

VigorAP 1000C 802.11ac Ceiling-mount AP



USER'S GUIDE

V1.0

VigorAP 1000C

802.11ac Ceiling-mount AP

User's Guide

Version: 1.0

Firmware Version: V1.3.2

Date: March 4, 2020

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 10 and Explorer are trademarks of Microsoft Corp.
	 Apple and Mac OS are registered trademarks of Apple Inc.
	• Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions	 Read the installation guide thoroughly before you set up the modem. The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself. Do not place the modem in a damp or humid place, e.g. a bathroom. The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius. Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources. Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards. Keep the package out of reach of children. When you want to dispose of the modem, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.
Be a Registered Owner	Web registration is preferred. You can register your Vigor modem via http://www.draytek.com.
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents. http://www.draytek.com

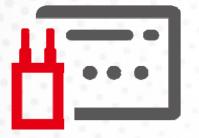
Table of Contents

Chapter I Installation	VII
I-1 Introduction	1
I-1-1 LED Indicators and Connectors	2
I-2 Hardware Installation	4
I-3 Network IP Configuration	
I-3-1 Windows 10 IP Address Setup	
I-4 Accessing to Web User Interface	
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	
Chapter II Connectivity	24
II-1 Operation Mode	
II-2 General Concepts for Wireless LAN (2.4GHz/5GHz)	
II-3 Wireless LAN (2.4GHz/5GHz/5GHz-2) 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	
II-3-7 WDS AP Status	
II-3-8 Bandwidth Management	
II-3-9 Airtime Fairness	
II-3-10 Station Control	53
II-3-11 Roaming	55
II-3-12 Band Steering (for Wireless LAN (2.4GHz))	
II-3-13 Station List	
II-4 Mesh Settings for Mesh Mode	68
II-4-1 Mesh Setup	
II-4-2 Mesh Status	
II-4-3 Mesh Discovery	
II-4-4 Configuration Sync II-4-5 Advanced Config Sync	
II-5 Universal Repeater Settings for Range Extender Mode	
II-6 LAN	
II-6-1 General Setup II-6-2 Port Settings	
······································	
Chapter III Management	
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 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	
Chapt	ter IV Others	
	IV-1 RADIUS Setting	
	IV-1-1 RADIUS Server	
	IV-1-2 Certificate Management	
	IV-2 Applications	
	IV-2-1 Schedule	
	IV-2-2 Apple iOS Keep Alive	
	IV-2-3 Wi-Fi Auto On/Off	
	IV-2-4 Sensor	101
	IV-2-4 Selisul	
Chapt		
Chapt	vter V Mobile APP, DrayTek Wireless	
Chapt	ter V Mobile APP, DrayTek Wireless	133
Chapt	t er V Mobile APP, DrayTek Wireless V-1 Introduction of DrayTek Wireless	
Chapt	t er V Mobile APP, DrayTek Wireless V-1 Introduction of DrayTek Wireless V-2 Select a VigorAP	 133
-	vter V Mobile APP, DrayTek Wireless V-1 Introduction of DrayTek Wireless V-2 Select a VigorAP V-3 Quick Start Wizard V-4 Login	133
-	 V-1 Introduction of DrayTek Wireless V-1 Introduction of DrayTek Wireless V-2 Select a VigorAP V-3 Quick Start Wizard V-4 Login 	133
-	vter V Mobile APP, DrayTek Wireless V-1 Introduction of DrayTek Wireless V-2 Select a VigorAP V-3 Quick Start Wizard V-4 Login	133
-	 V-1 Introduction of DrayTek Wireless V-1 Introduction of DrayTek Wireless V-2 Select a VigorAP V-3 Quick Start Wizard V-4 Login 	133 134 135 136 145 149 150
-	Ater V Mobile APP, DrayTek Wireless	133
-	Atter V Mobile APP, DrayTek Wireless	133
-	Atter V Mobile APP, DrayTek Wireless	133
-	Atter V Mobile APP, DrayTek Wireless	133
-	Atter V Mobile APP, DrayTek Wireless	133
-	Ater V Mobile APP, DrayTek Wireless	133
-	Atter V Mobile APP, DrayTek Wireless	133
-	Ater V Mobile APP, DrayTek Wireless	133 134 135 136 136 145 149 150 151 152 152 152 153 154 156 158
-	Ater V Mobile APP, DrayTek Wireless V-1 Introduction of DrayTek Wireless V-2 Select a VigorAP V-3 Quick Start Wizard V-4 Login V-4 Login V-1 Diagnostics VI-1 Diagnostics VI-1-1 System Log VI-1-2 Speed Test VI-1-3 Traffic Graph VI-1-4 Where am I VI-1-5 WLAN (2.4GHz) Statistics VI-1-7 WLAN (5GHz-2) Statistics VI-1-8 Interference Monitor VI-1-9 Support Area	133 134 135 135 136 145 149 150 151 151 151 152 152 152 153 154 155 156 158 158
-	Ater V Mobile APP, DrayTek Wireless V-1 Introduction of DrayTek Wireless V-2 Select a VigorAP V-3 Quick Start Wizard V-4 Login Ater VI Troubleshooting VI-1 Diagnostics VI-1 System Log VI-1-2 Speed Test VI-1-3 Traffic Graph VI-1-4 Where am I VI-1-5 WLAN (2.4GHz) Statistics VI-1-7 WLAN (5GHz-2) Statistics VI-1-8 Interference Monitor VI-19 Support Area VI-2 Checking the Hardware Status	133 134 135 136 136 136 136
-	Ater V Mobile APP, DrayTek Wireless. V-1 Introduction of DrayTek Wireless. V-2 Select a VigorAP V-3 Quick Start Wizard. V-4 Login V-4 Login V-1 Diagnostics VI-1 Diagnostics VI-1 System Log. VI-1-2 Speed Test. VI-1-3 Traffic Graph. VI-1-4 Where am I. VI-1-5 WLAN (2.4GHz) Statistics. VI-1-7 WLAN (5GHz) Statistics. VI-1-8 Interference Monitor VI-1-9 Support Area. VI-2 Checking the Hardware Status	133 134 135 136 136 136 136 136 136 145 149 150 151 151 152 152 153 154 155 156 158 159 160 160
-	Ater V Mobile APP, DrayTek Wireless. V-1 Introduction of DrayTek Wireless. V-2 Select a VigorAP V-3 Quick Start Wizard. V-4 Login Ater VI Troubleshooting. VI-1 Diagnostics VI-1 Diagnostics VI-1 Diagnostics VI-1 System Log. VI-1-2 Speed Test. VI-1-3 Traffic Graph. VI-1-4 Where am I. VI-1-5 WLAN (2.4GHz) Statistics. VI-1-6 WLAN (5GHz) Statistics. VI-1-7 WLAN (5GHz-2) Statistics. VI-1-8 Interference Monitor VI-1-9 Support Area. VI-2 Checking the Hardware Status VI-3 Tor Windows.	
-	Ater V Mobile APP, DrayTek Wireless. V-1 Introduction of DrayTek Wireless. V-2 Select a VigorAP V-3 Quick Start Wizard V-4 Login V-4 Login Atter VI Troubleshooting VI-1 Diagnostics VI-1 System Log. VI-1-2 Speed Test. VI-1-3 Traffic Graph VI-1-4 Where am I. VI-1-5 WLAN (2.4GHz) Statistics. VI-1-6 WLAN (5GHz-2) Statistics. VI-1-7 WLAN (5GHz-2) Statistics. VI-1-8 Interference Monitor VI-1-9 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	133 134 135 136 136 137 136 136 136 145 149 150 151 151 152 152 153 154 155 156 158 159 160 160 162 163

VI-5 Backing to Factory Default Setting	165
VI-5-1 Software Reset VI-5-2 Hardware Reset	
VI-6 Contacting DrayTek	166
ndex	167

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 this VigorAP 1000C!

As a tri-band AP, it provides an extra 5GHz Wireless band which increases the supported number of wireless devices. In Mesh mode or Range Extender mode, this extra band can also be dedicated as the Uplink band to the Internet. VigorAP 1000C is suitable to construct a small Wireless network.



VigorAP 1000C can operate in standalone mode for your office network or a classroom; connected to your LAN and offering you wireless access.

It makes high density with quality-performance be feasible for users as it is going to be implemented with DrayTek VigorACS 2 supports configuration, firmware upgrade, status, and monitoring.

The Power of Ethernet (PoE) on VigorAP 1000C relieves the installation of the power plug. The massive deployment of VigorAP 1000CC for hospitalities and school environment will be much easier.

With the optimized antennas built-in, DrayTek VigorAP 1000C ceiling-mount wireless access point is ideal for hospitalities, small offices, and small campus.

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

I-1-1 LED Indicators and Connectors

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



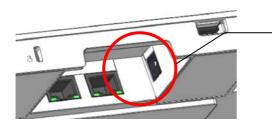
LED	Status	Explanation
5G-2 / 5G-1 / 2.4G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
P2 / P1(PoE)	On	The LAN port is connected.
(Left LED)	Off	LAN is disconnected.
(·)	Blinking	Data is transmitting (sending/receiving).
P2 / P1(PoE) (Right LED)	On	A normal connection (rate with 1000M) is through its corresponding port.
(Off	The LAN port is connected with a transmission rate of 10/100Mbps if left LED is on.



Connector P1(PoE) is used for PoE connection (for indoor use only).

- A	P2	P1(PoE)	

Interface	Description
RST	Restore the default settings. Usage: Switch on the access point. Press and hold reset button for at least 5 seconds. VigorAP will restart with the factory default configuration.
P2/P1(PoE)	Connectors for local networked devices.
USB	A connector for a USB device.
a 🛛	A security hole for installing the anti-theft lock.



The PWR connector (next to connector P1(PoE)) for a power adapter.

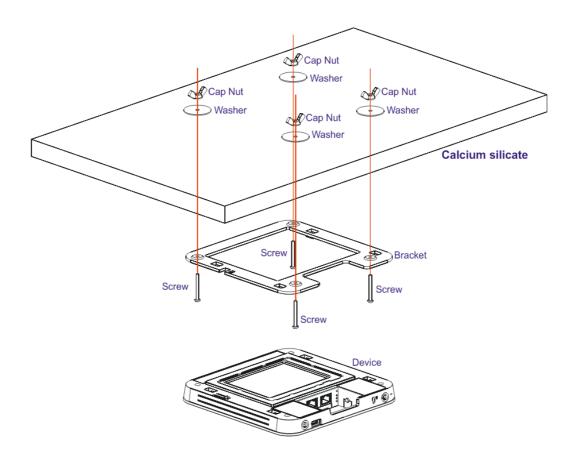
I-2 Hardware Installation

This section will guide you through installing the VigorAP.

(i) Note:

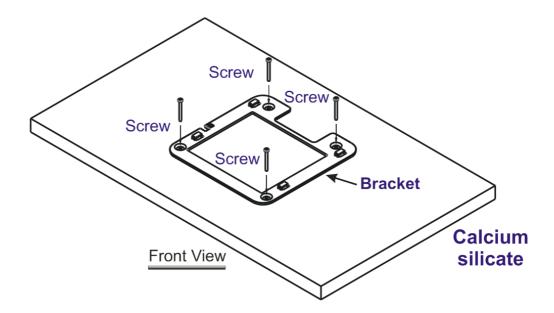
For the sake of personal safety, only trained and qualified personnel should install this access point.

VigorAP can be mounted on the board of calcium silicate. Below shows an exploded view of VigorAP installation.

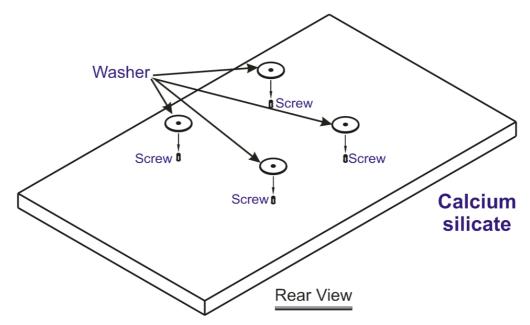


Follow the steps listed below to mount the access point.

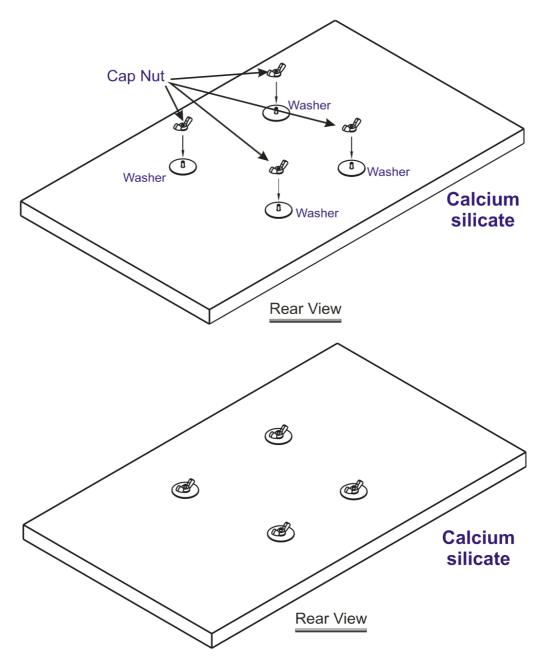
1. Place the bracket on the front side of the calcium silicate board and fasten it with four screws.



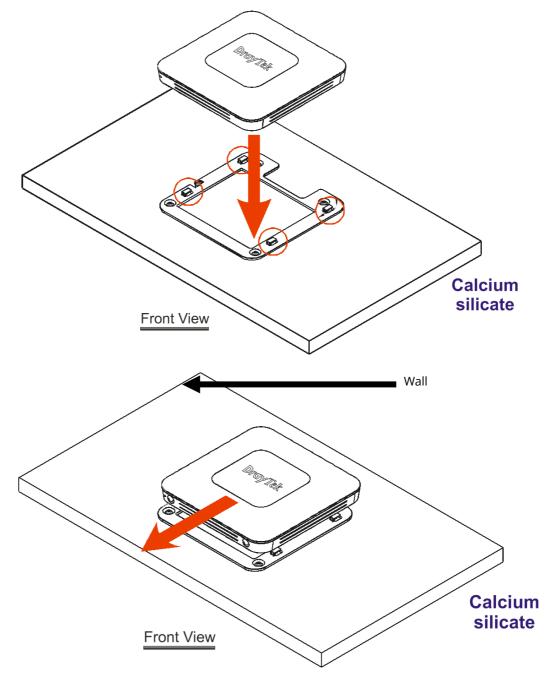
2. When the bracket is in place, reverse the board. Put the washer on the screw.



3. Insert the cap nut to the screw on the washer. Rotate the cap nut until it locks firmly on the washer.



4. There are four latches on the bracket. Put the device (VigorAP) on the bracket with the direction shown below.



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.

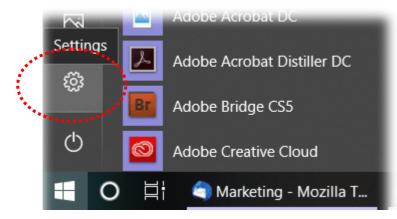
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address in the same subnet as this AP. If it's not connected to the same DHCP Server with the AP or you're unsure, please follow the following instructions to configure your computer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

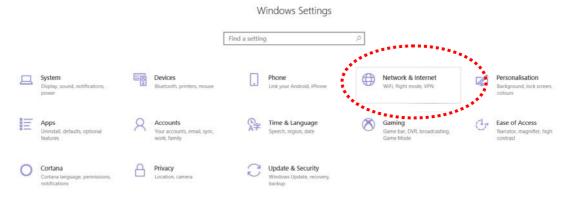
Windows 10 - please go to section I-3-1

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 ,	
← Settings		- 0
ය Home	Status	
Find a setting	Network status	Do you have a question? Get help
Network & Internet		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	Change connection properties Show weaking thetworks	
Proxy	Change your network settings	
	Change adapter options View network adapters and change connection settings. Surgeoptions For the network adapter and change connection settings. Network traditional set of the network adapters Network traditional set of the network and the network of the n	



Settings				0
	Windows Settings			
	Find a setting .0			
<- Settings				σ
ධ Home	Status			
Find a setting ,P	Network status		Do you have a question? Get help	
Network & Internet			Make Windows better Give us feedback	
Ethernet		- D	×	
🕾 Dial-up 👘 📼 🛧 🖢	Control Panel > All Control Panel Hands > Network Content cos	v O Search Ne.	P	
98° VPN Organise *		E • 0	0	
(9 Data usage	 AlbS-1 WinFi2 REB 32 REB 32 Realty kPCe GBE Family Co. WinFi2 Workes MU-MMO. 			
Ф Ргоху	· · · · · · · · · · · · · · · · · · ·			

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

🖳 Local Area Connection Properties 🛛	x
Networking Sharing	
Connect using:	
Realtek RTL8139/810x Family Fast Ethemet NIC	
Configure	
This connection uses the following items:	-
Client for Microsoft Networks QoS Packet Scheduler	
Generative Concerns of Microsoft Networks Generative Protocol Version 6 (TCP/IP♥6).	
🗹 🛥 Internet Protocol Version 4 (TCP/IPv4)	
 Link Laver Topology Discovery Member I/O Driver Link-Laver Topology Discovery Restander 	
E Enk-Layer topology Discovery hespitiber	
Install	
Description	
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
OK Cance	<u>+</u>

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 1000C 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**.

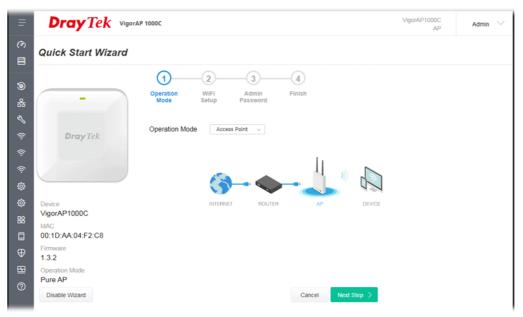
Dray Tek VigorAP1000C	User Name admin Password
	Login
(Copyright © 2018 DrayTek Corp

(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 1000C.**

- If there is no DHCP server on the network, then VigorAP 1000C will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 1000C 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:

Ŧ	DrayTek VigorAP 1000C		VigorAP1000C AP	Admin 💛
 Dashboard Quick Start Wizard 	WIRELESS CLIENTS PER RADIO	CHANNEL LOAD	DEVICE OVERVIEW Device Name VigorAP1000C	
 Operation Mode LAN > Central AP Management > 	0 0/128 0 0/128 5 GH₂ 0/128 5 GH₂ 0/128	Och 11 Moderate, 55% Moderate Ch 36 Light, 27% Ch 100 Light, 7%	IP Address 192.168.1.11 (via DHCP) Firmware 1.3.2 Uptime 0d 00.04.15	
 ♥ Wireless LAN (2.4GHz) > ♥ Wireless LAN (5GHz) > ♥ Wireless LAN (5GHz-2) > ♥ RADIUS Setting > Ø Objects Setting 	RADIO THROUGHPUT 2.4 GHz d. 0 bps d. 0 bps 5 GHz d. 0 bps d. 0 bps 5 GHz d. 0 bps d. 0 bps		Gateway 192.188.1.1 MAC 00.1D:AA:04.F2: Build Date r11481 Tue, 14 J 16:51:26 ACS Server	
B& Applications Applications Mobile Device Management System Maintenance	RECENT ACTIVITIES Last 24 hours		CPU Usage Memory Usage	2.1%
Diagnostics >	1.0	1.0 0.5 0 2AM SAM 8AM 11AM	WIRELESS OVERVIEW 2.4GHz Radio Enable MAC 00.1D/AA.04.F2.C8 SSID(1) DrayTek-04F2C8	~
	5 GHZ 1.0- 90 St 0.5	1.0 0.5 - 9	5GHz Radio Enable MAC 00:1D:AA:04:F2:C9	0

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	~
VigorAP1000C	Admin 💛	off	
off	^	1 min	
G Set Password	~	3 min	
V → Log Out		5 min	
1		10 min	
(1			

(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 2. Including non-alphanumeric charact	
	ain only a-z A-Z O-9 , ~ ` ! @ \$ % ^ * () _ + = {} [] ; < > . ? Itain only a-z A-Z O-9 , ~ ` ! @ # \$ % ^ & * () _ + = {} [] \ ; < > . ? /
	OK 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.

DrayTek VigorAP1000C	User Name admin Password
	Copyright © 2018 DrayTek Corp

I-6 Dashboard

Dashboard shows system status including the number of client connected, throughput, gateway, physical connection status, radio (2.4GHz / 5GHz / 5GHz-2) status, backhaul network, recent activities, wireless network usage, and so on.

=	DrayTek VigorAP 1000C		VigorAl	P1000C Admin V
 Dashboard 				
Quick Start Wizard	WIRELESS CLIENTS PER RADIO	CHANNEL LOAD	DEVICE OVERVIEW	
	• 2.4 GHz 0/128	Ch 11 Moderate, 55%		P1000C
Operation Mode	0 5 GHz 0/128	Moderate Ch36 Light 27%	IP Address 192.16 (via DF	
욺 LAN >	Clients 5 GHz2 0/128	• Ch 100 Light, 7%	Firmware 1.3.2	
			Uptime Od 00:0	04:15
🆏 Central AP Management >			Gateway 192.16	8.1.1
Wireless LAN (2.4GHz) >	RADIO THROUGHPUT	PORT STATUS	MAC 00:1D:	AA:04:F2:C8
⇔ Wireless LAN (5GHz)				Tue, 14 Jan 2020
🙊 Wireless LAN (5GHz-2)	2.4 GH₂ ≟ 0 bps ⊥ 0 bps		16:51:2	26
	5 GHz 🕹 0 bps 🗘 0 bps	30.10 50.10 50.10 50.10 50.10 50 50 50 50 50 50 50 50 50 50 50 50 50	ACS Server	•
RADIUS Setting >		2.45 0 F2 F1 F0E	SYSTEM RESOURCE	
ô Objects Setting >	5 GH22 🕁 0 bps 🗘 0 bps		CPU Usage	2.1%
88 Applications >			•	2.170
Mobile Device Management >	RECENT ACTIVITIES Last 24 hours ~		Memory Usage	65%
⊕ System Maintenance →	2.4 GHz Throughput Clients			_
Diagnostics	1.0-	1.0	WIRELESS OVERVIEW	\sim
⑦ Support →	that (set 1) 0.5	Cijents	2.4GHz	
() output	diraut	0.5 8	Radio Enable	0
	0	2AM 5AM 8AM 11AM	MAC 00:1D:AA:04:F2	2:08
		anni unu unu	SSID(1) DrayTek-04F20	8
	5 GHz		5GHz	
	1.0	1.0	Radio Enable	0
	in of the office	0.5 ee	MAC 00:1D:AA:04:F2	2:C9

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 /5G/5G-2 wireless setting and other corresponding settings for Vigor Access Point step by step.

(?) []]	Quick Start Wizard				
종	-	Operation V	2 ViFi Admin Password	Finish	
L ((i- (Dray Tek	Operation Mode	Access Point ~ Access Point ~		
(ŀ· (ŀ· ‡			Mesh Root Mesh Node Range Extender)	
\$ \$ ■	Device VigorAP1000C MAC 00:1D:AA:04:F2:C8		INTERNET ROUTER	AP	DEVICE
• ⊕ BI ©	Firmware 1.3.2 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.

Quick Start Wizard				
-	Operation V	2 3 ViFi Admin Password	-4 Finish	
DrayTek	Operation Mode	Access Point ~ Access Point ~ Mesh Root Mesh Node Range Extender	1	
Device VigorAP1000C MAC 00:1D:AA:04:F2:C8 Firmware 1.3.2 Operation Mode Pure AP		INTERNET ROUTER	ΑP	DEVICE
Disable Wizard			Cancel	ext Step >

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

 \sim

1

	0	-(2)		-4	
-	Operation Mode	WiFi Setup	Admin Password	Finish	
	Your AP is unde	er default co	nfig. Please setur	o first.	
Dray Tek	WiFi Name:		yTek-04F2C8		
	WiFi Password	•••	•••••		
	Enable 2nd	WiFi			
	2nd WiFi Name	9:			
Device	2nd WiFi Pass	word:			
VigorAP1000C MAC	Enable Ban	idwidth Limit	:		
00:1D:AA:04:F2:C8	Enable Stat	tion Control			
Firmware 1.3.2	Note: The WiFi	i settings wil	apply to all Wire	less bands.	
Operation Mode Pure AP					
< Back				Cancel	Next Step

Available settings are explained as follows:

ltem	Description
WiFi Name	Set a name for VigorAP 1000C 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 guest 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 device which can be identified and connected by wireless guest.
	2nd WiFi Password - Set 8~63 ASCII characters or 64 Hexadecimal digits leading by 0x which can be used for logging into VigorAP device 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 t 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**.

	(1)(2)	3	-(4)	
-	Operation WiFi Mode Setup	Admin Password	Finish	
	Your AP is under defaul	t config. Please setu	ıp first.	
Dray Tek	Admin Password:	•••••		
	Confirm Password:	•••••		
Device VigorAP1000C				
MAC 00:1D:AA:04:F2:C8				
Firmware 1.3.2				
Operation 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**.



÷

<u>(1)</u>			
U		J	4
Operation Mode	WiFi Setup	Admin Password	Finish

Basic settings are completed. Press Finish button apply changes.

	Operation Mode	Pure AP
	WiFi Name	DrayTek-04F2C8
	2nd WiFi Name	Disabled
1	Bandwidth Limit	Disabled
	Station Control	Disabled

Device VigorAP1000C MAC 00:1D:AA:04:F2:C8 Firmware 1.3.2 Operation Mode Pure AP

< Back

Cancel Finish

I-7-2 Settings for Mesh Root

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

	1	23)	
	Operation Mode	WiFi Adn Setup Passv		h	
Dray Tek	Operation Mode	Mesh Root 🛛 🗸			
	Group Name	VigorMesh			
		() -		, ,	
Device VigorAP1000C		INTERNET	ROUTER	MESH ROOT	MESH NODE
MAC 00:1D:AA:04:F2:C8					
Firmware 1.3.2					
Operation Mode Pure AP					
Disable Wizard			(Cancel	ext Step >

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

	1 2 3 4
- 7	Operation WiFi Admin Finish Mode Setup Password
	Your AP is under default config. Please setup first.
Dray Tek	WiFi Name: DrayTek-04F2C8
	WiFi Password:
	Enable 2nd WiFi
	2nd WiFi Name: marketing
Device	2nd WiFi Password:
VigorAP1000C	Enable Bandwidth Limit
MAC 00:1D:AA:04:F2:C8	Enable Station Control
Firmware 1.3.2	
	Note: The WiFi settings will apply to all Wireless bands.
Operation Mode Pure AP	
< Back	Cancel Next Step

Available settings are explained as follows:

ltem	Description
WiFi Name	Set a name for VigorAP 1000C 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 1000C which can be identified and connected by wireless guest.
	2nd WiFi Password - Set 8~63 ASCII characters or 64 Hexadecimal digits leading by 0x which can be used for logging into VigorAP 1000C 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**.

	Operation WiFi Mode Setup	Admin Password		
Dray Tek	Your AP is under default		up first.	
Diayick	Admin Password:	•••••		
	Confirm Password:	•••••		
Device VigorAP1000C				
MAC 00:1D:AA:04:F2:C8				
Firmware 1.3.2				
Operation 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	

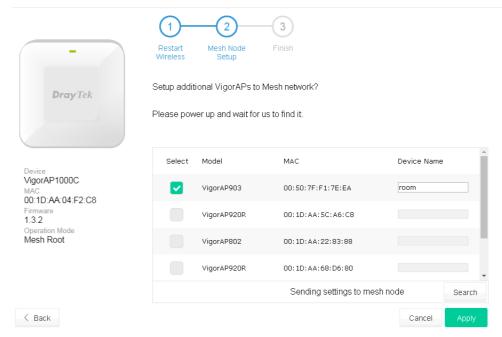
4. A summary of settings configuration will be shown on screen. Click **Finish**.

-		2 3 /iFi Admin etup Password	Finish	
DrayTek	Basic settings are c Operation Mode WiFi Name 2nd WiFi Name Bandwidth Limit Station Control	ompleted. Press Finish t Mesh Root DrayTek-04F2C8 marketing Disabled Disabled	button apply changes.	
Device VigorAP1000C MAC 00:1D:AA:04:F2:C8 Firmware 1.3.2 Operation Mode Pure AP Sack			Cancel	inish

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

1-2-	3			
Restart Mesh Nod Wireless Setup	e Finish			
Please wait for wireless	restart.			
-	(1) (2) Restart Mesh Node Wireless Setup	Finish		
DrayTek	Setup additional VigorAPs to Please power up and wait for			
Device VigorAP1000C MAC 00:1D:AA:04:F2:C8 Firmware 1.3.2 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.



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

-	Restart Wireless	2 Mesh Node Setup	Finish	
DrayTek		ional VigorAPs to I ver up and wait for u		
				Device Name
Device VigorAP1000C MAC 00:1D:AA:04:F2:C8				room
Firmware 1.3.2			00:1D:AA.50 A6:C8	
Operation Mode Mesh Root			00:1D:AA:22:83:88	
				sh node

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

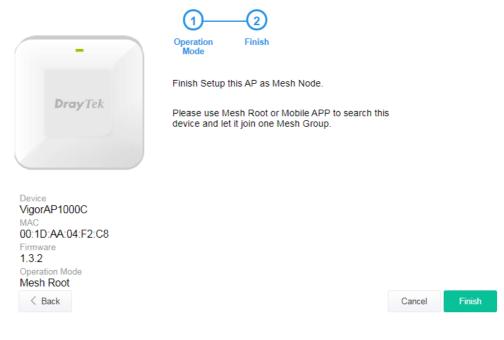
-	Restart Wireless	Mesh Node Setup	Finish		
Dray Tek	Setup 1 Mesh	Root and 1 M	lesh Node completed.		
	ROOT		VigorAP1000C VigorAP1000C		1 0 Node Offline
Device VigorAP1000C MAC 00:1D:AA:04:F2:C8 Firmware 1.3.2 Operation Mode Mesh Root			room VigorAP903	-Odbm ç	00:50:7F:F1:7E:EA
< Back				Cancel Finish	

I-7-3 Settings for Mesh Node

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



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



I-7-4 Settings for Range Extender

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



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

	1	2-		-4	5	
-	Operation Mode	WiFi Setup	Admin Password	Range Extender	Finish	
	Your AP is u	nder defa	ault config. Pl	ease setup fi	rst.	
Dray Tek	WiFi Name:		DrayTek-04F			
	WiFi Passw		•••••	•		
	2nd WiFi Na	ame:	marketing			
Device VigorAP1000C	2nd WiFi Pa	assword:	•••••	•		
MAC 00:1D:AA:04:F2:C8	Enable E	Bandwidt	h Limit			
Firmware 1.3.2	Enable S	Station C	ontrol			
Operation Mode Mesh Root	Note: The V	ViFi settir	ngs will apply	to all Wireles	s bands.	
< Back					Cancel	Next Step >

Available settings are explained as follows:

Item	Description
WiFi Name	Set a name for VigorAP 1000C 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 1000C which can be identified and connected by wireless guest.
	2nd WiFi Password - Set 8~63 ASCII characters or 64 Hexadecimal digits leading by 0x which can be used for logging into VigorAP 1000C 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**.

-	Operation Mode	2 WiFi Setup	Admin Password	Range Extender	Finish	
	Your AP is	under defa	ault config. Pl	ease setup f	irst.	
Dray Tek	Admin Pa	assword:	•••••			
	Confirm F	assword:	•••••			
Device VigorAP1000C						
MAC 00:1D:AA:04:F2:C8						
Firmware 1.3.2 Operation Mode						
Mesh Root					Cancel	Next Step >
Dath					Gancer	Next Step /

Available settings are explained as follows:

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

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 Mode) of the selected device will be shown below. Enter the Security Key. Then click **Next Step**.

	Mode Setup Pa:	3 4 dmin Range Extender GHz WLAN 5GI	-5 Finish Hz-2 WLAN				
DrayTek	SSID	BSSID	RSSI	Channel	Encryption	Authentication	
	FAE-Wendy-2925		56%(-75dbm)	11	AES	WPA2/PSK	
	FAE2925_Guest	02:1D:AA:F0:6D:F0	59%(-74dbm)	11 11	AES	WPA2	
	 DrayTek-3F4F4C DrayTekF19216 	00:1D:AA:3F:4F:4C	76%(-69dbm) 95%(-59dbm)	11	TKIP/AES	WPA2/PSK Mixed(WPA+W	
	 DrayTekF19216 918PQC helen 	02:50:7F:C1:92:16 00:1D:AA:04:F0:60	95%(-59dbm) 94%(-60dbm)	11	TKIP/AES TKIP/AES	Mixed(WPA+W Mixed(WPA+W	
ice	 DravTek-3F4F0A 	00:1D:AA:3F:4F:0A	84%(-67dbm)	11	AES	WPA2/PSK	PAZJ/POK
	 Vigor2927 POC T 	16:49:BC:42:37:D8	92%(-63dbm)	11	AES	WPA2/PSK WPA2/PSK	
prAP1000C	auests	06:1D:AA:3F:4F:86	98%(-54dbm)	1	AES	WPA2/PSK WPA2/PSK	
	 guests staffs 	02:50:7F:47:29:0C	28%(-83dbm)	1	AES	WPA2/PSK WPA2/PSK	
D:AA:04:F2:C8	Staris	12:1D:AA:04:F0:D8	73%(-70dbm)	1	AES	WPA2/PSK WPA2/PSK	
vare	o guests	02:50:7F:57:29:0C	32%(-82dbm)	1	AES	WPA2/PSK	
are	 guests staffs 	00:1D:AA:63:2C:10		1	AES	WPA2/PSK WPA2/PSK	
	G	12-1D-AA-3E-4E-86	100%(-53dbm)	1	AES	WDA2/PSK	
ion Mode Root							Sear
	SSID	Channel		Se	curity Mode	Encryp	tion Type
	guests	2412MHz (0	Channel 1) 🗸 🗸		WPA2/PSK	~ AES	~
	Security Key						
Back						Cancel	Next Step

Available settings are explained as follows:

ltem	Description
SSID	Displays the SSID of the selected access point.
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 AP 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/PSK or WPA2/PSK is selected:
	• Select TKIP or AES as the algorithm for WPA.
	Security Key - Enter 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**.



Device VigorAP1000C MAC 00:1D:AA:04:F2:C8 Firmware 1.3.2 Operation Mode Mesh Root < Back

Operation Mode	- 2 WiFi Setup	Admin Password	Range Extender	Finish
Basic setti	ngs are co	mpleted. Pres	ss Finish but	ton apply changes.

Operation ModeRange Extender (2.4GHz WLAN)Peer SSIDguestsWiFi NameDrayTek-04F2C82nd WiFi NamemarketingBandwidth LimitDisabledStation ControlDisabled

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:

 ${\sf AP}$ connects to gateway with Ethernet cable. It would be other ${\sf AP}$'s uplink connection.

Mesh Node:

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.



OK

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 1000C 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 1000C 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 1000C 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 1000C. 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 1000C 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 1000C) with the encryption of WPA and WPA2.



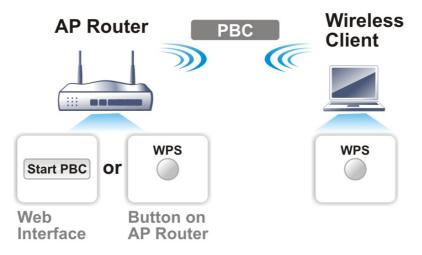
It is the simplest way to build connection between wireless network clients and VigorAP 1000C. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 1000C automatically.

(i) Note:

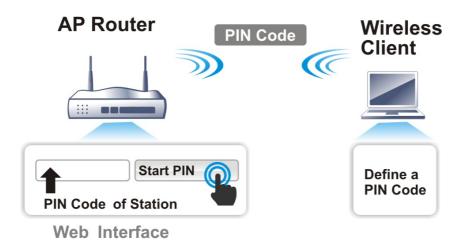
Such function is available for the wireless station with WPS supported.

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 1000C series which served as an AP, press **WPS** button once on the front panel of VigorAP 1000C 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 1000C.



II-3 Wireless LAN (2.4GHz/5GHz/5GHz-2) Settings for AP Mode

VigorAP 1000C is a tri-band, including 2.4GHz/5GHz/5GHz-2, access point. In which, the band of 5GHz-2 can deliver double bandwidths over 5GHz to offer more stable wireless performance.

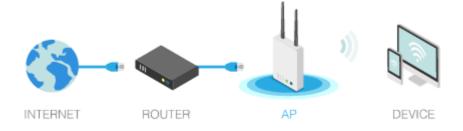
When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, WDS AP Status, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering (for 2.4GHz) and Station List.



(i) Note:

Available settings for **Wireless LAN (2.4GHz)**, **Wireless LAN (5GHz)** and **Wireless LAN (5GHz-2)** 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 select mode, channel, the SSID, the wireless channel, 2nd subnet and WDS. Please refer to the following figure for more information.

	802.11)			
nable Wireless	LAN			
Enable Clien	nt Limit 128 (3 ~ 128,	, default: 128)		
Enable Clien	nt Limit per SSID(3 ~ 128	, default: 128)		
Mode :	Mixed(11b+11g-	+11n) v		
Channel :	2462MHz (Chann	nel 11) 🗸 🗸		
Extension Chan	nel : 2442MHz (Chann	nel 7) 🗸		
Enable 2 Su	bnet (Simulate 2 APs)			
🗹 Enable Bridg	ge VLAN to Mesh			
Enable Hide SSID	SSID	Subnet	Isolate Isolate LAN Member	VLAN ID r(0:Untagged)
1	DrayTek-04F2C8	LAN-A 🗸		0
2 🗹 🗌	marketing	LAN-A 🗸		0
3		LAN-A 🗸		0
4		LAN-A 🗸		0
Hide SSID: Isolate LAN: Isolate Member: Isolate Exceptior	Prevent SSID from being Wireless clients (stations LAN. Wireless clients (stations other. I: Isolate Exception can be) with the same) with the same	e SSID cannot	access for each
	HY Mode : HTMIX)	D		
Security : Disabled	○ TKIP ○ AES	Peer MAC	Address :]:[]]:[]
Key :				
		2:		
		3:	: : : : : : : : : : : : : : : : : : : :	:
	configuration of APs which	4. 🗌 :		::

Available settings are explained as follows:

.

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 64.
Enable Client Limit per	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set

	is from 3 to 64.		
Mode	At present, VigorAP 1000C can connect to 11a only, 11n only, Mixed (11a+11n), and Mixed (11a+11n+11ac) stations simultaneously. Simply choose Mixed (11a+11n+11ac) mode.		
	Mixed(11b+11g+11n) \checkmark		
	11n Only		
	Mixed(11b+11g)		
	Mixed(11b+11g+11n) </td		
	(for 2.4GHz)		
	Mixed (11a+11n+11ac) ~		
	11a Only		
	Ac 11n Only (5G)		
	Ce Mixed (11a+11n)		
	(Si Mixed (11a+11n+11ac) ✓		
	SSID Subnet (for 5GHz / 5GHz-2)		
Channel	Means the channel of frequency of the wireless LAN.		
	As a tri-band access point, VigorAP offers different channels for WLAN 2.4GHz, 5GHZ and 5GHz-2 respectively.		
	You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please		
	You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please		
	You may switch channel if the selected channel is under serious		
Extension Channel (for 2.4GHz)	You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you. Filtered Out List - It will be shown if AutoSelect is selected as Channel . Click such link to access into Wireless LAN >> Advanced		
	 You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you. Filtered Out List - It will be shown if AutoSelect is selected as Channel. Click such link to access into Wireless LAN >> Advanced Settings page. 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. Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another 		
(for 2.4GHz) Enable 2 Subnet	 You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you. Filtered Out List - It will be shown if AutoSelect is selected as Channel. Click such link to access into Wireless LAN >> Advanced Settings page. 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. Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have 		
(for 2.4GHz) Enable 2 Subnet	 You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you. Filtered Out List - It will be shown if AutoSelect is selected as Channel. Click such link to access into Wireless LAN >> Advanced Settings page. 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. Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 1000C. If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to 		

SSID	Set a name for VigorAP 1000C to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Subnet	Choose LAN-A or LAN-B for each SSID. If you choose LAN-A, the wireless clients connecting to this SSID could only communicate with LAN-A.
lsolate 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.
lsolate 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 902 connects to.

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.

SID 1 SSID 2	SSID 3 SSID 4	
SSID	DrayTek-04F2C8	
Mode	WPA2/PSK 🗸	
	er if 802.1x is enabled.	
WPA		
WPA Algorithms	○ TKIP ○ AES ○ TKIP/AES	
Pass Phrase	•••••	
Key Renewal Interv	al 3600 seconds	
EAPOL Key Retry	💿 Enable i Disable	
WEP		
○ Key 1:		Hex 🗸
○ Key 2:		Hex 🗸
○ Key 3:		Hex 🗸
Key 4 :		Hex 🗸

Wireless LAN (2.4GHz) >> Security Settings

ltem	Description
Mode	There are several modes provided for you to choose.
	Disable - The encryption mechanism is turned off.
	WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.
	WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	WEP/802.1x - The built-in RADIUS client feature enables VigorAP 1000C to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.
	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field

	below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.
	WPA/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	WPA2/802.1x - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Type 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. 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 ASCI characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for WEP mode.

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

📀 RADIUS Server Setup - Google Chrome	XX]
① 不安全 192.168.1.11/wireless/radius.asp	
Radius Server	
Use internal RADIUS Server	
IP Address 0	
Port 1812	
Shared Secret DrayTek	
Session Timeout 0 second(s)	
ок Available settings are explained as follows:	

ed as follows: ıgs ۱

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

Use internal RADIUS Server	There is a RADIUS server built in VigorAP 1000C 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 1000C.		
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 SecretThe external RADIUS server and client share a secret that is used authenticate the messages sent between them. Both sides must 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.)		

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).

667D 4	COTO O		667D 4		
SSID 1	SSID 2	SSID 3	SSID 4		
	S	SID: Dray	/Tek-04F2C8		
	Po	Dicy: Di	isable 🗸		
			Address Filter		
	Index	MAC Addres	S	access comment	
	🔿 MAC 👩	Object			
	Device Grou	None 🗸	or Device Ob	ject None 🗸	
		Add	Limit:25	5 entries	
		ОК	Can	cel	
Backup ACL Cfg	: Backup	Upload Fro	m File: Uplo	ad	Restore

Wireless LAN (2.4GHz) >> Access Control

ltem	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 1000C. Disable M Activate MAC address filter Blocked MAC address filter
	Blocked MAC address filter

MAC Address Filter	Display all MAC addresses that are edited before.		
MAC	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.		
BackupClick it to store the settings (MAC addresses on MAC Address Fil table) on this page as a file.			
RestoreClick it to restore the settings (MAC addresses on MAC atable) from an existed file.			

II-3-4 WPS

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

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

Enable WPS	
Wi-Fi Protected Setup Information	
WPS Configured	Yes
WPS SSID	DrayTek-04F2C8
WPS Auth Mode	WPA2/PSK
WPS Encrypt Type	AES
Device Configure	
Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN
Status: Idle	

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

🗅 : WPS is Disabled.

♀: WPS is Enabled.

Waiting for WPS requests from wireless clients.

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 1000C 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 1000C. Only WPA2/PSK and WPA/PSK support WPS.			
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 1000C.			
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 1000C will wait for WPS requests from wireless clients about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 1000C 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 1000C 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.

Channel Bandwidth	🗌 20 MHz 📄 Auto 20/40 MHz 🔹 40 MHz				
Antenna	O 2T2R ○ 1T1R				
Tx Power	● 100% ○ 80% ○ 60% ○ 30% ○ 20%				
TX Power	0 10%				
Fragment Length (256 - 2346)	2346 bytes				
RTS Threshold (1 - 2347)	2347 bytes				
Country Code	(Reference)				
Auto Channel Filtered Out List	<u>1</u> 2 3 4 5 6 7 8 9 10				
	□ 11 □ 12 □ 13				
IGMP Snooping	• Enable O Disable				
Isolate 2.4GHz and 5GHz bands	• Enable O Disable				
Isolate members with IP	🔿 Enable 🗿 Disable				
WMM Capable	• Enable O Disable				
APSD Capable	🔿 Enable 🗿 Disable				
MAC Clone	🔿 Enable 🔹 Disable				
MAC Clone: Set the MAC address of of this MAC address mu	SSIDs and the Wireless client.Please notice that the last byte st be a multiple of 8.				
Note: Fragment Length takes effect whe	en mode is "11b Only" or "Mixed(11b+11g)".				

Wireless LAN (2.4GHz) >> Advanced Setting

Cancel

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 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.		
lsolate 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. 		
lsolate 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 devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. The default setting is Disable .		
MAC Clone	Click Enable and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this		

II-3-6 AP Discovery

VigorAP 1000C 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.

Wireless LAN (2.4GHz) >> Access Point Discovery

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
\bigcirc	1		12:1D:AA:04:F0:6C	25%(-84dbm)	11	AES	WPA2/PSK
\bigcirc	2	Ting_VC_2	00:1D:AA:E4:8E:80	11%(-88dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	3	DrayTek-04	00:1D:AA:04:F0:6C	22%(-85dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	4	rd8-ap1000	06:1D:AA:04:F0:6C	32%(-82dbm)	11	TKIP/AES	WPA2/PSK
\bigcirc	5		00:1D:AA:5E:D9:58	39%(-80dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	6	rd8rd8	00:1D:AA:57:5D:38	53%(-76dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	7	Ting_VC_2	00:1D:AA:3D:4F:14	39%(-80dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	8	Ting_VC_2	02:50:7F:C1:91:E7	8%(-89dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	9	DrayTek-LA	00:1D:AA:22:33:44	15%(-87dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	10	V2926_PQC	00:1D:AA:04:F0:D8	8%(-89dbm)	11	AES	WPA2/PSK
\bigcirc	11	staffs	02:50:7F:C1:7F:1D	91%(-64dbm)	1	AES	WPA2/PSK
\bigcirc	12	staffs	02:50:7F:C1:7E:CB	28%(-83dbm)	1	AES	WPA2/PSK
\bigcirc	13	guests	02:50:7F:D1:7F:1D	90%(-65dbm)	1	AES	WPA2/PSK
\bigcirc	14	guests	02:50:7F:D1:7E:CB	32%(-82dbm)	1	AES	WPA2/PSK
\bigcirc	15	guests	02:50:7F:D1:7E:EC	4%(-91dbm)	1	AES	WPA2/PSK
\bigcirc	16	DrayTek	00:1D:AA:92:6F:18	2%(-93dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	17	DrayTek	00:1D:AA:CB:A3:10	8%(-89dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	18	DrayTek	00:1D:AA:94:ED:E0	84%(-67dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	19	DrayTek	00:50:7F:F0:D5:B5	11%(-88dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	20	RD8_GW_24G	00:1D:AA:5B:A0:C8	5%(-90dbm)	13	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	21	staffs_2	00:1D:AA:62:0F:E8	19%(-86dbm)	3	AES	WPA2/PSK
\bigcirc	22	staffs_2	02:50:7F:C1:7E:CF	92%(-63dbm)	3	TKIP/AES	WPA2/PSK
\bigcirc	23	guests_2	02:50:7F:D1:7E:CF	91%(-64dbm)	3	TKIP/AES	WPA2/PSK
\bigcirc	24	rd8rd8	00:1D:AA:7F:5D:8C	2%(-93dbm)	4	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	25	guests_2	00:1D:AA:62:0F:E9	0%(-95dbm)	3	AES	WPA2/PSK
\bigcirc	26		12:1D:AA:63:2C:00	25%(-84dbm)	9	AES	WPA2/PSK
\bigcirc	27	PQC Mesh T	00:1D:AA:63:2C:00	22%(-85dbm)	9	AES	WPA2/PSK
\bigcirc	28	PQC-SmartP	00:1D:AA:04:F0:DC	0%(-95dbm)	11	AES	Mixed(WPA+WPA2)/PSK
\bigcirc	29	DrayTek-LA	02:1D:AA:20:33:44	0%(-95dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
\bigcirc	30	V2860Ln_PQ	00:1D:AA:DD:75:70	0%(-95dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK

Scan

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

ltem	Description
SSID	Display the SSID of the AP scanned by VigorAP 1000C.
BSSID	Display the MAC address of the AP scanned by VigorAP 1000C.
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 1000C.
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.

Each item is explained as follows:

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 1000C 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.

Wirele	Wireless LAN (5GHz) >> WDS AP Status				
WDS	AP List				
AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth	
		Refresh			

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.

SSID 1	SSID 2	SSID 3	SSID 4		
SSID Per Stat	ion Bandwidth Li		-04F2C8		
Enabl	e				
Upload	l Limit	User	defined \lor	К	bps (Default unit : K)
Downl	oad Limit	User	defined \lor	К	bps (Default unit : K)
Auto A	djustment				
Total (Jpload Limit	User	defined \lor	К	bps (Default unit : K)
	Download Limit		defined 🗸	K	bps (Default unit : K)
					g sent from a wireless station. ilable bandwidth.
		ОК	Ca	ncel	

Wireless LAN (2.4GHz) >> Bandwidth Management

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.

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.

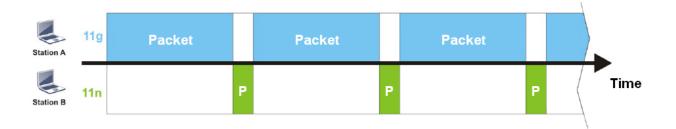
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

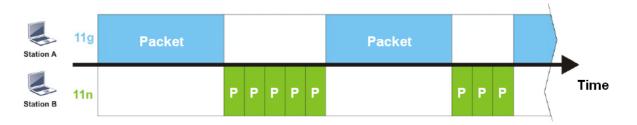
The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

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 1000C. 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 1000C. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



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

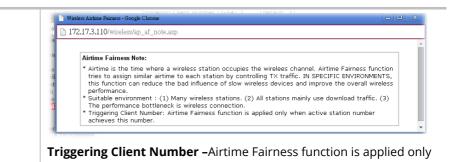
Suitable environment:

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

Wireless LAN (2.4GHz) >> Airtime Fairness

Enable Airtime Fairness			
Triggering Client Number 2	(2 ~ 128	3, Default: 2)	
Note: Please enable or disable this to NOT suitable for all environm		ling to the real situation and user experien	ce. It is
	ОК	Cancel	

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



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 (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-04F2C8	3
Enable			
Connection	Time	1 hour \sim	
Reconnecti	on Time	1 day \sim	
Display All	Station Control L	list	

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 (2.4GHz) >> Roaming

AP-assisted Client Roaming Parameters			
Minimum Basic Rate	1 ··· Mbps		
 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(WPA2/802.1x)			
Enable			
PMK Caching:Cache Period Pre-Authentication	10 minutes (10 ~ 600, Default: 10)		
	OK Cancel		

ltem	Description
AP-assisted Client Roaming Parameters	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 1000C 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 1000C 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 1000C 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

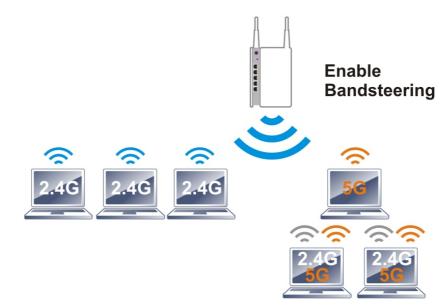
	 (defined in the field of With Adjacent AP RSSI over) is detected by VigorAP 1000C, VigorAP 1000C will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI). With Adjacent AP RSSI over – Specify a value as a threshold.
Fast Roaming (WPA2/802.1x)	Enable – Check the box to enable fast roaming configuration. 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 pro authenticated. Such foature is available for
	 SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode. Pre-Authentication - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication
	procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)
	Enable - Enable IEEE 802.1X Pre-Authentication.
	Disable - Disable IEEE 802.1X Pre-Authentication.

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 / 5GHz-2.

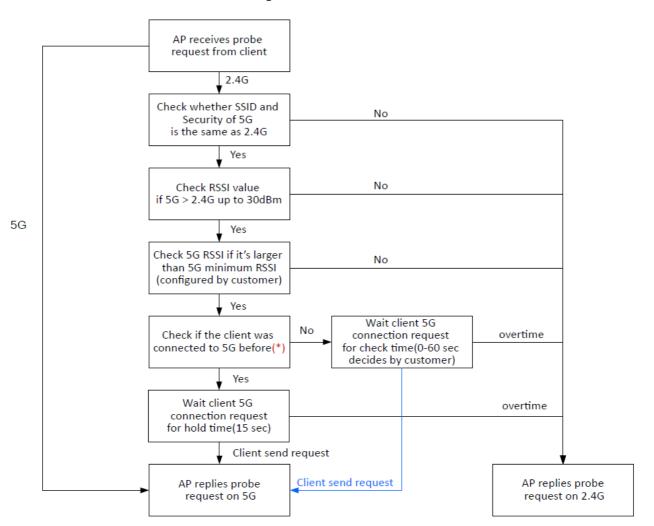
Open Wireless LAN (2.4GHz)>>Band Steering to get the following web page:

Wireless LA	l (2.4GHz) >>	Band Steering
-------------	---------------	---------------

E	nable Band Steering	
	Check Time for WLAN Client 5G Capabilit	y 15 seconds (1 ~ 60, Default: 15)
	Wait Full Time to Check 5G Capabi	lity
	🗹 5GHz Minimum RSSI	-78 dBm (29 %) (Default: -78)
	(Only do band steering when 5GHz signa	l is better than Minimum RSSI)
	Verloaded 🗸	
	2.4GHz Utilization Overload Threshold	70 % (Default: 70)
	5GHz Utilization Overload Threshold	70 % (Default: 70)
	(Only do band steering when 2.4GHz utili not)	zation is overloaded and 5GHz utilization is
Note:	Please setup at least one pair of 2.4GHz a security.	nd 5GHz Wireless LAN with the same SSID and
	ОК	Cancel

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 has 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 5GHz network connection, yet the signal performance might not be satisfied. Therefore, when the signal strength is below the value set here while the wireless station connecting to VigorAP 920RP, VigorAP will allow the client to connect to 2.4GHz network.
	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.



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	
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**, **Wireless LAN (5GHz)>>General Setup**, and **Wireless LAN (5GHz-2) >>General Setup**. Configure SSID as *ap1000-BandSteering* for these pages. Click **OK** to save the settings.

Wireless LAN (2.4 GHz) >> 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)	Wireless LAN (5GHz) >> General Setup
	General Setting (IEEE 802.11)
Mode: Mixed(11b+11q+11n) ~	C Enable Wireless LAN
Channel : 2417MHz (Channel 2) 🗸 (Active Chan	Enable Client Limit 128 (3 ~ 128, default: 128)
	Enable Client Limit per SSID (3 ~ 128, default: 128)
Extension Channel : 2437MHz (Channel 6) ~	Mode : Mixed (11a+11n+11ac) ~
Enable 2 Subnet (Simulate 2 APs)	Channel : 5260MHz (Channel 52) \vee (Active Channel: 44)
Enable Hide SSID Subnet Isolate Iso SSID Subnet LAN Me	
1 ap1000-BandSteerin LAN-A V	Enable 2 Subnet (Simulate 2 APs)
	Enable Hide SSID Subnet Isolate LAN ISolate VLAN ID SSID Subnet Isolate LAN Member (0:Untagged)
	1 ap1000-BandSteerin LAN-A V
Wireless LAN (5GHz-2) >> General	l Setup
General Setting (IEEE 802.11) Same value	
for 2.4GHz	28 (3 ~ 128, default: 128)
5GHz and	SSID (3 ~ 128, default: 128)
5GHz-2	
Mode :	Mixed (11a+11n+11ac) \sim
Channel :	5500MHz (Channel 100) 💛 (Active Channel: 100)
Details : []	DFS] 20/40MHz Ext Ch:104 , 80MHz Center Ch:106
Enable 2 Subnet (Sim	aulate 2 ABc)
Enable 2 Sublet (Sim	SSID Subnet Isolate LAN Member (0:Untagged)
A 2010	p1000-BandSteering LAN-A

Open Wireless LAN (2.4GHz)>>General Setup, Wireless LAN (5GHz)>>General Setup, and Wireless LAN (5GHz-2)>>General Setup. Configure Security as 12345678 for these pages. Click OK to save the settings.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4			
SSI			andSteering			
Mod	le	WPA2/P	PSK ~			
Set	up RADIUS Server	r if 802.1x is e	enabled.			
WPA						
WPA	A Algorithms	🔵 ТКІР	O AES ○ TKIP/AES	`		
Pass	s Phrase	•••••	••••			
Кеу	Renewal Interva		econds	J		
	OL Key Retry		/irelessLAN (5GHz) >> Security	y Settings		
WEP		/				
	Key 1:		SSID 1 SSID 2	SSID 3	SSID 4	
			Mode	WPA2/PS		
,			Set up RADIUS S WPA	erver if 802.1x is er	nabled.	
Same value			WPA Algorithms	🔘 ТКІР	o aes 🔿 tkip/aes	3
for 2.4GHz, 5GHz and -			Pass Phrase		•••	
5GHz and - 5GHz-2			Key Renewal Inte	erval 3600 sec	conds	
			EAPOL Key Retry	🗿 Enable	🔘 Disable	
``	`		WEP			
	Wireless LA	N (5GHz-2)>> S	Security Settings			Hex ~
	ssip 1	. SSID	0 2 SSID 3 S	SSID 4		
		SSID	ap1000-BandS	teerin		
		Modie	WPA2/PSK	~		
		\backslash	\			
			US Server if 802.1x is enable	ed.		
	WP	A WPA Algorith		AES 🔿 TKIP/AE	<u> </u>	
		Pass Phrase				
		Key Renewal	l Interval 3600 second			
	WE	Key Renewal EAPOL Key R	l Interval 3600 second			

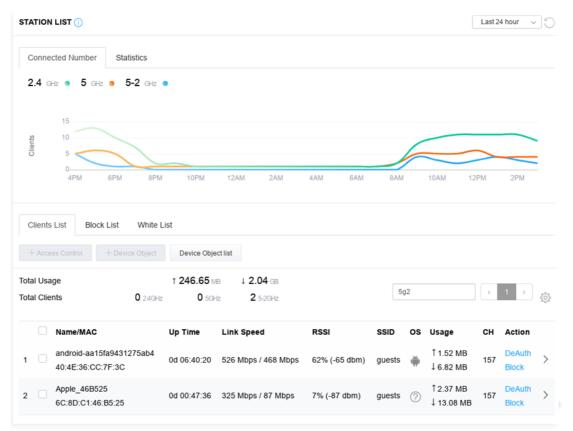
6. Now, VigorAP 1000C will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

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.

STAT	ION L	.IST ()							L	ast 24 hour	~ D
Co	nnect	ed Number Statistics									
	ſ	0% 0% Device OS 0% 100%	 Android 0 IOS 0 Windows 0 Linux 0 Others 58 		Polic	у	100% 0%	 Pass 58 Block 0 		I	5
Cli	ents L	ist Block List White L	List								
	Access	S Control + Device Object	Device Object	list							
Total Total	-			8.13 кв ↓ 45.89 кв 0 24GHz 64 5GHz	5g	4	1	2 3 4	5	6 7 >	÷
		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	1̂ 867 В ↓717 В	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	?	1 867 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	0	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	?	1̂ 867 В ↓717 В	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	?	1 867 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	1̂ 867 В ↓717 В	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	?	1̂ 867 В ↓717 В	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	?	1̂ 867 В ↓717 В	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	0	1 903 B ↓717 B	36	DeAuth Block	>

II-3-13-3 Clients List

The client list displays all the stations connecting to VigorAP.

	N LIST ()							L	ast 24 hour	C
Conne	ected Number Statistics									
(0% Device OS 0% 100%	 Android 0 iOS 0 Windows 0 Linux 0 Others 58 	1	Policy		100% 0%	Pass 58Block 0			
Clients + Acce	ts List Block List White	List Device Object	list							
Total Usa Total Clie	-		8.13 кв ↓ 45.89 кв 0 2.4GHz 64 5GHz	5g	ć	1	2 3 4	5	6 7 >	\$ <u>\$</u>
	Name/MAC	Up Time	Link Speed	RSSI	SSID	os	Usage	сн	Action	
1 [Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:42:47	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1̂ 867 В ↓717 В	36	DeAuth Block	>
2	 Unknown_07B0C1 00:BC:DA:07:B0:C1 	0d 03:42:47	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
3	Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:42:47	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1̂ 867 В ↓717 В	36	DeAuth Block	>
4 (Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:42:46	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>

Available settings are explained as follows:

em	Description						
Access Control	lt is availa List.	ble after choc	osing one of th	ne entries (clients) on Clients			
	Add Access	Control					
	Wireless LAN 5GHz ~						
	De SSID Policy	1 Black list AA-903	2 Disable ~ 3 AA-903-2	Disable v 4 Disable v AA-903-3 AA-903-4			
	From to list	D					
		Device MAC	Name	Apply to SSID			
	.s	00:BC:DA:07:B0:C1	Unknown_07B0C1	All 1 2 3 4			
		00:BC:DA:C3:4F:0A	Unknown_C34F0A	All 1 2 3 4			
	Total : 0/256						

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 saving 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 Usage - 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.

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.			

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	s List Block List W	hite List									
+ Acc	ess Control + Device	Object	evice 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										

ltem	Description					
Device Object list	Click it to open the Device Object List dialog for reference.					
	Profidx	MAC	Name			
		1	00:50/7F/F1:91:8C	TEST_1		
	2	00:50:7F:00:92:BA	TEST_2			
Name / MAC	Display the h	ost name / MAC Addres	s for the connecting client.			
SSID	Display the SSID that the wireless client connects to.					
Action	Display the a	iction that you can execu	ite for the station.			
	Block - Click	to block the entry.				

II-4 Mesh Settings for Mesh Mode

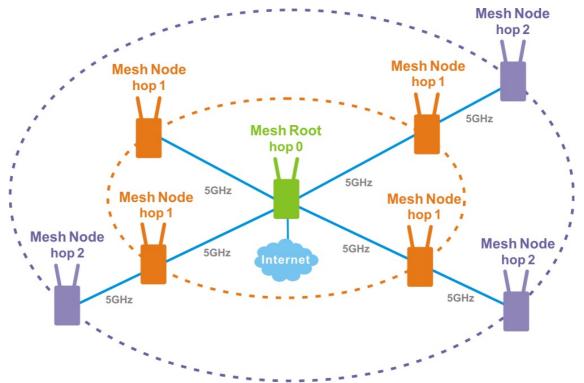
When you choose **Mesh** as the operation mode, the Mesh menu with the settings of Mesh Setup, Mesh Status, Mesh Discovery and Configuration Sync will be shown on the screen.

}∞ Mesh	~
Mesh Setup	
Mesh Status	
Mesh Discovery	
Basic Config Sync	
Advanced Config Sync	

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.

esh Setup				
tup				
		💿 Mesh Root 🛛 🔾	Mesh Node	
Name		VigorMesh		
		Basic 🗸		
up				
Index	Role	MAC Address		Model
1	Root	00:1D:AA:04:F2:	C8	VigorAP1000C
		ОК	Cancel	
Node				
rch butto	n below to	find and adopt the ne	w node into Mesh gr	oup.
1				
sh Config	l.			
D		Upload		Restore
	tup Name Ip Index 1 Node rch butto	tup Name Ip Index Role 1 Root Node rch button below to	tup Name VigorMesh Basic Jp Index Role MAC Address 1 Root 00:1D:AA:04:F2: OK Node rch button below to find and adopt the ne	tup Mesh Root Mesh Node Name VigorMesh Basic Jp Index Role MAC Address 1 Root 00:1D:AA:04:F2:C8 OK Cancel Node rch button below to find and adopt the new node into Mesh green and

Item	Description
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.
	Group Name - Display the name of the current mesh group.
When Mesh Root is selected	Log Level – Choose Basic or Detailed. Related information will be shown on the Diagnostics>>System Log.
When Mesh Node is selected	Wired Uplink – Check the box if such VigorAP connects to an uplinked mesh root or an uplinked mesh node with an Ethernet cable.
	Wireless Uplink Band – Choose a wireless band for connecting with an uplinked mesh root or an uplinked mesh node.
	Log Level – Choose Basic or Detailed. Related information will be shown on the Diagnostics>>System Log.
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 List Select MAC Address Model Operation Mode Device Name O0:1D: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. Upload/Restore – Click the Upload 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.

General Setup			
Role	ſ	🔾 Mesh Root 🕓 Mesh No	de
Group Name		VigorMesh	
Log Level		Basic 🗸	
Mesh Group			
Select Index	Role	MAC Address	Model
1	Root	00:1D:AA:04:F2:C8	VigorAP1000C
Reset			
		OK	cel
Add Mesh Node		find and adopt the new node i	nto Mesh group.
	n below to		

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

	Index	Role	MAC Address	Model	
	1	Root	00:1D:AA:04:F2:C8	VigorAP1000C	
Rese	et				
			OK C:	ancel	
d Mesh	Node				
id Mesh ress Se		ton below	to find and adopt the new nod	e into Mesh group.	
	earch but	ton below	to find and adopt the new nod	e into Mesh group.	
ress Se Sear	earch but		to find and adopt the new nod	e into Mesh group.	

3. Wait until the searching result appears.

Press S Seai		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	VigorAP903	MeshNode(Wireless)	
	00:1D:AA:04:F0:10	VigorAP1000C	MeshNode(Wireless)	
	00:1D:AA:32:BC:24	VigorAP920RPD	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)	

Backup Mesh Config

Backup Unload Restore
Backup Upload Restore

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.

ress S Sear		ind and adopt the ne	ew node into Mesh group.	
Search				
Select	MAC Address	Model	Operation Mode	Device Name
	00:50:7F:F1:7E:EA	VigorAP903	MeshNode(Wireless)	room1
	00:1D:AA:04:F0:10	VigorAP1000C	MeshNode(Wireless)	room2
	00:1D:AA:32:BC:24	VigorAP920RPD	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

Backup Upload Restore

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

ess S	earch button below to f	ind and adopt the ne	ew node into Mesh group.	
Sear	rch			
Search	List			
Select	MAC Address	Model	Operation Mode	Device Name
	00:50:7F:F1:7E:EA	VigorAP903	MeshNode(Wireless)	room1
✓	00:1D:AA:04:F0:10	VigorAP1000C	MeshNode(Wireless)	room2
	00:1D:AA:32:BC:24	VigorAP920RPD	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
Арр	ly 🌋			
ackup M	Mesh Config			
Back	an	Upload	R	estore

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	VigorAP 1000C		
MAC Address	00:1D:AA:04:F2:C8		
Model	VigorAP 1000C		
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 (VigorAP903)	Wireless 5GHz (Ch36) (-33dBm)	

Index	x Status	Device Name	IP Address	MAC Address (Model)	Нор	Uplink	Uptime	Clients
1	 Root 	VigorAP1000C	172.17.3.97	00:1D:AA:04:F2:C8 (VigorAP1000C)	0		Od 01:16:17	0
2	- Online	room1	172.17.3.12	00:50:7F:F1:7E:EA (VigorAP903)	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
🔍 Or	nline(sync read	y) 😑 Online	Offline			Last updated:	18:40:	51 202

II-4-2 Mesh Status

This page shows that one Mesh Group can contain up to 8 devices. In the following figure, the 7th Device with hop 0 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	VigorAP1	000C				
MAC Address	00:1D:AA	A:04:F2:C8				
Model	VigorAP1	000C				
Operation Mode	MeshRoot	t				
Group Name	VigorMes	h				
Link Status	Connecte	d				
Нор	0					
Downlink Number	0					
Devices					Total	number of Clients: 0
Index Status	Device Name	IP Address	MAC Address (Model)	Hop Uplink	Uptime	Clients Speed Tes
1 🔍 Root	VigorAP100	192.168.1.11	00:1D:AA:04:F2:C8 (VigorAP1000C)	0	0d 03:13:02	0
Online(sync read)	r) 😑 Online	Offline		Last upda	ated: Thu Feb	27 17:08:22 202

ltem	Description							
Local Status	Display general	informat	tion fo	r such V	'igor	AP.		
Devices	Display detailed node(s) in the g		ition fo	or this Vi	igor	AP (as me	sh roo	t) and me
	Index – Display	the num	ber of	the dev	vice	within a m	nesh g	roup.
	Status – Display	/ the role	e of the	e device	with	nin a mesł	ר grou	p.
	Device Name –	Display	the na	me of th	ne d	evice (for i	identi	fication).
	IP Address – Di							-
	MAC Address –						ice.	
	(wired). "1" to "3 group and it cor					•		
		nnects to y the MA	o other C addr	access ress of t	poir he d	it via wirel	less lir	ık.
	group and it cor Uplink – Display to.	nnects to y the MA	o other C addr	access ress of t	poir he d	it via wirel	less lir	ık.
	group and it cor Uplink – Display to. Display the station Station List of All Devices	y the MA on list of	o other C addr f all me	access ress of t esh devi	poir he d ces.	evice that	less lir the A	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices	nnects to y the MA ion list of	o other C addr f all me	access ress of t esh devi	poir he d ces.	el RSSI 68%(-63dBm) 41%(-73dBm)	less lir the A	ık. P connect
	group and it cor Uplink – Display to. Display the stati Station List of All Devices Index MAC Address	the MA ion list of	o other C addr f all me Vendor DrayTek	access ress of t esh devi	poir he d ces.	evice that evice that 68%(-63dBm) 41%(-73dBm) 100%	the A TxRate(Kb 0	nk. P connect: ^{pps)} RxRate(Kbps) 0
	group and it cor Uplink – Display to. Display the station Station List of All Devices 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:56:F2:52	hnects to y the MA ion list of Hostname TA001029 ta002171 Tze-Pingde Tyronetkil	o other C addr f all me DrayTek DrayTek DrayTek Apple	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F	poir he d ces.	el RSSI 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-68dBm)	the A	nk. P connect:
	group and it cor Uplink – Display to. Display the station 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:58:F2:52 5 00:50:71:37:60:E3:52	Hostname TA001029 ta002171 Tze-Pingde Tyronetkil N/A	o other C addr f all me DrayTek DrayTek Apple Apple DrayTek	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	poir he d ces.	evice that evice that 6%(-63dBm) 10% (-49dBm) 5%(-69dBm)	the A	nk. P connect:
	group and it cor Uplink – Display to. Display the stati Station List of All Devices I dours MAC Address 1 00:50:7F:F0:09:72 2 00:50:7F:F0:D1:10 3 5C:97:F3:00:E5 6 00:50:7F:37:60:E5 6 00:50:7F:37:60:E5	Hostname TA001029 ta002171 T2e-Pingde Tyronetkil N/A	o other C addr f all me DrayTek DrayTek Apple DrayTek DrayTek DrayTek	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	poir he d ces.	el RSSI 6896(-63dBm) 41%(-73dBm) 100% (-94dBm) 55%(-66dBm) 55%(-66dBm)	TxRate(Kb 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station 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:58:F2:52 5 00:50:71:37:60:E3:52	Hostname TA001029 ta002171 Tze-Pingde Tyronetkil N/A N/A	o other C addr f all me DrayTek DrayTek Apple Apple DrayTek	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	poir he d ces.	evice that evice that 6%(-63dBm) 10% (-49dBm) 5%(-69dBm)	the A	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:1D0 3 5C:97:F3:D3:D5:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:60:E110 3 5C:97:F3:76:DE:3D 5 00:50:7F:37:67:BE 7 30:F7:C5:1D:3D:111 8 40:F0:2F:22:EB:A0	Hostname TA001029 ta002171 Tze-Pingde Tyronetkii N/A N/A N/A	o other C addr C addr f all me DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F guests staffs_4F	ces.	evice that evice that 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-68dBm) 55%(-68dBm) 55%(-68dBm) 33%(-75dBm) 34%(-75dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 00:50:7F:F0:02:10 3 50:57:F10:02:10 3 50:57:F3:03:05:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:60:E5 6 00:50:7F:37:67:E5 7 30:F7:C5:1D:30:111 8 40:F0:F2:22:E8:A0 9 18:65:90:DE:D4:E5	Hostname TA001029 ta002171 Tze-Pingde Tyronetkii N/A N/A N/A N/A	o other C addr f all me ^{Vendor} DrayTek DrayTek DrayTek Apple DrayTek DrayTek Apple LiteonTe Apple	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	ces.	el RSSI 66%6/c63dBm) 100% (-49dBm) 55%6/c6dBm) 55%6/c6dBm) 55%6/c6dBm) 34%6(-76dBm) 100% (-44dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:70:02:12 3 5C:97:F3:02:05:F7 4 40:98:AD1:5B:F2:52 5 00:50:7F:37:67:BE 7 30:F7:C3:1D:3D1:11 8 40:F0:2F:22:EB:A0 9 18:65:90:DE:D4:E5 10 60:45:CB:57:1F:35	Hostname TA001029 Ta001029 Ta0021029 Ta0021029 Ta0021029 Ta0021029 Ta0021029 Ta002029 Ta002029 Ta002029 Ta002029 Ta002029 Ta002020 Ta0020 Ta00	o other C addr f all me DrayTek Apple Apple DrayTek Apple LiteonTe Apple N/A	access ress of t esh devi 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.	evice that 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 52%(-68dBm) 52%(-68dBm) 52%(-68dBm) 34%(-75dBm) 100% (-44dBm) 15%(-84dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:1D 3 5C:97:F3:C0:72 2 00:50:7F:70:C1:D 3 5C:97:F3:C0:72 5 00:50:7F:37:67:BE 7 30:F7:C5:1D:30:11 8 40:F0:C5:1D:30:11 8 40:F0:F0:F0:11 8 40:F0:F0:F0:11 8 40:F0:F0:F0:11 8 40:F0:F0:F0:11 8 40:F0:F0:F0:11 8 40:F0:F0:F0:11 8 40:F0:F0:F0:F0:11 8 40:F0:F0:F0:F0:F0:F0:F0:F0:F0:F0:F0:F0:F0	Hostname TA001029 ta002171 Tze-Pingde Tyronetkii N/A N/A N/A N/A N/A N/A N/A	o other C addr C addr f all me DrayTek DrayTek DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple Nray Apple Nray Apple Nray Apple Nray Apple	access ress of t esh devi 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.	el RSSI 66%(-63dBm) 100% (-49dBm) 55%(-68dBm) 55%(-68dBm) 83%(-57dBm) 100% (-44dBm) 100% (-44dBm) 10%(-84dBm) 15%(-84dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:1D 3 5C:97:F3:C0:72 2 00:50:7F:37:60:E1 3 5C:97:F3:C0:F2 5 00:50:7F:37:60:E1 4 40:98:AD:58:F2:52 5 00:50:7F:37:60:E1 9 18:65:90:DE:D4:E5 10 60:45:C8:57:1F:36 11 Ac:5F:1E:62:E6:C0	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	o other C addr f all me DrayTek Apple Apple DrayTek Apple LiteonTe Apple N/A	access ress of t esh devi 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	poir he d ces.	evice that 68%(-63dBm) 41%(-73dBm) 100% (-49dBm) 52%(-68dBm) 52%(-68dBm) 52%(-68dBm) 34%(-75dBm) 100% (-44dBm) 15%(-84dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:F0:C9:72 2 00:50:7F:F0:D1:10 3 5C:97:F3:03:D5:F7 4 40:98:AD:5B:F2:52 5 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 10 60:45:C8:57:1F:36 11 AC:5F:3E:62:E6:00 12 50:0E:66:E0:001 12 50:0E:66:E0:001 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	o other C addr C addr f all me Vendor DrayTek DrayTek DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple N/A Samsung Apple N/A	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	poir he d Ces.	et rssi 68%(-63dBm) 41%(-73dBm) 100% 5%(-68dBm) 55%(-68dBm) 55%(-68dBm) 35%(-76dBm) 100% (-44dBm) 15%(-44dBm) 15%(-44dBm) 15%(-44dBm) 15%(-24dBm) 45%(-72dBm)	TxRate(Kb TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:F0:C0:1D 3 5C:97:F3:D3:D5:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:6D:E1D 3 5C:97:F3:76:DE:E1D 3 5C:97:F3:76:DE:E1D 3 5C:97:F3:76:DE:E1D 3 5C:97:F3:16:2E:E1:A0 9 18:65:90:DE:E4:E5 10 60:45:CE:57:1F:36 11 AC:5F:3E:62:E6:00 12 50:EC:96:E0:00:111 13 04:B1:67:52:48:90 14 04:C2:3E:3F:CB:F6	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	o other C addr C addr f all me DrayTek DrayTek DrayTek Apple DrayTek Apple DrayTek Apple N/A Apple N/A Apple N/A	access ress of t esh devi 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	poir he d ces.	el RSSI 66%(-63dBm) 100% (-49dBm) 55%(-66dBm) 23%(-66dBm) 55%(-66dBm) 100% (-44dBm) 100% (-44dBm) 10% 10% (-44dBm) 10% 55%(-66dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:F0:C9:72 2 00:50:7F:F0:D1:10 3 5C:97:F3:03:D5:F7 4 40:98:AD:5B:F2:52 5 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 6 00:50:7F:37:67:DE5 10 60:45:C8:57:1F:36 11 AC:5F:3E:62:E6:00 12 50:0E:66:E0:001 12 50:0E:66:E0:001 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	o other C addr C addr f all me Vendor DrayTek DrayTek DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple N/A Samsung Apple N/A	access ress of t esh devi staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F staffs_4F	poir he d Ces.	et rssi 68%(-63dBm) 41%(-73dBm) 100% 5%(-68dBm) 55%(-68dBm) 55%(-68dBm) 35%(-76dBm) 100% (-44dBm) 15%(-44dBm) 15%(-44dBm) 15%(-44dBm) 15%(-24dBm) 45%(-72dBm)	TxRate(Kb TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the statistical station List of All Devices Index MAC Address 1 00:50:7F:F0:09:72 2 00:50:7F:F0:09:72 3 5C:97:F30:09:72 4 40:98:AD:5B:F2:52 5 00:50:7F:37:60:E5 6 00:50:7F:37:67:E6 7 30:F7:C5:1D:30:D1:11 8 40:F0:F2:22:E8:A0 9 18:65:90:DE:D4:E5 10 60:45:C9:F1:36:67:11:36 12 50:30:C9:6:E0:00:11 13 04:B1:67:52:48:90 14 04:C2:23:F2:E8:F8 15 0:35:05:79:13:10:87:78	Hostname TA001029 ta002171 T2c-Pingde N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	o other C addr C addr f all me DrayTek DrayTek Apple DrayTek Apple DrayTek Apple DrayTek Apple DrayTek DrayTek Apple Nra Samsung Apple N/A HTC	access ress of t esh devi 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. chann 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	el RSSI 6896(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-66dBm) 55%(-66dBm) 33%(-57dBm) 100% (-44dBm) 15%(-64dBm) 10% (-44dBm) 15%(-62dBm) 45%(-72dBm) 55%(-66dBm) 55%(-66dBm) 55%(-66dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
Total number of Clients	group and it cor Uplink – Display to. Display the station Station List of All Devices 1 00:50:7F:F0:C0:10 3 5C:97:F3:D3:D5:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:60:E1:10 3 5C:97:F3:C0:E5 6 00:50:7F:37:60:E5 7 30:F7:C5:10:30:11 8 40:F0:2F:22:E8:A0 9 18:65:90:0E:04:E5 10 60:45:0E:57:1F:36 11 AC:5F:3E:62:E6:00 12 50:BC:96:E0:00111 3 04:B1:67:52:48:90 14 04:C2:3E:3F:CB:F8 15 00:28:FD:31:08:78 16 58:48:22:EB:F8:62:E1 16 58:48:22:EB:F8:E1 17 CC:9F:7A:63:11:27 18 20:47:04:58:11:27	Hostname TA001029 ta002171 Tze-Pingde Tyronetkil N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	o other C addr C addr f all me DrayTek DrayTek Apple DrayTek Apple LiteonTe Apple LiteonTe Apple N/A HTC Intel Sony N/A	access ress of t esh devi staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4Fstaffs_4F staffs_4Fstaffs_4Fstaffs_4F staffs_4F	Cess.	evice that evice that 6%%(-63dBm) 100% (-49dBm) 5%(-69dBm) 5%(-69dBm) 5%(-69dBm) 100% (-44dBm) 15%(-64dBm) 13%(-75dBm) 10% (-44dBm) 15%(-68dBm) 5%(-68dBm)	TxRate(Kb TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:
	group and it cor Uplink – Display to. Display the station Station List of All Devices Index MAC Address 1 00:50:7F:F0:09:72 2 00:50:7F:F0:09:72 2 00:50:7F:F0:09:72 3 5C:97:F3:03:05:F7 4 40:98:AD:58:F2:52 5 00:50:7F:37:67:DE5 6 00:50:7F:27:60:E5 7 30:F7:C5:1D:30:D1:11 8 40:F0:27:22:E8:A0 9 18:65:90:DE:D4:E5 10 60:45:C8:F7:1F:36 11 30:41:67:52:E8:F8 12 50:8C:96:E0:00:11 13 04:B1:67:52:46:90 14 04:C2:3E:3F4:62:F8:F8 15 00:38:FD:31:08:76 16 58:48:22:E8:F8:62 17 CC:9F7:46:31:112	Hostname TA001029 ta002171 T2c-Pingde N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	o other C addr C addr f all me DrayTek DrayTek DrayTek DrayTek DrayTek Apple Liteonte Apple Liteonte Apple N/A Samsung Apple N/A HTC Intel Sony N/A	access ress of t esh devi staffs_4Fstaffs_4F staffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4F staffs_4Fstaffs_4Fstaffs_4F staffs_4Fstaffs_4Fstaffs_4F	Chann 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	el RSSI 6896(-63dBm) 41%(-73dBm) 100% (-49dBm) 55%(-66dBm) 55%(-66dBm) 33%(-57dBm) 100% (-44dBm) 15%(-64dBm) 10% (-44dBm) 15%(-62dBm) 45%(-72dBm) 55%(-66dBm) 55%(-66dBm) 55%(-66dBm)	TxRate(Kb 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nk. P connect:

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.

Mesh >> Mesh Discovery

Device List

Index	MAC Address	Model	Operation Mode	Link Status
1	00:50:7F:F1:7F:1D	VigorAP903	MeshNode(Wireless)	Connected
2	00:1D:AA:62:0F:E8	Vigor2862	MeshRoot	Connected
3	00:1D:AA:63:2C:00	VigorAP920R	MeshRoot	Connected
4	00:1D:AA:57:5D:38	VigorAP1000C	AP	
5	00:1D:AA:04:F0:D8	VigorAP1000C	MeshNode(Wireless)	Connected
6	00:1D:AA:04:F0:DC	VigorAP1000C	AP	
7	00:1D:AA:04:F0:6C	VigorAP1000C	MeshRoot	Connected
8	00:1D:AA:63:2C:10	VigorAP920RPD	MeshNode(Wireless)	Connected
9	00:50:7F:F1:7E:CB	VigorAP903	MeshRoot	Connected

Scan

Note: During the scanning process (about 10 seconds), no station is allowed to connect with the AP and Mesh Network may disconnect.

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 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.

	ct All	
Syst	em Maintenance	
ndex	Name	Value
1	ManagementServer.URL	
2	ManagementServer.Username	
3	ManagementServer.Password	*****
4	ManagementServer.ConnectionRequestUsername	vigor
5	ManagementServer.ConnectionRequestPassword	*****
6	ManagementServer.PeriodicInformEnable	1
7	ManagementServer.PeriodicInformInterval	900
8	X_00507F_System.Management.SkipQuickStartWizard	Enable
9	X_00507F_System.TR069Setting.CPEEnable	0
10	X_00507F_System.AdminmodePassword.Admin	admin
11	X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable	0
12	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
13	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
14	X_00507F_System.SyslogMail.SysLogAccess.LogLevel	
15	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
16	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
17	X_00507F_System.SyslogMail.MailAlert.MailTo	
18	X_00507F_System.SyslogMail.MailAlert.MailFrom	

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
Wireless LAN (5GHz)	connected mesh node. Note that this button is available only
Wireless LAN (5GHz-2)	when such AP is in mesh root mode.

Tips for Mesh Network Setup

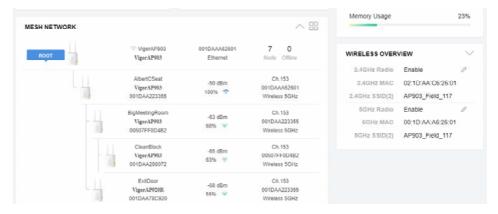
- Set up TWO mesh devices with uplink RSSI larger than -65dBm.
- Upgrade the firmware version of Mesh devices through Mesh link, starting from the mesh device with less hop number. For example, upgrade the firmware from the root, hop1 Mesh Node then hop2 Mesh Node, and so on.
- VigorMesh network supports 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 : 80Mbps
- iPad 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.



- 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 1000C 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	[ek		Syslog Utility
	Al 行取记錄(channe	- (NAR	
			- 智序
系統時間	路由器時間	主機	ine .
	路由器時間 Nov 8 10:58:05	主根 syslog	IR8 [dm] dm. pkt_recv Amounce-Keepalive
018-11-08 19:01:16			[dmn] dmn_pkt_recv Announce-Keepalive [dmn] dmn_pkt_send Alive
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 Nov 8 10:57:52	syslog syslog syslog	(dm) dm, pkt_recv Announce-Keepalve (dm) dm_pkt_send Alve (dm) dm_pkt_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	Nov 8 10:58:05 Nov 8 10:58:04 Nov 8 10:57:52 Nov 8 10:57:50	syslog syslog syslog syslog	(dwn) dwn, piłt, recv Announce-Keepalwe (dwn) dwn, piłt, send Alwe (dwn) dwn, piłt, recv Announce-Keepalwe (dwn) dwn, piłt, recv Announce-Keepalwe
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 19:01:01 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	syslog syslog syslog syslog kernel	long [dm] dm_pkt_recvAnnounce-Kespalive [dm] dm_pkt_sendAlve [dm] dm_pkt_recvAnnounce-Kespalive [dm] dm_pkt_recvAnnounce-Kespalive [dm] dm_pkt_recvAnnounce-Kespalive [7253:35596][dm] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C0
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	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 kernel syslog	(dm) dm_pkt_recv Announce-Kespalive (dm) dm_pkt_send Alve (dm) dm_pkt_send Alve (dm) dm_pkt_recv Announce-Kespalive (dm) dm_pkt_recv Announce-Kespalive [7525:332564] (dm) Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C0 (dm) dm_pkt_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 10:57:50 Nov 8 10:57:48 Nov 8 10:57:41 Nov 8 10:57:36	syslog syslog syslog syslog kernel syslog syslog	long [dm] dm_pkt_secvAnnounce-Kespalive [dm] dm_pkt_secvAnnounce-Kespalive [dm] dm_pkt_secvAnnounce-Kespalive [dm] dm_pkt_secvAnnounce-Kespalive [dm] dm_pkt_secvAnnounce-Kespalive [dm] dm_pkt_secvAnnounce-Kespalive
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 19:00:59 2018-11-08 19:00:53 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 10:57:48 Nov 8 10:57:41 Nov 8 10:57:30	syslog syslog syslog kernel syslog syslog syslog	Loss (dm.) dm., pl.t., rec. Announce-Keepalive [dm.) dm., pl.t., send Alive [dm.) dm., pl.t., send Alive [dm.) dm., pl.t., rec. Announce-Keepalive [m.253, 335504] [dm.) Mesh IE Record (Isolate) 00:10:AA:55:A6:08 [dm.) dm., pl.t., send Alive [dm.] dm., pl.t., send Alive [dm.] dm., pl.t., send Alive
018-11-08 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 19:00:47 2018-11-08 19:00:47 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 10:57:36 Nov 8 10:57:36 Nov 8 10:57:28	syslog syslog syslog kernel syslog syslog syslog syslog kernel	(dm) dm_pit_recv Announce-Kespalve [dm] dm_pit_send Alve [dm] dm_pit_send Alve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_send Alve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve
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 19:00:41 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 10:57:50 Nov 8 10:57:50 Nov 8 10:57:40 Nov 8 10:57:41 Nov 8 10:57:30 Nov 8 10:57:30 Nov 8 10:57:28 Nov 8 10:57:22	syslog syslog syslog kernel syslog syslog syslog syslog kernel syslog	Tool dam_pht_recv Announce-Keepalve [dam] dam_pht_recv Announce-Keepalve [dam] dam_pht_send Alve [dam] dam_pht_send Alve [dam] dam_pht_recv Announce-Keepalve [motion_pht_recv Announce-Keepalve [dam] dam_pht_recv Announce-Keepalve [motion_pht_recv Announce-Keepalve] [motion_pht_
米税時間 2016-11-08 19:01:15 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 19:00:47 2018-11-08 19:00:47 2018-11-08 19:00:33 2018-11-08 19:00:33 2018-11-08 19:00:33	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 10:57:36 Nov 8 10:57:36 Nov 8 10:57:28	syslog syslog syslog kernel syslog syslog syslog syslog kernel	(dm) dm_pit_recv Announce-Kespalve [dm] dm_pit_send Alve [dm] dm_pit_send Alve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_send Alve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve [dm] dm_pit_recv Announce-Kespalve

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.

Mesh >> Advanced Configuration Sync					
Se	lect All				
Bri	idge VLAN to Mesh				
Index	Name	Value			
1	X_00507F_LAN.GeneralSetup.BridgeVLANtoWDS	Enable			
	aming 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.SSI	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	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinBasicRate	6Mbps			
13	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.RSSI	Disable_RSSI_Requirement			
14	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	0			
18	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.CachePeriod	10			

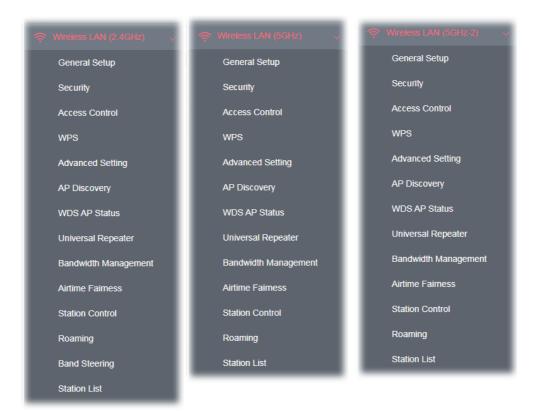
ltem	Description
Select All	All item(s) will be selected for making configuration sync.
Bridge VLAN to Mesh	Check to transmit the packets with VLAN tag to mesh nodes.

II-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/5GHz-2) 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.



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/PSK v
Encryption Type	AES 🗸
Pass Phrase	
Range Extender Band	None
Note: If Channel is modified, the Chan	nel setting of AP would also be changed.

Universal Repeater IP Configuration

Connection Type	DHCP	~		
Device Name	AP1000C			
	ок	Cancel		

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 1000C wants to connect to.
Channel	Means the channel of frequency of the wireless LAN.
	As a tri-band access point, VigorAP offers different channels for WLAN 2.4GHz, 5GHZ and 5GHz-2 respectively.
	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/PSK ~
	Open
	Shared
	WPA/PSK
Encryption Type for Open/Shared	This option is available when Open/Shared is selected as Security Mode.
	Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP .
	WEP Keys - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(! to 126(~) except '#' and ','.
Encryption Type for WPA/PSK and WPA2/PSK	This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode . Select TKIP or AES as the algorithm for WPA.
Pass Phrase	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 C	Configuration
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 Catoway	This setting is available when Statis ID is selected as Connection

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.

(i) Note:

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

thernet TCP / IP and DH	CP Setup	
LAN IP Network Configu	Iration	DHCP Server Configuration
Enable DHCP Client	t	Enable Server O Disable Server
IP Address	192.168.1.11	O Relay Agent
Subnet Mask	255.255.255.0	WLAN Trusted DHCP Server Server IP Address
Enable Managemen		WEAN HUSted DHCP Server Server IP Address
		WEAN HUSted DHCP Server Server IP Address
Enable Managemen	nt VLAN	WEAN HUSted Drick Server Server in Address
Enable Managemen VLAN ID	nt VLAN	WEAN HUSted Difer Server Server in Address

ltem	Description
LAN IP Network	Enable DHCP Client – When it is enabled, VigorAP 1000C will be
	treated as a client and can be managed / controlled by AP

Configuration	Management server offered by Vigor router (e.g., Vigor2860).
	 IP Address – Type in private IP address for connecting to a local private network (Default: 192.168.1.2).
	• Subnet Mask – Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
	Enable Management VLAN – VigorAP 1000C supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 1000C.
	 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 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.
	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 Port Settings

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

LAN >> Port Setting	IS
Port Control	
Enable Port C	Control
	Port 1 Port 2
Disable Port	
Port/Subnet Mappi	ing
	Port 1 Port 2
Subnet	LAN-A V LAN-B V
	OK Clear Cancel

Available settings are explained as follows:

Item	Description		
Port Control			
Enable Port ControlCheck it to enable the port control. If it is enabled, you are disable the function of physical LAN port by checking the corresponding check box.			
Disable Port	Choose and check the LAN port.		
Port/Subnet Mapping			
Subnet	When Enable 2 Subnet is enabled in Wireless LAN >> General Setup , you can set subnet (LAN-A or LAN-B) for LAN Port 2.		
	In AP mode, if you specify LAN-B for Port 2, wireless clients on LAN-B SSIDs can access Internet through Port 2 independently.		
	However, if you specify LAN-A for Port2, both LAN ports can access LAN-A while wireless clients on LAN-B SSIDs can use local service.		

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

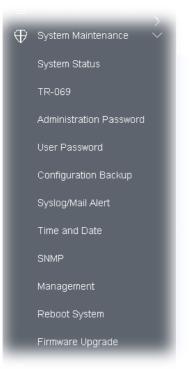
Chapter III Management



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.

System Status : VigorAP1000C : VigorAP1000C : 1.3.2 : r11481 Tue, 14 Jan 2020 16:51:26 Model Device Name Firmware Version Build Date/Time System Uptime 3d 20:15:08 : Range Extender **Operation Mode** System LAN Memory Total : 236760 kB MAC Address : 00:1D:AA:04:F2:C8 Memory Left : 73564 kB IP Address : 192.168.1.11 Cached Memory : 32804 kB / 236760 kB IP Mask : 255.255.255.0 Wireless LAN (2.4GHz) MAC Address : 00:1D:AA:04:F2:C8 : 11 SSID : DrayTek-04F2C8 Channel Driver Version : 10.4 Wireless LAN (5GHz) MAC Address : 00:1D:AA:04:F2:C9 SSID : 36 : DrayTek-04F2C8 Channel Driver Version : 10.4 Wireless LAN (5GHz-2) MAC Address : 00:1D:AA:04:F2:CA SSID : DrayTek-04F2C8 Channel : Auto(100) Driver Version : 10.4

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

Each item is explained as follows:

Item	Description	
Model /Device Name	Display the model name of the modem.	
Firmware Version	Display the firmware version of the modem.	
Build Date/Time	Display the date and time of the current firmware build.	
System Uptime	Display the period that such device connects to Internet.	
Operation Mode	Display the operation mode that the device used.	
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/5GHz-2)	
MAC Address	Display the MAC address of the WAN Interface.	
SSID	Display the SSID of the device.	

ChannelDisplay the channel that the station used for connecting with such device.	
--	--

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).

System Maintenance >> TR-069 Settings

ACS Settings		
URL	http://192.168.105.141:8080/ACSServer/services,	Wizard
Username	acs	
Password	•••••	
	Test With Inform Event Code PERIODIC ~	
Last Inform Response Time : ●		
CPE Settings		
Enable		
SSL(HTTPS) Mode		
On	LAN-A v	
URL	http://192.168.1.2:8069/cwm/CRN.html	
Port	8069	
Username	viqor	
Password	•••••	
	orks when Vigor ACS SI is 1.1.6 and above version.	
Please set derault gatewa	ay, no matter choose LAN-A or LAN-B.	
Periodic Inform Settings		
Enable		
Interval Time	900 second(s)	
STUN Settings		
오 Enable 🔘 Disable		
Server Address	192.168.105.141	
Server Port	8478	
Minimum Keep Alive Period	60 second(s)	
Maximum Keep Alive Period	-1 second(s)	
	OK Cancel	

ltem	Description		
ACS 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).		
	Enable – Check the box to allow the CPE Client to connect with Auto Configuration Server.		
	SSL(HTTPS) Mode - Check the box to allow the CPE client to connect with ACS through SSL.		
	On – Choose the interface (LAN-A or LAN-B) for VigorAP 1000C connecting to ACS server.		
	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 sensitive 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 sen binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.		

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

III-1-3 Administrator Password

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

System Maintenance >> Administration Passwore	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 characters	
	only a-z A-Z 0-9 , ~ ` ! @ \$ % ^ * () _ + = {} [] ; < > . ? n only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & * () _ + = {} [] \ ;



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 StrengthThe system will display the password strength (represented w word of weak, medium or strong) of the password specified at		

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	•••••
	i only a-z A-Z O-9 , ~ ` ! @ \$ % ^ * () _ + = {} [] ; < > . ? in 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 1000C settings.

System Ma	stem Maintenance >> Configuration Backup				
Configurat	nfiguration Backup / Restoration				
Restoratio	on				
	Select a configuration	file.			
	Upload				
	Please enter the passv	vord and click Restore to upload the configuration file.			
	Password (optional):	Restore			
		the same password to do configuration restoration. tion file from the supported model list would be adopted.			
Backup					
	Please specify a passw an encrypted file.	vord and click Backup to download current configuration as			
	V Protect with pass	word			
	Password	(Max. 23 characters allowed)			
	Confirm Password				
	Backup				

Available settings are explained as follows:

ltem	Description	
Restoration	Upload - 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**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

(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.

514
All ~

System Maintenance >> Syslog / Mail Alert Setup

ltem	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.
	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.
	Use TLS – Check this box to encrypt alert mail. However, if the SMTP server specified here does not support TLS protocol, the alert mail

with encrypted data will not be received by the receiver.
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.

me Information		
urrent System Time	2020 Mar 2 Mon 09:48:00 Inquire Time	
atus	NTP time synchronized	
ne Setting		
Exclusion official		
Enable NTP Client		
 Enable NTP Client Time Zone 	(GMT+08:00) China Beijing, Chongqing \sim	
Time Zone NTP Server	(GMT+08:00) China Beijing, Chongqing V pool.ntp.org Use Default	
Time Zone		

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.	
ОК	Save the settings.	

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 SNMP Agent			
✔ Enable SNMPV3 Agent			
USM User]	
Auth Algorithm	No Auth \sim		
Auth Password			
Note: SNMP V1/V2c is read-only ar	nd SNMP V3 is read-write.		

Cancel

Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check it to enable this function.
Enable SNMPV3 Agent	Check it to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm.
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.

Click **OK** to save these settings.

III-1-9 Management

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

System Maintenance >> Management

Access C	ontrol		Port Setup
🗸 Allow	management	from WLAN	HTTP Port 80 (Default:80)
🔽 Enabl	e Telnet Serv	er	HTTPS Port 443 (Default:443)
Access L	ist		Panel Control
🗌 Enab	le access list		Disable LED
List	IP	Mask	Enable Default Configuration Wizard
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 🗸	

Available parameters are explained as follows:

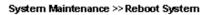
Item	Description
Device Name	The default setting is VigorAP 1000C. Change the name if required.
Access Control	Allow management from WLAN - Enable the checkbox to allow system administrators to login from wireless LAN.
	Enable Telnet Server – The administrator / user can access into the command line interface of VigorAP remotely for configuring settings.
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

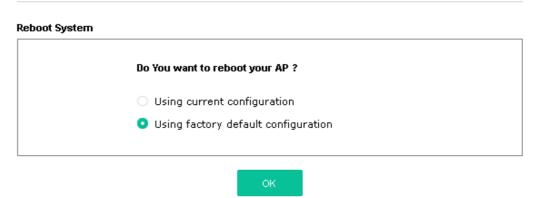
whenever clicking the DrayTek logo on the top of the web user interface.
Such function will be disabled if you have configured Operation Mode, WLAN>>General Setup, WLAN>>Bandwidth Management, WLAN>>Station Control or System Maintenance>>Administration Password.

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

ware Update			
Select a firm	nware file.		
Upload			
Click Upgrad	de to upload the file.	Upgrade	

Firmware Version Status		Refresh Latest Firmware
Current Firmware Version	: 1.3.2	
The Latest Firmware Version	: N/A	Download

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

System	Maintenance	>> Firmwar	e Uporade -
System	THUR TO THE TO THE TO THE TO THE TABLE TO TABLE TO THE TABLE TO THE TABLE TO TABLE TO TABLE TO TABLE TO TABLE TAB	~~ I II	c opgi auc

Firmware Update

Firmware Upgrade is in progress It must NOT be interrupted!	

Firmware Version Status		Refresh Latest Firmware
Current Firmware Version	: 1.3.3	
The Latest Firmware Version	: N/A	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

ОК	Cancel		
	ОК	OK Cancel	OK Cancel

Note: LAN-B cannot support APM feature.

Available settings are explained as follows:

ltem	Description
Enable AP Management	Check the box to enable the function of AP Management (APM).
Enable Auto Provision	VigorAP 1000C can be controlled under Central AP Management in Vigor2862 series. When both Vigor2862 series and VigorAP 1000C have such feature enabled, once VigorAP 1000C is registered to Vigor2862 series, the WLAN profile pre-configured on Vigor2862 series will be applied to VigorAP 1000C immediately. Thus, it is not necessary to configure VigorAP 1000C separately.

Click **OK** to save these settings.

III-2-2 APM Log

This page will display log information related to wireless stations connected to VigorAP 1000C 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.			
-	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 1000C) 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 1000C for data incoming and outgoing. Therefore, "Force Overload Disassociation" is required to terminate the network connection of the client's station to release network traffic. When the function of "Force Overload Disassociation" in web user interface of Vigor router (e.g., Vigor2860 or Vigor2925 series) is enabled, wireless clients specified in **black list** of such web page will be disassociated to solve the problem of traffic overload.

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

Central AP Management >> Overload Management

Client's MAC Address : : : : : : : : : : : : : : : : : :		MA	C Address Filter of F	orce Overload Disa	association	
Black List Client's MAC Address : : : Apply to : White List Comment : Add Delete Edit Cancel		Index	MAC Address	Comment		
Client's MAC Address : : : : : : : : : : : : : : : : : :	White List					
Client's MAC Address : : : : : : : : : : : : : : : : : :						
Client's MAC Address : : : : : : : : : : : : : : : : : :						
Apply to : White List Comment : Add Delete Edit Cancel	Black List					
Apply to : White List Comment : Add Delete Edit Cancel						
Apply to : White List Comment : Add Delete Edit Cancel						
Comment : Add Delete Edit Cancel	Client's MA	C Address :		: : : [
Add Delete Edit Cancel	Apply to :	1	White List	~]		
Add Delete Edit Cancel	Comment					
	conmotit			Edit	Consol	
		AU	Delete	Euli	Cancer	
OK Clear All						

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.

Available settings are explained as follows:

Item	Description
White List/Black List	Display the information (such as index number, MAC address and comment) for all of the members in White List/Black List.
	Wireless stations listed in Black List will be forcefully disconnected first when traffic overload occurs and "Force Overload Disassociation" is enabled.
Client's MAC 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 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 1000C) registered to Vigor 2862 or Vigor2926 series. This web page displays the settings related to Load Balance for VigorAP 1000C. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor 2862 or Vigor2926 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
Max WLAN(5GHz-2) Station Number		128
Traffic Threshold	×	
Upload Limit		None bps
Download Limit		None bps
Force Overload Disassociation	×	
Disassociate By		None
RSSI Threshold		-50 dBm
Rogue AP Detection		
Rogue AP Detection	×	

"X" means the function is not enabled or VigorAP 1000C has not registered to any Vigor router yet.

Below shows a setting example for Load Balance settings configured in Vigor 2862 or Vigor2926 series.

Central Management >> AP >> Load Balance

Station Number Thresh	old	
Wireless LAN (2.4GHz)	64 (3-128)	
Wireless LAN (5GHz)	64 (3-128)	
Traffic Threshold		
Upload Limit User de	efined 💙 OK bps (Default unit: K)	
Download Limit User de		
Action When Threshold	Exceeded	

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.

							Las	t 24 hour	민이
Connected Number Statistics									
2.4 are • 5 are •									
аб 6 2 0 12РМ 2РМ	4РМ БРМ	EPM 18	IPM 12AM	2AM 4AM	6/	AM BAM		10AM	
	ite List								
+ Accesso Contrast + Device Object	Device Object list								
+ Access Contrat + Denice Object		597.81 mi ∔ 4.3			Courth				
ital Usage		7555566754 D.C.S	2 ca 50Hz		Search][+	1 1	19
tal Usage	T	7555566754 D.C.S		SSID	Search	Usage	сн	1 > Action	49
tal Usage tal Clients	T : Up Time	4 24GHz 3	SOHE	SSID AP912C_117_2.4G_1					49
tal Usage tal Clients Name/MAC Unknown_52ACE5 26:3A-4D:52.AC:E5	Up Time 5d 21:10:59	4 24GHz 3	SOHE RSSI		os	Usage † 148.14 MB	сн	Action DeAuth	>
tal Usage tal Clients Name/MAC Unknown_52ACE5 28.3A-4D.52ACE5 Unknown_72C6E2 0C:9D:92.72:C6:E2 Bedmi5-tampi.ing	Up Time 5d 21:10:59 0d 01:48:06	4 24GHz 3 Link Speed 10 Mbps / 5 Mbps	50Hz RSSI 100% (-45 dbm)	AP912C_117_2.4G_1	os Ø	Usage ↑ 148.14 MB ↓ 296.73 MB ↑ 7.15 MB	сн 11	Action DeAuth Block DeAuth	>
Name/MAC Unknown_52ACE5 20:3A:4D.52.AC:E5 20:3A:4D.52.AC:E5 20:00:90:92:72:C6:E2 00:90:92:72:C6:E2 Redmi5-JenyLing	Up Time 5d 21:10.59 0d 01:48:06 0d 01:10.58	4 24082 3 Link Speed 10 Mbps / 5 Mbps 50 Mbps / 1 Mbps	SGIE RSSI 100% (-45 dbm) 62% (-65 dbm)	AP912C_117_2.4G_1 AP912C_117_2.4G_1	os ⑦	Usage 1 448.14 MB 1 296.73 MB 1 7.15 MB 1 60.17 MB 1 12.83 MB	сн 11 11	Action DeAuth Block DeAuth Block DeAuth	

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.	~ C
Co	nnecte	ed Number Stati	stics								
	ſ	Device OS	0% Android 0% IOS 0 0% Window 0% Linux 0 100% Others	'S 0	Polic	cy	100% 0%	 Pass 58 Block 0 			₹∑
Cli	ents L	ist Block List	White List								
	Access	Control + Device	e Object Device Ob	ject list							
	Usage Client:		1	1 58.13 кв ↓ 45.89 кв 0 24GHz 64 5GHz	59	¢	1	2 3 4	5	6 7 >	ŝ
		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:C	0d 03:41:17	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1 867 B ↓ 717 B	36	DeAuth Block	>
3		Unknown_C34F0A 00:BC:DA:C3:4F:0/	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	1 867 B ↓717 B	36	DeAuth Block	>
4		Unknown_0CEEE9 00:BC:DA:0C:EE:E	0d 03:41:16	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	0	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	?	1̂ 867 В ↓717 В	36	DeAuth Block	>
6		Unknown_9D28C0 00:BC:DA:9D:28:Cl	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1 867 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	1̂ 867 В ↓717 В	36	DeAuth Block	>
8		Unknown_9B07CE 00:BC:DA:9B:07:Cl	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	1̂ 867 В ↓717 В	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	?	1̂ 867 В ↓717 В	36	DeAuth Block	>
10		Unknown_DD1FA2 00:BC:DA:DD:1F:A	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	0	1 903 B ↓717 B	36	DeAuth	>

III-3-1-3 Clients List

The client list displays all the stations connecting to VigorAP.

SIAI	TION LIST ()							L	ast 24 hour	C ~
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.						
		lect 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	es - Save the changes	s and exit this page.				
+Device Object	To add a de	vice to device object l	ist, choose one of the entries				
·	(clients) on o button to op		the Device Object button. Click the				
		Device MAC	Name				
		00:BC:DA:F5:EB:B4	Unknown_F5EB34				
		00:BC:DA:94:CC:07	Unknown_94CC07				
	or name of		Cancel OK he page. Change the MAC address equired. Then click OK and exit the				
	page.						
Device Object list	The existed page.	device object profiles	s will be shown on the following				
	DEVICE OBJECT						
	Device Object Profiles						
			Search Bet to Factory Default				
	100000		1 · 1				
	Profidx	MAC 00.50.7F F1 91.BC	Name TEST_1				
	2	00:50.7F 00:92 BA	TEST_2				
Clients List	Display the	stations connecting to	o this Vigor device.				
	Total Usage	e - Display					
	Total Client	ts - Display the numb	er of the clients using 2.4GHz				
		C - Display the host n	ame / MAC address of the				
	Up Time - D	isplay the connection	n time.				
	-	- Display the link spee					
	-	ay the RSSI value.					
		-	used for connecting VigorAD				
	-	-	used for connecting VigorAP.				
		the OS of the client.					
		-	sage (up and down) of the client.				
		the channel used by					
		play the authentication list or white list.	on method used by the client, and if				
		A HIST OF WHITE HIST.					

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 MAC 1 00:50.7F F1:91:BC 2 00:50.7F 00:92:BA	Name TEST_1 TEST_2					
Name / MAC	Display the host name / MA	AC Address for the connecting client.					
SSID	Display the SSID that the wi	ireless client connects to.					
Reason	Display the reference information.						
Action	Display the action that you can execute for the station. Unblock - Click to unblock the entry.						

III-3-1-5 White List

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

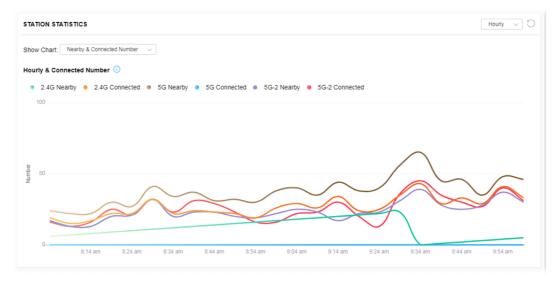
	11AM 1PM	3PM	5PM	7PM	9PM	11PM	1AM	3AM	5AM	7AM	9AM
Clients	s List Block List Wh	ite List									
+ Acc	ess Control + Device C	Dbject	evice Object list								
										Search	
											۲ (
	Name/MAC			SS	D		Action				
1	LiteonTe C8:FF:28:FC:2A:C1			mk	carrie		Block				
2	Unknown_A02925 3C:95:09:A0:29:25			mk	carrie		Block				
Total lis	ist 2										

Available settings are explained as follows:

Item	Description	I				
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			
	1	00:50 7F F1:91:8C 00:50 7F 00:92 BA	TEST_1 TEST_2			
Name / MAC	Display the l	nost name / MAC Addres	s for the connecting client.			
SSID	Display the S	SSID that the wireless clie	ent connects to.			
Action	Display the a	action that you can execu	te for the station.			
	Block - Click	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.
	T: 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 th 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

earl	by Num	ber					
2.4	GHz 🛢	5 GHz • 5-2 GHz •					
1	00						
						_	
	50					\frown	
					\sim	\sim	\sim
	0						
		8:19 am 8:29 am	8:39 am 8:49 am	8:59 am 9:09	am 9:19 am 9:21	9 am 9:39 ar	m 9:49 am 9:59 am
							+ Access Cont
							+ Access Cont
2.4	Glist	5G list					+ Access Cont
2.4	IG list	5G list					+ Access Cont
2.4	IG list	5G list	Vendor	Distance	RSSI	SSID	+ Access Cont
			Vendor ASUS	Distance 28.18m	R\$Si 56%(-74dbm)	SSID N/A	
		MAC					Up Time
		MAC 2C:FD:A1:B4:21:E1	ASUS	28.18m	56%(-74dbm)	N/A	Up Time Od: 0h:0m:0s
		MAC 2C:FD:A1:B4:21:E1 C8:FF:28:FC:2A:C1	ASUS	28.18m 7.94m	56%(-74dbm) 87%(-63dbm)	N/A N/A	Up Time 0d: 0h:0m:0s 0d: 0h:39m:38s
		MAC 2C:FD:A1:B4:21:E1 C8:FF:28:FC:2A:C1 1A:CB:30:40:43:EB	ASUS LiteonTe	28.18m 7.94m 79.43m	56%(-74dbm) 87%(-63dbm) 27%(-83dbm)	N/A N/A N/A	Up Time 0d: 0h:0m:0s 0d: 0h:39m:38s 0d: 0h:0m:0s
		MAC 2C:FD:A1:B4:21:E1 C8:FF:28:FC:2A:C1 1A:CB:30:40:43:EB DA:A1:19:63:06:0D	ASUS LiteonTe	28.18m 7.94m 79.43m 35.48m	56%(-74dbm) 87%(-63dbm) 27%(-83dbm) 50%(-76dbm)	N/A N/A N/A N/A	Up Time 0d: 0h:0m:0s 0d: 0h:39m:38s 0d: 0h:0m:0s 0d: 0h:0m:0s
		MAC 20:FD:A1:B4:21:E1 08:FF:28:FC:2A:C1 1A:CB:30:40:43:EB DA:A1:19:63:06:0D 6A:3B:B6:47:7D:D1	ASUS LiteonTe	28.18m 7.94m 79.43m 35.48m 14.13m	56%(-74dbm) 87%(-63dbm) 27%(-83dbm) 50%(-76dbm) 75%(-68dbm)	N/A N/A N/A N/A	Up Time 0d: 0h:0m:0s 0d: 0h:39m:38s 0d: 0h:0m:0s 0d: 0h:0m:0s 0d: 0h:0m:0s
1		MAC 20:FD:A1:B4:21:E1 08:FF:28:FC:2A:C1 1A:CB:30:40:43:EB DA:A1:19:63:06:0D 6A:3B:B6:47:7D:D1 30:95:09:A0:29:25	ASUS LiteonTe Google	28.18m 7.94m 79.43m 35.48m 14.13m 5.01m	56%(-74dbm) 87%(-63dbm) 27%(-63dbm) 50%(-76dbm) 75%(-68dbm) 90%(-59dbm)	N/A N/A N/A N/A N/A	Up Time 0d: 0h:0m:0s 0d: 0h:39m:38s 0d: 0h:0m:0s 0d: 0h:0m:0s 0d: 0h:0m:0s 0d: 0h:43m:58s
2.4		MAC 2C:FD:A1:B4:21:E1 C8:FF:28:FC:2A:C1 1A:CB:30:40:43:EB DA:A1:19:63:06:0D 6A:3B:B6:47:7D:D1 3C:95:09:A0:29:25 30:5A:3A:AB:18:F2	ASUS LiteonTe Google	28.18m 7.94m 79.43m 35.48m 14.13m 5.01m 4.47m	56%(-74dbm) 87%(-63dbm) 27%(-63dbm) 50%(-76dbm) 75%(-68dbm) 90%(-59dbm) 90%(-58dbm)	N/A N/A N/A N/A N/A N/A	Up Time 0d: 0h:0m:0s 0d: 0h:39m:38s 0d: 0h:0m:0s 0d: 0h:0m:0s 0d: 0h:0m:0s 0d: 0h:43m:58s 0d: 0h:0m:0s

This page displays the general information for the nearby stations.

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 v DrayTek-04F2C		Disable v 4 Disable v N/A N/A
From to list	Device MAC	Name	Apply to SSID
	C8:FF:28:FC:2A:C1	LiteonTe	All 1 2 3 4
	30:5A:3A:AB:18:F2	ASUStekC	All 1 2 3 4
Total : 0/256			Close Save changes

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

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

POLICIES			
Block	k Mobile Connections (OS:Android,iOS)	
Block	k PC Connections (OS:Windows,Linux,	iMac)	
Block	k Unknown Connections (OS:Others)		
WiFi(2.4 WiFi(5G	33107 3 3102 3		
WiFi(5G			
	HZ-2) SSID1 SSID2	SSID3 🖬 SSID4	
			OK

Each item is explained as follows:

Item	Description	
Block Mobile Connections	All of mobile devices will be blocked and not allowed to access into Internet via VigorAP.	
Block PC Connections	All of network connections based on PC, MAC or Linux platform will be blocked and terminated.	
Block Unknown Connections	Only the unknown network connections (unable to be recognized by Vigor router) will be blocked and terminated.	
WiFi(2.4GHz)	Specify the SSID(s) to apply such policy.	
WiFi(5GHz)	Specify the SSID(s) to apply such policy.	
WiFi(5GHz-2)	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

		Reset	 Online 	Offline			
		SSID	м	IAC	Connection Time	Reconnection Time	
1	•	AP912C_117_2.4G_1	28	8:3A:4D:52:AC:E5	0d 00:58:50	0d 00:00:00	
2	•	AP912C_117_2.4G_1	20	0:47:DA:25:A5:6B	0d 00:48:22	0d 00:00:00	
3	•	AP912C_117_5G_1	40	0:4E:36:5E:3F:A7	0d 00:59:55	0d 00:00:00	
4		AP912C 117 5G 1	D	0:37:45:34:7C:C8	0d 00:56:02	0d 00:00:00	

This page displays information related to the wireless stations connecting to the Vigor AP.

① This page is available when Station Control is enabled.

This page is left blank.

Chapter IV Others



IV-1 RADIUS Setting



IV-1-1 RADIUS Server

VigorAP 1000C offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 1000C. The AP can accept the wireless connection authentication requested by wireless clients.

	ver			
uthentication Type				
I	Radius EAP Type		PEAP ~	
Isers Profile (up to 2	56 users)			
Username	Password	Confirm Password	Confi	gure
			Add	
NO.	Userna	ime	Selec	t
NO. Delete Selected	Userna Delete All	ime	Selec	t
	Delete All	ome Confirm Secret Key	Selec	_
Delete Selected	Delete All (up to 16 clients)			_
Delete Selected	Delete All (up to 16 clients)	Confirm Secret Key	Confi	gure Cancel
Delete Selected	Delete All (up to 16 clients) Secret Key	Confirm Secret Key	Confi Add	gure Cancel
Delete Selected	Delete All (up to 16 clients) Secret Key Client	Confirm Secret Key	Confi Add Select	gure Cancel
Delete Selected	Delete All (up to 16 clients) Secret Key Client	Confirm Secret Key	Confi Add	gure Cancel

Available settings are explained as follows:

ltem	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 1000C 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 1000C as its external RADUIS server.
	Client IP – Type the IP address for the user to be authenticated by VigorAP 1000C when the user tries to use VigorAP 1000C as the external RADIUS server.
	Secret Key – Type the password for the user to be authenticated by VigorAP 1000C while the user tries to use VigorAP 1000C 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	Upload - 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

Available settings are explained as follows:

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 >>	Schedule				
Schedule : Curr	rent System 1	ime 2020 Mar	2 Mon 10:16:27		System time set Set to Factory Default
Index Enable	Name	Action	Ti	me	Active Finished Not reached Frequency
			ок	Add	. ,

Available settings are explained as follows: Available settings are explained as follows:

ltem			Description
	0	'	

ltem	Description			
Current System Time	Display current system time.			
System time set	Click it to open Time and Date page for configuring the time setting.			
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	Formkt
Start Date	2000 \sim - 1 \sim - 1 \sim (Year - Month - Day)
Start Time	$0 \sim : 0 \sim$ (Hour: Minute)
Duration Time	$0 \sim$: $0 \sim$ (Hour: Minute)
End Time	0 v: 0 v (Hour: Minute)
Action	Auto Reboot 🔍
WiFi(2.4GHz)	Radio SSID2 SSID3 SSID4
WiFi(5GHz)	Radio SSID2 SSID3 SSID4
WiFi(5GHz-2)	Radio SSID2 SSID3 SSID4
How Often	Once 🗸
Weekday	🗌 Monday 📄 Tuesday 📄 Wednesday 📄 Thursday 📄 Friday 📄 Saturday
Weekday	Sunday
	set WiFi schedule "Start Time" and "End Time" at exact same time, AP will execute the without an end time.
	net Pause" will add Mac into ACL, so please make sure ACL isn't full before applying .If ACL policy is "Disable", AP will change it to "Blocked".
	OK Cancel

Available settings are explained as follows:

ltem	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 TimeSpecify 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 tim schedule.					
Action	Specify which action should apply the schedule.				

	Auto Reboot 🗸 🗸				
	Auto Reboot				
	Wi-Fi UP				
	Wi-Fi DOWN				
	LED DISABLE				
	LED ENABLE				
	Sound Buzzer				
WiFi(2.4GHz)/	When Wi-Fi UP or Wi-Fi DOWN is selected as Action , you can check the Radio or SSID 2~4 boxes (2.4GHz, 5GHz and 5GHz-2 respectively)				
WiFi(5GHz)/	the Radio or SSID 2~4 boxes (2.4GHz, 5GHz and 5GHz-2 respectively)				
	the Radio or SSID 2~4 boxes (2.4GHz, 5GHz and 5GHz-2 respectively) to setup the network based on the schedule profile.				
WiFi(5GHz-2)	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				
WiFi(5GHz-2)	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.				
WiFi(5GHz)/ WiFi(5GHz-2) How Often	 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. Specify how often the schedule will be applied. 				

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.

Applica	ations >>	> Schedule							
Sched	ule : Cu	irrent Syster	n Time 2020 Mar 2	Mon 10:24:13		I	System time set	Set to Factory [)efault
Index	Enable	Name	Action		Time		Active	Finished 🔘 Not	reached
Index	Enable	Name	Action		Time			Frequency	
1		Formkt	Auto Reboot					Once	🧼 🗙
				ОК	Add				

IV-2-2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 1000C will send the UDP packets with 5353 port to the specific IP every five seconds.

Applications >> Apple iOS Keep Alive

🗌 Enable Apple iOS Keep Alive

Apple iOS Keep Alive:

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

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

Available settings are explained as follows:

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

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 Conn	ection Detection
Ping Host	
Turn on/off the W	able to ping the host: /i-Fi automatically when the AP is able/unable to ping the host. nable to ping the host:
Wi-Fi:	Off ~
Sound Buzzer:	None 🗸
LED:	No Change 🗸

Available settings are explained as follows:

Item	Description		
Enable Connection Detection	Check the box to enable such function.		
Ping Host	Type an IP address (e.g., 8.8.8.8) or a domain name (e.g., google.com) for testing if the access point is stable or not.		
When the AP is unable	e to ping the host		
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.		
Sound Buzzer	None - When the AP is unable to ping the host, VigorAP will not make any sound.		
	Beep i ~ BeepV - When the AP is unable to ping the host, VigorAP will sound with the selected buzzer type.		
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.

Applications >> Sensor Setting		
Sensor Graph	Sensor Settings	
Enable "Sensor Graph"		
Alerts once 🗸 via "Alerts	ert Method" when any sensor value is outside of "Alert Criteria" range	
Alert Method		
Syslog 🗌 Mai		
Alert Criteria		
2.4GHz Wi-Fi: -30.0	~ 90.0 • C • F , calibration/current val: 0.0 70.0	
	ок	

Temperature Sensor Settings

Note:

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

Available settings are explained as follows:

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.
	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.

Temperature Sensor Graph

Below shows an example of temperature graph:

Applications >> Sensor Graph



Chapter V Mobile APP, DrayTek Wireless



V-1 Introduction of DrayTek Wireless

VigorAP AP903 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>

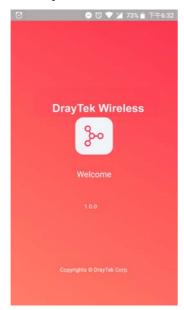
(i) Note:

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 Select a VigorAP

1. Run DrayTek Wireless APP.



2. Choose one AP in the network by clicking the inverted triangle icon to open a drop down list.

53 🖸	ଷ ⊝ • ♥⊿ ∎ 91%	(, ≑‡921,∎07
of o Dray	O Tek	DrayTek Wireless
Welco	ome	
DrayTek \	Vireless	Discovered AP
	\frown	0 192.168.50.117 AP1000C AP
Select VigorAP	×	1 192.168.50.253 Vigor2133 Mesh Root
Admin admin	\Box	
Password		
		Clear Selection
Log	in	
	t Wizard	

Available VigorAP devices with Model Name, IP and Operation mode of VigorAP found by DrayTek Wireless APP will be listed under **Discovered VigorAP**. Choose one of the devices to login (or use Quick Start Wizard function).

If no AP is found, Quick Start Wizard will start with Wi-Fi connection or start with wizard procedure directly.

V-3 Quick Start Wizard

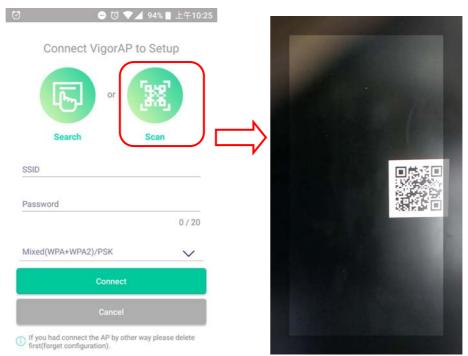
Quick Start Wizard in Wireless APP is useful for connecting an new installed AP and configuring with different Operation Mode.

How to create a Mesh Group?

1. Click Quick Start Wizard.

:56 P	ž	Q ⊖ •♥∡ ü 639
Dray	Tek Wirele	SS
O Select Vi	igorAP	\sim
User Name admin		
Password		
		0
	Login	
Qui	ck Start Wizard	i 👘
(ī) s	upported Model L	ist

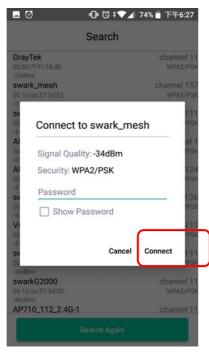
- 2. Under Quick Start Wizard, there are two methods to locate a mesh root, Search and Scan,
 - Click **Scan** to scan the QR code printed on <u>VigorAP packaging box</u> to connect the designated VigorAP.



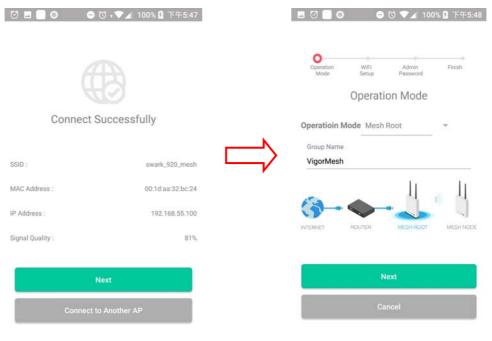
• Or, click **Search**. When the searching result appears, choose one of the AP devices to connect.

Connect Vigor AP to	Sotup	Search	n
Connect VigorAP to	o Setup	swarkTest	channel 1
		00:1d:aa:57:5d:80 -26%	WPA2/PS
	949	swark_wep	channel 1
L [b]	đã,	06:1d:aa:57:5d:80 -26%	WI
		AP810_111_2.4G	channel 1
Search	Scan	00:1d:aa:7e:84:38 -35%	WPA2/PS
		swarkTest	channel 4
		00:1d:aa:57:5d:81	WPA2/PS
SSID		-36%	
		AP710_112_2.4G-1	channel 1
		00:50:7f:f0:d4:e2 -40%	WPA2/PS
Password		DrayTek	channel 1
	1.1211.122	00:1d:aa:32:bc:24	WPA2/PS
	0/20	-41%	1 1 1 1 1
		DrayTek5G 00:1d:aa:68:d6:69	channel 15 WPA2/PS
Mixed(WPA+WPA2)/PSK		-43%	WPAZ/P3
VIIXed(WPA+WPAZ)/PSK	\sim	DrayTek	channel 1
and the second		00:1d:aa:68:d6:68	WPA2/PS
		-43%	
Connect		-43% DrayTek	channel 4
			channel 4 WPA2/PS
		DrayTek	

3. When the following page appears, enter the password for the VigorAP device. Then, click **Connect.**



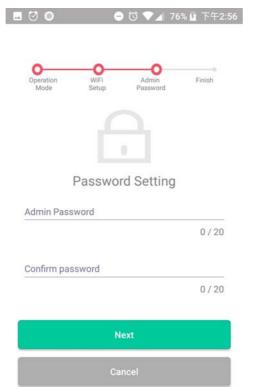
4. When the connection is successful, click **Next**. Then, set Operation Mode of VigorAP as **Mesh Root** and click **Next**.



5. In the following page, set the WiFi Name (SSID) and WiFi Password for your network. You can also enable 2nd SSID by enabling the function of 2nd WiFi. Then, click **Next.**

0	- (উ 🔻 💙 🖊 76	% 🛿 下午2
Operation Mode	WiFi Setup	© Admin Password	© Finish
WiFil	Name 8	& Passwo	rd
WiFi Name			
swark_920			
			9/20
WiFi Password			
			8 / 20
Enable guest W	/iFi		
	Ne	xt	
	Can	cel	

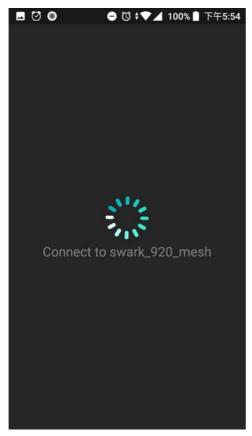
6. Change the default admin password for the network security and click **Next**.



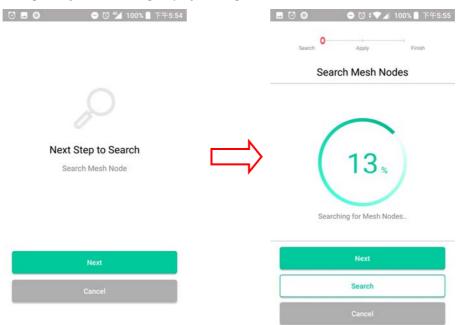
7. In the page of **Check and Apply**, click **Finish** to apply the settings to the specified VigorAP.

0 🖬 🔘	e	T 🗸 🕈	87% 月	下午5:45
0	-0			-0
Operation Mode	WiFi Setup	Admin Password	F	inish
	11.1			
	Check	& Apply		
WiFi Name :			swark_	mesh_5g
WiFi Password :			0	0057002
Admin Password	:			admin
				auriin
OP Mode :			M	esh Root
	Fi	nish		
	Ca	incel		

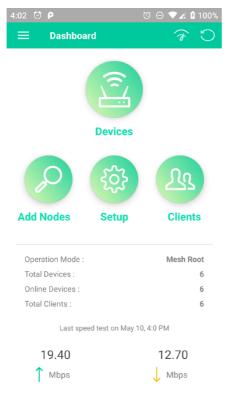
8. After sending configuration to VigorAP, it will take some time to take effect. DrayTek Wireless APP will try to reconnect to wireless network again. Please wait for a while here.



9. 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**.

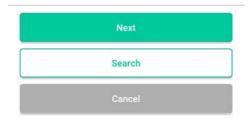


Or, click **Cancel** to return to the home page. Then, click **Add Nodes** to search several Mesh Nodes which do not belong to any other mesh group.



10. Later, available VigorAP devices will be shown on the page. Choose the Mesh Node you want to add and give a device name (e.g., VigorAP920R) for it. The selected mash node(s) will be grouped under such mesh root. Click **Next**.

Sea	ch Apply	Finish
Cł	noose Mesh Node	s to Add
5) 00	igorAP920R D:1D:AA:5C:A6:A8 gorAP920R	(
	igorAP920R 0:1D:AA:57:5D:90 gorAP920R	(
	igorAP920RPD D:1D:AA:5C:A6:D0 gorAP920RPD	(



11. The following page displays the total number of mesh nodes selected. Click **Apply**.

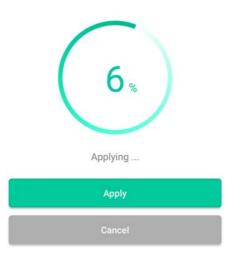
. 🖸	- T - Z	4 93% ■ 上午10:50
Search	O Apply	Finish
Mes	sh Nodes S	etup
Apply S	Settings to Mes	h Node
	3	
MESI	H NODES SELE	CTED
WiFi Name :		alc920_mesh
WiFi Password :		00000000
Group Name :		VigorMesh
	Apply	
	Cancel	

12. Wait until the mesh root applies general configuration to the mesh nodes.



Mesh Nodes Setup

Apply information to Mesh Node



13. Later, current status of the mesh node(s) will be shown on the following page. Click **Finish**.

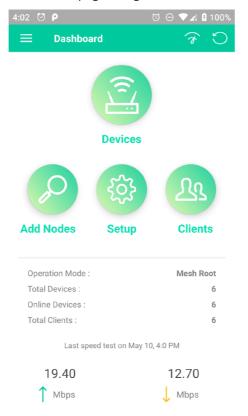


Mesh Nodes Setup

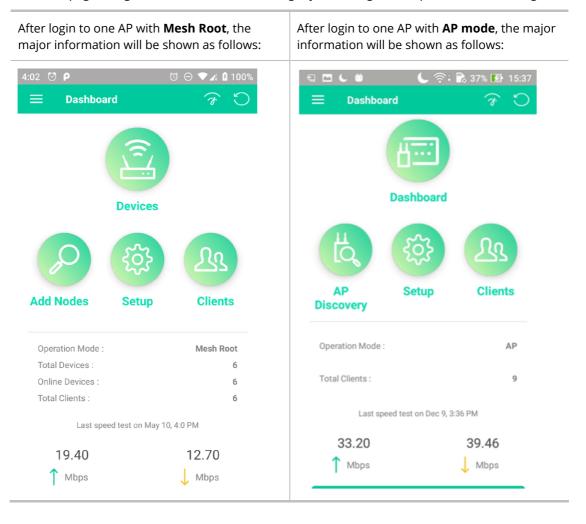
F	inish
Total Devices :	4
Online :	3
Offline :	1
Root :	00:1D:AA:5C:A6:38
ONLINE :	00:1D:AA:5C:A6:A8
ONLINE :	00:1D:AA:57:5D:90
OFFLINE :	00:1D:AA:5C:A6:D0

Finish

14. Now, the main page of VigorAP APP will be displayed as follows.



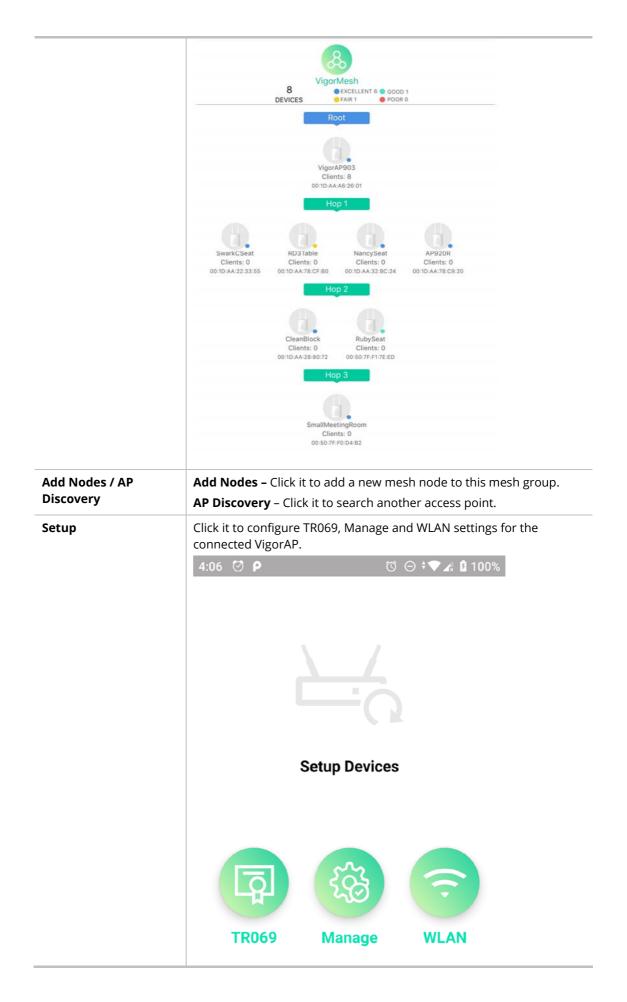
V-4 Login



The main page of VigorAP APP will be different slightly according to the operation mode of VigorAP.

Available settings are explained as follows:

ltem	Description
Devices / Dashboard	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 with hop number. One mesh group contains up to eight devices.



Clients

Displays general information for all clients in Mesh Group or all clients connected to the selected AP (non-mesh device).

	C C	C 奈 89% 下午6:37	
	CI	ients 10 CLIENTS	
	0C:9D:92:72:C6:E2	AP903_Field_117(VigorAP903)	
	76% 🗢	0 Kbps 🤳 0 Kbps 🕇	
	2 Guangdon	AP903_Field_117(AlbertCSeat) 0 Kbps 🕹 0 Kbps 🕇	
	3 android-179b2b4dc	AP903_Field_117(VigorAP903)	
	100 % ·•	0 Kbps 👃 0 Kbps 🕇	
	4 KuoChentekiiPad	AP903_Field_117(AlbertCSeat) 0 Kbps 📙 0 Kbps 🕇	
	F4:F5:DB:C7:4F:BF	AP903_Field_117(RD3Table)	
	5 18% 🔶	0 Kbps 🕹 0 Kbps 🕇	
	6 KuoChentekiiPad	AP903_Field_117(SmallMeetingRo 0 Kbps 上 0 Kbps 🕇	
	android-4d8ed542f		
	7 45% 🛜	AP903_Field_117(SmallMeetingRo 0 Kbps 📙 0 Kbps 🕇	
	android-6b1e2c1b2	AP903_Field_117(SmallMeetingRo	
	68% 🗢	22 Kbps 🤳 5410 Kbps 🕇	
	9 F4:F5:DB:C7:4F:BF 78 % 🗢	AP903_Field_117(SmallMeetingRo 0 Kbps 📙 0 Kbps 🕇	
	1 al Contrato del Casto Manifest		
	10 Fanny-iPad	AP903_Field_117(NancySeat)	
	10 Fanny-IPad	AP903, Field_117(NancySeat) 0 Kbps 上 0 Kbps 🕇	
Operation Mode	10 96% 🗢	0 Къря 🚺 0 Къря 🕇	ot, AP, Mesh Node) of this
Operation Mode Total Devices	Display the operation AP.	0 Къря 🚺 0 Къря 🕇	
-	Display the operation AP. Display the number of group.	окъря окъря † Окъря †	uped under this mesh
Total Devices	Display the operation AP. Display the number of group. Display current online	The total clients conr	uped under this mesh
Total Devices Online Devices	 Display the operation AP. Display the number of group. Display current online Display the number or the selected AP (not selected AP (not	The total clients conr	uped under this mesh ler this mesh group. nected to the mesh group

This page is left blank.

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 1000C.

Diagnostics V
System Log
Speed Test
Traffic Graph
Where am I ?
WLAN (2.4GHz) Statistics
WLAN (5GHz) Statistics
WLAN (5GHz-2) Statistics
Interference Monitor

Dray Tek

VI-1-1 System Log

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

Diagnostics >> System Log

System Log Information

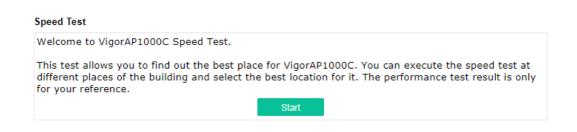
| Clear | Refresh | 🗌 Line wrap |

Mar	2 09:20:29	kernel: [330839.940723] ol_scan_unregister_event_handler: Failed to unregi
Mar	2 09:20:29	kernel: [330839.940723]
Mar	2 09:20:29	kernel: [330839.950384] osif_vap_stop: Scan in progress Cancelling it. vap
Mar	2 09:20:29	kernel: [330839.975642] br0: port 7(ath90) entered forwarding state
Mar	2 09:20:29	kernel: [330839.986752] Auto Channel Select :
Mar	2 09:20:29	kernel: [330839.986767] 100 104
Mar	2 09:20:29	kernel: [330839.986783] 108 112
Mar	2 09:20:29	kernel: [330839.986794] 116 120
Mar	2 09:20:29	kernel: [330839.986805] 124 128
Mar	2 09:20:29	kernel: [330839.988500] br0: port 7(ath90) entered disabled state
Mar	2 09:20:30	kernel: [330840.815668] br0: port 8(ath91) entered forwarding state
Mar	2 09:20:31	kernel: [330842.023482] osif_vap_init: Scan in progress Cancelling it. vap:
Mar	2 09:20:31	kernel: [330842.031806] osif_vap_init: Failed to cancel Scan!
Mar	2 09:20:31	kernel: [330842.066917] br0: port 7(ath90) entered forwarding state
Mar	2 09:20:31	kernel: [330842.071313] br0: port 7(ath90) entered forwarding state
Mar	2 09:20:31	kernel: [330842.077461] 8021q: adding VLAN 0 to HW filter on device ath90
Mar	2 09:20:31	kernel: [330842.158674] of scan unregister event handler: Failed to unregi

VI-1-2 Speed Test

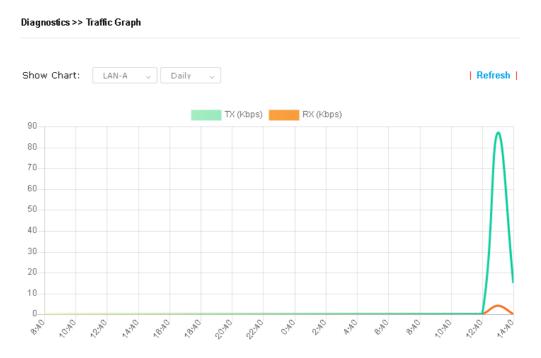
Click the **Start** button on the page to test the speed. Such feature can help you to find the best installation place for Vigor AP.

Diagnostics >> Speed Test



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 Where am I

This function is useful for the administrator to locate the access points to build the best signal transmitting position for multiple access points.

Diagnostics >> Where am I ?			
Where am I ?			
Welcome to VigorAP10	00C Where am I ?		
The buzzer will sound v locate the access point	when the "Sound" button is clicked. This is useful for network administrators to		

Available parameters are explained as follows:

ltem	Description
Sound	Use the drop down list to specify a special sound for such access point.
for XX seconds	Set the duration time of the beep sound.

Sound	Activate the buzzer of the access point.
Stop	Terminate the buzzer of the access point.

VI-1-5 WLAN (2.4GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (2.4GHz) Statistics

		Auto-Refree	sh Refresh
Tx Data Packets	0	Rx Data Packets	0
Tx Data Bytes	0	Rx Data Bytes	0
Average Tx Rate (kbps)	No Station	Average Rx Rate (kbps)	No Station
Tx Unicast Data Packets	0	Rx PHY errors	0
Tx Multi/Broadcast Data Packets	0	Rx CRC errors	737
Tx failures	0	Rx MIC errors	0
		Rx Decryption errors	0
		Rx errors	0

	SSID1 (DrayTek-04F2C8)	SSID2 (marketing)	S SID3 (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)	No Station	No Station	N/A	N/A
Average Rx Rate (kbps)	No 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-Refres	h Refresh
Tx Data Packets	0	Rx Data Packets	0
Tx Data Bytes	0	Rx Data Bytes	0
Average Tx Rate (kbps)	No Station	Average Rx Rate (kbps)	No Station
Tx Unicast Data Packets	0	Rx PHY errors	0
Tx Multi/Broadcast Data Packets	0	Rx CRC errors	12673
Tx failures	0	Rx MIC errors	0
		Rx Decryption errors	0
		Rx errors	0

	SSID1 (DrayTek-04F2C8)	SSID2 (marketing)	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)	No Station	No Station	N/A	N/A
Average Rx Rate (kbps)	No 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 WLAN (5GHz-2) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (5GHz-2) Statistics

		Auto-Refres	h Refresh
Tx Data Packets	0	Rx Data Packets	0
Tx Data Bytes	0	Rx Data Bytes	0
Average Tx Rate (kbps)	No Station	Average Rx Rate (kbps)	No Station
Tx Unicast Data Packets	0	Rx PHY errors	901493
Tx Multi/Broadcast Data Packets	0	Rx CRC errors	7430
Tx failures	0	Rx MIC errors	0
		Rx Decryption errors	0
		Rx errors	0

	SSID1 (DrayTek-04F2C8)	SSID2 (marketing)	S SID3 (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)	No Station	No Station	N/A	N/A
Average Rx Rate (kbps)	No Station	No Station	N/A	N/A
Rx errors	0	0	N/A	N/A
Tx failures	0	0	N/A	N/A

VI-1-8 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 or 5G-2) selected. Also, channel status can be seen easily from this page.

Current Channe	L .	All Channels			
				Auto-Refresh	Refresh
Channel Informa	tion				
land	2.4G	/	Country Code	FR	
hannel	11		Mode	Mixed(11b+1	11g+11n)
x Power	100%		Bandwidth	40 MHz	
Channel Status					
Channel Load		11 29%			
Noise Floor		5 1%			
APs		9			
Max RSSI		8			
Min RSSI		40			
The history of	1-5 minute	5 🗸			
18.5					Load
0.0	9:43:30	09:44:30	09:45:30 09:46:	30 09:47:	30

Diagnostics >> Interference Monitor

Dray Tek

All Channels

This page displays the utilization and energy result for all channels based on 2.4G/5G. Click **Refresh** to get the newly update interference situation.

Band	2.40	3 v	Refresh
Recommended ch	nannel for usage: 6		
Channel	Channel Load	Noise Floor	APs
1	35%	1%	6
2 2	3%	1%	0
3 16	%	3%	5
4 11	%	1%	0
5 18	%	1%	0
6 20	9%	1%	4
7 9%	6	1%	0
8 <mark>5</mark> 9	6	1%	0
9 17	%	1%	2
10	36%	1%	0
11	47%	1%	14
12 🔁	9%	1%	0
13 89	6	1%	1
			ed: 11/01 09:49:

Diagnostics >> Interference Monitor

VI-1-9 Support Area

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



Dray Tek

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

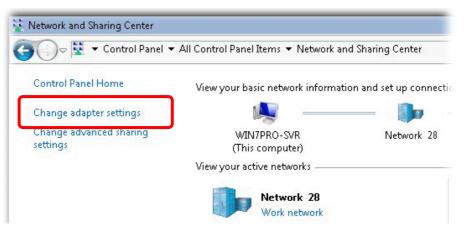
(i) Note:

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**.

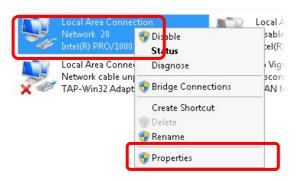
1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



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 Mic		
🗹 县 Privacyware		
🗹 📙 QoS Packet		
🗆 📇 File and Prin	ter Sharing for Microsoft	Networks
		6)
March Internet Prot	CONTRACTOR A CTORNER.	
	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.					
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 ddree		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.

€ 0	Network	\bigcirc
Show All Displays Sou	nd Network Startup Disk	
L	Show: Built-in Ethernet	
ТСР	IP PPPoE AppleTalk Proxies Ethernet	
Configure IPv4:	Using DHCP	
IP Address:	192.168.1.10 Renew DHCP Lease	
Subnet Mask:	255.255.255.0 DHCP Client ID:	
Router:	(If required) (192.168.1.2	
DNS Servers:	(Optional)	
Search Domains:	(Optional)	
IPv6 Address:	fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
	Configure IPv6	
Click the lock to p	revent further changes. Assist me Apply Now	\supset

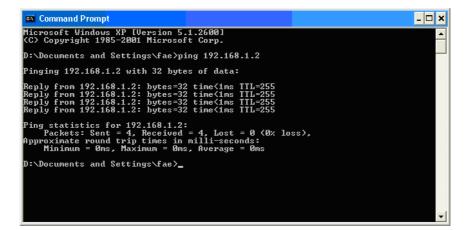
VI-4 Pinging the Device

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.

\varTheta 🔿 🔿 Terminal — bas	h — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1 Welcome to Darwin!	2
Vigor10:~ draytek\$ ping 192.168.1.1	
PING 192.168.1.1 (192.168.1.1): 56 data byte	es
64 bytes from 192.168.1.1: icmp_seq=0 ttl=2!	
64 bytes from 192.168.1.1: icmp_seq=1 ttl=2!	
64 bytes from 192.168.1.1: icmp_seq=2 ttl=2	55 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=2	55 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=2!	55 time=0.72 ms
192.168.1.1 ping statistics	
5 packets transmitted, 5 packets received, 1	0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 (SAME TO COMPANY AND A REPORT OF A R
Vigor10:~ draytek\$	58.6957

Dray Tek

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.

Do You want to reboot your AP ?
 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.

Dray Tek

Index

8

802.11n, 39

Α

Access Control, 44 Action, 127 Advanced Setting, 47 AES, 28 Airtime Fairness, 51 Antenna, 47 AP Discovery, 49 AP Management, 105 AP Mode, 37, 68, 81 AP Operation Mode, 17 APM Log, 106 Apple iOS Keep Alive, 129 Applications, 126 Auth Mode, 46 Authentication Client, 123 Authentication Type, 123 Auto Adjustment, 51 Auto Channel Filtered Out List, 48 Auto Logout, 13 Auto Provision, 105

В

Band Steering, 57 Bandwidth Limit, 18, 21, 27 Bandwidth Management, 50 Black List, 107

С

Central AP Management, 105 Certificate Management, 123 Changing Password, 14 Channel, 39, 82 Channel Width, 47 Client IP, 123 Client PinCode, 46 Client's MAC Address, 107 Configuration Backup, 95, 96 Connection Time, 54 Connection Type, 83 Country Code, 48

D

Data Flow Monitor, 152 Default Gateway, 83 Detection, 110, 116, 117 DHCP Client, 85 DHCP server, 11 Download Limit, 51

Ε

EAP Type, 123 Encryp Type, 46 End Time, 127 Extension Channel, 39

F

Factory Default Setting, 165 Fast Roaming, 56 Firmware Upgrade, 104 Force Overload Disassociation, 107 Fragment Length, 48

G

General Setup, LAN, 85

Η

Hardware Reset, 165 Hide SSID, 39 HTTP port, 101 HTTPS, 125 HTTPS port, 101

I

Interference Monitor, 156 IP Address, 83, 85 Isolate Member, 40

Κ

Keep Alive Period, 93 Key Renewal Interval, 42 Key Size, 125 Key Type, 125

L

LAN, 85 LAN port, 88 Lease Time, 86 LED Indicators and Connectors, 2 Limit Client, 38 Limit Client per SSID, 38 Load Balance, 107

Μ

MAC Address, 82 MAC Address Filter, 45 MAC Clone, 48 Main SSID, 17, 20, 26 Management, 101 Management VLAN, 85 Mobile Device Management, 110 Mode, 39, 41

Ν

NTP, 126 NTP Client, 99 NTP synchronization, 99

0

Once, 128 Open/Shared, 28, 83 Operation Mode, 32 Overload Management, 107

Ρ

Pass Phrase, 42, 83 Password, 14 Password Strength, 94 Periodic Inform Settings, 93 PIN Code, 35 PMK Cache Period, 56 Policy, 44, 118, 119 Port, 43 Port Control, 88 Pre-Authentication, 56 Primary DNS Server, 86 PSK, 34 Push Button, 46

Q

Quick Start Wizard, 16

R

RADIUS Server, 42, 122 RADIUS Setting, 122 Reboot System, 103 Reconnection Time, 54 Relay Agent, 86 Restore, 45 Roaming, 55 Router Name, 83 Routine, 128 RSSI, 55 RTS Threshold, 48

S

Schedule, 126 Secondary DNS Server, 86 Secret Key, 123 Security, 41 Security Mode, 82 Security Overview, 34 Security Settings, 41 Session Timeout, 43 Shared Secret, 43 Show Chart, 116 Simulate 2 APs, 39 Software Reset, 165 Speed Test, 151 SSL(HTTPS), 93 Start Date, 127 Start PBC, 35 Start Time, 127

DrayTek

Station Control, 18, 21, 27, 53 Station List, 62 Status of Settings, 108 STUN, 93 Subject Name, 124 Subnet, 40 Subnet Mask, 83, 85 Support Area, 158 Syslog/Mail Alert, 98 System Log, 151 System Maintenance, 90 System Status, 91

Т

Temperature Sensor, 130, 131 Temperature Sensor Graph, 132 Time and Date, 99 TKIP, 28, 34 Total Download Limit, 51 Total Upload Limit, 51 TR-069, 92 Traffic Graph, 152 traffic overload, 107 Triggering Client Number, 52 Trust DHCP Server, 86 Tx Power, 48

U

Upload Limit, 50 Users Profile, 123

V

VLAN ID, 40, 85

W

WEP, 28 WEP (Wired Equivalent Privacy), 34 White List, 107 Wi-Fi DOWN, 128 Wi-Fi UP, 128 Wireless LAN (2.4GHz/5GHz), 34 WLAN (2.4GHz) Statistics, 153 WLAN (5GHz) Statistics, 154, 155 WPA (Wi-Fi Protected Access), 34 WPA Algorithms, 42 WPS, 45 WPS (Wi-Fi Protected Setup), 34