DrayTek

VigorAP 906

802.11ax Access Point

USER'S GUIDE

V1.0

VigorAP 906

802.11ax Access Point

User's Guide

Version: 1.0

Firmware Version: V1.4.5

Date: Nov. 9, 2022

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 8, 10, 11 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the device.
- The device is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the device yourself.
- Do not place the device in a damp or humid place, e.g. a bathroom.
- Do not stack the devices.
- The device should be used in a sheltered area, within a temperature range of 0 to +45 Celsius.
- Do not expose the device 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 device, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor router via https://myvigor.draytek.com.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

https://www.draytek.com

Table of Contents

Chapter I Installation VII

I-1 Introduction 1

I-1-1 LED Indicators and Connectors 2

I-2 Hardware Installation 4

I-2-1 Wired Connection for PC in LAN 4
I-2-2 Wired Connection for Notebook in WLAN 5
I-2-3 Wireless Connection 6
I-2-4 PoE Connection 7
I-2-5 Wall-mount Connection 8

I-3 Network IP Configuration 9

I-3-1 Windows 10 IP Address Setup 9

I-4 Accessing to Web User Interface 12

I-5 Changing Password 15

I-6 Dashboard 16

I-7 Quick Start Wizard 17

I-7-1 Settings for Access Point 18
I-7-2 Settings for Mesh Root 21
I-7-3 Settings for Mesh Node 26

Chapter II Connectivity 27

II-1 Operation Mode 28

II-2 General Concepts for Wireless LAN (2.4GHz/5GHz) 29

II-3 Wireless LAN (2.4GHz/5GHz) Settings for AP Mode 32

II-3-1 General Setup 33
II-3-2 Security 36
II-3-3 Access Control 39
II-3-4 WPS 40
II-3-5 Advanced Setting 41
II-3-6 AP Discovery 44
II-3-7 WDS AP Status 45
II-3-8 Bandwidth Management 45
II-3-9 Airtime Fairness 46
II-3-10 Station Control 48
II-3-11 Roaming 50
II-3-12 Band Steering (for Wireless LAN (2.4GHz)) 52
II-3-13 Station List 57

II-4 Mesh Settings for Mesh Mode 63

II-4-1 Mesh Setup 65
II-4-2 Mesh Status 70
II-4-3 Mesh Discovery 71
II-4-4 Basic Configuration Sync 72
II-4-5 Advanced Config Sync 75
II-4-6 Support List 75
II-4-7 Mesh Syslog 76

II-5 LAN 77

II-5-1 General Setup 77
II-5-2 Hotspot Web Portal 81
II-5-3 Port Control 85
II-5-4 Hardware Acceleration 86

Chapter III Management 87

III-1 System Maintenance 88

III-1-1 System Status 89
III-1-2 TR-069 90
III-1-3 Administrator Password 92
III-1-4 User Password 93
III-1-5 Configuration Backup 94
III-1-6 Syslog/Mail Alert 96
III-1-7 Time and Date 97
III-1-8 SNMP 99
III-1-9 Management 100
III-1-10 Reboot System 102
III-1-11 Firmware Upgrade 103

III-2 Central AP Management 104

III-2-1 General Setup 104
III-2-2 APM Log 105
III-2-3 Overload Management 106
III-2-4 Status of Settings 107

III-3 Mobile Device Management 109

III-3-1 Station List 109
III-3-2 Station Statistics 115
III-3-3 Station Nearby 116
III-3-4 Policies 117
III-3-5 Station Control List 118

Chapter IV Others 119

IV-1 RADIUS Setting 120

IV-1-1 RADIUS Server 120
IV-1-2 Certificate Management 121

IV-2 Applications 124

IV-2-1 Schedule 124
IV-2-2 Wi-Fi Auto On/Off 127

IV-3 Objects Setting 128

IV-3-1 Device Object 128
IV-3-2 Device Group 130

Chapter V Mobile APP, DrayTek Wireless 133

V-1 Introduction of DrayTek Wireless 134

V-2 Create a New Network 135

V-3 Wizard - Mesh Root and Mesh Node 137

V-4 Login 141

V-4-1 Network 142
V-4-2 Connect 143
V-4-2-1 Dashboard of the Device 144
V-4-2-2 Devices 145
V-4-2-3 Clients / Groups 147
V-4-2-4 Setup 148

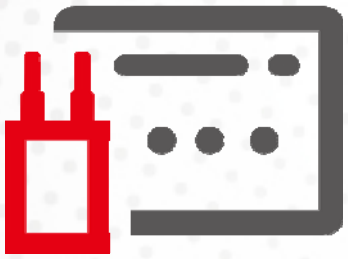
Chapter VI Troubleshooting 149

VI-1 Diagnostics 150

VI-1-1 System Log 151
VI-1-2 Speed Test 151
VI-1-3 Traffic Graph 152
VI-1-4 WLAN (2.4GHz) Statistics 153

VI-1-5 WLAN (5GHz) Statistics 154
VI-1-6 Interference Monitor 155
VI-1-7 Support Area 155
VI-2 Checking the Hardware Status 156
VI-3 Checking the Network Connection Settings 157
VI-3-1 For Windows 157
VI-3-2 For Mac Os 159
VI-4 Pinging the Device 160
VI-4-1 For Windows 160
VI-4-2 For Mac Os (Terminal) 160
VI-5 Backing to Factory Default Setting 162
VI-5-1 Software Reset 162
VI-5-2 Hardware Reset 162
VI-6 Contacting DrayTek 163

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 the local distributor.

Thank you for purchasing this VigorAP 906, the concurrent dual-band wireless (2.4G/5G) access point offering high-speed data transmission. With this high cost-efficient VigorAP 906, computers and wireless devices which are compatible with 802.11ax can connect to the existing wired Ethernet network via this VigorAP 906, at the speed of 300Mbps.

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

VigorAP 906 also is a Power over Ethernet Powered Device which adopts the technology of PoE for offering power supply and transmitting data through the Ethernet cable.

AP Management

The VigorAP 906 can operate in standalone mode for your office network or a classroom or a waiting room of some transportation terminals (e.g. ferry terminal, bus station, train station) or a clinic's waiting room; connected to your LAN and offering you with wireless access. If your network requires several VigorAP 906 units, centrally manage and monitor them individually as a group will be expected. DrayTek central wireless management (AP Management) lets control, efficiency, monitoring, and security of your company-wide wireless access easier be managed. Inside the web user interface, we name the “central wireless management” as Central AP Management which supports mobility, client monitoring/reporting, and load-balancing to multiple APs. For central wireless management, you will need a Vigor2865 or Vigor2927 series router; there is no per-node licensing or subscription required. For multiple wireless clients to apply the AP Load Balancing to the multiple APs, AP management will manage wireless traffic with smooth flow and enhanced efficiency.

Support Mesh Network

The message, information, and data can be transferred via wireless connection among VigorAP 906 devices without using Ethernet cables. It can reduce the construction cost and eliminate the trouble of wiring. Therefore, mesh AP is suitable for outdoor activities, or meetings.

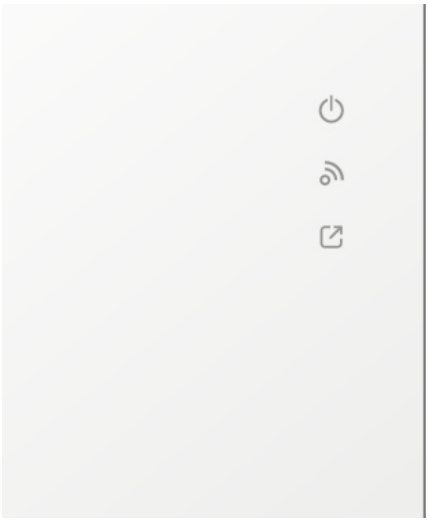
In short, VigorAP with mesh function has the following benefits:

- In the traditional wireless network, users must choose the best signal source manually from various SSIDs. The mesh AP can find out the best route automatically.
  Besides, if any one of the mesh AP devices disconnects due to an unknown reason, the mesh system will determine another accessible AP and transfer the packets to that AP.
- Maintain a certain degree of normal operation for it is not easily affected by connection interference or terrain blocking of walls or floors.
- For the mesh network system to adopt the mesh topology, each node in the network not only has a single connection but also interweaves to other nodes like a net. Because of such characteristics, the mesh network can set up stronger network architecture.

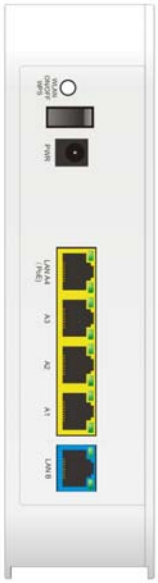
- Each node (mesh AP) in the mesh network can be operated as an independent wireless AP; therefore, the whole mesh network can offer a more stable and faster wireless connection.
- The mesh network is suitable for large spaces and large numbers of people for the configuration for each AP is easy and simple.

I-1-1 LED Indicators and Connectors

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



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
	Blinking with WLAN	WPS is enabled and waiting for the response from the wireless client.
WLAN	Off	Wireless function is not ready.
	On	Wireless function is ready.
	Blinking	Data is transmitting (sending/receiving).
	Blinking with ACT	WPS is enabled and waiting for the response from the wireless client.
UPLINK	On	Connects to a Gateway.
	Off	Disconnects to a Gateway.



Interface	Description
WLAN ON/OFF WPS	Wireless band will be switched /changed according to the button pressed and released. For example, ● 2.4G (On) and 5G (On) – in default. ● 2.4G (Off) and 5G (On) – pressed and released the button once. ● 2.4G (On) and 5G (Off) – pressed and released the button twice. ● 2.4G (Off) and 5G (Off) – pressed and released the button three times. WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds. The router will wait for any wireless client connecting to it through WPS.
	Power switch.
	PWR: Connecter for a power adapter.
 LAN A4-A1 A4 (PoE) LAN B	Connectors for local networked devices. ● Left LED on - The port is connected. ● Left LED off - The port is disconnected. ● Left LED Blinking - The data is transmitting. ● Right LED on -The port is connected with 1000Mbps. ● Right LED off - The port is connected with 10/100 Mbps. **In which,** LAN A4 is used for PoE connection (for indoor use).
 Factory Reset	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 10 seconds. Then the router will restart with the factory default configuration.

Note:

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

I-2 Hardware Installation

This section will guide you to install the VigorAP 906 through a hardware connection and configure the device's settings through the web browser.

Before starting to configure VigorAP 906, you have to connect your devices correctly.

I-2-1 Wired Connection for PC in LAN

1. Connect VigorAP 906 to xDSL modem, router, or switch/hub in your network through the **LAN B** port of the access point by Ethernet cable.

   You can also connect VigorAP 906 to a Vigor router via wireless connection. For detailed information, refer to VigorAP 906 User's Guide.

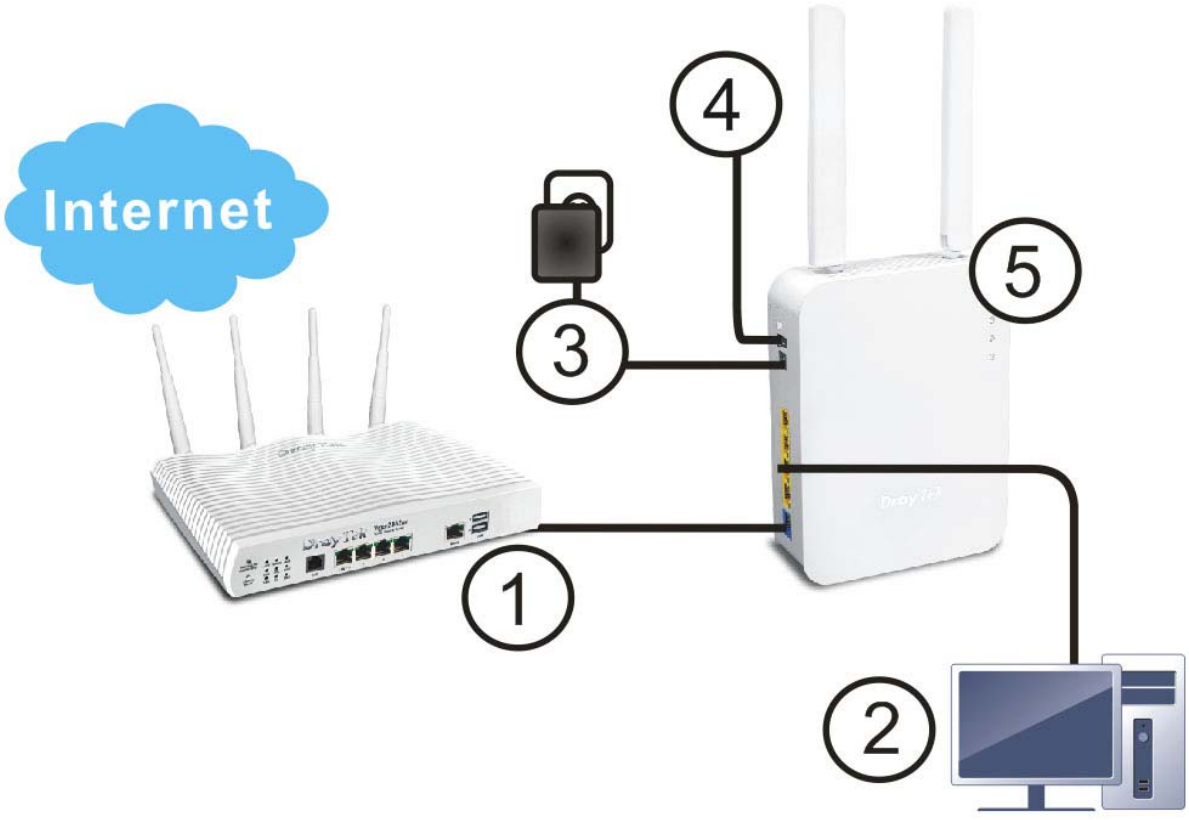
2. Connect a computer to other available LAN A port. Make sure the subnet IP address of the PC is the same as VigorAP 906 management IP, e.g., 192.168.1.X.

3. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.

4. Power on VigorAP 906.

5. Check all LEDs on the front and back panel. The ACT LED on the front panel should blink; WAN/LAN LED on the back panel should be on if the access point is correctly connected to the xDSL modem, router or switch/hub.

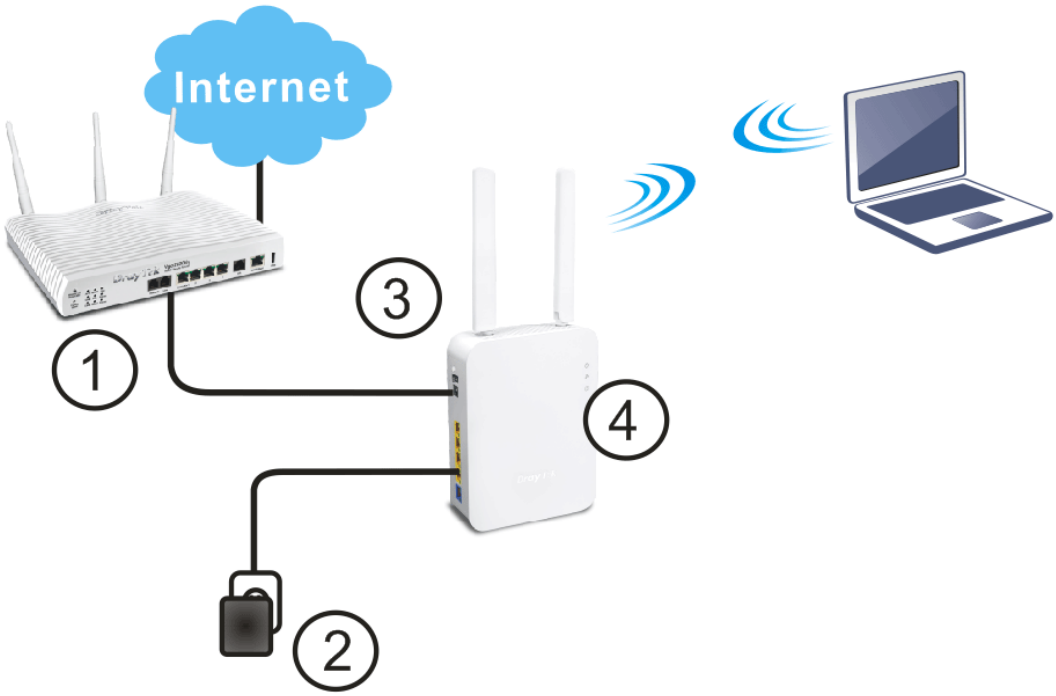
(For detailed information on LED status, please refer to section I-1-1.)



I-2-2 Wired Connection for Notebook in WLAN

1. Connect VigorAP 906 to the ADSL modem or router in your network through the **LAN A** port of the access point by Ethernet cable.
2. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.
3. Power on VigorAP 906.
4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem or router.

(For detailed information on LED status, please refer to section I-1-1.)

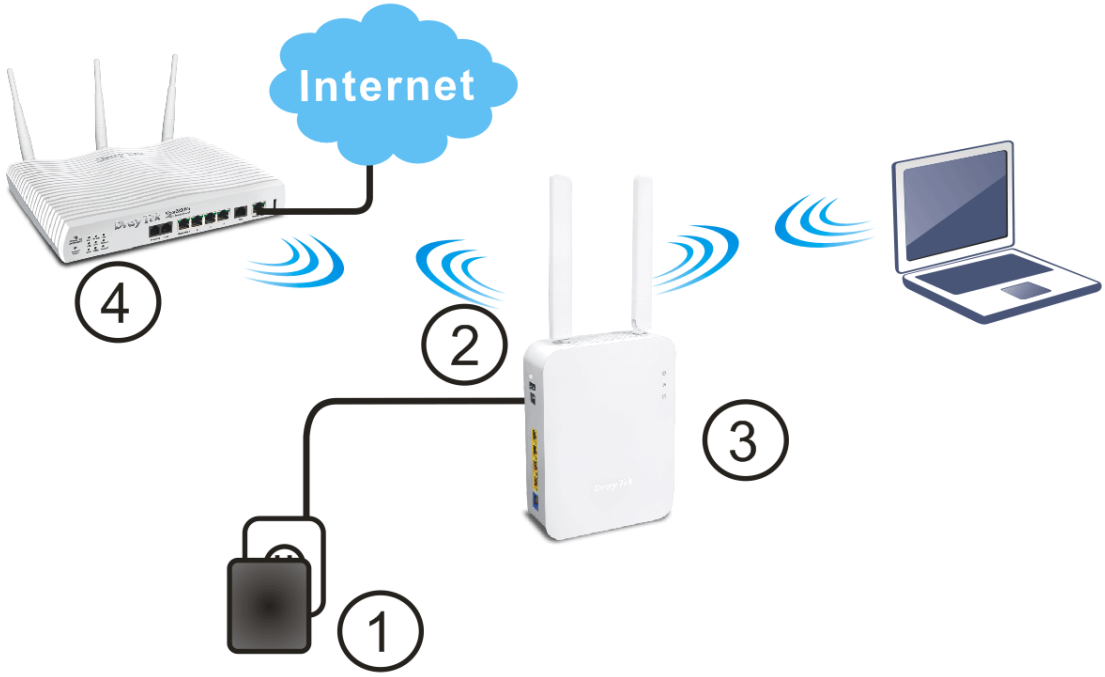


I-2-3 Wireless Connection

VigorAP 906 can access the Internet via an ADSL modem, router, or switch/hub in your network through a wireless connection.

1. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.
2. Power on VigorAP 906.
3. Check all LEDs on the front panel. **ACT** LED should be steadily on.
4. Connect VigorAP 906 to the ADSL modem or router via a wireless network.

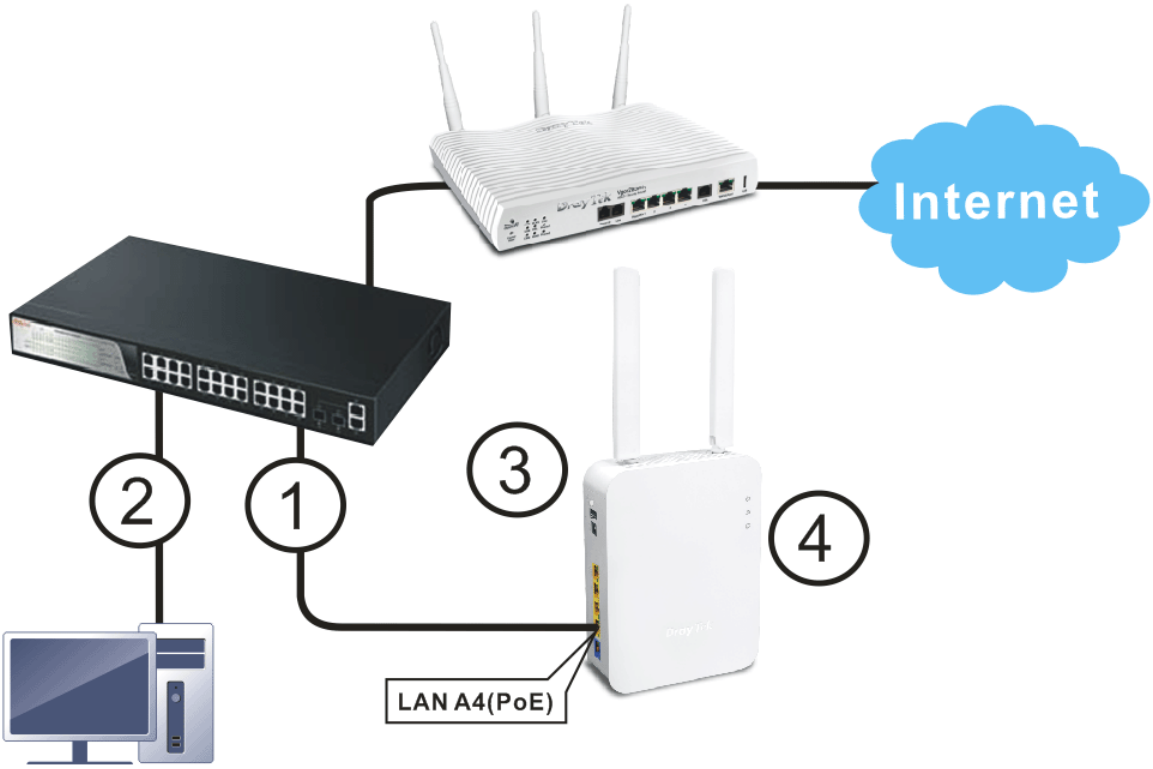
(For detailed information on LED status, please refer to section I-1-1.)



I-2-4 PoE Connection

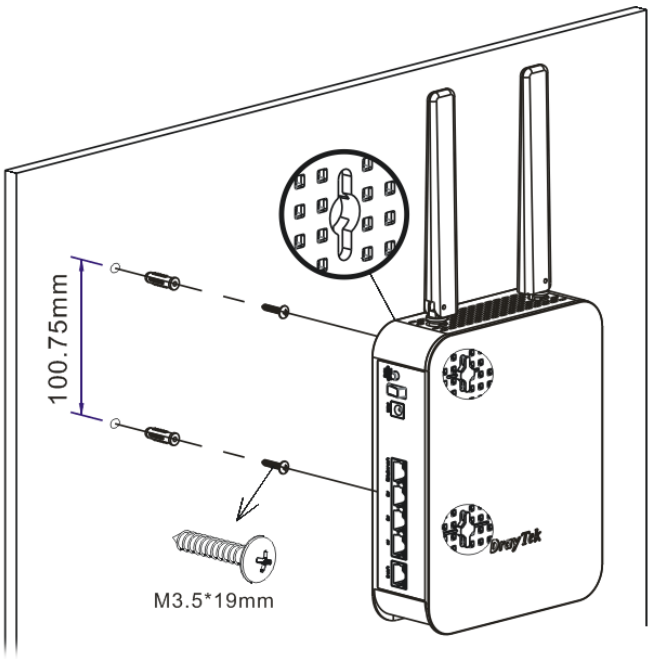
VigorAP 906 can gain power from the connected switch, e.g., VigorSwitch PQ2200xb. PoE (Power over Ethernet) can break the install limitation caused by the fixed power supply.

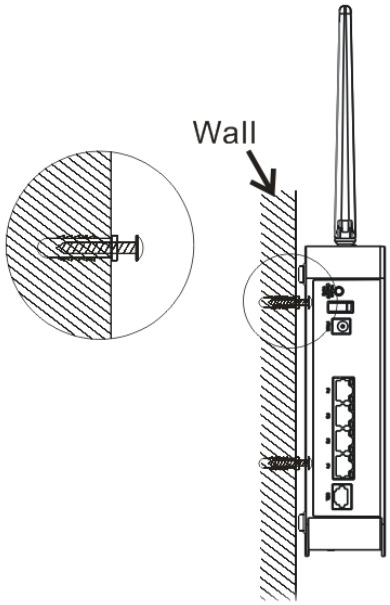
1. Connect VigorAP 906 to a switch in your network through the **LAN A4 (PoE)** port of the access point by Ethernet cable.
2. Connect a computer to VigorSwitch. Make sure the subnet IP address of the PC is the same as VigorAP 906 management IP, e.g., **192.168.1.X**.
3. Power on VigorAP 906.
4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem, router, or switch/hub.



I-2-5 Wall-mount Connection

1. Drill two holes on the wall. The distance between the holes shall be 100.75mm. The recommended drill diameter shall be 6.5mm (1/4”).
2. Fit screws into the wall using the appropriate type of wall plug.
3. Hang the VigorAP directly onto the screws.





I-3 Network IP Configuration

After the network connection is built, the next step you should do is set up VigorAP 906 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 the default IP address of this AP.

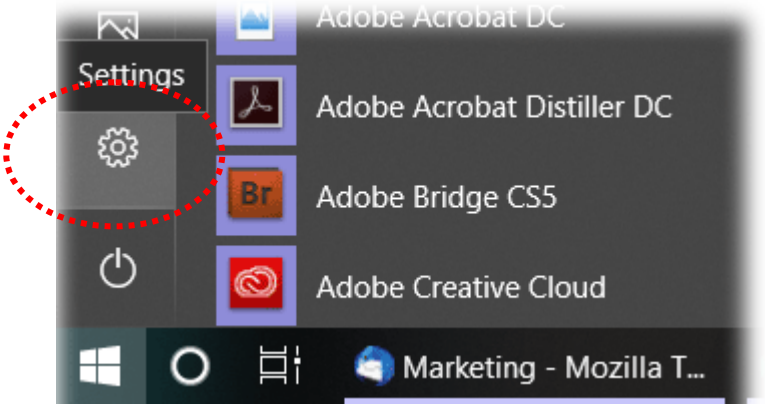
For the default IP address of this AP is set to "192.168.1.2", we recommend you to use "192.168.1.X (except 2)" in the field of IP address on this section for your computer.

If the operating system of your computer is...

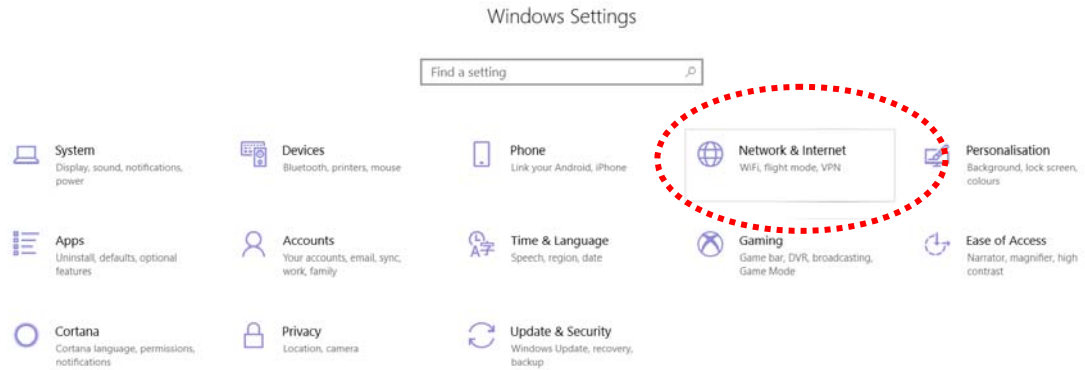
Windows 10 **- please go to section I-3-1**

I-3-1 Windows 10 IP Address Setup

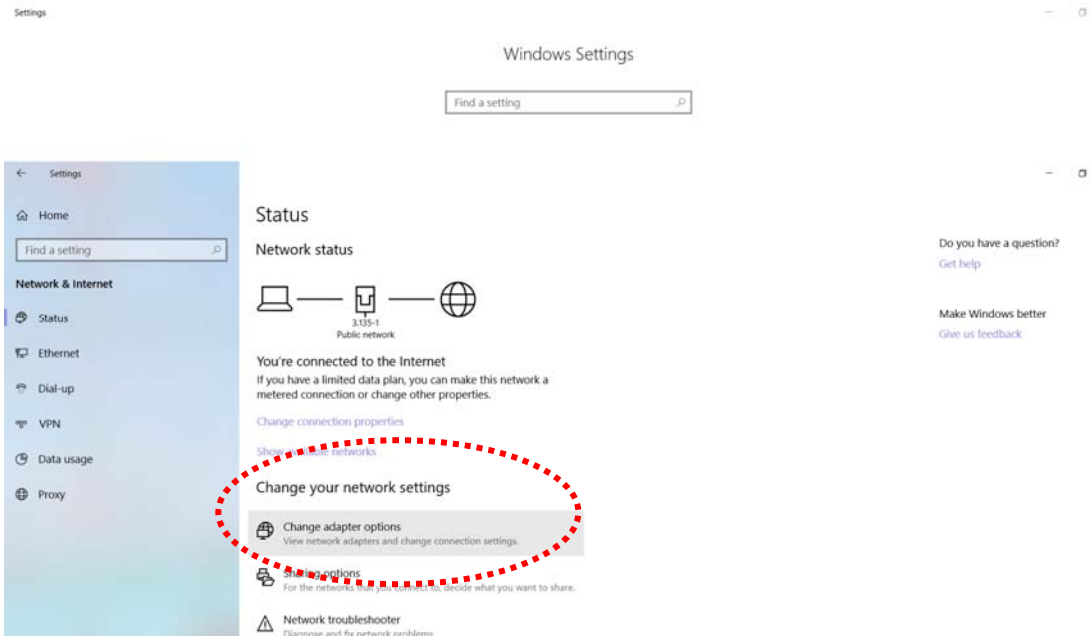
Click the **Start** button (it should be located at the lower-left corner of your computer), then click the **Settings** icon.



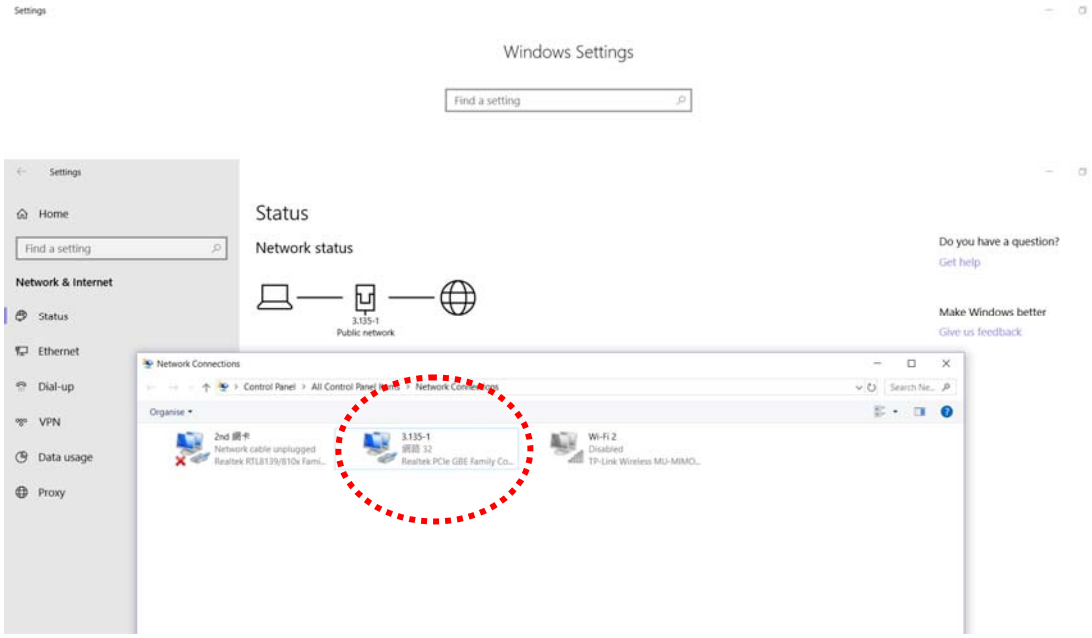
Double-click **Network & Internet**.



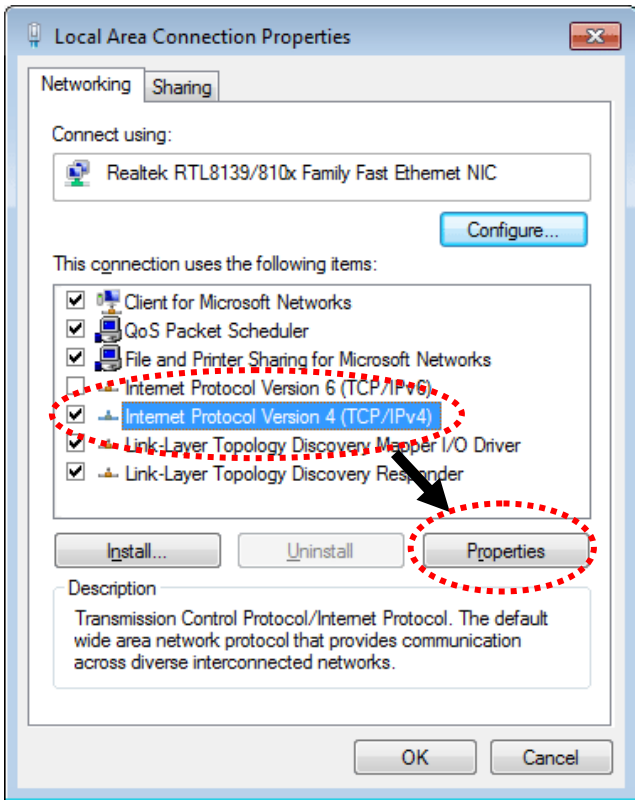
Next, click **Change adapter options**.



Click the local area connection.



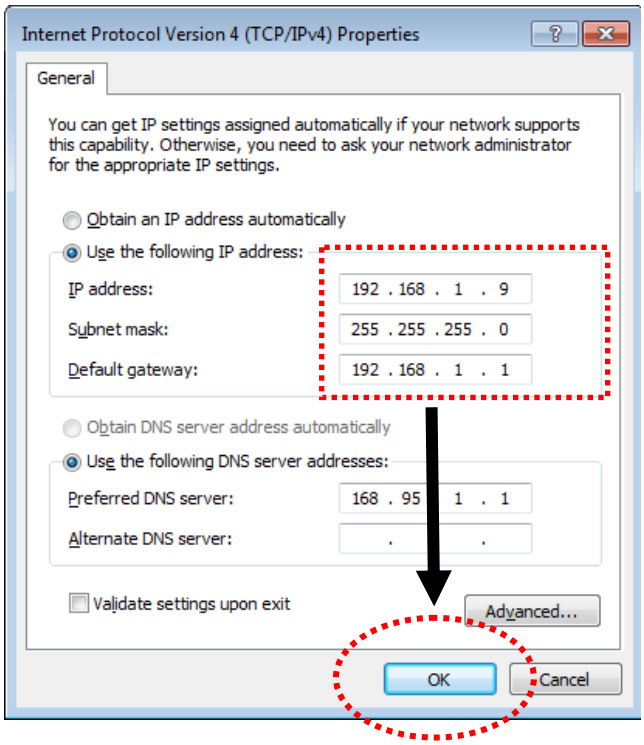
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



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

IP address: **192.168.1.9**

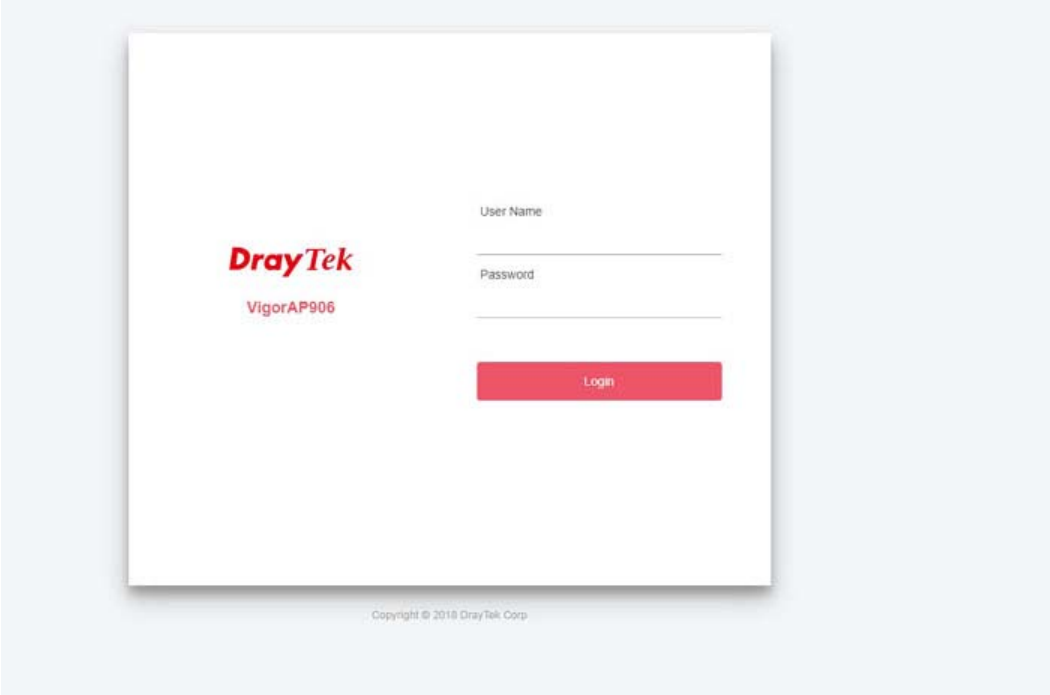
Subnet Mask: **255.255.255.0**



I-4 Accessing to Web User Interface

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

1. Make sure your PC connects to the VigorAP 906 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 a username and password. Please type “admin/admin” on Username/Password and click **OK**.

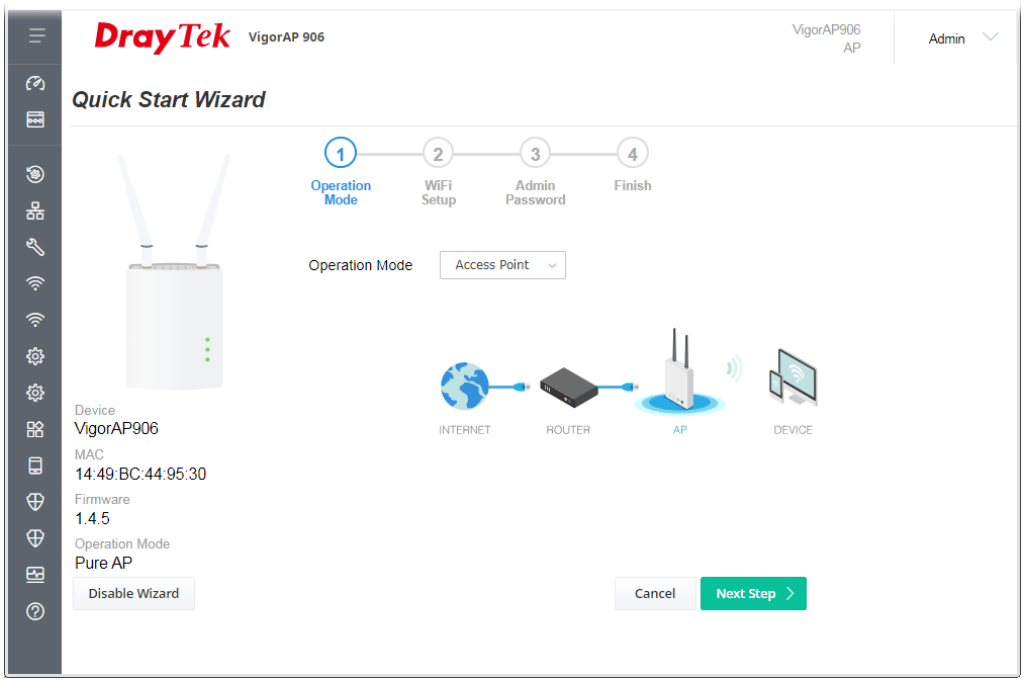


Note:

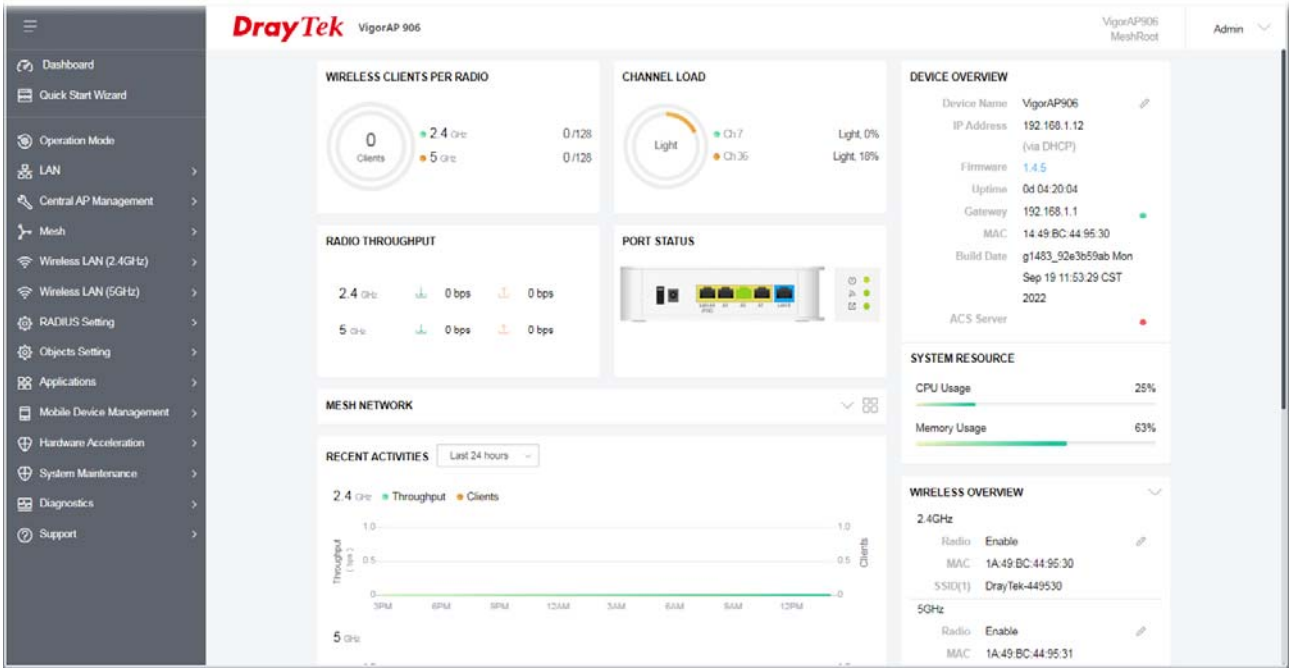
You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as **the IP address of VigorAP 906.**

- If there is no DHCP server on the network, then VigorAP 906 will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 906 will receive its 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.

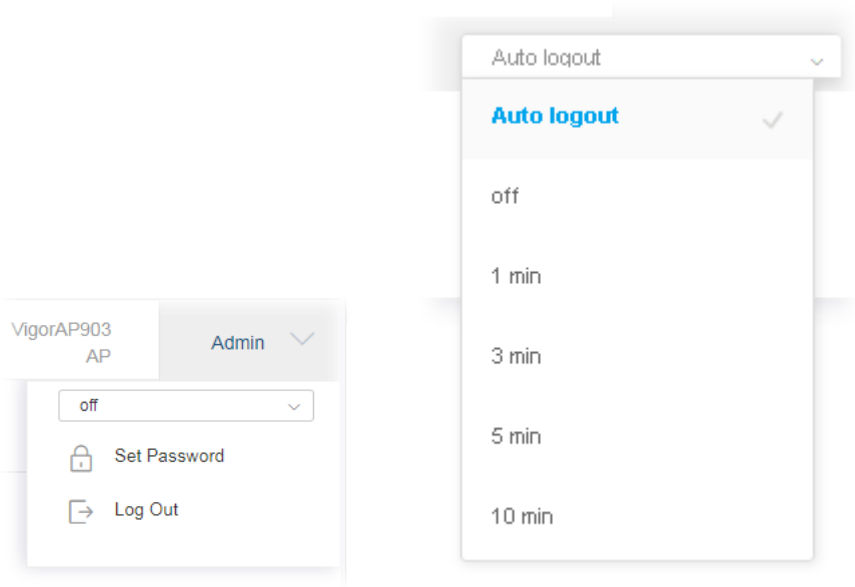
3. For the first time accessing VigorAP, the **Quick Start Wizard** for configuring wireless settings will appear as follows. Refer to *Section I-7 Quick Start Wizard for detailed information*.



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



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 log out after 5 minutes without any operation. Change the setting of auto-logout if you want.



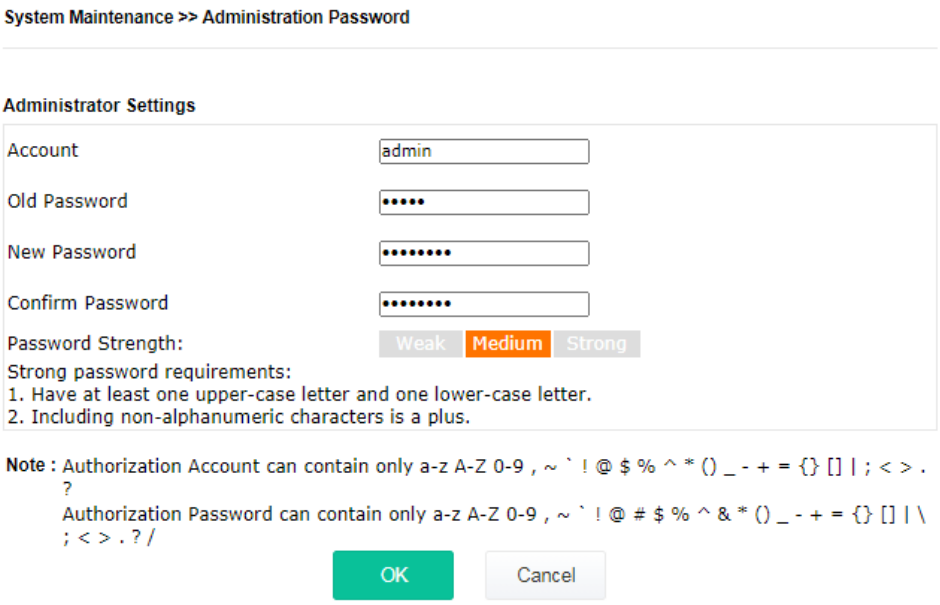
Note:

If you fail to access the web configuration, please go to the section “Trouble Shooting” for detecting and solving your problem.

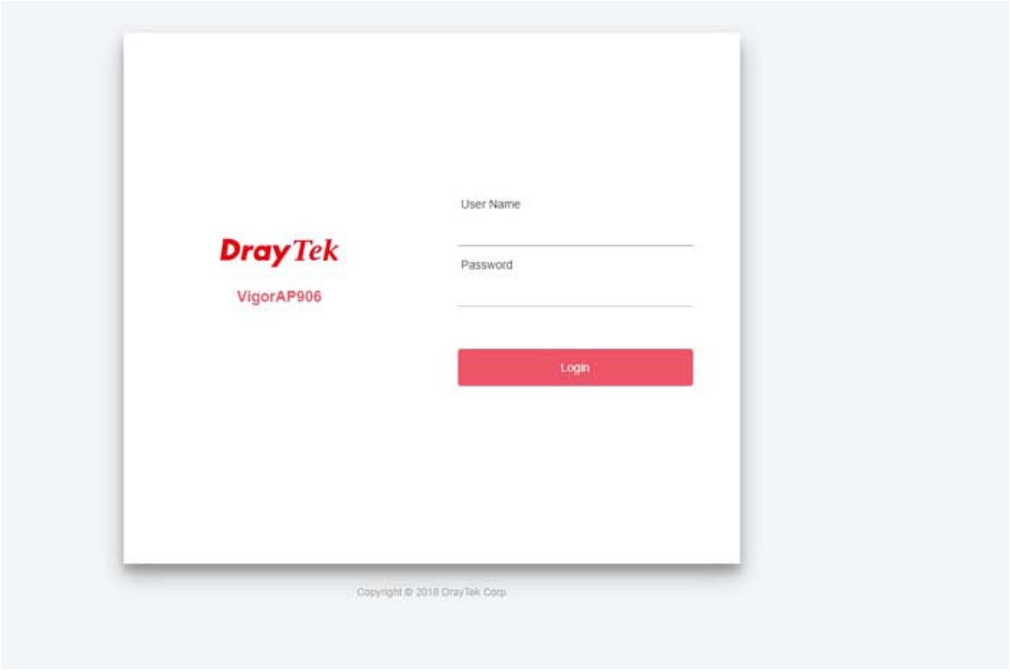
For using the device properly, it is necessary for you to change the password of the web configuration for security and adjust primary basic settings.

I-5 Changing Password

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



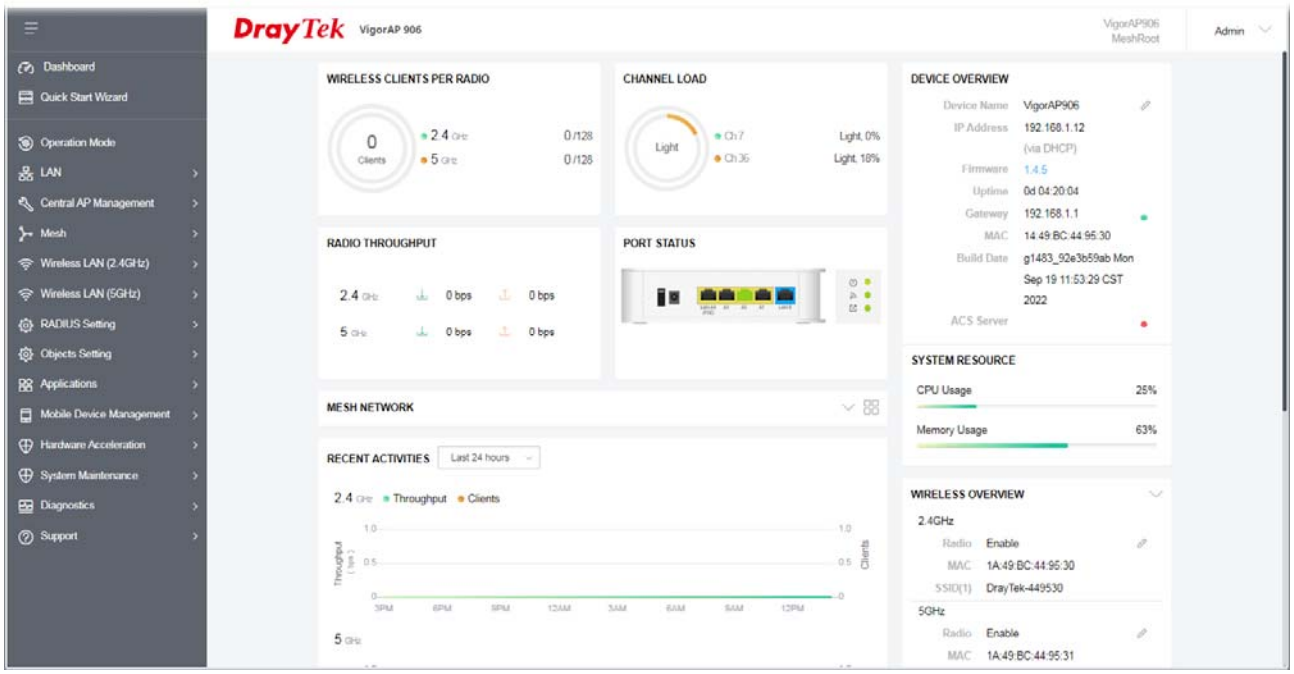
3. Enter the new login password on the field of **Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.



I-6 Dashboard

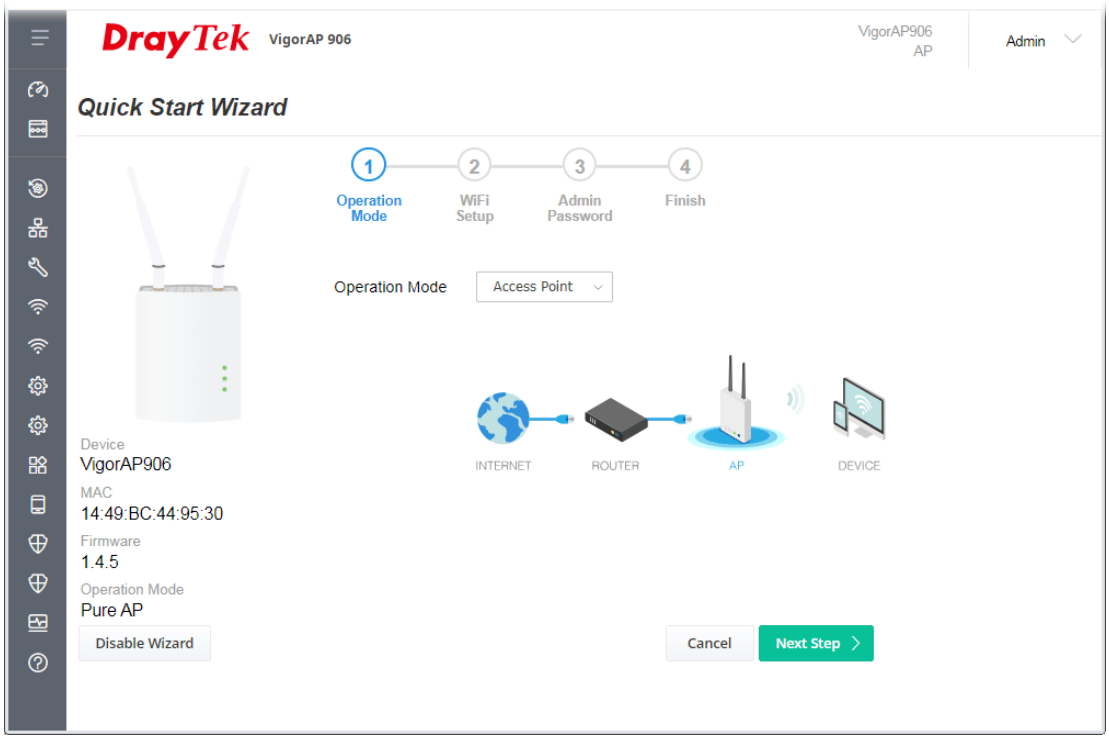
The dashboard shows system status including the number of clients connected, throughput, gateway, physical connection status, radio (2.4GHz / 5GHz) status, backhaul network, recent activities, wireless network usage, and so on.

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 the 2.4G wireless setting, 5G wireless setting, and other corresponding settings for Vigor Access Point step by step.



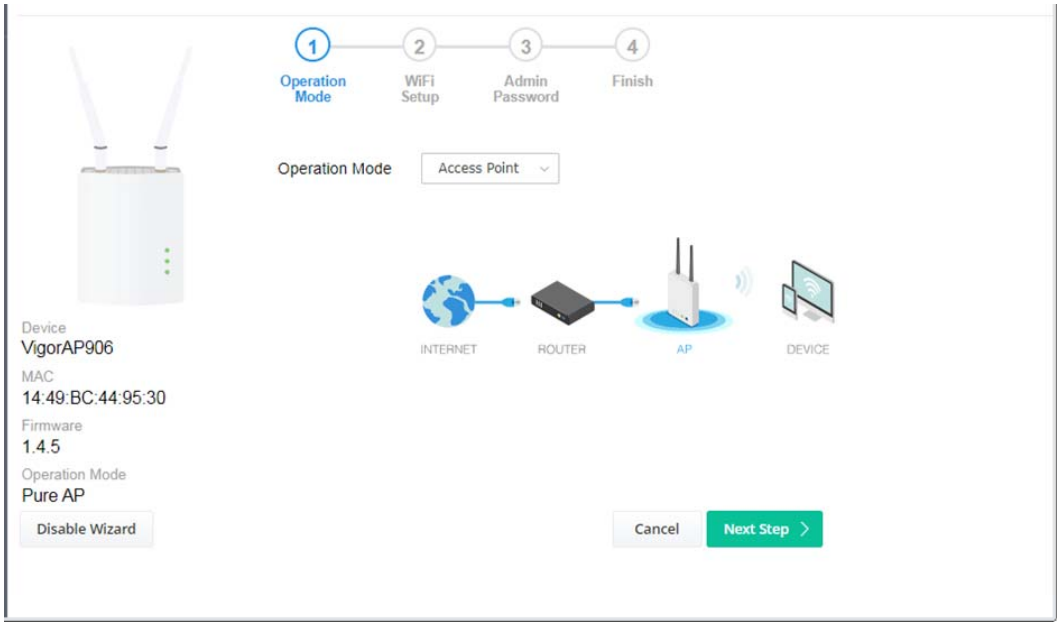
Available operation mode includes:

- Access Point
- Mesh Root
- Mesh Node

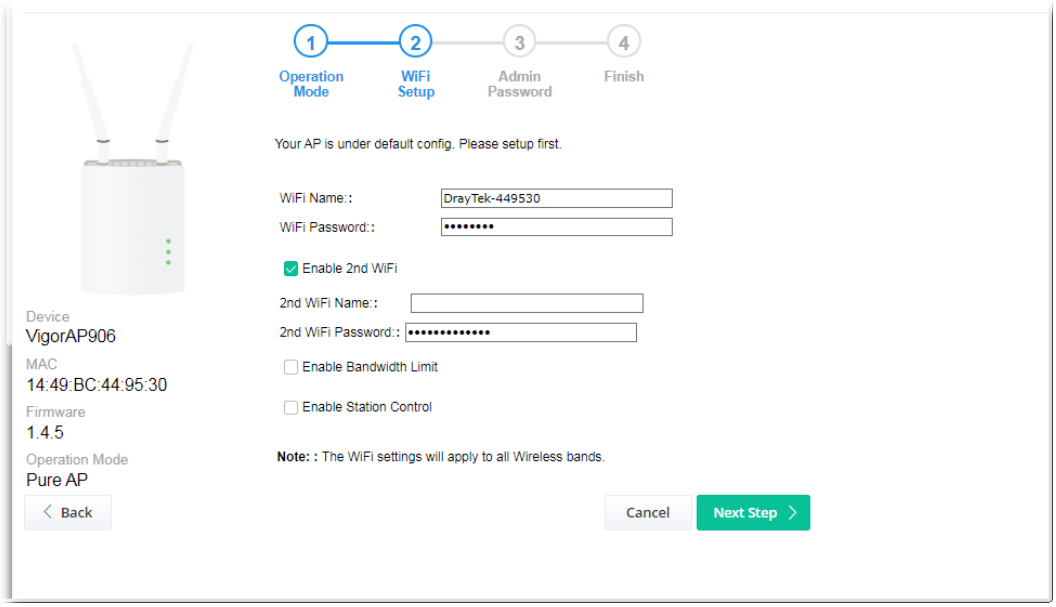
On this page, the advanced settings pages will vary according to the operation mode specified.

I-7-1 Settings for Access Point

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



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

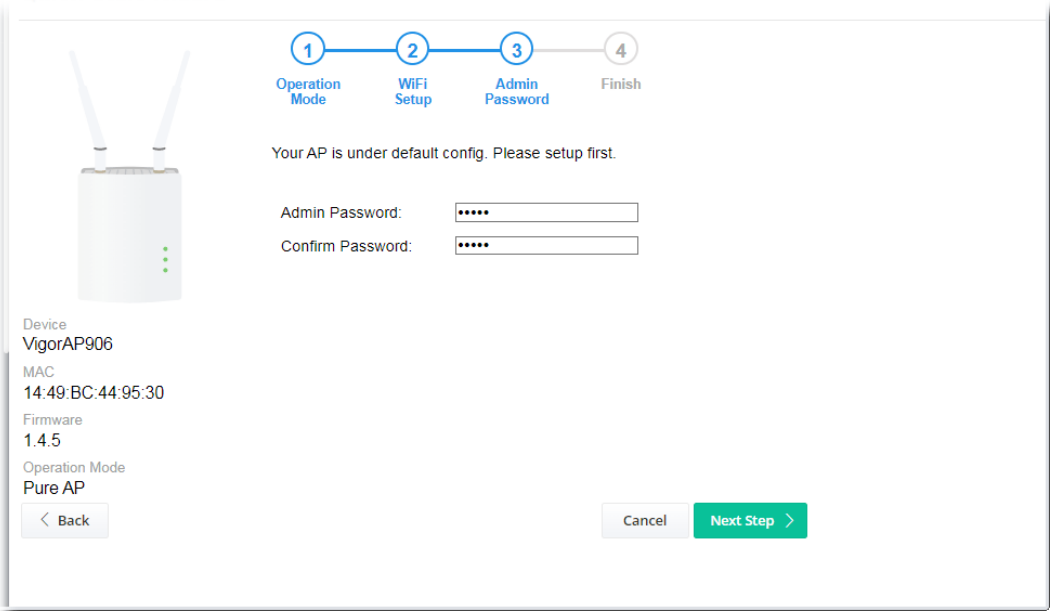


Available settings are explained as follows:

Item	Description
WiFi Name	Set a name for VigorAP 906 to be identified.
WiFi Password	Enter **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 a 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 906 which can be identified and connected by a wireless guest. **2nd WiFi Password -** Set **8~63** ASCII characters which can be used for logging into VigorAP 906 by a 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 the 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 the 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.

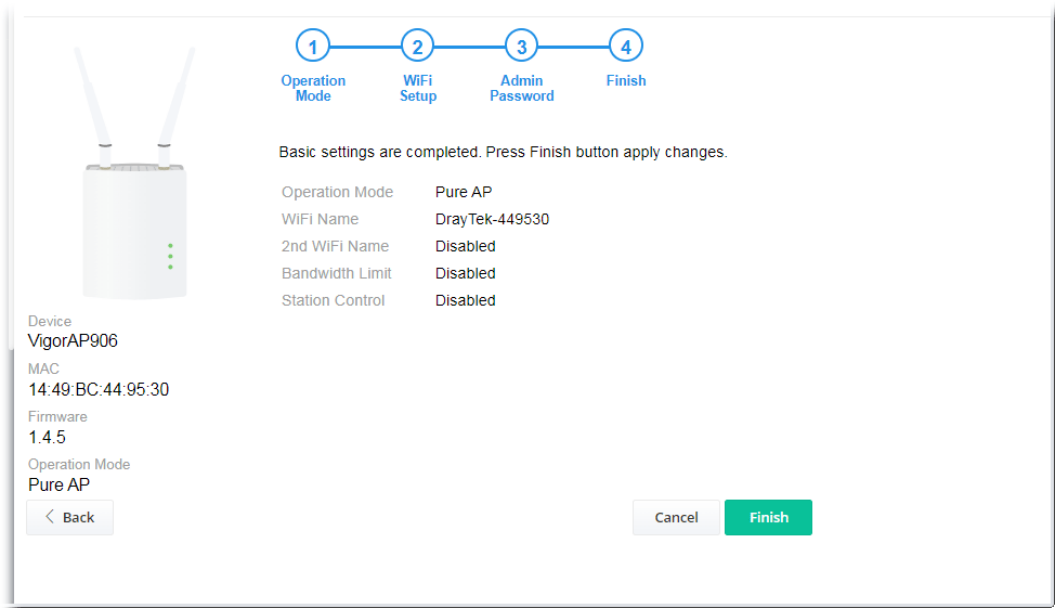
3. Change the default password for such a device with a new value. Then click **Next Step**.



Available settings are explained as follows:

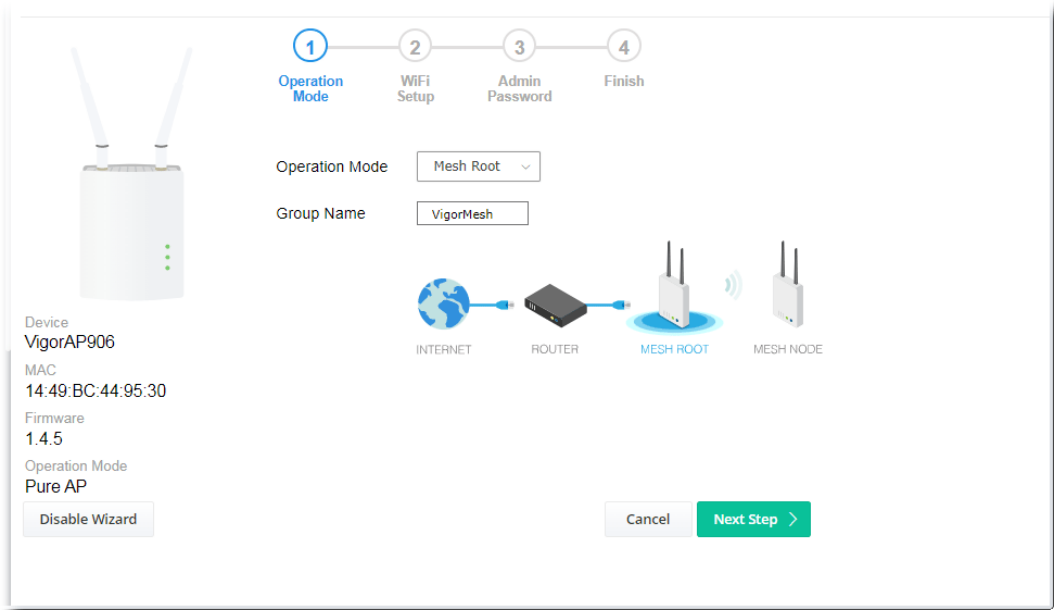
Item	Description
Admin Password	Enter a new password.
Confirm Password	Enter the new password again for confirmation.

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

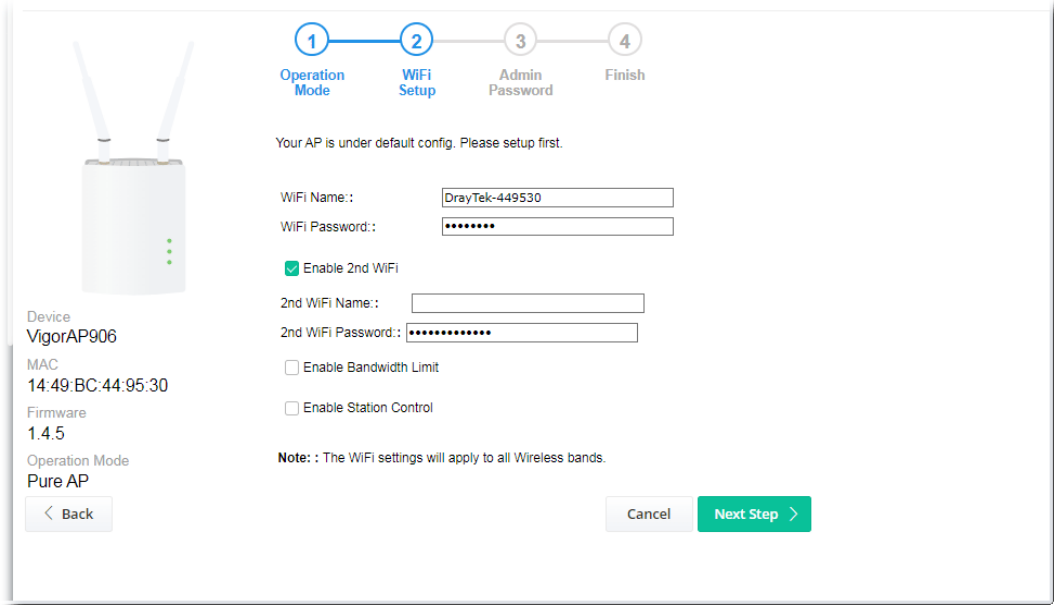


I-7-2 Settings for Mesh Root

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



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

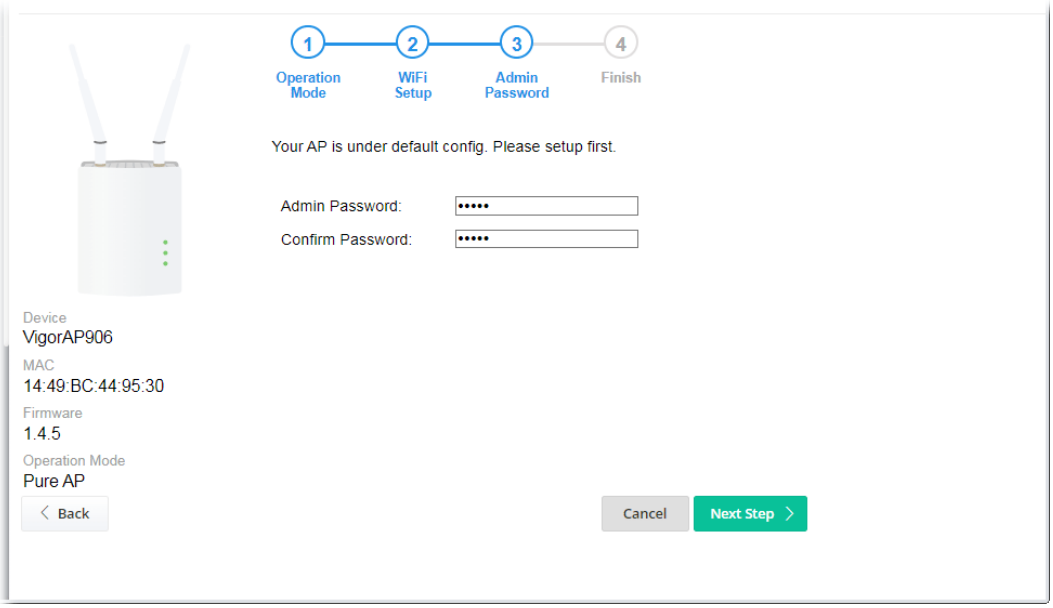


Available settings are explained as follows:

Item	Description
WiFi Name	Set a name for VigorAP 906 to be identified.
WiFi Password	Enter **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 a 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 906 which can be identified and connected by a wireless guest. **2nd WiFi Password -** Set **8~63** ASCII characters or **8~63** ASCII characters which can be used for logging into VigorAP 906 by a 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 the 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 the 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.

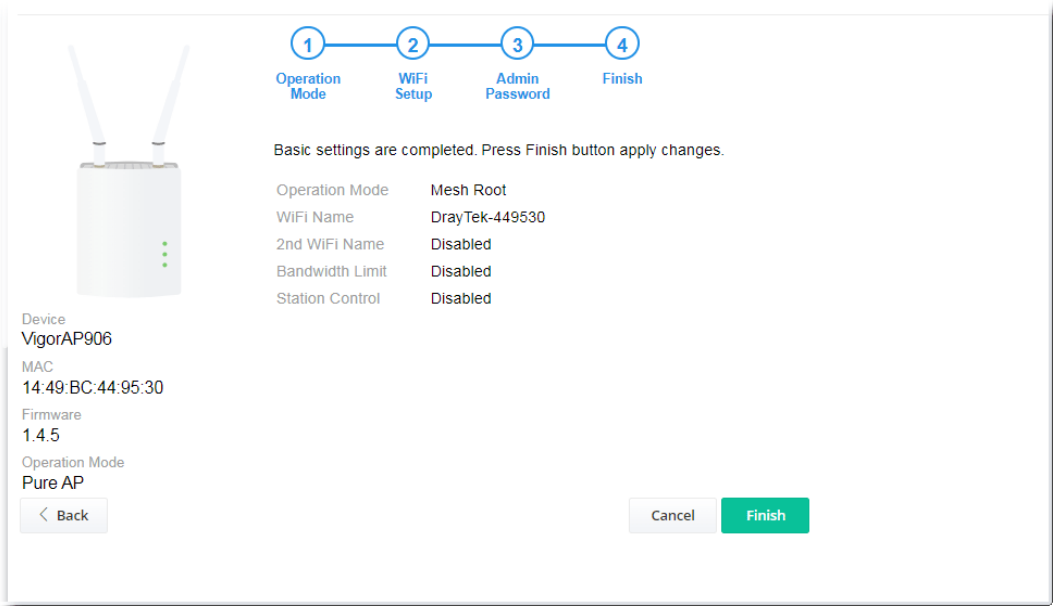
3. Change the default password for such a device with a new value. Then click **Next Step**.



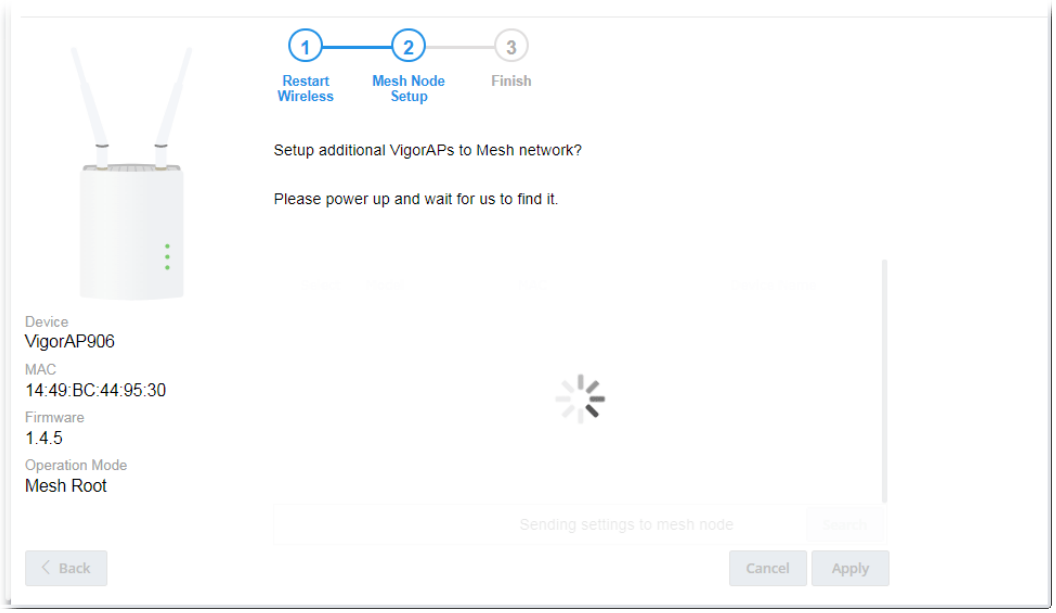
Available settings are explained as follows:

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

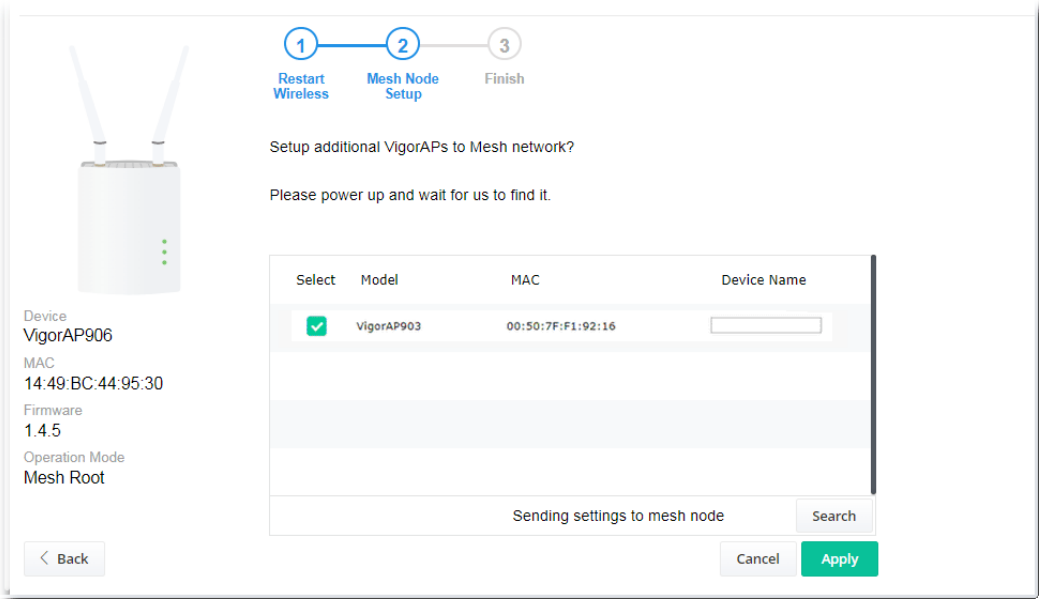
4. A summary of the settings configuration will be shown on the screen. Click **Finish**.



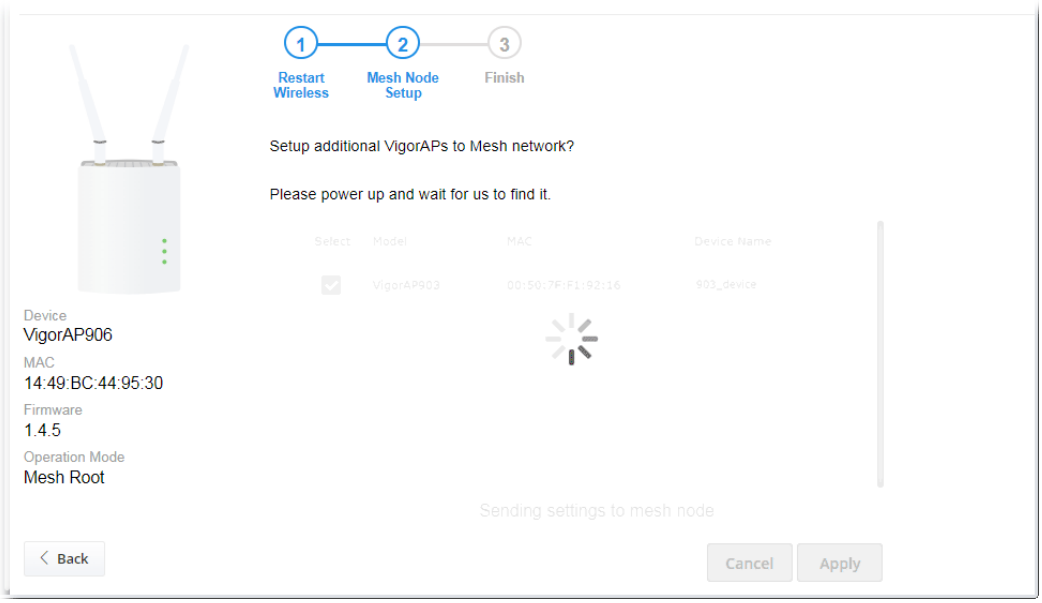
5. After clicking **Finish**, the following web page appears. VigorAP will search for mesh nodes around the network.



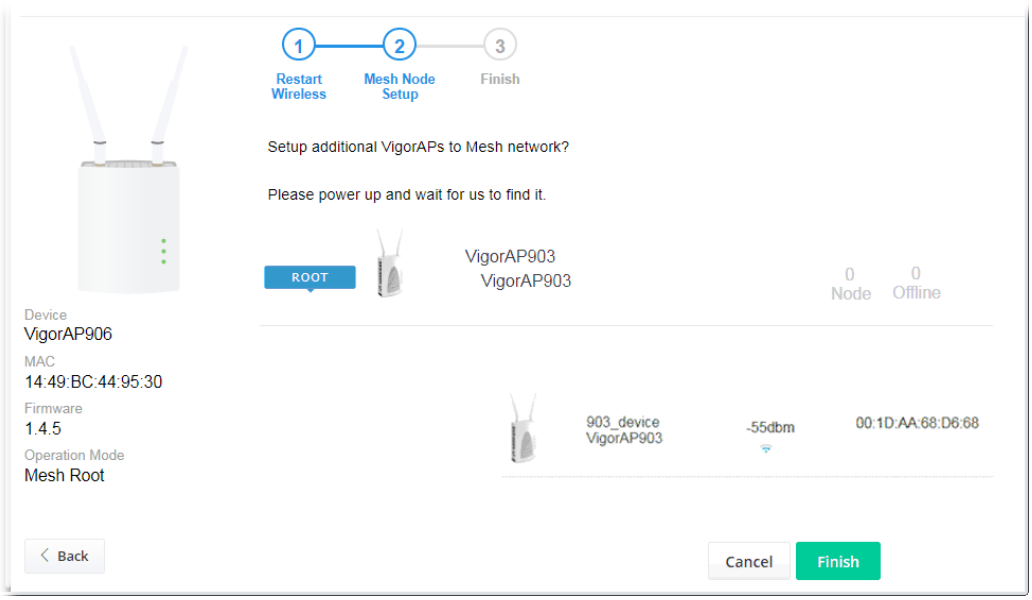
6. Available VigorAP devices will be shown on the screen. Select the device (as a mesh node) for grouping under such mesh group and enter a device name for identification.



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

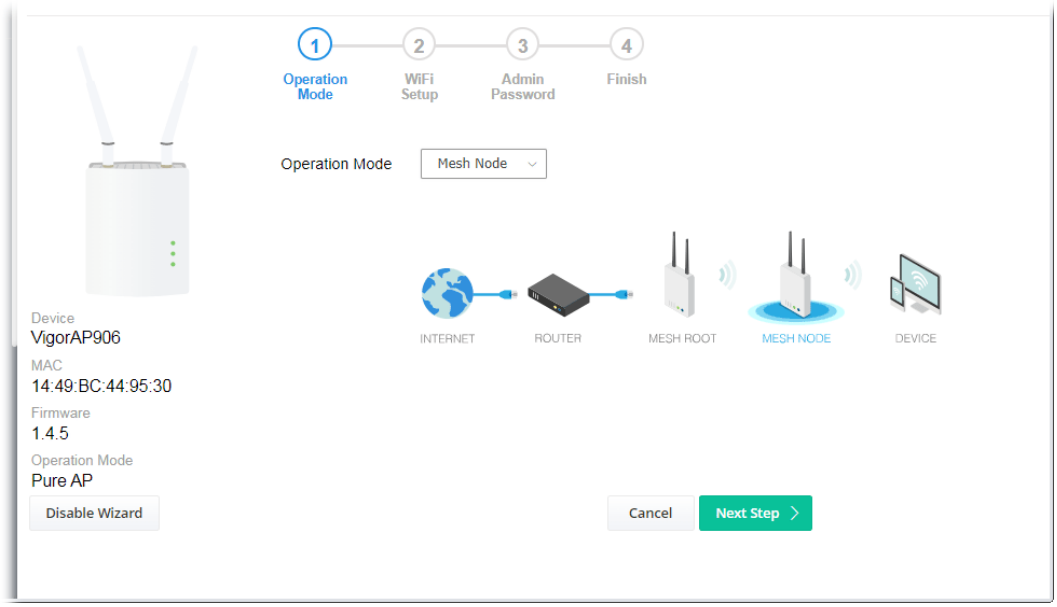


8. Later, a summary page of mesh root with mesh node will be shown on the screen.

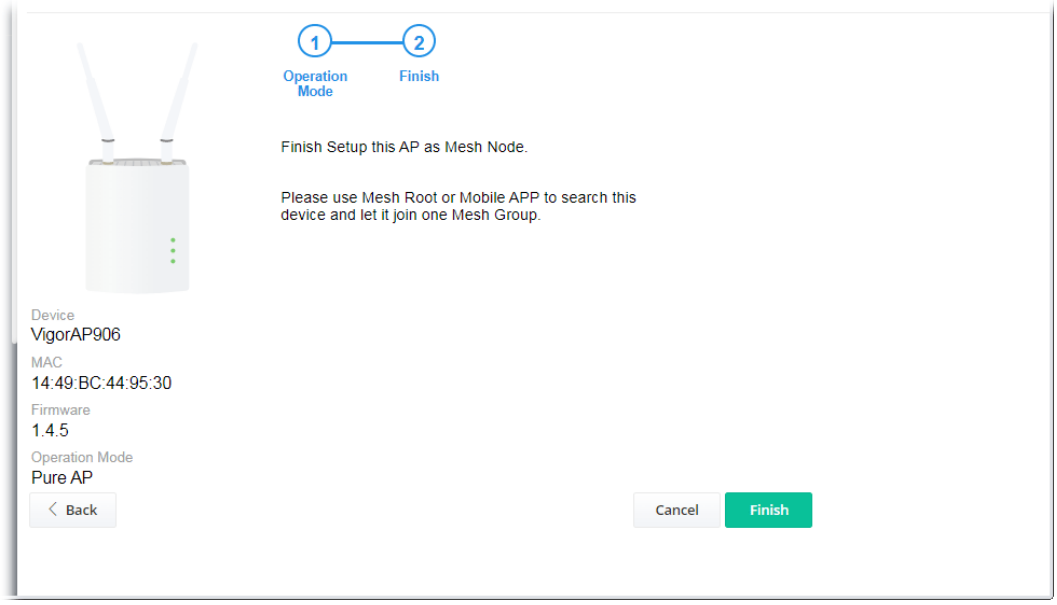


I-7-3 Settings for Mesh Node

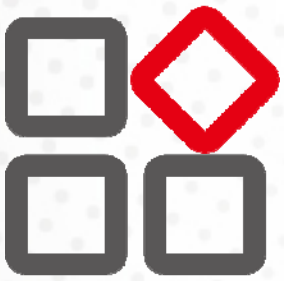
1. Choose **Mesh Node** as the operation mode and click **Next Step**.



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

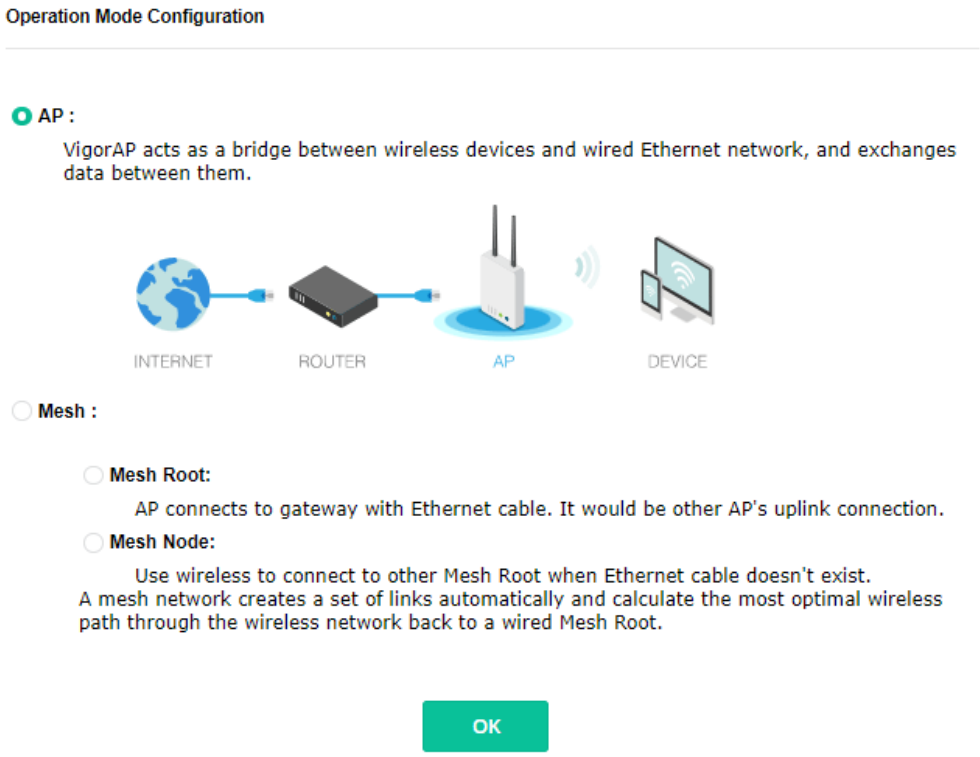


Chapter II Connectivity



II-1 Operation Mode

This page provides several available modes for you to choose from for different conditions. Click any one of them and click **OK**. The system will configure the required settings automatically.



Available settings are explained as follows:

Item	Description
AP	This mode allows wireless clients to connect to the 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 roots via the 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.

Note:

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

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

VigorAP 906 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 906 can support data rates up to 867 MBps in 802.11ac 80 MHz channels.

Note:

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

VigorAP 906 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 906. 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, the access point will previously set 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 the 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 906 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 the easy procedure to make a network connection between the wireless station and wireless access point (VigorAP 906) with the encryption of WPA and WPA2.

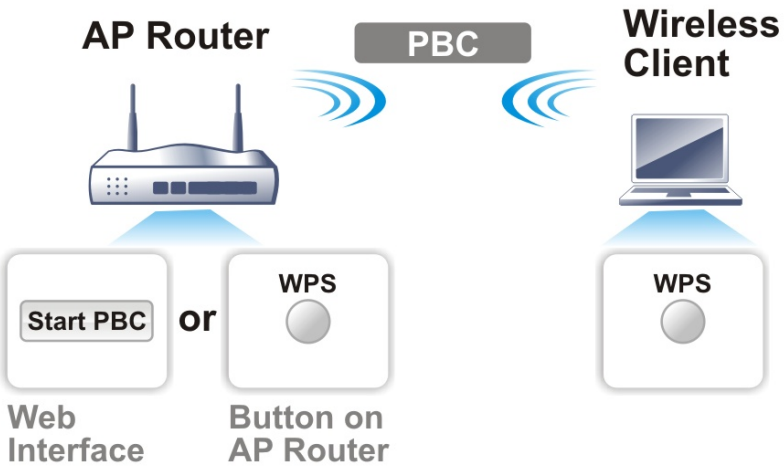
It is the simplest way to build a connection between wireless network clients and VigorAP 906. Users do not need to select any encryption mode and type any long encryption passphrase to set up a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 906 automatically.

Note:

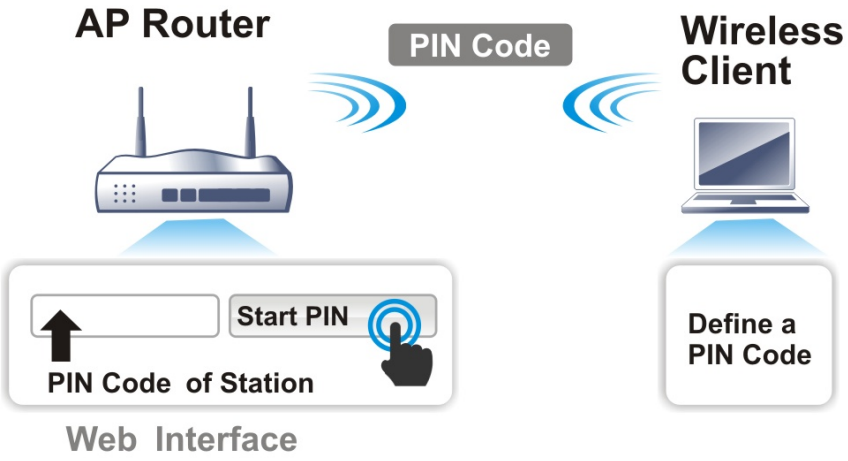
Such function is available for the wireless station with WPS supported.

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

On the side of the VigorAP 906 series which served as an AP, press **the WPS** button once on the front panel of VigorAP 906 or click **Start PBC** on the web configuration interface. On the side of a station with a network card installed, press **the Start PBC** button of a network card.

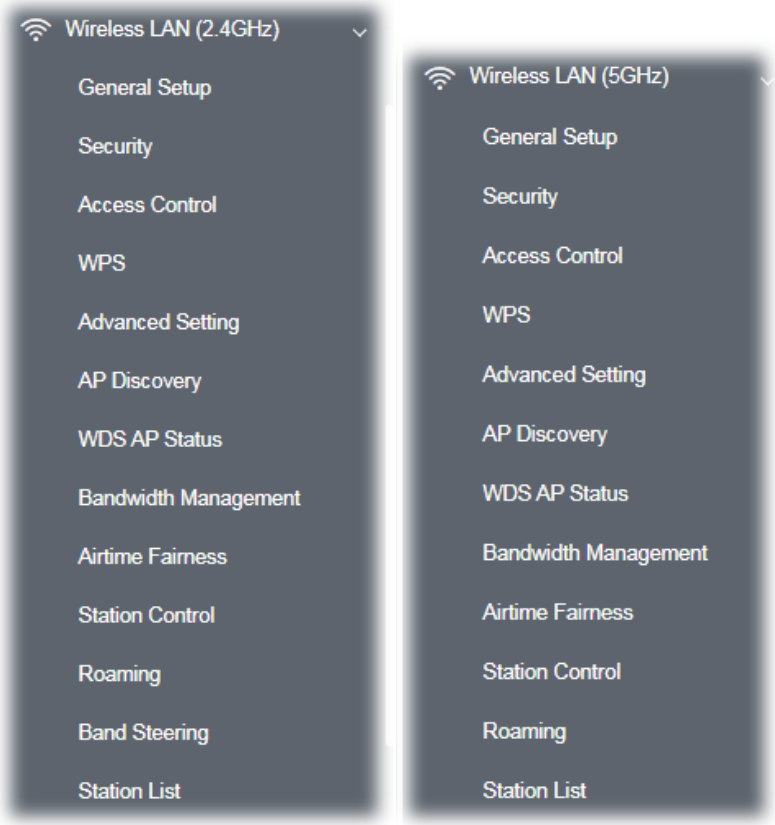


If you want to use a PIN code, you have to know the PIN code specified in the wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 906.


AP Router
PIN Code
Wireless Client
Start PIN
PIN Code of Station
Define a PIN Code
Web Interface

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

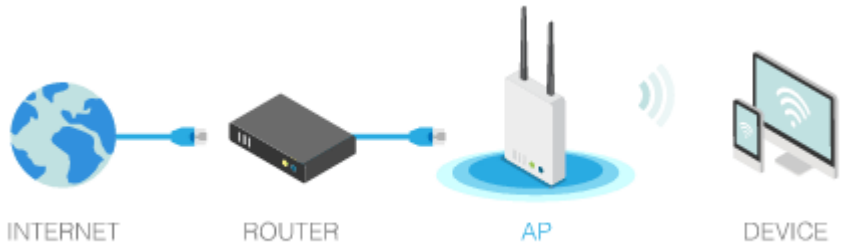
When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering, and Station List.



Note:

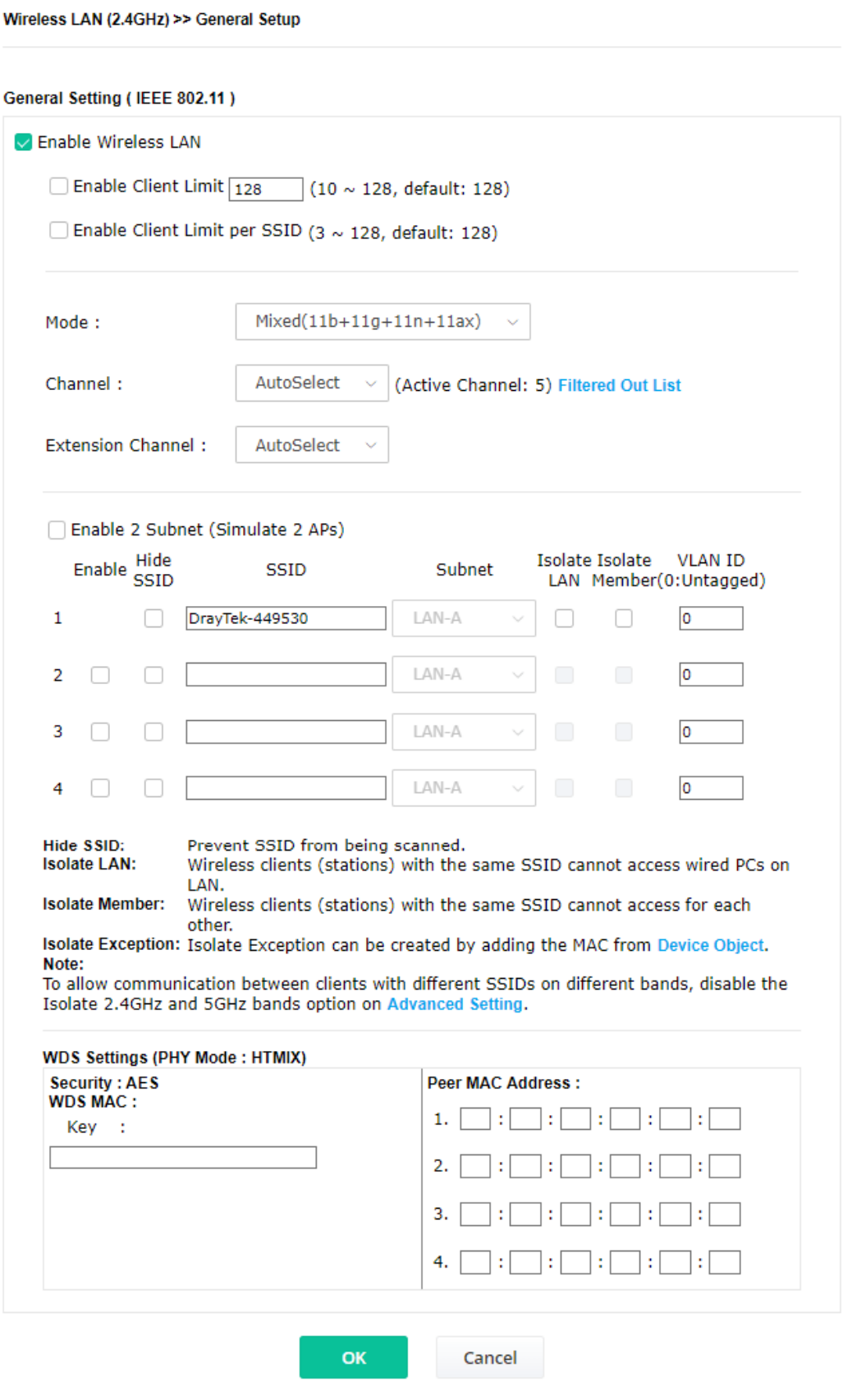
Available settings for **Wireless LAN (2.4GHz) and Wireless LAN (5GHz)** are almost the same, except for Band Steering.

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

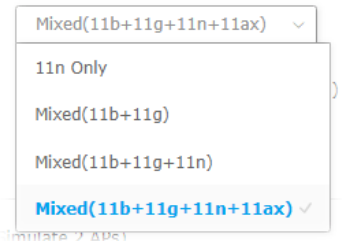


II-3-1 General Setup

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



Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable the wireless function.
Enable Client Limit	Check the box to set the maximum number of wireless stations which try to connect the Internet through the Vigor device. The number you can set is from 3 to 64.
Enable Client Limit per SSID	Define the maximum number of wireless stations per SSID which try to connect to the Internet through the Vigor device. The number you can set is from 3 to 64.
Mode	At present, VigorAP 906 can connect to 11n only, 11a only, 11n only (5G), Mixed (11b+11g), Mixed (11b+11g+11n) and Mixed (11b+11g+11n+11ax) stations simultaneously. Simply choose Mixed (11b+11g+11n+11ax) mode.  (2.4 GHz) (5GHz)
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let the system determine for you.
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above. Configure the extension channel you want.
Enable 2 Subnet (Simulate 2 APs)	Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such a mechanism can make you feel that you have two independent AP/subnet functions in one VigorAP 906. If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.
Hide SSID	Check it to prevent wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except for

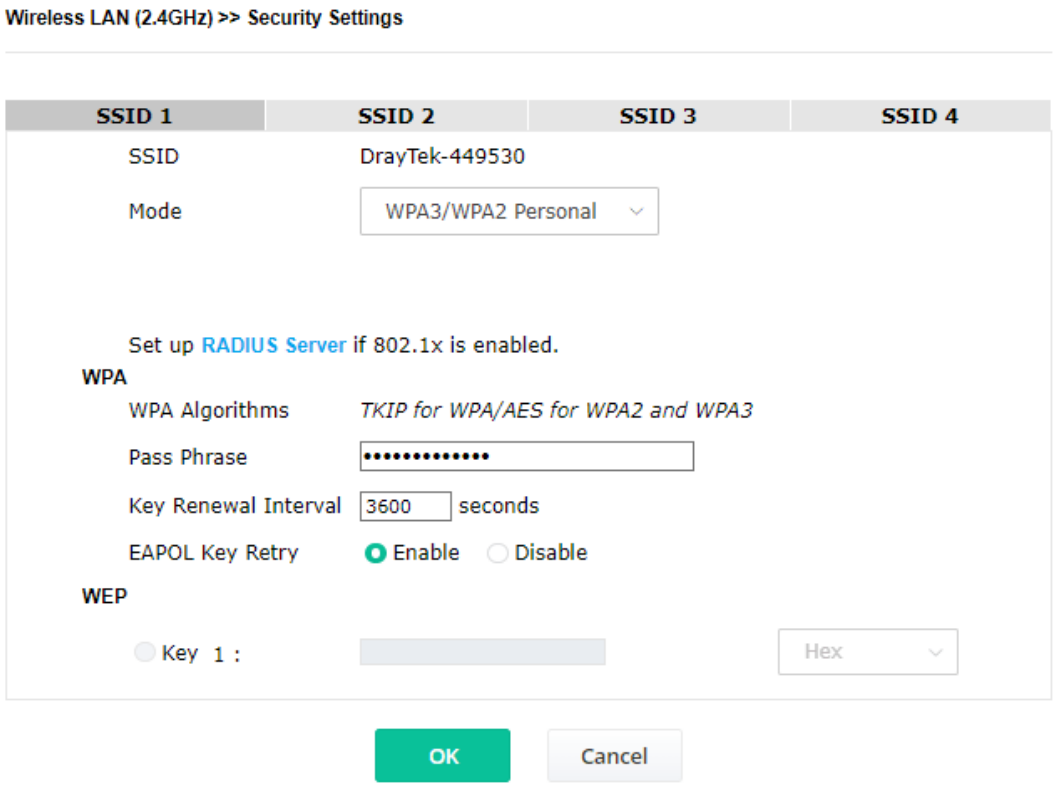
	SSID or just cannot see anything about VigorAP 906 while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 906 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When **Enable 2 Subnet** is enabled, you can specify the 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.
Isolate LAN	Check this box to make the LAN clients not access each other.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not access each other.
VLAN ID	Enter 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 set up to the same **Phy Mode** for connecting with each other.
Peer MAC Address	Enter the peer MAC address for the access point that VigorAP 906 connects to.

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

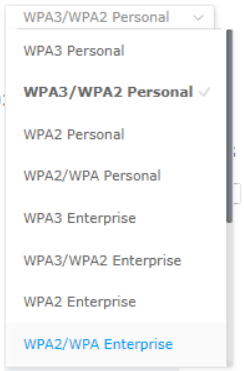
II-3-2 Security

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

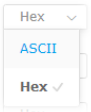
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.



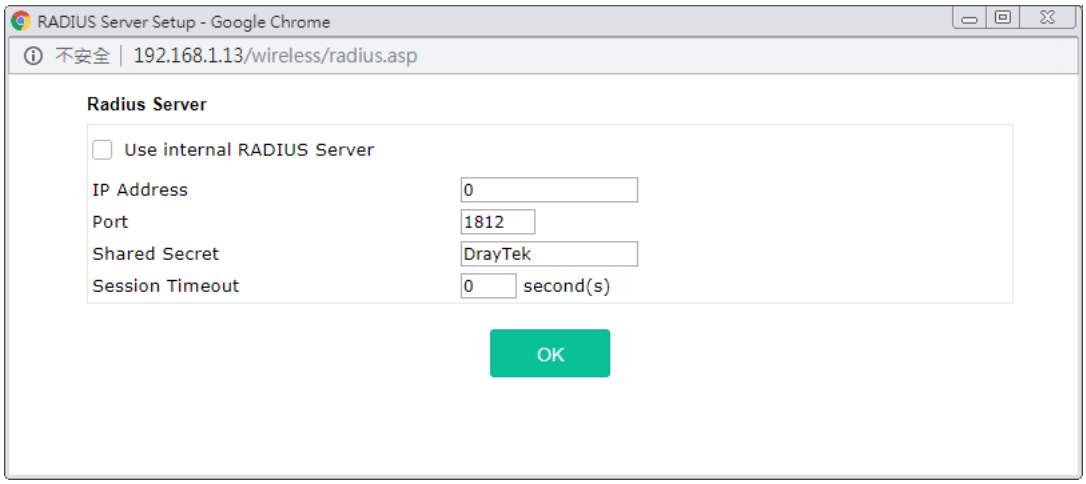
Available settings are explained as follows:

Item	Description
Mode 	There are several modes provided for you to choose from. Below shows the modes with higher security: ● **WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal -** Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. 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. ● **WPA3 Enterprise, WPA3/WPA2 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. ● **WPA2 Enterprise -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key)

	entered manually in this field below or automatically negotiated via 802.1x authentication. • **OWE** - WPA3 also introduces a new open and secure connection mode; "Opportunistic Wireless Encryption" (OWE). It allows the clients to connect without a password, ideal for hotspot networks, but the connection between each individual client is uniquely encrypted behind the scenes. Below shows the modes with basic security: • **WPA Personal** - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. • **WPA Enterprise** - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. • **WEP Personal** - Accepts only WEP clients and the encryption key should be entered in WEP Key. • **None** - The encryption mechanism is turned off.
WPA Algorithms	This feature is available for **WPA3 Enterprise, WPA2 Enterprise, WPA Enterprise, WPA3 Personal, WPA2 Personal, WPA Personal, WPA3/WPA2 Personal, or WPA2/WPA Personal** mode. Select TKIP, AES, or TKIP/AES as the algorithm for WPA. Note that not all modes of Vigor router support WPA3 mode. However, if the Vigor router supports WPA3 Personal/Enterprise security mode, the WPA algorithms will be set as AES.
Pass Phrase	Enter **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). This feature is available for **WPA Personal or WPA2 Personal or WPA2 / WPA Personal** mode, **WPA3 Personal** or **WPA3/WPA2 Personal**.
Key Renewal Interval	WPA uses a shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for **WPA3 Enterprise, WPA2 Enterprise, WPA Enterprise, WPA3 Personal, WPA2 Personal, WPA Personal, WPA3/WPA2 Enterprise, WPA2/WPA Enterprise, WPA3/WPA2 Personal,** or **WPA2/WPA Personal** mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Click **Enable** to make sure that the key will be installed and used once to prevent a key reinstallation attack.
Key 1	The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for **WEP Personal** mode.

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



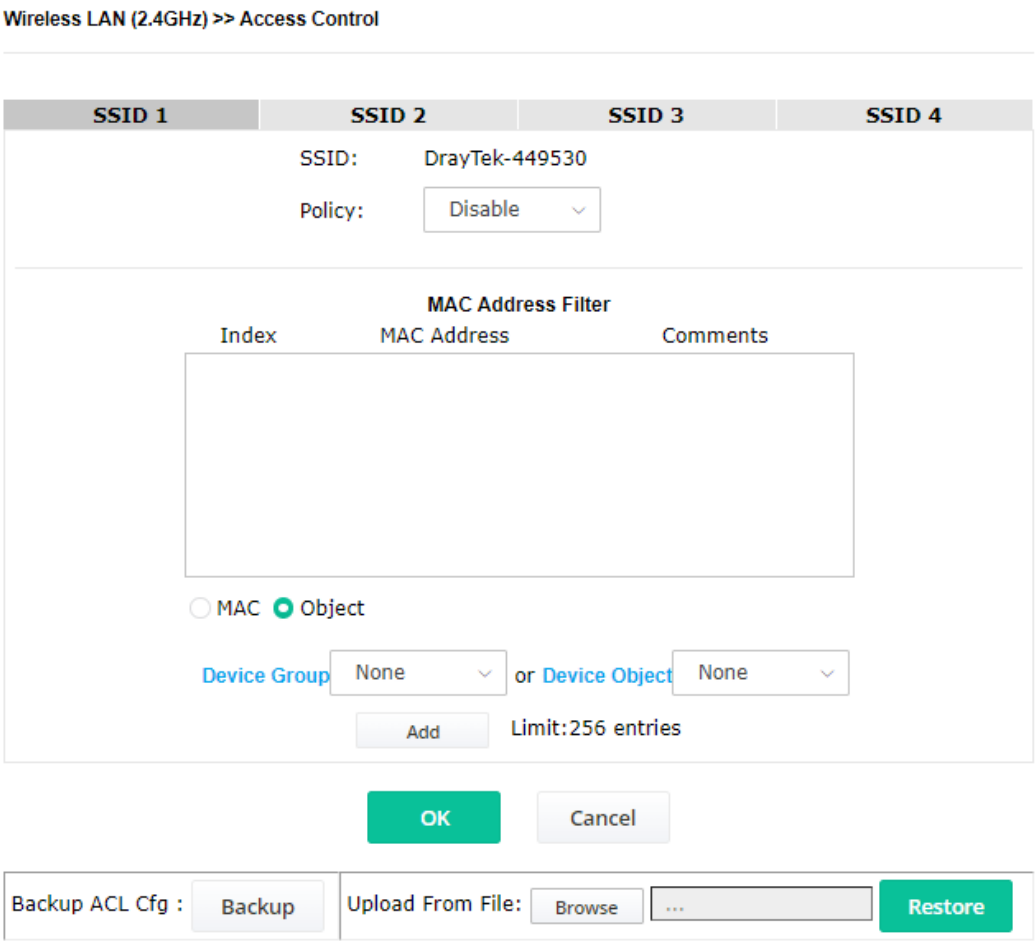
Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 906 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 906.
IP Address	Enter the IP address of the external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has been completed. (The unit is second.)

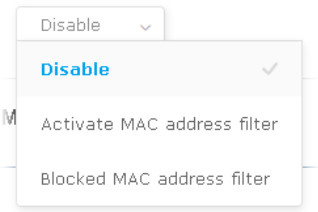
After finishing this web page configuration, please click **OK** to save the settings.

II-3-3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of the 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).



Available settings are explained as follows:

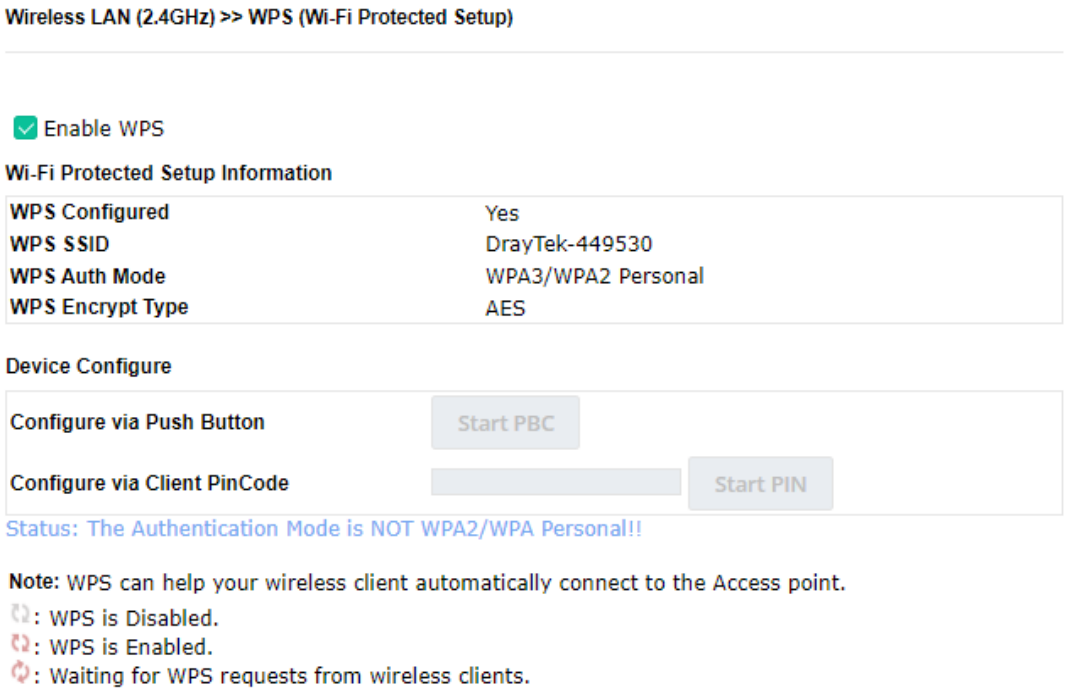
Item	Description
Policy	Select to enable any one of the following policies or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 906. 

MAC Address Filter	Display all MAC addresses that are edited before.
MAC	**Client's MAC Address -** Manually enter the MAC address of the wireless client. **Add -** Add a new MAC address to 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 objects and click **Add**. The MAC address of the device will be shown on the MAC Address Filter table.
Cancel	Give up the access control set up.
Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

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

II-3-4 WPS

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



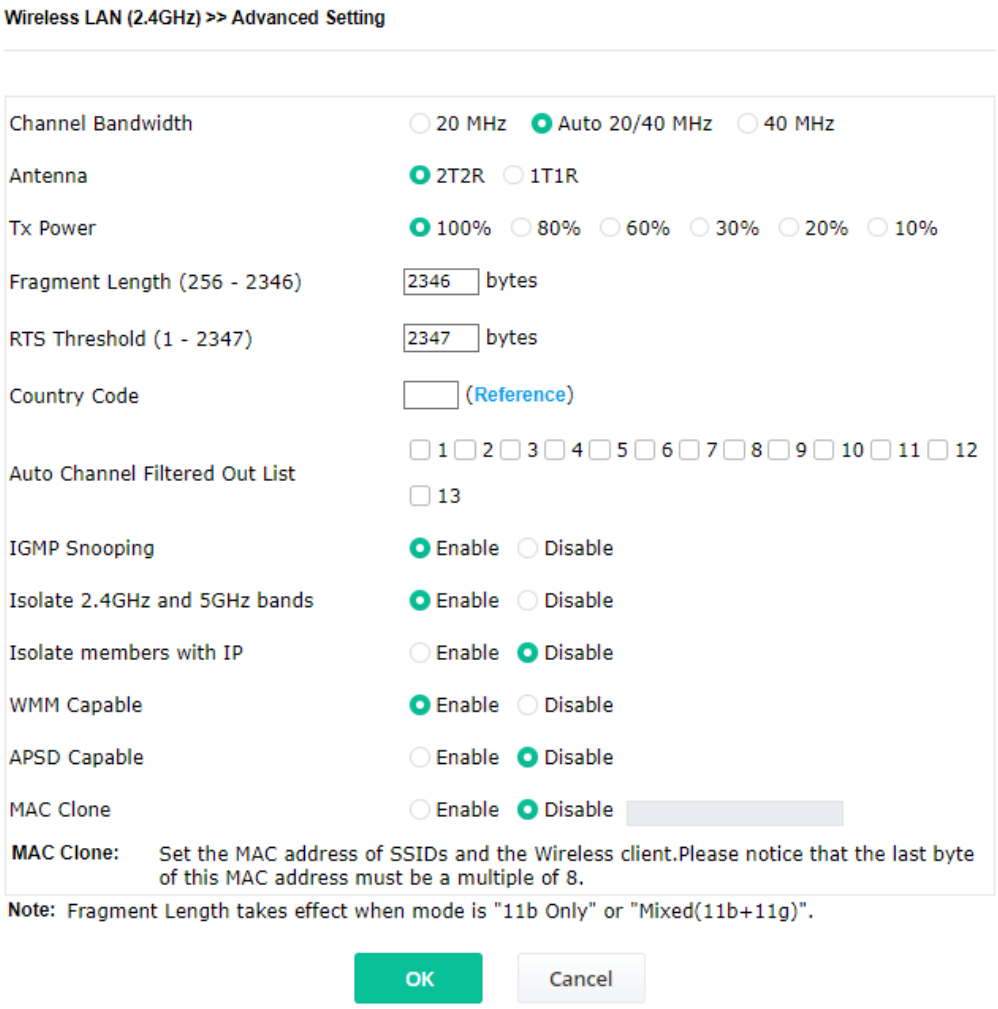
Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable the WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security

	(encryption) function of VigorAP 906 is properly configured, you can see the 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 906. Only WPA2 Personal and WPA Personal support WPS.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 906.
Configure via Push Button	Click **Start PBC** to invoke the Push-Button style WPS setup procedure. VigorAP 906 will wait for WPS requests from wireless clients for about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 906 will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to set up WPS within two minutes)
Configure via Client PinCode	Enter the PIN code specified in the wireless client you wish to connect with and click **the Start PIN** button. Both ACT and 2.4G WLAN LEDs on VigorAP 906 will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to set up WPS within two minutes).

II-3-5 Advanced Setting

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



Available settings are explained as follows:

Item	Description
Channel Bandwidth	**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 a 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 the range and throughput of wireless.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify the default value if you don't know what it is. The 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 the default value if you don't know what it is. The 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, the wireless station will be warned and is unable to make a network connection. Therefore, changing the country code to ensure a successful network connection will be necessary for some clients.
Auto Channel Filtered Out List	The selected wireless channels will be discarded if **AutoSelect** is selected as **Channel** selection mode in **Wireless LAN>>General Setup**.
IGMP Snooping	Click **Enable** to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Isolate 2.4GHz and 5GHz bands	The default setting is "Enable". It means that the wireless client using the 2.4GHz band is unable to connect to the wireless client with the 5GHz band, and vice versa. For WLAN 2.4GHz and 5GHz set with the same SSID name: • No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if **Isolate Member** (in **Wireless LAN>>General Setup**) is NOT enabled for such SSID. • Yet, if the function of **Isolate Member** (in **Wireless LAN>>General Setup**) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.

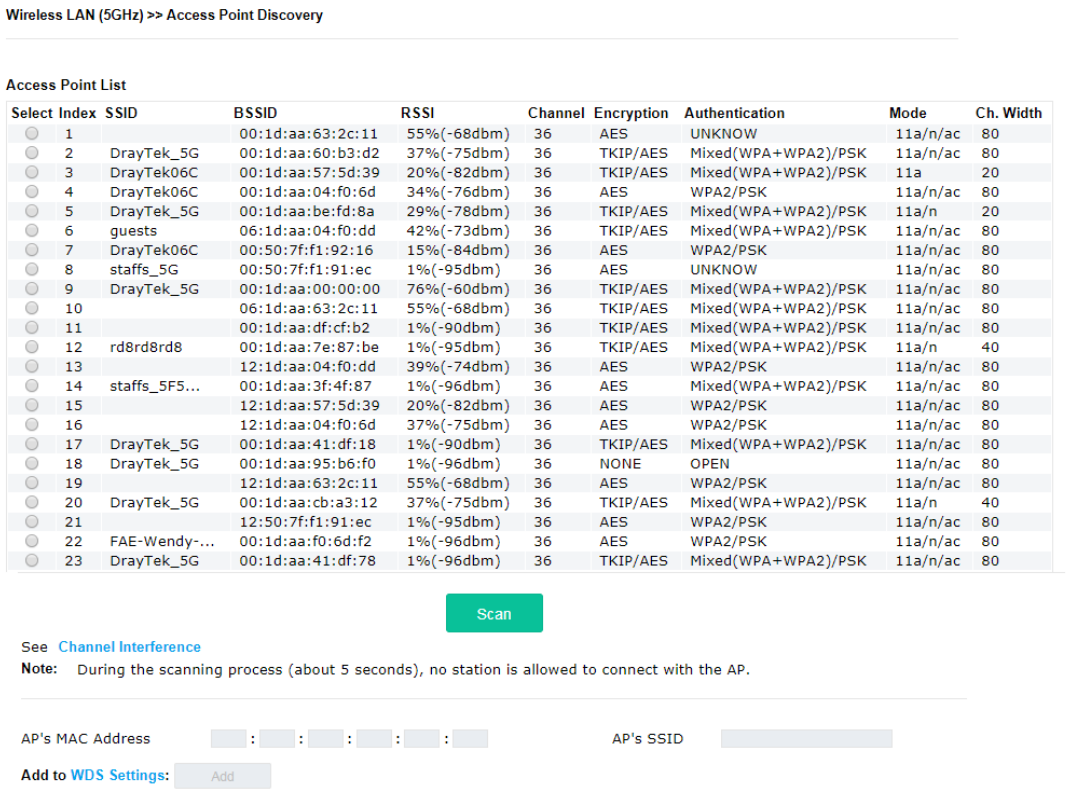
Isolate members with IP	The default setting is “Disable”. If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
APSD Capable	APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows 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 **(for 2.4GHz only)**	Click **Enable** and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.

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

II-3-6 AP Discovery

VigorAP 906 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.



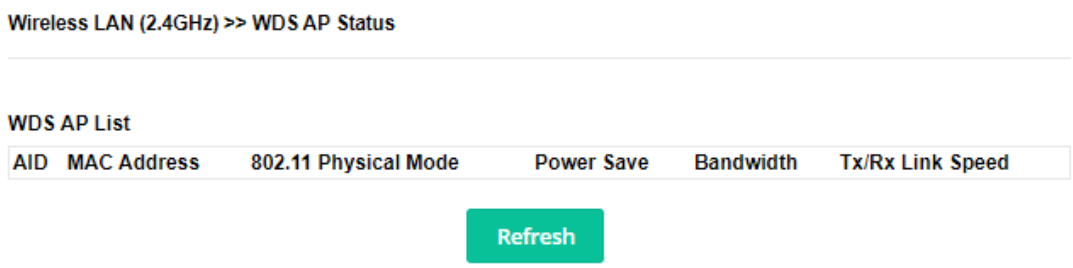
Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 906.
BSSID	Display the MAC address of the AP scanned by VigorAP 906.
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 906.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Mode	Display the wireless connection mode that the scanned AP used.
Ch. Width	Display the channel width that the scanned AP used.
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 /	Display the MAC address and SSID of the AP selected from the Access

AP's SSID	Point.
Add	Click it to add the AP selected from the Access Point List (with the same channel width) to the WDS Settings as peer's setting.

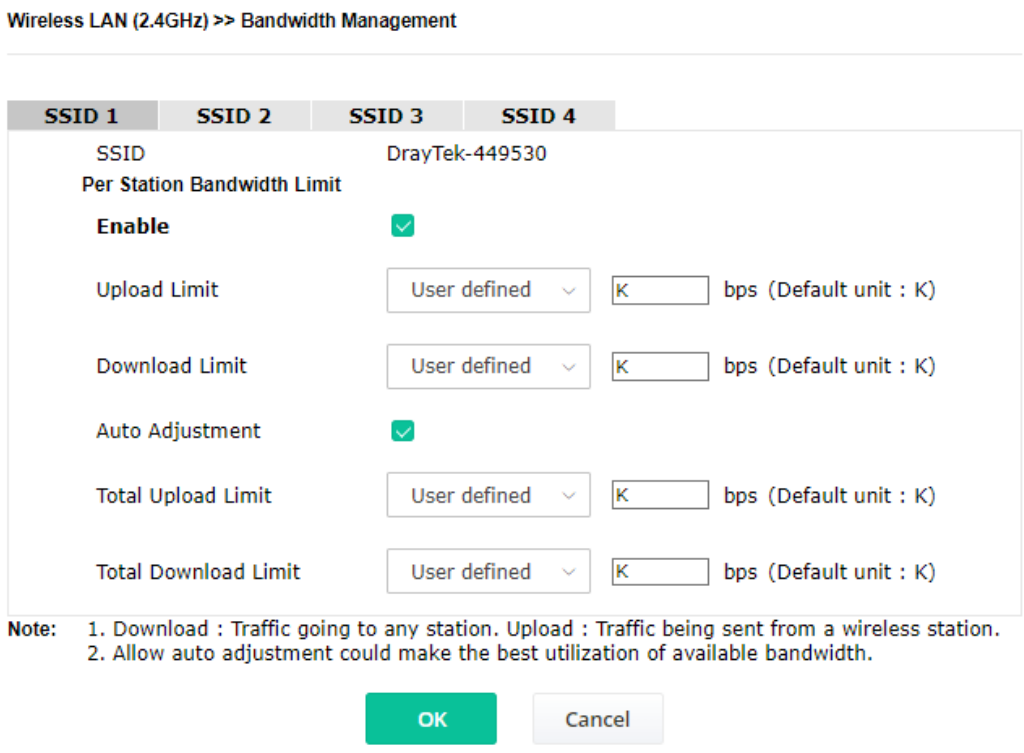
II-3-7 WDS AP Status

VigorAP 906 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.



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.



Available settings are explained as follows:

Item	Description
SSID	Display the specific SSID name.

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

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

II-3-9 Airtime Fairness

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

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

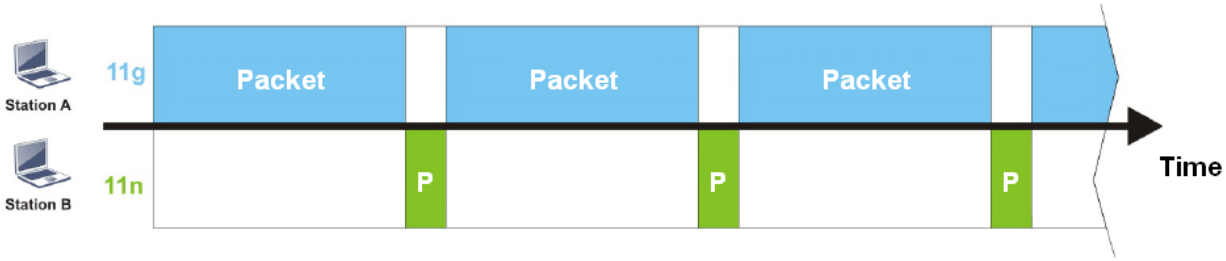
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

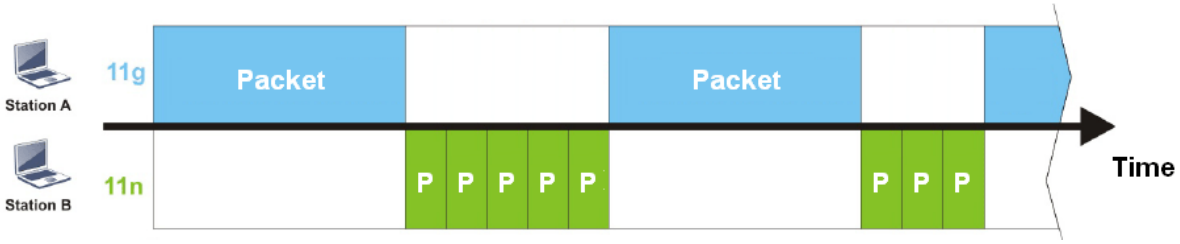
The principle behind the IEEE802.11 channel access mechanisms is that each station has ***an equal probability*** to access the channel. When wireless stations have similar data rates, this principle leads to a fair result. In this case, stations get a similar channel access time which is called airtime.

However, when stations have various data rates (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 906. Although they have an equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends a 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 906. 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 a higher probability to send data packets than Station A(11g). In this way, Station B(fast rate) gets fair airtime and its speed is not limited by Station A(slow rate).



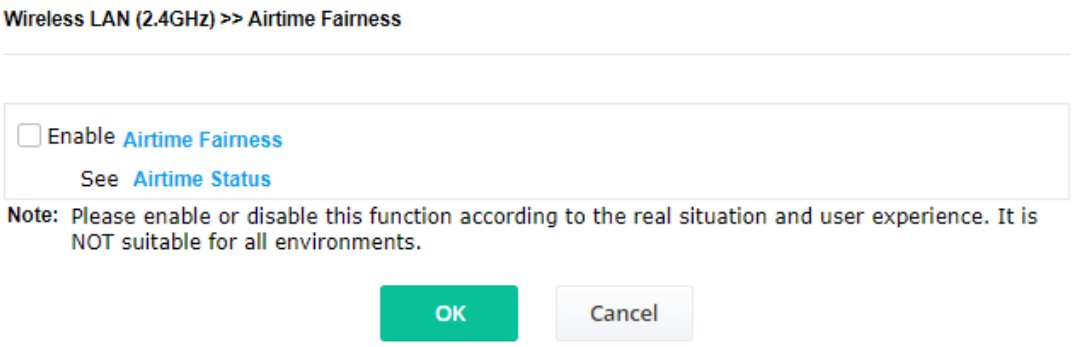
It is similar to the automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on the instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together because they all use 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.

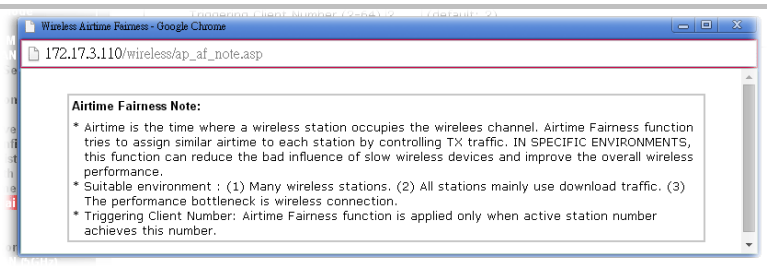
(2) All stations mainly use download traffic.

(3) The performance bottleneck is the wireless connection.



Available settings are explained as follows:

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



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

Note:

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

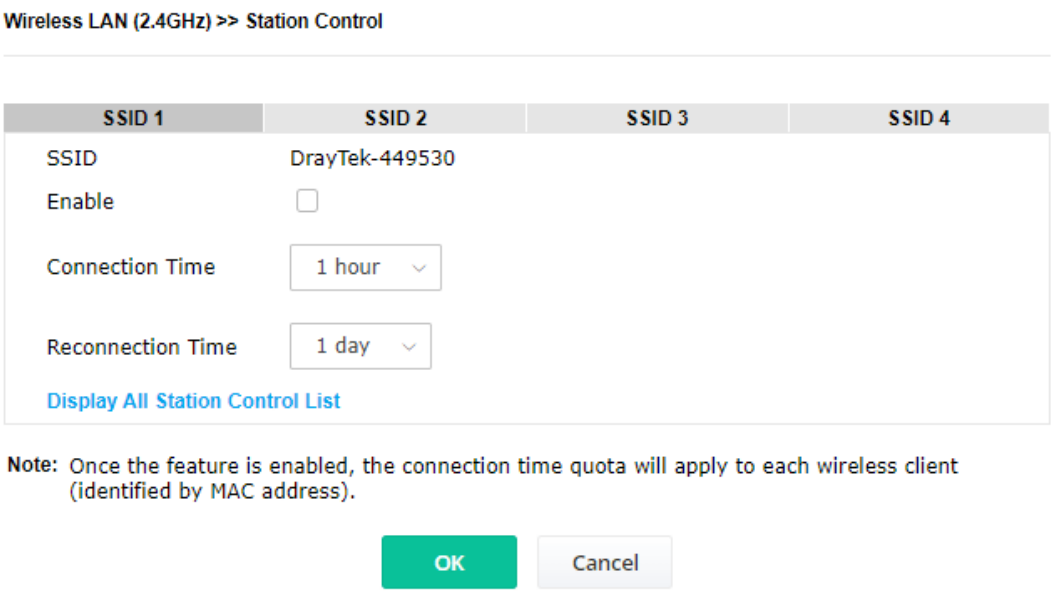
II-3-10 Station Control

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

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

Note:

Up to 300 Wireless Station records are supported by VigorAP.



Available settings are explained as follows:

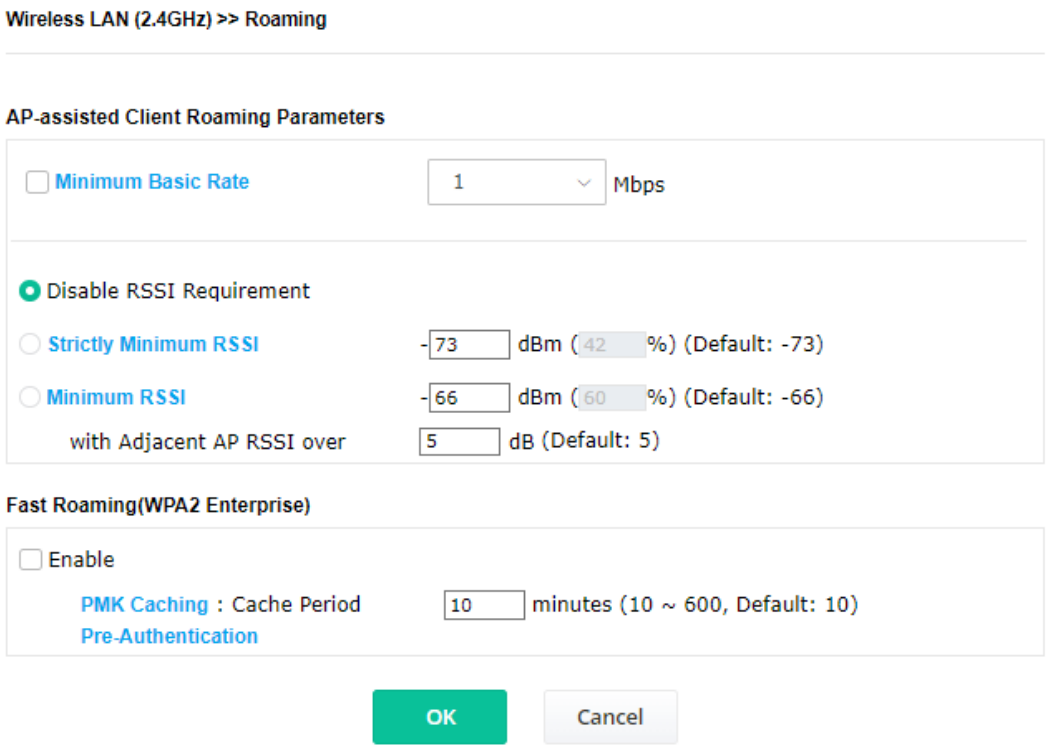
Item	Description
SSID	Display the SSID that the wireless station will use to connect with the Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop-down list to choose the duration for the wireless client connecting /reconnecting to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



Available settings are explained as follows:

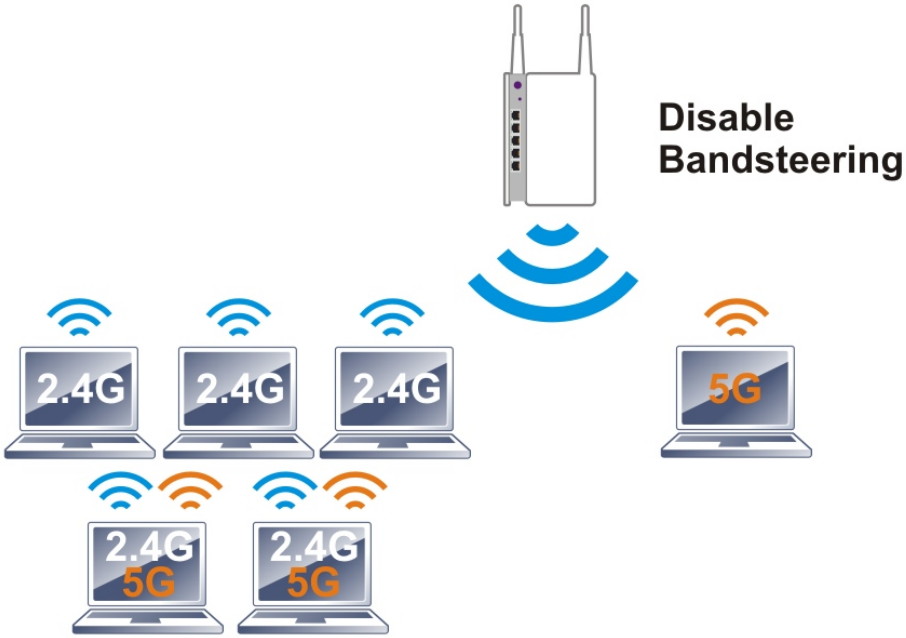
Item	Description
AP-assisted Client Roaming Parameters	When the link rate of the wireless station is too low or the signal received by the wireless station is too worse, VigorAP 906 will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless 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 a value, VigorAP 906 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 the wireless station. When the signal strength is below the value (**dBm**) set here, VigorAP 906 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 906, VigorAP 906 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 Enterprise)	**Enable –** Check the box to enable fast roaming configuration. **PMK Caching -** Set the expiration time of the WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such a feature is available for **WPA2 Enterprise** 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.

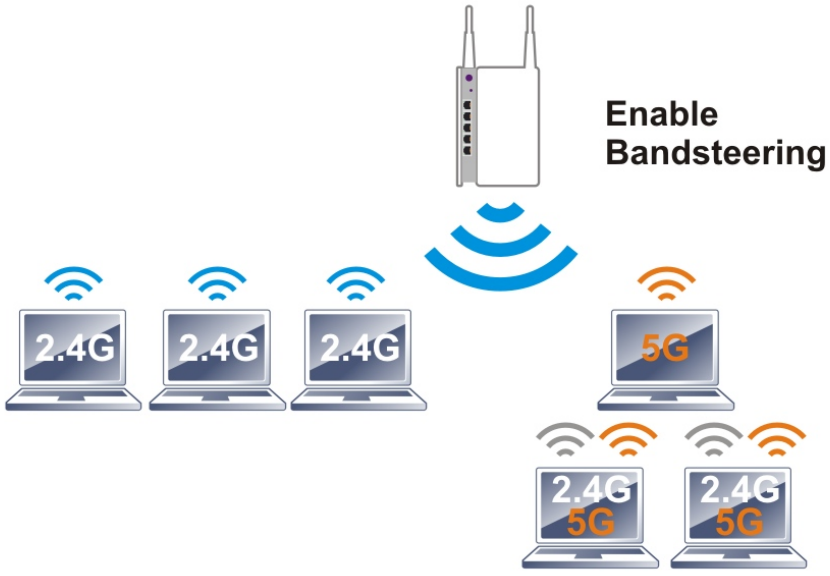
After finishing this web page configuration, please click **OK** to save the settings.

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

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



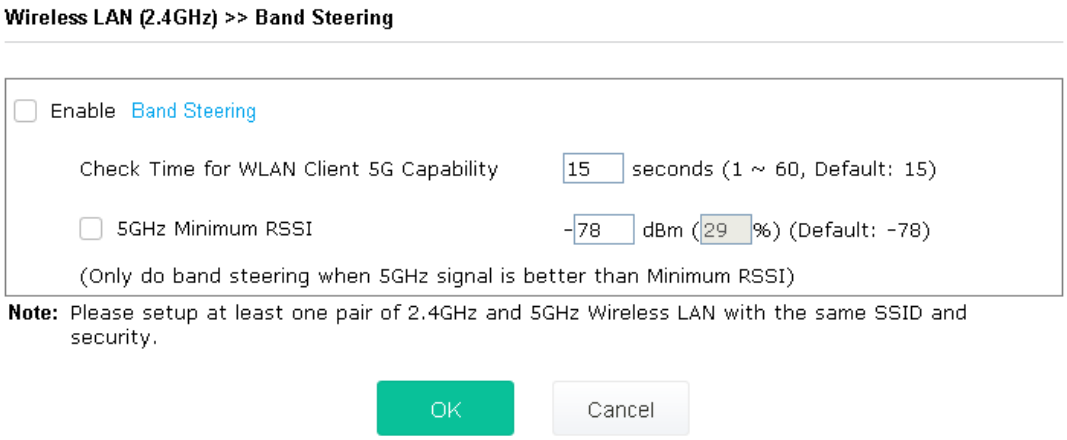
If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent network congestion.



Note:

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

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

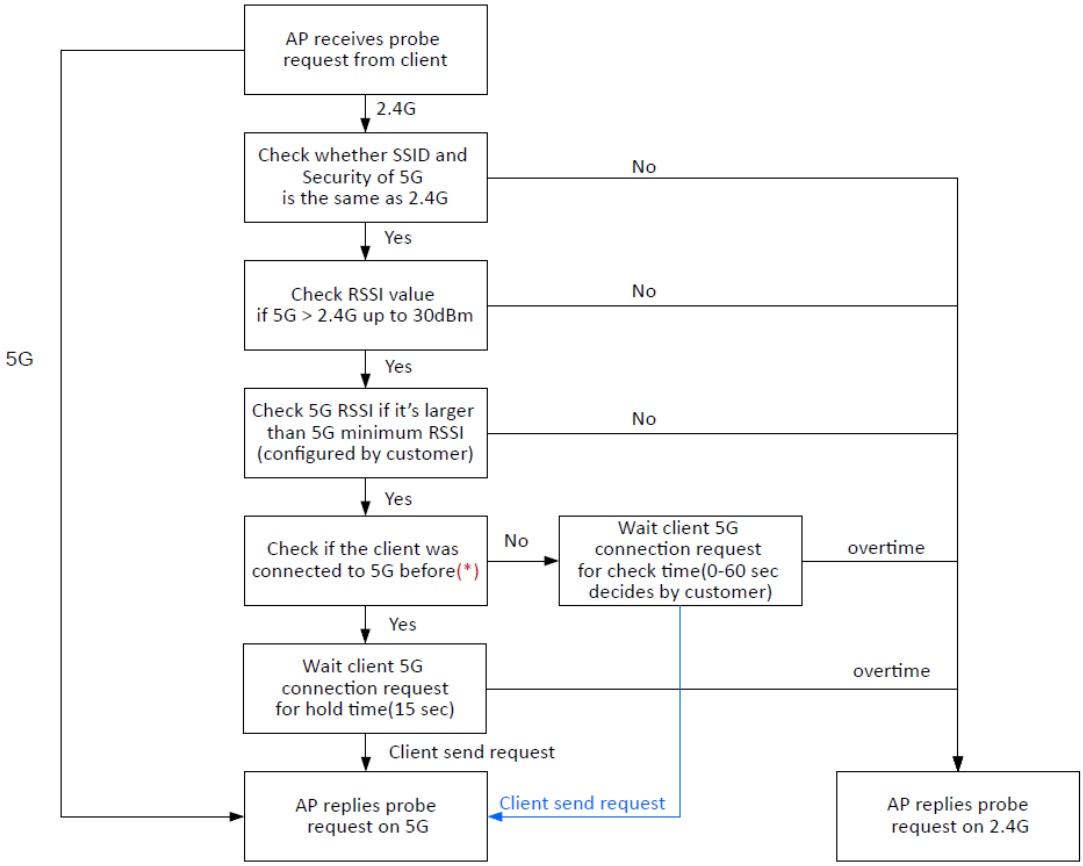


Available settings are explained as follows:

Item	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 a 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. **5GHz Minimum RSSI** – The wireless station has the capability of a 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 906, VigorAP will allow the client to connect to the 2.4GHz network.

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

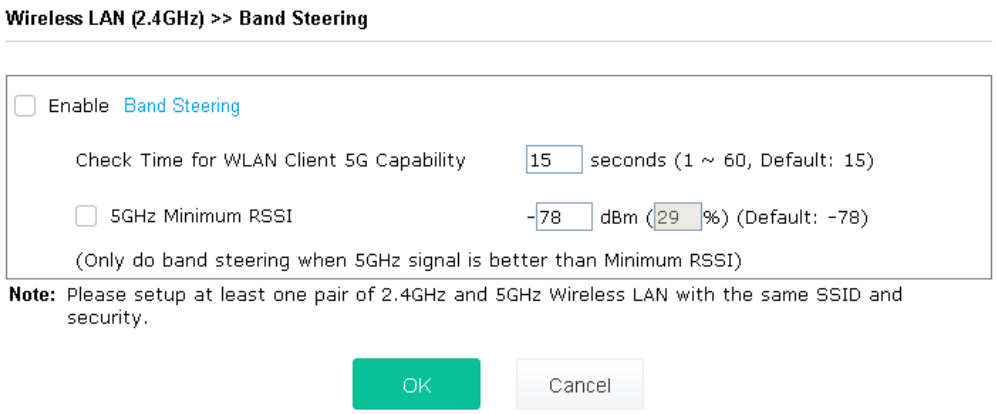
Below shows how Band Steering works.



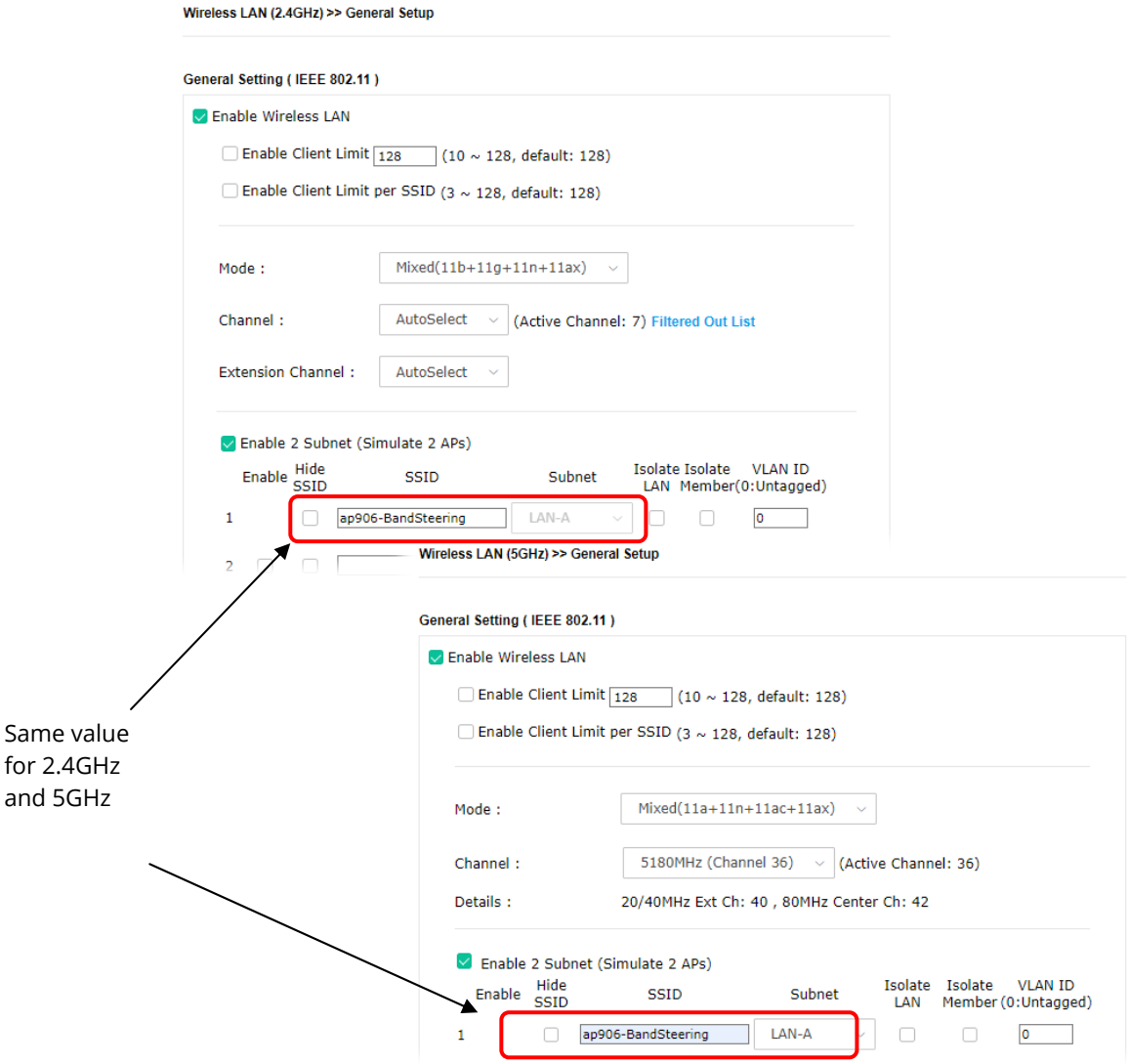
* AP will clear the 5G history station list every 2.5 mins.

How to Use Band Steering?

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

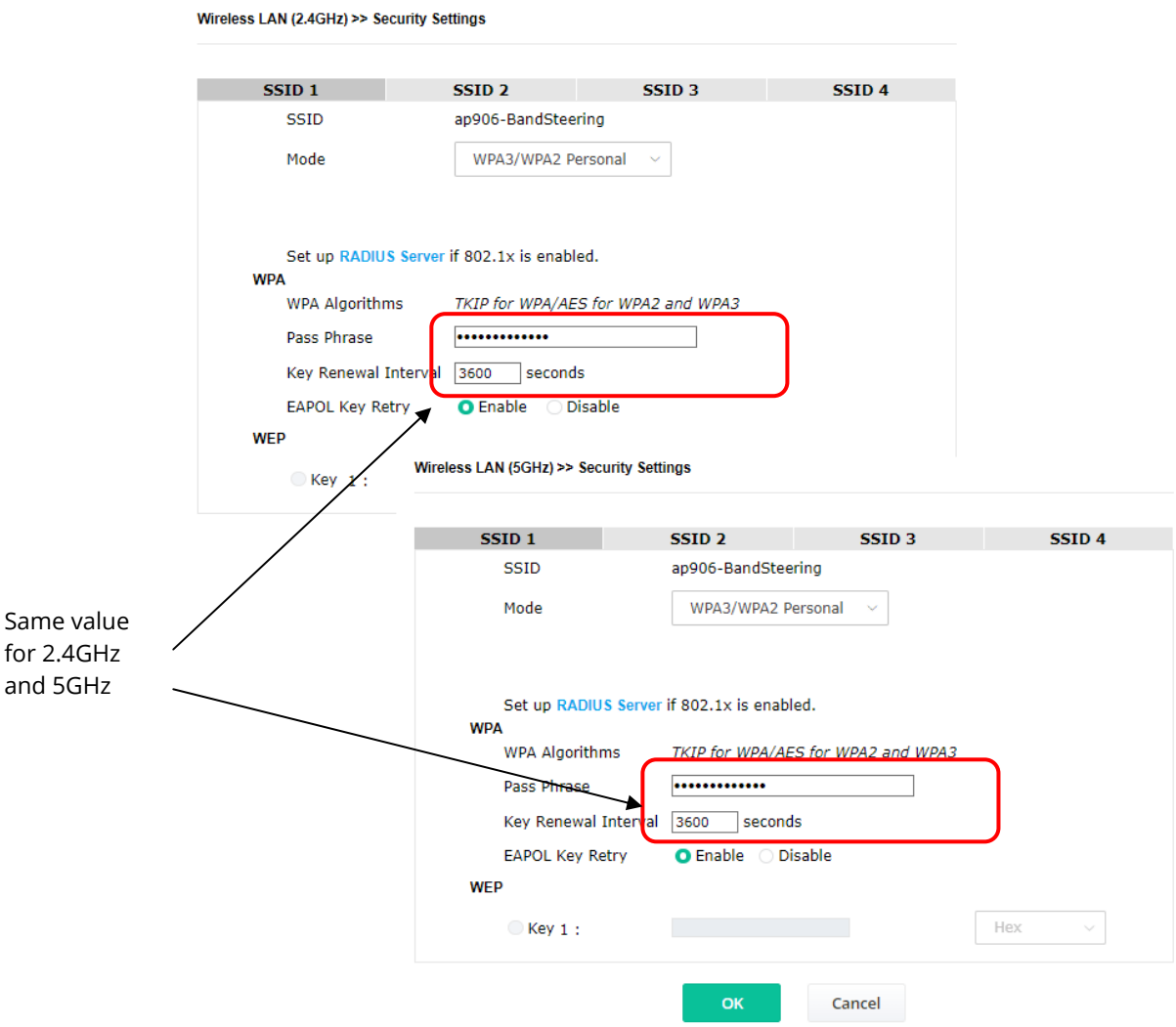


3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *ap906-BandSteering* for both pages. Click **OK** to save the settings.



Same value for 2.4GHz and 5GHz

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



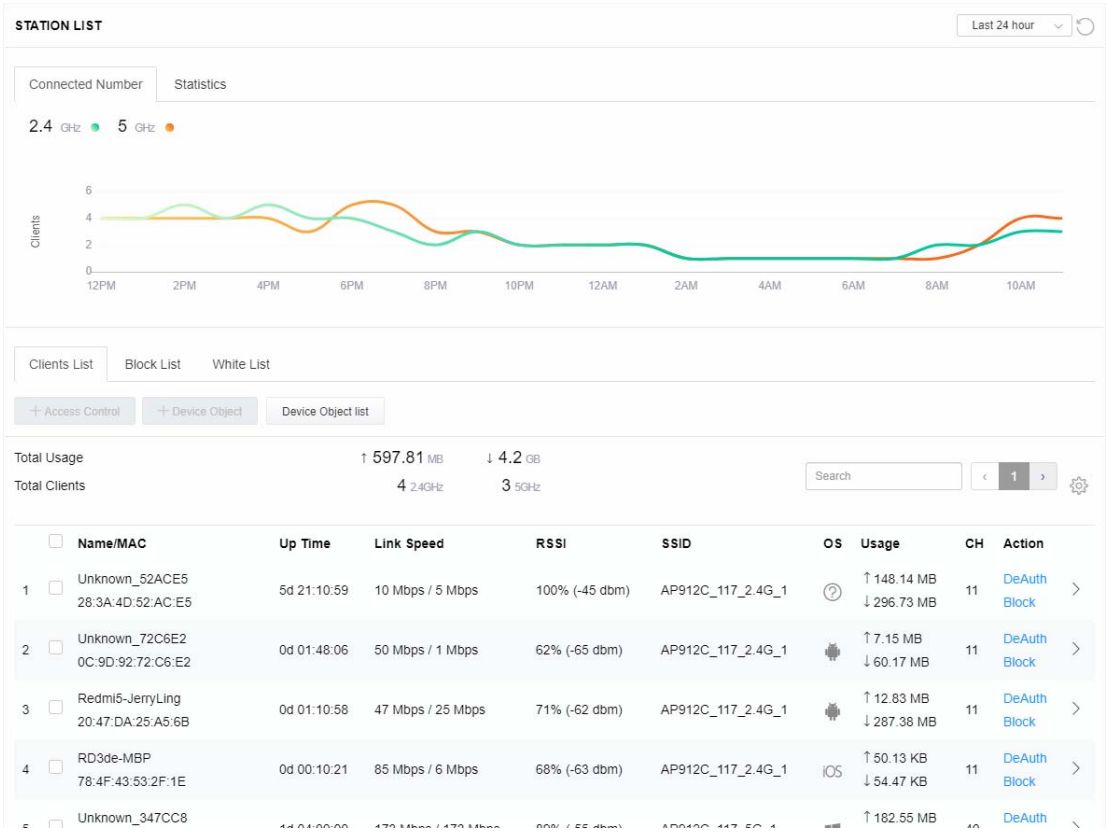
6. Now, VigorAP 906 will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent network congestion.

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 lists.

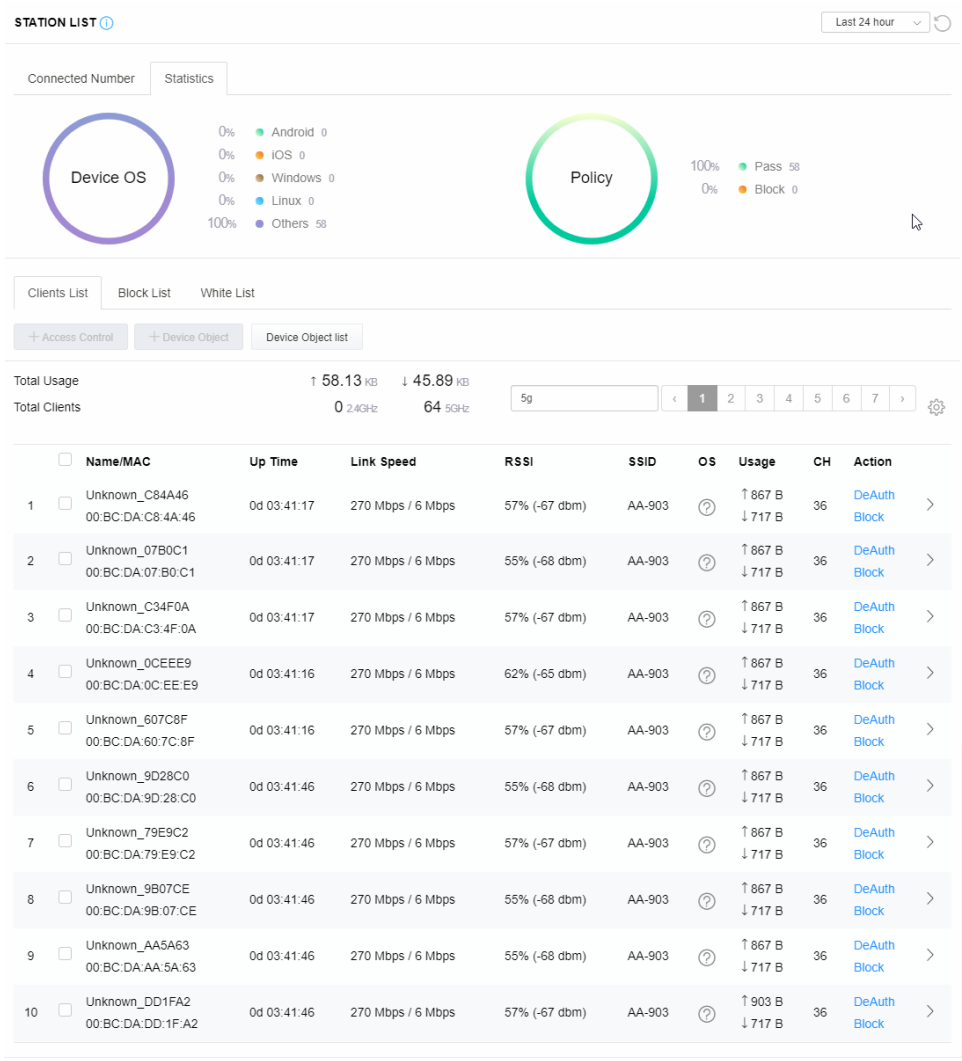
II-3-13-1 Connected Number

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

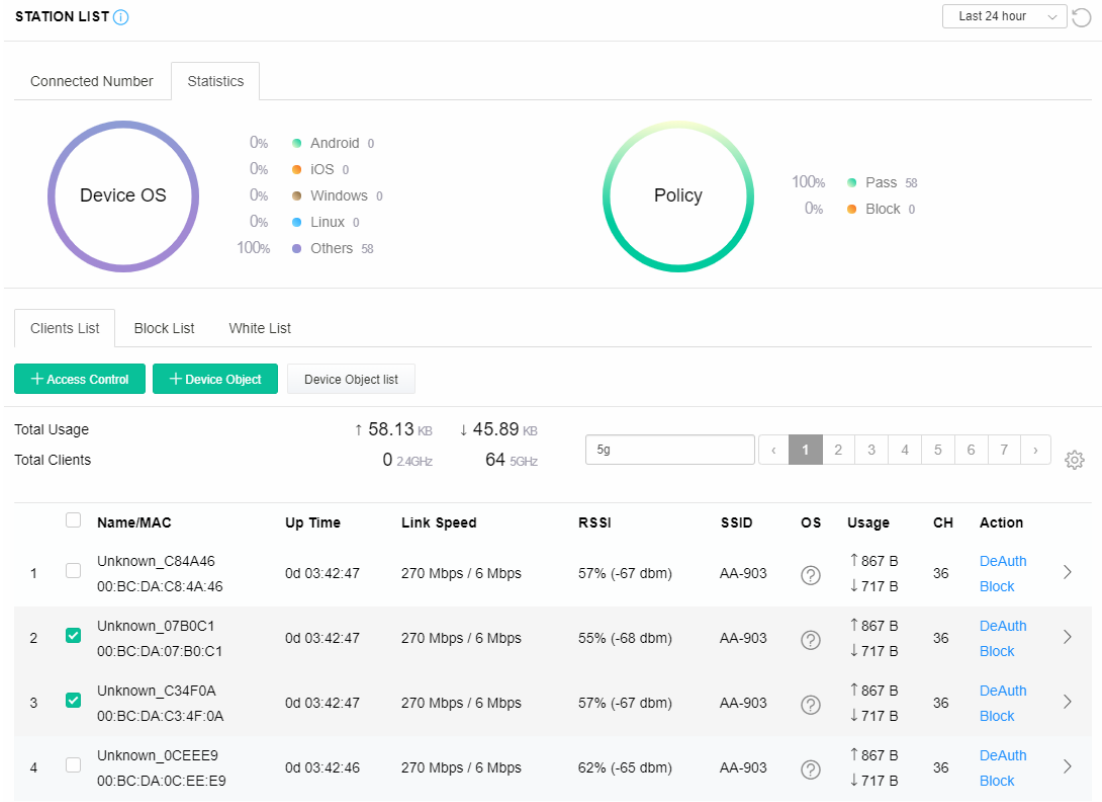
The number of detected devices and the number of devices passed/blocked according to the policy specified in **Mobile Device Management>>Policy** can be illustrated as a doughnut chart.



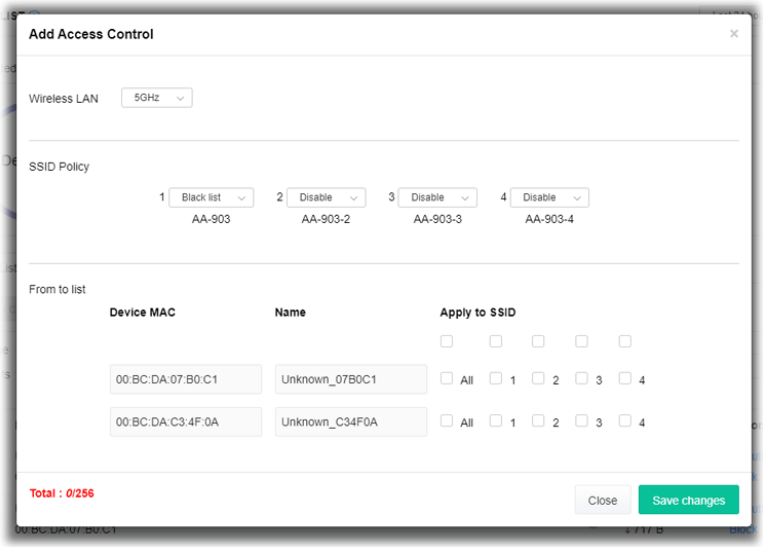
	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
2	Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:41:17	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
3	Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑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		↑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		↑867 B ↓717 B	36	DeAuth Block
6	Unknown_9D28C0 00:BC:DA:9D:28:C0	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑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		↑867 B ↓717 B	36	DeAuth Block
8	Unknown_9B07CE 00:BC:DA:9B:07:CE	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
9	Unknown_AA5A63 00:BC:DA:AA:5A:63	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
10	Unknown_DD1FA2 00:BC:DA:DD:1F:A2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑903 B ↓717 B	36	DeAuth Block

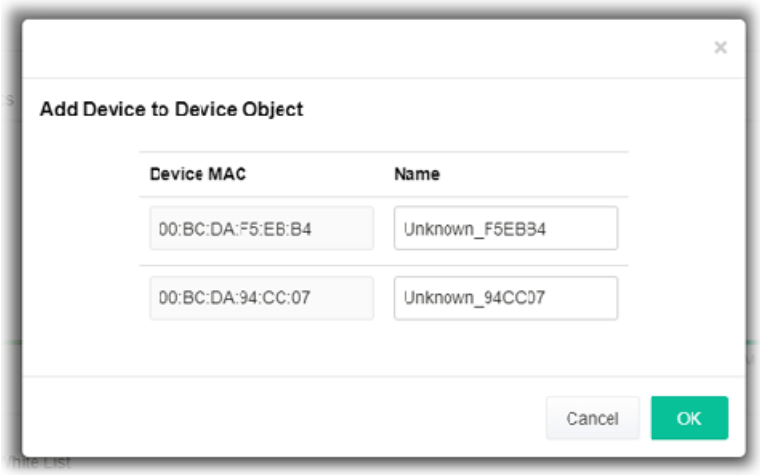
II-3-13-3 Clients List

The client list displays all the stations connecting to VigorAP.



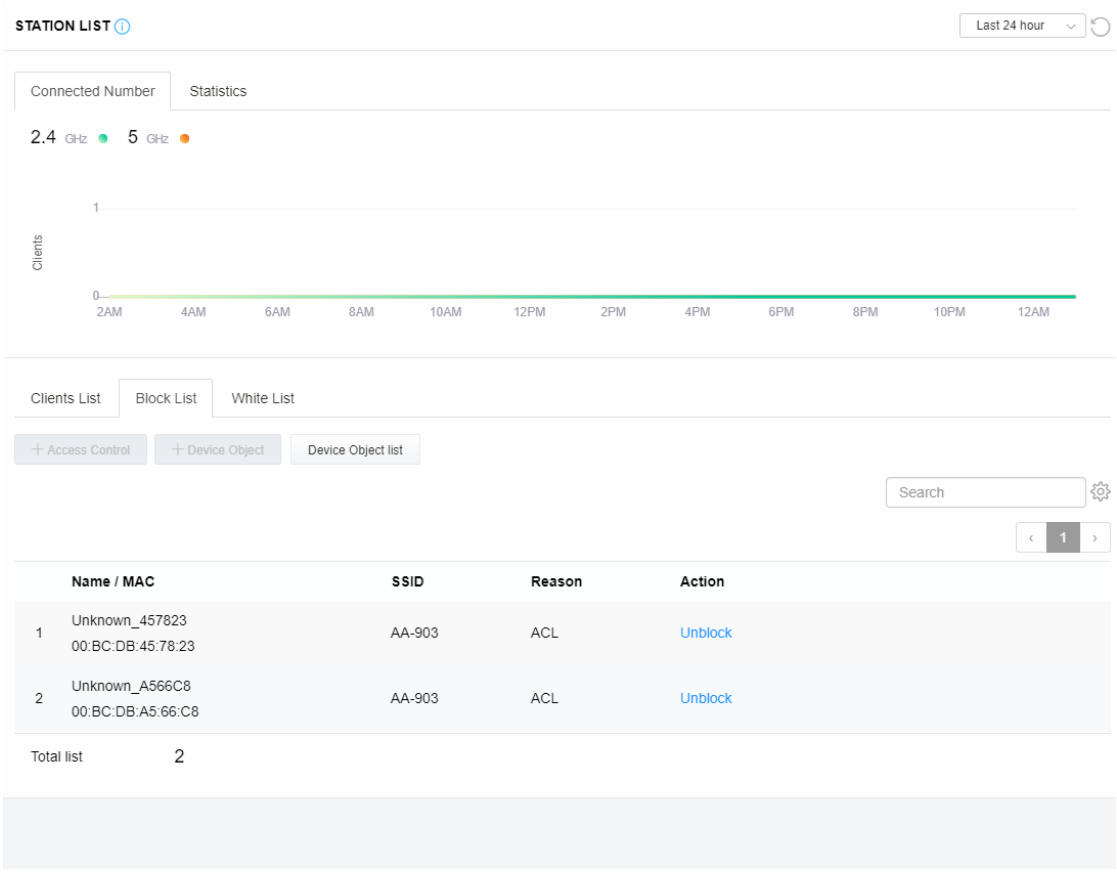
Available settings are explained as follows:

Item	Description
+Access Control	It is available after choosing one of the entries (clients) on the Clients List.  **Wireless LAN** - Specify the bandwidth for the access control list. **SSID Policy** - Set the policy for each SSID as a blacklist or whitelist or disable. **From to list** - Display the clients available for applying this access

	control. **Apply to SSID** - Check **All** to make the device apply the policies to all SSIDs. Or select the one(s) to make the device apply the policies to the selected SSIDs. **Close** - Exit this page without saving any changes. **Save changes** - Save the changes and exit this page.
+Device Object	To add a device to the device object list, choose one of the entries (clients) on the Clients List to enable the Device Object button. Click the button to open the following page.  Check the information listed on the page. Change the MAC address or name of the selected entry if required. Then click **OK** and exit the page.
Device Object list	The existed device object profiles will be shown on the following page.
Clients List	Display the stations connecting to this Vigor device. **Total Usage -** Display the total TX/RX rates. **Total Clients -** Display the number of clients in the state of TX or RX. **Name / MAC -** Display the host name / MAC address of the connecting client. **Up Time** - Display the connection time. **Link Speed**- Display the link speed. **RSSI** - Display the RSSI value. **SSID** - Display the SSID the client used for connecting VigorAP. **OS** - Display the OS of the client. **Usage** - Display the bandwidth usage (up and down) of the client. **CH** - Display the channel used by the client. **Action** - Display the authentication method used by the client, and if it is on a block list or white list.

II-3-13-4 Block List

This page displays information about the stations under the Block List.

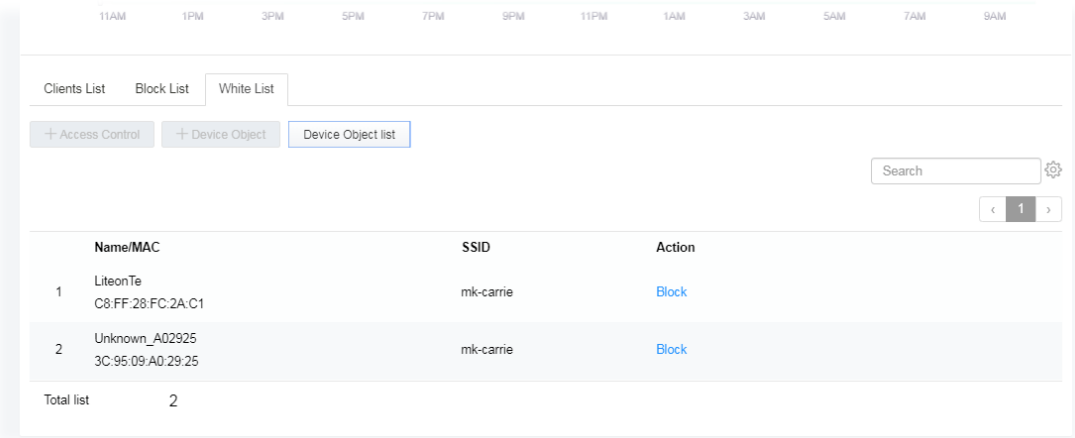


Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless 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.

II-3-13-5 White List

This page displays general information about the stations under the White List.

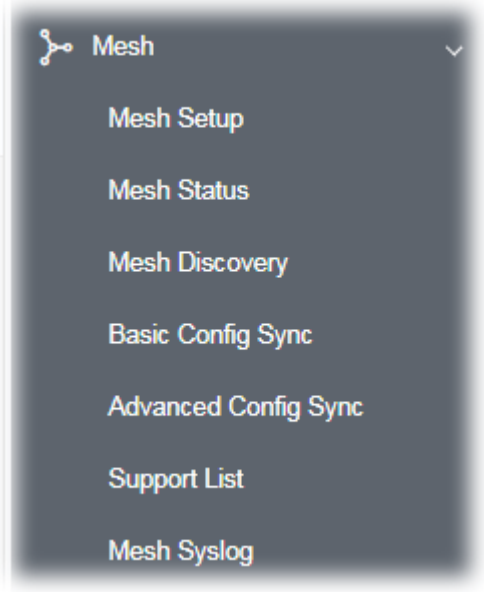


Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Action	Display the action that you can execute for the station. **Block** - Click to block the entry.

II-4 Mesh Settings for Mesh Mode

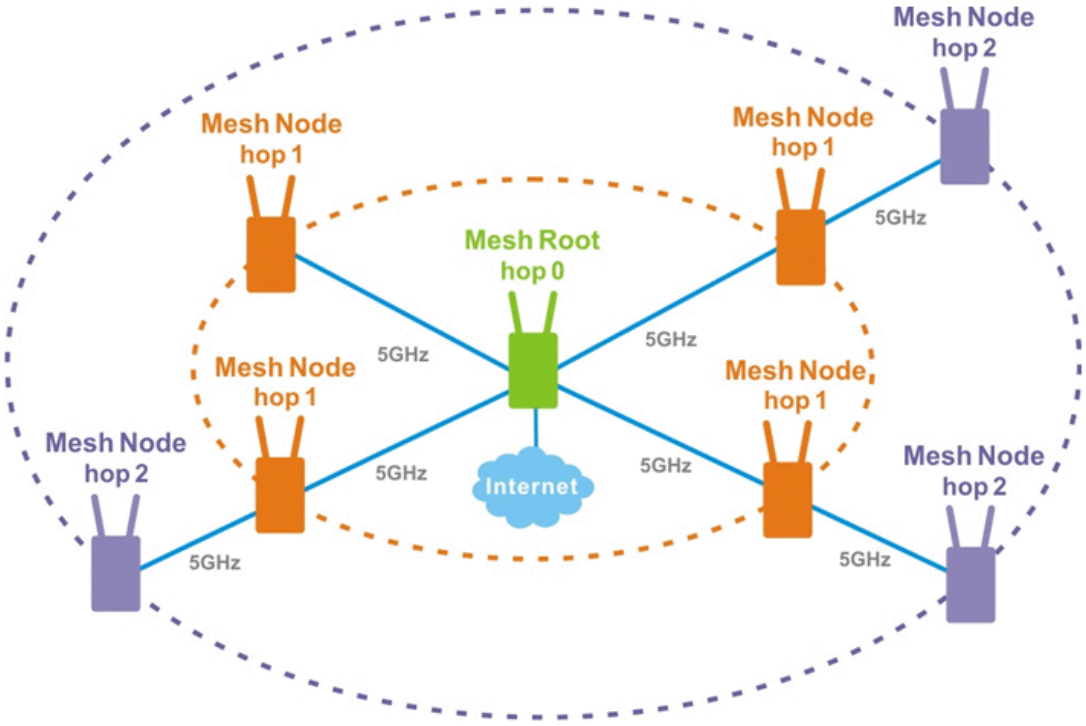
When you choose **Mesh** as the operation mode, the Mesh menu with the settings of Mesh Setup, Mesh Status, Mesh Discovery, Configuration Sync, Support List, and Mesh Syslog will be shown on the screen.



Please note that, within the VigorMesh network,

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

Refer to the following figure:



For the mesh group set within the VigorMesh network,

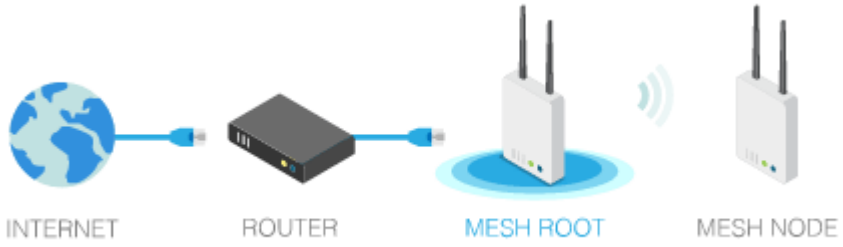
- It must be composed by “1” Mesh Root and “0~7” mesh nodes
- (Roaming) Normally members in a mesh group use the same Wireless SSID/security
- (Add) Only the mesh root can add a new mesh node into the mesh group
- (Recover) A disconnected mesh node will automatically try to connect to another connected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

Mesh Root and Mesh Node

Mesh Root indicates that VigorAP would be another AP's uplink connection. As a Mesh Root, VigorAP must connect to a gateway with an 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 a wireless network or physical connection with an Ethernet cable.

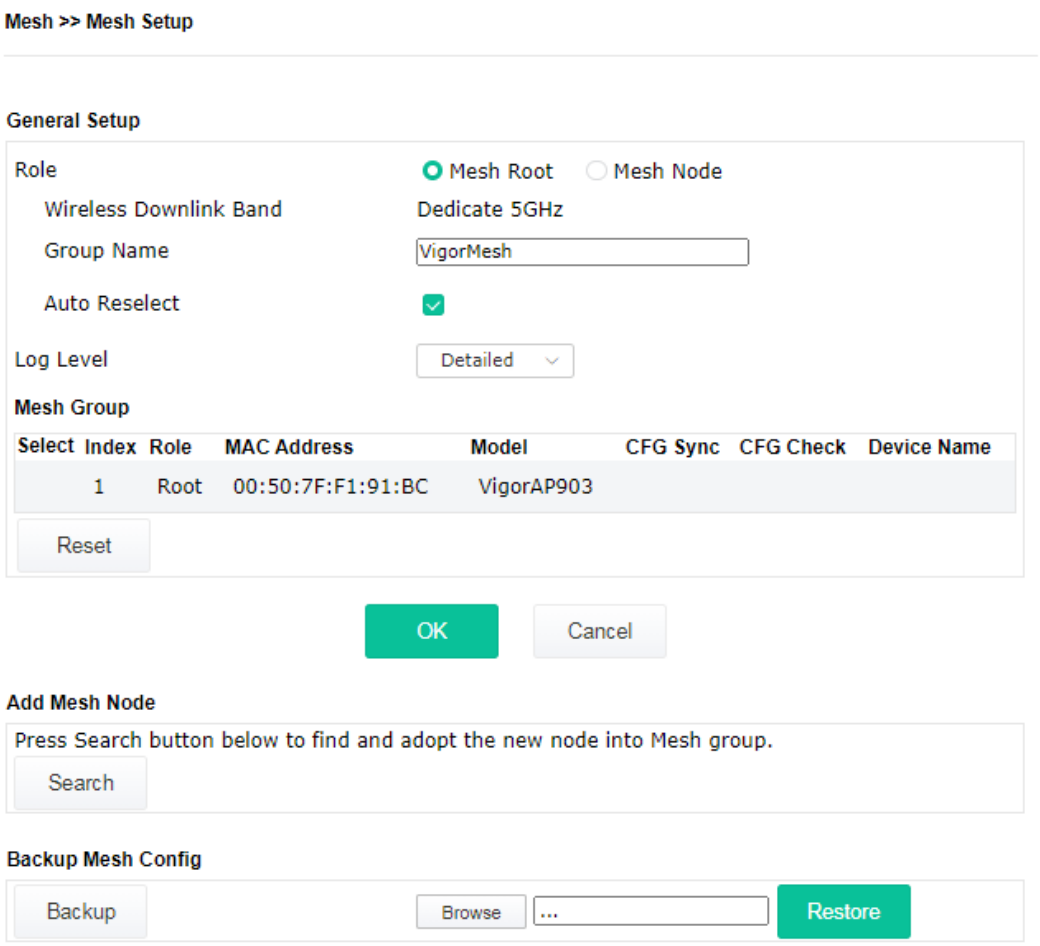
The following figure shows how VigorAP runs as MESH ROOT:



The following figure shows how VigorAP runs as MESH NODE:

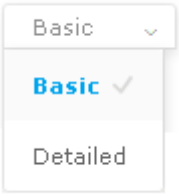
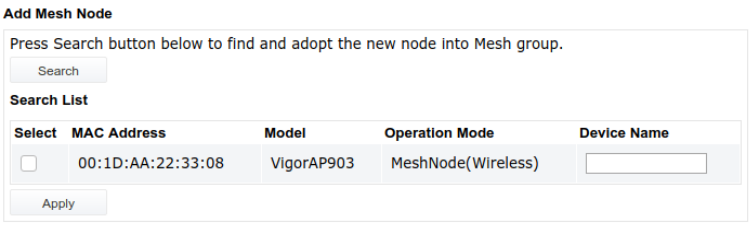
II-4-1 Mesh Setup

Such a 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 the current mesh group.



Available settings are explained as follows:

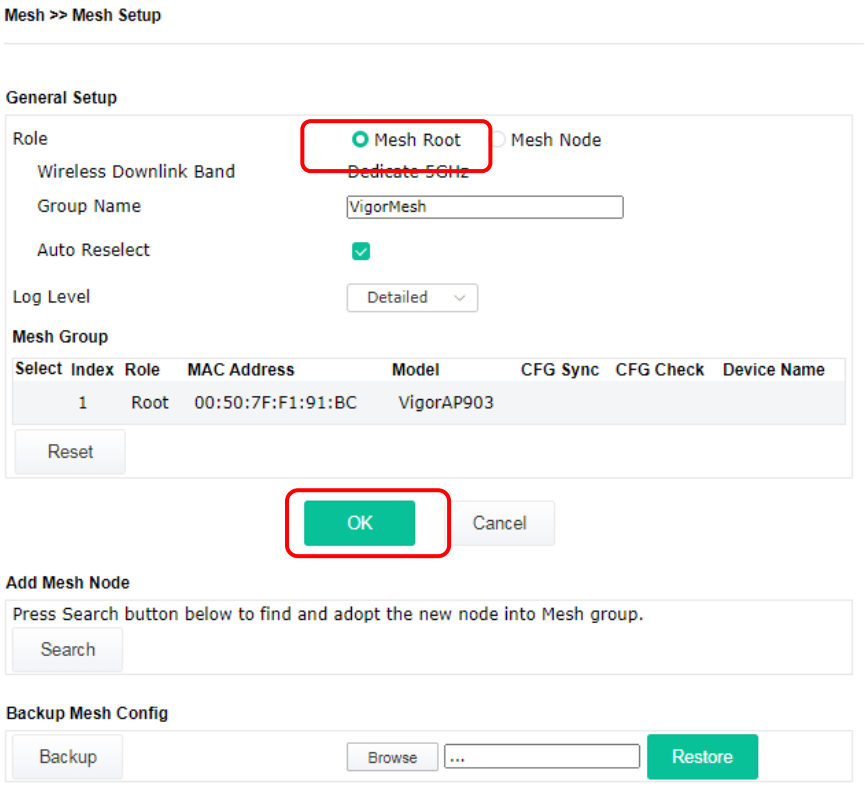
Item	Description
General Setup	
Role	**Mesh Root –** When VigorAP is connected to a Vigor router with a physical Ethernet cable, it can be set as a mesh root to deliver the wireless signals to a mesh node AP. **Mesh Node –** As a mesh node, such VigorAP can pass the wireless connection signal to another 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 the mesh node. **Log Level –** Choose **Basic** or **Detailed**. Related information will be shown on the **Diagnostics>>System Log.**

	
When Mesh Root is selected	**Wireless Downlink Band** – Choose a wireless band for connecting with a downlink mesh root or a downlink mesh node. **Group Name** - Display the name of the current mesh group. **Auto Reselect** - It is selected in default. To perform the auto reselect, make sure the process for CFG Sync and CFG Check for mesh nodes are successful. If enabled, after changing the environment of the mesh network (e.g., offline, disconnection), the root device will perform auto reselect to reconstruct the mesh network.
When Mesh Node is selected	**Wired Uplink –** Check the box if such VigorAP connects to an uplink mesh root or an uplink mesh node with an Ethernet cable. **Wireless Uplink/Downlink Band** – Choose a wireless band for connecting with an uplink/downlink mesh root or an uplink/downlink mesh node.
Mesh Group	When the VigorAP is set as mesh root or is added to a mesh group, the basic information including role, MAC address, and model name of the AP will be shown in this area. Up to 8 entries (one mesh root and seven mesh nodes) will be shown on this field. **Reset -** Click it to clear the Mesh Group information. **Delete** - Click it to remove the selected entry.
Add Mesh Node	Click **Search** to find out the available mesh node on the network.  Check the one you want and click **Apply**. The selected AP will be added to the 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.

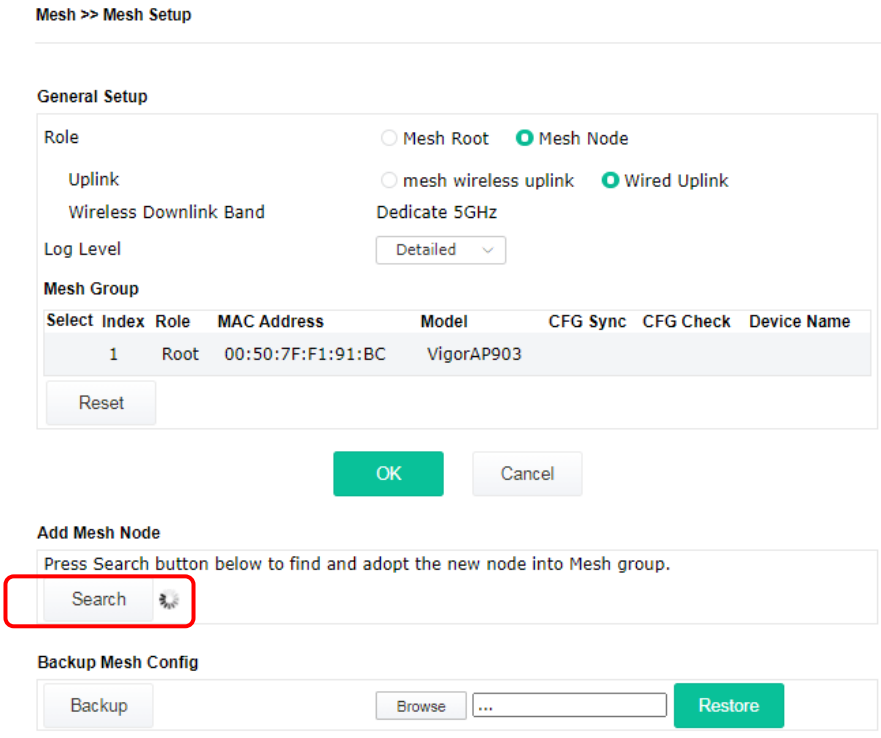
How to set up a mesh group?

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

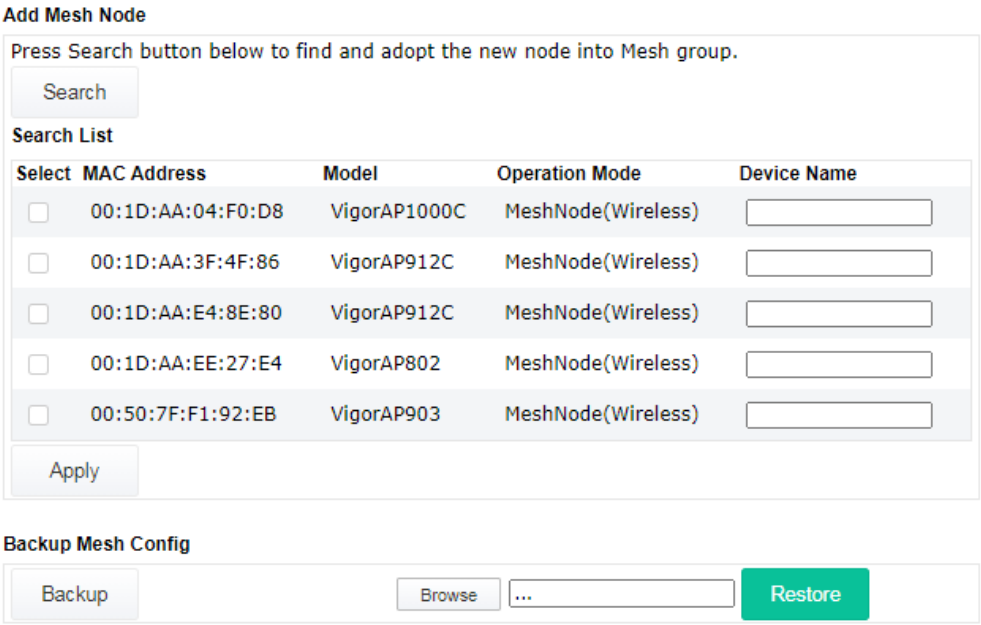
1. Open **Mesh>>Mesh Setup**. Click **Mesh Root** and click **OK** for the VigorAP connected to the PC with Ethernet cable. At first, a Mesh Group is with only Mesh Root.



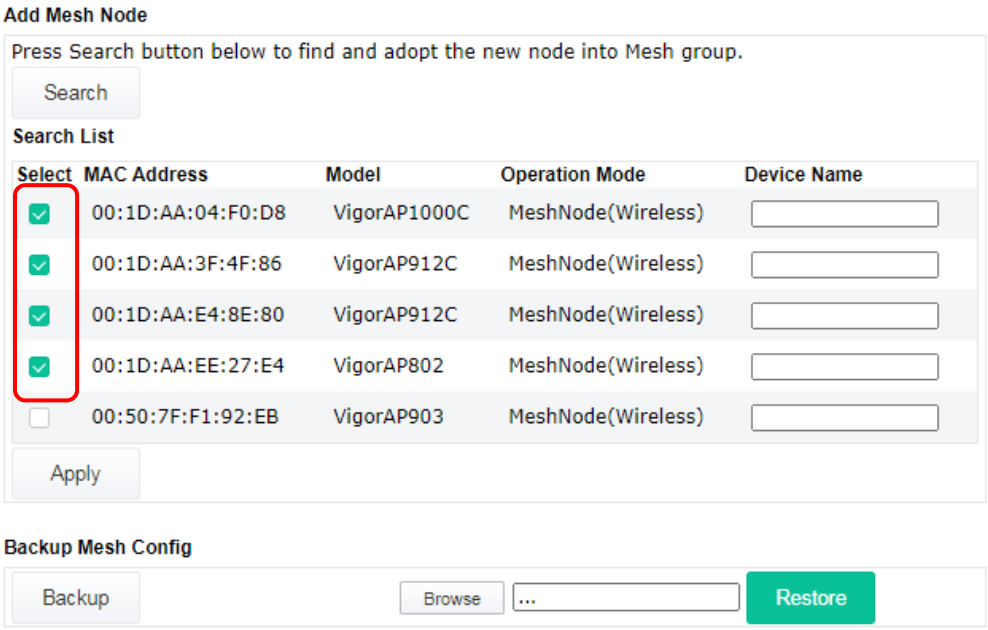
2. Click the **Search** button in the field of **Add Mesh Node**.



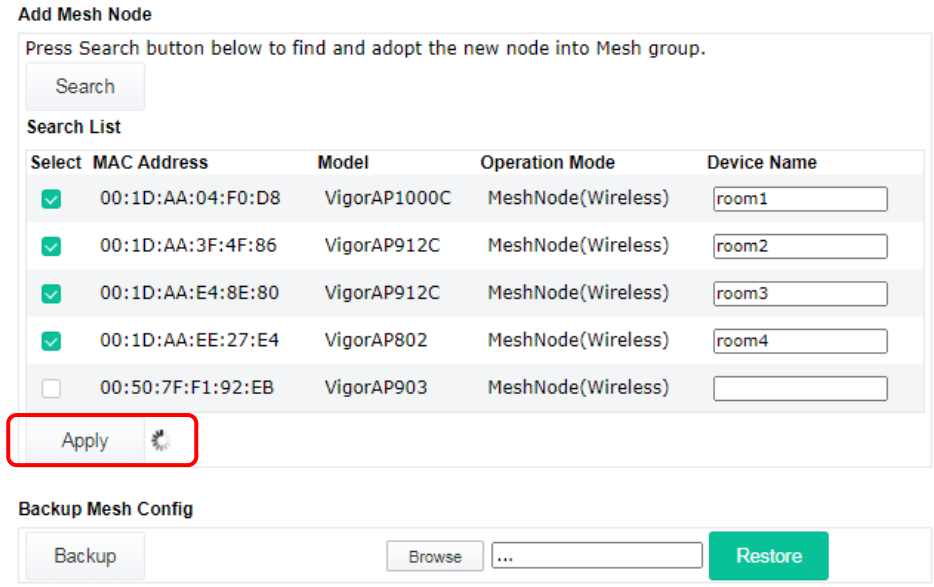
3. Wait until the searching result appears.



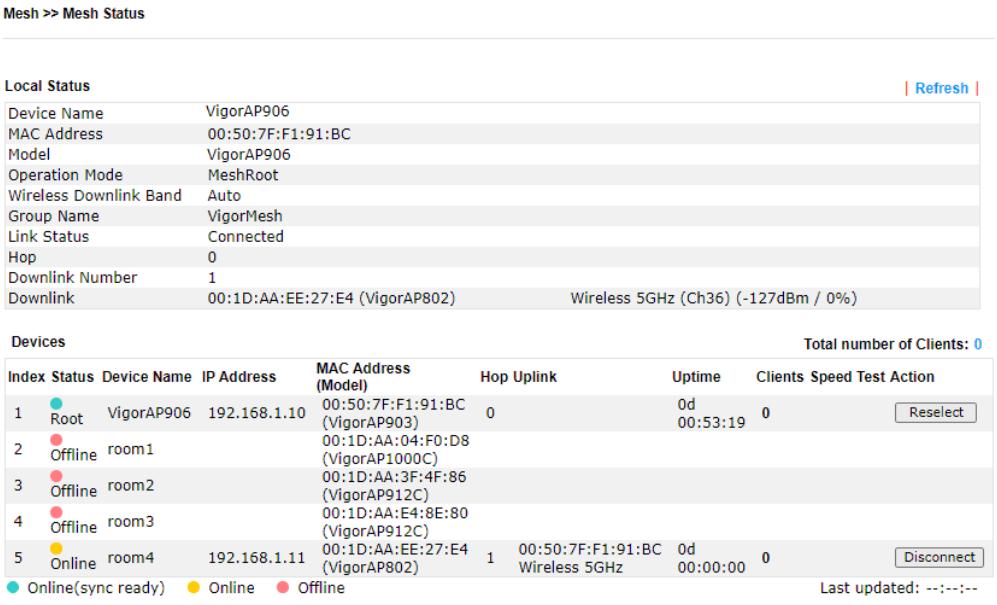
4. Choose the device(s) you want to add to the Mesh Group as mesh node(s) and define the **Device Name** for each node. In this example, five devices are specified as mesh nodes.



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

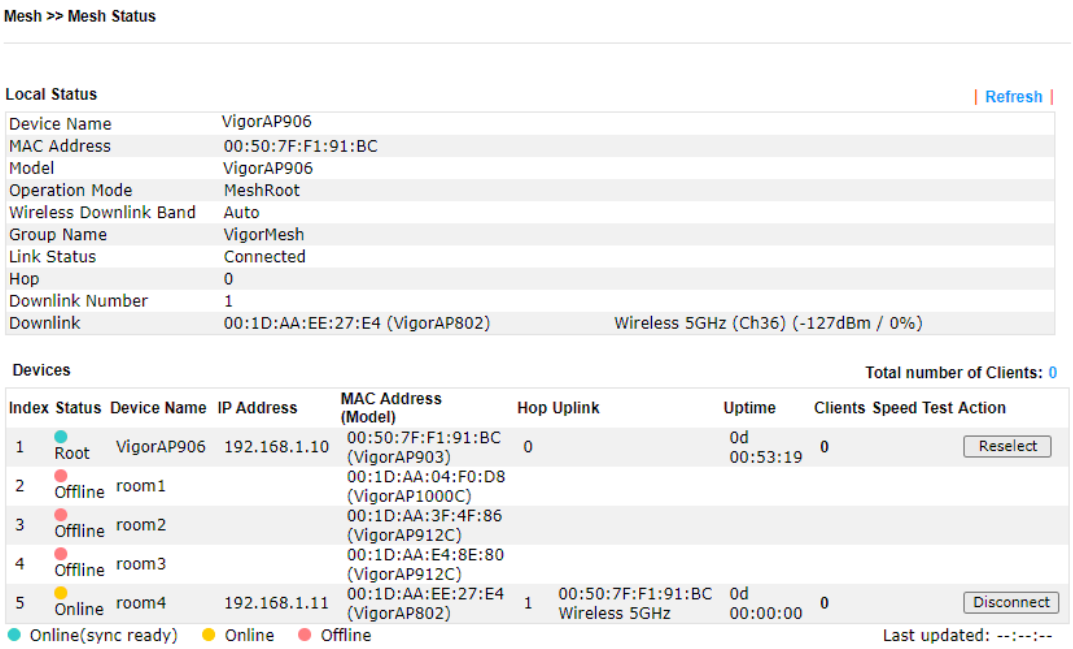


6. After finishing the mesh network configuration, refer to **Mesh>>Mesh Status** for viewing the result.

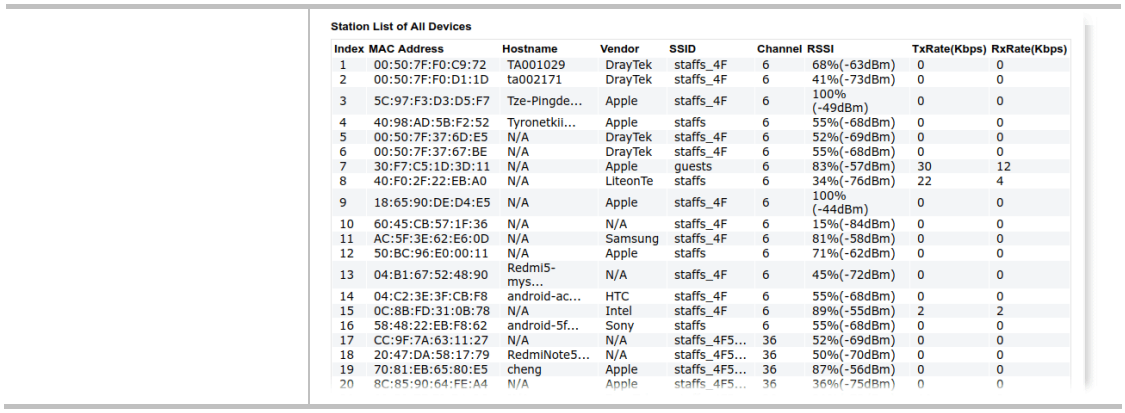


II-4-2 Mesh Status

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



Item	Description
Local Status	Display general information for such VigorAP.
Devices	Display detailed information for this VigorAP (as mesh root) and mesh node(s) in the group. **Index** – Display the number of the device within a mesh group. **Status** – Display the role of the device within a mesh group. **Device Name** – Display the name of the device (for identification). **IP Address** – Display the IP address of the device. **MAC Address** – Display the MAC address of the device. **Hop** – Display the level of the devices within a mesh group. “0” means the access point is connected to a device by using an Ethernet cable (wired). “1” to “3” means the level of the access point within a mesh group and it connects to other access points via a wireless link. **Uplink** – Display the MAC address of the device that the AP connects to.
Total number of Clients	Display the station list of all mesh devices.

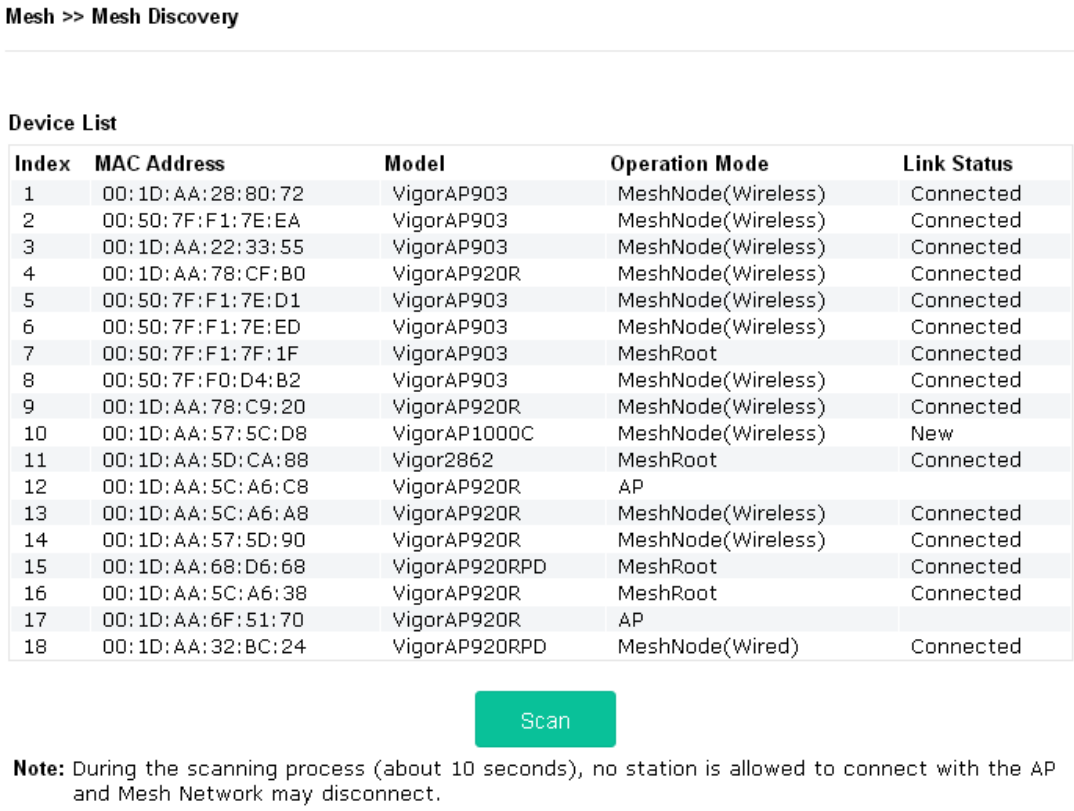


Station List of All Devices

Index	MAC Address	Hostname	Vendor	SSID	Channel	RSSI	TxRate(Kbps)	RxRate(Kbps)
1	00:50:7F:F0:C9:72	TA001029	DrayTek	staffs_4F	6	68%(-63dBm)	0	0
2	00:50:7F:F0:D1:1D	ta002171	DrayTek	staffs_4F	6	41%(-73dBm)	0	0
3	5C:97:F3:D3:D5:F7	Tze-Pingde...	Apple	staffs_4F	6	100% (-49dBm)	0	0
4	40:98:AD:5B:F2:52	Tyronetkii...	Apple	staffs	6	55%(-68dBm)	0	0
5	00:50:7F:37:6D:E5	N/A	DrayTek	staffs_4F	6	52%(-69dBm)	0	0
6	00:50:7F:37:67:BE	N/A	DrayTek	staffs_4F	6	55%(-68dBm)	0	0
7	30:F7:C5:1D:3D:11	N/A	Apple	guests	6	83%(-57dBm)	30	12
8	40:F0:2F:22:EB:A0	N/A	LiteonTe	staffs	6	34%(-76dBm)	22	4
9	18:65:90:DE:D4:E5	N/A	Apple	staffs_4F	6	100% (-44dBm)	0	0
10	60:45:CB:57:1F:36	N/A	N/A	staffs_4F	6	15%(-84dBm)	0	0
11	AC:5F:3E:62:E6:0D	N/A	Samsung	staffs_4F	6	81%(-58dBm)	0	0
12	50:BC:96:E0:00:11	N/A	Apple	staffs	6	71%(-62dBm)	0	0
13	04:B1:67:52:48:90	Redmi5-mys...	N/A	staffs_4F	6	45%(-72dBm)	0	0
14	04:C2:3E:3F:CB:F8	android-ac...	HTC	staffs_4F	6	55%(-68dBm)	0	0
15	0C:8B:FD:31:0B:78	N/A	Intel	staffs_4F	6	89%(-55dBm)	2	2
16	58:48:22:EB:F8:62	android-5f...	Sony	staffs	6	55%(-68dBm)	0	0
17	CC:9F:7A:63:11:27	N/A	N/A	staffs_4F5...	36	52%(-69dBm)	0	0
18	20:47:DA:58:17:79	RedmiNote5...	N/A	staffs_4F5...	36	50%(-70dBm)	0	0
19	70:81:EB:65:80:E5	cheng	Apple	staffs_4F5...	36	87%(-56dBm)	0	0
20	8C:85:90:64:FE:A4	N/A	Apple	staffs_4F5...	36	36%(-75dBm)	0	0

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	00:1D:AA:28:80:72	VigorAP903	MeshNode(Wireless)	Connected
2	00:50:7F:F1:7E:EA	VigorAP903	MeshNode(Wireless)	Connected
3	00:1D:AA:22:33:55	VigorAP903	MeshNode(Wireless)	Connected
4	00:1D:AA:78:CF:B0	VigorAP920R	MeshNode(Wireless)	Connected
5	00:50:7F:F1:7E:D1	VigorAP903	MeshNode(Wireless)	Connected
6	00:50:7F:F1:7E:ED	VigorAP903	MeshNode(Wireless)	Connected
7	00:50:7F:F1:7F:1F	VigorAP903	MeshRoot	Connected
8	00:50:7F:F0:D4:B2	VigorAP903	MeshNode(Wireless)	Connected
9	00:1D:AA:78:C9:20	VigorAP920R	MeshNode(Wireless)	Connected
10	00:1D:AA:57:5C:D8	VigorAP1000C	MeshNode(Wireless)	New
11	00:1D:AA:5D:CA:88	Vigor2862	MeshRoot	Connected
12	00:1D:AA:5C:A6:C8	VigorAP920R	AP	
13	00:1D:AA:5C:A6:A8	VigorAP920R	MeshNode(Wireless)	Connected
14	00:1D:AA:57:5D:90	VigorAP920R	MeshNode(Wireless)	Connected
15	00:1D:AA:68:D6:68	VigorAP920RPD	MeshRoot	Connected
16	00:1D:AA:5C:A6:38	VigorAP920R	MeshRoot	Connected
17	00:1D:AA:6F:51:70	VigorAP920R	AP	
18	00:1D:AA:32:BC:24	VigorAP920RPD	MeshNode(Wired)	Connected

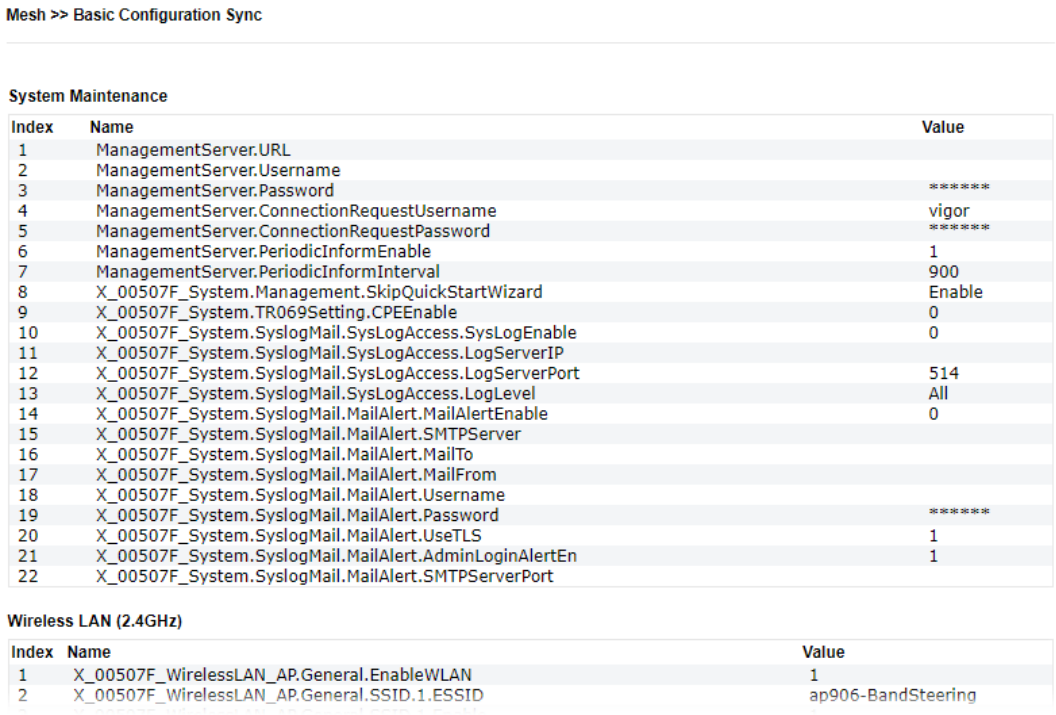
Scan

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, the surrounding VigorAP device(s) will be displayed on this page.

II-4-4 Basic Configuration Sync

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



Mesh >> Basic Configuration Sync

System Maintenance

Index	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.SyslogMail.SysLogAccess.SysLogEnable	0
11	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
12	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
13	X_00507F_System.SyslogMail.SysLogAccess.LogLevel	All
14	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
15	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
16	X_00507F_System.SyslogMail.MailAlert.MailTo	
17	X_00507F_System.SyslogMail.MailAlert.MailFrom	
18	X_00507F_System.SyslogMail.MailAlert.Username	
19	X_00507F_System.SyslogMail.MailAlert.Password	******
20	X_00507F_System.SyslogMail.MailAlert.UseTLS	1
21	X_00507F_System.SyslogMail.MailAlert.AdminLoginAlertEn	1
22	X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	

Wireless LAN (2.4GHz)

Index	Name	Value
1	X_00507F_WirelessLAN_AP.General.EnableWLAN	1
2	X_00507F_WirelessLAN_AP.General.SSID.1.ESSID	ap906-BandSteering

Available settings are explained as follows:

Item	Description
System Maintenance / Wireless LAN (2.4Hz) / Wireless LAN (5GHz)	Check the item(s) you want to make configuration sync. **Apply** – Click it to apply the settings configured by such AP to all connected mesh nodes. **Note that this button is available only 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 the 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 an internet speed test with different hop mesh nodes.)

  Internet Download Speed (for root and hop1 ~ hop3):

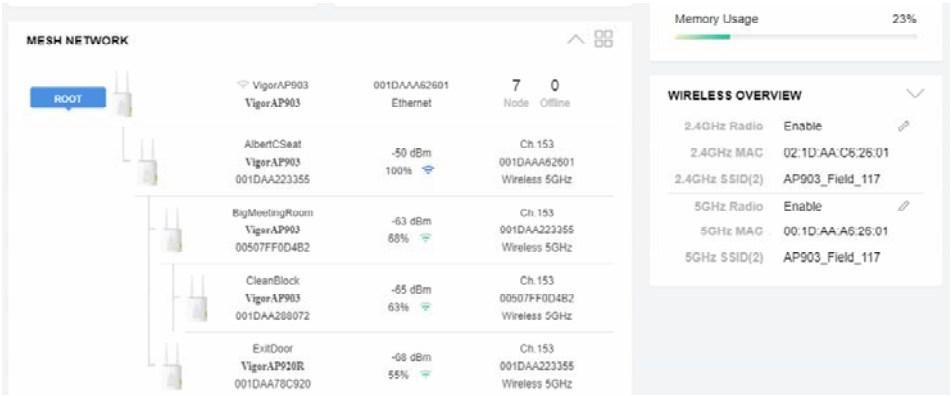
  iPad connects to Root : 80Mbps

  iPad connects to hop1 Node : 49Mbps (Uplink RSSI : -55dBm)

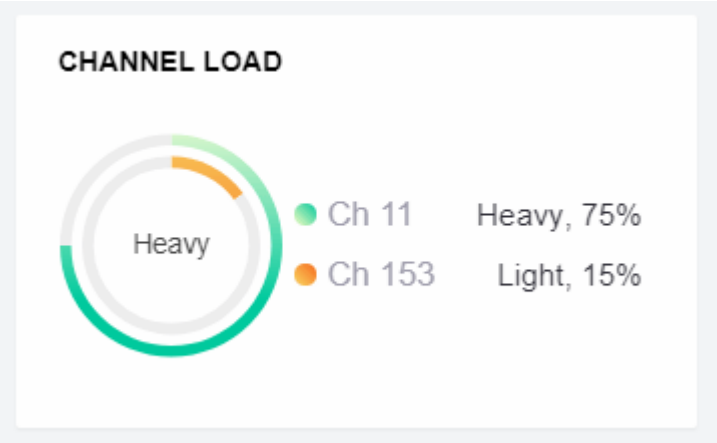
  iPad connects to hop2 Node : 41Mbps (Uplink RSSI : hop2 -64dBm / hop1 -55dBm)

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

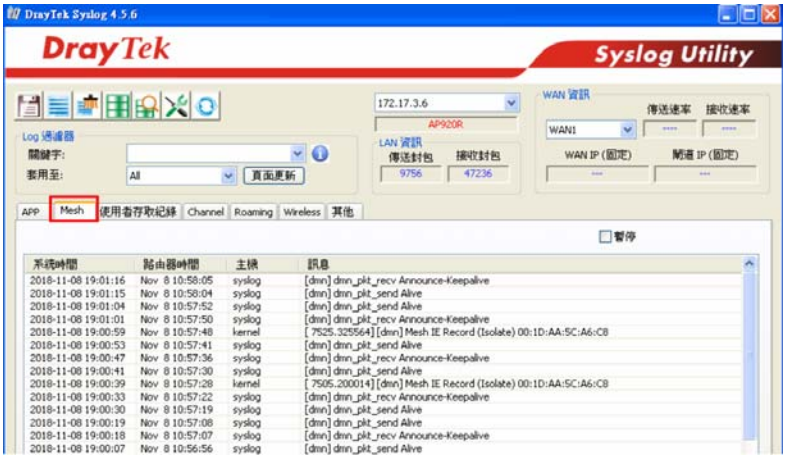
- It is not suggested to use a wireless Mesh Node with Ethernet cable connected to a Mesh Root.
- If resetting a Mesh Root,
  - All "connected" Mesh Nodes will be informed to reset.
  - Group List and Group Key will be reset, too.
  - For those Mesh Nodes unable to reset, reset them manually. Reset the 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 the 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 the 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 906 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 analysis.



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

Roaming

Index	Name	Value
1	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.EnMinBasicRate	0
2	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinBasicRate	1Mbps
3	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.RSSI	Disable_RSSI_Requirement
4	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.StrictlyRSSISignal	0
5	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinRSSISignal	0
6	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	0
7	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.Enable	0
8	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.CachePeriod	10
9	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.EnMinBasicRate	0
10	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinBasicRate	6Mbps
11	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.RSSI	Disable_RSSI_Requirement
12	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.StrictlyRSSISignal	0
13	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinRSSISignal	0
14	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	0
15	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.Enable	0
16	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.CachePeriod	10

Advanced Setting

Index	Name	Value
1	X_00507F_WirelessLAN_AP.AdvancedSetting.ChannelList	
2	X_00507F_WirelessLAN_AP.AdvancedSetting.IGMPSnoopingEn	1
3	X_00507F_WirelessLAN_AP.AdvancedSetting.IsolateBandsEn	1
4	X_00507F_WirelessLAN_AP.AdvancedSetting.IsolateMemWithIPEn	0
5	X_00507F_WirelessLAN_5G_AP.AdvancedSetting.ChannelList	
6	X_00507F_WirelessLAN_5G_AP.AdvancedSetting.IGMPSnoopingEn	1
7	X_00507F_WirelessLAN_5G_AP.AdvancedSetting.IsolateBandsEn	1

II-4-6 Support List

Mesh >> Support List

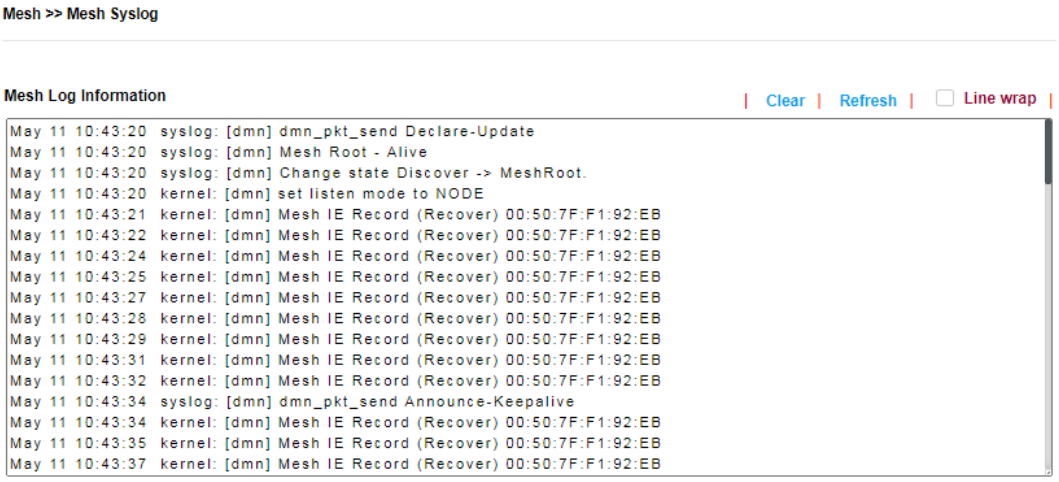
The following compatibility test lists Draytek AP models supported by this AP Mesh.

Model	Status	Firmware Version
VigorAP 906	Y	1.4.3

Y:Tested and is supported.

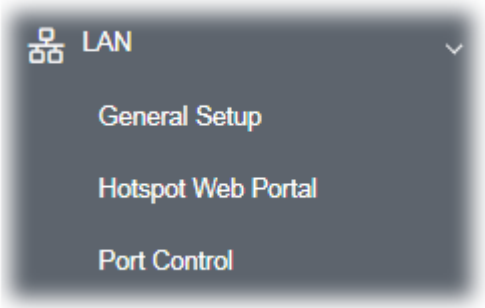
N:Not supported.

II-4-7 Mesh Syslog



II-5 LAN

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

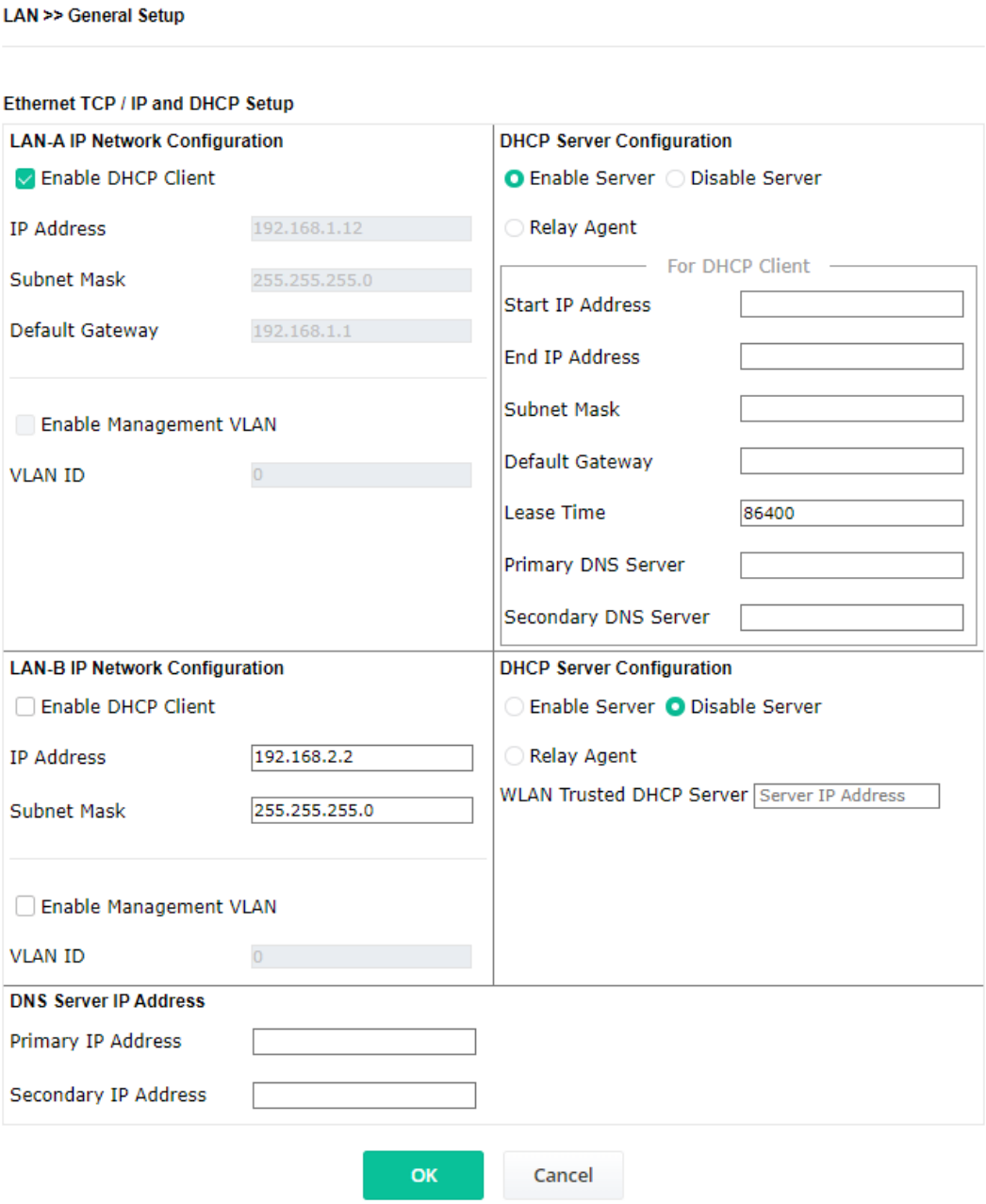


II-5-1 General Setup

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

Note:

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



Available settings are explained as follows:

Item	Description
LAN-A IP Network Configuration	**Enable DHCP Client** – When it is enabled, VigorAP 906 will be treated as a client and can be managed/controlled by the AP Management server offered by the Vigor router (e.g., Vigor2866). **IP Address** – Enter the private IP address for connecting to a local private network (Default: 192.168.1.2). **Subnet Mask** – Enter an address code that determines the size of the network. (Default: 255.255.255.0/ 24) **Default Gateway** - Enter an IP address. Traffic will be sent to the default gateway address of the specified interface. **Enable Management VLAN** – VigorAP 906 supports tag-based VLAN for wireless clients accessing Vigor devices. Only the clients with the specified VLAN ID can access VigorAP 906. • **VLAN ID** – Enter the number as VLAN ID tagged on the transmitted packet. “0” means no VLAN tag.

LAN-B IP Network Configuration	**Enable DHCP Client** – When it is enabled, VigorAP 906 will be treated as a client and can be managed/controlled by the AP Management server offered by the Vigor router (e.g., Vigor2866). **IP Address** – Enter the private IP address for connecting to a local private network (Default: 192.168.1.2). **Subnet Mask** – Enter an address code that determines the size of the network. (Default: 255.255.255.0/ 24) **Enable Management VLAN** – VigorAP 906 supports tag-based VLAN for wireless clients accessing Vigor devices. Only the clients with the specified VLAN ID can access VigorAP 906. • **VLAN ID** – Enter the number as VLAN ID tagged on the transmitted packet. "0" means no VLAN tag.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. A 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 an 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 a 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 use other DHCP servers to assign an IP address to every host in the LAN. • **WLAN Trusted DHCP Server (for LAN-B only)** - There is no right for this VigorAP to assign an IP address for another wireless LAN user. However, you can specify another valid DHCP server on another VigorAP to make the wireless LAN client obtaining the IP

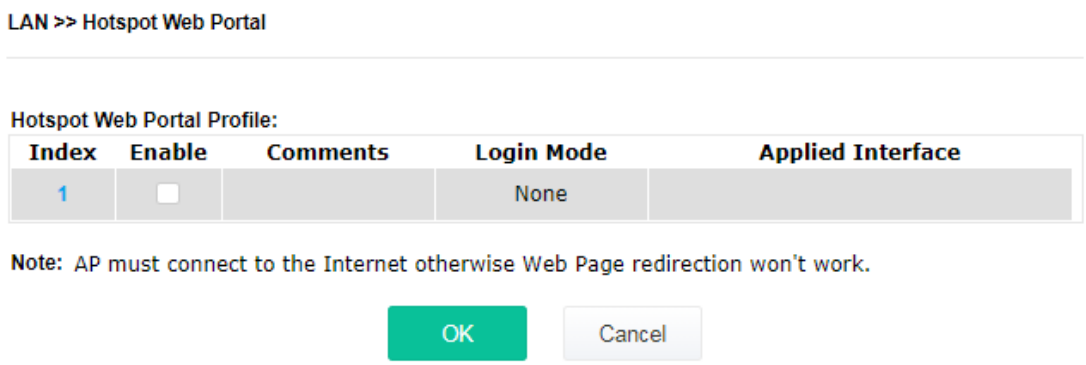
	address from the designated DHCP server. Specify a DHCP server in this field. All the IP addresses of the devices on the LAN of VigorAP will be assigned via such specified server. It is used to avoid IP assignment interference due to multiple DHCP servers in one LAN.
DNS Server IP Address	**Primary DNS 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 a 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-5-2 Hotspot Web Portal

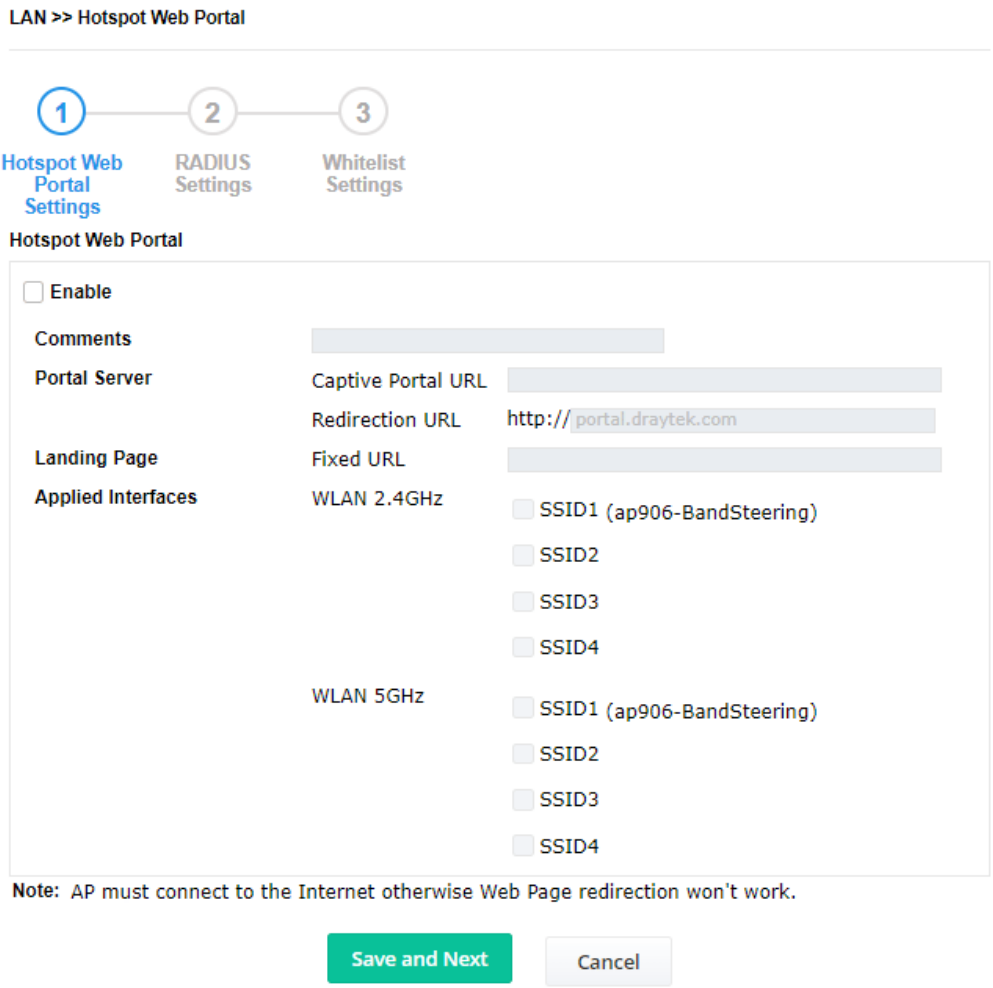
The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions or authenticate themselves, before gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials and the broadcast of public service announcements.

Click **LAN** to open the LAN settings page and choose **Hotspot Web Portal**. Follow the on-screen steps to configure settings.



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

(1) Hotspot Web Portal Settings



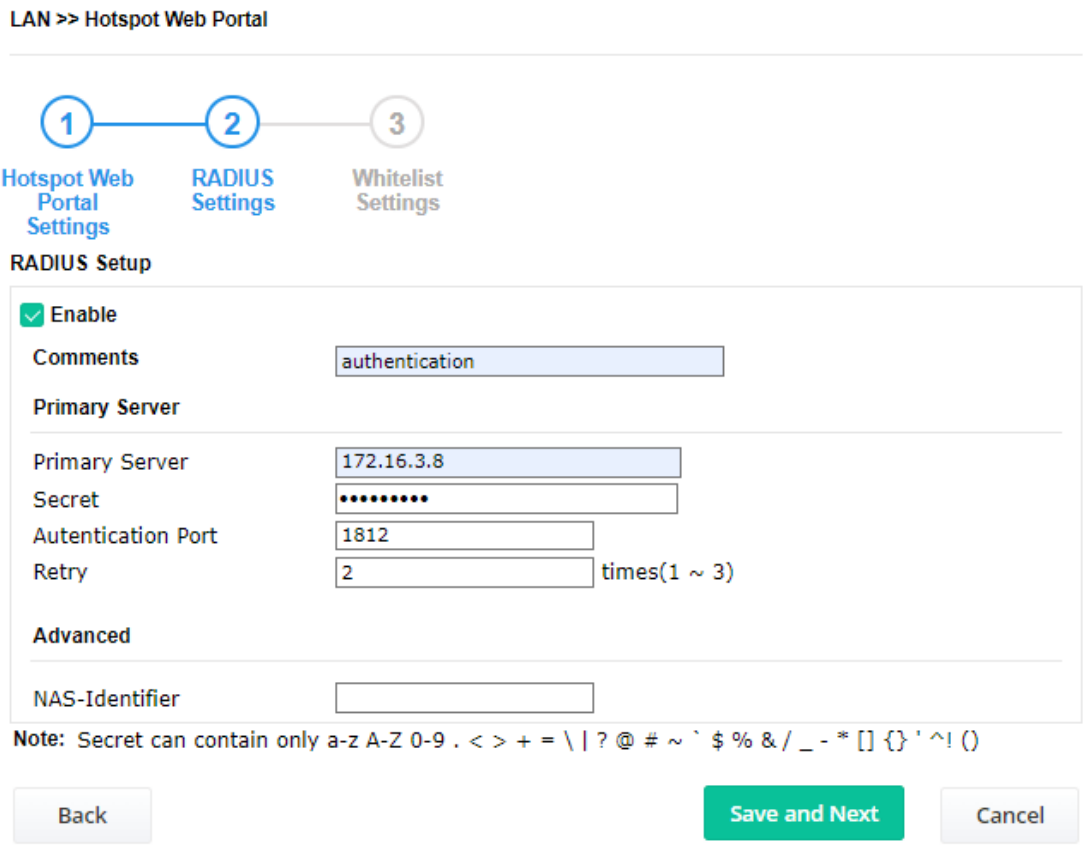
Available settings are explained as follows:

Item	Description
Enable	Check it to enable the hotspot web portal settings.
Comments	Enter a brief description for this profile.
Portal Server	**Captive Portal URL -** Enter the captive portal URL. **Redirection URL -** Enter the URL to which the client will be redirected.
Landing page	**Fixed URL** - Enter the URL as the landing page for wireless clients.
Applied Interfaces	**SSID1 to SSID4** - The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Save and Next	Click to access into next page.

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

(2) RADIUS Settings

Configure the external RADIUS server for mutual authentication.

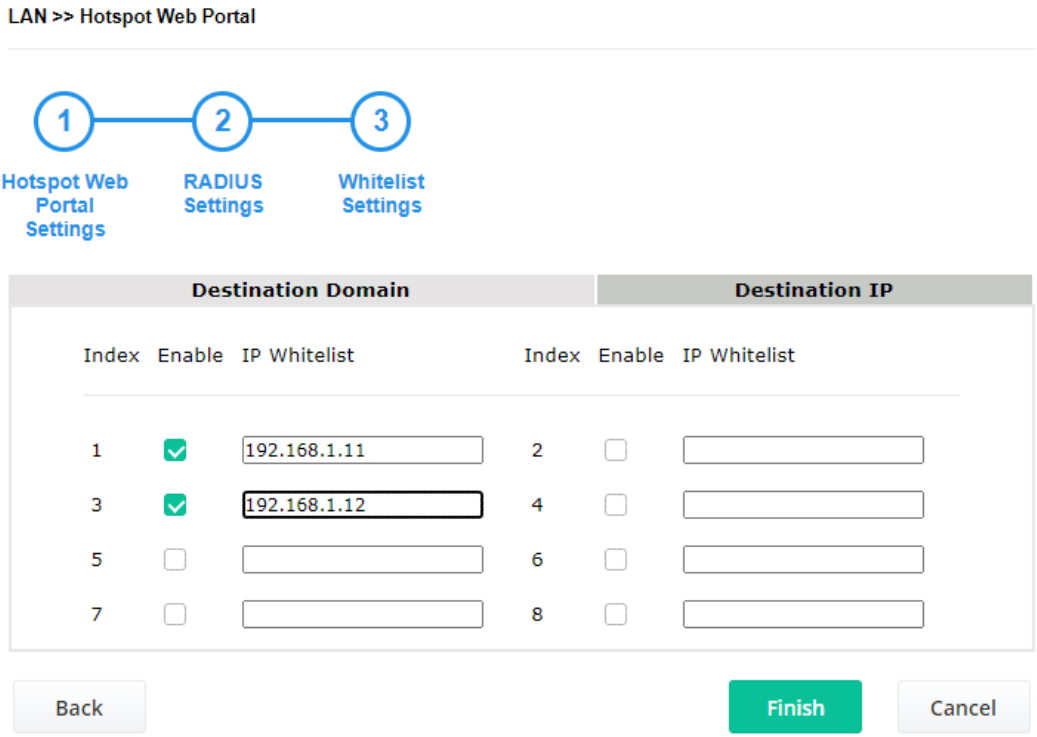


Item	Description
Enable	Check it to enable the RADIUS server settings.
Comments	Enter a brief description for this profile.
Primary Server	Enter the IP address of the RADIUS server.
Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides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

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

(3) Whitelist Settings

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

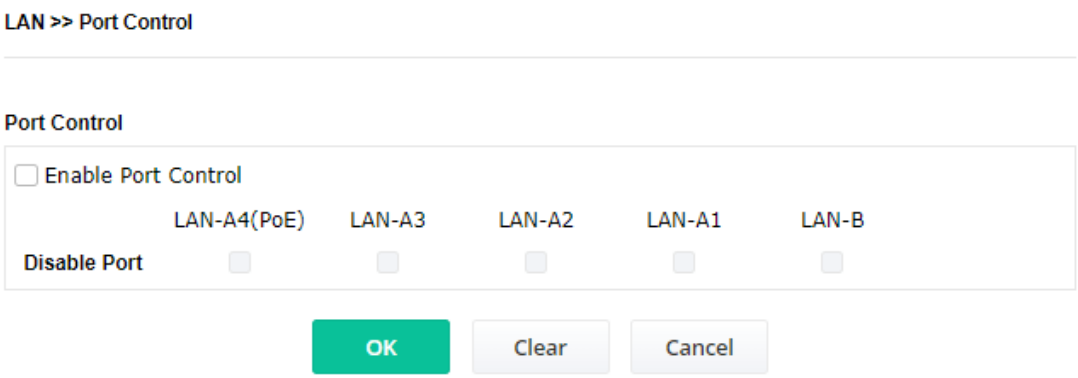


Destination Domain	
Enable	Check to enable the setting.
Domain Whitelist	Enter a domain (URL) / an IP address.
Destination IP	
Enable	Check to enable the setting.
IP Whitelist	LAN users with the IPs set on this page can access the Internet without entering other portals.
Finish	Click to save the settings.

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

II-5-3 Port Control

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



Available settings are explained as follows:

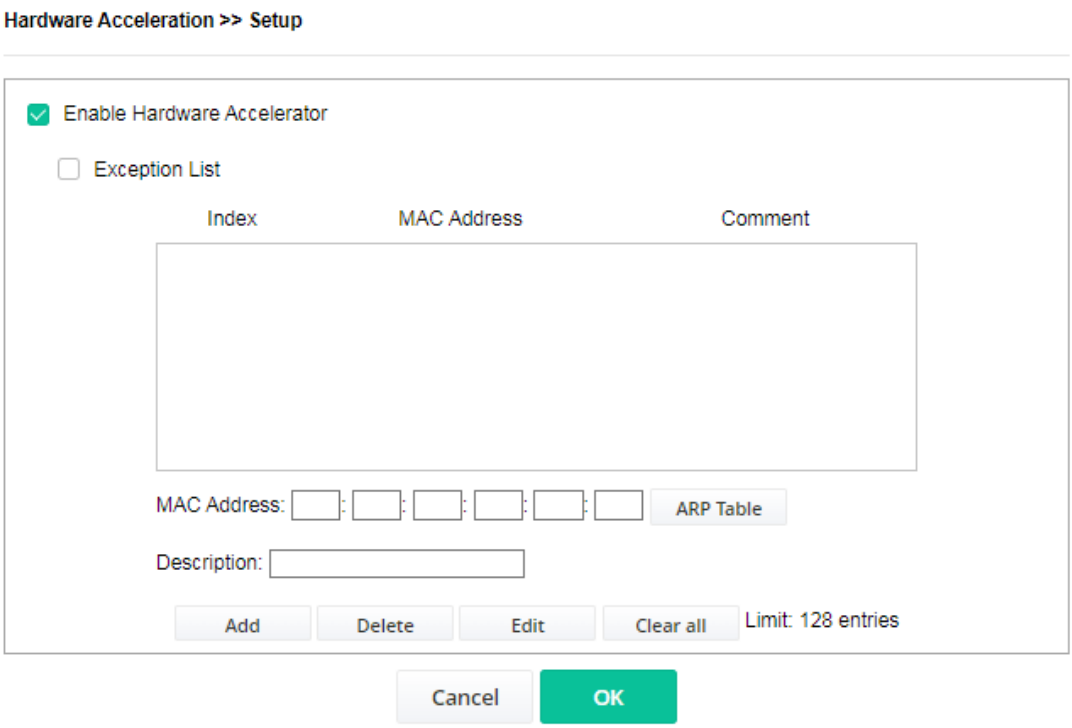
Item	Description
Enable Port Control	Check it to enable the port control. If it is enabled, you are allowed to disable the function of the physical LAN port by checking the corresponding check box.
Disable Port	Choose and check the LAN port.

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

II-5-4 Hardware Acceleration

Hardware Acceleration is also called **PPA** in DrayTek for it is based on **Protocol Processing Engine (PPE)** of Infineon. It can only support 4096 sessions for network traffic (IN & OUT).

When the data traffic is heavy and data transmission is getting slowly and slowly, you can configure this page to accelerate the data streaming by hardware itself. Open **Hardware Acceleration** to access into the following page:



Available settings are explained as follows:

Item	Description
Enable Hardware Acceleration	**Disable** – The default setting. **Enable** - Choose to enable the hardware acceleration function.
Exception List	If you want to restrict some users/clients from transmitting data through the router by using the hardware acceleration function, check this box to create an exclusion list. **MAC Address** - Enter the MAC address of the client. **ARP Table** - Click to select the client listed on the ARP table. Then, the MAC address of the selected client will be shown on the MAC Address field. **Description** - Enter a brief explanation for the selected client.

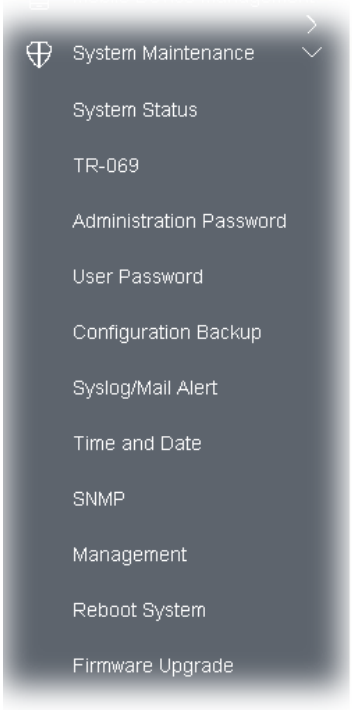
After finishing this web page configuration, please click **OK** to save the settings.

Chapter III Management

III-1 System Maintenance

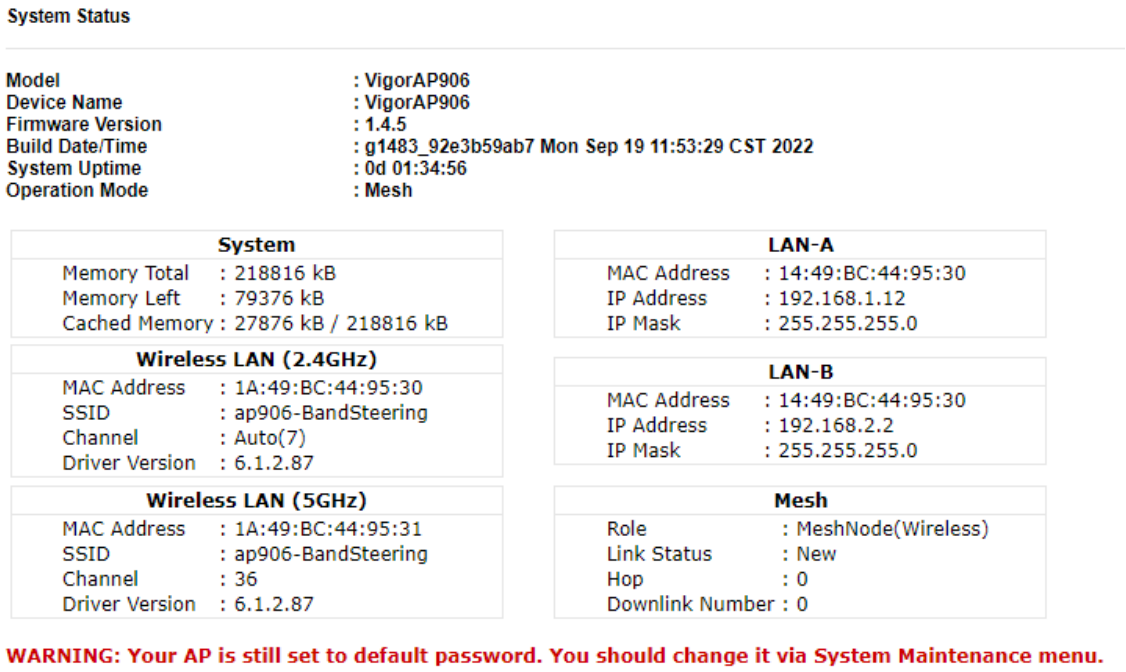
For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Configuration Backup, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



III-1-1 System Status

The **System Status** provides basic network settings of the 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.

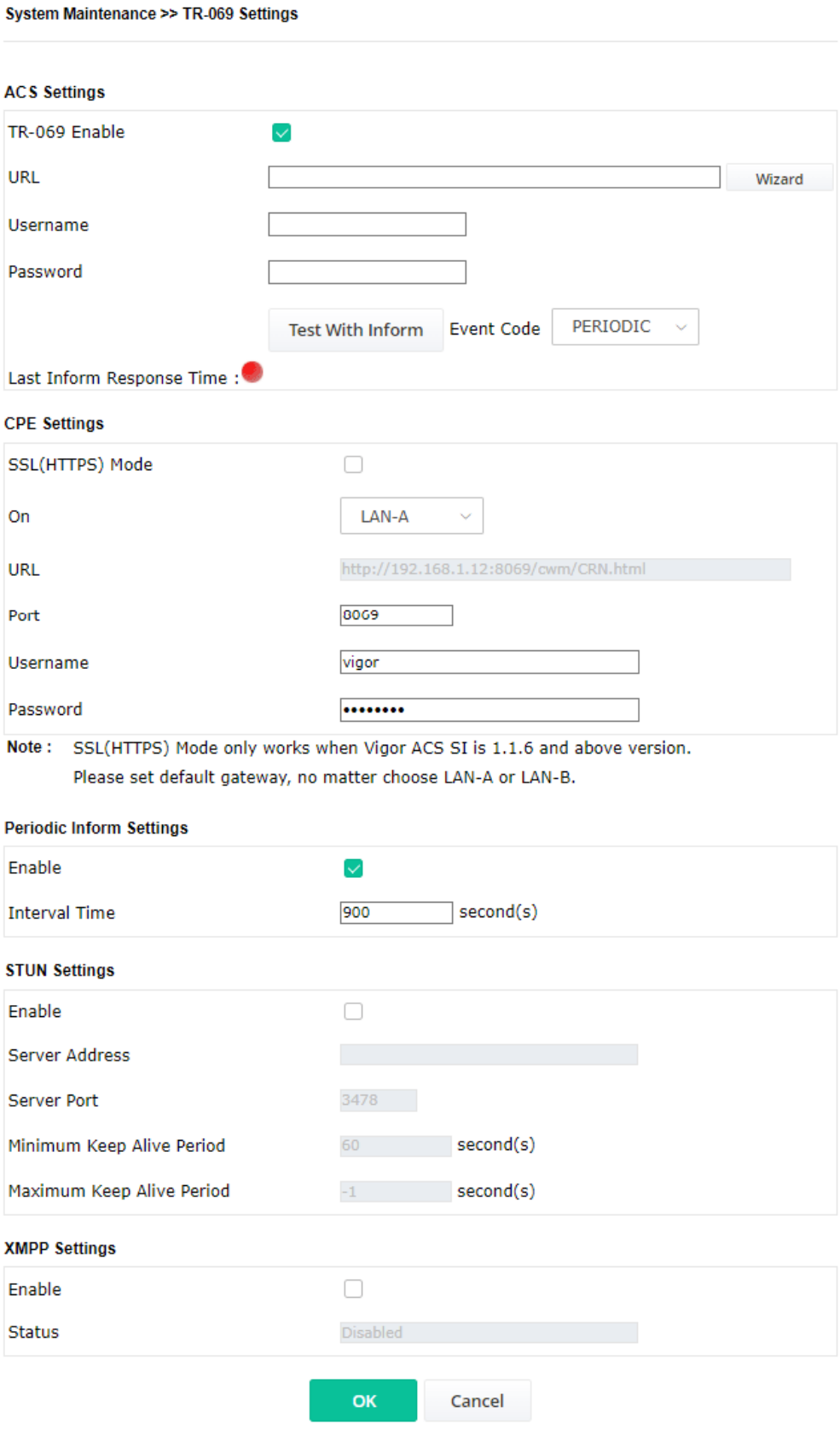


Each item is explained as follows:

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 the 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/5GHz)	
MAC Address	Display the MAC address of the WAN Interface.
SSID	Display the SSID of the device.
Channel	Display the channel that the station used for connecting with such a device.

III-1-2 TR-069

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



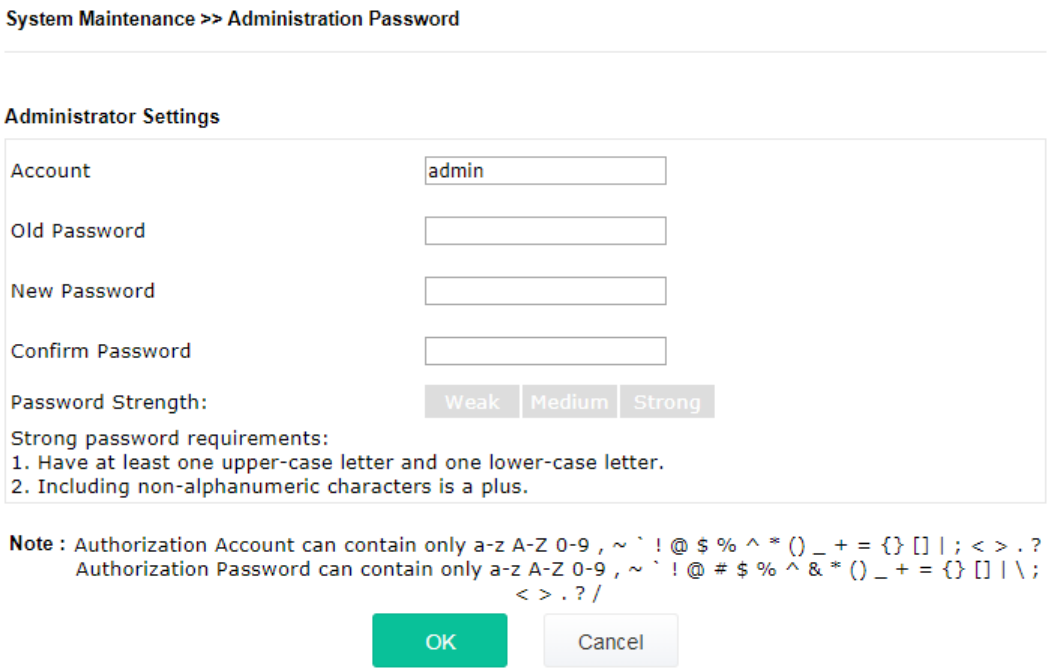
Available settings are explained as follows:

Item	Description
ACS Settings	**TR-069 Enable** - Select to enable TR-069 settings. **Wizard** – Click it to enter the IP address of the 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 the 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 can communicate with the VigorACS server. **Event Code** – Use the drop-down menu to specify an event to perform the test. **Last Inform Response Time** – Display the time that the VigorACS server made a response while receiving Inform message from CPE last time.
CPE Settings	Such information is useful for Auto Configuration Server (ACS). **SSL(HTTPS) Mode** - Check the box to allow the CPE client to connect with ACS through SSL. **On** – Choose the interface (LAN-A or LAN-B) for VigorAP 906 connecting to the ACS server. **Port** – Sometimes, port conflict might occur. To solve this problem, you might change the port number for CPE. **Username/Password –** Type the username and password that VigorACS can use to access such CPE.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the AP to send a notification to the VigorACS server. **Interval Time** – Type the value for the interval time setting. The unit is "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 send a binding request to the server to maintain 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 send a binding request to the server to maintain the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
XMPP Settings	XMPP is an abbreviation of Extensible Messaging and Presence Protocol. If your AP register to XMPP server, it could help VigorACS to manage the AP **under the NAT** at any time, without obstruction.

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

III-1-3 Administrator Password

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



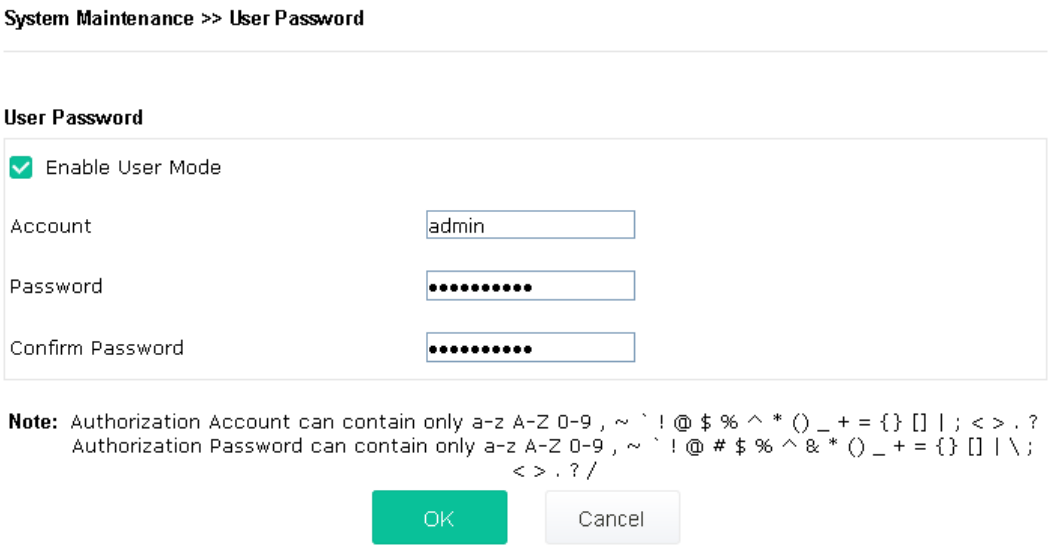
Available settings are explained as follows:

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

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

III-1-4 User Password

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



Available settings are explained as follows:

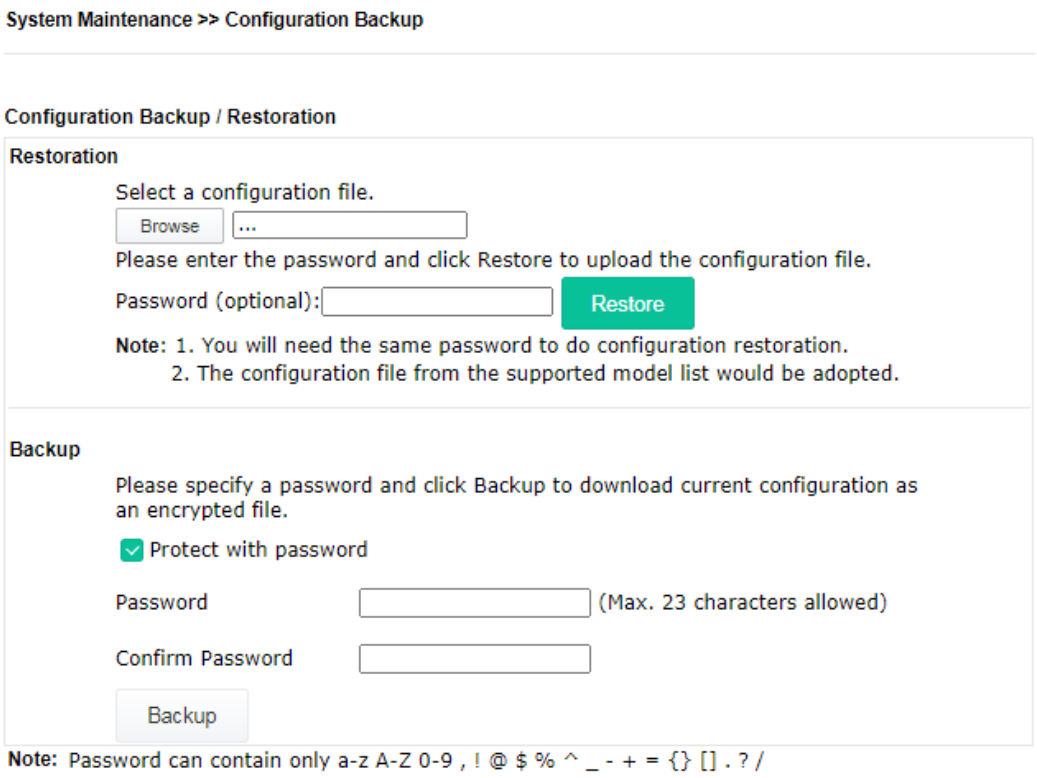
Item	Description
Enable User Mode	After checking this box, you can access the web user interface with the password typed here for simple web configuration. The settings on a simple web user interface will be different from a full web user interface accessed by using the administrator password.
Account	Enter a user name.
Password	Enter a 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 a function can be used to backup/restore the VigorAP 906 settings.



Available settings are explained as follows:

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

Follow the steps below to backup your configuration.

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

Note:

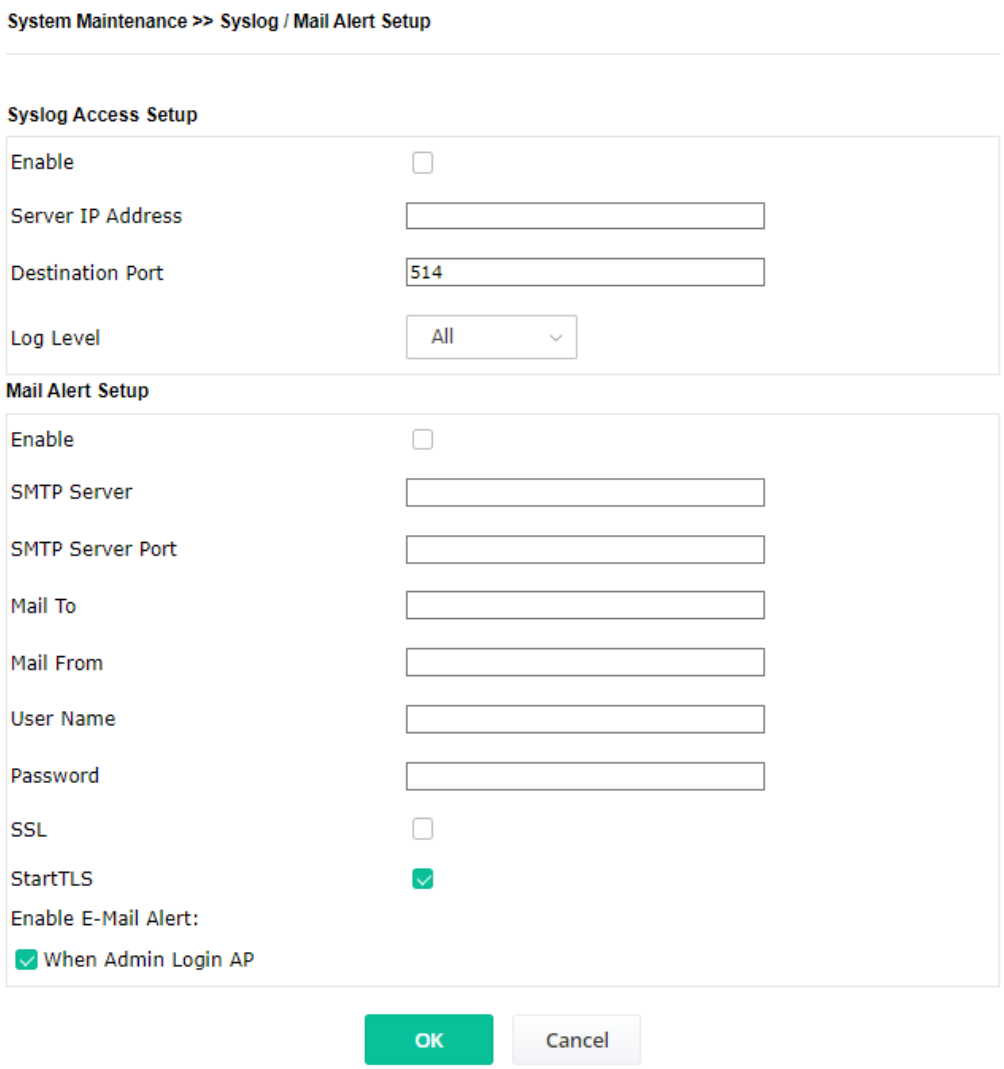
Backup for Certification must be done independently. The Configuration Backup does not include information on the Certificate.

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 the equipment.



Available settings are explained as follows:

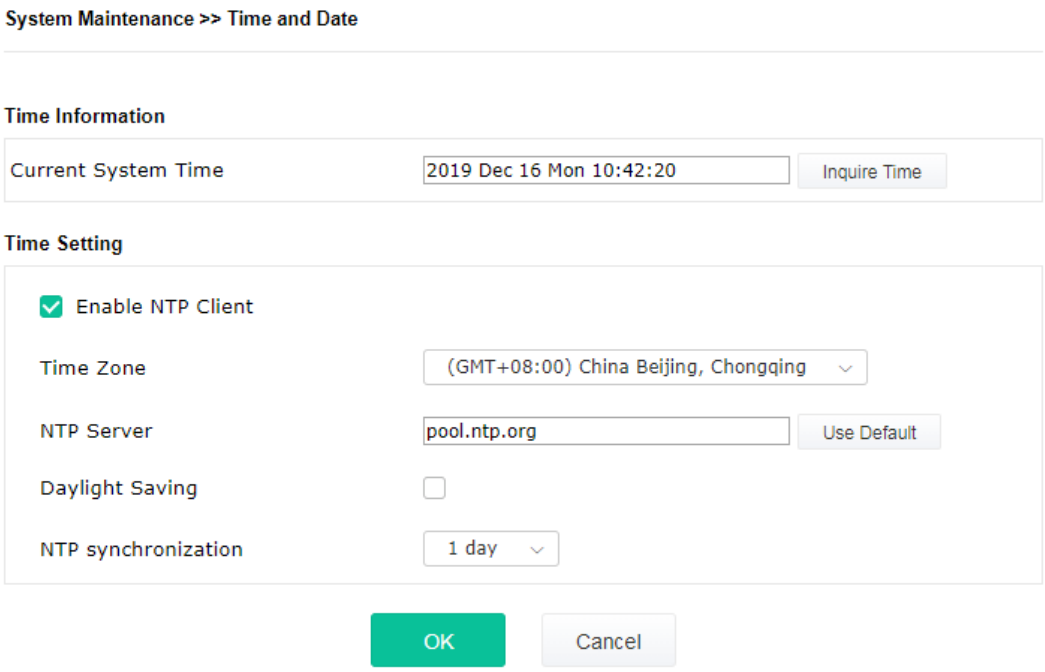
Item	Description
Syslog Access Setup	**Enable** - Check **Enable** to activate the function of Syslog. **Server IP Address** -The IP address of the Syslog server. **Destination Port** -Assign a port for the Syslog protocol. The default setting is 514. **Log Level** - Specify which level of the severity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

	Mail From - Assign a path for receiving the mail from outside. **User Name** - Type the user name for authentication. **Password** - Type the password for authentication. **SSL** - Check this box to enable SSL certificate for the SMTP server. **StartTLS** - Check this box to encrypt alert mail. However, if the SMTP server specified here does not support TLS protocol, the alert mail with encrypted data will not be received by the receiver. **Enable E-Mail Alert** - VigorAP will send an e-mail out when a user accesses 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 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.



Available parameters are explained as follows:

Item	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 the 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.

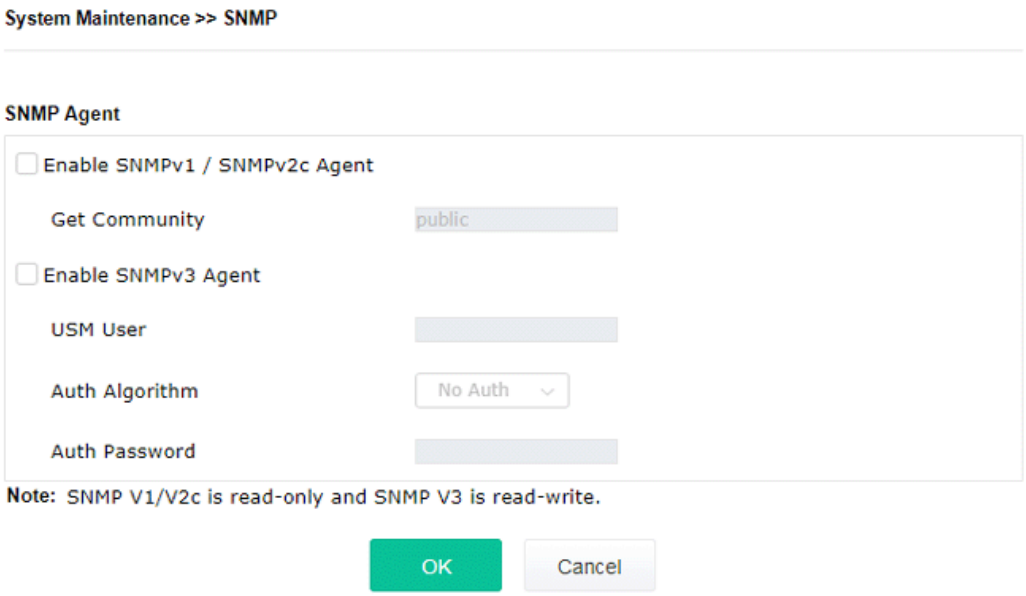
Daylight Saving	Check the box to enable daylight saving. This feature is available for a certain area.
NTP synchronization	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

III-1-8 SNMP

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

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



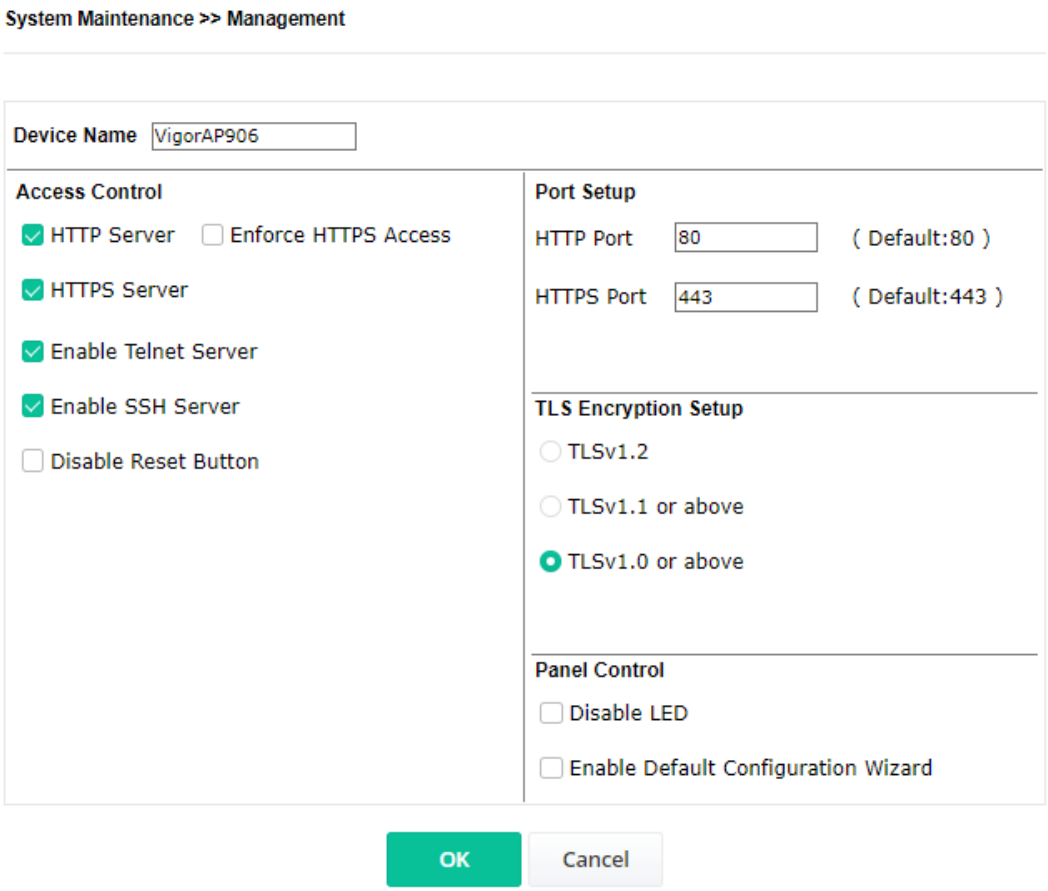
Available settings are explained as follows:

Item	Description
Enable SNMPv1/SNMPv2c 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 that 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 servers.



Available parameters are explained as follows:

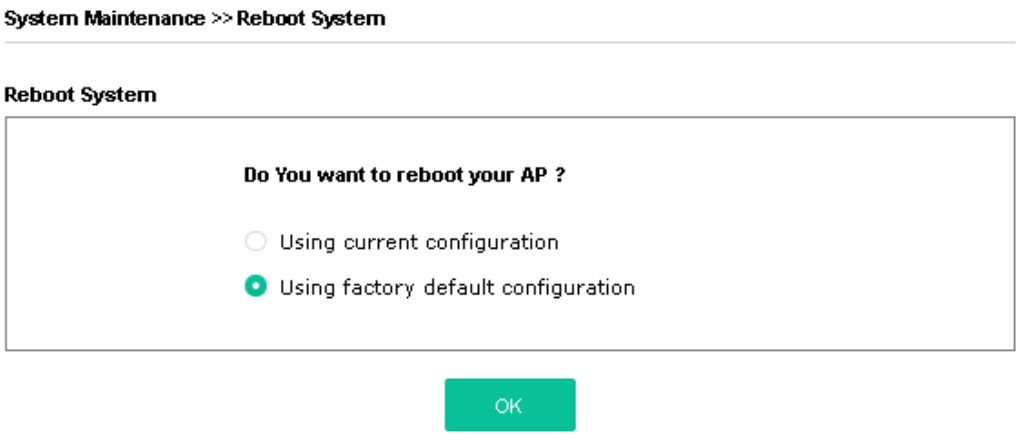
Item	Description
Device Name	The default setting is VigorAP 906. Change the name if required.
Access Control	Check the box(es) listed in this area to enable the various servers.
Port Setup	**HTTP port/HTTPS port** -Specify user-defined port numbers for the HTTP and HTTPS servers.
TLS Encryption Setup	**TLSv1.2/ TLSv1.1 or above/TLSv1.0 or above –** Check the box to enable TLS encryption protocols. For improved security, the HTTPS servers that are built into the router have been upgraded to TLS 1.x protocol.
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** – The 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.

Note:

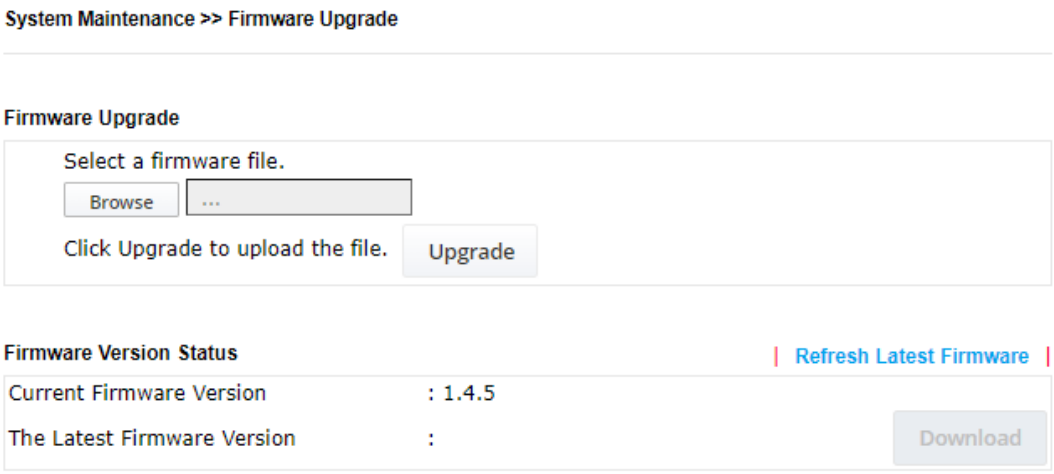
When the system pops up Reboot System web page after configuring the web settings, please click **OK** to reboot your device for ensuring normal operation and preventing unexpected errors of the modem in the future.

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 website or FTP site. The DrayTek website is www.draytek.com (or local DrayTek's web site) and the FTP site is ftp.draytek.com.

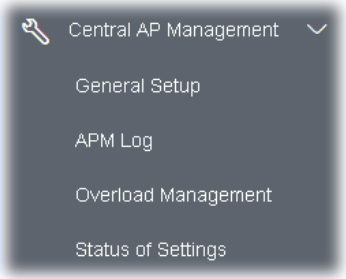
Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.



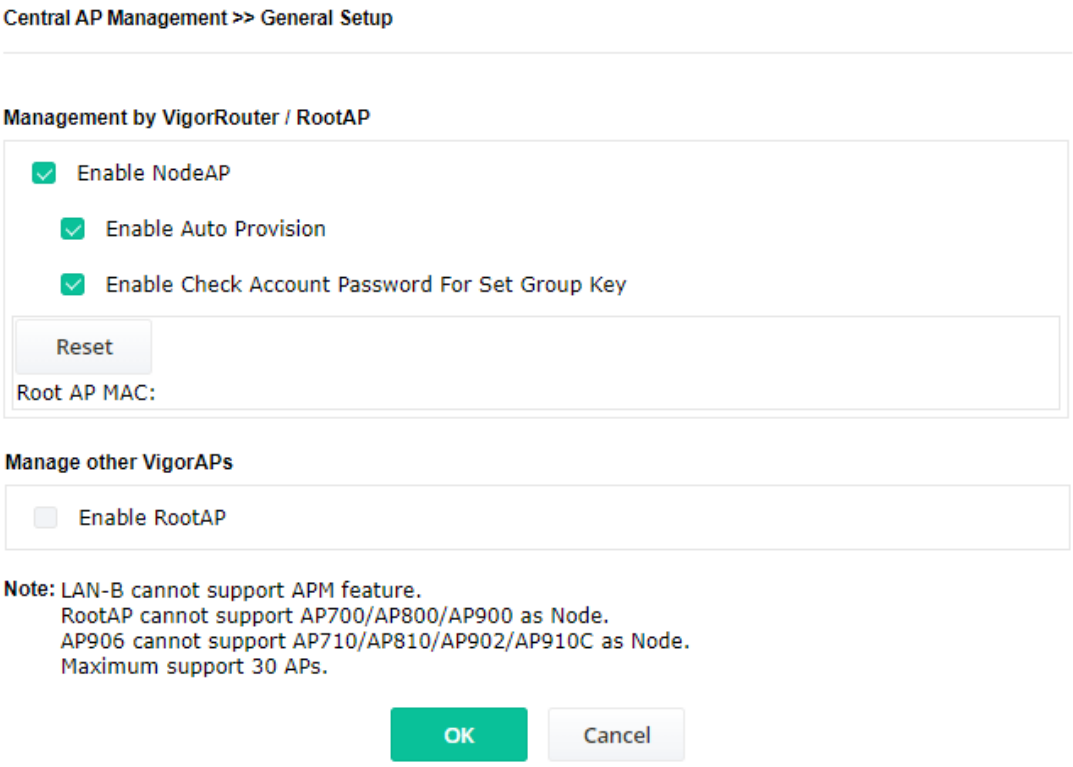
Click **Download** to locate the newest firmware from your hard disk and click **Upgrade**.

III-2 Central AP Management

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



III-2-1 General Setup



Available settings are explained as follows:

Item	Description
Management by VigorRouter/RootAP	
Enable NodeAP	Check the box to enable the function of AP Management (APM). **Enable Auto Provision -** VigorAP 906 can be controlled under Central AP Management in the Vigor router. When both the Vigor router series and VigorAP 906 have such feature enabled, once VigorAP 906 is registered to the Vigor router series, the **WLAN profile** pre-configured on the Vigor router series will be applied to VigorAP 906 immediately. Thus, it is not necessary to configure VigorAP 906 separately.

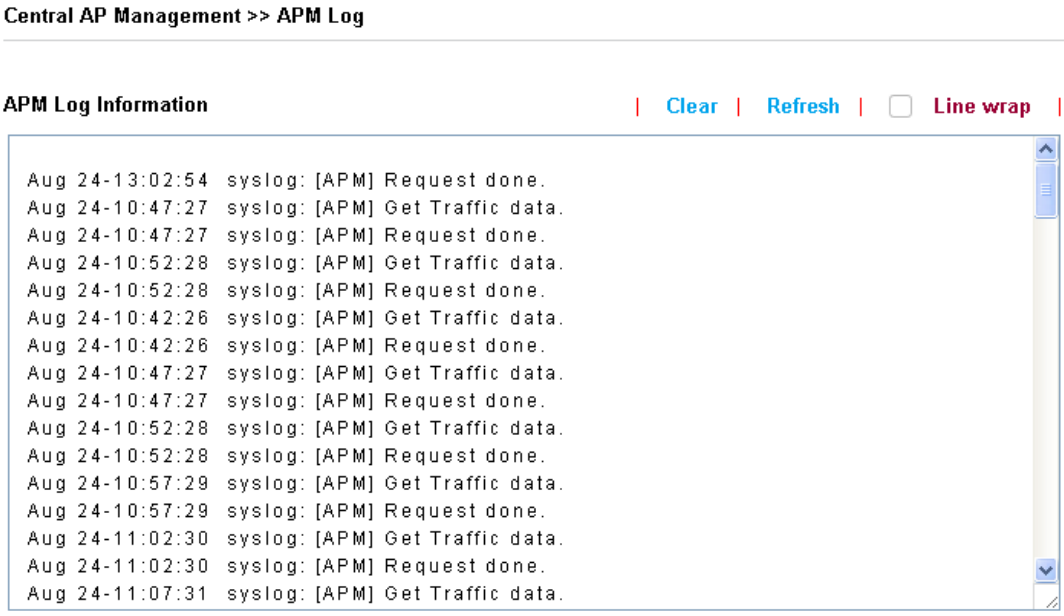
Manage other VigorAPs	
Enable RootAP	Check this box to enable AP management. The role of this AP is "Root".

Click **OK** to save these settings.

III-2-2 APM Log

This page will display log information related to wireless stations connected to VigorAP 906 and central AP management.

Such information also will be delivered to the Vigor router (e.g., Vigor2865 or Vigor2927 series) and be shown on **Central AP Management>>Event Log** of Vigor router.

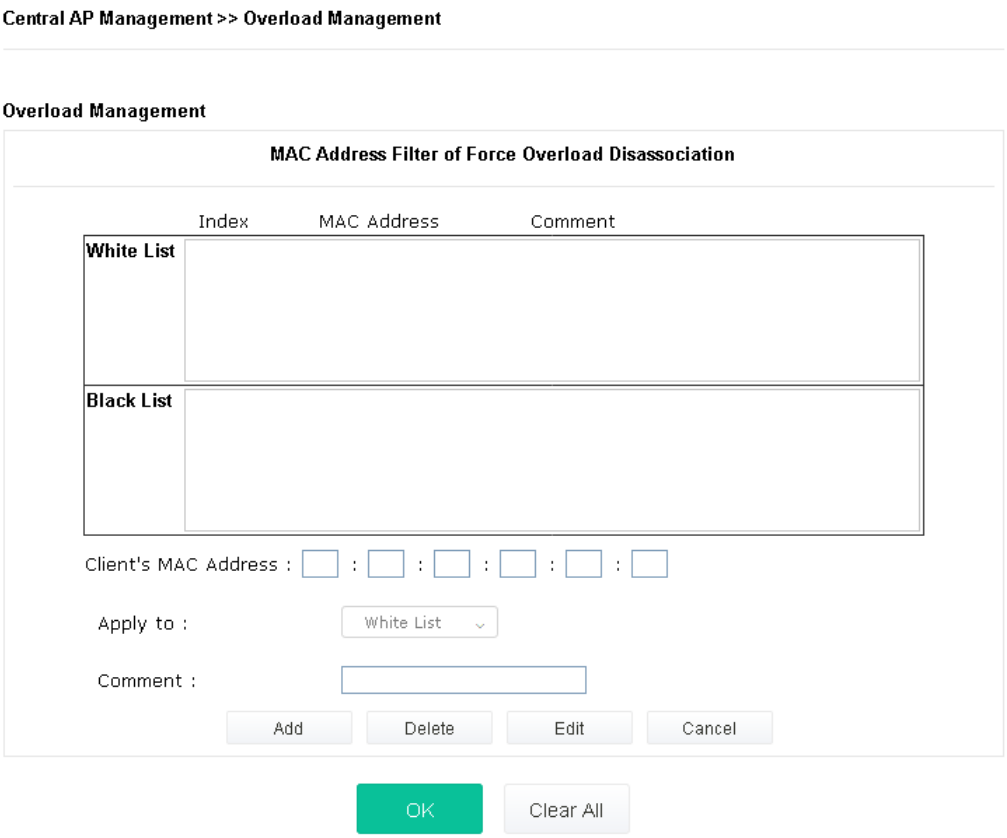


III-2-3 Overload Management

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 906) registered to the Vigor router. Thus, the bandwidth will not be occupied by certain access points.

However, traffic overload might occur if too many wireless stations are connected to VigorAP 906 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 the web user interface of the Vigor router is enabled, wireless clients specified in the **Black List** of such web page will be disassociated to solve the problem of traffic overload.

The following web page is used to configure the white list and the Black List for wireless stations.



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 the members in White List. **Black List** - MAC address listed inside Client's MAC Address will be categorized as one of the members in Black List.

Comment	Type a brief description for the specified client's MAC address.
Add	Add a new MAC address into the White List/Black List.
Delete	Delete the selected MAC address in the White List/Black List.
Edit	Edit the selected MAC address in the White List/Black List.
Cancel	Give up the configuration.

Click **OK** to save these settings.

III-2-4 Status of Settings

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 906) registered to Vigor 2865 or Vigor2927 series. This web page displays the settings related to Load Balance for VigorAP 906. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor 2865 or Vigor2927 series.

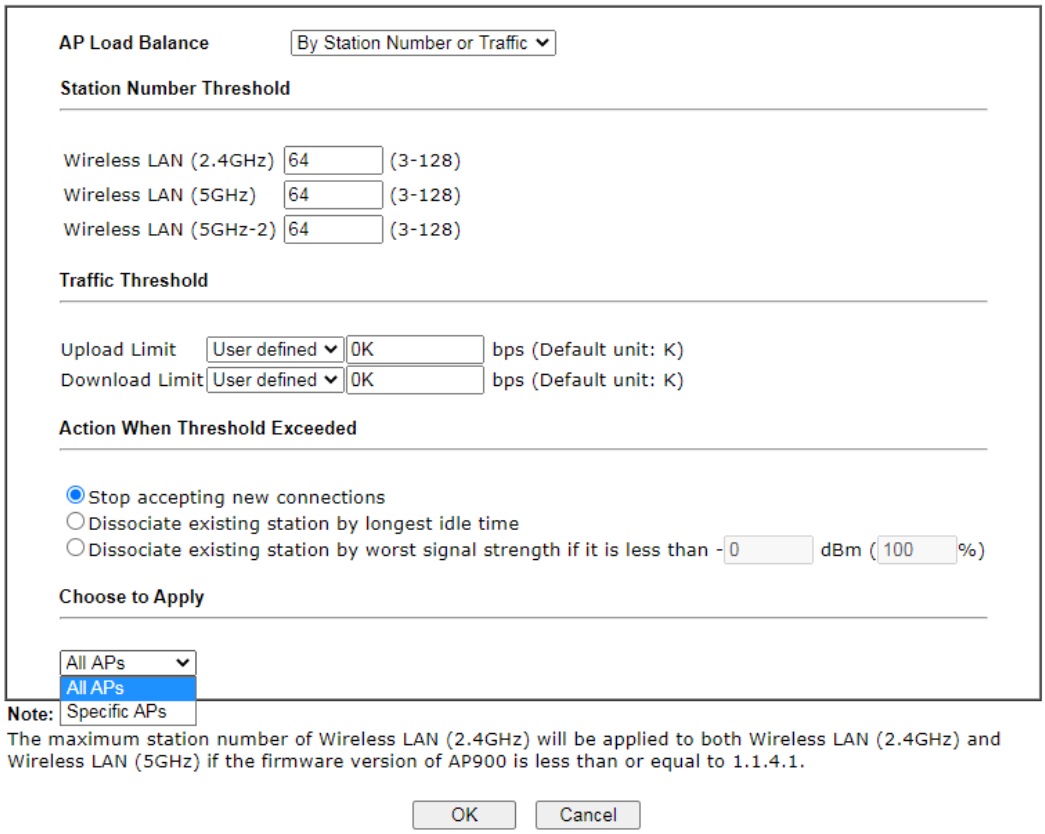
Central AP Management >> Status of Settings

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

"X" means the function is not enabled or VigorAP 906 has not registered to any Vigor router yet.

Below shows a setting example for Load Balance settings configured in Vigor 2865 or Vigor2927 series.

Central Management >> AP >> Load Balance



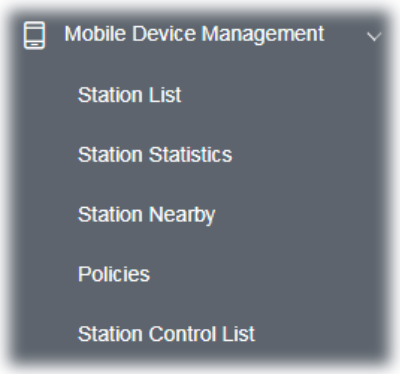
Note:
The maximum station number of Wireless LAN (2.4GHz) will be applied to both Wireless LAN (2.4GHz) and Wireless LAN (5GHz) if the firmware version of AP900 is less than or equal to 1.1.4.1.

OK Cancel

III-3 Mobile Device Management

Such a 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).

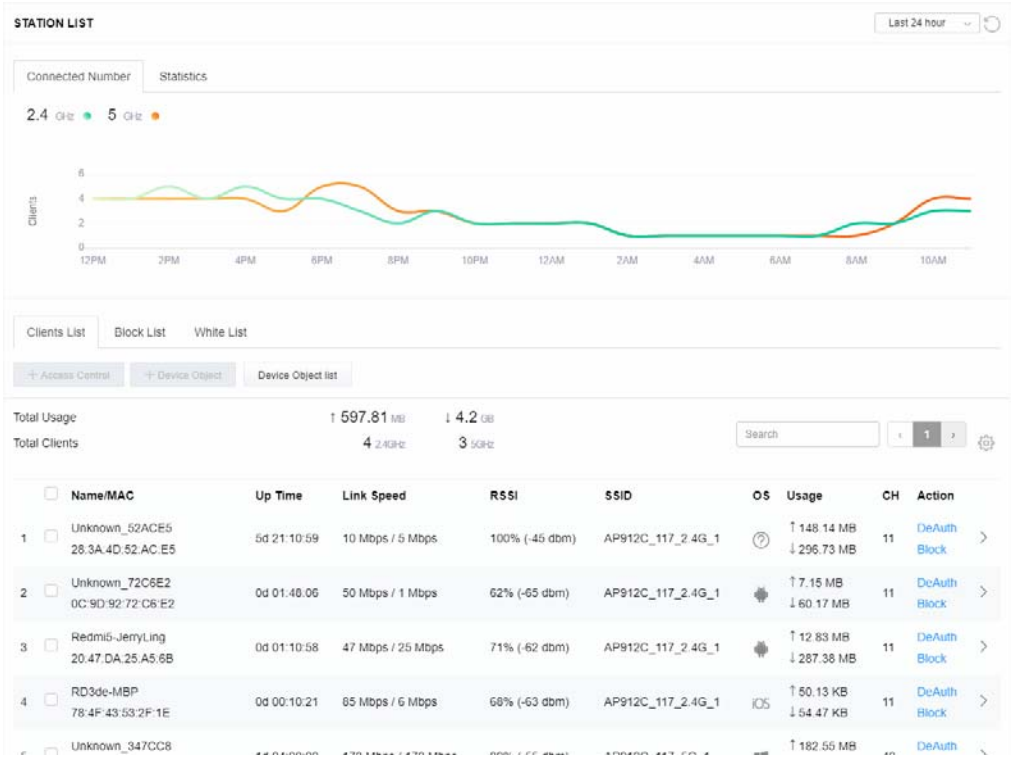


III-3-1 Station List

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 lists.

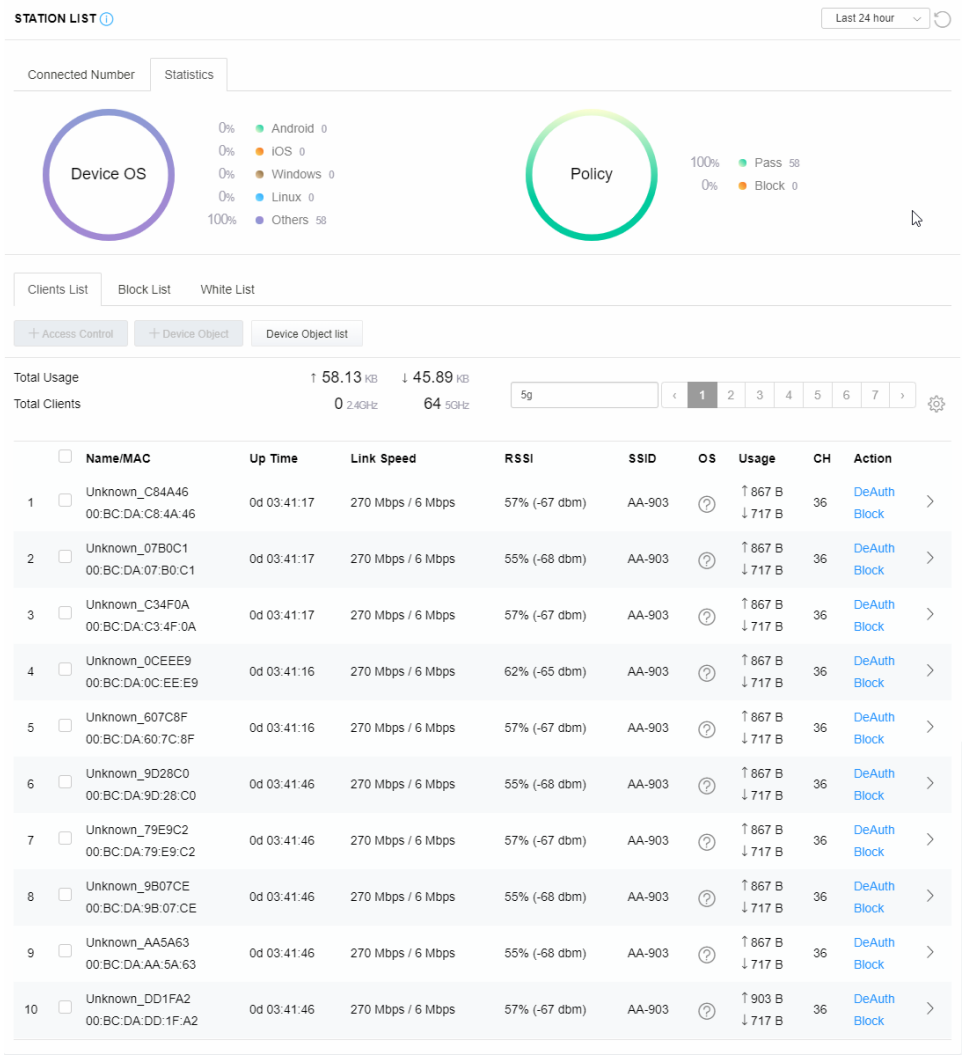
III-3-1-1 Connected Number

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



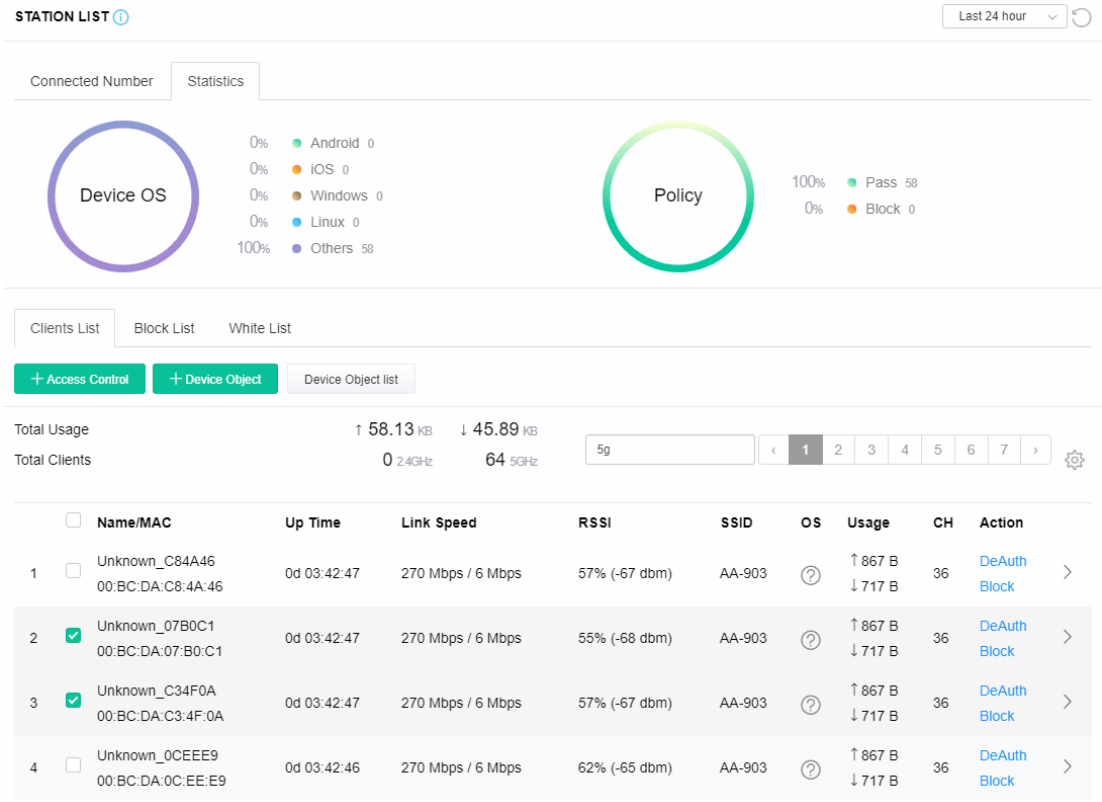
III-3-1-2 Statistics

The number of detected devices and the number of devices passed/blocked according to the policy specified in **Mobile Device Management>>Policies** can be illustrated as a doughnut chart.

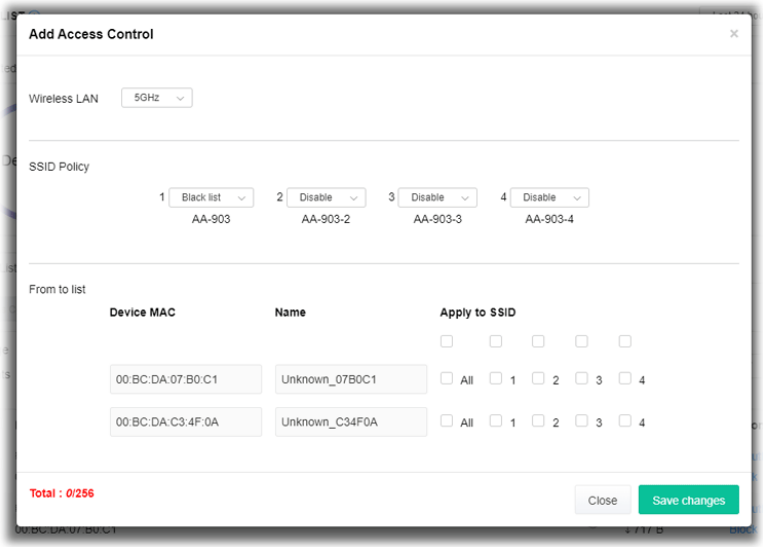


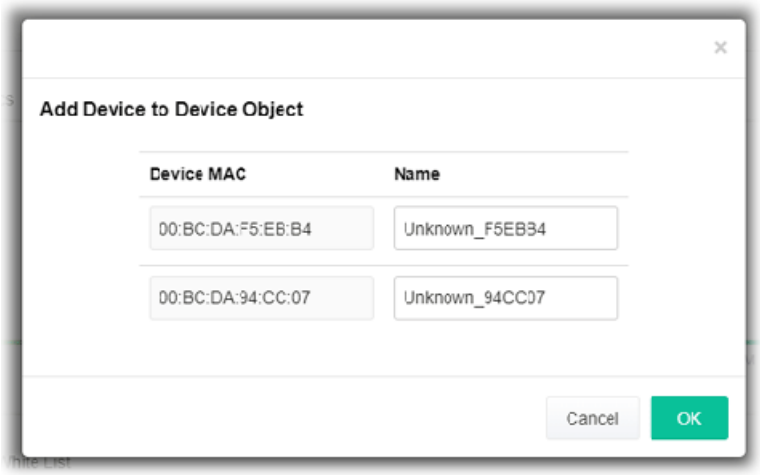
III-3-1-3 Clients List

The client list displays all the stations connecting to VigorAP.



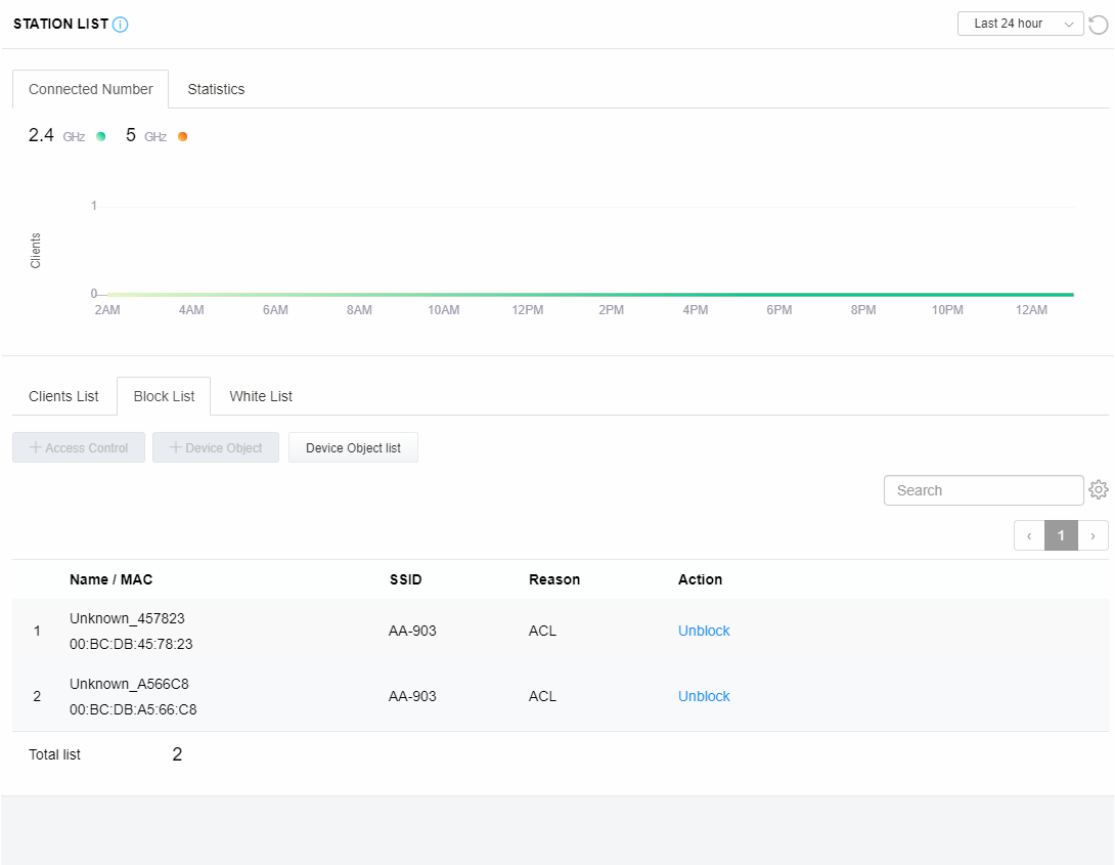
Available settings are explained as follows:

Item	Description
+Access Control	It is available after choosing one of the entries (clients) on the Clients List.  **Wireless LAN** - Specify the bandwidth for the access control list. **SSID Policy** - Set the policy for each SSID as a blacklist or whitelist or disable. **From to list** - Display the clients available for applying this access

	control. **Apply to SSID** - Check **All** to make the device apply the policies to all SSIDs. Or select the one(s) to make the device apply the policies to the selected SSIDs. **Close** - Exit this page without saving any changes. **Save changes** - Save the changes and exit this page.
+Device Object	To add a device to the device object list, choose one of the entries (clients) on the Clients List to enable the Device Object button. Click the button to open the following page.  Check the information listed on the page. Change the MAC address or name of the selected entry if required. Then click **OK** and exit the page.
Device Object list	The existed device object profiles will be shown on the following page.
Clients List	Display the stations connecting to this Vigor device. **Total Usage** - Display **Total Clients** - Display the number of the clients using 2.4GHz **Name / MAC** - Display the host name / MAC address of the connecting client. **Up Time** - Display the connection time. **Link Speed** - Display the link speed. **RSSI** - Display the RSSI value. **SSID** - Display the SSID the client used for connecting VigorAP. **OS** - Display the OS of the client. **Usage** - Display the bandwidth usage (up and down) of the client. **CH** - Display the channel used by the client. **Action** - Display the authentication method used by the client, and if it is on the block list or white list.

II-3-13-4 Block List

This page displays information on the stations under the block list.

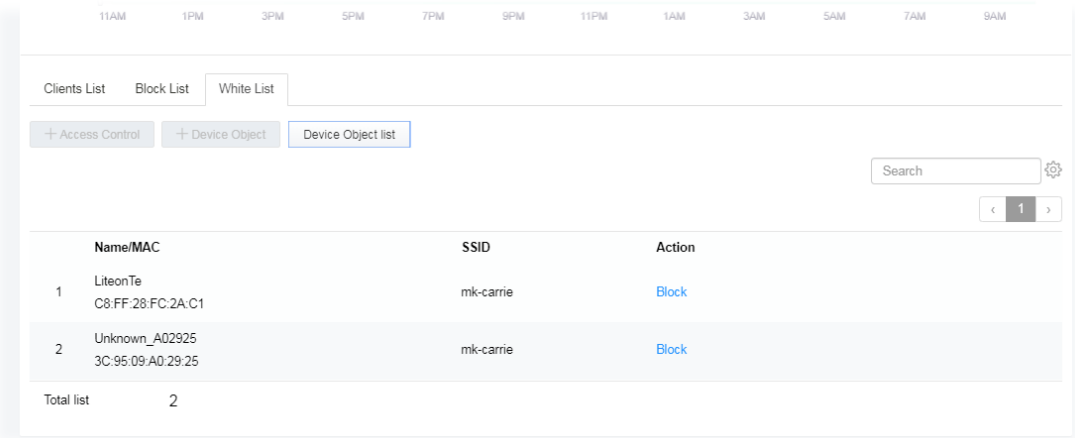


Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless 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 about the stations under the white list.

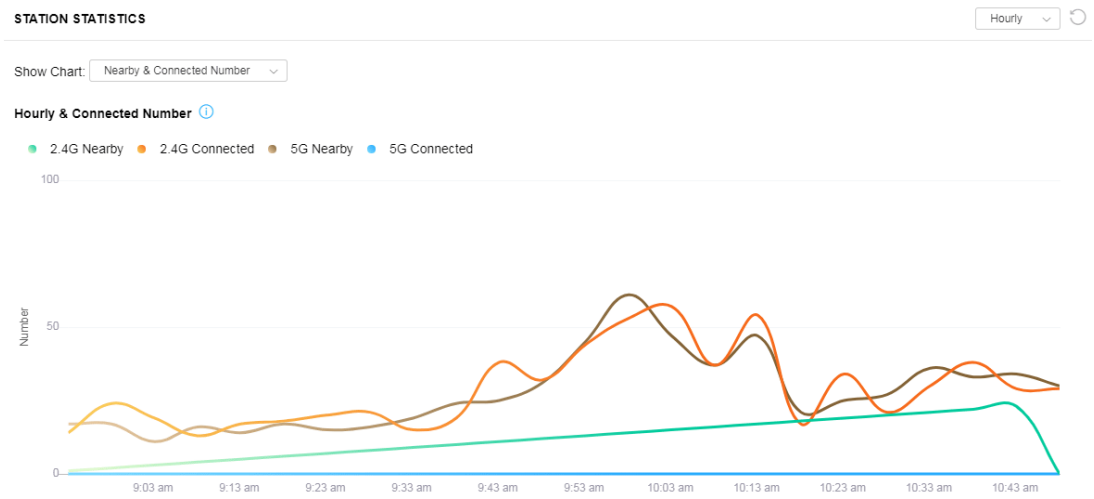


Available settings are explained as follows:

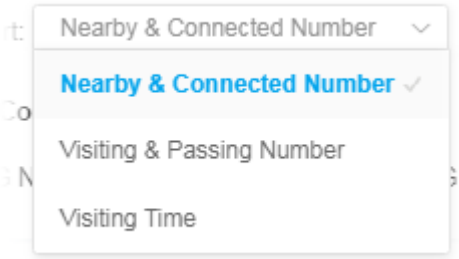
Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Action	Display the action that you can execute for the station. **Block** - Click to block the entry.

III-3-2 Station Statistics

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

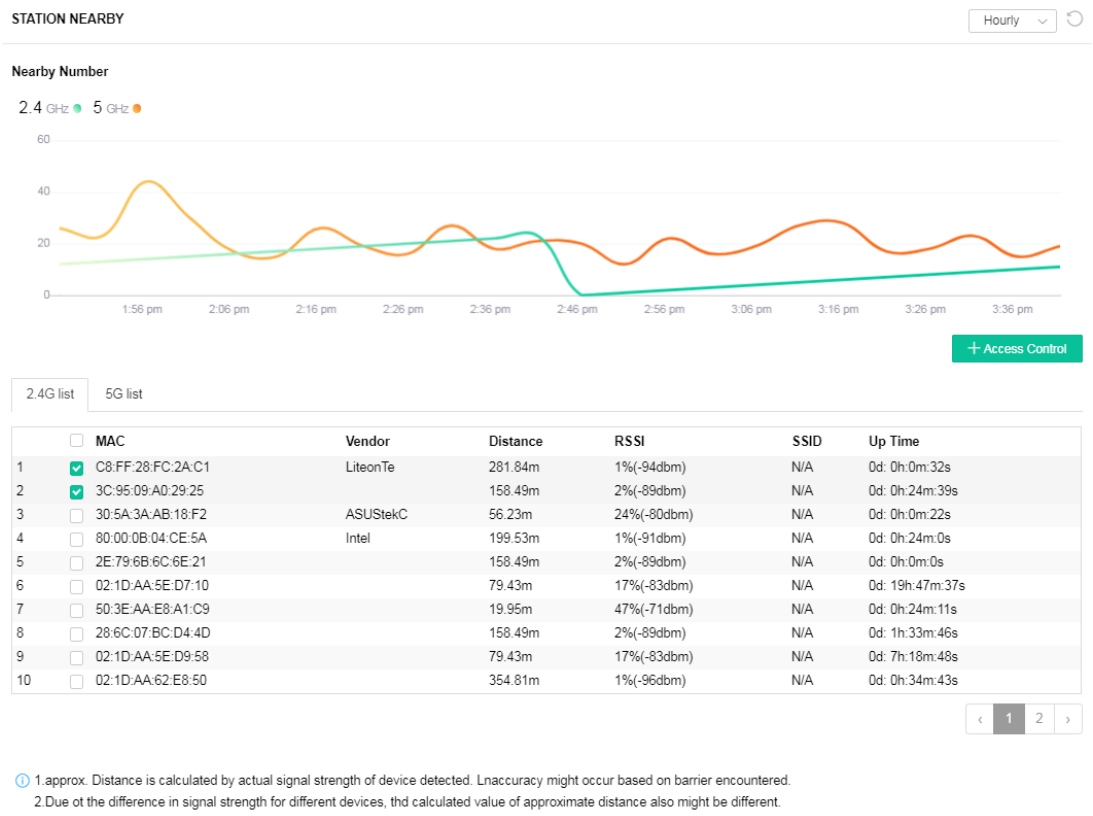


Available parameters are explained as follows:

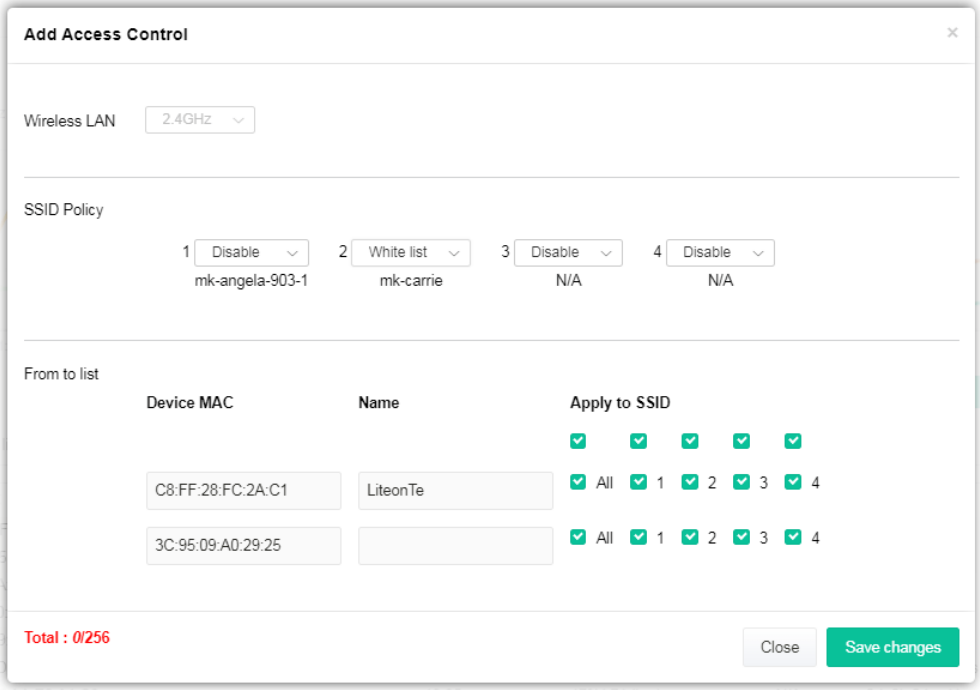
Item	Description
Show Chart	Choose one of the items to display the statistics chart for wireless stations.  **Nearby & Connected Number** – Choose it to have the statistics of the wireless stations which is nearby and connected to VigorAP 906. **Visiting & Passing Number** – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP 906. **Visiting Time** - Choose it to have the statistics of the wireless stations which is visiting VigorAP 906.

III-3-3 Station Nearby

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 like the one(s) to pass through VigorAP or to be blocked by VigorAP.

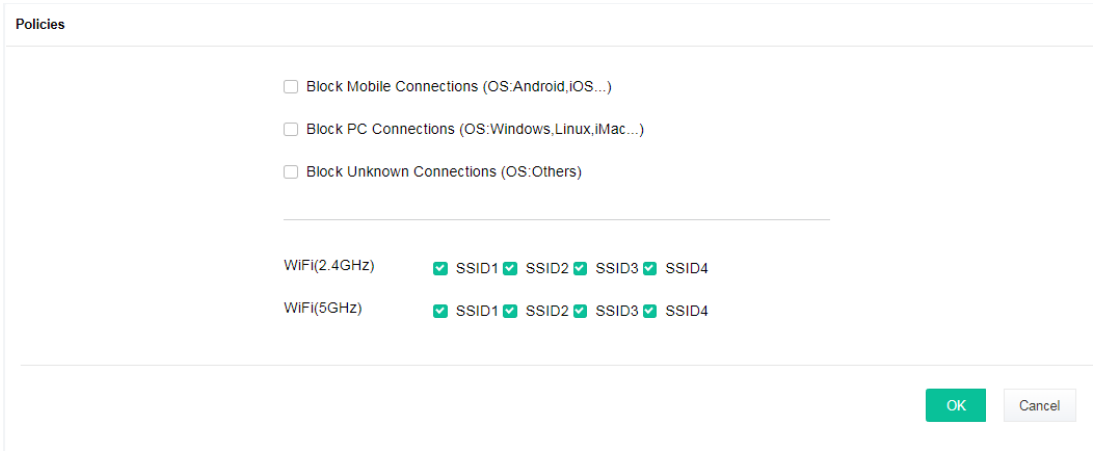


Available parameters are explained as follows:

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

III-3-4 Policies

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



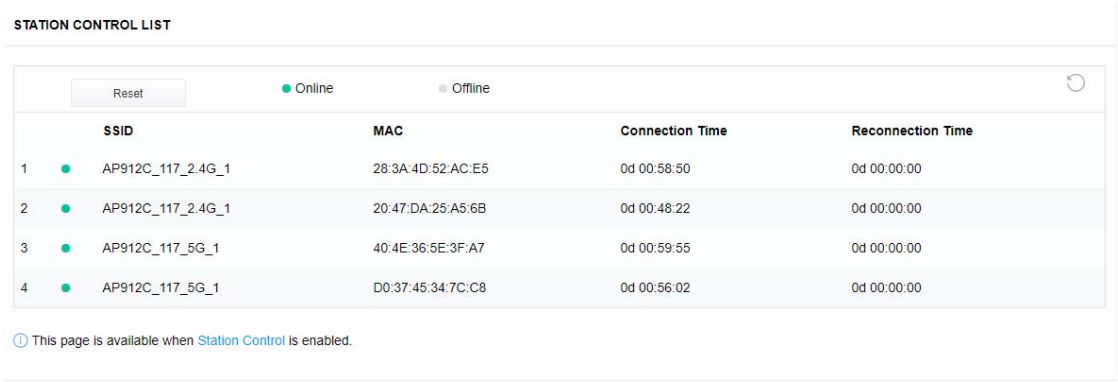
Each item is explained as follows:

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

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

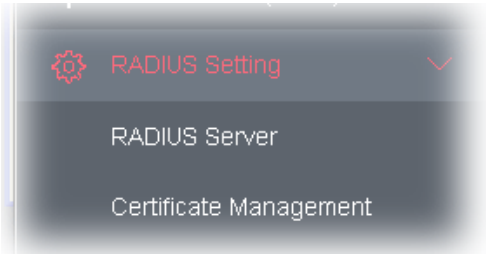
III-3-5 Station Control List

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



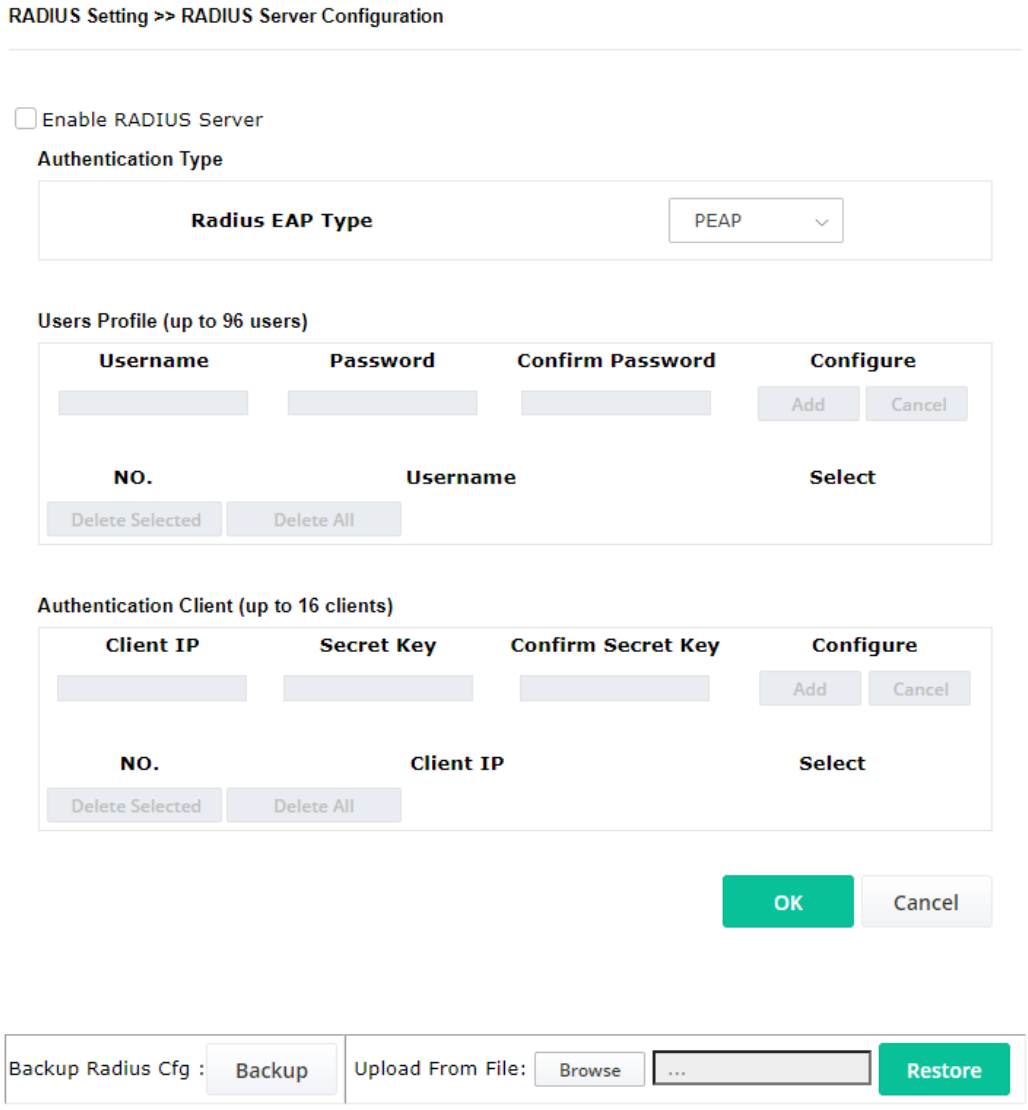
Chapter IV Others

IV-1 RADIUS Setting



IV-1-1 RADIUS Server

VigorAP 906 offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 906. The AP can accept the wireless connection authentication requested by wireless clients.



Available settings are explained as follows:

Item	Description
Enable RADIUS Server	Check it to enable the internal RADIUS server.
Authentication Type	Let the user choose the authentication method for the 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** – Enter a new name for the user profile. **Password** – Enter a new password for this 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 906 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 906 as its external RADIUS server. **Client IP** – Type the IP address for the user to be authenticated by VigorAP 906 when the user tries to use VigorAP 906 as the external RADIUS server. **Secret Key** – Type the password for the user to be authenticated by VigorAP 906 while the user tries to use VigorAP 906 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 on this page as a file.
Upload From File	**Browse** - Click to upload the RADIUS configuration file from the host to VigorAP. **Restore** - Click to restore the RADIUS configuration file to VigorAP.

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

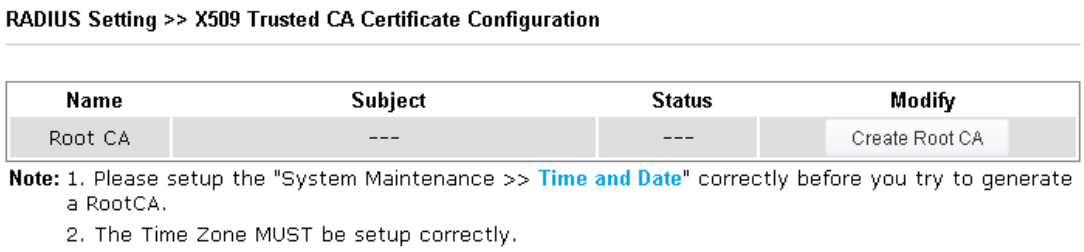
IV-1-2 Certificate Management

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

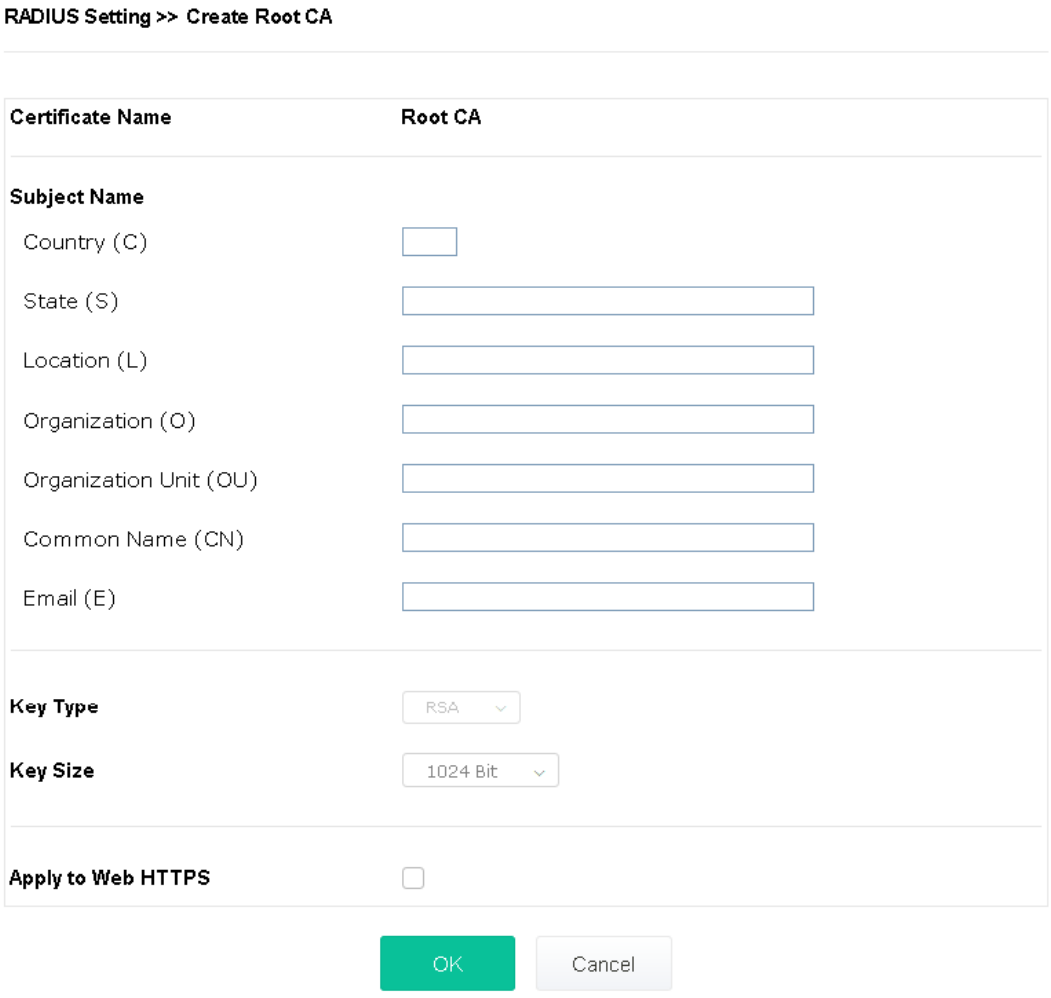
However, the procedure of applying a digital certificate from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor AP offers a mechanism that allows you to

generate root CA to save time and provide convenience for a general user. Later, such root CA generated by the DrayTek server can perform the issuing of a 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.



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.



Available settings are explained as follows:

Item	Description
Subject Name	Enter the required information for creating a root CA. Country (C) – Enter 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) – Enter the email address for the root CA with a length of fewer than 32 characters.
Key Type	At present, only RSA (an encryption algorithm) is supported by such a 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 the Internet via Web HTTPS. Check this box to use the user-defined root CA certificate which will substitute for the original certificate applied by web HTTPS.

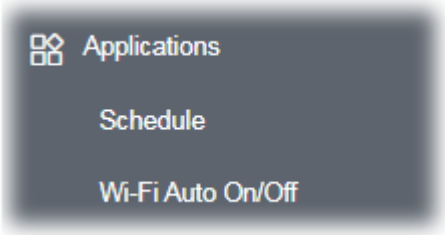
Note:

"Common Name" must be configured with router's WAN IP or domain name.

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

IV-2 Applications

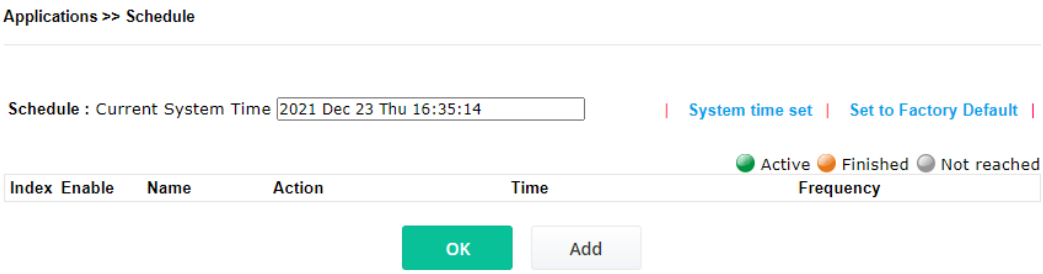
Below shows the menu items for Applications.



IV-2-1 Schedule

The VigorAP has a built-in clock that can update itself manually or automatically using Network Time Protocols (NTP). As a result, you can not only schedule the AP to dial-up 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 setting the schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the VigorAP's clock to the 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 a time. You can inquiry about 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.



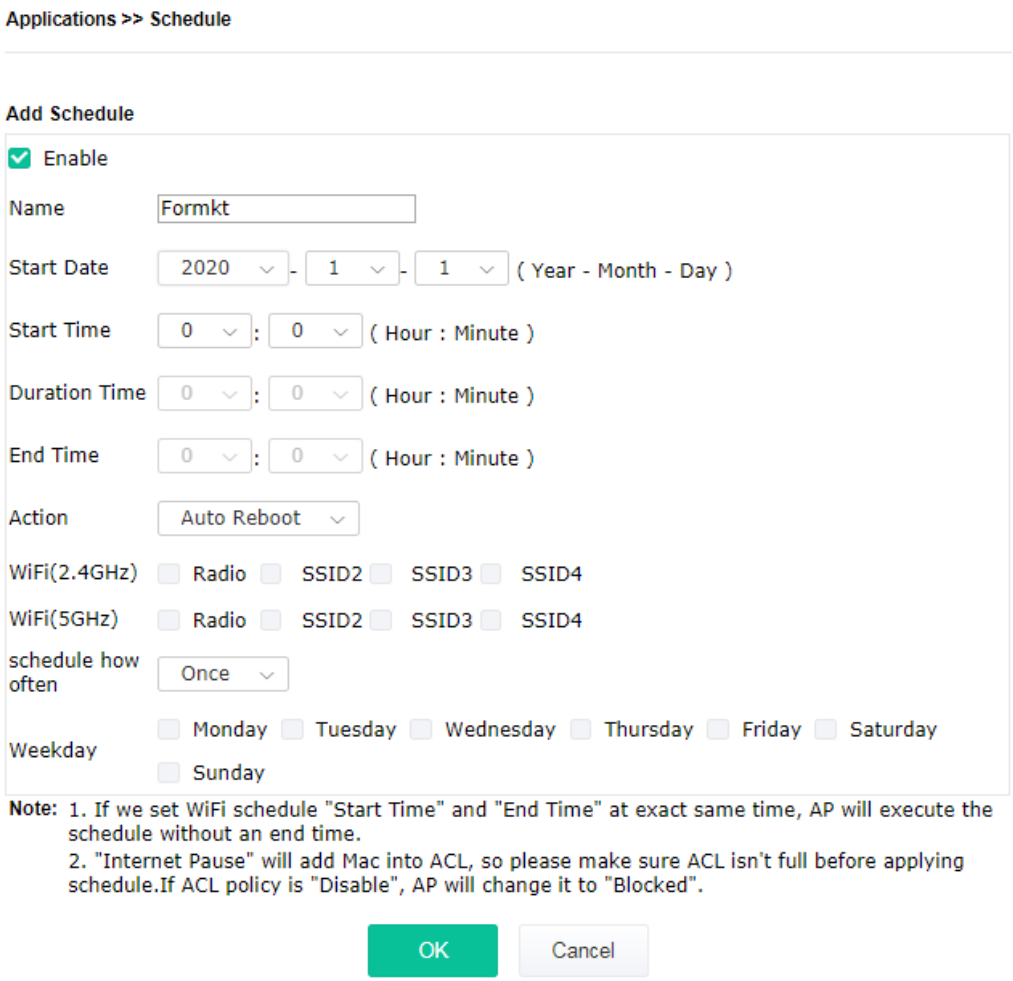
Available settings are explained as follows:

Item	Description
Current System Time	Display current system time.
System time set	Click it to open the 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 schedule.

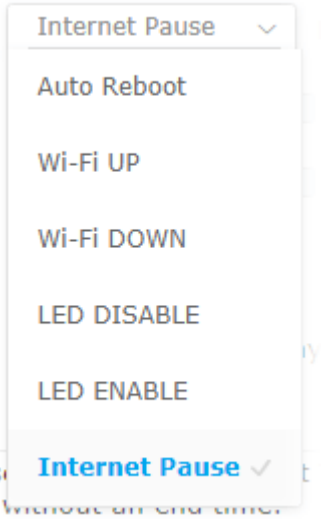
You can set up to **15** schedules. To add a schedule:

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

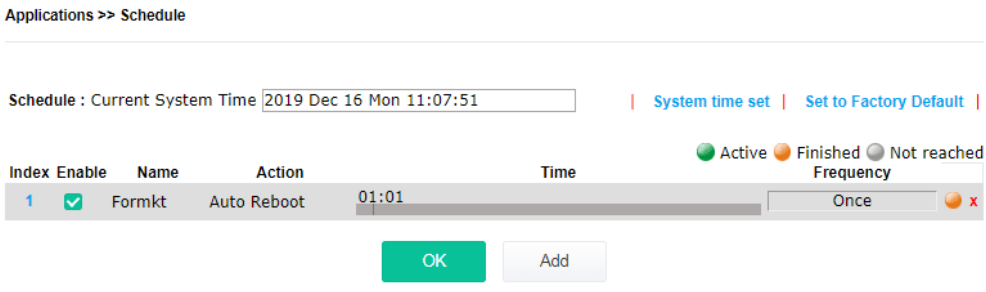


Available settings are explained as follows:

Item	Description
Enable	Check to enable such a schedule profile.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
Duration Time	Specify the duration (or period) for the schedule. It is available only for the action set with WIFI UP, WIFI Down, or Internet Pause.
End Time	Display the ending time (sum of start time and duration time) of the schedule.
Action	Specify which action should apply to the schedule.

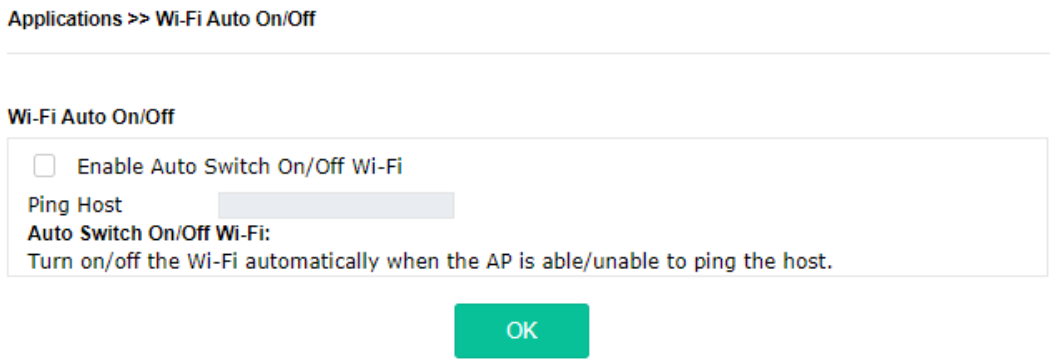
	 In which, you have to specify the device object/device group profile for blocking certain wireless clients when Internet Pause is selected as the Action.
WiFi(2.4GHz)/ WiFi(5GHz)	When **Wi-Fi UP** or **Wi-Fi DOWN** is selected as **Action**, you can check the Radio or SSID 2~4 boxes (2.4GHz and 5GHz respectively) to set up 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.
Acts	Specify how often the schedule will be applied. **Once -**The schedule will be applied just once **Routine -**Specify which days in one week should perform the schedule.
Weekday	Choose and check the day to perform the schedule. It is available when the **Routine** is selected as **Acts**.

2. 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.



IV-2-2 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 the Internet.



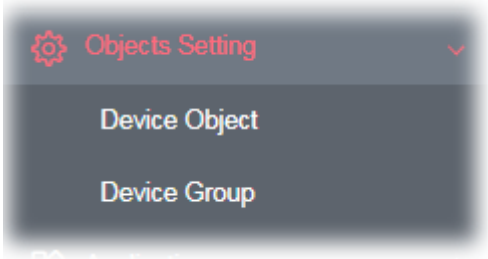
Available settings are explained as follows:

Item	Description
Enable Auto Switch On/Off Wi-Fi	Check the box to enable such a function.
Ping Host	Enter an IP address (e.g., 8.8.8.8) or a domain name (e.g., google.com) for testing if the access point is stable or not.

Click **OK** to save the settings.

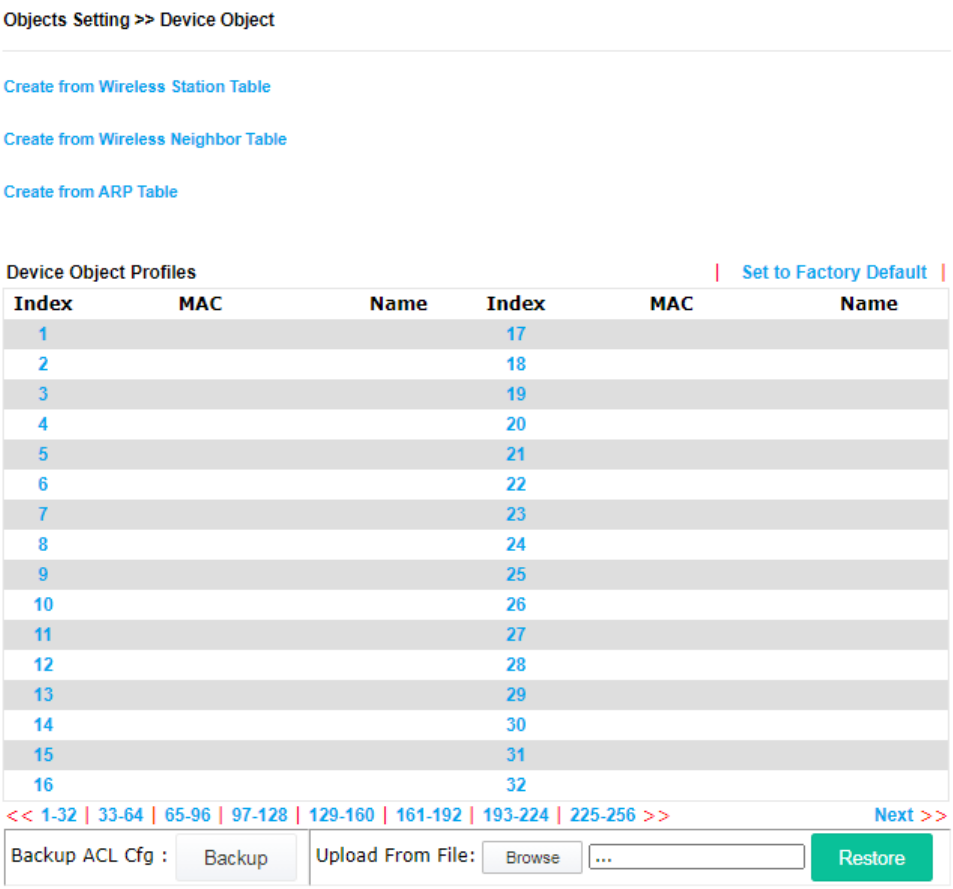
IV-3 Objects Setting

Below shows the menu items for Objects Setting.



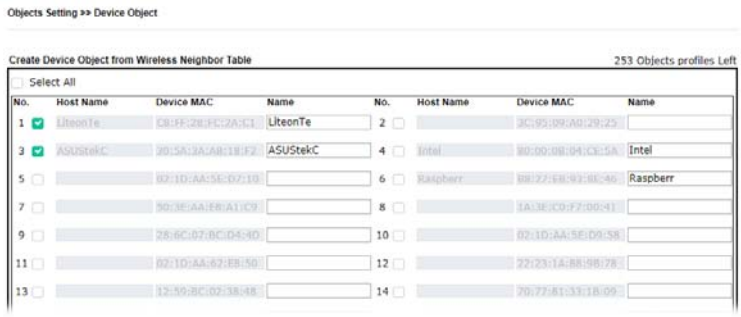
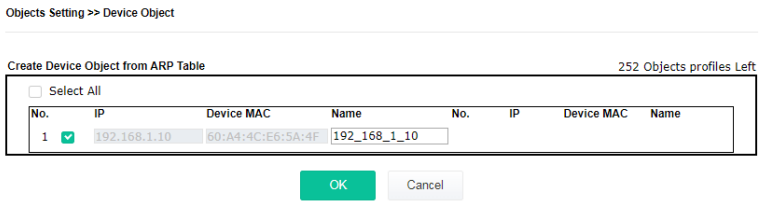
IV-3-1 Device Object

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

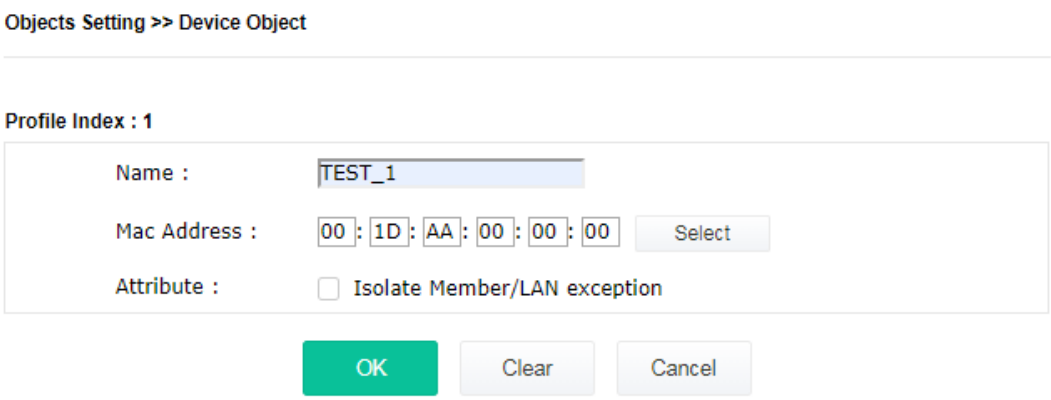


Available settings are explained as follows:

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

	 Choose the one(s) you want and click **OK**. The selected entries will be listed on the Device Object Profiles.
Create from Wireless Neighbor Table	Click the link to open the following page.  Choose the one(s) you want and click **OK**. The selected entries will be listed on the Device Object Profiles.
Create from ARP Table	Click the link to open the following page.  Choose the one(s) you want and click **OK**. The selected entries will be listed on the Device Object Profiles.
Set to Factory Default	Click it to return to the factory default setting and remove all the device object profiles.
Index	Display the index number of the device object profile.
MAC	Display the MAC address specified by the device object profile.
Name	Display the name of the device object profile.

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

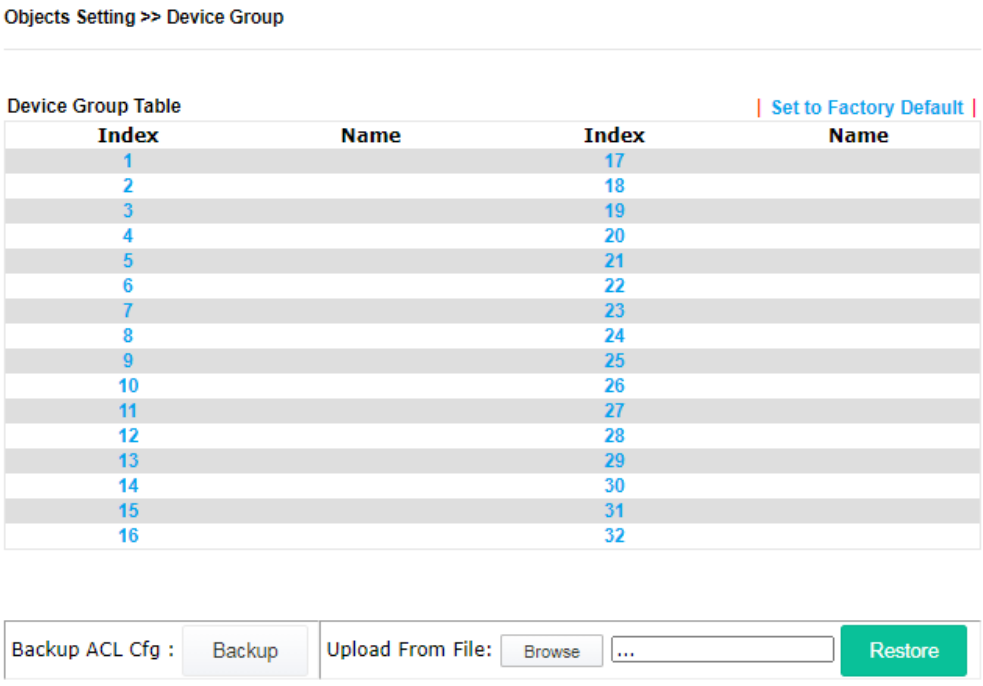


Available settings are explained as follows:

Item	Description
Name	Enter the name of the profile.
Mac Address	Enter the MAC address of the client.
Attribute	Check the box to ignore the function of Isolate LAN / Member.
OK	Save the settings.
Clear	Remove the settings.
Cancel	Discard the settings and return to the previous page.

IV-3-2 Device Group

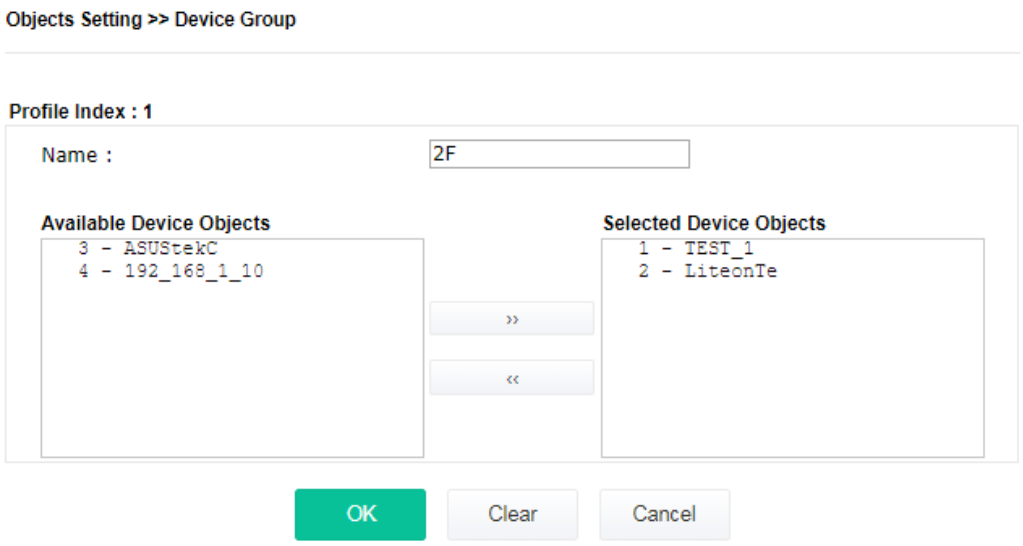
Clients can be integrated as a group and be used by other applications.



Available settings are explained as follows:

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

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



Available settings are explained as follows:

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

This page is left blank.

Chapter V Mobile APP, DrayTek Wireless

V-1 Introduction of DrayTek Wireless

VigorAP 906 supports Android/iOS APP : DrayTek Wireless. The mobile user can find the APP through Apple App Store / Google Play Store.

After downloading the APP, a mobile user is able to access and login the configuration page of VigorAP.

Note:

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

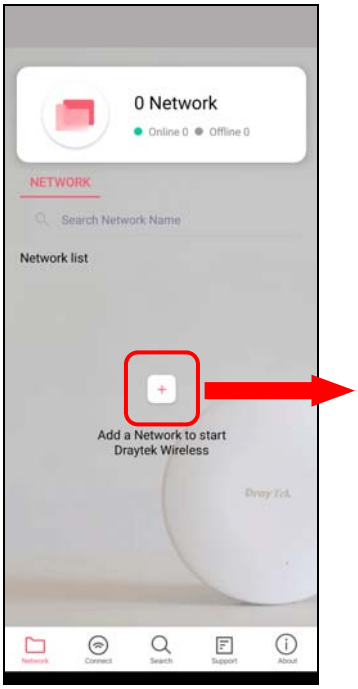
It is not necessary to connect to VigorAP physically. The mobile user must connect to one network with the same subnet as the VigorAP.

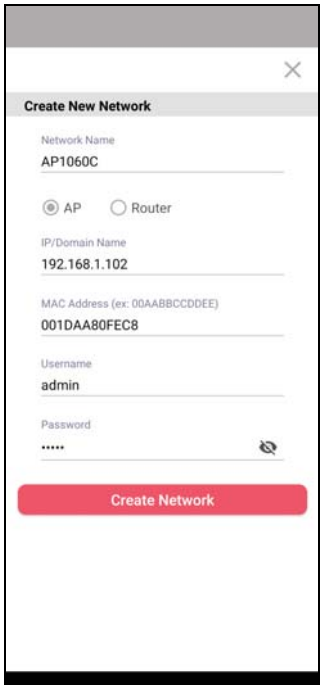
V-2 Create a New Network

1. Run DrayTek Wireless APP.

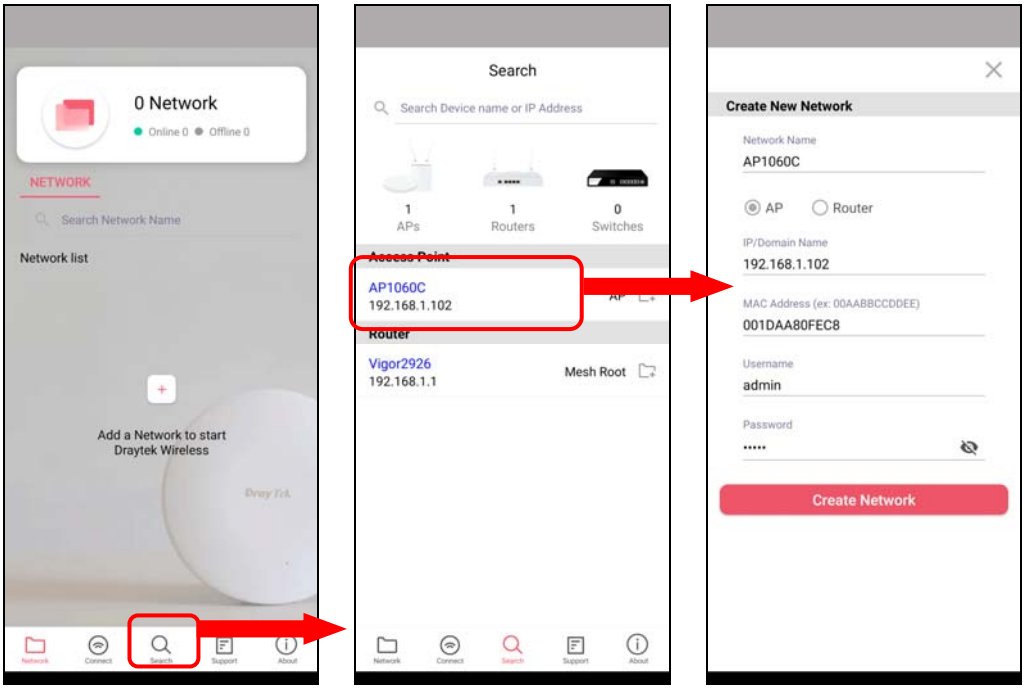
2. The system will open the NETWORK page to ask you create a new network first.
3. There are two methods for creating a new network. Click "+" or press the search button

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

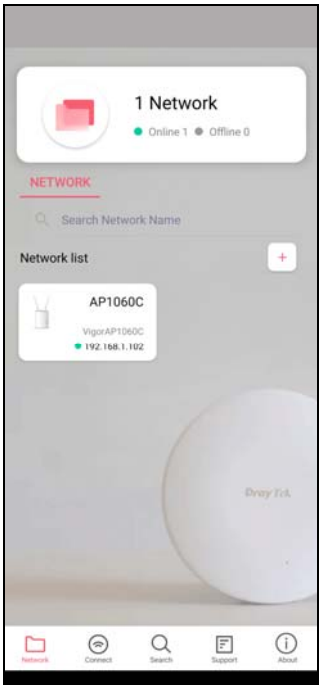




B: Press the search button. Later, the system will show the device searched. Select the one you want and click the name to get the detailed information.



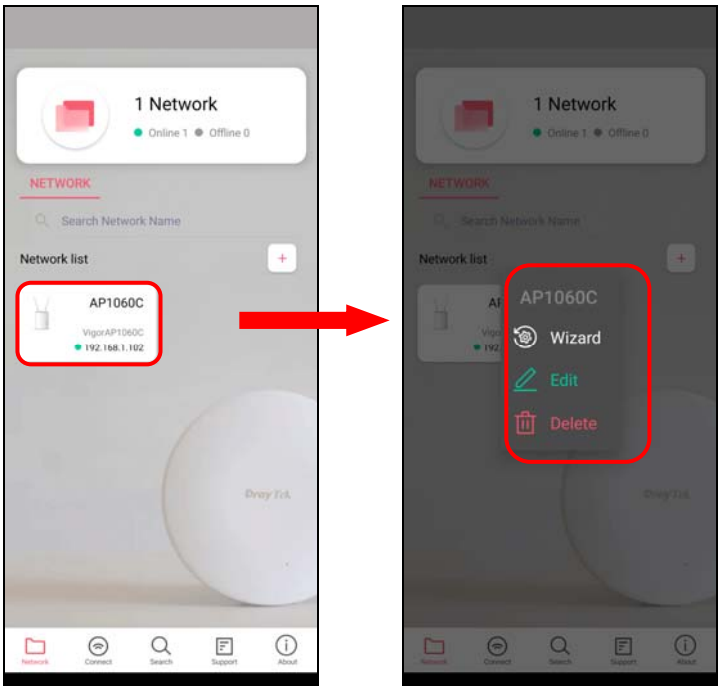
4. After clicking **Create Network**, a new network will be shown on the screen.



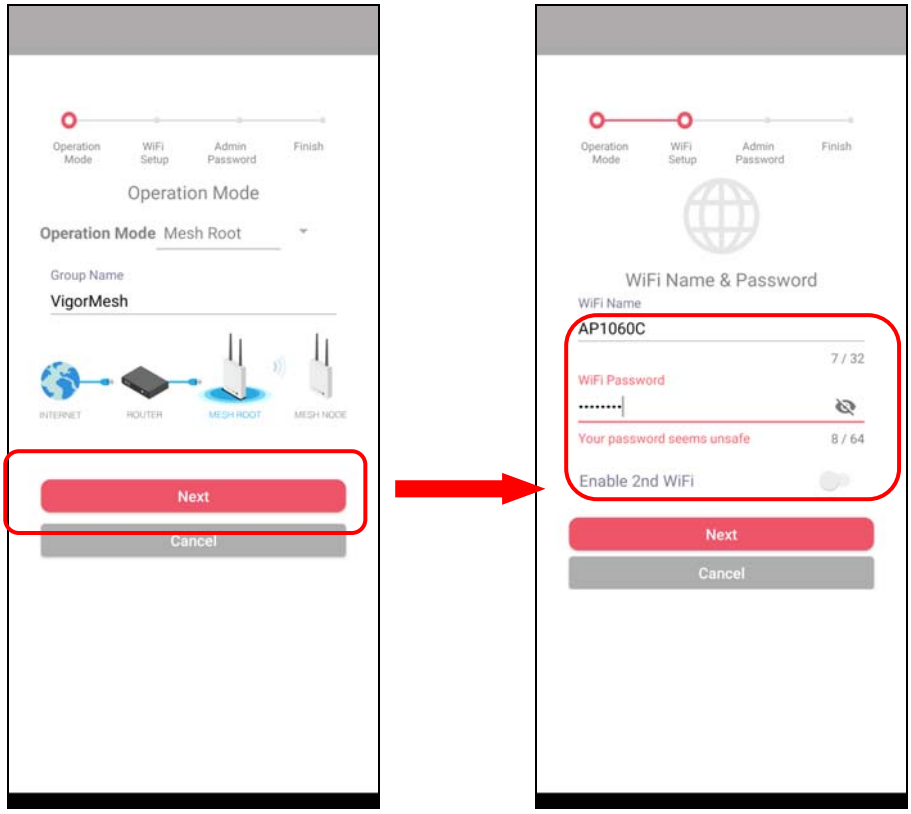
V-3 Wizard - Mesh Root and Mesh Node

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

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

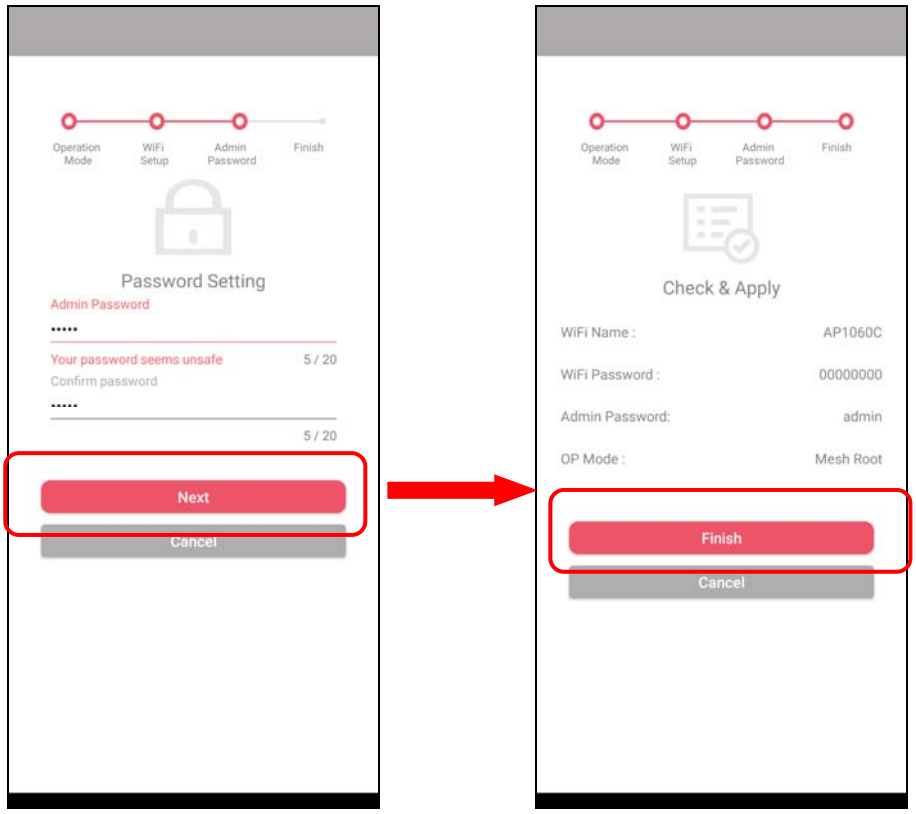


2. After clicking **Wizard**, select **Mesh Root** as the Operation Mode. The default Group Name is VigorMesh. Change the name if required. Click **Next** to enter the next page.

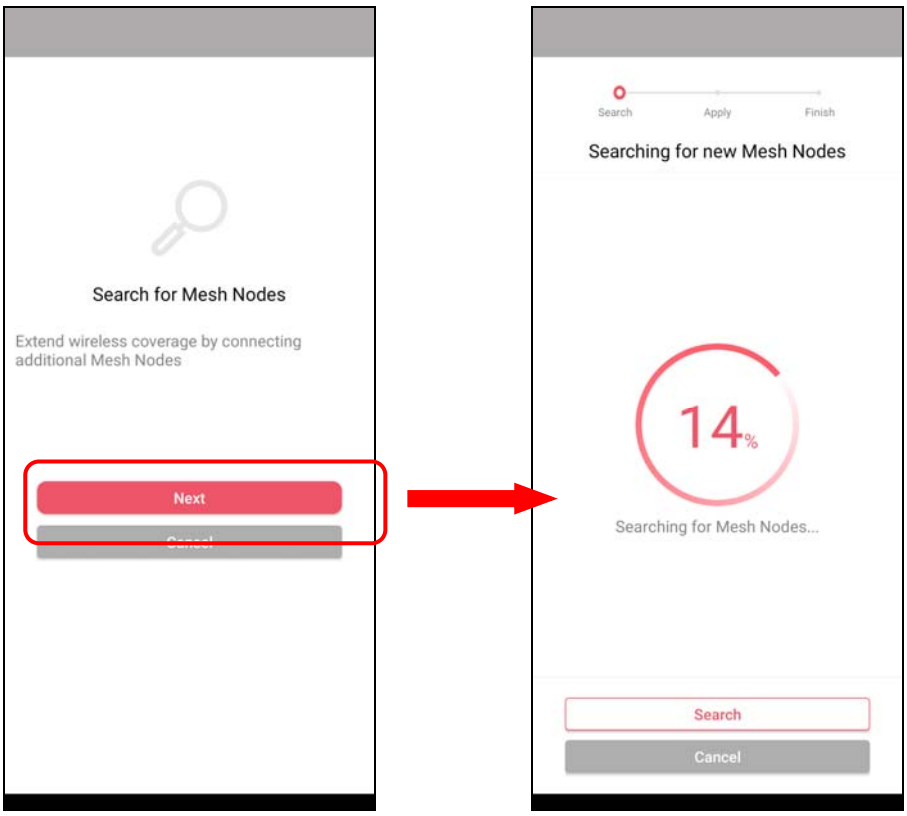


On the WiFi Name & Password page, enter the WiFi Name and the password (should be the same as the security settings set on the device's WUI). You can also enable 2nd SSID by enabling the function of 2nd WiFi. Then click the **Next** button.

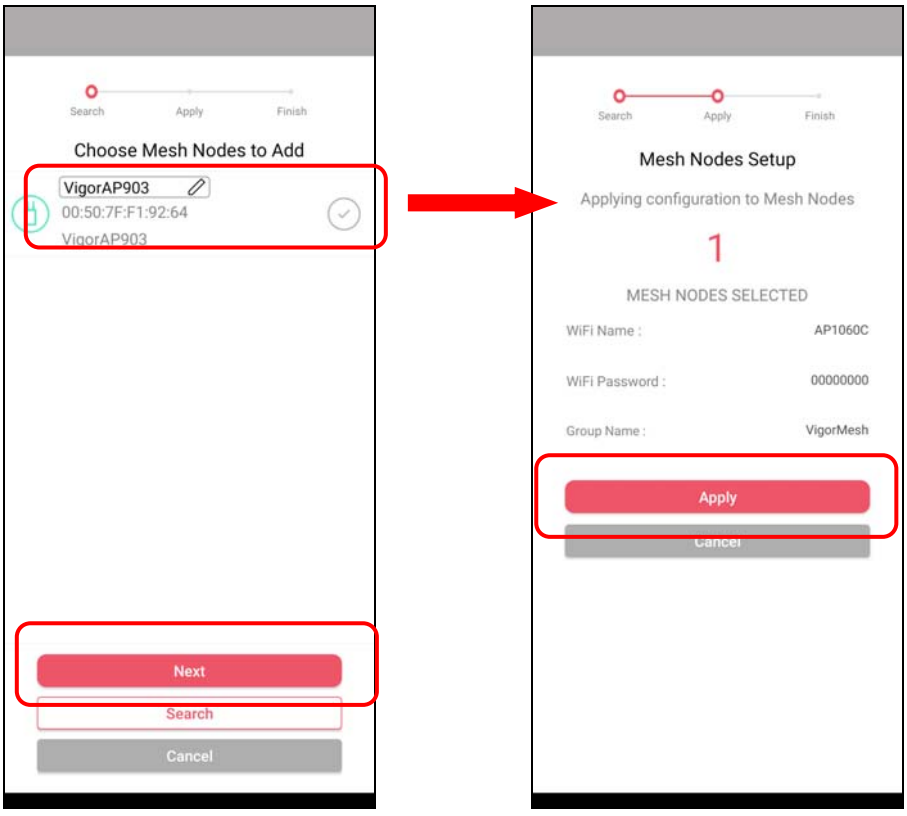
3. On the **Password Setting** page, enter the admin password and confirm the password. Then click **Next** for the APP to verify the password. If successful, the **Finish** button will appear.



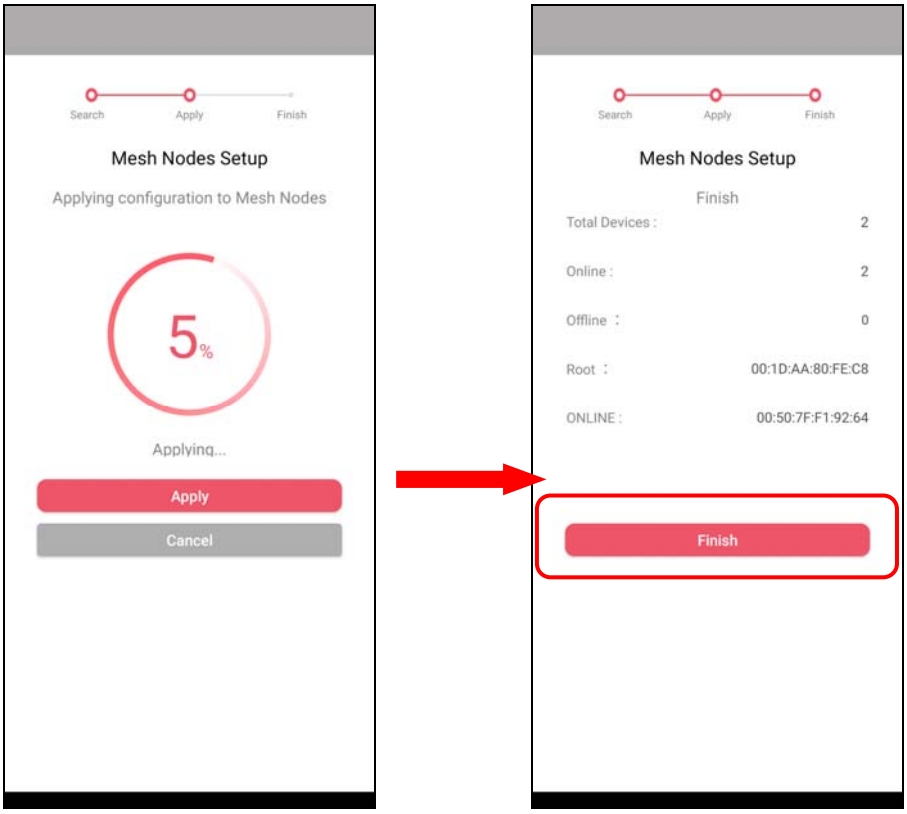
4. After sending configuration to VigorAP, it will take some time to take effect. Now, the VigorAP has been set as Mesh Root. You can search several Mesh Nodes which do not belong to any other mesh group by clicking **Next**.



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



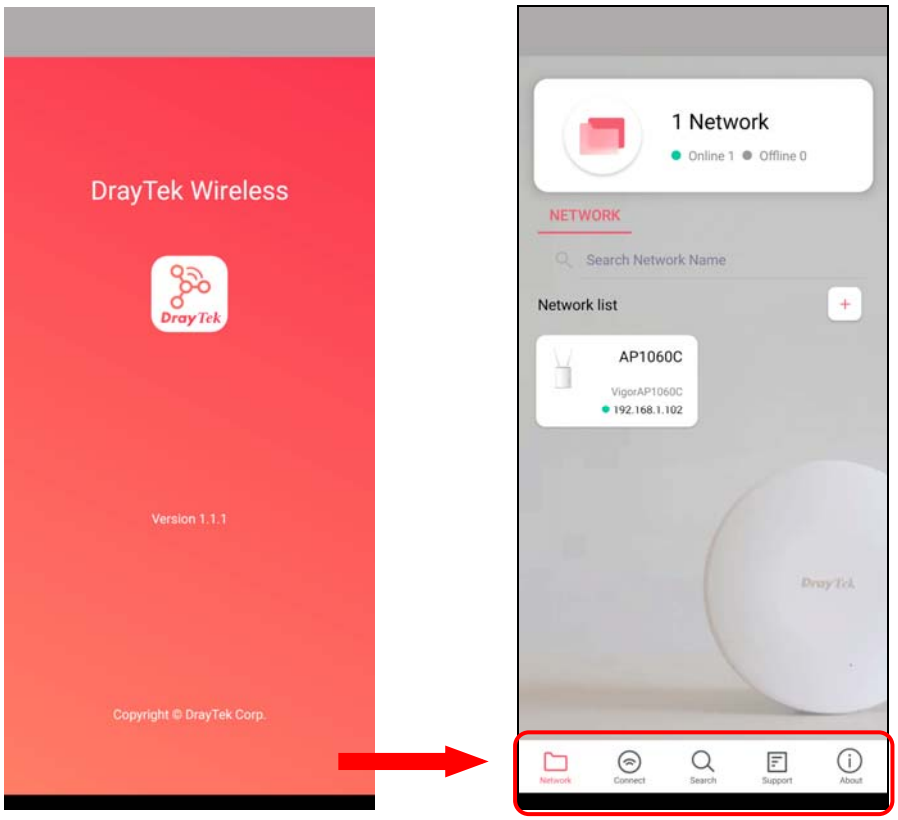
6. Wait until the mesh root applies general configuration to the mesh nodes. Later, current status of the mesh node(s) will be shown on the following page. Click **Finish**.



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

V-4 Login

Run DrayTek Wireless APP.

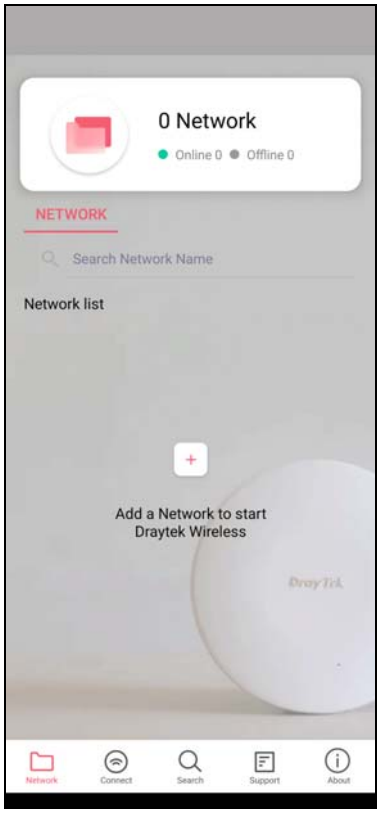


Available settings are explained as follows:

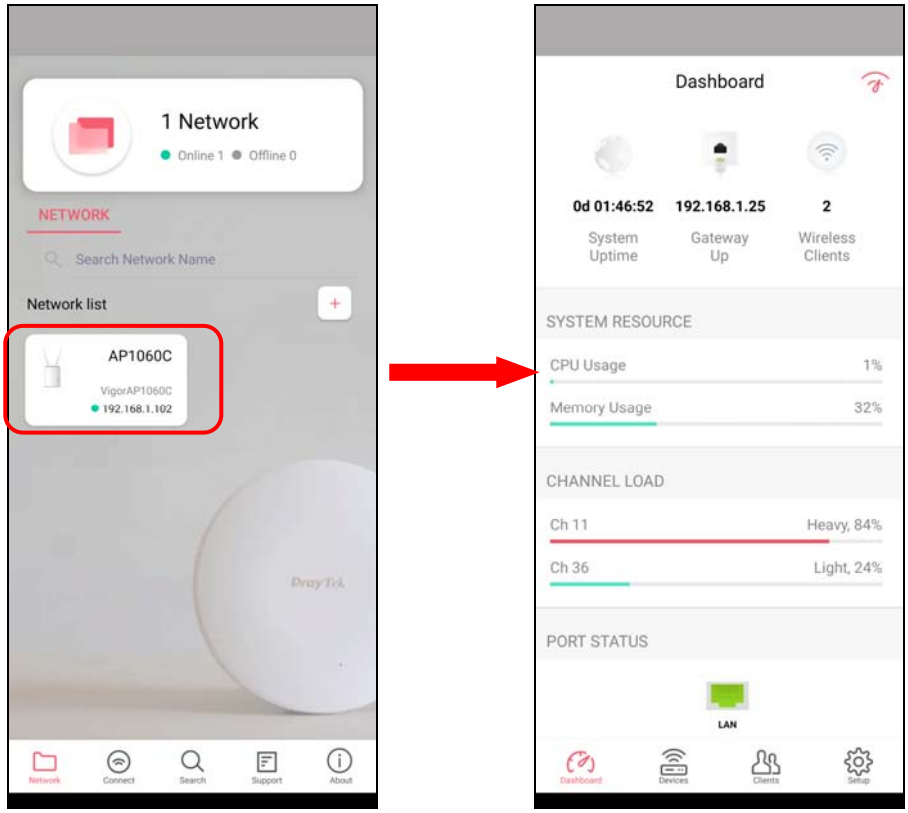
Item	Description
Network	Create a new network.
Connect	Connect to a device (AP/CPE).
Search	Search available devices for connection.
Support	Display a list of models supported by this APP.
About	Display the version information of this APP.

V-4-1 Network

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



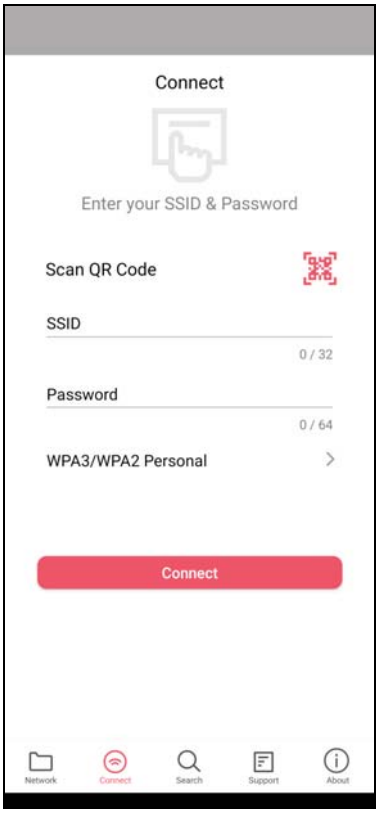
For checking the general information of certain device, click the existing item under the Network list to open the **Dashboard** of the selected device.

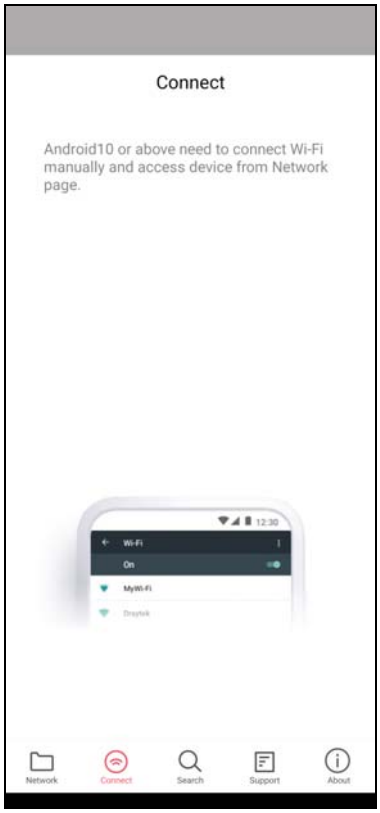


V-4-2 Connect

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

Then click the **Connect** button (Connect) for accessing into the dashboard of the device.



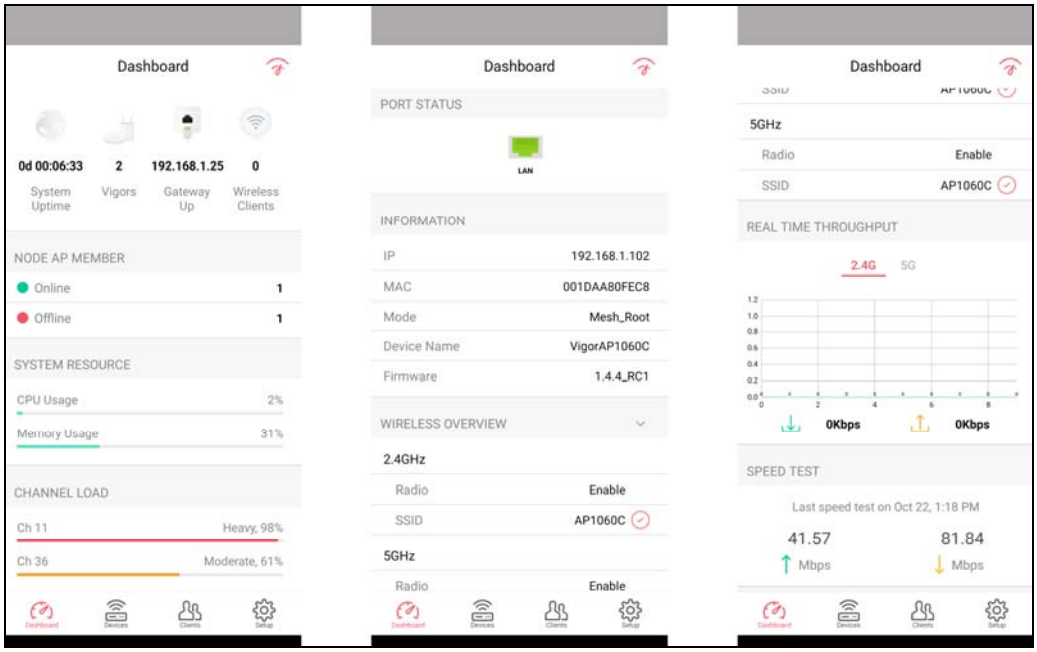


Or, click **Scan (** **)** to scan the QR code printed on VigorAP packaging box to connect the designated VigorAP.

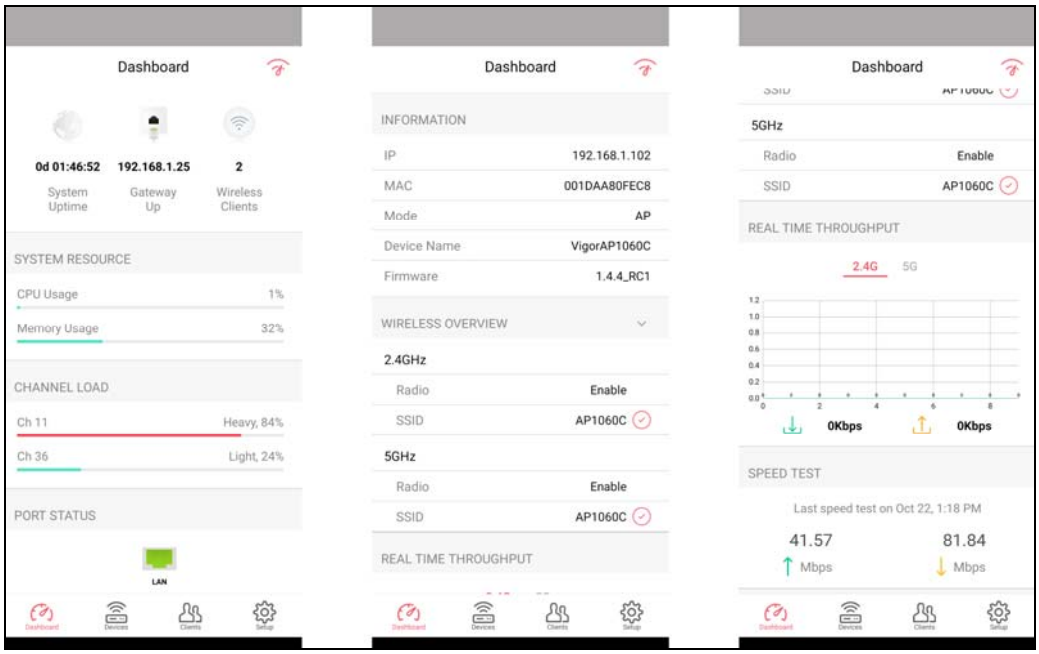
V-4-2-1 Dashboard of the Device

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

Information for **Mesh Root** Mode



Information for **AP** Mode



Available settings are explained as follows:

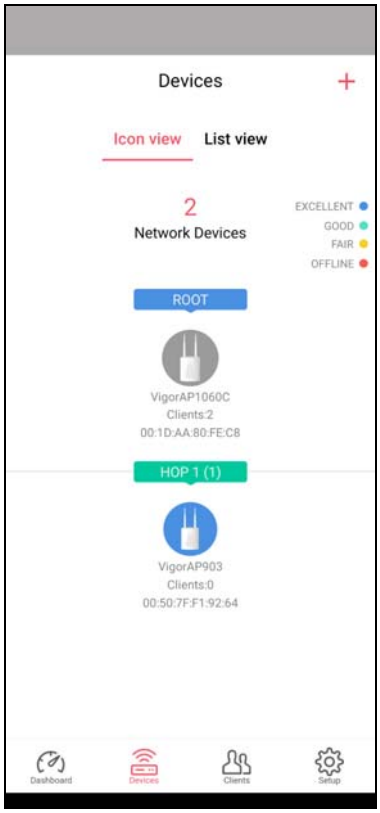
Item	Description
Dashboard	The dashboard is designed with Responsive Web Design. You can click **Dashboard** to connect to the selected VigorAP WUI.
Devices	All of the devices (mesh root and mesh nodes) controlled by the mesh group will be shown on this page. One mesh group contains up to eight devices.

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

V-4-2-2 Devices

Below shows the icon view and list view of the device. One mesh group contains up to eight devices.

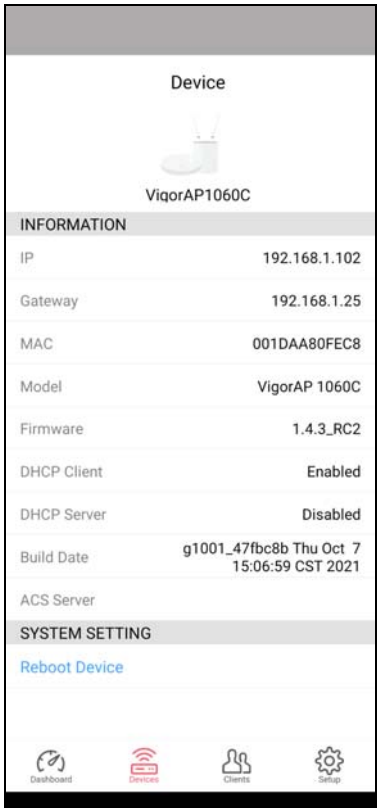
Icon view and List view for **Mesh Root** Mode



Available settings are explained as follows:

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

Device for **AP** Mode



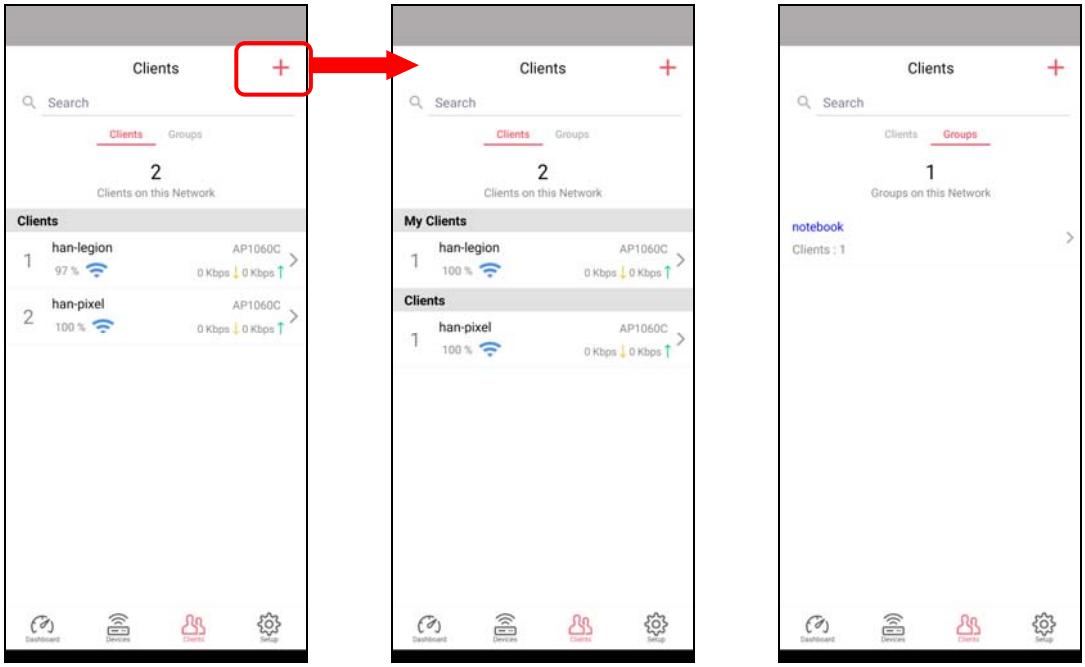
Available settings are explained as follows:

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

V-4-2-3 Clients / Groups

This page shows relationship between devices and groups.

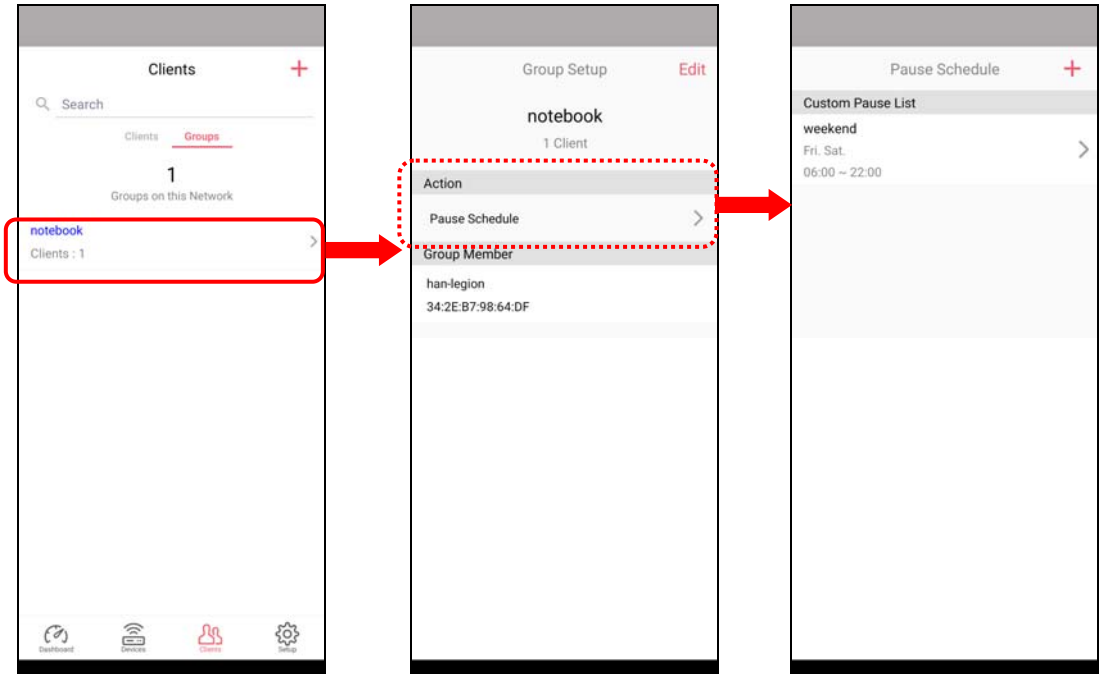
All client members can be classified (into groups). Additionally, the network connection time of the device group can be adjusted.



Available settings are explained as follows:

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

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



V-4-2-4 Setup

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

Chapter VI Troubleshooting

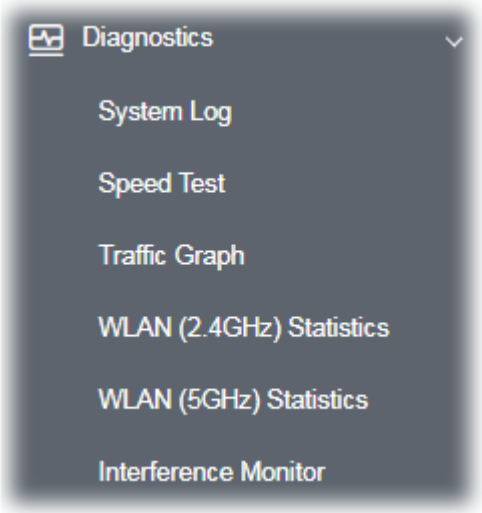
VI-1 Diagnostics

This section will guide you to solve abnormal situations if you cannot access the Internet after installing the router and finishing the web configuration. Please follow the 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 the factory default setting if necessary.

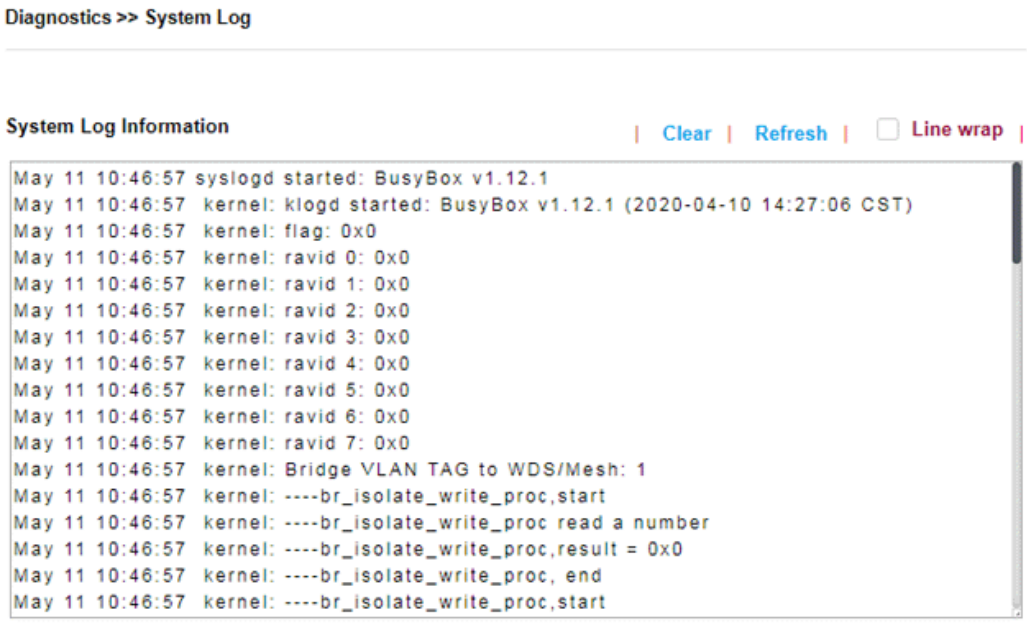
If all the above stages are done and the router still cannot run normally, it is time for you to contact your dealer or DrayTek technical support for advanced help.

Diagnostic tools provide a useful way to **view** or **diagnose** the status of your VigorAP 906.



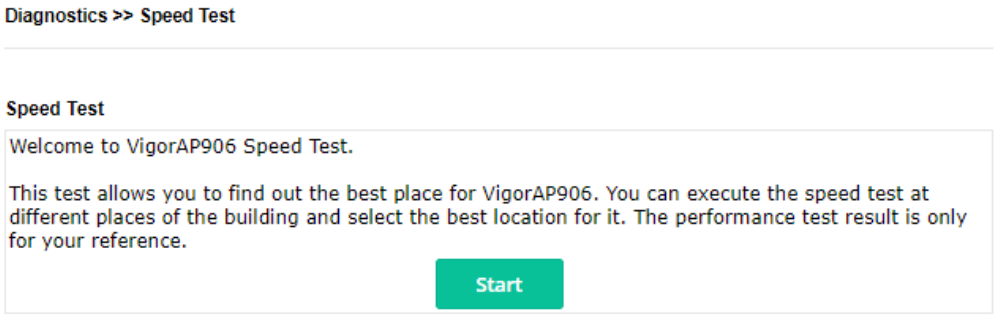
VI-1-1 System Log

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



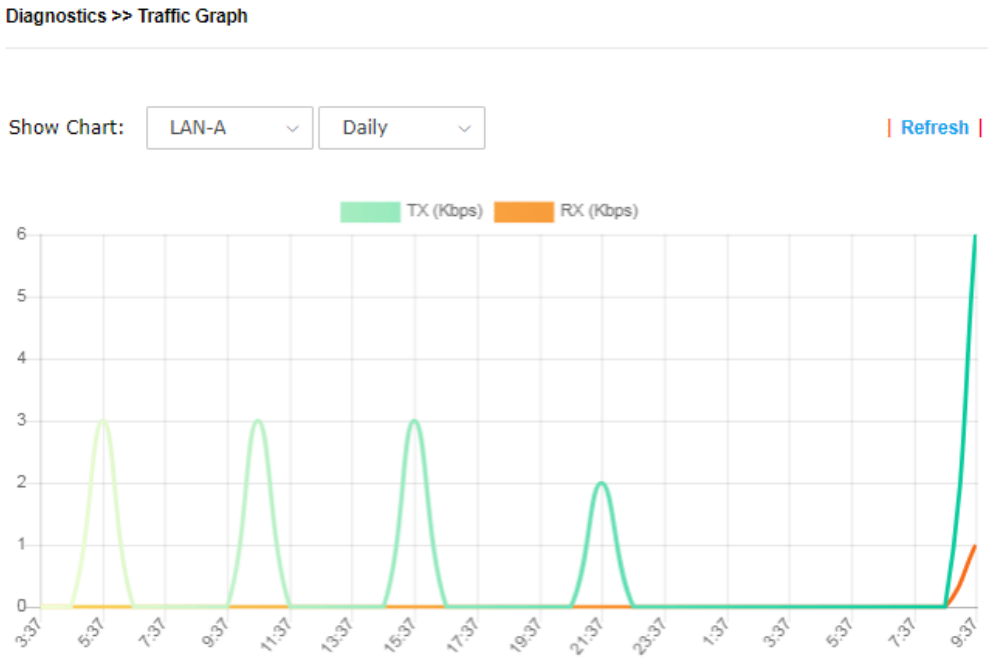
VI-1-2 Speed Test

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



VI-1-3 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, daily or weekly for viewing the 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 WLAN (2.4GHz) Statistics

This page is used for debugging by RD only.

Diagnostics >> WLAN (2.4GHz) Statistics

Auto-Refresh | Refresh

	SSID1 (ap906-Band Steering)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Rx Data Packets	0	N/A	N/A	N/A
Rx Data Bytes	0	N/A	N/A	N/A
Rx Dropped	0	N/A	N/A	N/A
Tx Data Packets	0	N/A	N/A	N/A
Tx Data Bytes	0	N/A	N/A	N/A
Rx Unicast Data Packets	0	N/A	N/A	N/A
Tx Unicast Data Packets	0	N/A	N/A	N/A
Rx Multicast Data Packets	0	N/A	N/A	N/A
Tx Multicast Data Packets	0	N/A	N/A	N/A
Rx Broadcast Data Packets	0	N/A	N/A	N/A
Tx Broadcast Data Packets	0	N/A	N/A	N/A

VI-1-5 WLAN (5GHz) Statistics

This page is used for debugging by RD only.

Diagnostics >> WLAN (5GHz) Statistics

Auto-Refresh | Refresh

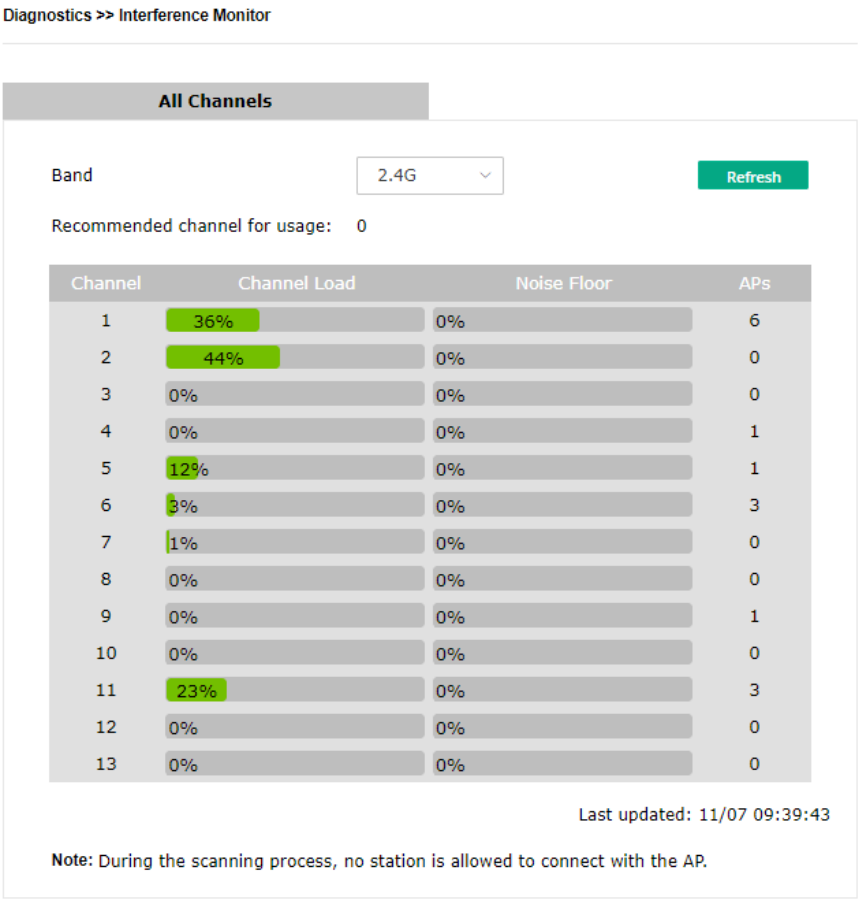
	SSID1 (ap906-Band Steering)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Rx Data Packets	0	N/A	N/A	N/A
Rx Data Bytes	0	N/A	N/A	N/A
Rx Dropped	0	N/A	N/A	N/A
Tx Data Packets	0	N/A	N/A	N/A
Tx Data Bytes	0	N/A	N/A	N/A
Rx Unicast Data Packets	0	N/A	N/A	N/A
Tx Unicast Data Packets	0	N/A	N/A	N/A
Rx Multicast Data Packets	0	N/A	N/A	N/A
Tx Multicast Data Packets	0	N/A	N/A	N/A
Rx Broadcast Data Packets	0	N/A	N/A	N/A
Tx Broadcast Data Packets	0	N/A	N/A	N/A

VI-1-6 Interference Monitor

As an interference detector, VigorAP can detect all of the environmental interference factors for the certain channel used or for all of the wireless channels.

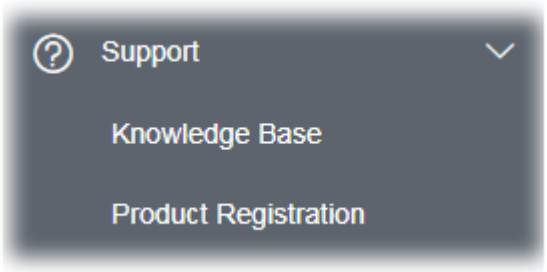
All Channels

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



VI-1-7 Support Area

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



VI-2 Checking the Hardware Status

Follow the steps below to verify the hardware status.

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

VI-3 Checking the Network Connection Settings

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

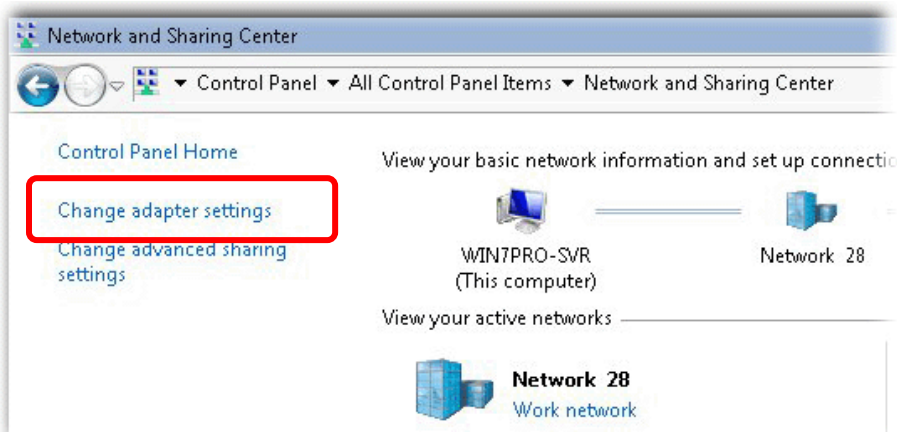
VI-3-1 For Windows

Note:

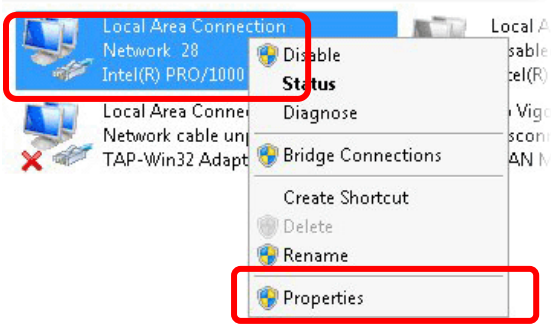
The example is based on Windows 7 (Professional Edition). As to the examples for other operating systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

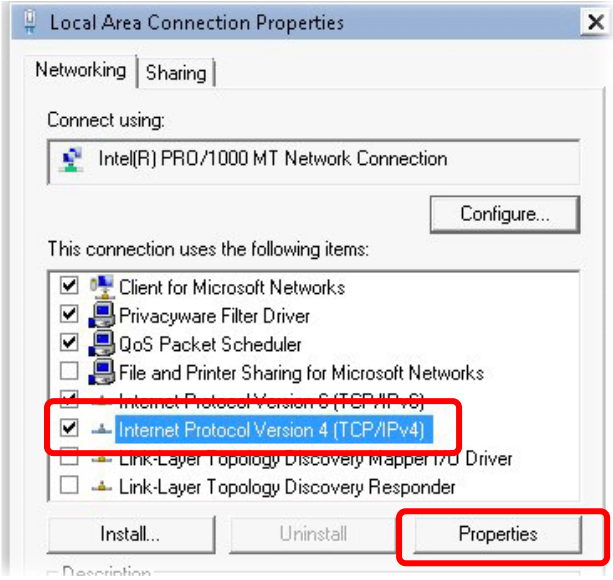
2. In the following window, click **Change adapter settings**.



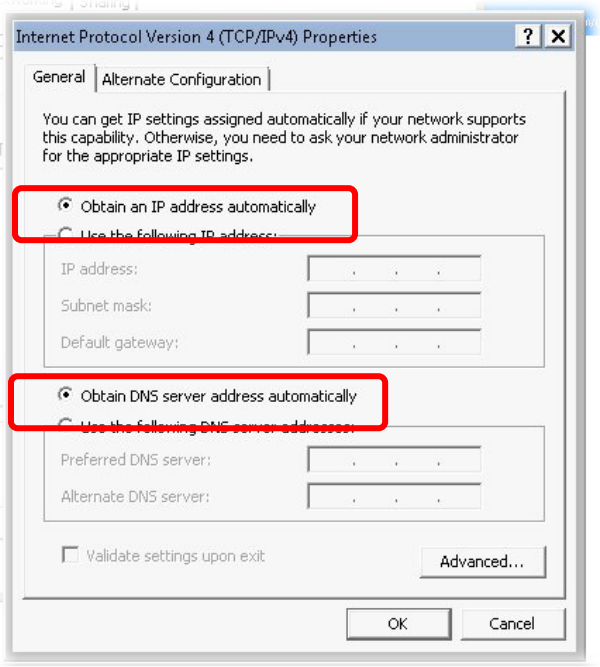
3. Icons of the network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

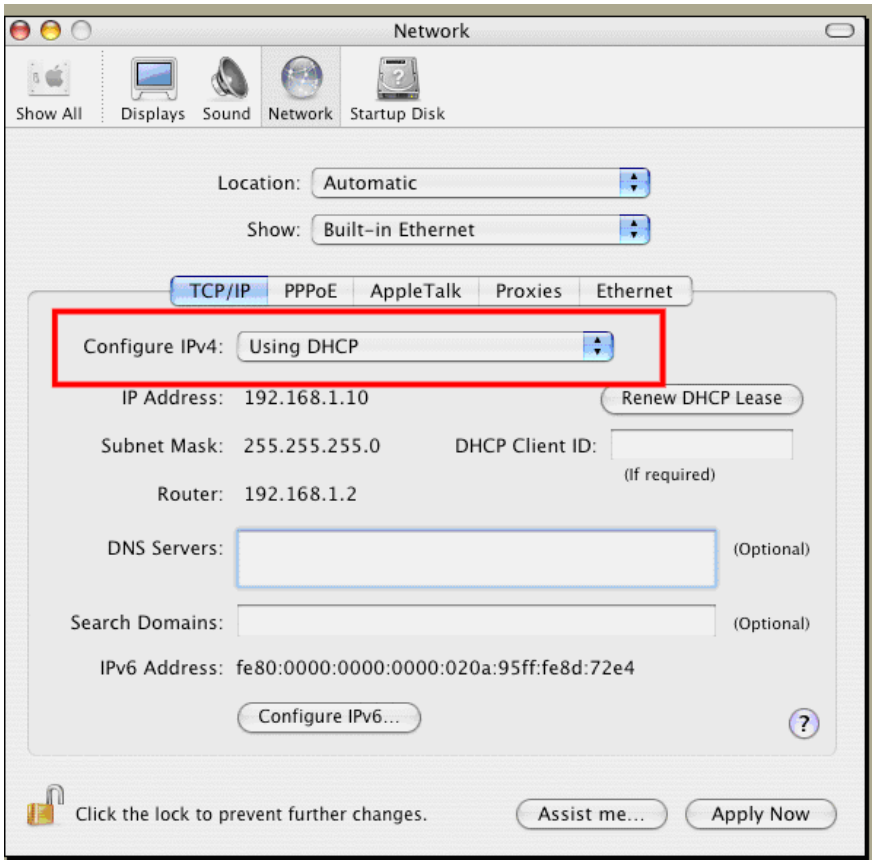


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



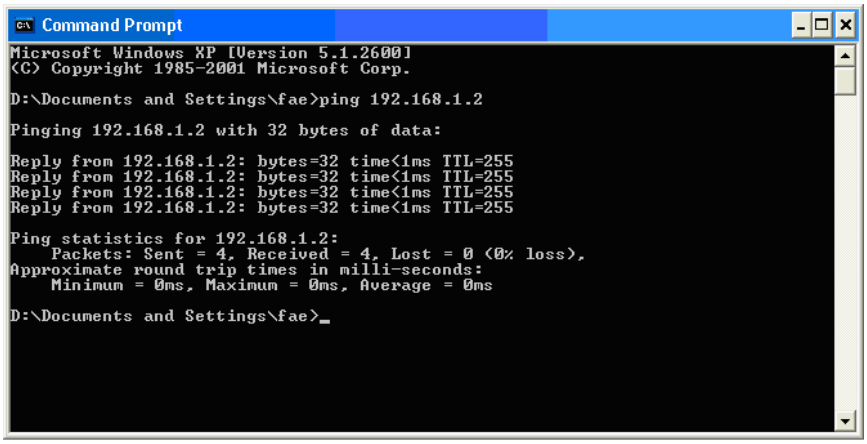
VI-4 Pinging the Device

The default gateway IP address of the modem is 192.168.1.2. For some reason, you might need to use the "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 set the network connection to **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

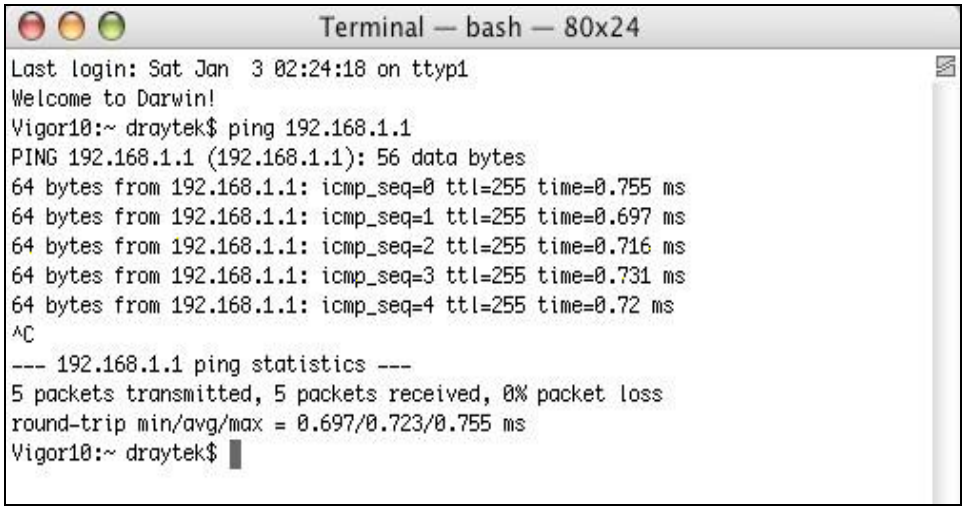
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/2000/XP/Vista/7). The DOS command dialog will appear.



3. Type ping 192.168.1.2 and press [Enter]. If the link is OK, the line **"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.


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

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.

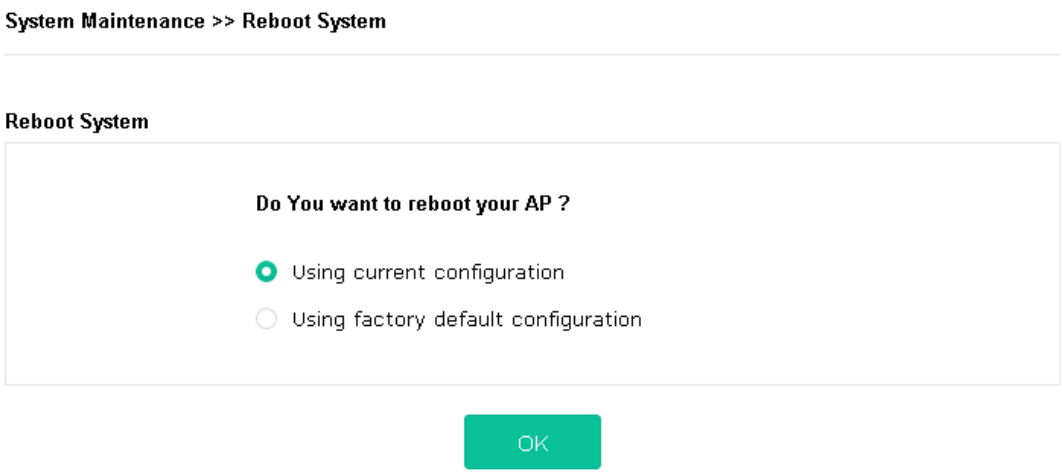
Warning:

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

VI-5-1 Software Reset

You can reset the modem to factory default via the 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.



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 restoring the factory default setting, you can configure the settings for the modem again to fit your 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 an e-mail to support@draytek.com.