	36	DeAuth Block	>
	Unknown_9B07CE 00:BC:DA:9B:07:CE	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	0	1 867 B ↓717 B	36	DeAuth Block	>
	Unknown_AA5A63 00:BC:DA:AA:5A:63	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
	Unknown_DD1FA2 00:BC:DA:DD:1F:A2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1 903 B ↓717 B	36	DeAuth Block	>
	nts Li Ccess Jsage	Device OS 0% 0%	Inected Number Statistics Device OS 0% • Android 0 0% • OS 0 • Windows 0 0% • Others 50 0% nts List Block List White List ccess Control + Device Object Device Object sage 1 58 lints Device C84A46 0d 03:41:17 0.05.BC:DA:07.05.01 0d 03:41:17 0.05.BC:DA:07.05.01 0d 03:41:17 0.05.BC:DA:07.05.01 0d 03:41:16 0.05.BC:DA:07.05.02 0d 03:41:46 0.05.BC:DA:07.05.02 0d 03:41:46 0.05.BC:DA:07.05.02 0d 03:41:46 0.05.BC:DA:07.05.02 0d 03:41:46 0.05.CDA:07.05.02 0d 03:41:46 0.05.CDA:07.05.02 0d 03:41:46 0.05.CDA:07.05.02 0d 03:41:46 0.05.CDA:07.05.02 <td>Inected Number Statistics Device OS 0% + 10S 0 0% + 10S 0 0% + 10S 0 0% + 10S 0 0% + 10S 0 0% + Unix 0 0% + Unix 0 100% - 0thers 58 - 0thers 58 ints List Block List White List Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.6 CDA C2.4A46 0d 03.41:17 270 Mbps / 6 Mbps 0 Unknown_CB4A6 0d 03.41:17 270 Mbps / 6 Mbps 0 Unknown_OCBEF 0 d 03.41:16 270 Mbps / 6 Mbps 0 Unknown_OC26F 0 d 03.41:46 270 Mbps / 6 Mbps 0 Unknown_P928C0 0 d 03.41:46 270 Mbps / 6 Mbps</td> <td>Inected Number Statistics Device OS 0% • Android 0 0% • IOS 0 0% • IOS 0 0% • Unax 0 100% • Others 38 Ints List Block List Block List White List ccccss Control + Device Object Device Object Device Object list Istents 1 58.13 kB 1 45.89 kB 0 2.4GR2 64 5GR2 59 O 0.6C:DA/C8.4A46 0d 03:41:17 270 Mbps / 6 Mbps 57% (-67 dbm) O 0.6C:DA/C8.4A46 0d 03:41:17 270 Mbps / 6 Mbps 55% (-68 dbm) O 0.6C:DA/C8.4A46 0d 03:41:17 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_07B0C1 0d 03:41:17 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_02CEE9 0d 03:41:16 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_072B2C 0d 03:41:46 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_072B2C 0d 03:41:46 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_072B2C2 0d</td> <td>Inected Number Statistics Ops Android 0 Ops Ops<td>Inected Number Statistics Device OS Ob - Android 0 Ob - IOS 0 Ob - IOS 0 Ob - OIS 0 Ob - OIS 0 Ob - OIS 0 Ob - OIhers 0 Ob - OIhers 58 Ist List Block List Ist List Block List White List - Others 58 O 2464c 64 534c Sage 1 O BCDA C8 4A.46 Od 03.41:17 O DBCDA C9 BOC 1 Od 03.41:16 O DBCDA A0C EEE9 Od 03.41:16</td><td>nected Number Statistics</td><td>nected Number Statistics Device OS 0% Android 0 0% IOS 0 0% Unkros 0 100% Others 30 0% Unkros 0 100% Others 30 100% Others 30 100% Others 50 100% Others 60 11177 270 Mbps / 6 Mbps 57% (-67 dbm) 11778 36</td><td>Increded Number Statistics Device OS 0% - Android 0 0% - OS 0 0% - Others 50 0% - Others 50 0% - Others 50 0% - Others 50 0 - Others 50 0</td></td>	Inected Number Statistics Device OS 0% + 10S 0 0% + 10S 0 0% + 10S 0 0% + 10S 0 0% + 10S 0 0% + Unix 0 0% + Unix 0 100% - 0thers 58 - 0thers 58 ints List Block List White List Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.46 k2 64 5042 Isage 1 58.13 kB 1 45.89 kB 0 2.6 CDA C2.4A46 0d 03.41:17 270 Mbps / 6 Mbps 0 Unknown_CB4A6 0d 03.41:17 270 Mbps / 6 Mbps 0 Unknown_OCBEF 0 d 03.41:16 270 Mbps / 6 Mbps 0 Unknown_OC26F 0 d 03.41:46 270 Mbps / 6 Mbps 0 Unknown_P928C0 0 d 03.41:46 270 Mbps / 6 Mbps	Inected Number Statistics Device OS 0% • Android 0 0% • IOS 0 0% • IOS 0 0% • Unax 0 100% • Others 38 Ints List Block List Block List White List ccccss Control + Device Object Device Object Device Object list Istents 1 58.13 kB 1 45.89 kB 0 2.4GR2 64 5GR2 59 O 0.6C:DA/C8.4A46 0d 03:41:17 270 Mbps / 6 Mbps 57% (-67 dbm) O 0.6C:DA/C8.4A46 0d 03:41:17 270 Mbps / 6 Mbps 55% (-68 dbm) O 0.6C:DA/C8.4A46 0d 03:41:17 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_07B0C1 0d 03:41:17 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_02CEE9 0d 03:41:16 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_072B2C 0d 03:41:46 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_072B2C 0d 03:41:46 270 Mbps / 6 Mbps 55% (-66 dbm) O Unknown_072B2C2 0d	Inected Number Statistics Ops Android 0 Ops Ops <td>Inected Number Statistics Device OS Ob - Android 0 Ob - IOS 0 Ob - IOS 0 Ob - OIS 0 Ob - OIS 0 Ob - OIS 0 Ob - OIhers 0 Ob - OIhers 58 Ist List Block List Ist List Block List White List - Others 58 O 2464c 64 534c Sage 1 O BCDA C8 4A.46 Od 03.41:17 O DBCDA C9 BOC 1 Od 03.41:16 O DBCDA A0C EEE9 Od 03.41:16</td> <td>nected Number Statistics</td> <td>nected Number Statistics Device OS 0% Android 0 0% IOS 0 0% Unkros 0 100% Others 30 0% Unkros 0 100% Others 30 100% Others 30 100% Others 50 100% Others 60 11177 270 Mbps / 6 Mbps 57% (-67 dbm) 11778 36</td> <td>Increded Number Statistics Device OS 0% - Android 0 0% - OS 0 0% - Others 50 0% - Others 50 0% - Others 50 0% - Others 50 0 - Others 50 0</td>	Inected Number Statistics Device OS Ob - Android 0 Ob - IOS 0 Ob - IOS 0 Ob - OIS 0 Ob - OIS 0 Ob - OIS 0 Ob - OIhers 0 Ob - OIhers 58 Ist List Block List Ist List Block List White List - Others 58 O 2464c 64 534c Sage 1 O BCDA C8 4A.46 Od 03.41:17 O DBCDA C9 BOC 1 Od 03.41:16 O DBCDA A0C EEE9 Od 03.41:16	nected Number Statistics	nected Number Statistics Device OS 0% Android 0 0% IOS 0 0% Unkros 0 100% Others 30 0% Unkros 0 100% Others 30 100% Others 30 100% Others 50 100% Others 60 11177 270 Mbps / 6 Mbps 57% (-67 dbm) 11778 36	Increded Number Statistics Device OS 0% - Android 0 0% - OS 0 0% - Others 50 0% - Others 50 0% - Others 50 0% - Others 50 0 - Others 50 0

II-3-13-3 Clients List

The client list displays all the stations connecting to VigorAP.

STAT		LIST 🕕							L	ast 24 hour	C ~
Coi	nnect	ted Number Statistics									
		0% Device OS 0% 100%	 iOS 0 Windows Linux 0 	0	Polic	у	100% 0%	 Pass 58 Block 0 			
Clie	ents l	.ist Block List White	List								
++	Access	s Control + Device Object	Device Object	t list							
Total (Usag	e		t list 8.13 kB ↓ 45.89 kB 0 2.4GHz 64 5GHz	5g		1	2 3 4	5	6 7 >	\$ <u>\$</u> }
Total	Usag	e ts		8.13 kв ↓ 45.89 kв	5g RSSI	SSID	1 OS	2 3 4 Usage	5 CH	6 7 > Action	\$\$\$
Total	Usag Client	e ts	† 5	8.13 кв ↓ 45.89 кв 0 24GHz 64 5GHz							>
Total (Usag Client	e ts Name/MAC Unknown_C84A46	↑ 5 Up Time	8.13 kg ↓ 45.89 kg 0 249Hz 64 59Hz Link Speed	RSSI	SSID	os	Usage ↑ 867 B	сн	Action DeAuth	- U -
Total (Total (Usag Client	e ts Name/MAC Unknown_C84A46 00:BC:DA:C8:4A:46 Unknown_07B0C1	1 5 Up Time 0d 03:42:47	8.13 KB ↓ 45.89 KB 0 2.4GHz 64 5GHz Link Speed 270 Mbps / 6 Mbps	RSSI 57% (-67 dbm)	SSID AA-903	os ?	Usage ↑ 867 B ↓ 717 B ↑ 867 B	СН 36	Action DeAuth Block DeAuth	>

Available settings are explained as follows:

em	Descripti	on				
Access Control	lt is availa List.	ble after choo	osing one of th	ne entries (clients) on Clients		
	Add Access Control					
	ed Wireless LAN	5GHz 🗸				
	De SSID Policy	1 Black list AA-903	2 Disable v 3 AA-903-2	Disable v 4 Disable v AA-903-3 AA-903-4		
	From to list	Device MAC	Nama			
		Device MAC	Name	Apply to SSID		
	ts.	00:BC:DA:07:B0:C1	Unknown_07B0C1	All 1 2 3 4		
		00:BC:DA:C3:4F:0A	Unknown_C34F0A	Ali 1 2 3 4		

From to list - Display the clients available for applying this access

	control.		
		elect the one(s) to mal	e the device apply the policies to all ke the device apply the policies to
	Close - Exit	this page without sav	ing any changes.
	Save chang	ges - Save the changes	s and exit this page.
+Device Object	(clients) on button to o		ist, choose one of the entries the Device Object button. Click the e.
		Device MAC	Name
		Device MAC	Name
		00:BC:DA:F5:EB:B4	Unknown_F5EB34
		00:BC:DA:94:CC:07	Unknown_94CC07
	-		
			Cancel OK
	Vhite List		
			he page. Change the MAC address equired. Then click OK and exit the
-			
Device Object list	The existed page.	device object profiles	s will be shown on the following
	DEVICE OBJECT		×
	Device Object Profiles		Search Secto Factory Default
	Profidx	MAC	Name
	1	00.50.7F.F1.91.BC	TEST_1
	2	00:50.7F:00:92.8A	TEST_2
Clients List	Display the	stations connecting to	o this Vigor device.
	Total Usag	e - Display	
	Total Clien	ts - Display the numb	er of the clients using 2.4GHz
			name / MAC address of the
	connecting		
	Up Time - 🛛	Display the connection	n time.
	Link Speed	- Display the link spee	ed.
	RSSI - Displ	ay the RSSI value.	
	SSID - Displ	ay the SSID the client	used for connecting VigorAP.
		the OS of the client.	
			sage (up and down) of the client.
		y the channel used by	
		-	on method used by the client, and if
		k list or white list.	on method used by the cheft, and li

II-3-13-4 Block List

This page displays information of the stations under block list.

Connected Number	Statist	tics										
2.4 GHz 🌒 5 G	iHz 😑											
1												
Clients												
0— 2AM	4AM	6AM	8AM	10AM	12PM	2PM	4PM	6PM	8PM	10PM	12AM	-
	ck List	White List	Device Object	t list					S	Search		
	+ Device		Device Objec	t list SSID	Reasor		Action		S	Search	۲ (۲	
+ Access Control Name / MAC	+ Device		Device Objec		Reason		Action		5	Search	(1	
Access Control Name / MAC	+ Device		Device Objec	SSID					2	Search	. 1	

Available settings are explained as follows:

Item	Description	l						
Device Object list	Click it to open the Device Object List dialog for reference.							
	DEVICE OBJECT							
	Device Object Profiles		Search Set to Factory Defout					
	Profidx	MAC	Name					
	4 J	00.50.7F.F1.91.BC	TEST_1					
	2	00:50:7F:00:92:8A	TEST_2					
Name / MAC	Display the	host name / MAC Addre	ess for the connecting client.					
SSID	Display the	SSID that the wireless c	lient connects to.					
Reason	Display the	reference information.						
Action	Display the action that you can execute for the station. Unblock - Click to unblock the entry.							

II-3-13-5 White List

This page displays general information of the stations under white list.

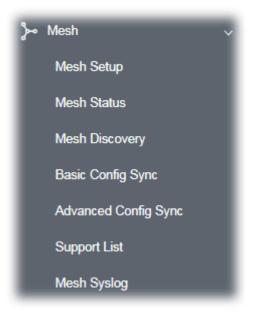
	11AM 1PM	3PM	5PM	7PM	9PM	11PM	1AM	3AM	5AM	7AM	9AM
Clients	List Block List	White List									
+ Acc	ess Control + De	evice Object	Device Object list								
										Search	
											۲ (
	Name/MAC			\$\$	ID		Action				
1	LiteonTe C8:FF:28:FC:2A:C1			mk	-carrie		Block				
2	Unknown_A02925 3C:95:09:A0:29:25			mk	-carrie		Block				
Total lis	st 2										

Available settings are explained as follows:

Item	Description							
Device Object list	Click it to open the Device Object List dialog for reference.							
	DEVICE OBJECT		28					
	Device Object Profiles		Search Settle Factory Default					
	Profidx	MAC	Name					
	4.5	00.50.7F F1.91.BC	TEST_1					
	2	00:50:7F.00:92:BA	TEST_2					
Name / MAC	Display the l	nost name / MAC Addre	ess for the connecting client.					
SSID	Display the SSID that the wireless client connects to.							
Action	Display the action that you can execute for the station.							
	Block - Click	to block the entry.						

II-4 Mesh Settings for Mesh Mode

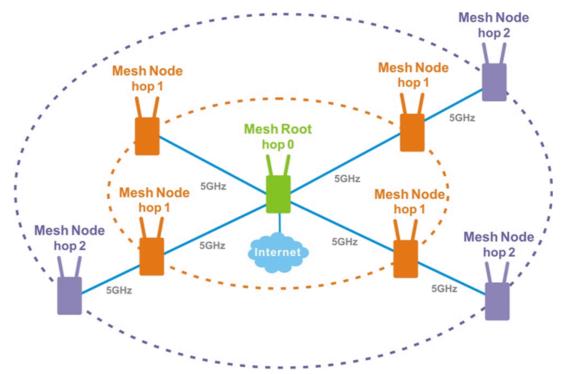
When you choose **Mesh** as the operation mode, the Mesh menu with the settings of Mesh Setup, Mesh Status, Mesh Discovery, Configuration Sync, Support List and Mesh Syslog will be shown on the screen.



Please note that, within VigorMesh network,

- the total number allowed for mesh nodes is 8 (including the mesh root)
- the maximum number of hop is 3

Refer to the following figure:



For the mesh group set within VigorMesh network,

- It must be composed by "1" Mesh Root and "0~7" mesh nodes
- (Roaming) Normally members in a mesh group use the same Wireless SSID/security
- (Add) Only the mesh root can add a new mesh node into the mesh group
- (Recover) A disconnected mesh node will automatically try to connect to another connected mesh node of the same group

Mesh Root and Mesh Node

Mesh Root indicates that VigorAP would be other AP's uplink connection. As a Mesh Root, VigorAP must connect to a gateway with Ethernet cable first to have an internet connection.

As a Mesh Node, VigorAP can connect to the mesh root or mesh node within the same mesh group via wireless network or physical connection with an Ethernet cable.

The following figure shows how VigorAP runs as MESH ROOT:



The following figure shows how VigorAP runs as MESH NODE:



II-4-1 Mesh Setup

Such page can determine the role of the VigorAP connecting to the computer physically. For a mesh root, you can search and specify mesh nodes as members under current mesh group.

onorai	Setup									
Role				O Mesh Root 🛛 Mesh Node						
Wireless Downlink Band				Auto v						
Group Name				VigorMesh]				
Auto	Resele	ect								
Log Lev	vel			Detailed \lor						
Mesh G	roup									
Select	Index		MAC Address	Model	CFG Sync	CFG Check	Device Name			
	1	Root	00:1D:AA:3F:B2:3	30 VigorAP918R						
Re	set									
lote: M			rk when Enable Man	agement VLAN is sele ОК Cano		> General Set	tup menu.			
dd Mes	in Noue		elow to find and add	opt the new node into	Mesh group.					
	earch l	outton b								
Sea	earch l rch nsuppo	orted mo		Search List. Please c	heck Mesh Sup	port List.				

Available settings are explained as follows:

ltem	Description
General Setup	
Role	Mesh Root – When VigorAP is connected to a Vigor router with a physical Ethernet cable, it can be set as mesh root to deliver the wireless signals to a mesh node AP.
	Mesh Node – As a mesh node, such VigorAP can pass the wireless connection signal to other mesh node or a remote device (PC, CPE, mobile phone).
	In addition, VigorAP can be searched by mesh root AP and join the mesh group of the root AP. The configuration set for mesh root can be applied to mesh node.
	Log Level – Choose Basic or Detailed . Related information will be shown on the Diagnostics>>System Log .

	Basic V Basic V Detailed						
When Mesh Root is selected	 Wireless Downlink Band – Choose a wireless band for connecting with a downlink mesh root or a downlink mesh node. Group Name - Display the name of the current mesh group. Auto Reselect - It is selected in default. To perform the auto reselect, make sure the process for CFG Sync and CFG Check for mesh nodes are successful. If enabled, after changing the environment of mesh network (e.g., offline, disconnection), the root device will perform autor reselect to reconstruct the mesh network. 						
When Mesh Node is selected	 Wired Uplink – Check the box if such VigorAP connects to an uplink mesh root or an uplink mesh node with an Ethernet cable. Wireless Uplink/Downlink Band – Choose a wireless band for connecting with an uplink/downlink mesh root or an uplink/downlink mesh node. 						
Mesh Group	 When the VigorAP is set as mesh root or is added to a mesh group, the basic information including role, MAC address, and model name of the AP will be shown in this area. Up to 8 entries (one mesh root and seven mesh nodes) will be shown on this field. Reset - Click it to clear the Mesh Group information. Delete - Click it to remove the selected entry. 						
Add Mesh Node	Click Search to find out available mesh node on the network. Add Mesh Node Press Search button below to find and adopt the new node into Mesh group. Search Search Search Seiect MAC Address Model Operation Mode Device Name 00:1D:AA:22:33:08 VigorAP903 MeshNode(Wireless) Apply Check the one you want and click Apply. The selected AP will be added onto current mesh root.						
Backup Mesh Config	Backup – Click the button to save the configuration as a file. Browse/Restore – Click the Browse button to specify a configuration file. Then click Restore to apply the configuration. When the MAC address of such VigorAP does not appear under the mesh group, the restore operation will not succeed and the error message, "Device MAC is not in mesh group list", will be shown instead.						

How to set up a mesh group?

The following steps will guide you how to setup a Mesh Group (with mesh root and mesh node) from **Mesh >> Mesh Setup**.

1. Open **Mesh>>Mesh Setup**. Click **Mesh Root** and click **OK** for the VigorAP connected to PC with Ethernet cable. At first, a Mesh Group is with only Mesh Root.

eneral	Setup							
Role	octup		ſ	0	lesh Root 🔿 Me	sh Node		
			L			Shinouc		
Wire	eless Do	ownlink	Band	Au	ito ~			
Grou	ıp Nam	e		Vigo	rMesh]	
Auto	Resel	ect						
.og Lev	/el			De	etailed 🗸			
Mesh G								
Select	Index	Role	MAC Address		Model	CFG Sync	CFG Check	Device Name
	1	Root	00:1D:AA:3F:B2:3	80	VigorAP918R			
Res	set							

2. Click the **Search** button in the field of **Add Mesh Node**.

		Role	MAC Address	Model	
	1	Root	00:1D:AA:3F:B2:30	VigorAP918R	
Rese	at				
			ок	Cancel	

Add Mesh Node

Press Search	hut	ton below to find and adopt the new node into Mesh group.
Search	34	

3. Wait until the searching result appears.

ress S Sea		ind and adopt the ne	ew node into Mesh group.	
Search	List			
Select	MAC Address	Model	Operation Mode	Device Name
	00:50:7F:F1:7E:EA	VigorAP918R	MeshNode(Wireless)	
	00:1D:AA:04:F0:10	VigorAP1000C	MeshNode(Wireless)	
	00:1D:AA:32:BC:24	VigorAP918RPD	MeshNode(Wired)	
	00:1D:AA:78:C9:20	VigorAP920R	MeshNode(Wireless)	
	00:1D:AA:78:CF:B0	VigorAP920R	MeshNode(Wireless)	
	00:1D:AA:68:D6:18	VigorAP920RPD	MeshNode(Wired)	

4. Choose the device(s) you want to add to the Mesh Group as mesh node(s) and define the **Device Name** for each node. In this example, five devices are specified as mesh nodes.

Press Si	earch button below to fi	ind and adopt the ne	w node into Mesh group.			
Sear	ch					
Search List						
Select	MAC Address	Model	Operation Mode	Device Name		
	00:50:7F:F1:7E:EA	VigorAP918R	MeshNode(Wireless)	room1		
	00:1D:AA:04:F0:10	VigorAP1000C	MeshNode(Wireless)	room2		
	00:1D:AA:32:BC:24	VigorAP918RPD	MeshNode(Wired)			
	00:1D:AA:78:C9:20	VigorAP920R	MeshNode(Wireless)	room3		
	00:1D:AA:78:CF:B0	VigorAP920R	MeshNode(Wireless)	room4		
	00:1D:AA:68:D6:18	VigorAP920RPD	MeshNode(Wired)	room5		

Backup Mesh Config

5. Click the **Apply** button and wait for it to finish the procedure.

		ind and adopt the h	ew node into Mesh group.	
Sea	rcn			
Search	List			
Select	MAC Address	Model	Operation Mode	Device Name
	00:50:7F:F1:7E:EA	VigorAP918R	MeshNode(Wireless)	room1
	00:1D:AA:04:F0:10	VigorAP1000C	MeshNode(Wireless)	room2
	00:1D:AA:32:BC:24	VigorAP918RPD	MeshNode(Wired)	
	00:1D:AA:78:C9:20	VigorAP920R	MeshNode(Wireless)	room3
	00:1D:AA:78:CF:B0	VigorAP920R	MeshNode(Wireless)	room4
	00:1D:AA:68:D6:18	VigorAP920RPD	MeshNode(Wired)	room5

6. After finishing the mesh network configuration, refer to **Mesh>>Mesh Status** for viewing the result. A mesh root with 5 mesh nodes is online.

Mesh >> Mesh Status

Local Status		Refresh
Device Name	VigorAP918R	
MAC Address	00:50:7F:F1:7E:ED	
Model	VigorAP918R	
Operation Mode	MeshRoot	
Link Status	Connected	
Нор	0	
Downlink Number	5	
Downlink	00:1D:AA:04:F0:10 (VigorAP1000C)	Wireless 5GHz (Ch36) (-38dBm)
	00:1D:AA:78:CF:B0 (VigorAP920R)	Wireless 5GHz (Ch36) (-74dBm)
	00:1D:AA:68:D6:18 (VigorAP920RPD)	Ethernet
	00:1D:AA:78:C9:20 (VigorAP920R)	Wireless 5GHz (Ch36) (-54dBm)
	00:50:7F:F1:7E:EA (VigorAP918R)	Wireless 5GHz (Ch36) (-33dBm)
Devices		Total number of Clients:

Index	Status	Device Name	IP Address	MAC Address (Model)	Нор	Uplink	Uptime	Client
1	Root	VigorAP918R	172.17.3.97	00:50:7F:F1:7E:ED (VigorAP918R)	0		Od 01:16:17	0
2	 Online 	room1	172.17.3.12	00:50:7F:F1:7E:EA (VigorAP918R)	1	00:50:7F:F1:7E:ED Wireless 5GHz (Ch36) (-30dBm)	Od 00:21:43	0
з	 Online 	room2	172.17.3.8	00:1D:AA:04:F0:10 (VigorAP1000C)	1	00:50:7F:F1:7E:ED Wireless 5GHz (Ch36) (-40dBm)	0d 00:44:50	0
4	 Online 	room3	172.17.3.6	00:1D:AA:78:C9:20 (VigorAP920R)	1	00:50:7F:F1:7E:ED Wireless 5GHz (Ch36) (-47dBm)	Od 01:01:46	0
5	 Online 	room4	172.17.3.98	00:1D:AA:78:CF:B0 (VigorAP920R)	1	00:50:7F:F1:7E:ED Wireless 5GHz (Ch36) (-64dBm)	Od 01:02:01	0
6	Online	room5	172.17.3.10	00:1D:AA:68:D6:18 (VigorAP920RPD)	0	00:50:7F:F1:7E:ED Ethernet	Od 01:03:05	0

II-4-2 Mesh Status

This page shows that one Mesh Group can contain up to 8 devices. A device with hop 0 indicates that it is one special Ethernet Backhaul. It means this node will use Ethernet cable to join the mesh group while others use the wireless link.

Mesh >> Mesh Status							
Local Status							Refresh
Device Name	VigorAP9	18R					
MAC Address	00:1D:A	A:3F:B2:30					
Model	VigorAP9	18R					
Operation Mode	MeshRoo	t					
Group Name	VigorMes	h					
Link Status	Connecte	d					
Нор	0						
Downlink Number	0						
Devices						Total r	number of Clients: (
Index Status	Device Name	IP Address	MAC Address (Model)	1	Hop Uplink	Uptime	Clients Speed Tes
1 🔍 Root	VigorAP918	192.168.1.14	00:1D:AA:3F:B2:30 (VigorAP918R)		0	0d 03:53:41	0
Online(sync read	y) 😑 Online	Offline			Last upda	ted: Wed Jan	22 14:58:29 202

Item	Description							
Local Status	Display general	informat	ion fo	r such V	igor	AP.		
Devices	Display detailed node(s) in the gr		tion fo	or this Vi	gor/	AP (as me	sh roc	ot) and me
	Index – Display the number of the device within a mesh group.							
	Status – Display the role of the device within a mesh group.							
	Device Name -						0	•
	IP Address – Dis					-		
	MAC Address –						ice.	
	(wired). "1" to "3 group and it cor					•		
		nnects to y the MA	other C addi	access ress of t	poin he d	t via wirel	ess lir	nk.
	group and it cor Uplink – Display to.	nnects to y the MA	other C addi	access ress of t	poin he d	t via wirel	ess lir	nk.
Total number of Clients	group and it cor Uplink – Display to. Display the stati	nnects to y the MA ion list of	other C addi ⁻ all mo	esh devi	poin he d ces.	t via wirel evice that	ess lin the A	nk. NP connec bps) RxRate(Kbps)
	group and it cor Uplink – Display to. Display the stati	nnects to y the MA	other C addi ⁻ all me	ress of the second s	poin he d ces.	t via wirel evice that rssi ^{68%(-63dBm)} 41%(-73dBm)	ess lir the A	nk. NP connec (Kipps) RxRate(Kipps)
	group and it cor Uplink – Display to. Display the stati Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:72	ion list of TA001029 ta002171 Tze-Pingde	other C addi ^c all me ^c all me ^{vendor} DrayTek DrayTek Apple	access ress of tl esh devi staffs_4F staffs_4F	poin he d ces.	t via wirel evice that RSSI 68%(-63dBm)	ess lin the A	nk. P connec bps) RxRate(Kbps) 0 0 0 0
	group and it cor Uplink – Display to. Display the stati Index MAC Address 1 00:50:7F:F0:C9:72 2 00:50:7F:F0:D1:1D 3 5C:97:F3:D3:D5:F7 4 40:98:AD:58:F2:55	Hostname TA001029 ta002171 Tze-Pingde Tyronetki	other C addi ^C all me ^{DrayTek} DrayTek DrayTek Apple	ssiD staffs_4F staffs_4F staffs_4F	poin he d ces.	t via wirel evice that evice that 68%(63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-68dBm)	ess lin the A	nk. P connec pps) RxRate(Kbps) 0 0 0 0 0 0 0 0 0 0 0 0 0
	group and it cor Uplink – Display to. Display the stati station List of All Devices Index MAC Address 1 00:50:7F:F0:20:12 2 00:50:7F:F0:21:10 3 5C:97:F3:03:D5:F7 4 40:98:AD:58:F2:52 5 00:50:7*:37:60:E5	hnects to y the MA ion list of Hostname TA001029 ta002171 Tze-Pingde Tyronetkil N/A	other C addr C addr C all mo DrayTek DrayTek Apple DrayTek	ssiD staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	ces.	t via wirel evice that 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-69dBm)	ess lin the A	nk. P connec bps) RxRate(Kbps) 0 0 0 0 0 0 0 0 0 0 0 0 0
	group and it cor Uplink – Display to. Display the stati Index MAC Address 1 00:50:7F:F0:C9:72 2 00:50:7F:F0:D1:1D 3 5C:97:F3:D3:D5:F7 4 40:98:AD:58:F2:55	Hostname TA001029 ta002171 Tze-Pingde Tyronetki	other C addi ^C all me ^{DrayTek} DrayTek DrayTek Apple	ssiD staffs_4F staffs_4F staffs_4F	poin he d ces.	t via wirel evice that evice that 68%(63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-68dBm)	ess lin the A	nk. P connec pps) RxRate(Kbps) 0 0 0 0 0 0 0 0 0 0 0 0 0
	group and it cor Uplink – Display to. Display the stati Station List of All Devices I 00:50:7F:F0:00:72 2 00:50:7F:F0:01:10 3 5::97:F3:03:05:F7 4 40:98:AD:5B:F2:52 5 00:50:77:37:67:0E:5 6 00:50:77:37:67:0E:5	Hostname TA001029 ta002171 Tze-Pingde Tyronetkii N/A	other C addi ^c all me DrayTek Apple DrayTek DrayTek DrayTek	ssip staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	poin he d ces.	t via wirel evice that 68%(-63dBm) 10% (-49dBm) 55%(-66dBm) 55%(-66dBm) 55%(-66dBm) 83%(-57dBm)	ess lin the A	nk. P connec ^{Dps)} RxRate(Kbps) 0 0 0 0 0 0 0 0 0 0 0 0 0
	group and it cor Uplink – Display to. Display the stati station List of All Devices Index MAC Address 1 00/50:7F:F0:C9:72 2 00:50:7F:F0:C9:72 3 5C:97:F3:03:D5:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:67:E8 7 30:F7:51:D1:3D11	hnects to y the MA ion list of TA001029 ta002171 Tze-Pingde Tyronetki N/A N/A	other C addi C a	saccess ress of tl esh devi staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	ces.	t via wirel evice that 68%(-63dBm) 41%(-73dBm) 100% 5%(-68dBm) 55%(-68dBm) 55%(-68dBm) 35%(-75dBm) 34%(-75dBm) 100%	ess lin the A	hk. P connec bps) RxRate(Кbps) 0 0 0 0 0 12
	group and it cor Uplink – Display to. Display the stati Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:72 2 00:50:7F:F0:D1:1D 3 5::97:F3:D3:D5:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:60:E5 6 00:50:7F:37:60:E5 6 00:50:7F:37:60:E5 9 18:65:90:DE:D4:E5	Hostname TA001029 ta002171 Tze-Pingde N/A N/A N/A N/A	other C adda F all ma DrayTek Apple DrayTek Apple DrayTek Apple LiteonTe Apple	ssin staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	ces.	t via wirel evice that 68%(-63dBm) 10% (-49dBm) 55%(-68dBm) 55%(-68dBm) 55%(-68dBm) 34%(-75dBm) 100% (-44dBm)	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec
	group and it cor Uplink – Display to. Display the stati station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:72 2 00:50:7F:F0:D11D 3 5C:97:F3:D3:D5:F7 4 00:98:AD:5B:F2:52 5 00:50:7F:37:60:E5 6 00:50:7F:37:60:E5 7 30:F7:22:E8:A0 9 18:65:90:DE:D4:E5 10 60:45:C8:57:1F:36	hnects to y the MAd ion list of Hostname TA001029 ta002171 Tze-Pingde Yronetkii N/A N/A N/A N/A	other C addi all me DrayTek DrayTek Apple DrayTek Apple LiteonTe Apple N/A	saccess ress of the staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	ces.	t via wirel evice that 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-68dBm) 55%(-68dBm) 34%(-76dBm) 100% (-44dBm) 15%(-44dBm)	ess lin the A TxRate(K) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec
	group and it cor Uplink – Display to. Display the stati Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:72 2 00:50:7F:F0:D1:1D 3 5::97:F3:D3:D5:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:60:E5 6 00:50:7F:37:60:E5 6 00:50:7F:37:60:E5 9 18:65:90:DE:D4:E5	Hostname TA001029 ta002171 Tze-Pingde N/A N/A N/A N/A	other C adda F all ma DrayTek Apple DrayTek Apple DrayTek Apple LiteonTe Apple	ssin staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	ces.	t via wirel evice that 68%(-63dBm) 10% (-49dBm) 55%(-68dBm) 55%(-68dBm) 55%(-68dBm) 34%(-75dBm) 100% (-44dBm)	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	hk. P connec
	group and it cor Uplink – Display to. Display the stati Station List of All Devices I 00:50:7F:F0:02:72 2 00:50:7F:F0:01:10 3 5::97:F3:76:7E 4 40:96:AD:58:F2:52 5 00:50:77:37:67:E 6 00:50:77:37:67:E 7 30:F7:C5:1D:301:11 8 40:F0:C5:1D:301:11 8 40:F0:C5:1D:301:11 9 18:65:90:DE:D4:E5 10 60:45:C8:F7:1F:36 12 50:8C:96:E0:00:11	Hostname TA001029 ta002171 Tze-Pingde Tyronetkii N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	other C addi all mo C addi C addi C addi DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple	ssio staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	Channe Ces. Channe 6 6 6 6 6 6 6 6	t via wirel evice that 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-68dBm) 55%(-68dBm) 83%(-57dBm) 100% (-44dBm) 10%(-84dBm) 11%(-62dBm) 71%(-62dBm)	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec
	group and it cor Uplink – Display to. Display the stati Index MAC Address 1 00:50:7F:F0:29:72 2 00:50:7F:F0:1110 3 5C:97:F3:03:D5:F7 4 40:98:AD:5B:F2:52 5 00:50:77:37:67:DE5 6 00:50:77:37:67:DE5 7 30:F7:C5:1D:3D:D1:11 8 40:F0:2F:22:EB:A0 9 18:65:90:DE:D4:E5 10 60:45:CB:57:1F:36 11 AC:5F:3E:62:E6:001 12 50:BC:66:E0:011 13 04:B1:67:52:48:90	Hostname TA001029 ta002171 Tze-Pingde Tyronetkii N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	other C addi C a	staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	Ces. Channe 6 6 6 6 6 6 6 6 6 6	t via wirel evice that 68%(-63dBm) 41%(-73dBm) 100% (-44dBm) 55%(-68dBm) 55%(-68dBm) 55%(-68dBm) 10% (-44dBm) 13%(-54dBm) 13%(-54dBm) 13%(-54dBm) 13%(-54dBm)	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec
	group and it cor Uplink – Display to. Display the stati Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:110 3 5C:97:F3:D3:D5:F7 4 40:98:AD:5B:F2:52 5 00:50:7F:37:60:E110 3 5C:97:F3:C0:E5 6 00:50:7F:37:67:E8 7 30:F7:C5:10:30:11 8 40:F0:2F:22:E8:A0 9 18:65:90:0E:04:E5 10 60:45:CB:57:1F:36 11 AC:5F:3E:62:E6:00 12 50:BC:96:E0:00:111 13 04:B1:67:52:48:90 14 04:C2:3E:3F:CB:F8	Hostname TA001029 ta002171 Tze-Pingde V/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N	other C addi C addi C addi C addi C addi DrayTek DrayTek DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple N/A Apple N/A Apple N/A	ssip staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	Ces. Channet Ces. Channet 6 6 6 6 6 6 6 6	t via wirel evice that 68%(-63dBm) 10% (-49dBm) 55%(-69dBm) 55%(-69dBm) 10% (-44dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 55%(-64dBm) 55%(-64dBm) 55% (-64dBm) 55%(-6	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec
	group and it cor Uplink – Display to. Display the stati Station List of All Devices I 00:50:7F:F0:09:72 2 00:50:7F:F0:D1:1D 3 5C:97:F37:60:E5 6 00:50:7F:37:60:E5 6 00:50:77:37:67:E6 7 30:F7:25:22:E8:A0 9 18:65:90:DE:D4:E5 10 60:45:C8:57:1F:36 11 AC:5F:3E:62:E6:0D 12 50:8C:96:E0:00:11 3 04:B1:67:52:48:90 14 04:C2:3E:3F:C8:F8 15 0c:88:F0:31:08:78	Hostname TA001029 ta002171 Tze-Pingde V/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N	other C addi C a	ssip staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	Ces. Channe 6 6 6 6 6 6 6 6 6 6	t via wirel evice that 6%%(-63dBm) 100% (-49dBm) 5%(-68dBm) 5%(-68dBm) 3%(-57dBm) 10% (-44dBm) 15%(-68dBm) 10% (-44dBm) 15%(-68dBm) 2%(-55dBm) 55%(-68dBm) 55%(-68dBm) 55%(-68dBm)	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec
	group and it cor Uplink – Display to. Display the stati Station List of All Devices I 00:50:7F:F0:09:72 2 00:50:7F:F0:D1:1D 3 5C:97:F37:60:E5 6 00:50:7F:37:60:E5 6 00:50:77:37:67:E6 7 30:F7:25:22:E8:A0 9 18:65:90:DE:D4:E5 10 60:45:C8:57:1F:36 11 AC:5F:3E:62:E6:0D 12 50:8C:96:E0:00:11 3 04:B1:67:52:48:90 14 04:C2:3E:3F:C8:F8 15 0c:88:F0:31:08:78	Hostname TA001029 ta002171 Tze-Pingde V/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N	other C addi C addi C addi C addi C addi DrayTek DrayTek DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple N/A Apple N/A Apple N/A	ssip staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	Ctess. Ctess. Cteannue 6 6 6 6 6 6 6 6	t via wirel evice that 68%(-63dBm) 10% (-49dBm) 55%(-69dBm) 55%(-69dBm) 10% (-44dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 10% (-64dBm) 55%(-64dBm) 55%(-64dBm) 55% (-64dBm) 55%(-6	ess lin the A	nk. P connec
	group and it cor Uplink – Display to. Display the stati station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:110 3 5C:97:F3:D3:D5:F7 4 40:98:A0:58:F7:E25 5 00:50:7F:37:60:E5 7 30:F7:C5:D13:D11 8 40:F0:2F:22:E8:A0 9 18:65:90:DE:D4:E5 10 60:45:E8:F7:IF:36 11 AC:5F:3E:62:E6:00 12 50:8C:96:E9:00:111 13 04:8B:167:52:48:90 14 04:C2:3E:BF:R6:C8 15 00::88:FD:31:08:77 16 58:48:22:E8:F8:62 17 CC:9F:7A:63:11:27 18 20:47:N4:58:17:79 18 20:47:N4:58:17:79 18 20:47:N4:58:17:79 18 20:47:N4:58:17:79 18 20:47:N4:58:17:79 19 20:47:N4:58:17:79 10 58:48:22:E8:F8:62 10 00:45:E8:F7:E1:58 10 00:28:FD:31:08:78 10 00:45:E8:F7:E1:58 10 00:45:E8:F7:E1:58 10 00:45:E8:F7:E1:58 10 00:45:E8:F7:E1:58 10 00:45:E8:F7:E1:58 10 00:45:E8:F7:E1:58 10 00:45:E8:F7:E1:58 10 00:45:E8:F7:E1:58 10 00:45:E8:F8:59 10	Hostname TA001029 ta002171 Tze-Pingde N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	other C addi C a	staffs_4F staffs_4Fstaffs_4F staffs_4F staffs_4F staffs_4Fstaffs_4F staffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs	Ces. Channe 6 6 6 6 6 6 6 6 6 6 6 6 6	t via wirel evice that 68%(-63dBm) 100% (-49dBm) 55%(-69dBm) 55%(-69dBm) 55%(-64dBm) 10% (-44dBm) 11%(-44dBm) 15%(-44dBm) 15%(-64dBm) 55%(-66dBm) 25%(-66dBm) 25%(-66dBm) 25%(-66dBm)	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec
	group and it cor Uplink – Display to. Display the stati Station List of All Devices I 00:50:7F:F0:00:72 2 00:50:7F:F0:01:10 3 5::97:F3:30:55:F7 4 40:96:AD:58:F2:52 5 00:50:77:37:67:BE 7 30:F7:C5:1D:301:11 8 40:F0:C5:1D:301:11 8 40:F0:C5:1D:301:11 8 40:F0:C5:1D:301:11 8 40:F0:C5:1D:301:11 8 40:F0:C5:1D:301:11 13 04:81:67:52:48:90 14 04:C2:3E:3F:CB:F8 15 00:88:FD:31:08:F8 15 00:88:FD:31:08:F8 15 00:88:FD:31:08:F8 15 00:88:FD:31:08:F8 15 00:88:FD:31:08:F8 16 95:84:82:2E:BF:F8:62 17 CC:9F:74:63:11:27 17 CC:9F:74:63:11:27 1	Hostname TA001029 ta002171 Tze-Pingde N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	other C addi C a	ssio staffs_4F s	Chamme 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	t via wirel evice that 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-66dBm) 55%(-66dBm) 83%(-57dBm) 100% (-44dBm) 15%(-64dBm) 81%(-58dBm) 81%(-58dBm) 81%(-53dBm) 55%(-66dBm) 55%(-66dBm) 55%(-66dBm)	ess lin the A 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connec

II-4-3 Mesh Discovery

Before a Mesh Node is connected, it is unable to check the device status from Mesh Root. This page can help to discover all Mesh devices around and offer the Link Status and Operation Mode of each Mesh device.

Device List						
ndex	MAC Address	Model	Operation Mode	Link Status	RSSI	
1	00:1D:AA:80:FE:CC	VigorAP1060C	MeshRoot	Connected	-36dBm(excellent)	
2	14:49:BC:42:7D:B0	VigorAP960C	MeshNode(Wireless)	Connected	-31dBm(excellent)	
3	00:1D:AA:04:F0:C4	VigorAP1000C	MeshNode(Wireless)	Connected	-85dBm(weak)	
4	00:1D:AA:06:34:95	VigorAP960C	AP		-66dBm(good)	
5	00:1D:AA:18:EE:C0	Vigor2765	MeshRoot	Connected	-67dBm(good)	
6	00:1D:AA:52:E5:30	VigorAP960C	AP		-69dBm(good)	
7	00:1D:AA:91:2C:15	VigorAP912C	AP		-66dBm(good)	
8	00:1D:AA:58:69:74	VigorAP1060C	AP		-57dBm(good)	
9	00:1D:AA:04:F0:54	VigorAP1000C	AP		-66dBm(good)	

For obtaining the list of devices around this VigorAP, click **Scan**. Later, surrounding VigorAP device(s) will be displayed on this page.

II-4-4 Basic Configuration Sync

If you add one Mesh Node in a mesh group, the Mesh Root will send the basic configuration to the device. This page could help you to change the Mesh Root settings and deliver the new configuration of the Mesh Root to all "connected" Mesh Nodes.

incom PP	Basic Configuration Sync	
Sele	ct All	
Syst	em Maintenance	
Index	Name	Value
1	ManagementServer.URL	
2	ManagementServer.Username	
3	ManagementServer.Password	******
4	ManagementServer.ConnectionReguestUsername	vigor
5	ManagementServer.ConnectionRequestPassword	password
6	X_00507F_System.Management.SkipQuickStartWizard	Enable
7	X_00507F_System.TR069Setting.CPEEnable	0
8	X_00507F_System.AdminmodePassword.Admin	admin
9	X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable	0
10	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
11	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
12	X_00507F_System.SyslogMail.SysLogAccess.LogLevel	
13	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
14	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
15	X_00507F_System.SyslogMail.MailAlert.MailTo	
16	X_00507F_System.SyslogMail.MailAlert.MailFrom	
17	X_00507F_System.SyslogMail.MailAlert.Username	
18	X_00507F_System.SyslogMail.MailAlert.Password	*****
19	X_00507F_System.SyslogMail.MailAlert.UseTLS	1
20	X_00507F_System.SyslogMail.MailAlert.AdminLoginAlertEn	1
21	X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	
22	X_00507F_System.AdminmodePassword.Password	*****
Wire	eless LAN (2.4GHz)	
Index I	Vame	Value
	X_00507F_WirelessLAN_AP.General.EnableWLAN	1
	X 00507F WirelessLAN AP.General.SSID.1.ESSID	DravTek-3FB230
	X 00507F WirelessLAN AP.General.SSID.1.Enable	1
	X 00507F WirelessLAN AP.General.SSID.1.Hide	ō
	X 00507F WirelessLAN AP.General.SSID.1.IsolateLAN	ő
6	X 00507F WirelessI AN AP General SSID 1 IsolateMember	0

Available settings are explained as follows:

ltem	Description
System Maintenance /	Check the item(s) you want to make configuration sync.
Wireless LAN (2.4Hz) /	Apply – Click it to apply the settings configured by such AP to all connected mesh node. Note that this button is available only
Wireless LAN (5GHz)	when such AP is in mesh root mode.

Tips for Mesh Network Setup

- Set up TWO mesh devices with uplink RSSI larger than -65dBm.
- Upgrade the firmware version of Mesh devices through Mesh link, starting from the mesh device with less hop number. For example, upgrade the firmware from the root, hop1 Mesh Node then hop2 Mesh Node, and so on.
- VigorMesh network supports up to 3 hops of mesh devices. However, it is suggested to connect the mesh group with less than or equals to 2 hops.

For your reference, we make a real mesh environment test and get the following record. (Use VigorAP APP to do internet speed test with different hops mesh node.)

Internet Download Speed (for root and hop1 ~ hop3):iPad connects to Root: 80MbpsiPad connects to hop1 Node: 49Mbps (Uplink RSSI : -55dBm)iPad connects to hop2 Node: 41Mbps (Uplink RSSI : hop2 -64dBm / hop1 -55dBm)

iPad connects to hop3 Node : 26Mbps (Uplink RSSI : hop3 -62dBm / hop2 -68dBm / hop1 -55dBm)

- It is not suggested to use a wireless Mesh Node with Ethernet cable connected to a Mesh Root.
- If resetting a Mesh Root,
 - All "connected" Mesh Nodes will be informed to reset.
 - Group List and Group Key will be reset, too.
 - For those Mesh Nodes unable to reset, reset them manually. Reset the Group List by web or factory default.
- If resetting a Mesh Node,
 - Group List and Group Key will be cleared.
 - Link Status will become "New".
- Mesh network status also can be viewed and checked through the dashboard by clicking MESH NETWORK.

MESH NETWORK			~ 88	Memory Usage	23%
ROOT	VigorAP903 VigorAP903	001DAAA62601 Ethernet	7 0 Node Offline	WIRELESS OVERVIEW	
	AlbertCSeat VigorAP903 001DAA223355	-50 dBm 100% 🗢	Ch.153 001DAAA62601 Wireless 5GHz	2.4GHz MAC 02	able 0 1D:AA:C6:26:01 903_Field_117
	BigMeetingRoom VigerAP903 00507FF0D4B2	-63 dBm 68% 穿	Ch. 153 001DAA223355 Wireless 5GHz	5GHz MAG 00:	able // 1D:AA:A6:26:01 903 Field 117
	CleanBlock VigerAP903 001DAA288072	-65 dBm 63% 👳	Ch.153 00507FF0D482 Wireless SGHz		
	ExitDoor VigerAP920R 001DAA78C920	-68 dBm 55% 🖙	Ch. 153 001DAA223355 Wireless 5GHz		

- If Mesh Search / Apply / Discover is worked too fast or is done with empty result, your request may be rejected. Please try again.
- Troubleshooting:
 - Check the firmware version. Please make sure all APs within the mesh group are in the newest firmware version.
 - Check the OP (operation) Mode. Make sure new Mesh Node doesn't accidentally get DHCP IP and becomes AP mode.
 - Check the country code and channels. For example, it is impossible for connecting a VigorAP 918R Mesh Root with 5G channel 36 to VigorAP920R Wireless Mesh Node in EU country code.
 - Check the channel load. Make sure it is not over 70%.



Collect some Mesh logs and send the result to DrayTek for analyzing.

-

Dray	Tek		Syslog Uti	ility
■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		- (ABR	172.17.3.6 WAN 貸田 AP9008 WAN I LAN 資田 中正 博送地名 接收以合金 WAN IP (図)E) M用 P 9756 47236	会 牧速率
(C) 10000 (0/114)	117 NALDE COMPANY	e round	HIG6027 7110	
			□暫停	
系统時間	路由器時間	主機	□ 暫停 訊息	
	路由器 时間 Nov 8 10:58:05	主機 syslog	iRe	-
2018-11-08 19:01:16				-
2018-11-08 19:01:16 2018-11-08 19:01:15	Nov 8 10:58:05	syslog	IR8 [dm] dm_pkt_recv Amounce-Keepalve	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:04	Nov 8 10:58:05 Nov 8 10:58:04	syslog syslog	IR.8 [dwn] dwn_pit_recv Announce-Keepalive [dwn] dwn_pit_send Alive [dwn] dwn_pit_send Alive [dwn] dwn_pit_recv Announce-Keepalive	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:04 2018-11-08 19:01:04 2018-11-08 19:01:01	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52	syslog syslog syslog	IRB [dm:] dm:_pit_recv Announce-Keepalve [dm:] dm:_pit_send Alve [dm:] dm:_pit_recv Announce-Keepalve [dm:] dm:_pit_recv Announce-Keepalve [Tr253:35554] [dm:] Mesh IR Record (Solate) 00:10:AA-5C:A6-CB	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:04 2018-11-08 19:01:04 2018-11-08 19:01:01 2018-11-08 19:00:59	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50 Nov 8 10:57:48 Nov 8 10:57:41	syslog syslog syslog syslog	IFL8 [dwn] dwn_pit_recv Announce-Keepalive [dwn] dwn_pit_send Alve [dwn] dwn_pit_send Alve [dwn] dwn_pit_send Alve [dwn] dwn_pit_recv Announce-Keepalive [7535.335564] [dwn] Mesh IE Record (Isolate) 00:1D-AA:5C:A6:C8 [dm] dwn_pit_send Alve	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:04 2018-11-08 19:01:01 2018-11-08 19:00:59 2018-11-08 19:00:53 2018-11-08 19:00:47	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50 Nov 8 10:57:48	syslog syslog syslog syslog kernel	IRB [dm] dm_pit_recv Announce-Keepalive [dm] dm_pit_send Alive [dm] dm_pit_send Alive [dm] dm_pit_recv Announce-Keepalive [dm] dm_pit_recv Announce-Keepalive [dm] dm_pit_send Alive [dm] dm_pit_recv Announce-Keepalive	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:04 2018-11-08 19:01:01 2018-11-08 19:00:59 2018-11-08 19:00:53 2018-11-08 19:00:47	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50 Nov 8 10:57:48 Nov 8 10:57:41 Nov 8 10:57:41 Nov 8 10:57:30	syslog syslog syslog kernel syslog syslog syslog	Eta [dwn] dwn, pikt_recv Announce-Keepalve (dwn] dwn, pikt_send Alve (dwn] dwn, pikt_send Alve (dwn] dwn, pikt_recv Announce-Keepalve [7523:332564] [dwn] Mesh IE Record (Solate) 00:10-AA:5C:A6:C8 [dwn] dwn, pikt_recv Announce-Keepalve [dwn] dwn, pikt_recv Announce-Keepalve [dwn] dwn, pikt_recv Announce-Keepalve [dwn] dwn, pikt_recv Announce-Keepalve	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:01 2018-11-08 19:01:01 2018-11-08 19:00:05 2018-11-08 19:00:53 2018-11-08 19:00:47 2018-11-08 19:00:41 2018-11-08 19:00:41	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50 Nov 8 10:57:56 Nov 8 10:57:36 Nov 8 10:57:36 Nov 8 10:57:30 Nov 8 10:57:30	syslog syslog syslog kernel syslog syslog syslog syslog kernel	IBB [dm:] dm:_pit_recv Announce-Keepalive [dm:] dm:_pit_send Alive [dm:] dm:_pit_recv Announce-Keepalive [dm:] dm:_pit_recv Announce-Keepalive [Tr253:35254] [dm:] dms:] Record (Isolate) 00:1D:AA:5C:A6:C8 [dm:] dm:_pit_recv Announce-Keepalive [dm:] dm:_pit_recv Announce-Keepalive [dm:] dm:_pit_recv Announce-Keepalive [dm:] dm:_pit_recv Announce-Keepalive [dm:] dm:_pit_recv Announce-Keepalive [dm:] dm:_pit_recv Announce-Keepalive	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:04 2018-11-08 19:01:01 2018-11-08 19:00:59 2018-11-08 19:00:53 2018-11-08 19:00:47 2018-11-08 19:00:41 2018-11-08 19:00:39 2018-11-08 19:00:39	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50 Nov 8 10:57:40 Nov 8 10:57:40 Nov 8 10:57:36 Nov 8 10:57:36 Nov 8 10:57:28 Nov 8 10:57:22	syslog syslog syslog kernel syslog syslog syslog ikernel syslog	Eta Edwin Jam, jult, Jess' Announce-Keepalve dmn Jam, jult, send Alve dmn Jam, jult, send Alve dmn Jam, jult, send Alve dmn Jam, jult, ress' Announce-Keepalve T7525.3255441 [dmn] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8 [dmn] dmn, jult, send Alve [mn] dmn, ju	ĺ
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:04 2018-11-08 19:01:01 2018-11-08 19:00:59 2018-11-08 19:00:53 2018-11-08 19:00:47 2018-11-08 19:00:41 2018-11-08 19:00:39 2018-11-08 19:00:39	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50 Nov 8 10:57:48 Nov 8 10:57:48 Nov 8 10:57:30 Nov 8 10:57:30 Nov 8 10:57:22 Nov 8 10:57:29	syslog syslog syslog kernel syslog syslog syslog syslog kernel	[dm] dm_plt_recv Announce-Keepalive [dm] dm_plt_recv Announce-Keepalive [dm] dm_plt_send Alive [dm] dm_plt_recv Announce-Keepalive	ĺ
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:01 2018-11-08 19:01:01 2018-11-08 19:00:53 2018-11-08 19:00:53 2018-11-08 19:00:47 2018-11-08 19:00:39 2018-11-08 19:00:39 2018-11-08 19:00:30 2018-11-08 19:00:30	Nov 8 10:58:05 Nov 8 10:57:50 Nov 8 10:57:50 Nov 8 10:57:50 Nov 8 10:57:41 Nov 8 10:57:41 Nov 8 10:57:41 Nov 8 10:57:36 Nov 8 10:57:28 Nov 8 10:57:29 Nov 8 10:57:29 Nov 8 10:57:29	syslog syslog syslog syslog syslog syslog syslog syslog syslog syslog syslog syslog syslog syslog	ERB End dnn, pikt_recv Announce-Keepalve dnn) dnn, pikt_send Alve dnn) dnn, pikt_send Alve dnn) dnn, pikt_recv Announce-Keepalve TX523.3255441 [dnn) Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8 (mn) dnn, pikt_recv Announce-Keepalve (dnn) dnn, pikt_recv Announce-Keepalve [dnn) dnn, pikt_recv Announce-Keepalve [dnn] dnn, pikt_recv Announce-Keepalve	
2018-11-08 19:01:16 2018-11-08 19:01:15 2018-11-08 19:01:01 2018-11-08 19:01:01 2018-11-08 19:00:59 2018-11-08 19:00:59 2018-11-08 19:00:41 2018-11-08 19:00:41 2018-11-08 19:00:33 2018-11-08 19:00:30	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50 Nov 8 10:57:48 Nov 8 10:57:48 Nov 8 10:57:30 Nov 8 10:57:30 Nov 8 10:57:22 Nov 8 10:57:29	syslog syslog syslog syslog kernel syslog syslog kernel syslog syslog syslog syslog	[dm] dm_plt_recv Announce-Keepalive [dm] dm_plt_recv Announce-Keepalive [dm] dm_plt_send Alive [dm] dm_plt_recv Announce-Keepalive	

II-4-5 Advanced Config Sync

If you add one Mesh Node in a mesh group, the Mesh Root will synchronize the advanced configuration to the device based on the setting results on this page.

lesh≯	> Advanced Configuration Sync	
Se	lect All	
В	idge VLAN to Mesh	
Index	Name	Value
1	X_00507F_LAN.GeneralSetup.BridgeVLANtoWDS	Enable
	aaming Name	Value
1	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.EnMinBasicRate	0
2	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinBasicRate	1Mbps
3	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.RSSI	Disable_RSSI_Requirement
4	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.StrictlyRSSISignal	73
5	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinRSSISignal	66
6	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	5
7	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.Enable	0
8	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.CachePeriod	10
9	X_00507F_WirelessLAN_AP.Roaming.FastTransitionRoaming.Enable	0
10	X_00507F_WirelessLAN_AP.Roaming.FastTransitionRoaming.DsOrAir	1
11	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.EnMinBasicRate	0
12 13	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinBasicRate X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.RSSI	6Mbps Disable RSSI Requirement
13	X 00507F WirelessLAN_5G AP.Roaming.APAClientRoaming.KSSI X 00507F WirelessLAN_5G AP.Roaming.APAClientRoaming.StrictlyRSSISignal	73
15	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinRSSISignal	66
16	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	5
17	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.Enable	9
18	X 00507F WirelessLAN 5G AP.Roaming.FastRoaming.CachePeriod	10

Available settings are explained as follows:

Item Description	
Select All	All item(s) will be selected for making configuration sync.
Bridge VLAN to Mesh	Check to transmit the packets with VLAN tag to mesh nodes.

II-4-6 Support List

Mesh >> Support List

The following compatibility test lists Draytek AP models supported by this AP Mesh.

Model	Status	Firmware Version	
VigorAP 903	Y	1.3.7	
VigorAP 912C	Y	1.3.5	
VigorAP 918R	Y	1.3.4	
VigorAP 920R	Y	1.3.4	
VigorAP 960C	Y	1.4.0	
VigorAP 1060C	Y	1.3.8	

Y:Tested and is supported. N:Not supported.

II-4-7 Mesh Syslog

Mesh >> Mesh Syslog

Moch	Inform	ation

Mesh Log Information	1	Clear	T	Refresh	I.	Line v	vrap
Apr 28 13:43:20 kernel: [11850.898534] [dmn] Mesh IE Record (Backhaul) 00:1D:AA	80:	FE:D5					
Apr 28 13:43:20 kernel: [11850.898592] [dmn] Mesh IE Record (Backhaul) 00:50:7F:	F1:7	7F:1D					
Apr 28 13:43:21 kernel: [11851.119521] [dmn] Mesh IE Record (Backhaul) 00:1D:AA	80:	FE:CO					
Apr 28 13:43:21 kernel: [11851.119611] [dmn] Mesh IE Record (Advertise) 00:1D:AA	7C	F5:A5					
Apr 28 13:43:21 kernel: [11851.119669] [dmn] Mesh IE Record (Backhaul) 00:1D:AA	7C:	F5:BD					
Apr 28 13:43:21 kernel: [11851.119727] [dmn] Mesh IE Record (Backhaul) 14:49:BC:	17:	70:08					
Apr 28 13:43:21 kernel: [11851.119785] [dmn] Mesh IE Record (Backhaul) 00:1D:AA	80:	FE:D5					
Apr 28 13:43:21 kernel: [11851.119843] [dmn] Mesh IE Record (Backhaul) 00:50:7F:	F1:7	F:1D					
Apr 28 13:43:22 kernel: [11852.224281] [dmn] Mesh IE Record (Backhaul) 00:1D:AA	80:	FE:D4					
Apr 28 13:43:22 kernel: [11852.447742] [dmn] Mesh IE Record (Backhaul) 00:1D:AA	80:	FE:D4					
Apr 28 13:43:23 kernel: [11853.110516] [dmn] Mesh IE Record (Backhaul) 14:49:BC:	02::	38:48					
Apr 28 13:43:23 kernel: [11853.331662] [dmn] Mesh IE Record (Backhaul) 14:49:BC:	02:	38:48					
Apr 28 13:43:23 kernel: [11853.773637] [dmn] Mesh IE Record (Advertise) 00:1D:AA	:63:	2C:00					
Apr 28 13:43:23 kernel: [11853.773714] [dmn] Mesh IE Record (Advertise) 00:1D:AA	:63:	20:01					
Apr 28 13:43:23 kernel: [11853.773774] [dmn] Mesh IE Record (Advertise) 00:1D:AA	:04:	F0:6E					
Apr 28 13:43:24 kernel: [11853.994690] [dmn] Mesh IE Record (Advertise) 00:1D:AA	:63:	2C:00					
Apr 28 13:43:24 kernel: [11853.994767] [dmn] Mesh IE Record (Advertise) 00:1D:AA	:63:	2C:01					

II-5 Universal Repeater Settings for Range Extender Mode

When you choose **Range Extender** as the operation mode, the Wireless LAN menu items (for 2.4GHz and 5GHz) will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, WDS AP Status, Universal Repeater, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering and Station List.

This section will introduce settings for Universal Repeater only.

For other wireless setting items (e.g., General Setup, Security, WPS, and etc.), please refer to II-3.

General Setup	General Setup
Security	Security
Access Control	Access Control
WPS	WPS
Advanced Setting	Advanced Setting
AP Discovery	AP Discovery
WDS AP Status	WDS AP Status
Universal Repeater	Universal Repeater
Bandwidth Management	Bandwidth Management
Airtime Fairness	Airtime Fairness
Station Control	Station Control
Roaming	Roaming
Band Steering	Station List
Station List	

The following figure shows how VigorAP runs as Range Extender:



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.

(i) 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 AP mode.

Wireless LAN (2.4GHz) >> Universal Repeater

Universal Repeater Parameters	
SSID	
MAC Address (Optional)	
Channel	2462MHz (Channel 11) $$
Security Mode	WPA2 Personal V
Encryption Type	AES 🗸
Pass Phrase	
Range Extender Band	None
Note: If Channel is modified, the Chann	el setting of AP would also be changed.

Universal Repeater IP Configuration

Connection Type	DHCP 🗸
Device Name	AP918R
	OK Cancel

Available settings are explained as follows:

ltem	Description				
Universal Repeater Parameters					
SSID	Display the SSID defined for Range Extender operation mode in Quick Start Wizard. Change the name of SSID whenever you want.				
MAC Address (Optional)	Type the MAC address of access point that VigorAP 918R wants to connect to.				
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.				
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.				

	WPA2 Personal V WPA2 Personal V WPA Personal Shared
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 Personal and WPA2 Personal	This option is available when WPA Personal or WPA2 Personal is selected as Security Mode . Select TKIP or AES as the algorithm for WPA.
Pass Phrase	Type 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
Range Extender Band	Display which wireless band (2.4G/5G) is currently used for Universal Repeater. None - No network connection.
Universal Repeater IP Co	onfiguration
Connection Type	Choose DHCP or Static IP as the connection mode. DHCP – The wireless station will be assigned with an IP from VigorAP. Static IP – The wireless station shall specify a static IP for connecting to Internet via VigorAP.
Device Name	This setting is available when DHCP is selected as Connection Type . Type a name for the VigorAP as identification. Simply use the default name.
IP Address	This setting is available when Static IP is selected as Connection Type . Type an IP address with the same network segment of the LAN IP setting of VigorAP. Such IP shall be different with any IP address in LAN.
Subnet Mask	This setting is available when Static IP is selected as Connection Type . Type the subnet mask setting which shall be the same as the one configured in LAN for VigorAP.
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 VigorAP.
--

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

II-6 LAN

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



II-6-1 General Setup

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



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

Ethernet TCP / IP and DHC	.P Setup	
LAN IP Network Configur	ation	DHCP Server Configuration
Enable DHCP Client		🔾 Enable Server 🔾 Disable Server
IP Address	172.17.3.97	🔿 Relay Agent
Subnet Mask	255.255.255.0	WLAN Trusted DHCP Server Server IP Address
Default Gateway	172.17.3.253	
Enable Management	VLAN	
VLAN ID	0	
DNS Server IP Address		-
Primary IP Address		
Secondary IP Address		

Available settings are explained as follows:

ltem	Description				
LAN IP Network Configuration	Enable DHCP Client – When it is enabled, VigorAP 918R will be treated as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2865).				
	IP Address – Type in private IP address for connecting to a local private network (Default: 192.168.1.2).				
	Subnet Mask – Type in an address code that determines the size of the network (Default: 255.255.255.0/ 24).				
	Default Gateway - Type in an IP address. Traffic will be sent to the default gateway address of the specified interface.				
	Enable Management VLAN – VigorAP 918R supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 918R.				
	 VLAN ID – Type the number as VLAN ID tagged on the transmitted packet. "0" means no VALN tag. 				
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client.				
	Enable Server - Enable Server lets the modem assign IP address to every host in the LAN.				
	• Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254.				
	 End IP Address - Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses. 				
	• Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)				
	 Default Gateway - Enter a value of the gateway IP address for the DHCP server. 				
	• Lease Time - It allows you to set the leased time for the specified PC.				
	 Primary 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 IF 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. 				
	Relay Agent - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.				
	• DHCP 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.				
	Disable Server - Disable Server lets you manually or use other DHCP				

	server to assign IP address to every host in the LAN.
	• WLAN Trusted DHCP Server — 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.
DNS Server IP Address	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.

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

II-6-2 Hotspot Web Portal

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

LAN >> Hotspot Web Portal

Hotspot Web Portal Profile:						
Index	Enable	Comments	Login Mode	Applied Interface		
1			None			

Note: AP must connect to the Internet otherwise Web Page redirection won't work.



Available settings are explained as follows:

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

Click the index number (e.g., #1 in this case) to open the setting pages.

(1) Hotspot Web Portal Settings

1		3	
Hotspot Web Portal Settings	RADIUS Settings	Whitelist Settings	
Hotspot Web Porta	ıl		
Enable			
Comments			
Portal Server		Captive Portal URL	
		Redirection URL	http:// portal.draytek.com
Landing Page		Fixed URL	
Applied Interfac	es	LAN	LAN (Works on Universal Repeater mode)
		WLAN 2.4GHz	SSID1 (DrayTek-5CA6A0)
			SSID2
			SSID3
			SSID4
		WLAN 5GHz	SSID1 (DrayTek-5CA6A0)
			SSID2
			SSID2
Notes an event			SSID4

Note: AP must connect to the Internet otherwise Web Page redirection won't work.

Save and Next

Available settings are explained as follows:

ltem	Description		
Enable	Check it to enable the hotspot web portal settings.		
Comments Enter a brief description for this profile.			
Portal ServerCaptive Portal URL - Enter the captive portal URL.Redirection URL - Enter the URL to which the client will be red			
Landing page Fixed URL - Enter the URL as the landing page for wire			
Applied Interfaces	LAN - The current Hotspot Web Portal profile will be in effect for the selected LAN.		
	SSID1 to SSID4 - The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.		
Next	Click to access into next page.		

Cancel

After finishing this web page configuration, please click **Next** for next setting page.

(2) RADIUS Settings

Configure the external RADIUS server for mutual authentication.

LAN >>	Hotspot We	eb Portal
--------	------------	-----------

()(2)	3				
lotspot Web RADIUS Portal Settings Settings RADIUS Setup	Whitelist Settings				
Zenable					
Comments Primary Server	authentication				
Primary Server	172.16.3.8				
Secret	•••••				
Autentication Port	1812				
Retry	2 times(1 ~ 3)				
Advanced					
NAS-Identifier					
Note: Secret can contain on	y a-z A-Z 0-9 . < > + = \ ? @ # ~ ` \$ % & / * [] {} ' ^! ()				
Back	Save and Next Cancel				

Available settings are explained as follows:

Item	Description		
Enable	Check it to enable the RADIUS server settings.		
Comments Enter a brief description for this profile.			
Primary ServerEnter the IP address of RADIUS server.			
Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.		
Authentication Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.		
Retry	Set the number of attempts to perform reconnection with RADIUS server.		
Advanced	NAS-Identifier - Enter an ID.		
Next	Click to access into next page.		

After finishing this web page configuration, please click **Next** for next setting page.

(3) Whitelist Settings

Users are allowed to send and receive the traffic that satisfies whitelist settings. IPs under whitelist will not be redirected to other website (URL).

LAN >> Hotspot Web Portal



Settings

Settings

Hotspot Web Portal Settings

	Destination Domain			Destination IP		
	Index	Enable	IP Whitelist	Index	Enable	IP Whitelist
	1		192.168.1.11	2		
	3		192.168.1.12	4		
	5			6		
	7			8		
Ba	ack					Finish Cancel

Available settings are explained as follows:

ltem	Description
Destination Domain	
Enable	Check to enable the setting.
Domain Whitelist	Enter a domain (URL) / an IP address.
Destination IP	
Enable	Check to enable the setting.
IP Whitelist	LAN users with the IPs set in this page are able to access into Internet without entering other portal.
Finish	Click to save the settings.

After finishing this web page configuration, please click **Finish** to complete the configuration.

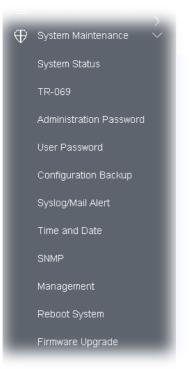
Chapter III Management



III-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, TR-069, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



III-1-1 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.

del vice Name mware Version ild Date/Time stem Uptime eration Mode	: VigorAP9 : VigorAP9 : 1.4.6 : g1556_29 : 1d 03:09: : AP	3R If48da6 Fri, 24 Feb 2023 14:32:	21
	System		LAN
Memory Total	: 236776 kB	MAC Address	: 00:1D:AA:3F:B2:30
Memory Left	: 90804 kB	IP Address	: 192.168.1.14
Cached Memor	y : 25584 kB / 236776 kB	IP Mask	: 255.255.255.0
Wirele	55 LAN (2.4GHz)		
MAC Address	: 00:1D:AA:3F:B2:30		
SSID	: DrayTek-3FB230		
Channel	: Auto(5)		
Driver Version	: 10.4		
Wirel	ess LAN (5GHz)		
MAC Address	: 00:1D:AA:3F:B2:31		
SSID	: DrayTek-3FB230		
Channel	: Auto(44)		
Driver Version	: 10.4		

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

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.	
System		
Memory total	Display the total memory of your system.	
Memory left	Display the remaining memory of your system.	
LAN		
MAC Address	Display the MAC address of the LAN Interface.	
IP Address	Display the IP address of the LAN interface.	
IP Mask	Display the subnet mask address of the LAN interface.	
Wireless LAN (2.4GHz/5G	Hz)	
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.	

Each item is explained as follows:

III-1-2 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).

Wizard
Test With Inform Event Code PERIODIC
http://192.168.1.11:8069/cwm/CRN.html
8069
vigor
•••••
y works when Vigor ACS SI is 1.1.6 and above version.
900 second(s)
3478
3478 60 second(s)
60 second(s)
60 second(s)
60 second(s) -1 second(s)
60 second(s) -1 second(s)

Available settings are explained as follows:

ltem	Description
ACS Settings	TR-069 Enable - Select to enable TR-069 settings.
	Wizard – Click it to enter the IP address of VigorACS server host, port number and the handler.
	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.
	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.
	Event Cod e – Use the drop down menu to specify an event to perform the test.
	Last Inform Response Time – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
CPE Settings	Such information is useful for Auto Configuration Server (ACS).
	SSL(HTTPS) Mode - Check the box to allow the CPE client to connect with ACS through SSL.
	Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
	Username/Password – Type the username and password that VigorACS can use to access into such CPE.
Periodic Inform Settings	The default setting is Enable . Please set interval time or schedule tim for the AP to send notification to VigorACS server.
	Interval Time – Type the value for the interval time setting. The unit "second".
STUN Settings	The default is Disable .
	If you click Enable , please type the relational settings listed below:
	Server Address – Type the IP address of the STUN server.
	Server Port – Type the port number of the STUN server.
	Minimum Keep Alive Period – If STUN is enabled, the CPE must sen binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	Maximum Keep Alive Period – If STUN is enabled, the CPE must serbinding 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.
XMPP Settings	XMPP is an abbreviation of Extensible Messaging and Presence Protocol. If your AP register to XMPP server, it could help VigorACS to manage the AP under the NAT at any time, without obstruction.

After finishing this web page configuration, please click ${\bf OK}$ to save the settings.

III-1-3 Administrator Password

This page allows you to set new password for accessing into web user interface of VigorAP.

Administrator Settings

Account	admin
Old Password	
New Password	
Confirm Password	
Password Strength:	Weak Medium Strong
Strong password requirements: 1. Have at least one upper-case letter ar 2. Including non-alphanumeric character	
	only a-z A-Z 0-9 , ~ ` ! @ \$ % ^ * () _ + = {} [] ; < > . ? n only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & * () _ + = {} [] \ ; < > . ? /
	OK Cancel

Available settings are explained as follows:

ltem	Description	
Account	Enter the name for accessing into web user Interface.	
Old Password	Enter the old password for accessing into the web user interface.	
New Password	Enter in new password in this filed.	
Confirm Password	Enter 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.

III-1-4 User Password

System Maintenance >> User Password

This page allows you to set new account and password for accessing the web pages under User Mode.

User Password	
🗹 Enable User Mode	
Account	admin
Password	•••••
Confirm Password	••••••
	in only a-z A-Z O-9 , ~ ` ! @ \$ % ^ * () _ + = {} [] ; < > . ? ain only a-z A-Z O-9 , ~ ` ! @ # \$ % ^ & * () _ + = {} [] \ ;



Available settings are explained as follows:

ltem	Description	
Enable User Mode	After checking this box, you can access into the web user interface with the password typed here for simple web configuration.	
	The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.	
Account	Enter a user name.	
Password	Enter in new password in this field. The length of the password is limited to 31 characters.	
Confirm Password	Enter the new password again.	

Click **OK** to save the settings.

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

III-1-5 Configuration Backup

Such function can be used to backup/restore the VigorAP 918R settings.

Johngun	tion Backup / Restoration
Restorat	on
	Select a configuration file.
	Browse
	Please enter the password and click Restore to upload the configuration file.
	Password (optional): Restore
	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.
	an encrypted file. Protect with password
	Protect with password
	Protect with password Password (Max. 23 characters allowed)

Note: Password can contain only a-z A-Z 0-9 , ! @ \$ % ^ _ - + = {} [] . ? /

Available settings are explained as follows:

ltem	Description	
Restoration	Browse - Click it to specify a file to be restored.	
	Password (optional) – Enter a password for configuration restoration.	
	Restore – Click it to restore the configuration file to VigorAP.	
Backup	Perform the configuration backup of this device.	
	Protect with password- For the sake of security, the configuration file for the access point can be encrypted.	
	Password – Type several characters as the password for encrypting the configuration file.	
	Confirm Password – Type the password again for confirmation.	
	Backup – Click it to backup the configuration file.	

Follow the steps below to backup your configuration.

- 1. Go to System Maintenance >> Configuration Backup.
- 2. If required, check the box of Protect with password and enter the password.
- 3. Click **Backup** to get into the following dialog. The configuration will download automatically to your computer as a file named **config.cfg**.

(i) Note:

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

Follow the steps below to restore your configuration.

- 1. Go to System Maintenance >> Configuration Backup.
- 2. Click **Upload** to choose the correct configuration file for uploading to the AP.
- 3. Click **Restore** and wait for few seconds.

III-1-6 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.

Syslog Access Setup	
Enable	
Server IP Address	
Destination Port	514
Log Level	All
Mail Alert Setup	
Enable	
SMTP Server	
SMTP Server Port	
Mail To	
Mail From	
User Name	
Password	
SSL	
StartTLS	
Enable E-Mail Alert:	
☑ When Admin Login AP	
	OK Cancel

System Maintenance >> Syslog / Mail Alert Setup

Item	Description	
Syslog Access Setup	Enable - Check Enable to activate function of Syslog.	
	Server IP Address - The IP address of the Syslog server.	
	Destination Port -Assign a port for the Syslog protocol. The default setting is 514.	
	Log Level - Specify which level of the severity of the event will be recorded by Syslog.	
Mail Alert Setup	Enable - Check Enable to activate function of mail alert.	
	SMTP Server - The IP address of the SMTP server.	
	SMTP Server Port - Set the port number for the SMTP server.	
	Mail To - Assign a mail address for sending mails out.	

Mail From - Assign a path for receiving the mail from outside.
User Name - Type the user name for authentication.
Password - Type the password for authentication.
SSL - Check this box to encrypt alert mail. However, if the SMTP server specified here does not support SSL protocol, the alert mail with encrypted data will not be received by the receiver.
StartTLS - 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.
Enable E-Mail Alert - VigorAP will send an e-mail out when a user accesses into the user interface by using web or telnet.
When Admin Login AP - Enable/disable the function. When it 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.

Click **OK** to save the settings.

III-1-7 Time and Date

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

System Maintenance >> Time and Date		
Fime Information		
Current System Time	2020 Jan 22 Wed 15:20:53 Inquire Time	
status	NTP time synchronized	
Time Setting		
Enable NTP Client		
Time Zone	(GMT+08:00) China Beijing, Chongqing \sim	
NTP Server	pool.ntp.org Use Default	
Daylight Saving		
NTP synchronization	1 day \sim	
	OK Cancel	

Available parameters are explained as follows:

ltem	Description	
Current System Time	Click Inquire Time to get the current time.	
Enable 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.

III-1-8 SNMP

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

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

System Maintenance >> SNMP		
SNMP Agent		
Enable SNMPv1 / SNMPv2c	Agent	
Get Community	public	
Enable SNMPv3 Agent		
USM User		
Auth Algorithm	No Auth \sim	
Auth Password		
Note: SNMP V1/V2c is read-onl	y and SNMP V3 is read-write	2.
	OK Can	ncel

Available settings are explained as follows:

ltem	Description	
Enable SNMPv1	Check it to enable this function.	
/SNMPv2c Agent	Get Community - Set the name for getting community by typing a proper character. The default setting is public.	
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 - Enter a password for authentication. The maximum length of the text is limited to 23 characters.	

Click **OK** to save these settings.

III-1-9 Management

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

Access Control		Port Setup
HTTP Server 🗌 Enfo	orce HTTPS Access	HTTP Port 80 (Default:80)
HTTPS Server		HTTPS (Default:443)
Allow management fro	om WLAN	
Enable Telnet Server		Panel Control
✓ Enable SSH Server		Disable LED
Disable Reset Button		Enable Default Configuration Wizard
		_
Access List		
Enable access list	M1-	
List IP	Mask	
1.	255.255.255 / 32 🗸	
2.	255.255.255 / 32 ~	
3.	255.255.255 / 32 🗸	
4.	255.255.255 / 32 🗸	
5.	255.255.255 / 32 🗸	

System Maintenance >> Management

Available parameters are explained as follows:

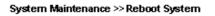
ltem	Description	
Device Name	The default setting is VigorAP 918R. Change the name if required.	
Access Control	HTTP Server / HTTPS Server - Enable the checkbox to allow system administrators to log in from HTTP or HTTPS server.	
	Enforce HTTPS Access - Enable the checkbox to allow system administrators to log in from HTTPS server only.	
	Allow management from WLAN - Enable the checkbox to allow system administrators to login from wireless LAN.	
	Enable Telnet Server – The administrator / user can access into the command line interface of VigorAP remotely for configuring settings.	
	Disable Reset Button - If enabled, the function of the Reset button	

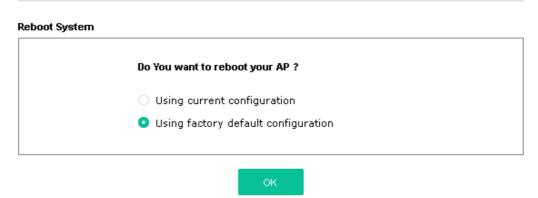
	will be invalid.
Access List	Enable access list – Check the box to specify that the system administrator can only login from a specific host or network defined in the list. A maximum of five IPs/subnet masks is allowed.
Port Setup	HTTP port/HTTPS port -Specify user-defined port numbers for the HTTP and HTTPS servers.
Panel Control	Disable LED - The LEDs blink always since VigorAP is powered on. Some people might not like that. Therefore the function of LED is allowed to be disabled to make people feeling comfortable and undisturbed. After checking it, all the LEDs on VigorAP will light off immediately after clicking OK.
	Enable Default Configuration Wizard – Default setting is enabled. When it is enabled, you will be guided into Quick Start Wizard whenever clicking the DrayTek logo on the top of the web user interface.
	Such function will be disabled if you have configured Operation Mode WLAN>>General Setup, WLAN>>Bandwidth Management, WLAN>>Station Control or System Maintenance>>Administration Password.

Click **OK** to save these settings.

III-1-10 Reboot System

The web user interface may be used to restart your modem. Click **Reboot System** from **System Maintenance** to open the following page.





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

(i) Note:

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

III-1-11 Firmware Upgrade

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

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

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

System Maintenance >> Firmware Upgrade Firmware Upgrade Click Upgrade to upload the file. Upgrade Firmware Version Status Current Firmware Version : 1.4.6 The Latest Firmware Version : 1.4.6 Download

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

System Maintenance >> Firmware Upgrade

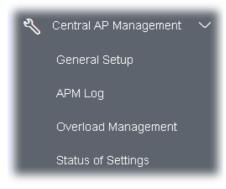
Firmware Update

Firmware Upgrade is in progress It must NOT be interrupted!	

Firmware Version Status		Refresh Latest Firmware	
Current Firmware Version	: 1.4.5		
The Latest Firmware Version	: 1.4.6	Download	

III-2 Central AP Management

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



III-2-1 General Setup

Central AP Management >> General Setup

Management by VigorRouter / RootAP	
Enable NodeAP	
Enable Auto Provision	
Enable Check Account Password For Set Group Key	
Reset	
Root AP MAC:	
Manage other VigorAPs	
Enable RootAP	
Note: LAN-B cannot support APM feature. RootAP cannot support AP700/AP800/AP900 as Node. Maximum support 30 APs.	

Available settings are explained as follows:

ltem	Description		
Management by VigorRouter/RootAP			
Enable NodeAP	Check the box to enable the function of AP Management (APM). Enable Auto Provision - VigorAP can be controlled under Central AP Management in the Vigor router. When both the Vigor router series and VigorAP have such feature enabled, once VigorAP is registered to the Vigor router series, the WLAN profile pre-configured on the Vigor router series will be applied to VigorAP immediately. Thus, it is not		

Cancel

	necessary to configure VigorAP separately.
	Enable Check Account Password For Set Group Key - If it is disabled, the RootAP can manage this AP (node AP) without entering the username/password of the node AP.
	If it is enabled, any RootAP must enter the username/password of this node AP to manage this device. The username/password can be seen on the router's Central Management >> AP >> Status page or AP's Central AP Management >> Node Status. An exception is that the RootAP can manage the device directly without entering the username/password of the node AP if the target node AP uses the default username/password (admin/admin).
Manage other VigorAPs	
Enable RootAP	Check this box to enable AP management. The role of this AP is "Root".

Click **OK** to save these settings.

III-2-2 APM Log

This page will display log information related to wireless stations connected to VigorAP 918R and central AP management.

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

M Log Information		Clear	Refresh 🗌	Line wrap
				1
Aug 24-13:02:54	syslog: [APM] Request done.			
Aug 24-10:47:27	syslog: [APM] Get Traffic data.			
Aug 24-10:47:27	syslog: [APM] Request done.			
Aug 24-10:52:28	syslog: [APM] Get Traffic data.			
Aug 24-10:52:28	syslog: [APM] Request done.			
Aug 24-10:42:26	syslog: [APM] Get Traffic data.			
Aug 24-10:42:26	syslog: [APM] Request done.			
Aug 24-10:47:27	syslog: [APM] Get Traffic data.			
Aug 24-10:47:27	syslog: [APM] Request done.			
Aug 24-10:52:28	syslog: [APM] Get Traffic data.			
Aug 24-10:52:28	syslog: [APM] Request done.			
Aug 24-10:57:29	syslog: [APM] Get Traffic data.			
Aug 24-10:57:29	syslog: [APM] Request done.			
Aug 24-11:02:30	syslog: [APM] Get Traffic data.			
Aug 24-11:02:30	syslog: [APM] Request done.			
Aug 24-11:07:31	syslog: [APM] Get Traffic data.			

Central AP Management >> APM Log

III-2-3 Overload Management

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 918R) 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 918R 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., Vigor2866 or Vigor2927 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.

	MA	C Address Filter of F	orce Overload Disassociation	
	Index	MAC Address	Comment	
White List				
Black List				
Client's MAC	2 Address	::		
Apply to :		White List \sim		
Comment				
Comment				
Comment	A	dd Delete	Edit Cancel	

Central AP Management >> Overload Management

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

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 Address	Specify the MAC Address of the remote/local client.
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.	
Comment	Type a brief description for the specified client's MAC address.	
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.	

Click **OK** to save these settings.

III-2-4 Status of Settings

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 918Rs) registered to Vigor2865 or Vigor2927 series. This web page displays the settings related to Load Balance for VigorAP 918R. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor2865 or Vigor2927 series.

Central AP Management >> Status of Settings

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

"X" means the function is not enabled or VigorAP 918R has not registered to any Vigor router yet.

Below shows a setting example for Load Balance settings configured in Vigor2865 or Vigor2927 series.

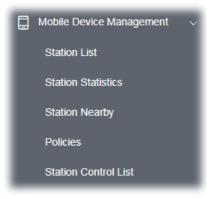
Central Management >> AP >> Load Balance

Station Number Threshol	ld		
Wireless LAN (2.4GHz)	64 (3-128)		
Wireless LAN (5GHz)	64 (3-128)		
Wireless LAN (5GHz-2)	64 (3-128)		
Upload Limit User de Download Limit User de	fined V OK fined V OK	bps (Default unit: K) bps (Default unit: K)	
Action When Threshold E	Exceeded		
	connections		
 Stop accepting new of Obissociate existing st 	and the local base of the second states		

III-3 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 (MDM).

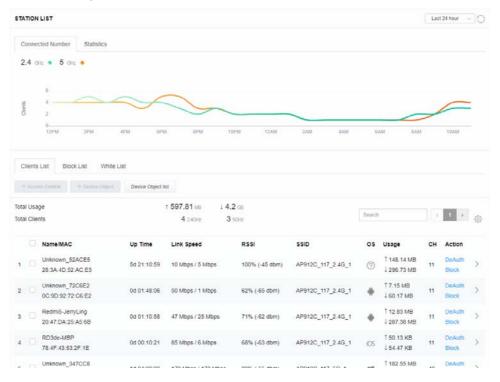


III-3-1 Station List

Station List provides the information related to the number of clients connecting to VigorAP, used bandwidth and the statistics of the AP device OS. Besides, users can create access control policies, device objects and set black & white list for

III-3-1-1 Connected Number

This page lists the graph for the number of wireless stations connected to this Access Point with different time phases.



III-3-1-2 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.

STAT	ION L	IST 🕕							L	ast 24 hour	~ 0
Co	nnecte	ed Number Statistics									
	ſ	0% Device OS 0% 0% 100%	Windows (Linux 0)	Polic	y	100% 0%	Pass 58Block 0			₹
Cli	ents Li	ist Block List White	List								
	Access	Control + Device Object	Device Object	list							
	Usage Clients			8.13 кв ↓ 45.89 кв 0 24GHz 64 5GHz	5g	ć	1	2 3 4	5	6 7 >	<u>ين</u>
		Name/MAC	Up Time	Link Speed	RSSI	SSID	os	Usage	сн	Action	
1		Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	0	1 867 B ↓ 717 B	36	DeAuth Block	>
2		Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:41:17	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1̂ 867 В ↓717 В	36	DeAuth Block	>
3		Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1867 B ↓717 B	36	DeAuth Block	>
4		Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:41:16	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
5		Unknown_607C8F 00:BC:DA:60:7C:8F	0d 03:41:16	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
6		Unknown_9D28C0 00:BC:DA:9D:28:C0	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1867 B ↓717 B	36	DeAuth Block	>
7		Unknown_79E9C2 00:BC:DA:79:E9:C2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	0	1 867 B ↓717 B	36	DeAuth Block	>
8		Unknown_9B07CE 00:BC:DA:9B:07:CE	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
9		Unknown_AA5A63 00:BC:DA:AA:5A:63	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
10		Unknown_DD1FA2 00:BC:DA:DD:1F:A2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1 903 B ↓ 717 B	36	DeAuth Block	>

III-3-1-3 Clients List

The client list displays all the stations connecting to VigorAP.

SIAI	TION LIST ()							L	ast 24 hour	~ O
Co	onnected Number Statist	ics								
	Device OS	0% • Android 0 0% • iOS 0 0% • Windows 0% • Linux 0 100% • Others 58	0	Polic	y	100% 0%	Pass 58Block 0			
	ents List Block List	White List	t list							
Total	Usage Clients		8.13 кв ↓ 45.89 кв 0 24GHz 64 5GHz	5g	ć	1	2 3 4	5	6 7 >	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Total	Usage		8.13 kB ↓ 45.89 kB	5g RSSI	SSID	1 OS	2 3 4 Usage	5 CH	6 7 > Action	Ś
Total	Usage Clients	↑ 5	8.13 кв ↓ 45.89 кв 0 24GHz 64 5GHz		SSID AA-903					> >
Total Total	Usage Clients Name/MAC Unknown_C84A46	↑ 5 Up Time	8.13 kg ↓ 45.89 kg 0 24GHz 64 5GHz Link Speed	RSSI		os	Usage ↑ 867 B	сн	Action DeAuth	
Total Total 1	Usage Clients Name/MAC Unknown_C84A46 00:BC:DA:C8:4A:46 Unknown_07B0C1	↑ 5 Up Time 0d 03:42:47	8.13 kB ↓ 45.89 kB 0 240Hz 64 soHz Link Speed 270 Mbps / 6 Mbps	RSSI 57% (-67 dbm)	AA-903	os ?	Usage ↑ 867 B ↓ 717 B ↑ 867 B	СН 36	Action DeAuth Block DeAuth	>

Available settings are explained as follows:

tem	Description
Access Control	It is available after choosing one of the entries (clients) on Client List.
	Add Access Control
	Wireless LAN 50Hz v
	DE SSID Policy 1 Black list v 2 Disable v 3 Disable v 4 Disable v AA-903 AA-903-2 AA-903-3 AA-903-4
	From to list
	Device MAC Name Apply to SSID
	¹³ 00/BC:DA:07/B0/C1 Unknown_07B0/C1 All 1 2 3 4
	00:BC:DA:C3:4F:0A Unknown_C34F0A All 1 2 3 4
	Total : 0/256 Close Save chara

From to list - Display the clients available for applying this access

	control.		
		elect the one(s) to ma	ke the device apply the policies to all ake the device apply the policies to
	Close - Exit	this page without say	ving any changes.
		ges - Save the change	
Device Object			
+Device Object	(clients) on button to o	-	list, choose one of the entries the Device Object button. Click the ge.
		Device MAC	Name
		Berice IIIAo	
		00:BC:DA:F5:EB:B4	Unknown_F5EB34
		00:BC:DA:94:CC:07	Unknown_94CC07
			Cancel OK
	White List		
	Check the ir	oformation listed on	the page. Change the MAC address
			required. Then click OK and exit the
	page.	, , , , , , , , , , , , , , , , , , ,	
Device Object list	The existed	device object profile	s will be shown on the following
	page.		
	DEVICE OBJECT		× .
	DEVICE OBJECT Device Object Profiles		X
			Search Series Pacery Default
	Device Object Profiles		
		MAC 00.50.7F #1.51.IDC	Search Series Factory Default
	Device Object Profiles		Kame
	Device Object Profiles Profile 1 2	00 50 7F F1 91 BC 00 50 7F 00 92 8A	Name TEST_1 TEST_2
Clients List	Device Object Profiles Profiax 1 2 Display the	00 50 77 71 91 BC 00 50 77 70 92 BA stations connecting 1	Name TEST_1 TEST_2
Clients List	Device Object Profiles Profile 1 Display the Total Usage	stations connecting f	Name TEST_1 TEST_2 TEST_2
Clients List	Device Object Profiles Profile 1 Display the Total Usage	stations connecting f	Name TEST_1 TEST_2
Clients List	Device Object Profiles Profidx 1 2 Display the Total Usag Total Clien	stations connecting t e - Display ts - Display the number k - Display the host	Name TEST_1 TEST_2 TEST_2
Clients List	Device Object Profiles Profex 1 2 Display the Total Usag Total Clien Name / MA connecting	stations connecting t e - Display ts - Display the number k - Display the host	to this Vigor device.
Clients List	Device Object Profiles Profids 1 2 Display the Total Usag Total Clien Name / MA connecting Up Time - D	stations connecting t e - Display ts - Display the numbre C - Display the host of client. Display the connection	to this Vigor device.
Clients List	Device Object Profiles Profes 1 2 Display the Total Usage Total Clien Name / MA connecting Up Time - D Link Speed	stations connecting f e - Display ts - Display the numb C - Display the host f client. Display the connectio - Display the link spe	to this Vigor device.
Clients List	Device Object Profiles Profes 1 2 Display the Total Usag Total Clien Name / MA connecting Up Time - D Link Speed RSSI - Display	stations connecting t e - Display ts - Display the numb C - Display the host of client. Display the connectio - Display the link spe ay the RSSI value.	to this Vigor device. Deer of the clients using 2.4GHz name / MAC address of the n time. red.
Clients List	Device Object Profiles Profes 1 2 Display the Total Usage Total Clien Name / MA connecting Up Time - D Link Speed RSSI - Displ SSID - Displ	stations connecting f e - Display ts - Display the numb C - Display the host f client. Display the connectio - Display the link spe ay the RSSI value. ay the SSID the client	to this Vigor device. Deer of the clients using 2.4GHz name / MAC address of the n time. red.
Clients List	Device Object Profiles Profes 1 2 Display the Total Usag Total Clien Name / MA connecting Up Time - D Link Speed RSSI - Displ SSID - Displ OS - Display	stations connecting t e - Display ts - Display the numb C - Display the host of client. Display the connectio - Display the link spe ay the RSSI value. ay the SSID the client.	to this Vigor device. Deer of the clients using 2.4GHz name / MAC address of the In time. red. t used for connecting VigorAP.
Clients List	Device Object Profiles Profes 1 2 Display the Total Usage Total Clien Name / MA connecting Up Time - D Link Speed RSSI - Displ SSID - Displ OS - Display Usage - Dis	stations connecting f e - Display ts - Display the numb C - Display the host f client. Display the connectio - Display the link spe ay the RSSI value. ay the SSID the client the OS of the client.	None TENT_1 TENT_1 TENT_2 to this Vigor device. oer of the clients using 2.4GHz name / MAC address of the n time. red. t used for connecting VigorAP. usage (up and down) of the client.
Clients List	Device Object Profiles Profes Profes 1 2 Display the Total Usage Total Clien Name / MA connecting Up Time - D Link Speed RSSI - Displ SSID - Displ OS - Display Usage - Dis CH - Display	stations connecting t e - Display ts - Display the numb C - Display the host of client. Display the connectio - Display the link spe ay the RSSI value. ay the SSID the client. play the bandwidth u y the channel used by	None TENT_1 TENT_1 TENT_2 to this Vigor device. oer of the clients using 2.4GHz name / MAC address of the n time. red. t used for connecting VigorAP. usage (up and down) of the client.

II-3-13-4 Block List

This page displays information of the stations under block list.

STATION LIST ()				Last	t 24 hour 🗸 🏷
Connected Number Statistics					
2.4 GHz • 5 GHz •					
1					
Clients					
0— 2AM 4AM 6AM 8AM	10AM -	12PM 2PM	4PM 6PM	8PM 10PM	12AM
Clients List Block List White List	ct list			Search	¢
Name / MAC	SSID	Reason	Action		
Unknown_457823 00:BC:DB:45:78:23	AA-903	ACL	Unblock		
2 Unknown_A566C8 00:BC:DB:A5:66:C8	AA-903	ACL	Unblock		
Total list 2					

Available settings are explained as follows:

ltem	Description	Description						
Device Object list	Click it to open the Device Object List dialog for reference.							
	DEVICE OBJECT							
	Device Object Profiles		Search Set to Factory Default					
	Profidx 1 2	MAC 00.50.7F.F1.91.BC 00.50.7F.00.92.BA	Name TEST_1 TEST_2					
Name / MAC	Display the h	ost name / MAC Address	s for the connecting client.					
SSID	Display the S	SID that the wireless clie	ent connects to.					
Reason	Display the re	eference information.						
Action		ction that you can execu ck to unblock the entry.	ite for the station.					

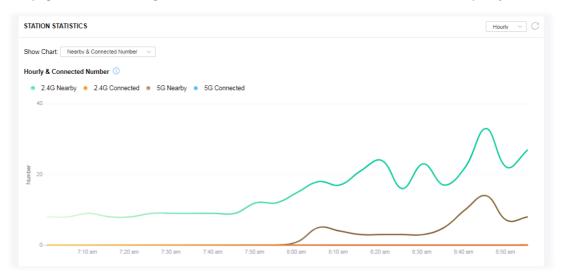
III-3-1-5 White List

This page displays general information of the stations under white list.

	11AM 1PM	3PM	5PM	7PM	9PM	11PM	1AM	3AM	5AM	7AM	9AM
Clients	List Block List	White List									
+ Acc	ess Control + De	evice Object	Device Object list								
										Search	
											۲ (
	Name/MAC			\$\$	ID		Action				
1	LiteonTe C8:FF:28:FC:2A:C1			mk	-carrie		Block				
2	Unknown_A02925 3C:95:09:A0:29:25			mk	-carrie		Block				
Total lis	st 2										

Item	Description							
Device Object list	Click it to open the Device Object List dialog for reference.							
	DEVICE OBJECT		.*					
	Device Object Profiles		Search Set to Factory Default					
	Profidx	MAC	Name					
	4	00.50.7F.F1.91.BC	TEST_1					
	2	00.50.7F.00.92.BA	TEST_2					
Name / MAC	Display the l	nost name / MAC Addre	ess for the connecting client.					
SSID	Display the s	SSID that the wireless cl	lient connects to.					
Action	Display the	action that you can exe	cute for the station.					
		to block the entry.						

III-3-2 Station Statistics



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

Available parameters are explained as follows:

ltem	Description						
Show Chart	Choose one of the items to display the statistics chart for wireless stations.						
	It: Nearby & Connected Number \sim						
	Nearby & Connected Number ~						
	Visiting & Passing Number						
	Visiting Time						
	Nearby & Connected Number – Choose it to have the statistics of the wireless stations which is nearby and connected to VigorAP 918R.						
	Visiting & Passing Number – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP 918R.						
	Visiting Time - Choose it to have the statistics of the wireless stations which is visiting VigorAP 918R.						

III-3-3 Station Nearby



This page displays the general information for the nearby stations.

1.approx. Distance is calculated by actual signal strength of device detected. Lnaccuracy might occur based on barrier encountered.
 2.Due ot the difference in signal strength for different devices, thd calculated value of approximate distance also might be different.

You can select the station(s) and click **+Access Control** to configure the nearby stations as the one(s) to pass through VigorAP or to be blocked by VigorAP.

Add Access	Control										
Wireless LAN	2.4GHz v										
SSID Policy											
	1 Disable ~	2 White list \checkmark 3	Disable 🗸	4	Dis	able	э.	~			
	mk-angela-903-1	mk-carrie	N/A			N/A	Ą				
From to list											
	Device MAC	Name	Apply	to SSII)						
				<	~		~		~		
	C8:FF:28:FC:2A:C1	LiteonTe	🗹 All	1	~	2	~	3		4	
					_		_		_		
	3C:95:09:A0:29:25		🗹 All	~ 1	~	2	~	3	×	4	
	3C:95:09:A0:29:25		✓ All	⊻ 1		2		3		4	

Available parameters are explained as follows:

ltem	Description
SSID Policy	Determine the policy (disable, white list or black list) applied for the SSID (1 to 4).
From to list	Device MAC - Display the MAC address of the selected station. Name - Display the name of the selected station.
	Apply to SSID - Check the box(es) to apply the SSID to the selected station.
	Close - Exit the dialog without saving the changes.
	Save changes - Save the changes and exit the dialog.

III-3-4 Policies

This page determines which devices (mobile, PC, MAC or others) allowed to make network connections via VigorAP or blocked by VigorAP.

Policies				
	Block Mobile Connections (OS:Android,iOS) Block PC Connections (OS:Windows,Linux,iMac) Block Unknown Connections (OS:Others)			
	WiFi(2.4GHz) WiFi(5GHz)	 SSID1 SSID2 SSID3 SSID4 SSID1 SSID2 SSID3 SSID4 		
			ОК	Cancel

Each item is explained as follows:

ltem	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.

III-3-5 Station Control List

STATION CONTROL LIST Online • Offline Reset MAC Connection Time SSID Reconnection Time AP912C_117_2.4G_1 28:3A:4D:52:AC:E5 0d 00:58:50 0d 00:00:00 . 1 AP912C_117_2.4G_1 20:47:DA:25:A5:6B 0d 00:48:22 0d 00:00:00 2 . 3 • AP912C_117_5G_1 40:4E:36:5E:3F:A7 0d 00:59:55 00:00:00 b0 0d 00:00:00 AP912C_117_5G_1 D0:37:45:34:7C:C8 0d 00:56:02 4 .

This page displays information related to the wireless stations connecting to the VigorAP.

① This page is available when Station Control is enabled.

Chapter IV Others



IV-1 RADIUS Setting



IV-1-1 RADIUS Server

۸

VigorAP 918R offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 918R. The AP can accept the wireless connection authentication requested by wireless clients.

	r			
Authentication Type				
Radiu	s EAP Type	PEAP	~	
Jsers Profile (up to 256				
Username	Password	Confirm Password		igure
			Add	Cancel
NO.	Userna	me	Sele	ct
Delete Selected	Delete All			
Client IP	ip to 16 clients) Secret Key	Confirm Secret Key	Conf	igure
-		Confirm Secret Key	Conf Add	igure Cancel
-				Cancel
Client IP	Secret Key		Add	Cancel
Client IP NO.	Secret Key Client 1		Add Select	Cancel
Client IP NO.	Secret Key Client 1		Add	Cancel
Client IP NO.	Secret Key Client 1		Add Select	Cancel

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			
	• Add – Make a new user profile with the name and password specified on the left boxes.			
	• Cancel – Clear current settings for user profile.			
	Delete Selected – Delete the selected user profile (s).			
	Delete All – Delete all of the user profiles.			
Authentication Client	This internal RADIUS server of VigorAP 918R 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 918R as its external RADUIS server.			
	Client IP – Type the IP address for the user to be authenticated by VigorAP 918R when the user tries to use VigorAP 918R as the externa RADIUS server.			
	Secret Key – Type the password for the user to be authenticated by VigorAP 918R while the user tries to use VigorAP 918R as the external RADIUS server.			
	Confirm Secret Key – Type the password again for confirmation.			
	Configure			
	• Add – Make a new client with IP and secret key specified on the left boxes.			
	• Cancel – Clear current settings for the client.			
	Delete Selected – Delete the selected client(s).			
	Delete All – Delete all of the clients.			
Backup Radius Cfg	Backup - Click to store the configuration set on this page as a file.			
Upload From File	Browse - Click to upload the RADIUS configuration file from the host to VigorAP.			
	Restore - Click to restore the RADIUS configuration file to VigorAP.			

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

IV-1-2 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.

Certificate Name	Root CA
Subject Name	
Country (C)	
State (S)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA ~
Key Size	1024 Bit 🗸
Apply to Web HTTPS	
	OK Cancel

RADIUS Setting >> Create Root CA

ltem	Description
Subject Name	Type the required information for creating a root CA.
	Country (C) – Type the country code (two characters) in this box.
	State (S)/ Location (L)/ Organization (O)/ Organization Unit (OU) /Common Name (CN) - Type the name or information for the root CA with length less than 32 characters.
	Email (E) – Type the email address for the root CA with length less than 32 characters.

Кеу Туре	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	VigorAP needs a certificate to access into Internet via Web HTTPS. Check this box to use the user-defined root CA certificate which will substitute for the original certificate applied by web HTTPS.

(Note:

"Common Name" must be configured with 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.

IV-2 Applications

Below shows the menu items for Applications.



IV-2-1 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 >> Sc	hedule					
Schedule : Curren	nt System Time				System time set	Set to Factory Default
Index Enable	Name	Action	Ti	me		Finished) Not reached Jency
			ОК	Add		

Item Description			
Current System Time Display current system time.			
System time set Click it to open Time and Date page for configuring the time			
Set to Factory Default	Click it to return to the factory default setting and remove all the schedule profiles.		
Index	Display the sort number of the schedule profile.		

Enable	Check it to enable the function of schedule configuration.		
Name	Display the name of the schedule.		
Action	Display the action adopted by the schedule profile.		
Time	Display the time setting of the schedule.		
Frequency	Display the frequency of the time schedule.		

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

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

Applications >> Schedule

Add Schedule	
🗹 Enable	
Name	
Start Date	2000 \checkmark - 1 \checkmark - 1 \checkmark (Year - Month - Day)
Start Time	$0 \sim : 0 \sim$ (Hour : Minute)
Duration Time	$0 \sim$: $0 \sim$ (Hour: Minute)
End Time	$0 \sim : 0 \sim$ (Hour : Minute)
Action	Auto Reboot 🛛 🗸
WiFi(2.4GHz)	Radio SSID2 SSID3 SSID4
WiFi(5GHz)	Radio SSID2 SSID3 SSID4
How Often	Once ~
Weekday	Monday 🗌 Tuesday 📄 Wednesday 📄 Thursday 📄 Friday 📄 Saturday
weekday	Sunday
schedule	set WiFi schedule "Start Time" and "End Time" at exact same time, AP will execute the e without an end time. net Pause" will add Mac into ACL, so please make sure ACL isn't full before applying
schedule	If ACL policy is "Disable", AP will change it to "Blocked".

Available settings are explained as follows:

Item	Description
Enable	Check to enable such schedule profile.
Name	Enter the name of the 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. It is available only for the action set with WIFI UP, WIFI Down, or Internet Pause.
End Time	Display the ending time (sum of start time and duration time) of the

Cancel

	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. Moreover, SSID2, SSID3, and SSID4 are not available for choosing if they are not enabled.
How Often	Specify how often the schedule will be applied. Once - The schedule will be applied just once Weekdays - Specify which days in one week should perform the schedule.
Weekday	Choose and check the day to perform the schedule. It is available when Weekdays is selected as How Often .

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

Applications >> Schedule				
Schedule : Current System	Time 2019 De	c 16 Mon 11:07:51		System time set Set to Factory Default
Index Enable Name	Action		Time	Active Finished Not reached Frequency
1 🔽 Formkt A	uto Reboot	01:01		Once 🥥 🗴
		ОК	Add	

IV-2-2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 918R will send the UDP packets with 5353 port to the specific IP every five seconds.

Applications >> Apple iOS Keep Alive	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	
		4	
3			
3 5		6	

ltem	Description
Enable Apple iOS Keep	Check to enable the function.

Alive	
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.

Click **OK** to save the settings.

IV-2-3 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 Conne	ction Detection
Ping Host	
	Fi automatically when the AP is able/unable to ping the host. able to ping the host:
Wi-Fi:	Off ~
LED:	No Change 🗸

Available settings are explained as follows:

ltem	Description
Enable Connection Detection	Check the box to enable this function.
Ping Host	Enter an IP address (e.g., 8.8.8.8) or a domain name (e.g., google.com) for testing if the access point is stable or not.
Wi-Fi	 Off - When VigorAP is unable to ping the host, disconnect the Wi-Fi network. No Change - Wi-Fi network will keep the original state (no mater on or off) even VigorAP is unable to ping the host.
LED	Off - When VigorAP is unable to ping the host, the LED (2.4G/5G) will be off automatically.
	No Change - When VigorAP is unable to ping the host, the LED (2.4G/5G) will keep the original state (no matter on or off).

Click **OK** to save the settings.

IV-2-4 Sensor

A USB Thermometer is now available that complements your installed DrayTek AP installations that will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.



During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible VigorAP will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted via Syslog.

For a list of supported USB thermometers, visit our website at https://www.draytek.com/en/products/usb-thermometer/ or contact your local DrayTek partner.

Temperature Sensor Settings

Applications >> Sensor Setting			
Sensor Graph	Sensor Settings	5	
Enable "Sensor Graph"			
🗸 Alerts 🛛 once 🗸 via "A	lert Method" when any ser	nsor value is outside of "Alert Criteria	" range
	acterited and any set		lange
Alert Method			
Syslog 🗌 Ma	il		
Alert Criteria			
	-30.0 ~ 90.0 🔾	°C , calibration/current val:	0.0
2.4GHz Wi-Fi 🗸	: ○ °F	52.0	
	0.4	52.0	
Humidity Sensor:	0.0 ~ 98.0 %	, calibration/current val:	0.0 33.3
	ОК		

Note:

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

ltem	Description
Enable "Sensor Graph"	Check it to display the sensor graph on Applications >> Sensor Setting >> Sensor Graph .

Alerts once/per min	It can determine the time/interval to send an alert message.				
via	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 log containing the alarm message will be recorded on Syslog if it is enabled.				
	Mail - The 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. Please type the upper limit and lower limit for VigorAP system to send out temperature alert.				
	• Calibration / current val- Type values used for correcting the temperature error.				
	• C°/F° - Choose the display unit of the temperature. There are two types for you to choose.				
	Humidity Sensor - Specify a range.				

Temperature Sensor Graph

Below shows an example of temperature graph:

Applications >> Sensor Graph



IV-3 Objects Setting

Below shows the menu items for Objects Setting.



IV-3-1 Device Object

VigorAP can specify a client as a device object to be used by other applications.

Objects Setting >> Device Object

Create from Wireless Station Table

Create from Wireless Neighbor Table

Create from ARP Table

Device Object		Nama	Tuday		t to Factory Default
Index	MAC	Name	Index	MAC	Name
1			17		
2			18		
3			19		
4			20		
5			21		
6			22		
7			23		
8			24		
9			25		
10			26		
11			27		
12			28		
13			29		
14			30		
15			31		
16			32		
< 1-32 33-	64 65-96 97-128 1	29-160 161-192	2 193-224 225	i-256 >>	Next >
Backup ACL	Cfg : Backup	Upload From Fi	le: Browse		Restore

Available settings are explained as follows:

ltem	Description
Create from Wireless Station Table	Click the link to open the following page.

	不安全 192.168.1.13/adm	/devobistat.asp				
	Objects Setting >> D					
	Select All	tost Name Device MAC Name	No. Host Name Devi	255 Objects prof	Des Lett	
	NO. P	OK NAME DEVICE MAL	Cancel	CE MAC Name		
	Choose the c	one(s) you want an	d click OK . Th	e selected e	ntries will	
	listed on the	Device Object Prot	files.			
Create from Wireless Neighbor Table		to open the follow	ving page.			
	Objects Setting >> Device O	bject				
	Create Device Object from Select All	Wireless Neighbor Table		2	53 Objects profiles Le	
	No. Host Name	Device MAC Name	No. Host Name	Device MAC	Name	
	3 ASUSTRAC	2015A12ALAR:181F7 ASUStekC	4 1 Intel	80:00:08:04:CE:SA	Intel	
	s 🖂 📗	02:10:AA:56:07:10	6 🗇 Estpher	88.22.68.07.86.46	Raspberr	
	7 🗆	50:3E(AA)E8(A1)C9	8	1A.3E.(C0:F7(00:41)		
	9	25:60:07:80:04:40	10	02:10:AA:5E:09:58		
	11	12:50:80:02:38:48	12	70:77:81:33:18:09		
Create from ARP Table	Click the link to open the following page. Objects Setting >> Device Object					
	Create Device Object from ARP Table 252 Objects profiles Let					
	Create Device Object fro	m ARP Table		4	52 Objects profiles	
	Select All		ame No			
		Device MAC Na	ame No. 92_168_1_10	IP Device MAC		
	Select All	Device MAC Na	92_168_1_10			
	Select All	Device MAC Ni 8.1.10 60:A4:4C:E6:5A:4F 1	92_168_1_10			
	Choose the c	Device MAC Ni 8.1.10 60:A4:4C:E6:5A:4F 1	22_168_1_10 Cancel	IP Device MA(C Name	
Set to Factory Default	Choose the clisted on the	Device MAC No. 8.1.10 00:A4:4C:E6:5A:4F 1 one(s) you want an Device Object Prot urn to the factory of	d click OK . Th	IP Device MAC	ntries will	
Set to Factory Default Index	Choose the clisted on the Click it to ret device object	Device MAC No. 8.1.10 00:A4:4C:E6:5A:4F 1 one(s) you want an Device Object Prot urn to the factory of	d click OK . Th files.	P Device MAC e selected e g and remov	ntries will	
-	Choose the clisted on the Click it to ret device object	Device MAC No. 8.1.10 SO:A4:4C:E6:SA:4F 1 Done(s) you want an Device Object Prot urn to the factory of t profiles.	d click OK . Th files. default setting	e selected e g and remov	ntries will re all the	
Index	Choose the clisted on the Click it to ret device object Display the in	Device MAC No. 8.1.10 50:A4:4C:E6:SA:4F 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	d click OK . Th files. default setting evice object pr fied by the der	e selected e g and remov rofile. vice object p	ntries will re all the	
MAC	Choose the clisted on the Click it to ret device object Display the in Display the n	Device MAC No. 8.1.10 50:A4:4C:E6:SA:4F 1 00 00 00 00 00 00 00 00 00 00 00 00 00	d click OK . Th files. default setting evice object pr fied by the dee object profile	e selected e g and remov rofile. vice object p	ntries will re all the	
Index MAC Name	Choose the clisted on the Click it to ret device object Display the in Display the n Display the r Backup - Click	Device MAC No. 8.1 10 50:A4:4C:E6:SA:4E 1 00 00 00 00 00 00 00 00 00 00 00 00 00	Cancel Cancel d click OK . Th files. default setting evice object pr fied by the der object profile nt configuration lected file ont	e selected e g and remov rofile. vice object p on. :o Vigor devi	ntries will re all the profile.	

In addition to choosing from the wireless station table, neighbor table or ARP table, you can click any index number link to create a new device object profile by entering the name and MAC address manually.

Profile Index : 1

Name : Mac Address : Attribute :	00:00:00:00:00 Select Isolate LAN exception		
	OK Clear Cancel		
ltem	Description		
Name	Enter the name of the profile.		
Mac Address	Enter the MAC address of the client.		
Attribute	Check the box to ignore the function of Isolate LAN.		
ОК	Save the settings.		
Clear	Remove the settings.		
Cancel	Discard the settings and return to previous page.		

IV-3-3 Device Group

Clients can be integrated as a group and be used by other applications.

Objects Setting >> Device Group

Device Group Table			Set to Factory Default
Index	Name	Index	Name
1		17	
2		18	
3		19	
4		20	
5		21	
6		22	
7		23	
8		24	
9		25	
10		26	
11		27	
12		28	
13		29	
14		30	
15		31	
16		32	

Backup ACL Cfg :	Backup	Upload From File:	Browse	 Restore	

Available settings are explained as follows:

ltem	Description
------	-------------

Set to Factory Default	Click it to return to the factory default setting and remove all the device group profiles.
Index	Display the index number of the device group profile.
Name	Display the name of the device group profile.

Click any index number link to create a new device group profile.

Objects Setting >> Device Group

ame :	2F	
ailable Device Objects	Selecte	d Device Objects
3 - ASUStekC 4 - 192_168_1_10		TEST_1 LiteonTe
	>>	
	~~	

Available settings are explained as follows:

ltem	Description
Name	Enter the name of the new group profile.
Available Device Objects	Display current available device objects. Choose the one(s) and click the >> button to move them under the Selected IP Objects.
Selected Device Objects	Display the selected device objects. Choose the one(s) and click the << button to discard the selections.
ОК	Save the settings.
Clear	Remove the settings.
Cancel	Discard the settings and return to previous page.

This page is left blank.

Chapter V Mobile APP, DrayTek Wireless



V-1 Introduction of DrayTek Wireless

VigorAP AP918R supports Android/iOS APP : DrayTek Wireless. The mobile user can find the APP through Apple Store / Android APP.

After downloading the APP, a mobile user is able to access and login the configuration page of VigorAP. It can be used to set up or check status of VigorAP device in different Operation Mode.

- To access into the VigorAP configured previously, please refer to <u>V-2 Select a VigorAP</u>
- To access into a new installed VigorAP, please refer to <u>V-3 Quick Start Wizard</u>

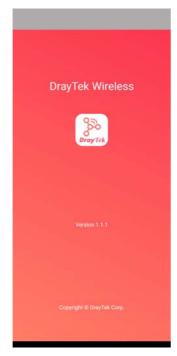
(i) Note:

Before using the DrayTek Wireless APP, please **ENABLE** your Wi-Fi feature first. Then, select the Wi-Fi network with Vigor access point(s) connected physically.

It is not necessary to connect to VigorAP physically. The mobile user must connect to one network with the same subnet as the VigorAP.

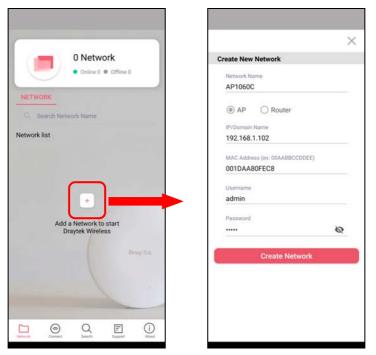
V-2 Create a New Network

1. Run DrayTek Wireless APP.



- 2. The system will open the NETWORK page to ask you create a new network first.
- 3. There are two methods for creating a new network. Click "+" or press the search button

A: Click "+" to enter the next page. Enter the required information for the device that you want to create a network.



B: Press the search button. Later, the system will show the device searched. Select the one you want and click the name to get the detailed information.

		Search				×
0 Network	Q Search Devic	e name or IP A	ddress		Create New Network	
Online 0 Offline 0 NETWORK	<u></u>		-	1 00004	Network Name AP1060C	
C Search Network Name	1 APs	1 Routers	SV	0 vitches	AP Router	
Network list	Access Point				192.168.1.102	
	AP1060C 192.168.1.102 Router			Aro L+ I	MAC Address (ex: 00AABBCCDDEE) 001DAA80FEC8	
•	Vigor2926 192.168.1.1		Mesh F	Root 🕞	Username admin	
Add a Network to start Draytek Wireless					Password	Ø
DrayTit					Create Network	
Heterot Connect Q Exactly Support About	Network Connect	Q	F	(i) About		

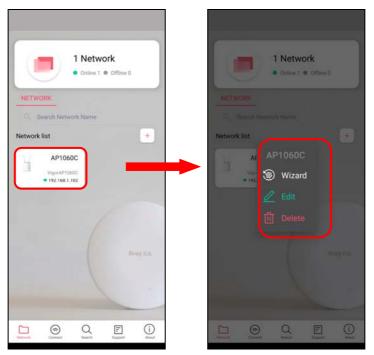
4. After clicking **Create Network**, a new network will be shown on the screen.



V-3 Wizard - Mesh Root and Mesh Node

The wizard can assist to configure mesh root and mesh node(s).

1. Click and hold the network item till available actions (**Wizard, Edit** and **Delete**) shown on the screen. Select and click **Wizard**.

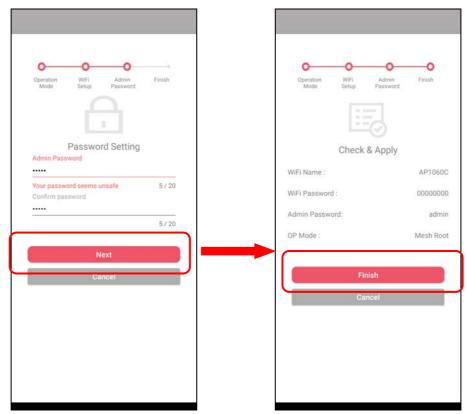


2. After clicking **Wizard**, select **Mesh Root** as the Operation Mode. The default Group Name is VigorMesh. Change the name if required. Click **Next** to enter the next page.

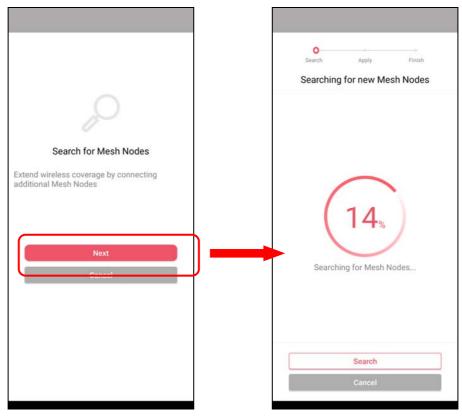
0	o <u>o</u>	
Operation WIFI Admin Finish Mode Setup Password	Operation WiFi Admin Mode Setup Passwo	
Operation Mode		
Operation Mode Mesh Root *		
Group Name	WiFi Name & Pass	word
VigorMesh	WiFI Name	
h h	AP1060C	
		7/32
	WiFi Password	ø
INTERNET ROUTER MESH ROOT MESH NOCE		8/64
	Your password seems unsafe	8/64
Next	Enable 2nd WiFi	02
Cancel	Next	
	Cancel	
	-	2

On the WiFi Name & Password page, enter the WiFi Name and the password (should be the same as the security settings set on the device's WUI). You can also enable 2nd SSID by enabling the function of 2nd WiFi. Then click the **Next** button.

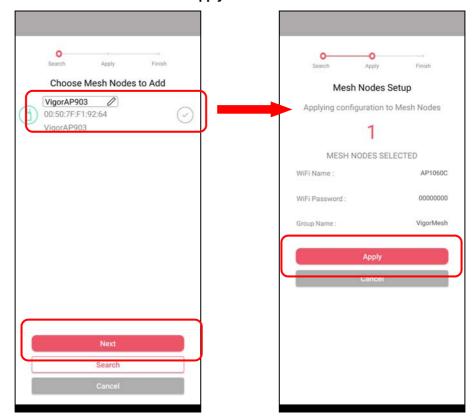
3. On the **Password Setting** page, enter the admin password and confirm the password. Then click **Next** for the APP to verify the password. If successful, the **Finish** button will appear.



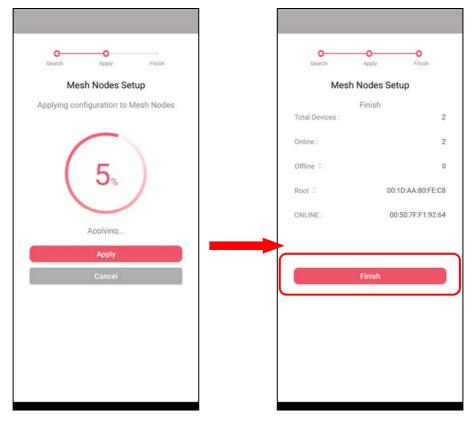
4. After sending configuration to VigorAP, it will take some time to take effect. Now, the VigorAP has been set as Mesh Root. You can search several Mesh Nodes which do not belong to any other mesh group by clicking **Next**.



5. Later, available VigorAP devices will be shown as the left figure below. Choose the Mesh Node you want to add and give a device name (e.g., VigorAP903) for it. The selected mesh node(s) will be grouped under such mesh root. Click **Next**. After checking the quantity of mesh node and mesh information and click **Apply**.



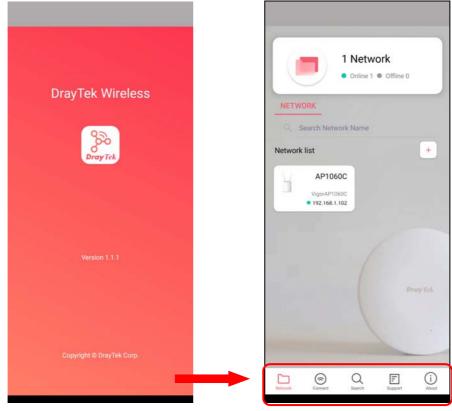
6. Wait until the mesh root applies general configuration to the mesh nodes. Later, current status of the mesh node(s) will be shown on the following page. Click **Finish**.



7. A network with mesh root and mesh node has been set up successfully.



Run DrayTek Wireless APP.

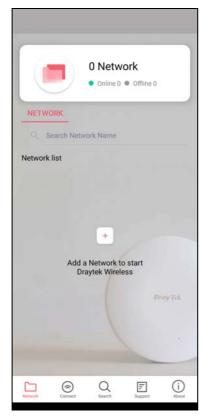


Available settings are explained as follows:

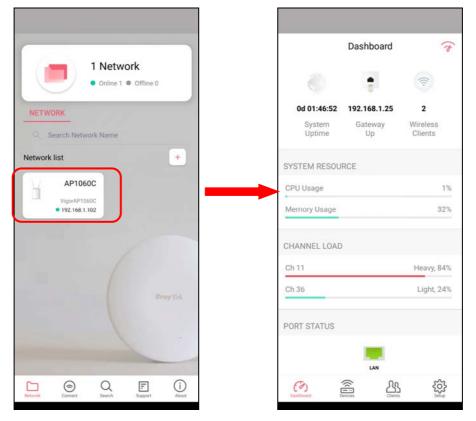
ltem	Description
Network	Create a new network.
Connect	Connect to a device (AP/CPE).
Search	Search available devices for connection.
Support	Display a list of models supported by this APP.
About	Display the version information of this APP.

V-4-1 Network

The Network page allows you to search devices (CPE/AP) for creating a network or editing an existing network (refer to V-2 for detailed information).

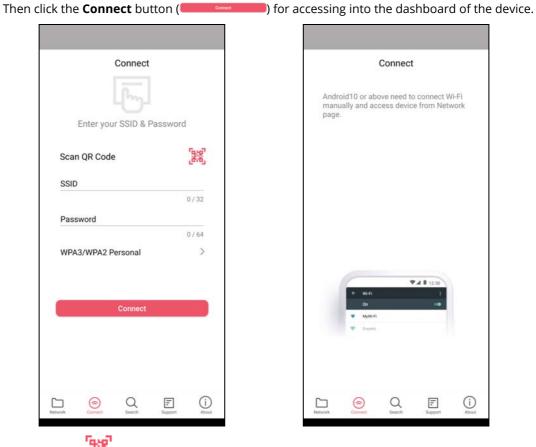


For checking the general information of certain device, click the existing item under the Network list to open the **Dashboard** of the selected device.



V-4-2 Connect

For viewing the detailed information of a selected CPE/AP, click the **Connect** icon (connect) to open the following left figure. Enter the SSID, password and select an encryption mode of the device.



Or, click **Scan** ()) to scan the QR code printed on <u>VigorAP packaging box</u> to connect the designated VigorAP.

V-4-2-1 Dashboard of the Device

Below shows the dashboard of the device. Use the scroll bar up and down for viewing other information.

Information for Mesh Root Mode

Dasi	hboard	7	Das	hboard	8	Das	hboard
			PORT STATUS			3310	AP 10000 (
				_		5GHz	
2	192.168.1.25	0		LAN		Radio	Enable
Vigors	Gateway Up	Wireless Clients	INFORMATION			SSID	AP1060C (
IBER			IP	192.168.1.	102		
		1	MAC	001DAA80F	EC8		5G
		1	Mode	Mesh_F	toot	1.0	
			Device Name	VigorAP10	60C	0.8	
URCE			Firmware	1.4.4_	RC1	0.4	
		2%				0.0 4 4 4 4	6 6 8
		31%	WIRELESS OVERVIEW		~	UKbps	1 OKbps
			2.4GHz			SPEED TEST	
D			Radio	Enable		Last seend test	on Oct 22, 1-19 DM
	1	Heavy, 98%	SSID	AP1060C	\odot		81.84
	Mod	lerate, 61%	5GHz				81.84
			Radio	Enable		1 maps	×
	23	ŝ	Con Concern	스와 성	33	Contract Coverage	<u>_</u>
	2 VVigors BBER URCE	2 192.168.1.25 Vigors Gateway Up BER URCE	2 192.168.1.25 0 Vigors Gateway Wireless BER 1 UP 1 URCE 2% 31% 31% D Heavy, 98% Moderate, 61% 1%	PORT STATUS 2 192.168.1.25 Vigors Gateway Up Clients BER INFORMATION IP MAC I MAC DURCE 2% 2% 31% 2% 2% 31% 2.4GHz D Heavy, 98% Moderate, 61% SGHz Radio	PORT STATUS 2 192.168.1.25 Vigors Gateway Up Clients BER 1 1 1 Mode Mesh_F DURCE 2% 2% 31% 24GHz Heavy, 98% Moderate, 61% Radio Enable SID AP1060C 5GHz Radio Enable SID Ap1060C	PORT STATUS 2 192.168.1.25 Vigors Gateway Up Viceless Up Clients InFORMATION BER 1 1 MAC 001DAA80FEC8 Mode Mesh_Root Device Name VigorAP1060C Firmware 1.4.4.RC1 Vigor Sibo AP1060C Firmware SSID AP1060C SSID SSID AP1060C SSID AP1060C	PORT STATUS 2 192.168.1.25 Vigors Gateway Up Vieneless Up Vieneless Up Vieneless INFORMATION BER IP 1 MAC 001DAA80FECS Mode Mesh_Root Device Name VigorAP1060C 2% MineLESS OVERVIEW 2% VigorAP1060C 2% VigorAP1060C 2% Xineless 31% 2.4GHz SID AP1060C (C) Heavy, 9% SID Moderate, 61% SGHz Radio Enable

	Dashboard	F	Dashbo	ard 😙	3310	Dashboard 🔗
		((1-	INFORMATION		5GHz	
	192.168.1.25	2	IP	192.168.1.102	Radio	Enable
System	Gateway	Wireless	MAC	001DAA80FEC8	SSID	AP1060C 🕗
Uptime	Up	Clients	Mode	AP	REAL TIME TH	ROUGHPUT
STEM RESOUR	oe.		Device Name	VigorAP1060C	HERE TIME IT	
	VE		Firmware	1.4.4_RC1		2.4G 5G
PU Usage lemory Usage		1%	WIRELESS OVERVIEW	~	12 10 08	
			2.4GHz		0.6	
HANNEL LOAD			Radio	Enable	02 60* * *	
h 11		Heavy, 84%	SSID	AP1060C 🕗	° 2	0Kbps î
h 36		Light, 24%	5GHz			
			Radio	Enable	SPEED TEST	
ORT STATUS			SSID	AP1060C 🕗	Last s	peed test on Oct 22, 1:18 PM
	LAN		REAL TIME THROUGHPUT		41.57 ↑ Mbps	
		ŝ	(7) a	令 (1) (1) (1) (1) (1) (1) (1) (1)	()	

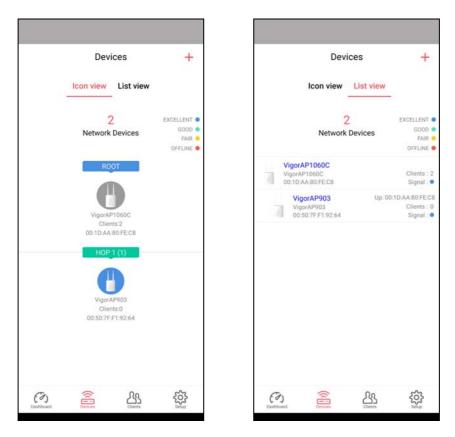
Available settings are explained as follows:

ltem	Description
Dashboard	The dashboard is designed with Responsive Web Design. You can click Dashboard to connect to the selected VigorAP WUI.
Devices	All of the devices (mesh root and mesh nodes) controlled by the mesh group will be shown on this page. One mesh group contains up to eight devices.

Clients	Displays general information for all clients / groups in Mesh Group.
Setup	Configures TR-069, Manage and WLAN settings for the connected VigorAP.

V-4-2-2 Devices

Below shows the icon view and list view of the device. One mesh group contains up to eight devices. Icon view and List view for **Mesh Root** Mode



Available settings are explained as follows:

ltem	Description
lcon view / List view	Switch to display the network devices in icons or a list.
"+"	To add more mesh node, click the "+" link.

Device for AP Mode

De	evice	
Vigor	AP1060C	
ON		
	19	2.168.1.102
	1	92.168.1.25
	001	DAA80FEC8
	Vig	orAP 1060C
		1.4.3_RC2
		Enabled
		Disabled
ç		b Thu Oct 7 9 CST 2021
TTING		
ice		
((([ሪዔ	ŝ
	Vigor/ ON	19 1 001 Vig 91001_47fbc8 15:06:5

Available settings are explained as follows:

Item	Description
INFORMATION	Display general information of the device (e.g., IP address, Gateway, MAC and etc.)
SYSTEM SETTINGS	Reboot Device - Click to reboot the device immediately.

V-4-2-3 Clients / Groups

This page shows relationship between devices and groups.

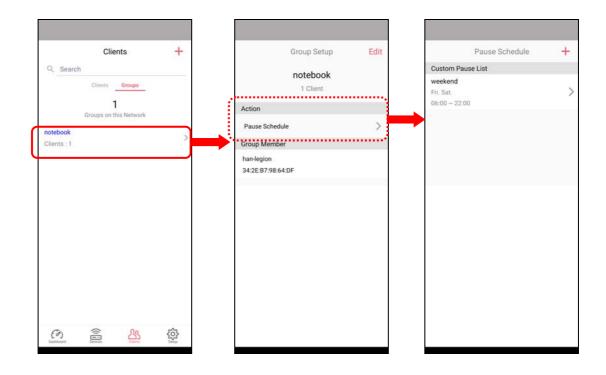
All client members can be classified (into groups). Additionally, the network connection time of the device group can be adjusted.

Q Search Clients	ients +	Q Search Clients	ents + Groups 2 this Network	Q Search Clients	dients +
Clients han-legion	AP1060C	My Clients	AP1060C	notebook Clients : 1	>
2 han-pixel 100 % 😴	АР1060С 0 Къря 10 Къря 7	Clients	AP1060C 0 Kbps 0 Kbps 1		
Constituent Devices	<u>삼.</u> 향:	Contract Contract	<u>路</u> 發	Contract Decore	<u>路</u> 登

Available settings are explained as follows:

ltem	Description
Search	Search available CPE/AP around.
Clients	+ - Click it to open the page containing My Clients for adding new clients under My Clients.
	My Clients - Devices under this area can be classified under a group.
	Clients - Displays devices which have not been classified under any network group.
Groups	Displays the group member and action. + - Click it to display the items listed under My Clients. Select the one you want to add it under current group.

Click the group to access the group setup page. If required, click **Edit** to add or remove the group member. Or click **Pause Schedule** to modify the schedule of the group.



V-4-2-4 Setup

Setup page is used for configuring TR-069, Admin Password, Wireless LAN and Wi-Fi Blocklist settings of the Vigor device.

TR069 Managem WLAN	ent	>
Wi-Fi Bloc	klist	>

•

Chapter VI Troubleshooting



VI-1 Diagnostics

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router 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 router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

Diagnostic tools provide a useful way to **view** or **diagnose** the status of your VigorAP 918R.

Diagnostics ~
System Log
Speed Test
Traffic Graph
treeapp alert event
WLAN (2.4GHz) Statistics
WLAN (5GHz) Statistics
Interference Monitor

VI-1-1 System Log

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

```
Diagnostics >> System Log
```

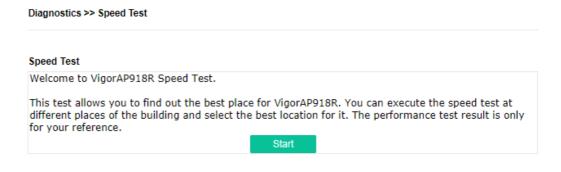
System Log Information

| Clear | Refresh | 🗌 Line wrap |

Aug 27 09:3	26:25 syslog:[APM] Get Traffic data. 🔨
Aug 27 09:3	26:26 syslog:[APM] Request done. 🗧
Aug 27 09:3	30:01 syslog:(]DRAY_BAND_INFO : Mon Aug 27 09:30:01 2018 (1535333401)^1
Aug 27 09:3	31:26 syslog:[APM] Get Traffic data.
Aug 27 09:3	31:26 syslog:[APM] Request done.
Aug 27 09:3	36:27 syslog:[APM] Get Traffic data.
Aug 27 09:3	36:27 syslog:[APM] Request done.
Aug 27 09:4	40:01 syslog:(<pre>@DRAY_BAND_INFO : Mon Aug 27 09:40:01 2018 (1535334001)^1</pre>
Aug 27 09:4	41:28 syslog:[APM] Get Traffic data.
Aug 27 09:4	41:28 syslog:[APM] Request done.
Aug 27 09:4	41:38 kernel:A	PPeerProbeReqAction():shiang! PeerProbeReqSanity failed!
Aug 27 09:4	41:38 kernel:A	PPeerProbeReqAction():shiang! PeerProbeReqSanity failed!
Aug 27 09:4	46:29 syslog:[APM] Get Traffic data.
Aug 27 09:4	46:29 syslog:[APM] Request done.
Aug 27 09:	50:01 syslog:(<pre>@DRAY_BAND_INFO : Mon Aug 27 09:50:01 2018 (1535334601)^*</pre>
Aug 27 09:	51:30 syslog:[APM] Get Traffic data. 🗸 🗸 🗸
<		

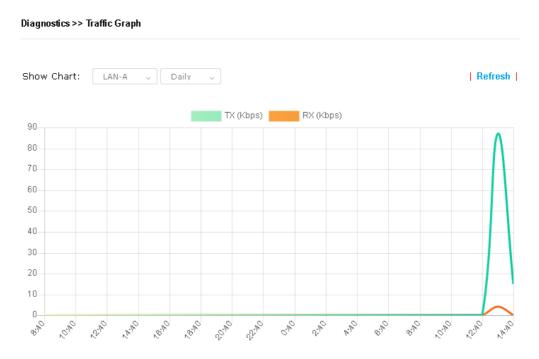
VI-1-2 Speed Test

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.



VI-1-3 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.



The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).

VI-1-4 Alert Event



VI-1-5 WLAN (2.4GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (2.4GHz) Statistics

			Auto-F	Refresh	Refresh
Tx Data Packets	0	Rx Data P	ackets		0
Tx Data Bytes	0	Rx Data B	lytes		0
Average Tx Rate (kbps)	No Station	Average F	Rx Rate (kbps)		No Station
Tx Unicast Data Packets	0	Rx PHY er	rrors		0
Tx Multi/Broadcast Data Packets	0	Rx CRC e	rrors		81483
Tx failures	0	Rx MIC er	rors		0
		Rx Decry	ption errors		0
		Rx errors			0
	SSID1 (DrayTek-3FB23	30)	SSID2 (mk_carrie)	SSID3 (N/A)	SSID4 (N/A)
Tx Data Packets		0	0	N/A	N/A
Tx Data Bytes		0	0	N/A	N/A
Tx Data BytesTx Data Payload Bytes		0	0	N/A	N/A
Rx Data Packets		0	0	N/A	N/A
Rx Data Bytes		0	0	N/A	N/A
Rx Data Payload Bytes		0	0	N/A	N/A
Tx Unicast Data Packets		0	0	N/A	N/A
Tx Multi/Broadcast Data Packets		0	0	N/A	N/A
Average Tx Rate (kbps)	N	o Station	No Station	N/A	N/A
Average Rx Rate (kbps)	N	o Station	No Station	N/A	N/A
Rx errors		0	0	N/A	N/A
Tx failures		0	0	N/A	N/A

VI-1-6 WLAN (5GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (5GHz) Statistics

			Auto-R	efresh	Refresh
Tx Data Packets	0	Rx Data Pa	ckets		0
Tx Data Bytes	0	Rx Data By	rtes		0
Average Tx Rate (kbps)	No Station	Average R	x Rate (kbps)	1	No Station
Tx Unicast Data Packets	0	Rx PHY err	rors		0
Tx Multi/Broadcast Data Packets	0	Rx CRC er	rors		20006
Tx failures	0	Rx MIC err	ors		0
		Rx Decryp	tion errors		0
		Rx errors			0
	SSID1 (DrayTek-3FB2	30)	SSID2 (mk_carrie)	SSID3 (N/A)	SSID4 (N/A)
Tx Data Packets		0	0	N/A	N/A
Tx Data Bytes		0	0	N/A	N/A
Tx Data BytesTx Data Payload Bytes		0	0	N/A	N/A
Rx Data Packets		0	0	N/A	N/A
Rx Data Bytes		0	0	N/A	N/A
Rx Data Payload Bytes		0	0	N/A	N/A
Tx Unicast Data Packets		0	0	N/A	N/A
Tx Multi/Broadcast Data Packets		0	0	N/A	N/A
Average Tx Rate (kbps)	N	lo Station	No Station	N/A	N/A
Average Rx Rate (kbps)	N	lo Station	No Station	N/A	N/A
Rx errors		0	0	N/A	N/A
Tx failures		0	0	N/A	N/A

VI-1-7 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.

		_			
Current Channe	el All	Channels			
				Auto-Refresh	Refresh
hannel Inform	ation				
land	2.4G 🗸		Country Code	TW	
Channel	11		Mode	Mixed(11b+)	11g+11n)
Tx Power	100%		Bandwidth	40 MHz	
Channel Status					
Channel Load	Q	44%			
Noise Floor		1%			
APs		12			
Max RSSI		5			
Min RSSI		31			
The history of	1-5 minutes	~			
72					
	\backslash				Load
36	\bigvee	$\rightarrow \sim$	$\sim\sim\sim$		
					Noise
0					
	5:11:38 1	6:12:38 1	6:13:38 16:14:	38 16:15:	:38

Diagnostics >> Interference Monitor

All Channels

Diagnostics >> Interference Monitor

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.

Band	2.4G	~	Refresh
Recommended o	channel for usage: 2		
Channel	Channel Utilization	Channel Energy	APs
1	34%	32%	3
2 1	1%	10%	0
3 1	<mark>.5%</mark>	13%	0
4	30%	29%	0
5	32%	31%	1
6	47%	32%	16
7	34%	32%	1
8 🚦	23%	23%	0
9	29%	29%	0
10	31%	29%	0
11	63%	42%	20

VI-1-8 Support Area

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



VI-2 Checking the Hardware Status

Follow the steps below to verify the hardware status.

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

VI-3 Checking the Network Connection Settings

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

VI-3-1 For Windows

(Note:

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**.

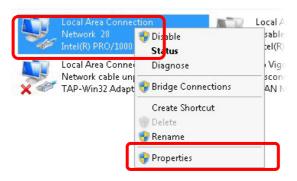
1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



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.

tworking Sharing		
🔮 Intel(R) PRO/1	000 MT Network Conne	ection
		Configure
his connection uses	the following items:	
🗹 🛃 Client for Mid		
🗹 💂 Privacyware		
🗹 📙 QoS Packet		10 IV
💷 📇 File and Prin	ter Sharing for Microsoft	Networks
		741
🗹 📥 Internet Prot	ocol Version 4 (TCP/IP) opology Discovery Map	

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

eneral Alternate Configuration 'ou can get IP settings assigned a his capability. Otherwise, you nee or the appropriate IP settings.	automatio				
Obtain an IP address autom	atically	٦			
- C. Use the following IP address					
IP address:			1		
Subnet mask:					
Default gateway:					
Obtain DNS server address a	automati	ally	٦		
C Use the following DNC come	e addrea		J		
Preferred DNS server:		- i.		- Q.	
Alternate DNS server:		2	,		
🔽 Validate settings upon exit				Adv	anced

VI-3-2 For Mac Os

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

● ● ○	Network	\bigcirc
Show All Displays S	with the second	
	Location: Automatic	
Т	P/IP PPPoE AppleTalk Proxies Ethernet	
Configure IPv4	I: Using DHCP	
IP Addres	s: 192.168.1.10 (Renew DHCP Lease)	
Subnet Mas	c: 255.255.255.0 DHCP Client ID:	
Route	r: 192.168.1.2 (If required)	
DNS Server	5: (Optional	D
Search Domain	5: Optional	Ð
IPv6 Addres	s: fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
	Configure IPv6	
Click the lock to	prevent further changes. Assist me Apply Nov	v

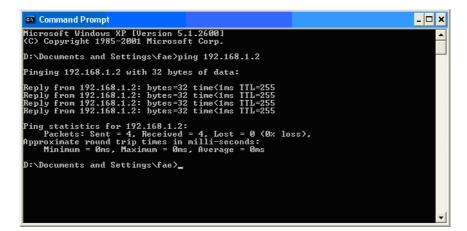
VI-4 Pinging the Device

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 V-2)

Please follow the steps below to ping the modem correctly.

VI-4-1 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.



- 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.

VI-4-2 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.

$\Theta \Theta \Theta$	Terminal — bash — 80x24	
Last login: Sat Jan Welcome to Darwin!	n 3 02:24:18 on ttyp1	S
Vigor10:~ draytek\$	2. 특히 가격 이번 것이 가격 이번 이번 것이 있는 것은 것은 것이 많이 있는 것은 것이 있는 것이 없다. 것이 있는 것이 있는 것이 없는 것이 없는 것이 없는 것이 없는 것이 없는 것이 없다. 것이 있는 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 있	
	192.168.1.1): 56 data bytes	
64 bytes from 192.1	168.1.1: icmp_seq=0 ttl=255 time=0.755 ms	
64 bytes from 192.1	168.1.1: icmp_seq=1 ttl=255 time=0.697 ms	
64 bytes from 192.1	168.1.1: icmp_seq=2 ttl=255 time=0.716 ms	
64 bytes from 192.1	168.1.1: icmp_seq=3 ttl=255 time=0.731 ms	
64 bytes from 192.1 ^C	168.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
192.168.1.1 pin	ng statistics	
5 packets transmitt	ted, 5 packets received, 0% packet loss /max = 0.697/0.723/0.755 ms	

VI-5 Backing to Factory Default Setting

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

(i) Warning:

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

VI-5-1 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

Do You want to reboot your AP ?
O Using current configuration
 Using factory default configuration

VI-5-2 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.

VI-6 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.