VigorAP 802

11ac Dual-band Wall Plug AP

USER'S GUIDE

V1.1

VigorAP 802

802.11ac Access Point

User's Guide

Version: 1.1

Firmware Version: V1.3.4

Date: May 12, 2020

Intellectual Property Rights (IPR) Information

Copyrights

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the modem.
- The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself.
- Do not place the modem in a damp or humid place, e.g. a bathroom.
- The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the modem, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor modem via http://www.draytek.com.

Firmware & Tools Updates

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

http://www.draytek.com

Table of Contents

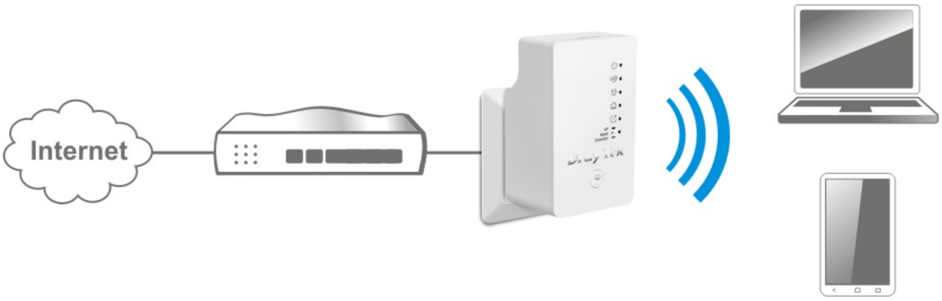
Chapter I Installation

I-1 Introduction

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

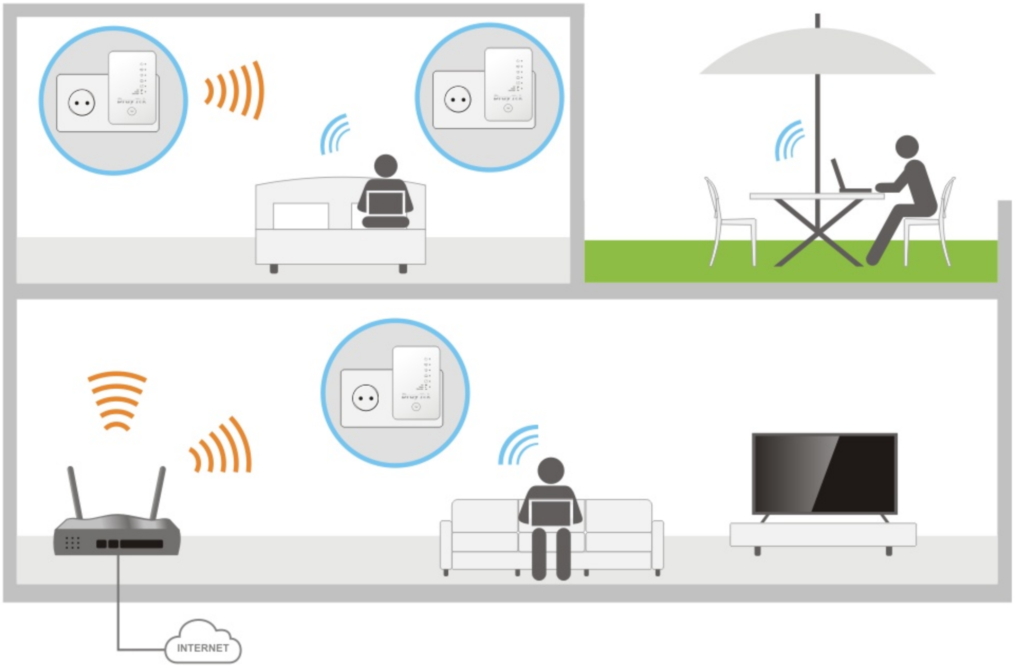
Thank you for purchasing this device, VigorAP 802.

Without any cable, the plug design of VigorAP brings an easy hardware installation (by plugging to a wall outlet) for any computer users to set up a network environment in a very short time - within minutes, even inexperienced users.



Besides, the software installation can be completed easily by using a mobile phone to scan the QR code on the front side of VigorAP device. The DrayTek Wireless APP will guide the users to configure the device in AP or Range Extender mode just with several steps.

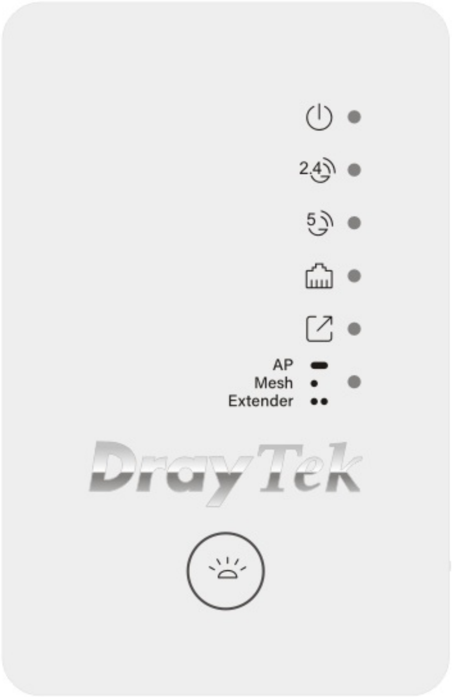
VigorAP supports AP, Mesh Node and Range Extender mode. In which, the Range Extender mode can extend the wireless coverage for wireless network.



Follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

I-1-1 LED Indicators and Connectors

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



LED	Status	Explanation
ACT ⏻	Off	The system is not ready or is failed.
	Blinking	Slowly: The system is ready and can work normally. Quickly: The system is booting up or resetting to the Factory Default value.
2.4G 2.4	On	Wireless function (2.4G) is ready.
	Off	Wireless function (2.4G) is not ready.
	Blinking	Data is transmitting (sending/receiving).
5G 5	On	Wireless function (5G) is ready.
	Off	Wireless function (5G) is not ready.
	Blinking	Data is transmitting (sending/receiving).
LAN	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
Uplink ↗	On	Connect to Mesh network or other AP.
	Off	Disconnect to Mesh network or other AP.
	Blinking	The system is trying to connect to mesh network or other AP. For AP mode, the system is scanning the surrounding network. Or WPS is enabled and the system is waiting for response from the wireless client.
Mode AP ▬ Mesh • Extender ••	On	Indicate VigorAP is configured as AP mode.
	Flash one time	Indicate VigorAP is configured as Mesh Node mode.
	Flash twice	Indicate VigorAP is configured as Range Extender mode.

Button	Factory Reset	Press it for more than 15 seconds. When the ACT LED flashes rapidly, release the button.
	Mesh Node Mode	This AP is configured with Mesh Node mode. Press it for more than 2 seconds. Within 5 seconds, the AP is trying to connect to the mesh network.
	Range Extender Mode	This AP is configured as Range Extender mode. Press it for more than 2 seconds. Within 5 seconds, the AP is trying to connect to the AP.
	AP Mode	This AP is configured as AP mode and the WPS function is enabled. Press it for more than 2 seconds. VigorAP will wait for any wireless client connecting to this AP through WPS.

Interface	Description
LAN	Connecter for Ethernet device. You can connect 10/100M Ethernet network devices, such as a PC, TV, camera and anything else you want to put on your networks.

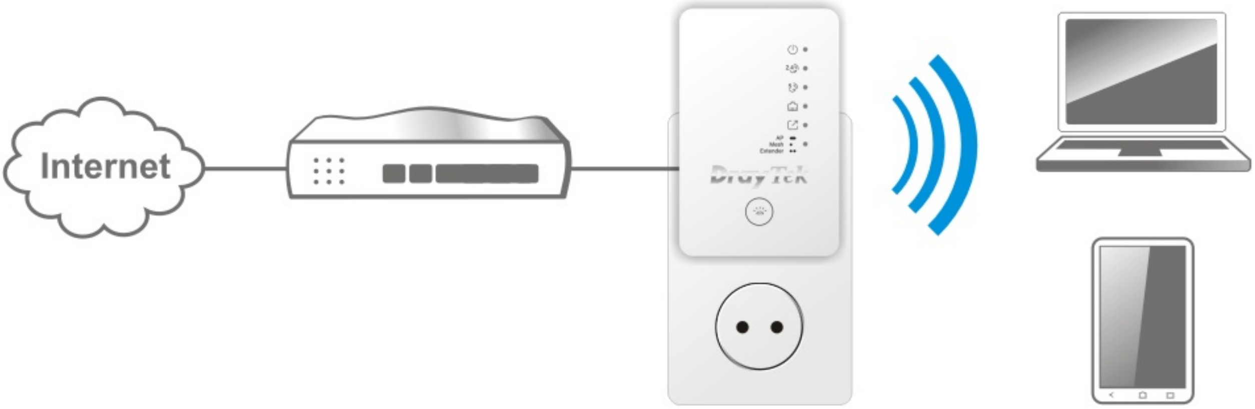
Note:

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

I-2 Hardware Installation

This section will guide you to install the AP through hardware connection and configure the settings through web browser.

Before starting to configure the device, you have to connect your device correctly.



1. Plug VigorAP into a power outlet.
2. Use a twisted-pair cable with RJ-45 plugs at both ends, and plug into Ethernet device (e.g., Vigor router) and Ethernet port of VigorAP.

I-3 Network IP Configuration

After the network connection is built, the next step you should do is setup VigorAP 802 with proper network parameters, so it can work properly in your network environment.

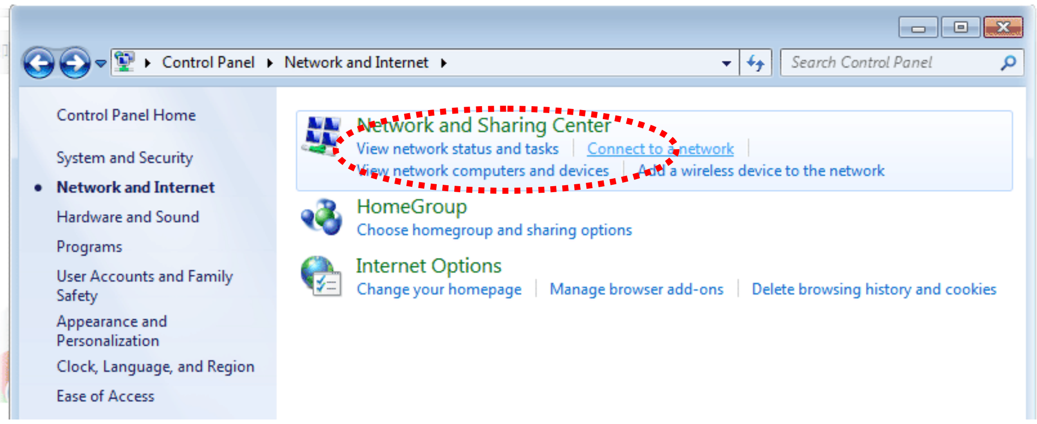
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it’s set to use static IP address, or you’re unsure, please follow the following instructions to configure your computer to use dynamic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

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

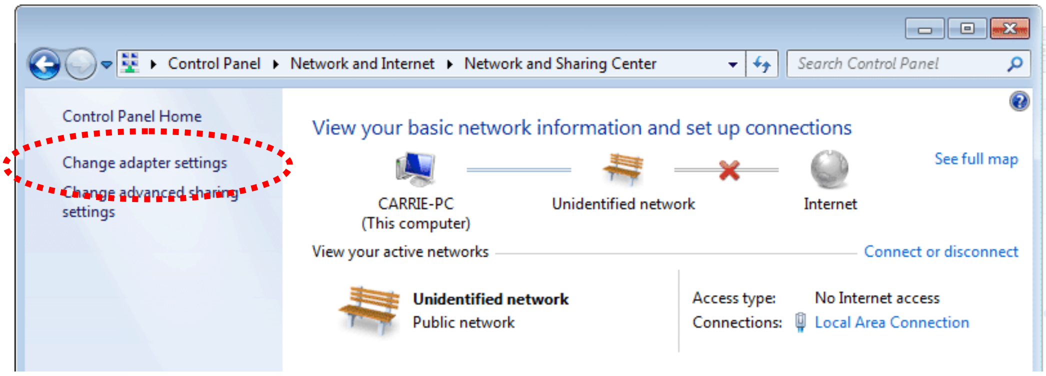
Windows 7 - **please go to section I-3-1**

I-3-1 Windows 7 IP Address Setup

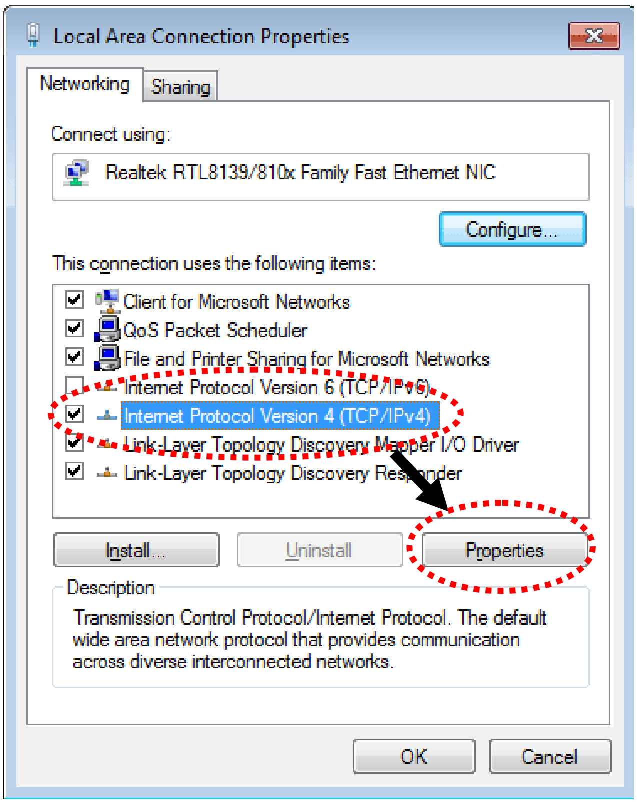
Click **Start** button (it should be located at lower-left corner of your computer), then click Control Panel. Double-click **Network and Internet**, and the following window will appear. Click **Network and Sharing Center**.


Control Panel ▸ Network and Internet ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Change your homepage
Manage browser add-ons
Delete browsing history and cookies

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



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



Local Area Connection Properties

Networking | Sharing

Connect using:

Realtek RTL8139/810x Family Fast Ethernet NIC

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- □ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

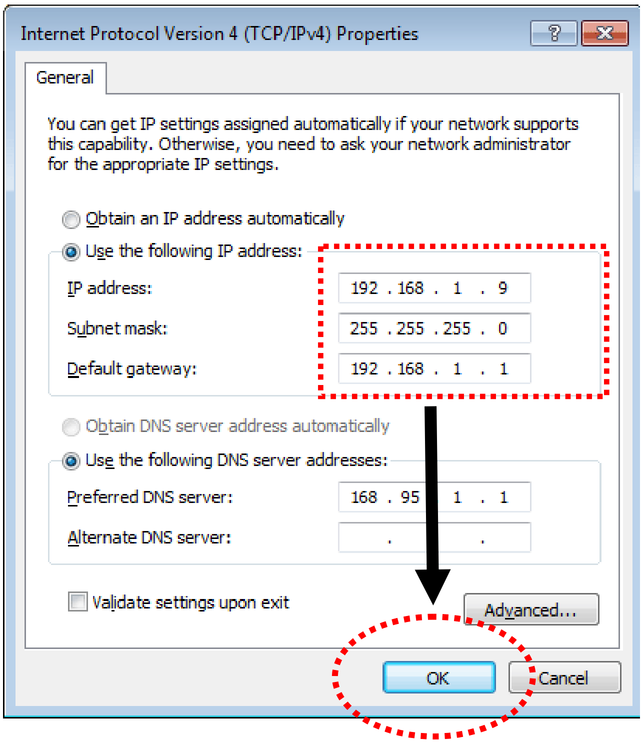
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

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

IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 168 . 95 . 1 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

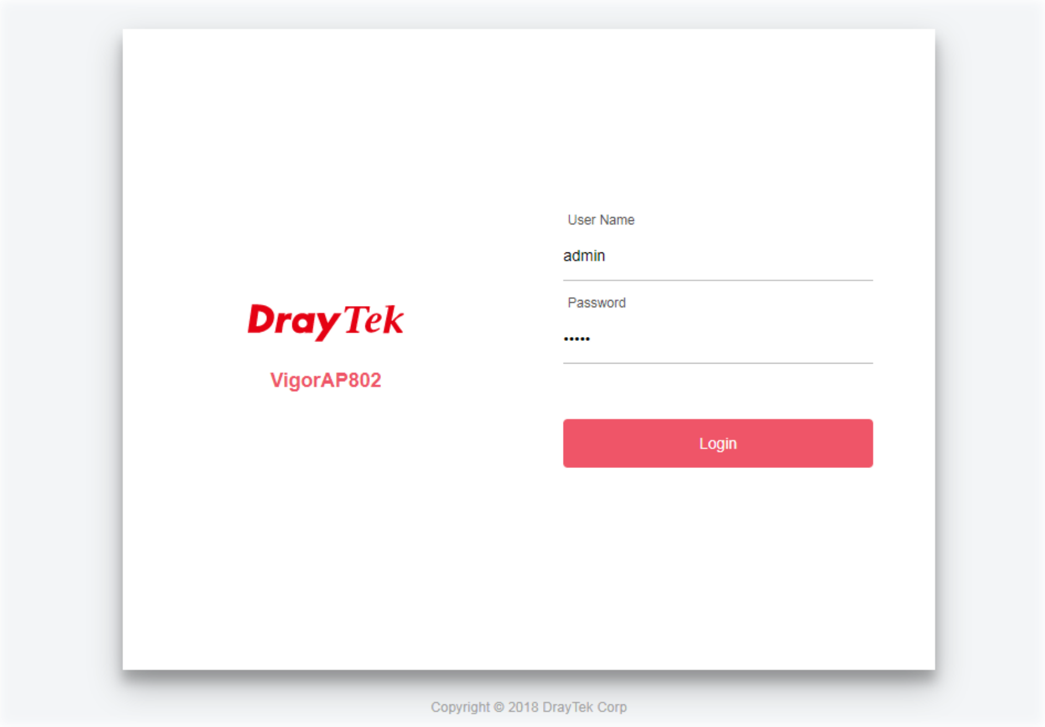
Advanced...

OK | Cancel

I-4 Accessing to Web User Interface

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

1. Make sure your PC connects to the VigorAP 802 correctly.
2. Open a web browser on your PC and type **http://192.168.1.2.** A pop-up window will open to ask for username and password. Pease type "admin/admin" on Username/Password and click **OK**.



User Name: admin

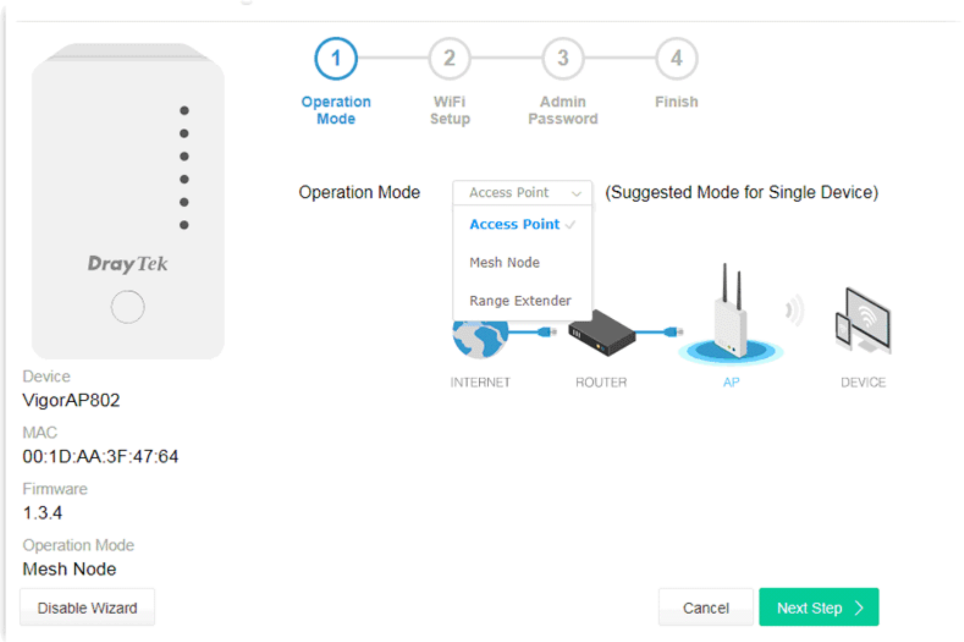
Password: •••••

ⓘ **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 802.**

- If there is no DHCP server on the network, then VigorAP 802 will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 802 will receive it's IP address via the DHCP server.
- If you connect to VigorAP by wireless LAN, you could try to access the web user interface through http://vigorap.com.

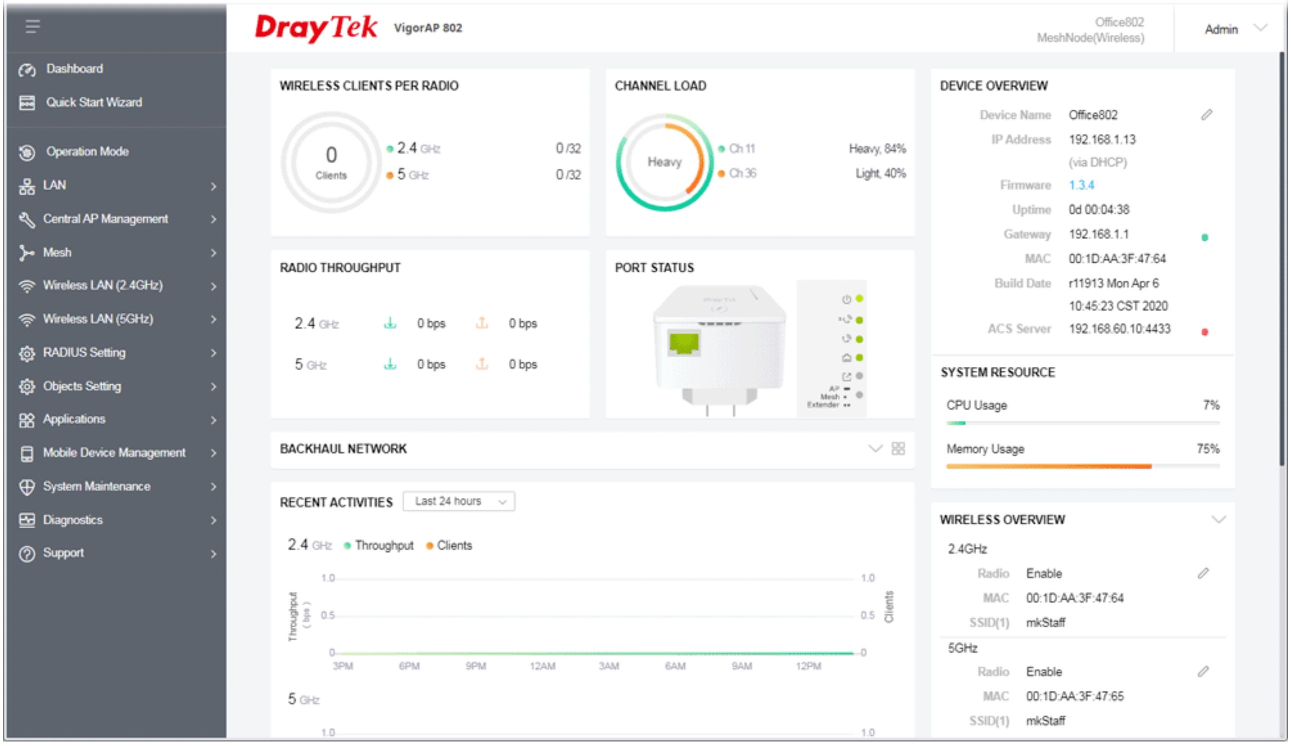
3. For the first time accessing VigorAP, the **Quick Start Wizard** for configuring wireless settings will appear as follows. Refer to *Section I-7 Quick Start Wizard for detailed information*.



Device
VigorAP802
MAC
00:1D:AA:3F:47:64
Firmware
1.3.4
Operation Mode
Mesh Node

Operation Mode: Access Point (Suggested Mode for Single Device)

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



WIRELESS CLIENTS PER RADIO

0 Clients

2.4 GHz	0 /32
5 GHz	0 /32

CHANNEL LOAD

Ch 11	Heavy, 84%
Ch 36	Light, 40%

RADIO THROUGHPUT

2.4 GHz	0 bps	0 bps
5 GHz	0 bps	0 bps

PORT STATUS

BACKHAUL NETWORK

RECENT ACTIVITIES Last 24 hours

2.4 GHz ● Throughput ● Clients

5 GHz

DEVICE OVERVIEW

Device Name	Office802
IP Address	192.168.1.13 (via DHCP)
Firmware	1.3.4
Uptime	0d 00:04:38
Gateway	192.168.1.1
MAC	00:1D:AA:3F:47:64
Build Date	r11913 Mon Apr 6 10:45:23 CST 2020
ACS Server	192.168.60.10:4433

SYSTEM RESOURCE

CPU Usage	7%
Memory Usage	75%

WIRELESS OVERVIEW

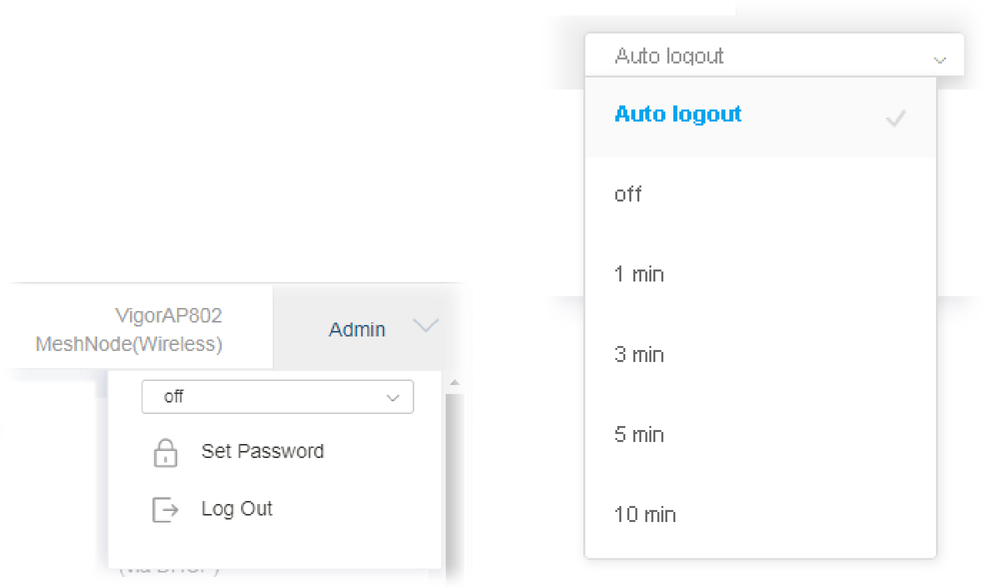
2.4GHz

Radio	Enable
MAC	00:1D:AA:3F:47:64
SSID(1)	mkStaff

5GHz

Radio	Enable
MAC	00:1D:AA:3F:47:65
SSID(1)	mkStaff

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



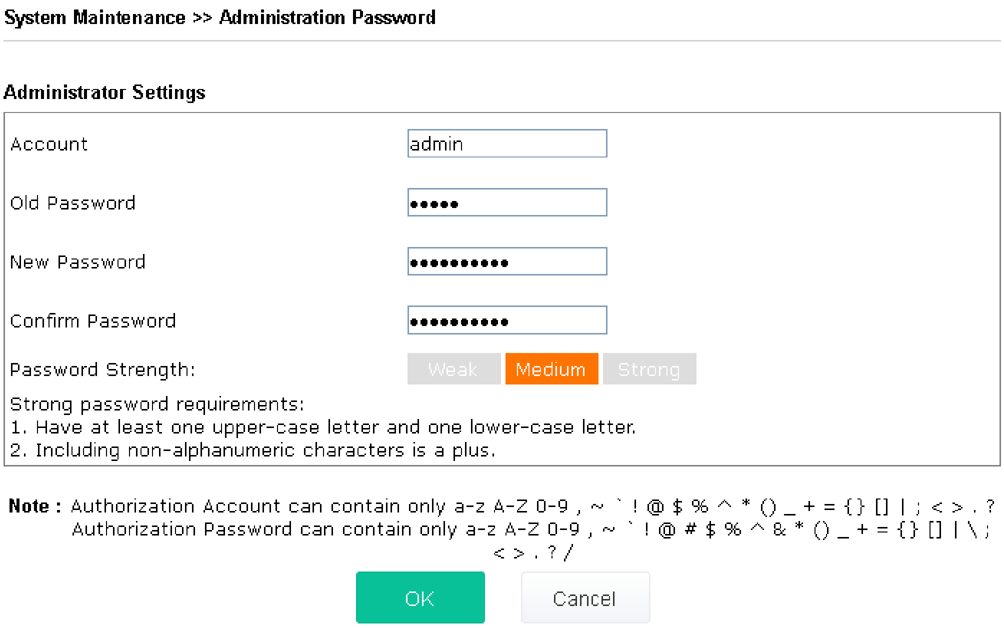
Note:

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

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

I-5 Changing Password

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



System Maintenance >> Administration Password

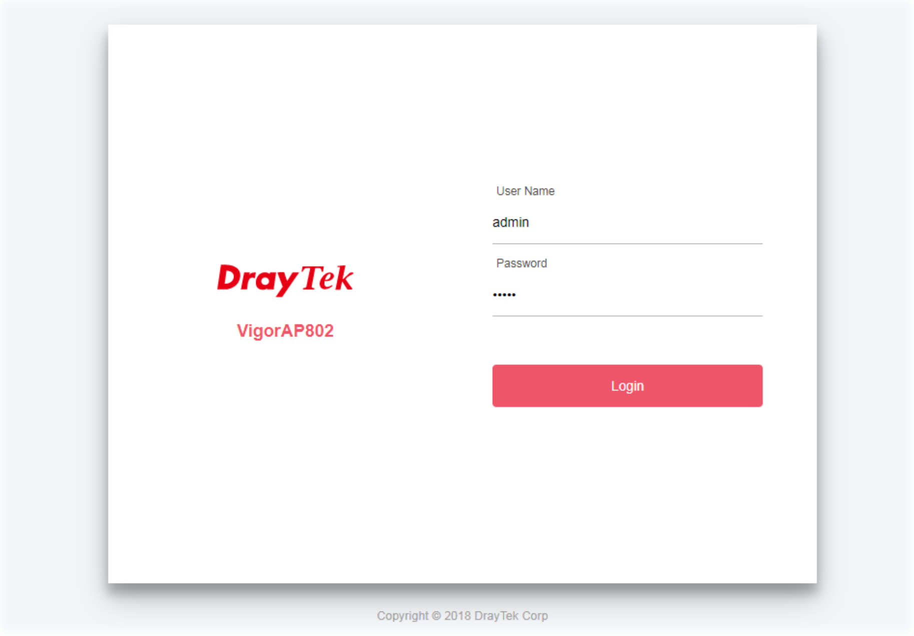
Administrator Settings

Account	admin
Old Password	●●●●●
New Password	●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●
Password Strength:	Weak Medium Strong

Strong password requirements:
1. Have at least one upper-case letter and one lower-case letter.
2. Including non-alphanumeric characters is a plus.

Note : Authorization Account can contain only a-z A-Z 0-9 , ~ ` ! @ $ % ^ * () _ + = {} [] | ; < > . ?
Authorization Password can contain only a-z A-Z 0-9 , ~ ` ! @ # $ % ^ & * () _ + = {} [] | \ ; < > . ? /

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



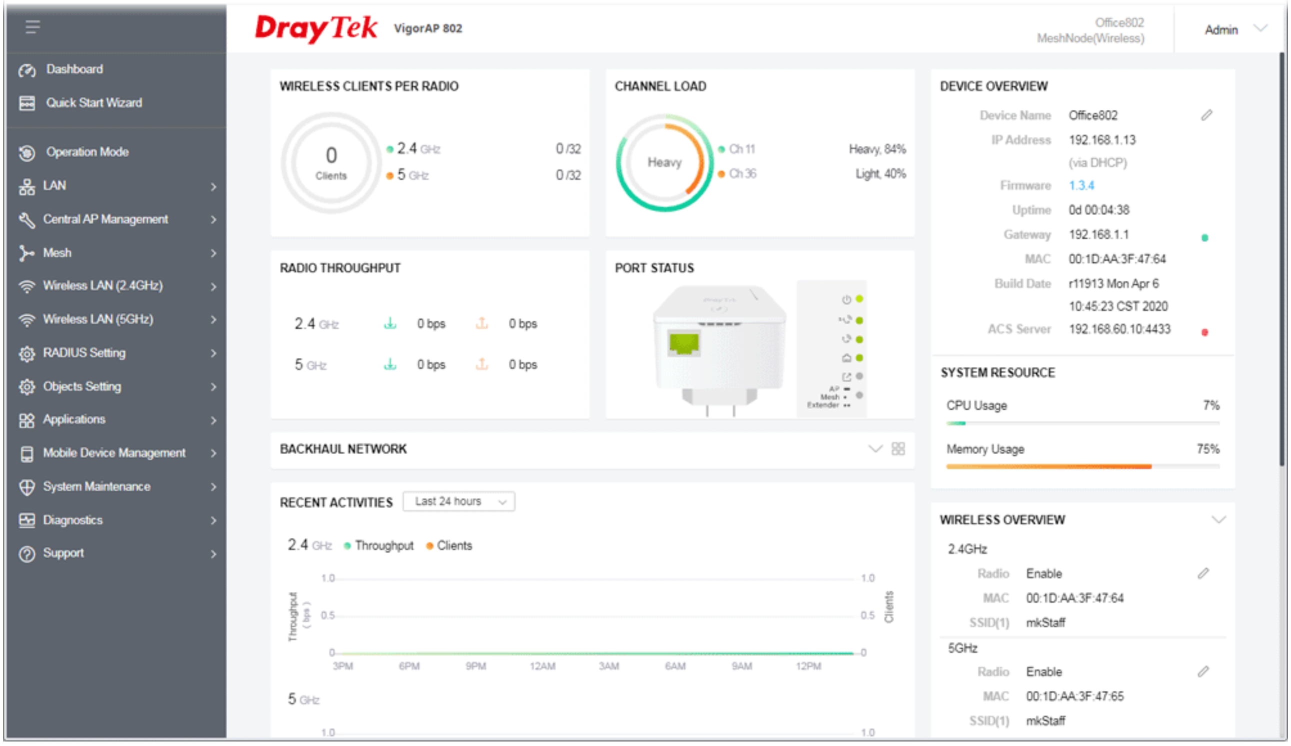
User Name: admin

Password: •••••

I-6 Dashboard

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

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



WIRELESS CLIENTS PER RADIO

0 Clients

- 2.4 GHz 0 /32
- 5 GHz 0 /32

CHANNEL LOAD

- Ch 11 Heavy, 84%
- Ch 36 Light, 40%

DEVICE OVERVIEW

Device Name Office802
IP Address 192.168.1.13 (via DHCP)
Firmware 1.3.4
Uptime 0d 00:04:38
Gateway 192.168.1.1
MAC 00:1D:AA:3F:47:64
Build Date r11913 Mon Apr 6 10:45:23 CST 2020
ACS Server 192.168.60.10:4433

RADIO THROUGHPUT

2.4 GHz 0 bps 0 bps
5 GHz 0 bps 0 bps

PORT STATUS

SYSTEM RESOURCE

CPU Usage 7%
Memory Usage 75%

BACKHAUL NETWORK

RECENT ACTIVITIES Last 24 hours

2.4 GHz ● Throughput ● Clients

5 GHz

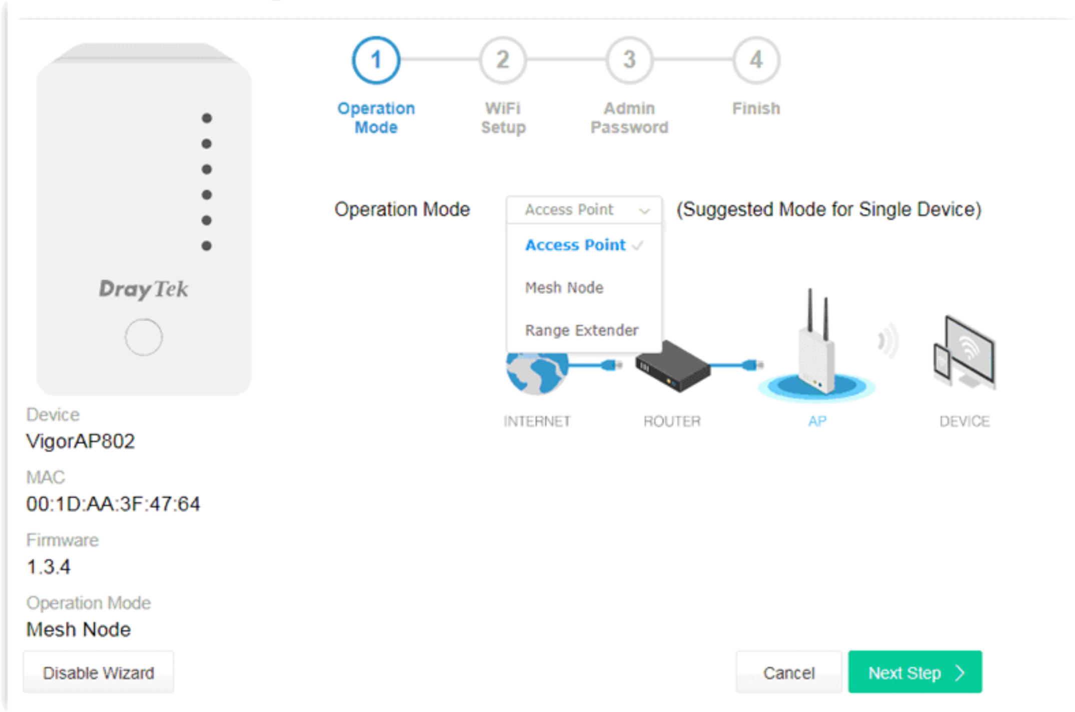
WIRELESS OVERVIEW

2.4GHz
Radio Enable
MAC 00:1D:AA:3F:47:64
SSID(1) mkStaff

5GHz
Radio Enable
MAC 00:1D:AA:3F:47:65
SSID(1) mkStaff

I-7 Quick Start Wizard

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



Operation Mode: Access Point (Suggested Mode for Single Device)

Device: VigorAP802

MAC: 00:1D:AA:3F:47:64

Firmware: 1.3.4

Operation Mode: Mesh Node

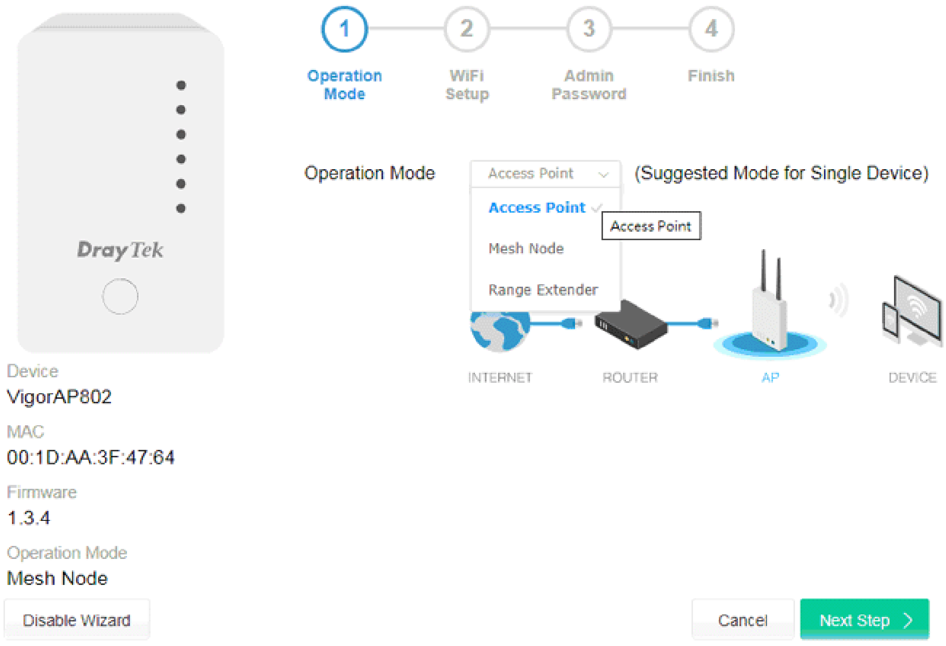
Available operation mode includes:

- Access Point
- Mesh Node
- Range Extender

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

I-7-1 Settings for Access Point

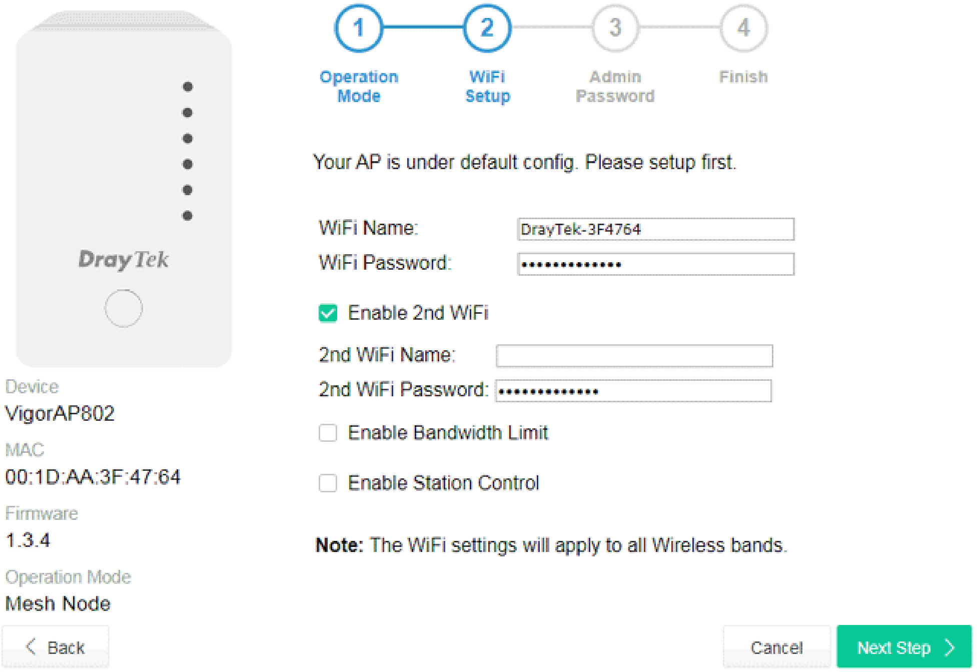
1. Choose **Access Point** as the operation mode and click **Next Step**.



Device
VigorAP802
MAC
00:1D:AA:3F:47:64
Firmware
1.3.4
Operation Mode
Mesh Node

Operation Mode: Access Point (Suggested Mode for Single Device)

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



Device
VigorAP802
MAC
00:1D:AA:3F:47:64
Firmware
1.3.4
Operation Mode
Mesh Node

Your AP is under default config. Please setup first.

WiFi Name: DrayTek-3F4764
WiFi Password: •••••••••••••

☑ Enable 2nd WiFi

2nd WiFi Name:
2nd WiFi Password: •••••••••••••

□ Enable Bandwidth Limit

□ Enable Station Control

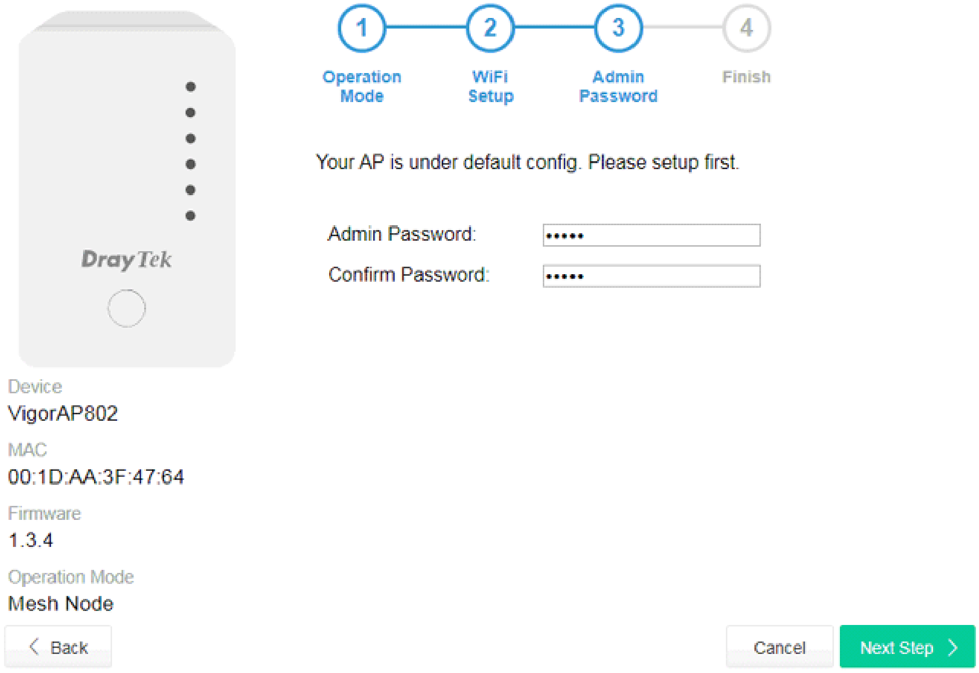
Note: The WiFi settings will apply to all Wireless bands.

Available settings are explained as follows:

Item	Description
WiFi Name	Display the default name with the rule of DrayTek-last three MAC address.

	Change a name for VigorAP 802 to be identified if you want.
WiFi Password	Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Enable 2nd WiFi	Check the box to enable the second wireless setting. Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. **2nd WiFi Name** - Set a name for VigorAP 802 which can be identified and connected by wireless guest. **2nd WiFi Password -** Set **8~63** ASCII characters which can be used for logging into VigorAP 802 by wireless guest.
Enable Bandwidth Limit	Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID. **Upload Limit** – Scroll the radio button to choose the value you want. **Download Limit** –Scroll the radio button to choose the value you want.
Enable Station Control	Check the box to set the duration for the guest connecting /reconnecting to Vigor device. **Connection Time** –Scroll the radio button to choose the value you want. **Reconnection Time** –Scroll the radio button to choose the value you want.

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



Your AP is under default config. Please setup first.

Admin Password: •••••

Confirm Password: •••••

Device
VigorAP802

MAC
00:1D:AA:3F:47:64

Firmware
1.3.4

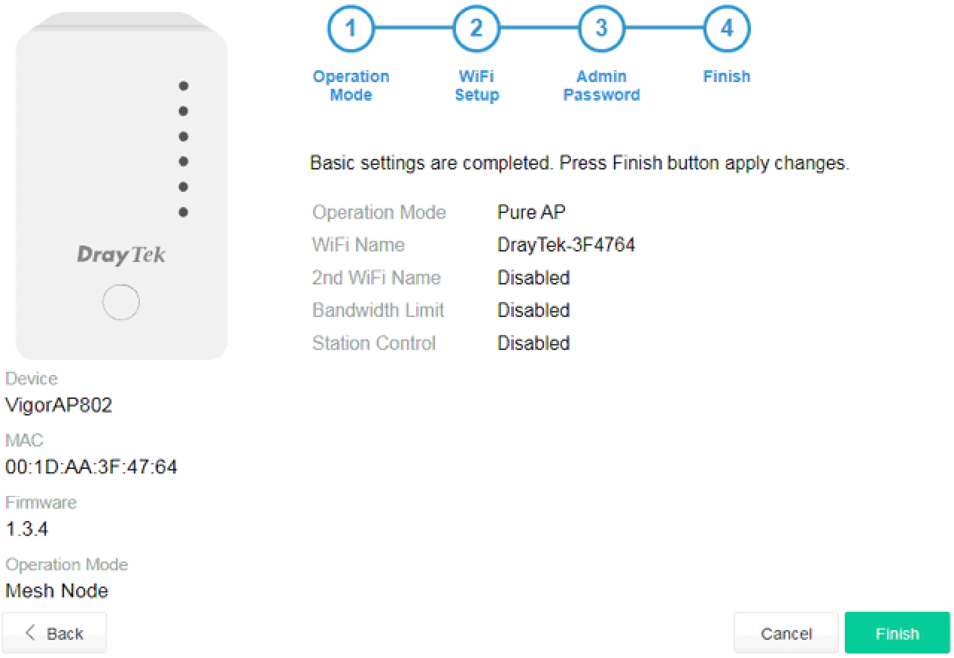
Operation Mode
Mesh Node

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 settings configuration will be shown on screen. Click **Finish**.



Basic settings are completed. Press Finish button apply changes.

Operation Mode	Pure AP
WiFi Name	DrayTek-3F4764
2nd WiFi Name	Disabled
Bandwidth Limit	Disabled
Station Control	Disabled

Device
VigorAP802

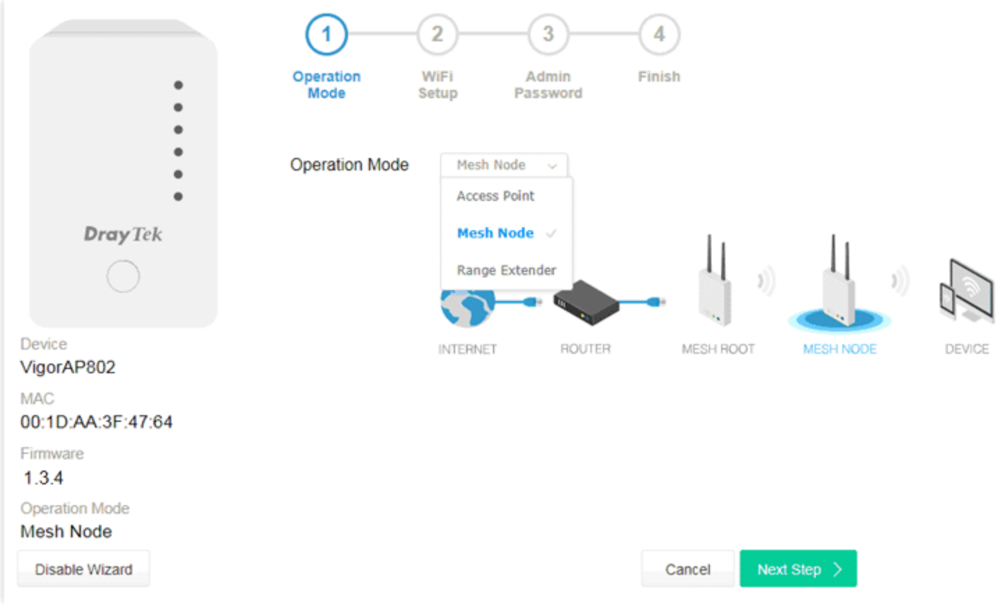
MAC
00:1D:AA:3F:47:64

Firmware
1.3.4

Operation Mode
Mesh Node

I-7-2 Settings for Mesh Node

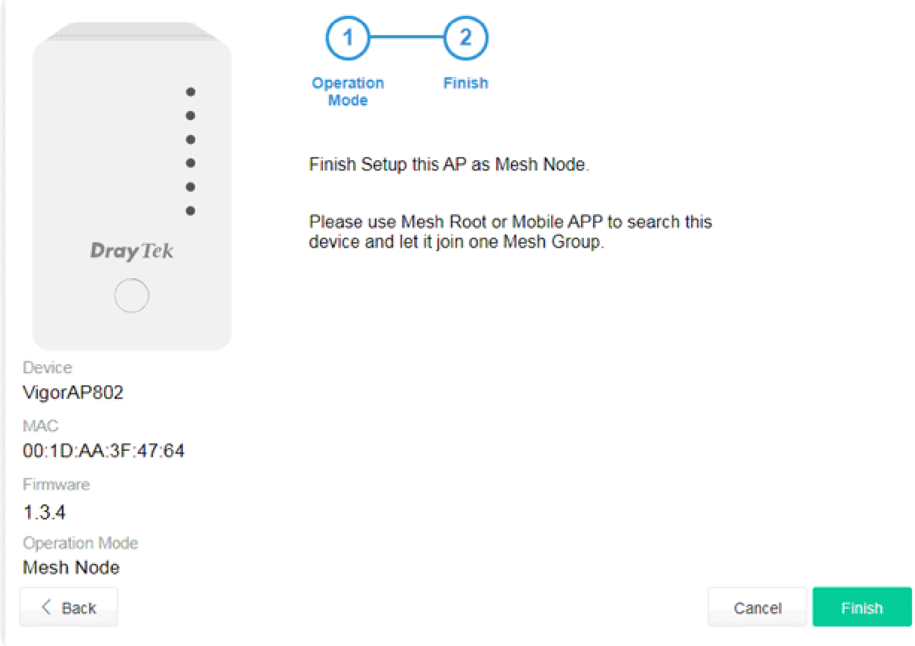
1. Choose **Mesh Node** as the operation mode and click **Next Step**.



Operation Mode: Mesh Node

Device
VigorAP802
MAC
00:1D:AA:3F:47:64
Firmware
1.3.4
Operation Mode
Mesh Node

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



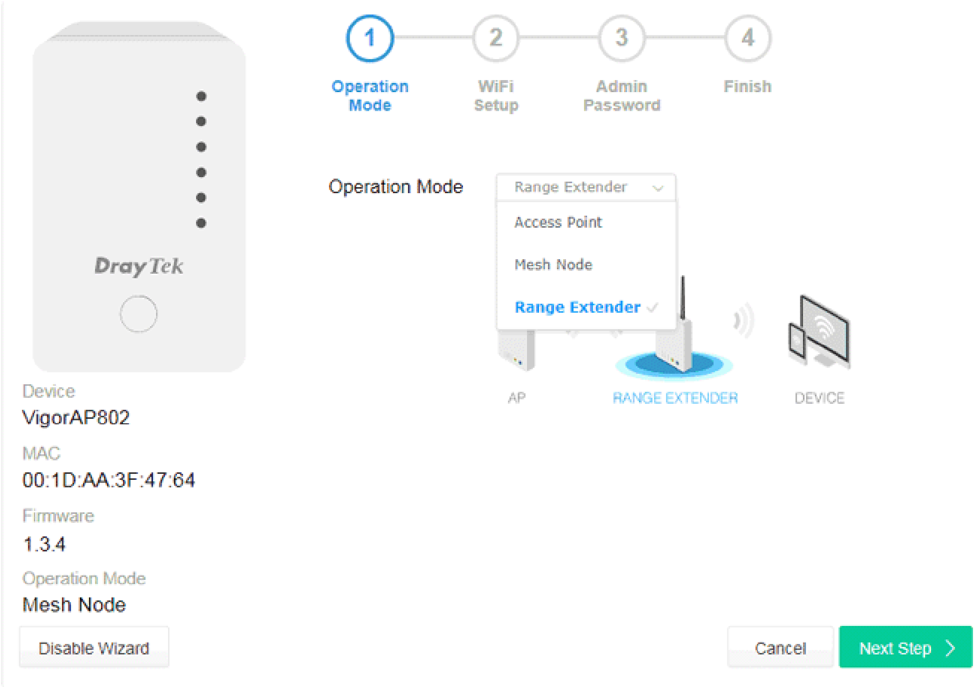
Finish Setup this AP as Mesh Node.

Please use Mesh Root or Mobile APP to search this device and let it join one Mesh Group.

Device
VigorAP802
MAC
00:1D:AA:3F:47:64
Firmware
1.3.4
Operation Mode
Mesh Node

I-7-3 Settings for Range Extender

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



Operation Mode: Range Extender

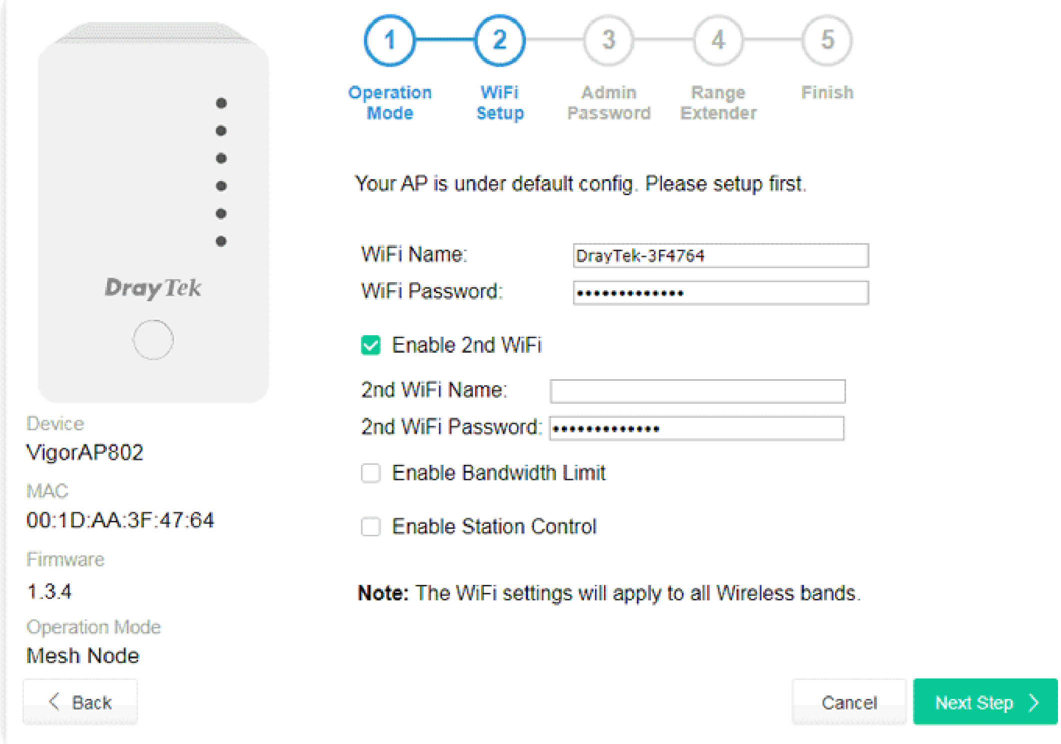
Device
VigorAP802

MAC
00:1D:AA:3F:47:64

Firmware
1.3.4

Operation Mode
Mesh Node

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



Your AP is under default config. Please setup first.

WiFi Name: DrayTek-3F4764

WiFi Password: •••••••••••••

☑ Enable 2nd WiFi

2nd WiFi Name:

2nd WiFi Password: •••••••••••••

☐ Enable Bandwidth Limit

☐ Enable Station Control

Note: The WiFi settings will apply to all Wireless bands.

Device
VigorAP802

MAC
00:1D:AA:3F:47:64

Firmware
1.3.4

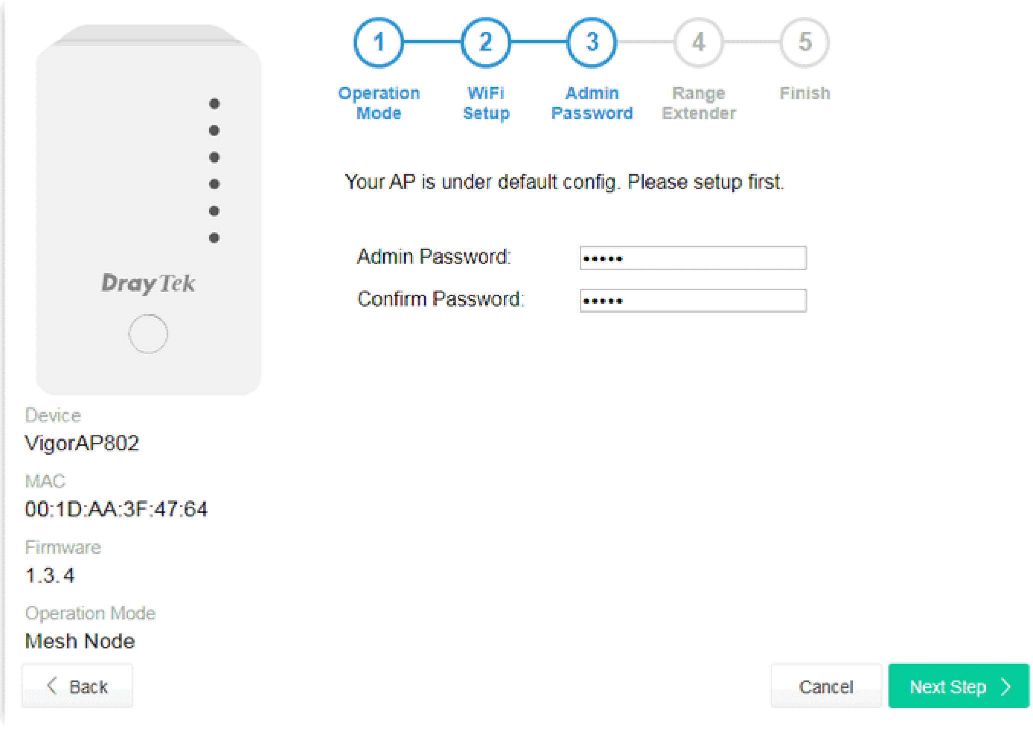
Operation Mode
Mesh Node

Available settings are explained as follows:

Item	Description

WiFi Name	Display the default name with the rule of DrayTek-last three MAC address. Change a name for VigorAP 802 to be identified if you want.
WiFi Password	Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Enable 2nd WiFi	Check the box to enable the second wireless setting. Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. **2nd WiFi Name** - Set a name for VigorAP 802 which can be identified and connected by wireless guest. **2nd WiFi Password -** Set **8~63** ASCII characters or **8~63** ASCII characters which can be used for logging into VigorAP 802 by wireless guest.
Enable Bandwidth Limit	Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID. **Upload Limit** – Scroll the radio button to choose the value you want. **Download Limit** –Scroll the radio button to choose the value you want.
Enable Station Control	Check the box to set the duration for the guest connecting /reconnecting to Vigor device. **Connection Time** –Scroll the radio button to choose the value you want. **Reconnection Time** –Scroll the radio button to choose the value you want.

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



Your AP is under default config. Please setup first.

Admin Password: •••••

Confirm Password: •••••

Device
VigorAP802

MAC
00:1D:AA:3F:47:64

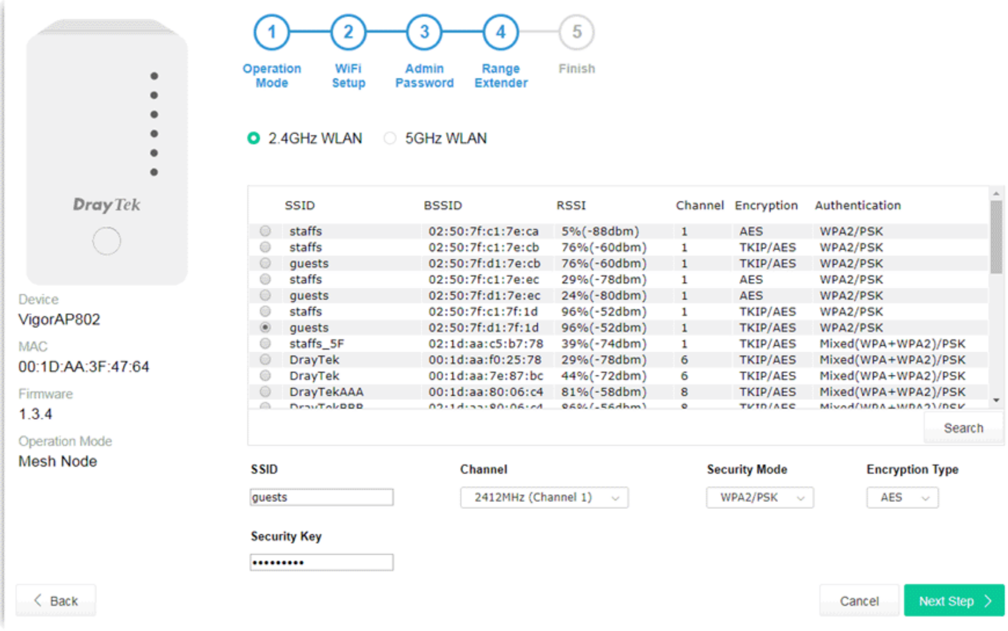
Firmware
1.3.4

Operation Mode
Mesh Node

Available settings are explained as follows:

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

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



● 2.4GHz WLAN ○ 5GHz WLAN

	SSID	BSSID	RSSI	Channel	Encryption	Authentication
○	staffs	02:50:7f:c1:7e:ca	5%(-88dbm)	1	AES	WPA2/PSK
○	staffs	02:50:7f:c1:7e:cb	76%(-60dbm)	1	TKIP/AES	WPA2/PSK
○	guests	02:50:7f:d1:7e:cb	76%(-60dbm)	1	TKIP/AES	WPA2/PSK
○	staffs	02:50:7f:c1:7e:ec	29%(-78dbm)	1	AES	WPA2/PSK
○	guests	02:50:7f:d1:7e:ec	24%(-80dbm)	1	AES	WPA2/PSK
○	staffs	02:50:7f:c1:7f:1d	96%(-52dbm)	1	TKIP/AES	WPA2/PSK
●	guests	02:50:7f:d1:7f:1d	96%(-52dbm)	1	TKIP/AES	WPA2/PSK
○	staffs_5F	02:1d:aa:c5:b7:78	39%(-74dbm)	1	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	DrayTek	00:1d:aa:f0:25:78	29%(-78dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	DrayTek	00:1d:aa:7e:87:bc	44%(-72dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	DrayTekAAA	00:1d:aa:80:06:c4	81%(-58dbm)	8	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	DrayTekBBB	02:1d:aa:80:06:c4	86%(-56dbm)	8	TKIP/AES	Mixed(WPA+WPA2)/PSK

SSID: guests

Channel: 2412MHz (Channel 1)

Security Mode: WPA2/PSK

Encryption Type: AES

Security Key: •••••••••

Device
VigorAP802

MAC
00:1D:AA:3F:47:64

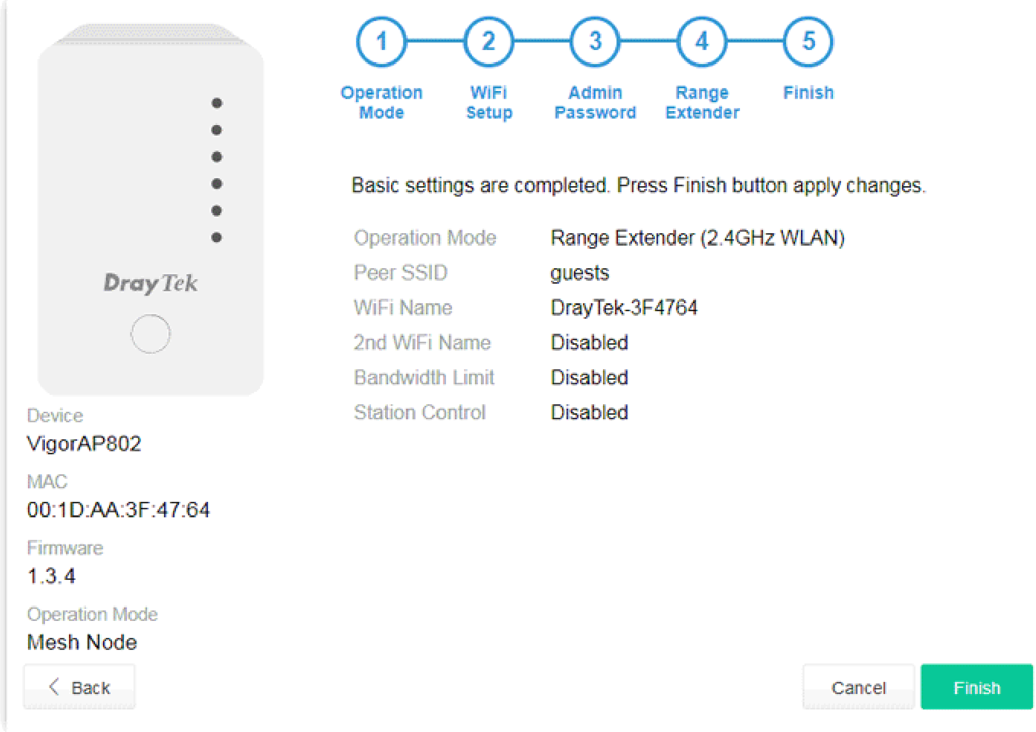
Firmware
1.3.4

Operation Mode
Mesh Node

Available settings are explained as follows:

Item	Description
SSID/Security Key	Once the access point specified above, the name / security key of the AP will be shown automatically in these fields.
Channel	Means the channel frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.
Encryption Type	Available options will vary according to the selected **Security Mode**. **When Open** i**s selected**: ● Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. ● **WEP Keys** –To enable WEP encryption for data transmission, please choose **WEP**. Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. **When Shared** i**s selected**: ● **WEP Keys** - To enable WEP encryption for data transmission, please choose **WEP**. Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. **When WPA/PSK or WPA2/PSK** i**s selected**: ● Select **TKIP** or **AES** as the algorithm for WPA. ● **Security Key** - Select WEP, TKIP or AES as the encryption algorithm. Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

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



Basic settings are completed. Press Finish button apply changes.

Operation Mode	Range Extender (2.4GHz WLAN)
Peer SSID	guests
WiFi Name	DrayTek-3F4764
2nd WiFi Name	Disabled
Bandwidth Limit	Disabled
Station Control	Disabled

Device
VigorAP802

MAC
00:1D:AA:3F:47:64

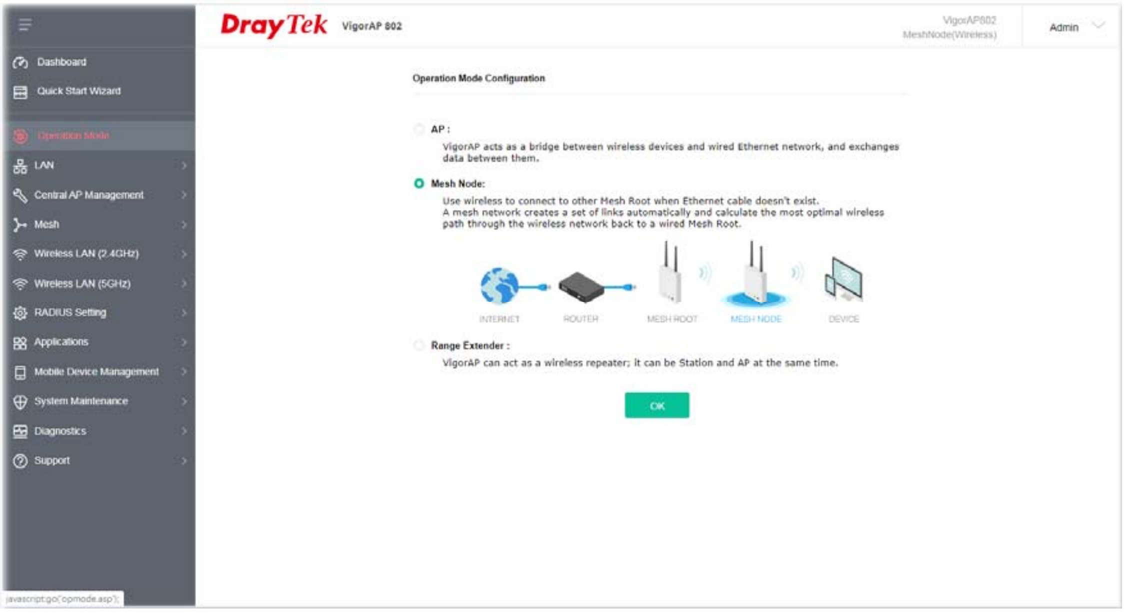
Firmware
1.3.4

Operation Mode
Mesh Node

Chapter II Connectivity

II-1 Operation Mode

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



Operation Mode Configuration

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

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

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

Available settings are explained as follows:

Item	Description
AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
Mesh	**Mesh Root –** VigorAP must connect to a gateway with an Ethernet cable. **Mesh Node –** VigorAP can connect to other mesh root via wireless connection. A mesh network creates one set of links automatically and calculates the most optimal wireless path through the wireless network back to a wired mesh root.
Range Extender	VigorAP can act as a wireless repeater which will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.

ⓘ **Note:**

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

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

VigorAP 802 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 802 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 802 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 802. The **General Setup** will set up the information of this wireless network, including its SSID as identification, located channel etc.

Security Overview

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

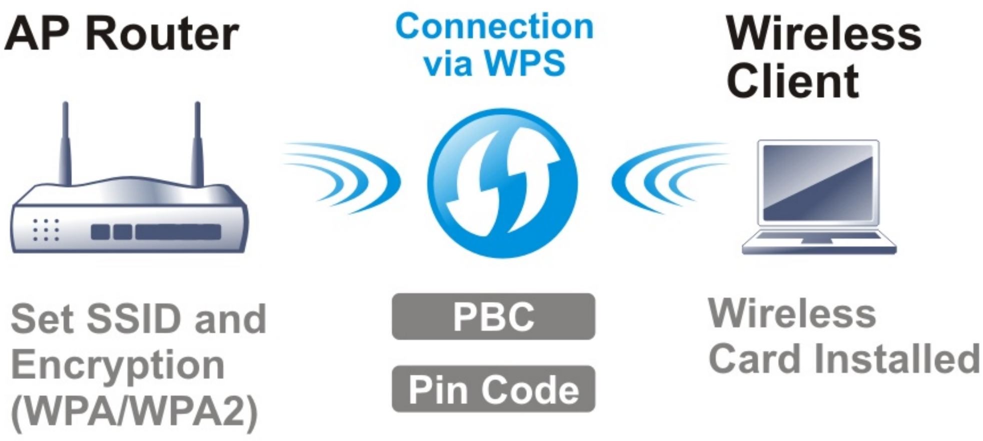
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The VigorAP 802 is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

WPS Introduction

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (VigorAP 802) with the encryption of WPA and WPA2.



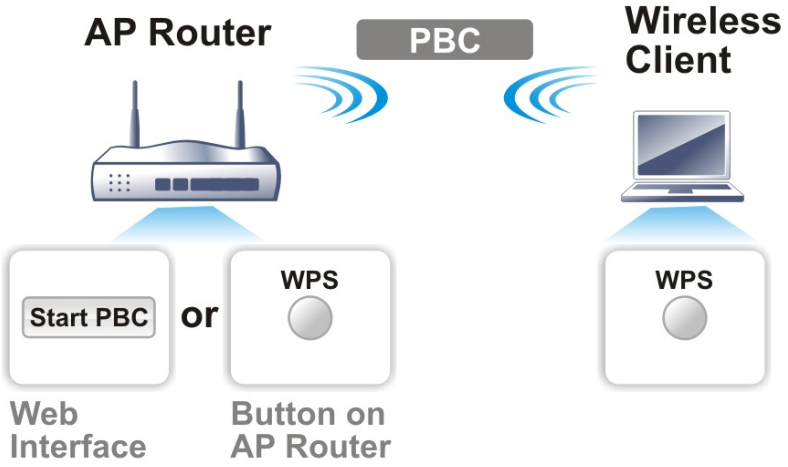
It is the simplest way to build connection between wireless network clients and VigorAP 802. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 802 automatically.

ⓘ **Note:**

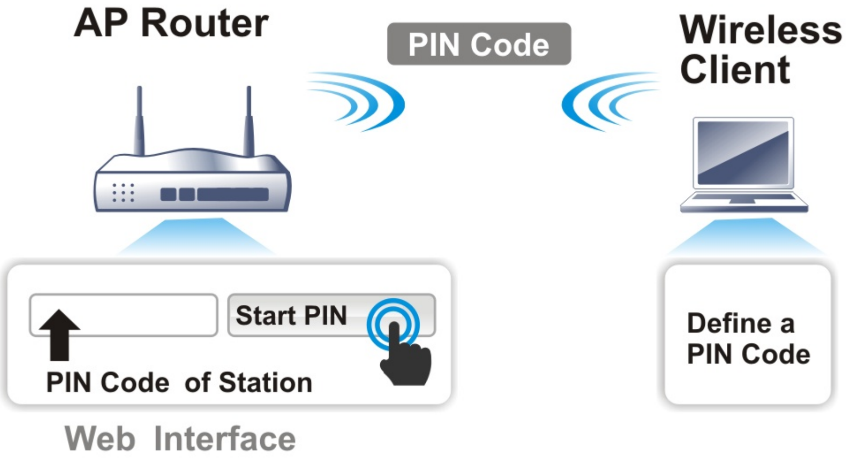
Such function is available for the wireless station with WPS supported.

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

On the side of VigorAP 802 series which served as an AP, press **WPS** button once on the front panel of VigorAP 802 or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.

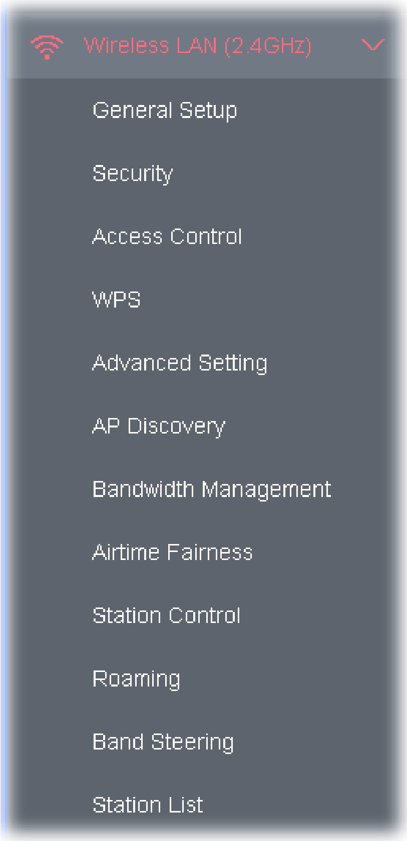


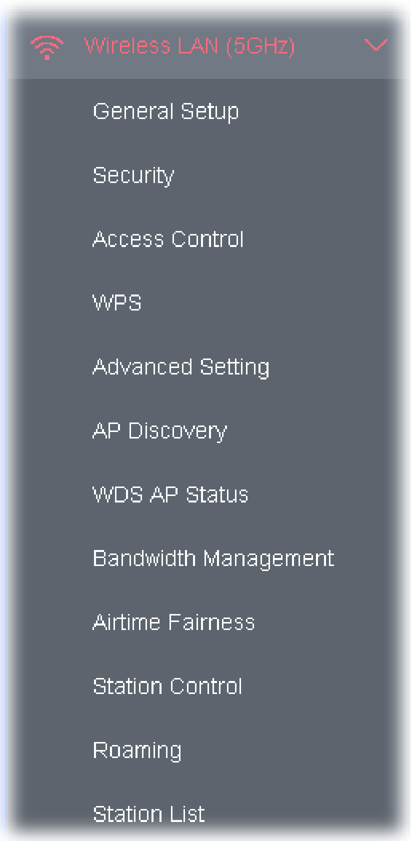
If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 802.


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

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.

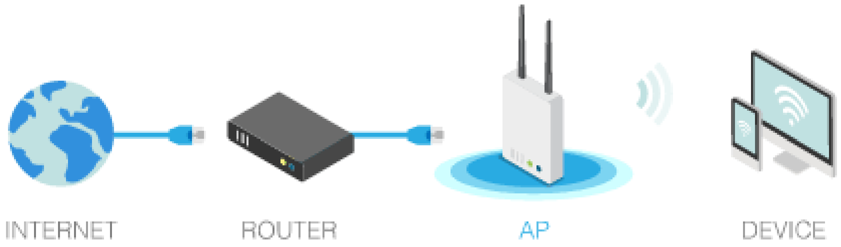




Note:

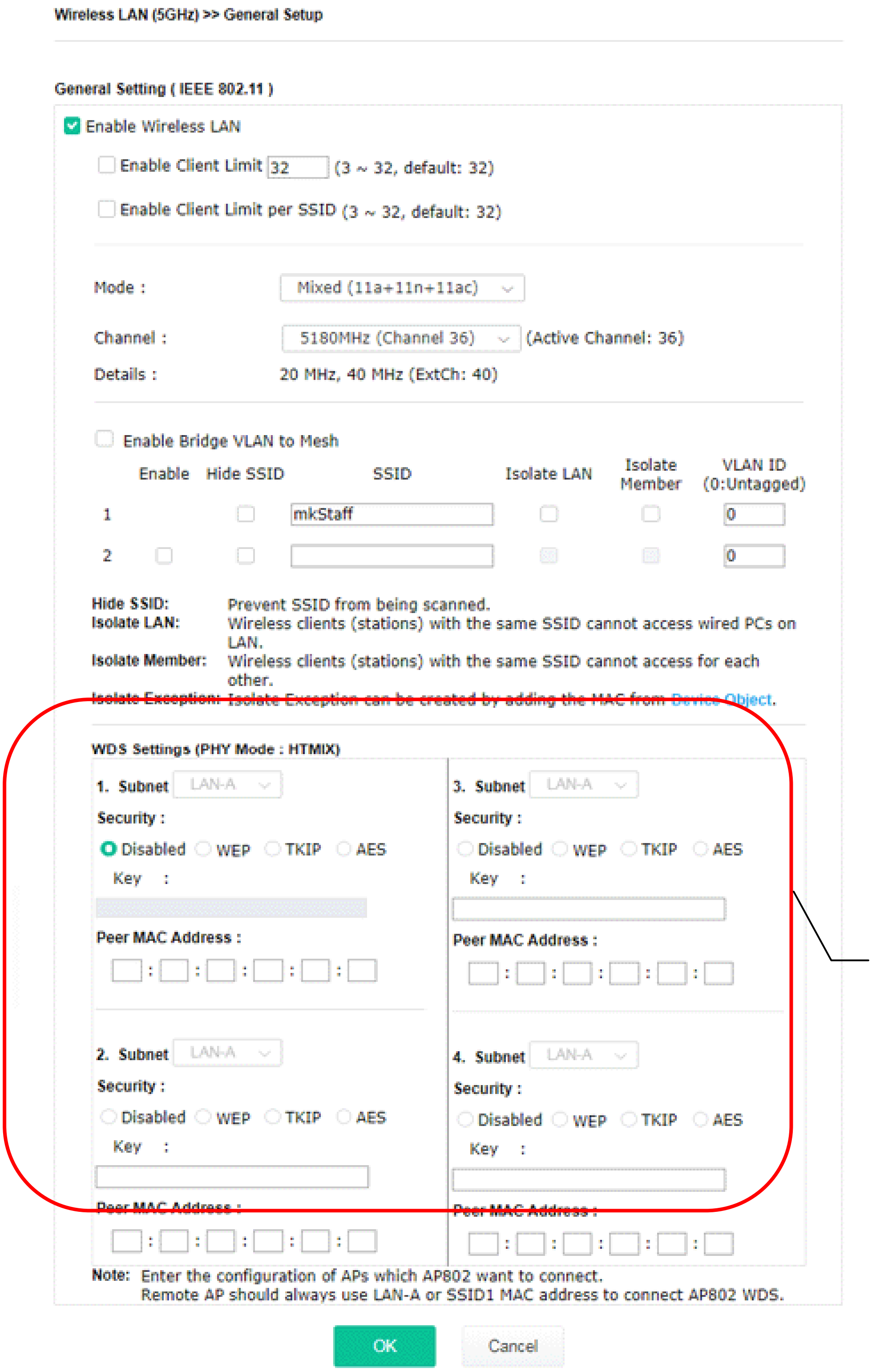
Available settings for **Wireless LAN (2.4GHz) and Wireless LAN (5Ghz)** are almost the same, except for Band Steering.

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 WDS. Please refer to the following figure for more information.



Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

□ Enable Client Limit 32 (3 ~ 32, default: 32)

□ Enable Client Limit per SSID (3 ~ 32, default: 32)

Mode : Mixed (11a+11n+11ac)

Channel : 5180MHz (Channel 36) (Active Channel: 36)

Details : 20 MHz, 40 MHz (ExtCh: 40)

□ Enable Bridge VLAN to Mesh

	Enable	Hide SSID	SSID	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)
1		□	mkStaff	□	□	0
2	□	□		□	□	0

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

WDS Settings (PHY Mode : HTMIX)

1. Subnet LAN-A
Security :
● Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

2. Subnet LAN-A
Security :
○ Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

3. Subnet LAN-A
Security :
○ Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

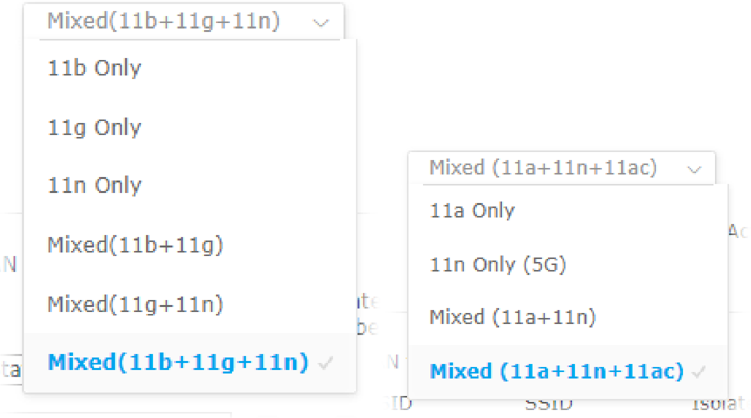
4. Subnet LAN-A
Security :
○ Disabled ○ WEP ○ TKIP ○ AES
Key :
Peer MAC Address :
□ : □ : □ : □ : □ : □

Note: Enter the configuration of APs which AP802 want to connect.
Remote AP should always use LAN-A or SSID1 MAC address to connect AP802 WDS.

Available for 5GHz Access Point Mode

Available settings are explained as follows:

Item	Description

Enable Wireless LAN	Check the box to enable wireless function.
Enable Client Limit	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor device. The number you can set is from 3 to 64.
Enable Client Limit per SSID	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
Mode	At present, VigorAP 802 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.  Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n) Mixed (11a+11n+11ac) 11a Only 11n Only (5G) Mixed (11a+11n) Mixed (11a+11n+11ac)
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let system determine for you.
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above. Configure the extension channel you want.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 802 while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Display the default name with the rule of DrayTek-last three MAC address. Change a name for VigorAP 802 to be identified if you want.
Isolate LAN	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not access for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0

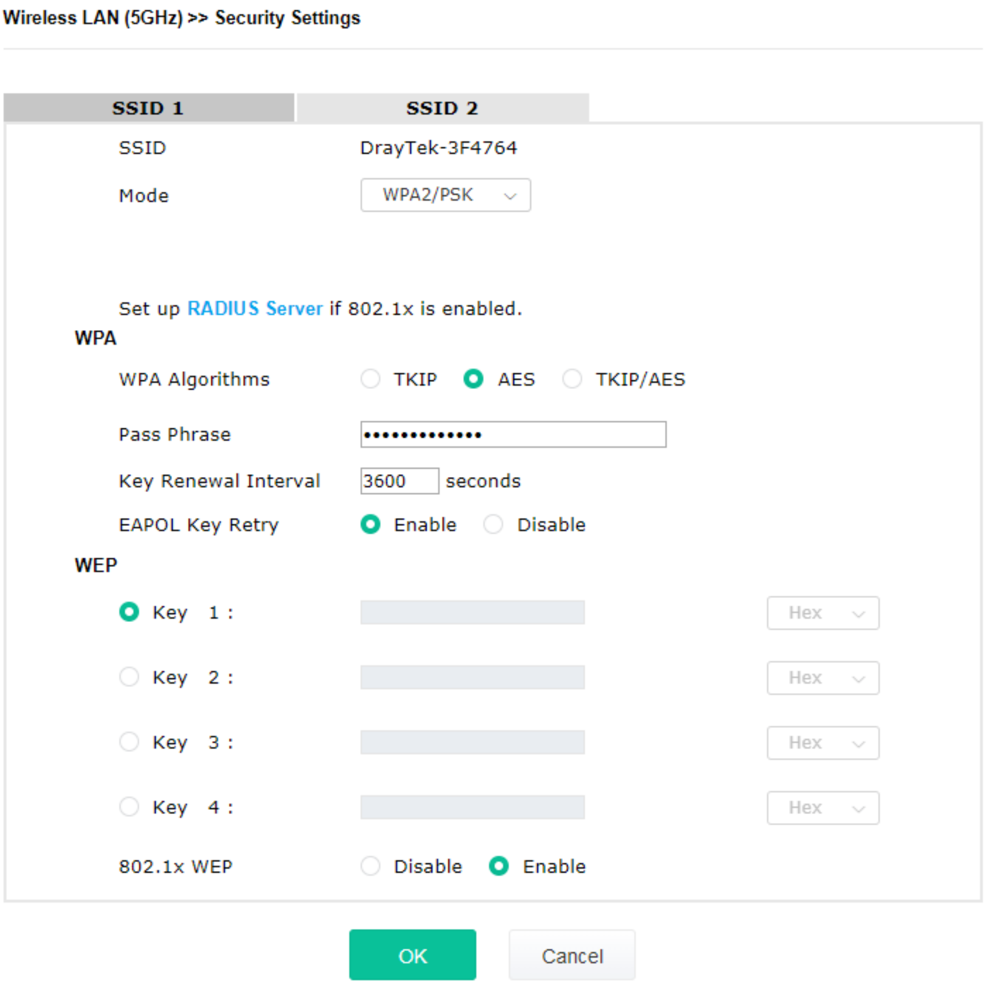
	by default, it means disabling the VLAN function for the SSID.
PHY Mode	Data will be transmitted via HTMIX mode. Each access point should be setup to the same **Phy Mode** for connecting with each other.
Security	Select WEP, TKIP or AES as the encryption algorithm. Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 902 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.



Wireless LAN (5GHz) >> Security Settings

SSID	DrayTek-3F4764
Mode	WPA2/PSK

Set up RADIUS Server if 802.1x is enabled.

WPA

WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Pass Phrase	•••••••••••••
Key Renewal Interval	3600 seconds
EAPOL Key Retry	● Enable ○ Disable

WEP

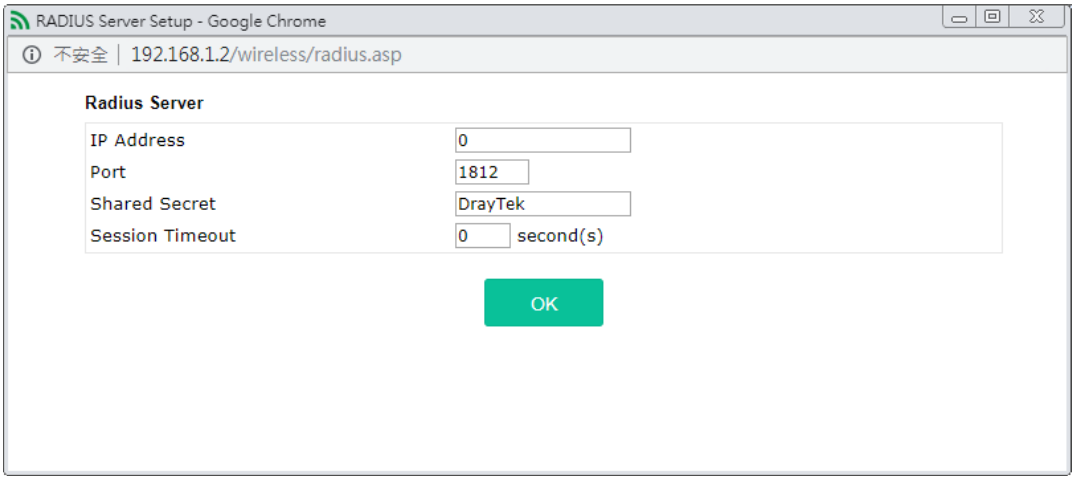
● Key 1 :		Hex
○ Key 2 :		Hex
○ Key 3 :		Hex
○ Key 4 :		Hex
802.1x WEP	○ Disable ● Enable	

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose. **Disable** - The encryption mechanism is turned off. **WEP** - Accepts only WEP clients and the encryption key should be entered in WEP Key. **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK -** Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. **WEP/802.1x -** The built-in RADIUS client feature enables VigorAP 802 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized

	remote access authentication for network management. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode. **WPA/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. **WPA2/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for **WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Pass Phrase	Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for **WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Click **Enable** to make sure that the key will be installed and used once in order to prevent key reinstallation attack.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for **WEP** mode.
802.1x WEP	**Disable** - Disable the WEP Encryption. Data sent to the AP will not be encrypted. **Enable** - Enable the WEP Encryption. Such feature is available for **WEP/802.1x** mode.

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


RADIUS Server Setup - Google Chrome
不安全 | 192.168.1.2/wireless/radius.asp
OK

Radius Server

IP Address	0
Port	1812
Shared Secret	DrayTek
Session Timeout	0 second(s)

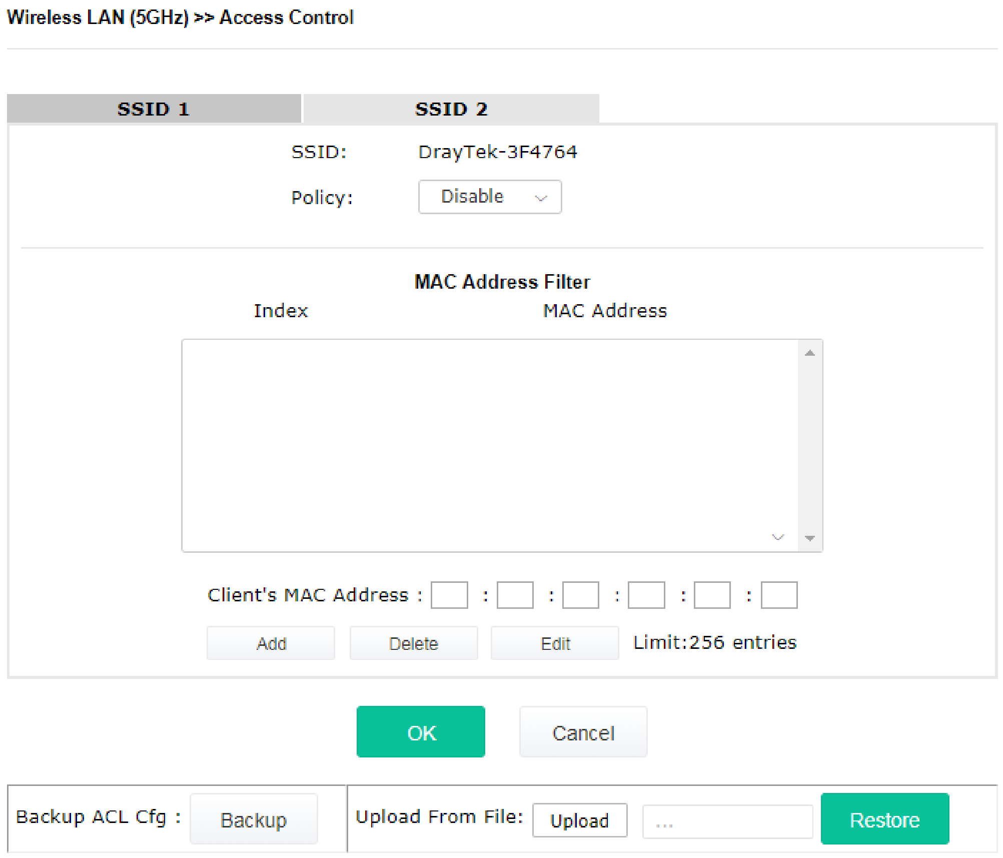
Available settings are explained as follows:

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

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

II-3-3 Access Control

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



Wireless LAN (5GHz) >> Access Control

SSID 1 | SSID 2

SSID: DrayTek-3F4764

Policy: Disable

MAC Address Filter

Index | MAC Address

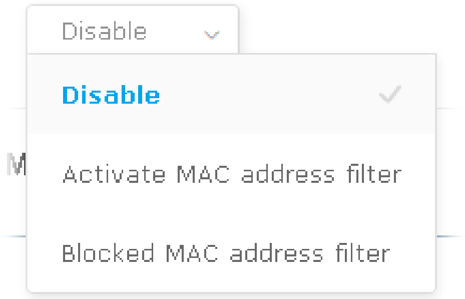
Client's MAC Address : __ : __ : __ : __ : __ : __

Add | Delete | Edit | Limit:256 entries

OK | Cancel

Backup ACL Cfg : Backup | Upload From File: Upload ... | Restore

Available settings are explained as follows:

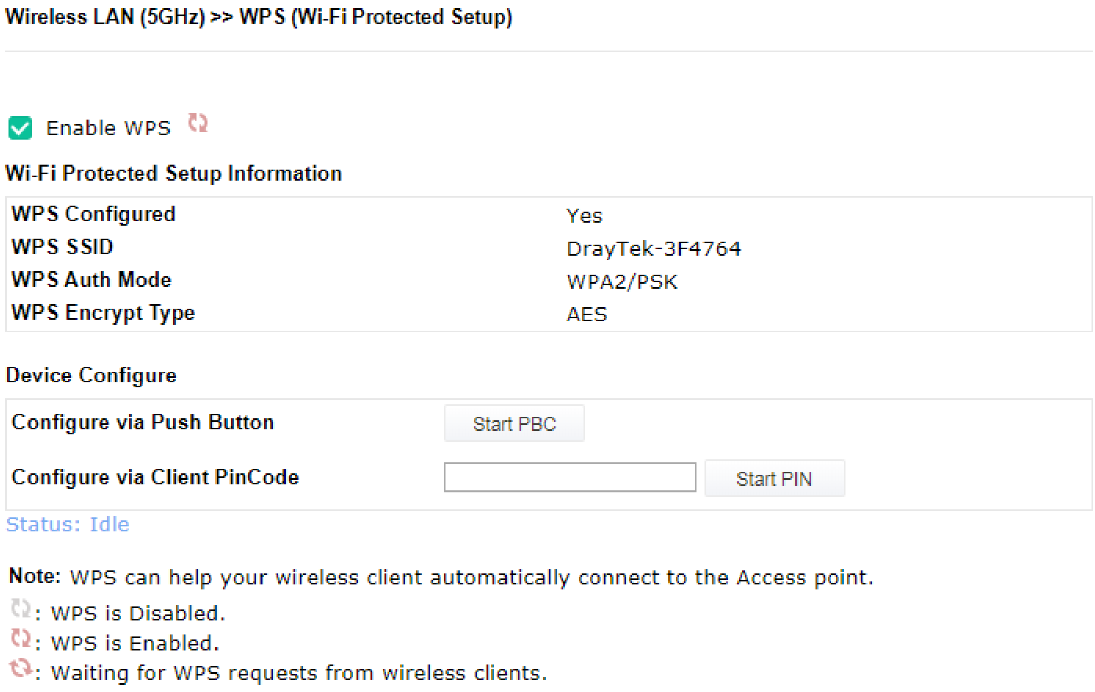
Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 802.  Disable Disable ✓ Activate MAC address filter Blocked MAC address filter

MAC Address Filter	Display all MAC addresses that are edited before.
MAC	**Client's MAC Address -** Manually enter the MAC address of wireless client. **Add -** Add a new MAC address into the list. **Delete -** Delete the selected MAC address in the list. **Edit -** Edit the selected MAC address in the list.
Object	In addition to enter the MAC address of the device manually, you can **Device Group** - Select one of the existed device groups and click **Add**. All the devices belonging to the selected group will be shown on the MAC Address Filter table. **Device Object** - Select one of the existed device object and click **Add**. The MAC address of the device will be shown on the MAC Address Filter table.
Cancel	Give up the access control set up.
Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

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

II-3-4 WPS

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



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

☑ Enable WPS ⟳

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek-3F4764
WPS Auth Mode	WPA2/PSK
WPS Encrypt Type	AES

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	______ Start PIN

Status: Idle

Note: WPS can help your wireless client automatically connect to the Access point.
⟳: WPS is Disabled.
⟳: WPS is Enabled.
⟳: Waiting for WPS requests from wireless clients.

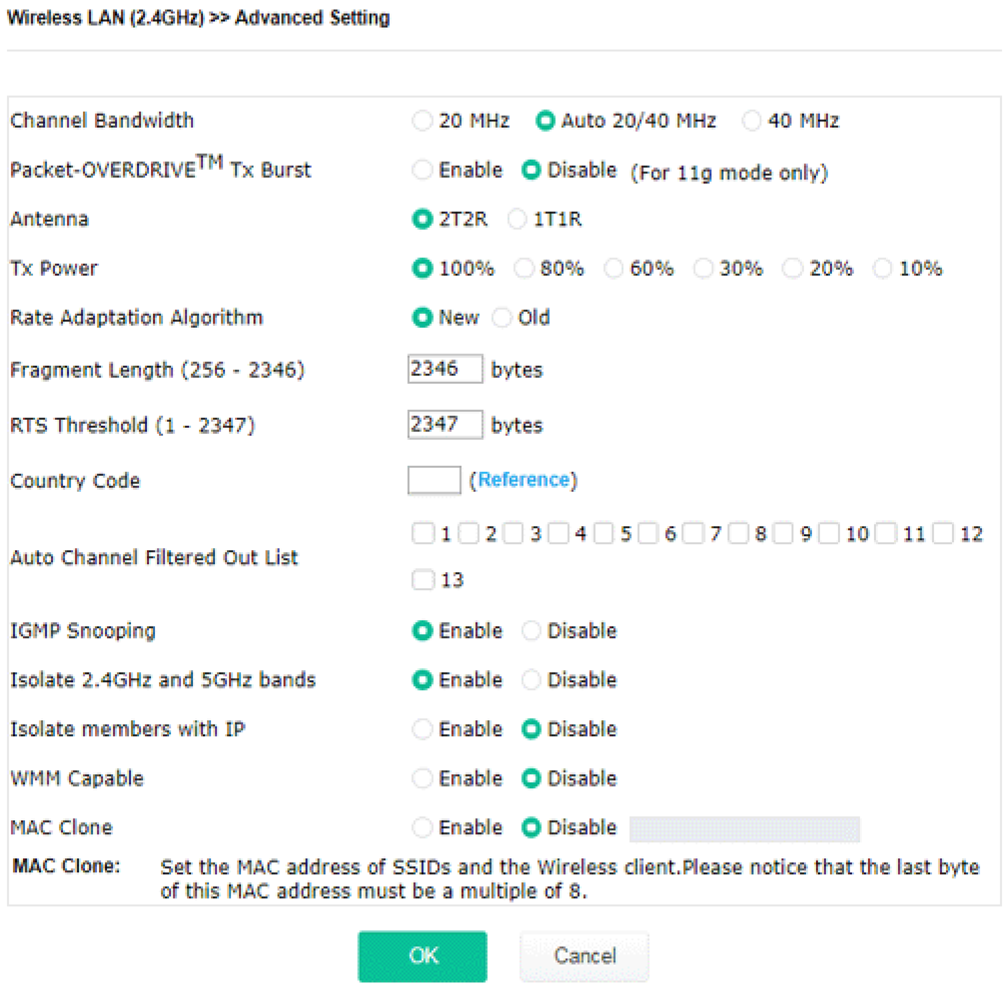
Available settings are explained as follows:

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

	(encryption) function of VigorAP 802 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 802. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 802.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 802 will wait for WPS requests from wireless clients about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 802 will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. Both ACT and 2.4G WLAN LEDs on VigorAP 802 will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

II-3-5 Advanced Setting

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

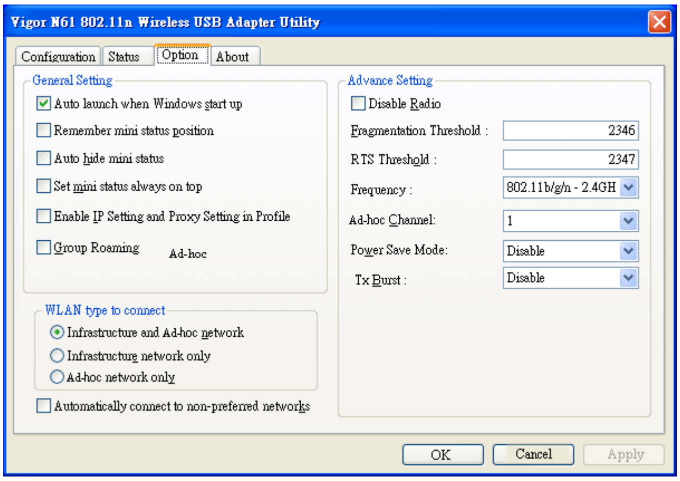


Wireless LAN (2.4GHz) >> Advanced Setting

Channel Bandwidth	○ 20 MHz ● Auto 20/40 MHz ○ 40 MHz
Packet-OVERDRIVE^{TM} Tx Burst	○ Enable ● Disable (For 11g mode only)
Antenna	● 2T2R ○ 1T1R
Tx Power	● 100% ○ 80% ○ 60% ○ 30% ○ 20% ○ 10%
Rate Adaptation Algorithm	● New ○ Old
Fragment Length (256 - 2346)	2346 bytes
RTS Threshold (1 - 2347)	2347 bytes
Country Code	(Reference)
Auto Channel Filtered Out List	□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13
IGMP Snooping	● Enable ○ Disable
Isolate 2.4GHz and 5GHz bands	● Enable ○ Disable
Isolate members with IP	○ Enable ● Disable
WMM Capable	○ Enable ● Disable
MAC Clone	○ Enable ● Disable

MAC Clone: Set the MAC address of SSIDs and the Wireless client.Please notice that the last byte of this MAC address must be a multiple of 8.

Available settings are explained as follows:

Item	Description
Channel Width	**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.
Packet-OVERDRIVE **(for 2.4GHz only)**	This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too. Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).  Vigor N61 802.11n Wireless USB Adapter Utility Configuration | Status | Option | About General Setting ☑ Auto launch when Windows start up □ Remember mini status position □ Auto hide mini status □ Set mini status always on top □ Enable IP Setting and Proxy Setting in Profile □ Group Roaming Ad-hoc WLAN type to connect ● Infrastructure and Ad-hoc network ○ Infrastructure network only ○ Ad-hoc network only □ Automatically connect to non-preferred networks Advance Setting □ Disable Radio Fragmentation Threshold : 2346 RTS Threshold : 2347 Frequency : 802.11b/g/n - 2.4GH Ad-hoc Channel: 1 Power Save Mode: Disable Tx Burst : Disable
Antenna **(for 2.4GHz only)**	VigorAP can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.
Tx Power	The default setting is the maximum (100%). Lowering down the value may degrade range and throughput of wireless.
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2346.
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold of wireless radio. Do not modify default value if you don’t know what it is, default value is 2347.
Country Code	VigorAP broadcasts country codes by following the 802.11d standard.

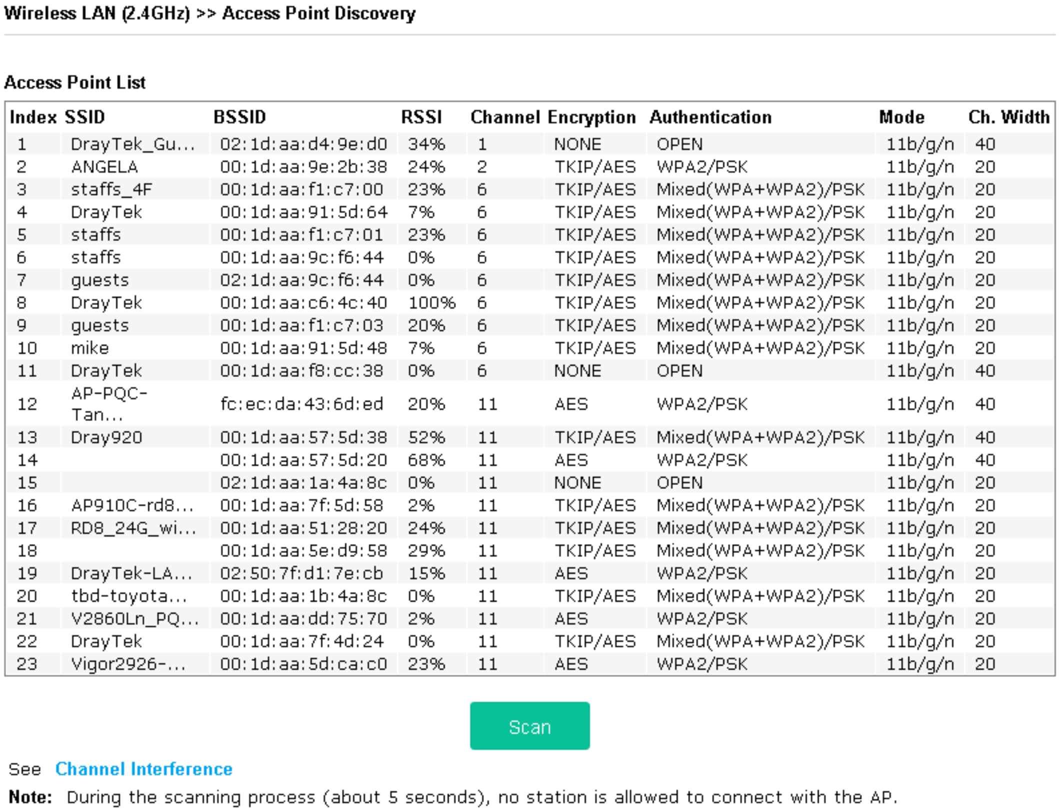
	However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
Auto Channel Filtered Out List	The selected wireless channels will be discarded if **AutoSelect** is selected as **Channel** selection mode in **Wireless LAN>>General Setup**.
IGMP Snooping	Click **Enable** to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Isolate 2.4GHz and 5GHz bands	The default setting is “Enable”. It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa. For WLAN 2.4GHz and 5GHz set with the same SSID name: ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if **Isolate Member** (in **Wireless LAN>>General Setup**) is NOT enabled for such SSID. ● Yet, if the function of **Isolate Member** (in **Wireless LAN>>General Setup**) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
Isolate members with IP	The default setting is “Disable”. If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
APSD Capable **(for 5GHz only)**	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 802 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to VigorAP.

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



Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Mode	Ch. Width
1	DrayTek_Gu...	02:1d:aa:d4:9e:d0	34%	1	NONE	OPEN	11b/g/n	40
2	ANGELA	00:1d:aa:9e:2b:38	24%	2	TKIP/AES	WPA2/PSK	11b/g/n	20
3	staffs_4F	00:1d:aa:f1:c7:00	23%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
4	DrayTek	00:1d:aa:91:5d:64	7%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
5	staffs	00:1d:aa:f1:c7:01	23%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
6	staffs	00:1d:aa:9c:f6:44	0%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
7	guests	02:1d:aa:9c:f6:44	0%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
8	DrayTek	00:1d:aa:c6:4c:40	100%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
9	guests	00:1d:aa:f1:c7:03	20%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
10	mike	00:1d:aa:91:5d:48	7%	6	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
11	DrayTek	00:1d:aa:f8:cc:38	0%	6	NONE	OPEN	11b/g/n	40
12	AP-PQC-Tan...	fc:ec:da:43:6d:ed	20%	11	AES	WPA2/PSK	11b/g/n	40
13	Dray920	00:1d:aa:57:5d:38	52%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	40
14		00:1d:aa:57:5d:20	68%	11	AES	WPA2/PSK	11b/g/n	40
15		02:1d:aa:1a:4a:8c	0%	11	NONE	OPEN	11b/g/n	20
16	AP910C-rd8...	00:1d:aa:7f:5d:58	2%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
17	RD8_24G_wi...	00:1d:aa:51:28:20	24%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
18		00:1d:aa:5e:d9:58	29%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
19	DrayTek-LA...	02:50:7f:d1:7e:cb	15%	11	AES	WPA2/PSK	11b/g/n	20
20	tbd-toyota...	00:1d:aa:1b:4a:8c	0%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
21	V2860Ln_PQ...	00:1d:aa:dd:75:70	2%	11	AES	WPA2/PSK	11b/g/n	20
22	DrayTek	00:1d:aa:7f:4d:24	0%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK	11b/g/n	20
23	Vigor2926-...	00:1d:aa:5d:ca:c0	23%	11	AES	WPA2/PSK	11b/g/n	20

See **Channel Interference**

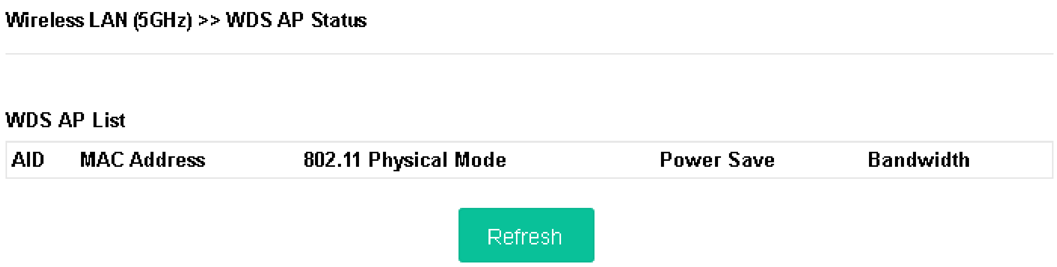
Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 802.
BSSID	Display the MAC address of the AP scanned by VigorAP 802.
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 802.
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

II-3-7 WDS AP Status

VigorAP 802 can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.



Wireless LAN (5GHz) >> WDS AP Status

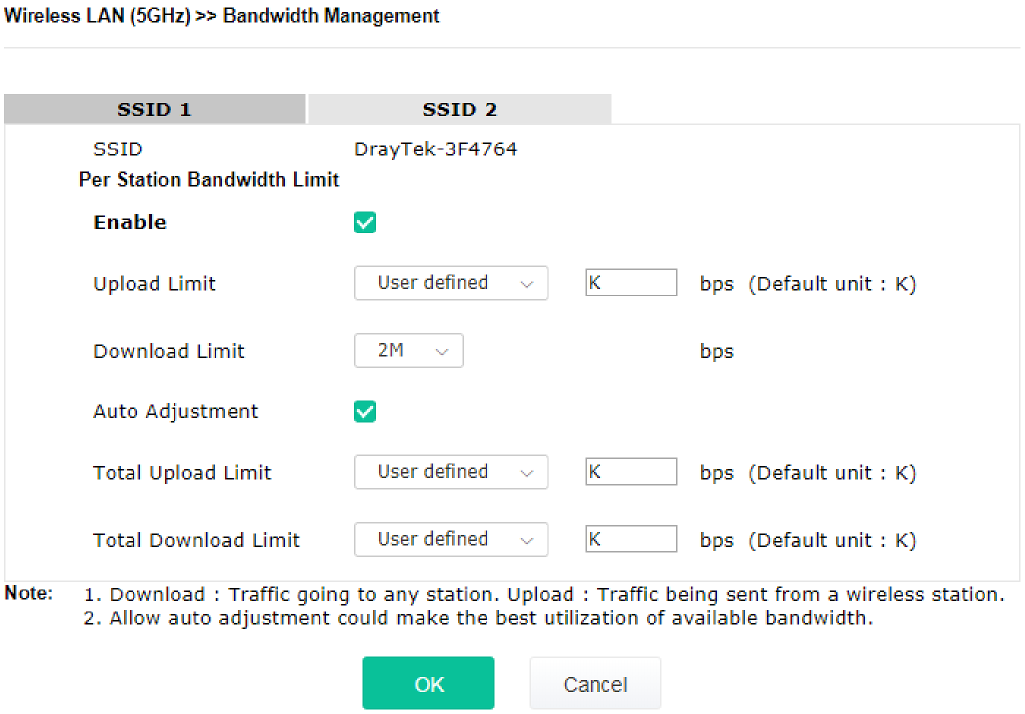
WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth

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

II-3-8 Bandwidth Management

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



Wireless LAN (5GHz) >> Bandwidth Management

SSID DrayTek-3F4764

Per Station Bandwidth Limit

Enable ☑

Upload Limit: User defined, K bps (Default unit : K)

Download Limit: 2M bps

Auto Adjustment ☑

Total Upload Limit: User defined, K bps (Default unit : K)

Total Download Limit: User defined, K bps (Default unit : K)

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

Available settings are explained as follows:

Item	Description
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor device with the same SSID.

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

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

II-3-9 Airtime Fairness

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

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

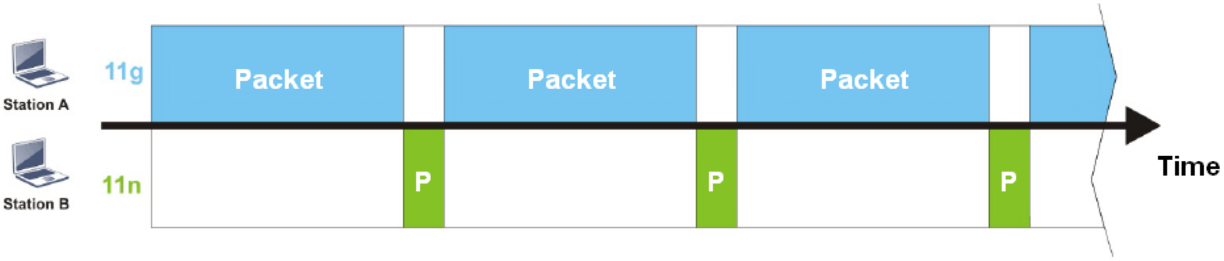
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

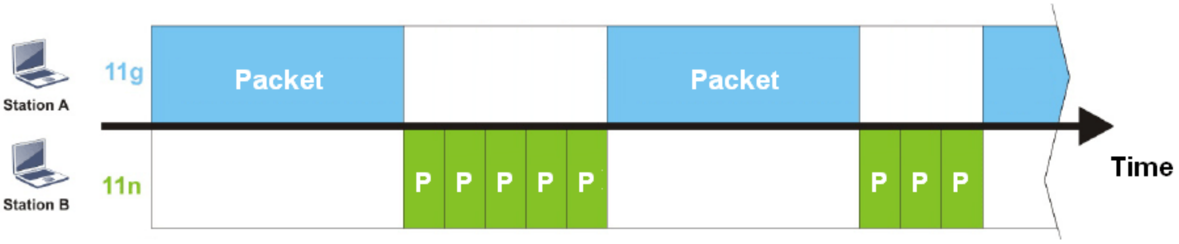
The principle behind the IEEE802.11 channel access mechanisms is that each station has ***equal probability*** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

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

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 802. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 802. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



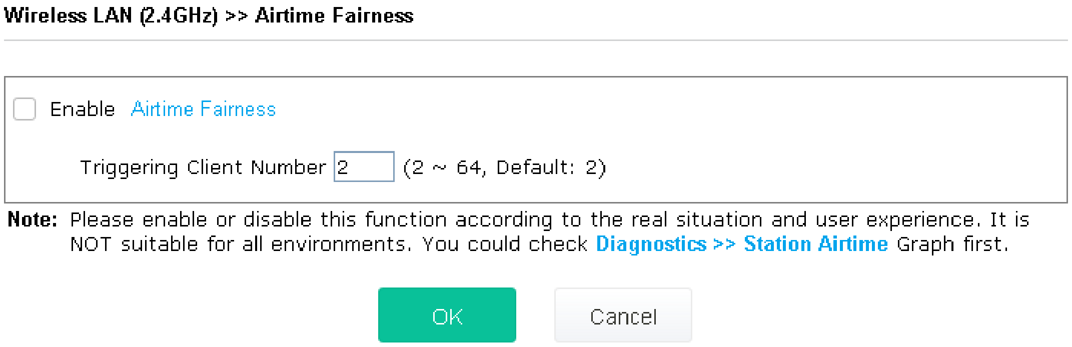
It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same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

Suitable environment:

(1) Many wireless stations.

(2) All stations mainly use download traffic.

(3) The performance bottleneck is wireless connection.



Wireless LAN (2.4GHz) >> Airtime Fairness

☐ Enable Airtime Fairness

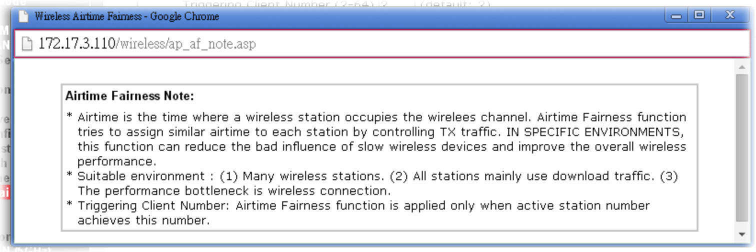
Triggering Client Number 2 (2 ~ 64, Default: 2)

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

OK Cancel

Available settings are explained as follows:

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

	 Wireless Airtime Fairness - Google Chrome 172.17.3.110/wireless/ap_af_note.asp **Airtime Fairness Note:** * Airtime is the time where a wireless station occupies the wirelees channel. Airtime Fairness function tries to assign similar airtime to each station by controlling TX traffic. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance. * Suitable environment : (1) Many wireless stations. (2) All stations mainly use download traffic. (3) The performance bottleneck is wireless connection. * Triggering Client Number: Airtime Fairness function is applied only when active station number achieves this number. **Triggering Client Number –**Airtime Fairness function is applied only when active station number achieves this number.

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

Note:

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

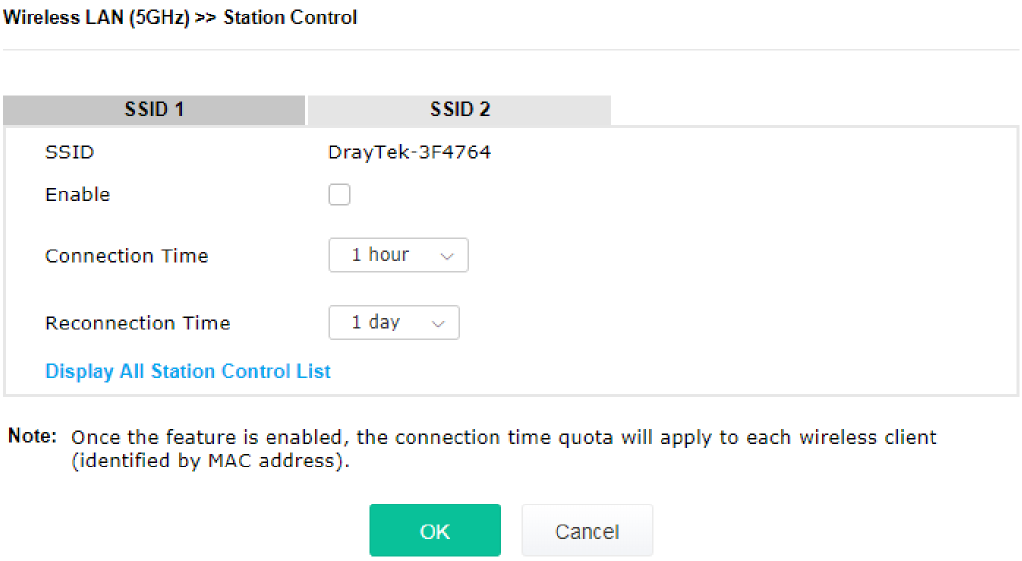
II-3-10 Station Control

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

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

Note:

Up to 300 Wireless Station records are supported by VigorAP.


Wireless LAN (5GHz) >> Station Control

SSID	DrayTek-3F4764
Enable	□
Connection Time	1 hour
Reconnection Time	1 day

Display All Station Control List

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

Available settings are explained as follows:

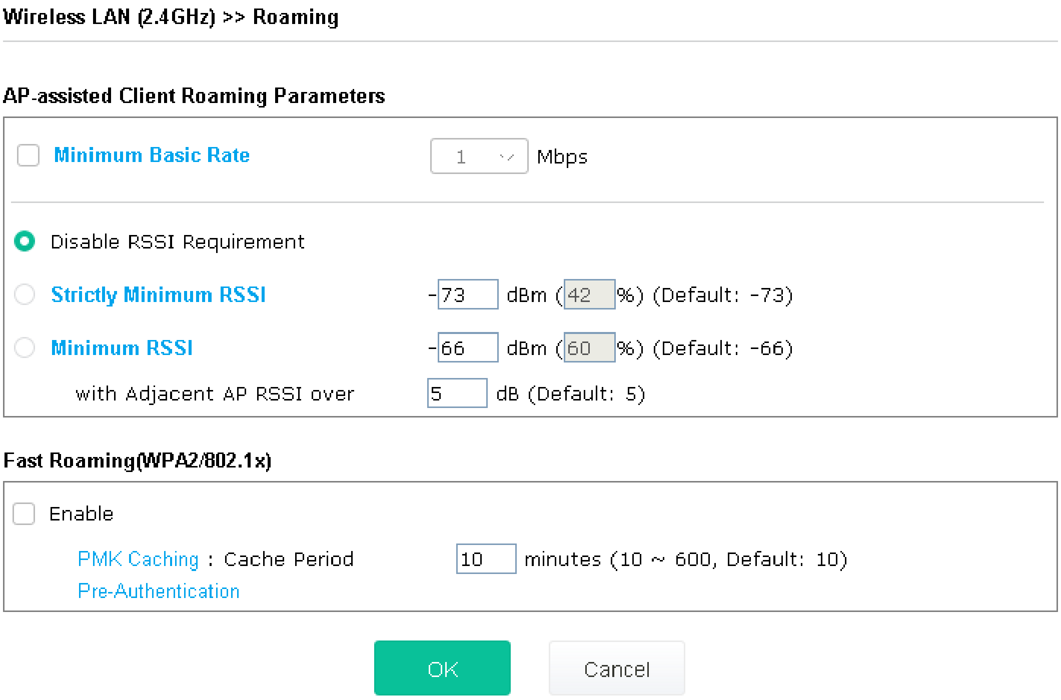
Item	Description
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to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

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

II-3-11 Roaming

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

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



Wireless LAN (2.4GHz) >> Roaming

AP-assisted Client Roaming Parameters

□ Minimum Basic Rate 1 Mbps

● Disable RSSI Requirement

○ Strictly Minimum RSSI -73 dBm (42 %) (Default: -73)

○ Minimum RSSI -66 dBm (60 %) (Default: -66)

with Adjacent AP RSSI over 5 dB (Default: 5)

Fast Roaming(WPA2/802.1x)

□ Enable

PMK Caching : Cache Period 10 minutes (10 ~ 600, Default: 10)

Pre-Authentication

Available settings are explained as follows:

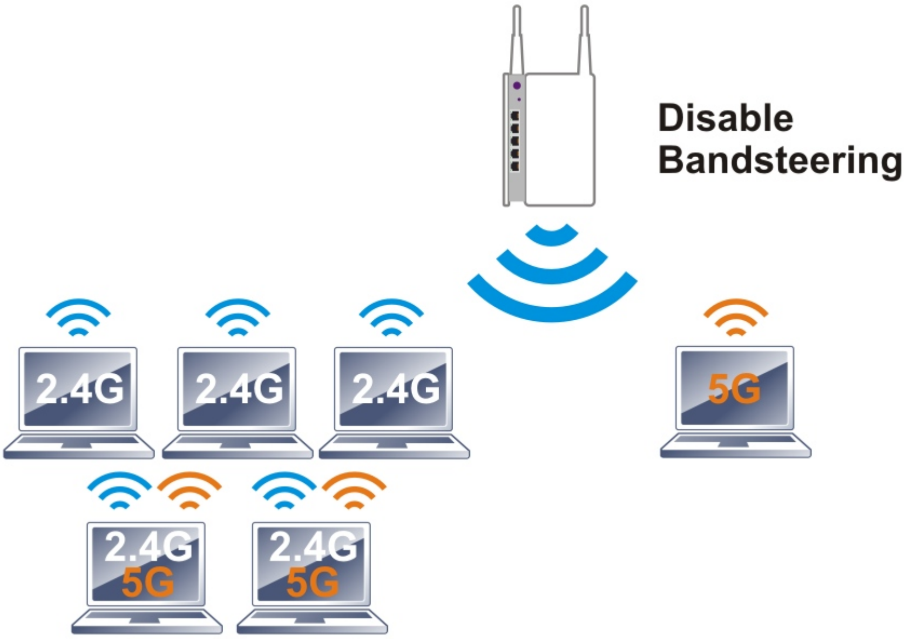
Item	Description
AP-assisted Client Roaming Parameters	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 802 will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal. **Minimum Basic Rate –** Check the box to use the drop down list to specify a basic rate (**Mbps**). When the link rate of the wireless station is below such value, VigorAP 802 will terminate the network connection for that wireless station. **Disable RSSI Requirement -** If it is selected, VigorAP will not terminate the network connection based on RSSI. **Strictly Minimum RSSI -** VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (**dBm**) set here, VigorAP 802 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 802, VigorAP 802 will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI). ● **With Adjacent AP RSSI over –** Specify a value as a threshold.
Fast Roaming (WPA2/802.1x)	**Enable –** Check the box to enable fast roaming configuration. **PMK Caching -** Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for **WPA2/802.1** mode. **Pre-Authentication -** Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.

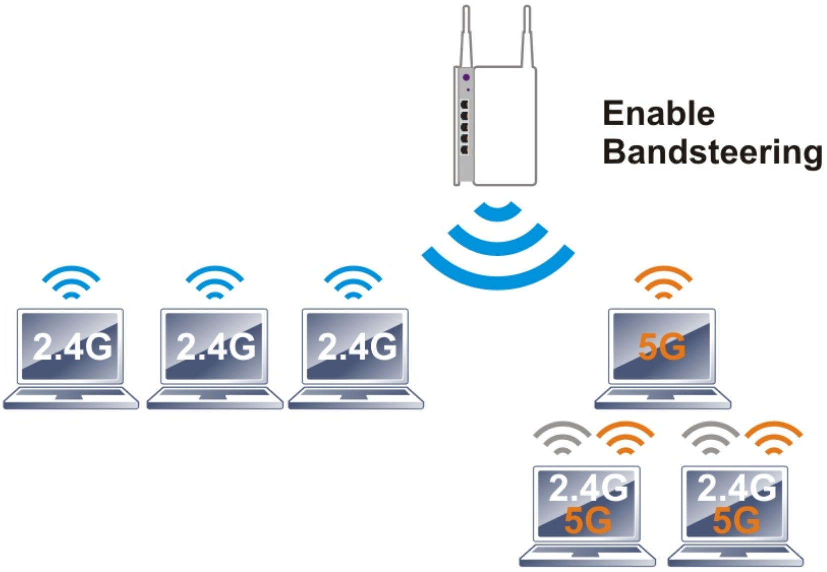
After finishing this web page configuration, please click **OK** to save the settings.

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

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



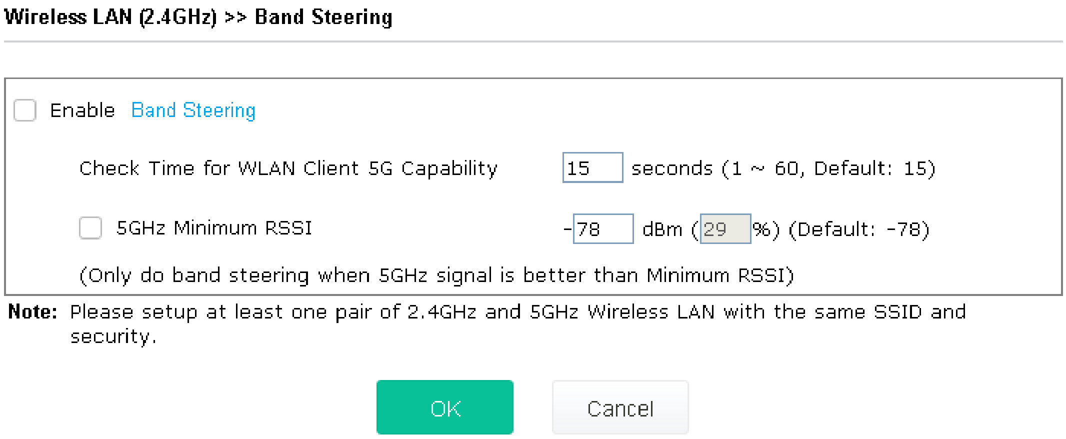
If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



Note:

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

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



Wireless LAN (2.4GHz) >> Band Steering

□ Enable Band Steering

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

□ 5GHz Minimum RSSI -78 dBm (29 %) (Default: -78)

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

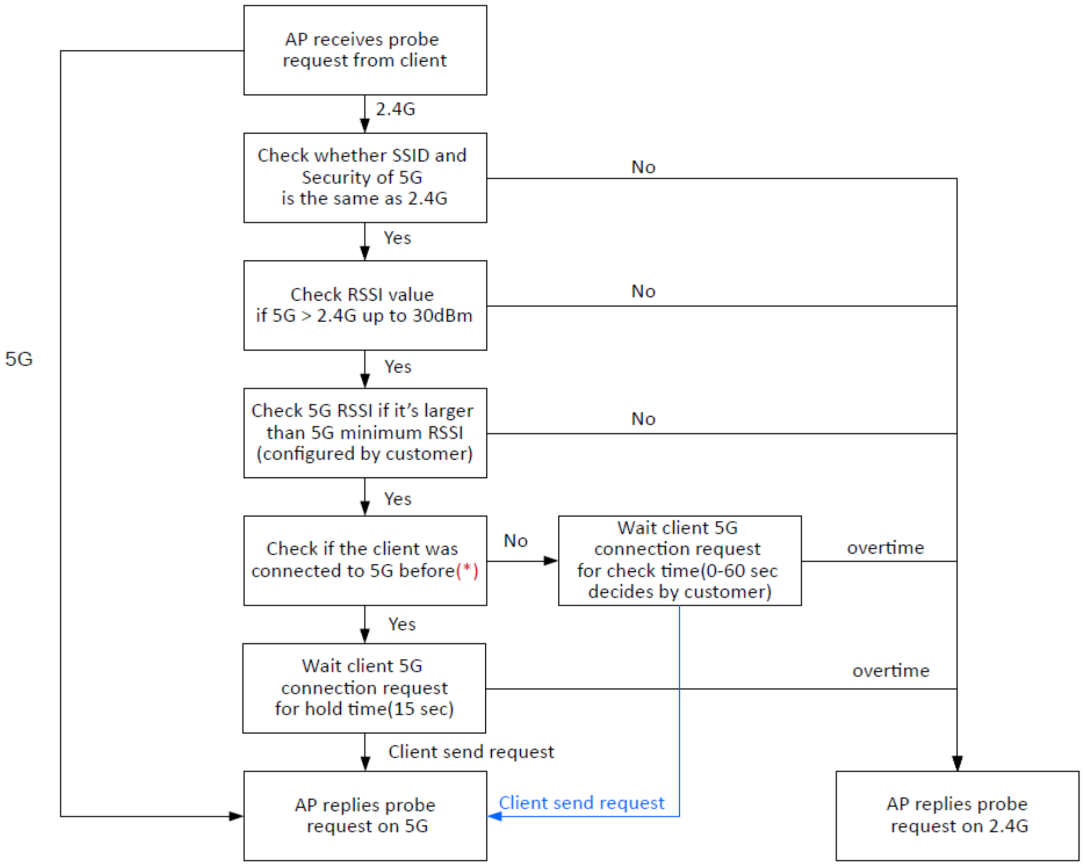
Note: Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

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 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 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 802, VigorAP will allow the client to connect to 2.4GHz network.

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

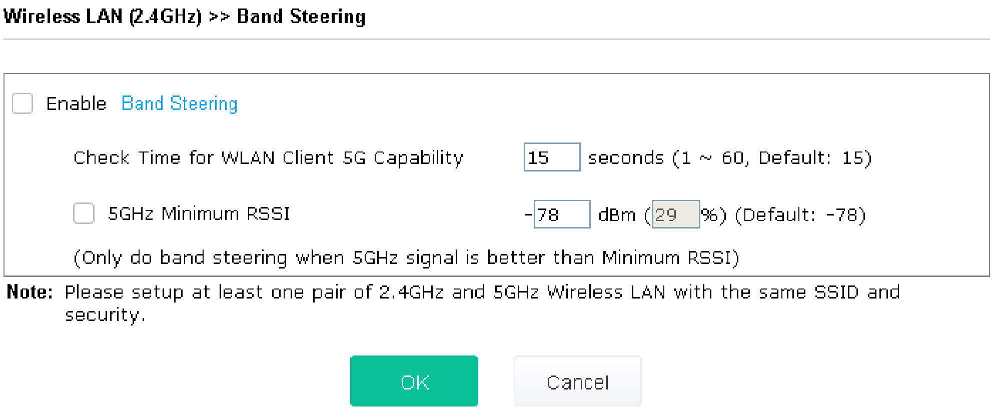
Below shows how Band Steering works.


AP receives probe request from client
2.4G
5G
Check whether SSID and Security of 5G is the same as 2.4G
No
Yes
Check RSSI value if 5G > 2.4G up to 30dBm
No
Yes
Check 5G RSSI if it's larger than 5G minimum RSSI (configured by customer)
No
Yes
Check if the client was connected to 5G before(*)
No
Wait client 5G connection request for check time(0-60 sec decides by customer)
overtime
Yes
Wait client 5G connection request for hold time(15 sec)
overtime
Client send request
AP replies probe request on 5G
Client send request
AP replies probe request on 2.4G

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

How to Use Band Steering?

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



Wireless LAN (2.4GHz) >> Band Steering

□ Enable Band Steering

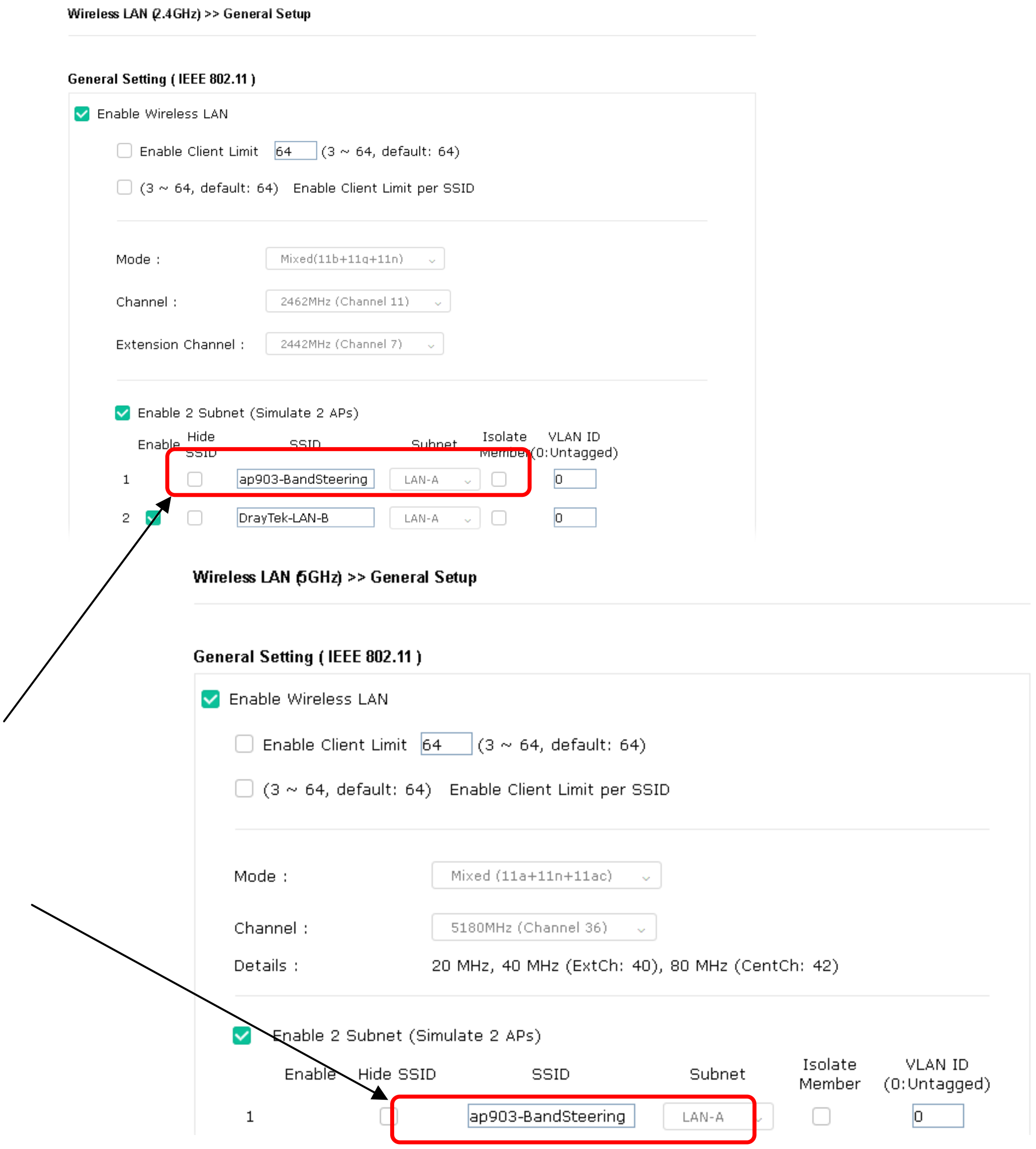
Check Time for WLAN Client 5G Capability 15 seconds (1 ~ 60, Default: 15)

□ 5GHz Minimum RSSI -78 dBm (29 %) (Default: -78)

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

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

3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *ap802-BandSteering* for both pages. Click **OK** to save the settings.



Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

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

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

Mode : Mixed(11b+11g+11n)

Channel : 2462MHz (Channel 11)

Extension Channel : 2442MHz (Channel 7)

☑ Enable 2 Subnet (Simulate 2 APs)

	Enable	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0:Untagged)
1		□	ap903-BandSteering	LAN-A	□	0
2	☑	□	DrayTek-LAN-B	LAN-A	□	0

Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

☑ Enable Wireless LAN

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

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

Mode : Mixed (11a+11n+11ac)

Channel : 5180MHz (Channel 36)

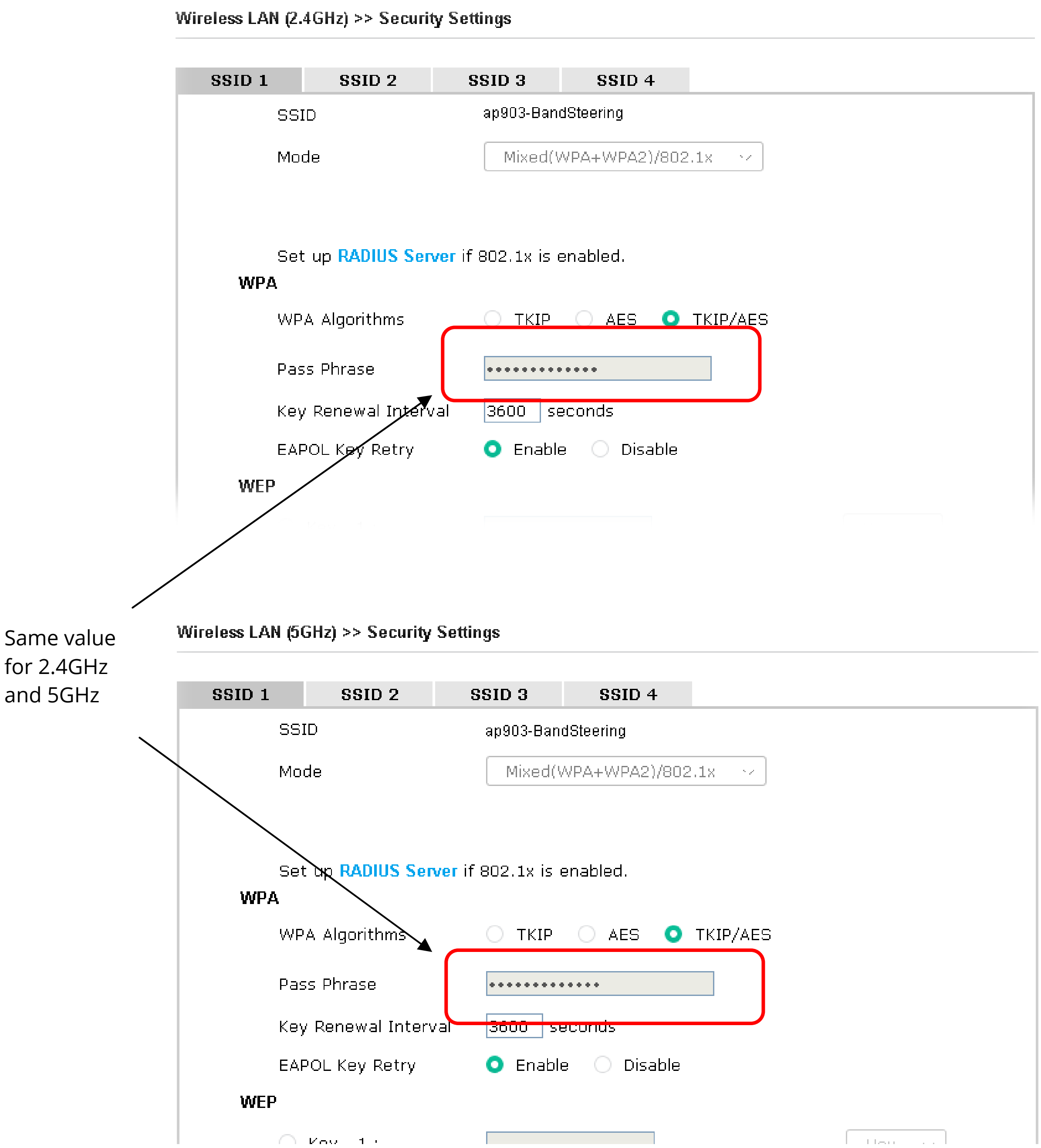
Details : 20 MHz, 40 MHz (ExtCh: 40), 80 MHz (CentCh: 42)

☑ Enable 2 Subnet (Simulate 2 APs)

	Enable	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0:Untagged)
1		□	ap903-BandSteering	LAN-A	□	0

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.



Wireless LAN (2.4GHz) >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

SSID	ap903-BandSteering
Mode	Mixed(WPA+WPA2)/802.1x

Set up RADIUS Server if 802.1x is enabled.

WPA

WPA Algorithms	○ TKIP ○ AES ● TKIP/AES
Pass Phrase	•••••••••••••
Key Renewal Interval	3600 seconds
EAPOL Key Retry	● Enable ○ Disable

WEP

Same value for 2.4GHz and 5GHz

Wireless LAN (5GHz) >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

SSID	ap903-BandSteering
Mode	Mixed(WPA+WPA2)/802.1x

Set up RADIUS Server if 802.1x is enabled.

WPA

WPA Algorithms	○ TKIP ○ AES ● TKIP/AES
Pass Phrase	•••••••••••••
Key Renewal Interval	3600 seconds
EAPOL Key Retry	● Enable ○ Disable

WEP

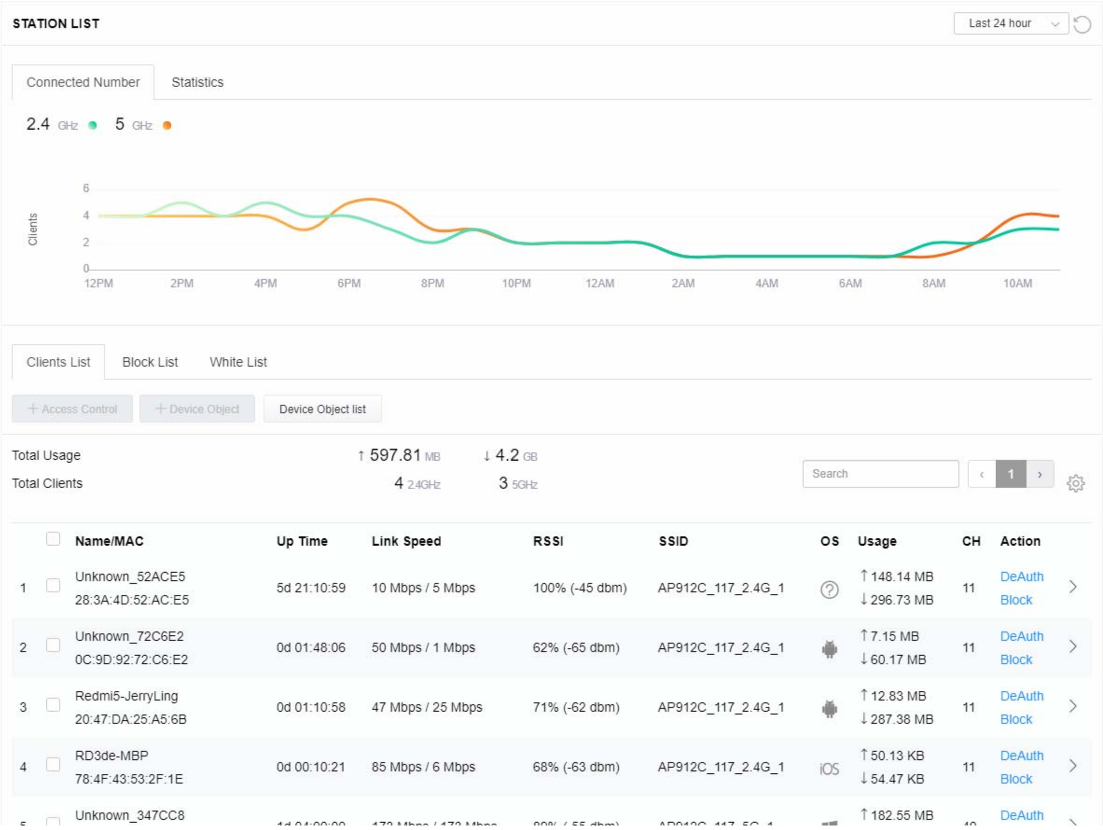
6. Now, VigorAP 802 will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

II-3-13 Station List

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

II-3-13-1 Connected Number

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



STATION LIST

Last 24 hour

Connected Number | Statistics

2.4 GHz ● 5 GHz ●

Clients List | Block List | White List

+ Access Control | + Device Object | Device Object list

Total Usage ↑ 597.81 MB ↓ 4.2 GB

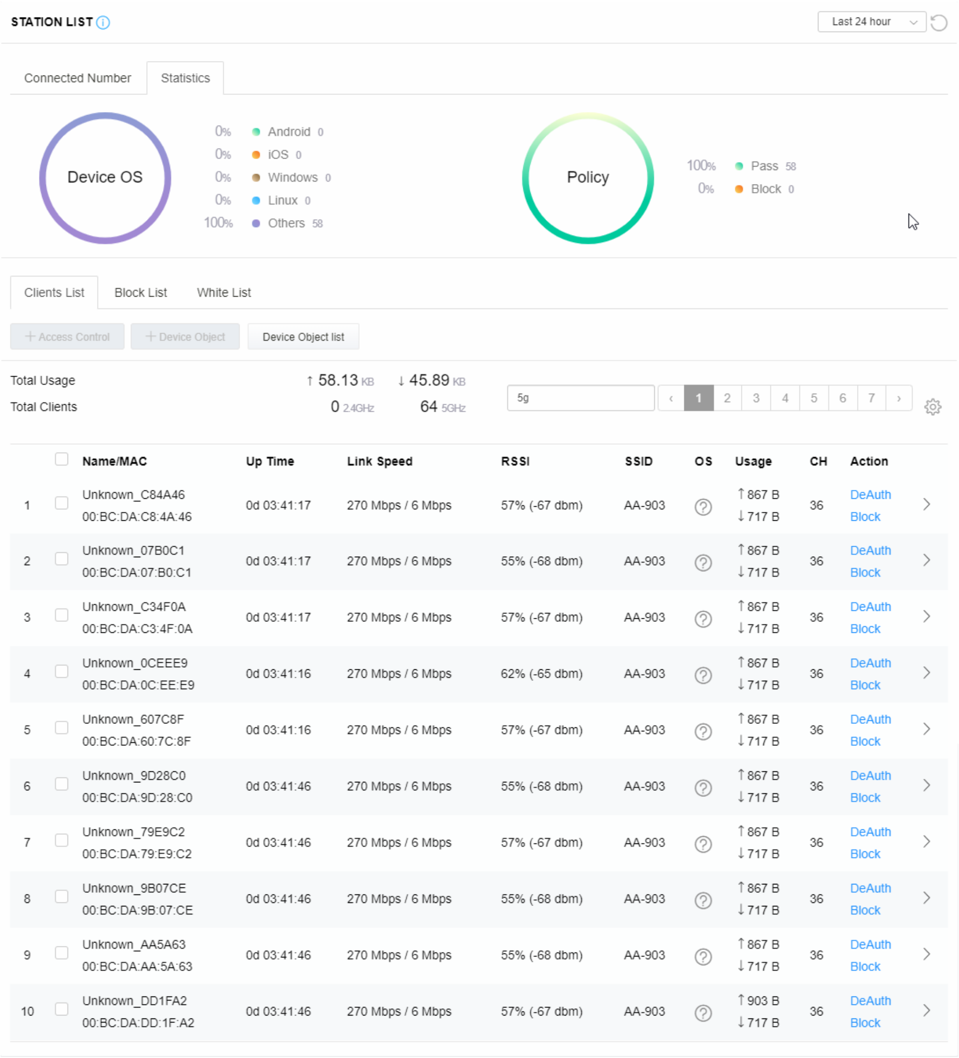
Total Clients 4 2.4GHz 3 5GHz

Search

	□	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	□	Unknown_52ACE5 28:3A:4D:52:AC:E5	5d 21:10:59	10 Mbps / 5 Mbps	100% (-45 dbm)	AP912C_117_2.4G_1	?	↑148.14 MB ↓296.73 MB	11	DeAuth Block
2	□	Unknown_72C6E2 0C:9D:92:72:C6:E2	0d 01:48:06	50 Mbps / 1 Mbps	62% (-65 dbm)	AP912C_117_2.4G_1		↑7.15 MB ↓60.17 MB	11	DeAuth Block
3	□	Redmi5-JerryLing 20:47:DA:25:A5:6B	0d 01:10:58	47 Mbps / 25 Mbps	71% (-62 dbm)	AP912C_117_2.4G_1		↑12.83 MB ↓287.38 MB	11	DeAuth Block
4	□	RD3de-MBP 78:4F:43:53:2F:1E	0d 00:10:21	85 Mbps / 6 Mbps	68% (-63 dbm)	AP912C_117_2.4G_1	iOS	↑50.13 KB ↓54.47 KB	11	DeAuth Block
	□	Unknown_347CC8						↑182.55 MB		DeAuth

II-3-13-2 Statistics

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



0% ● Android 0
0% ● iOS 0
0% ● Windows 0
0% ● Linux 0
100% ● Others 58

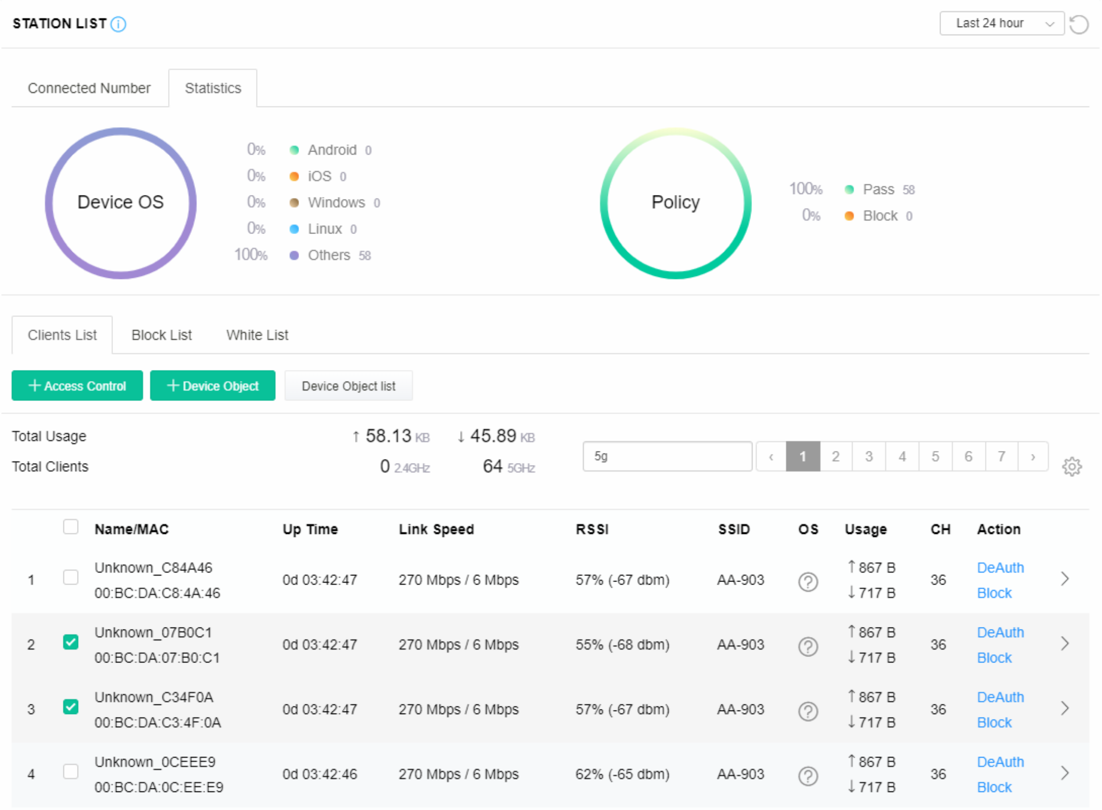
100% ● Pass 58
0% ● Block 0

Total Usage ↑ 58.13 KB ↓ 45.89 KB
Total Clients 0 2.4GHz 64 5GHz

	□	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.



Device OS		
0%	Android	0
0%	iOS	0
0%	Windows	0
0%	Linux	0
100%	Others	58

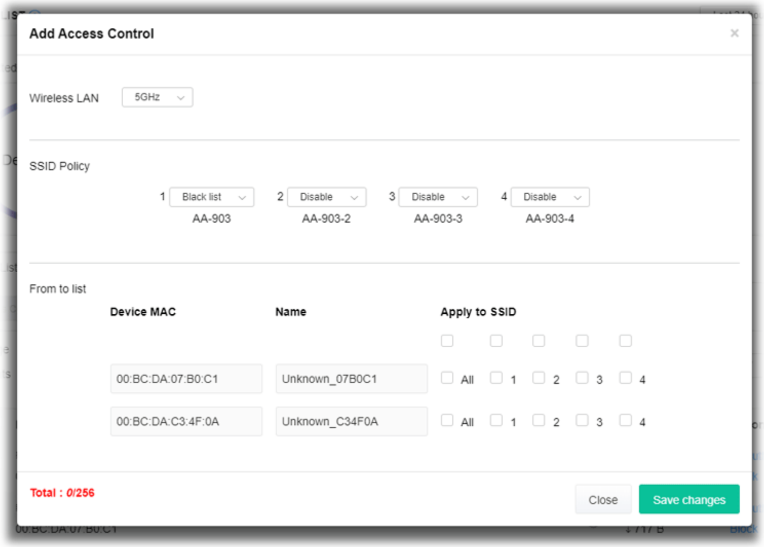
Policy		
100%	Pass	58
0%	Block	0

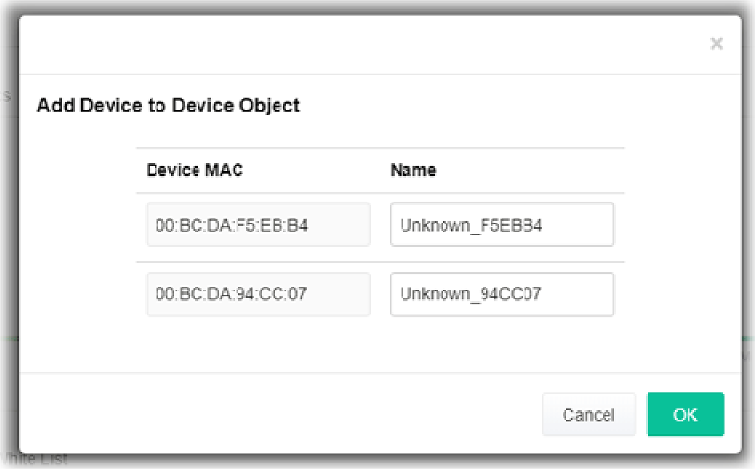
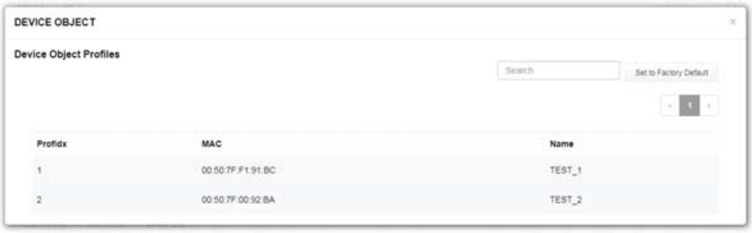
Total Usage ↑ 58.13 KB ↓ 45.89 KB

Total Clients 0 2.4GHz 64 5GHz

		Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	□	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:42:47	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 03:42:47	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 03:42:47	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 03:42:46	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	↑867 B ↓717 B	36	DeAuth Block

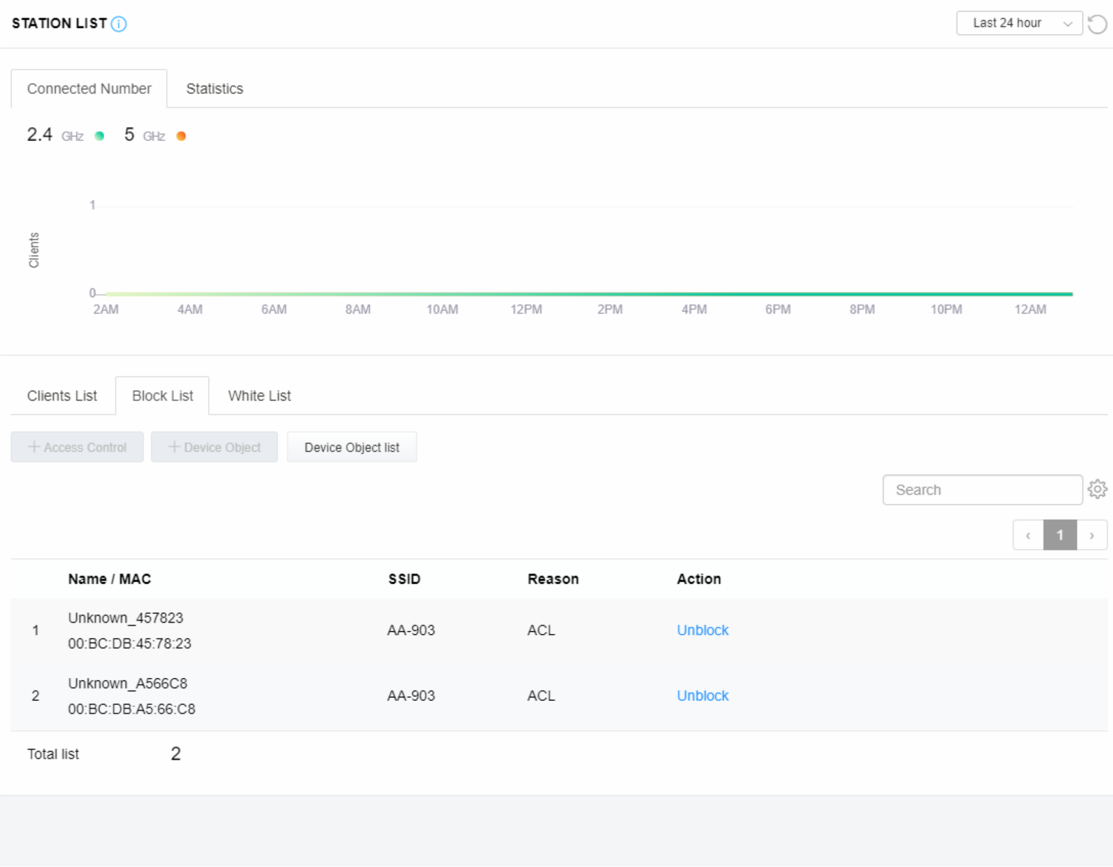
Available settings are explained as follows:

Item	Description
+Access Control	It is available after choosing one of the entries (clients) on Clients List.  Add Access Control Wireless LAN: 5GHz SSID Policy: 1 Black list AA-903; 2 Disable AA-903-2; 3 Disable AA-903-3; 4 Disable AA-903-4 From to list Device MAC / Name / Apply to SSID 00:BC:DA:07:B0:C1 / Unknown_07B0C1 / □ All □ 1 □ 2 □ 3 □ 4 00:BC:DA:C3:4F:0A / Unknown_C34F0A / □ All □ 1 □ 2 □ 3 □ 4 Total : 0/256 Close Save changes **Wireless LAN** - Specify the bandwidth for the access control list. **SSID Policy** - Set the policy for each SSID as black list or white list 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 device object list, choose one of the entries (clients) on Clients List to enable the Device Object button. Click the button to open the following page.  Add Device to Device Object Device MAC: 00:BC:DA:F5:EB:B4 — Name: Unknown_F5EBB4 Device MAC: 00:BC:DA:94:CC:07 — Name: Unknown_94CC07 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.  DEVICE OBJECT Device Object Profiles Profidx — MAC — Name 1 — 00:50:7F:F1:91:BC — TEST_1 2 — 00:50:7F:00:92:BA — TEST_2
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 block list or white list.

II-3-13-4 Block List

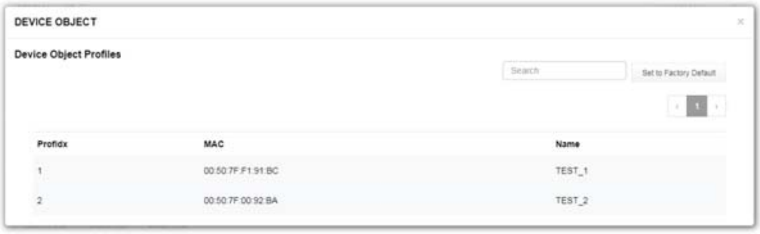
This page displays information of the stations under block list.



	Name / MAC	SSID	Reason	Action
1	Unknown_457823 00:BC:DB:45:78:23	AA-903	ACL	Unblock
2	Unknown_A566C8 00:BC:DB:A5:66:C8	AA-903	ACL	Unblock

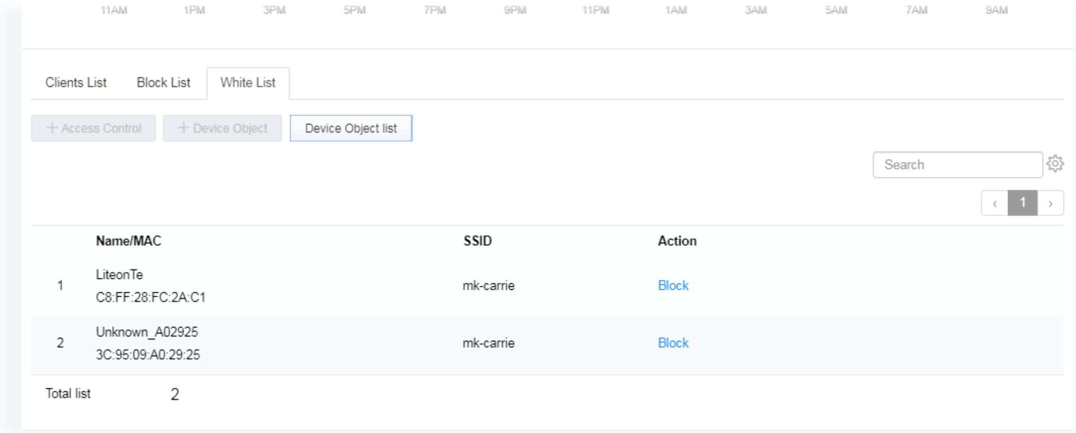
Total list 2

Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.  DEVICE OBJECT Device Object Profiles Search Set to Factory Default Profidx MAC Name 1 00:50:7F:F1:91:BC TEST_1 2 00:50:7F:00:92:BA TEST_2
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

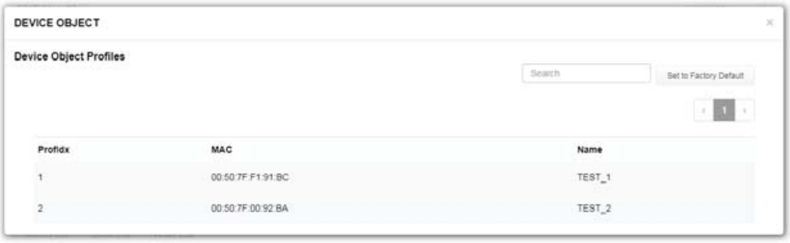
This page displays general information of the stations under white list.



	Name/MAC	SSID	Action
1	LiteonTe C8:FF:28:FC:2A:C1	mk-carrie	Block
2	Unknown_A02925 3C:95:09:A0:29:25	mk-carrie	Block

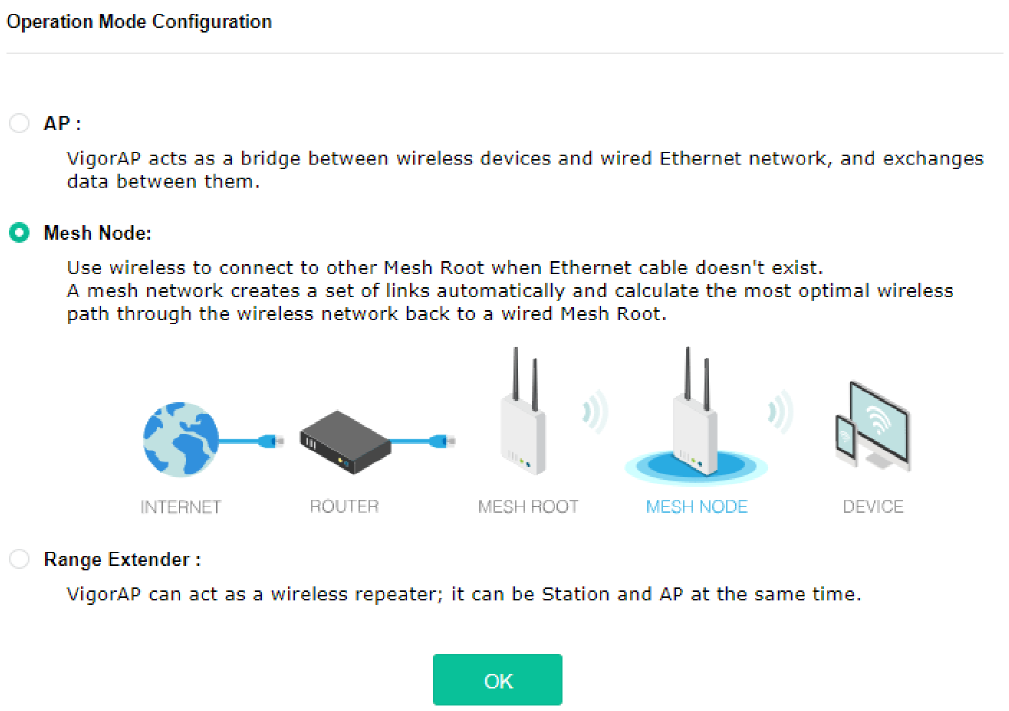
Total list 2

Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.  DEVICE OBJECT Device Object Profiles Search Set to Factory Default Profidx / MAC / Name 1 / 00:50:7F:F1:91:BC / TEST_1 2 / 00:50:7F:00:92:BA / TEST_2
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 Node Mode

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



Operation Mode Configuration

○ **AP :**

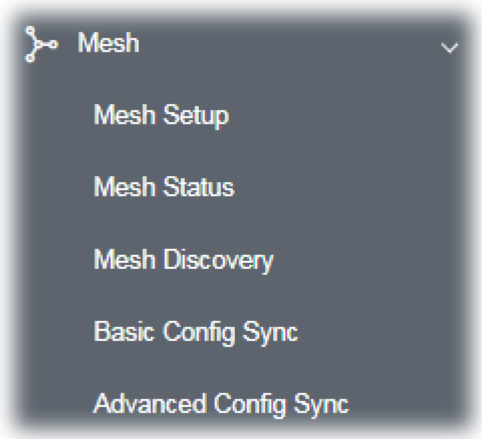
VigorAP acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

● **Mesh Node:**

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

○ **Range Extender :**

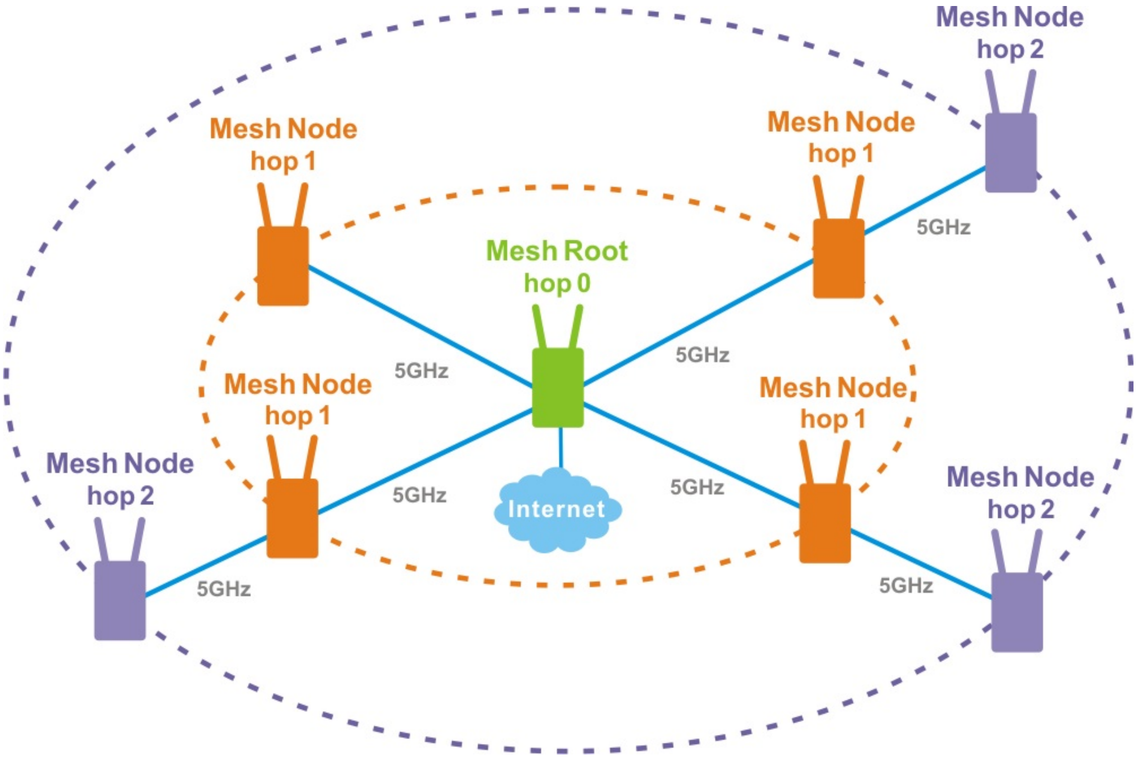
VigorAP can act as a wireless repeater; it can be Station and AP at the same time.



Please note that, within VigorMesh network,

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

Refer to the following figure:



For the mesh group set within VigorMesh network,

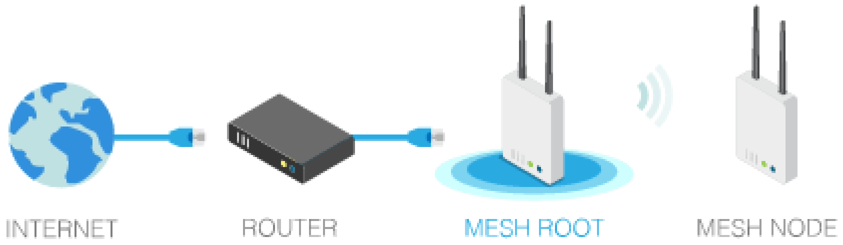
- It must be composed by “1” Mesh Root and “0~7” mesh nodes
- (Roaming) Normally members in a mesh group use the same Wireless SSID/security
- (Add) Only the mesh root can add a new mesh node into the mesh group
- (Recover) A disconnected mesh node will automatically try to connect to another connected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

Mesh Root and Mesh Node

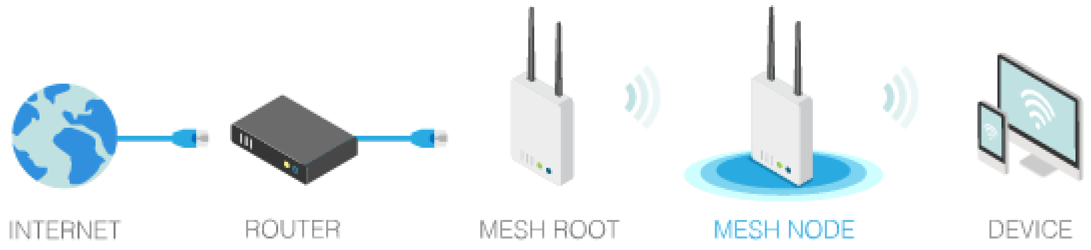
Mesh Root indicates that VigorAP would be other AP's uplink connection. As a Mesh Root, VigorAP must connect to a gateway with Ethernet cable first to have an internet connection.

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

The following figure shows how VigorAP runs as MESH ROOT:



The following figure shows how VigorAP runs as MESH NODE:

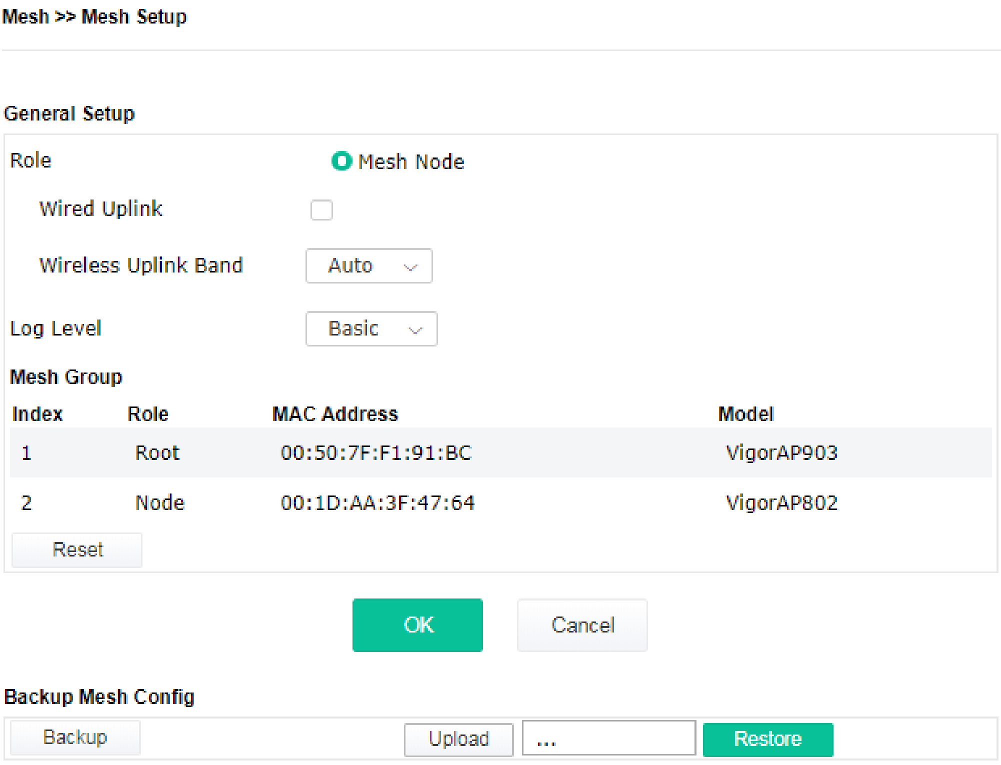


Important:

The VigorAP 802 can be ONLY set as a "mesh node" to be used with a Mesh Root (e.g., VigorAP 903).

II-4-1 Mesh Setup

Such page can determine the role of the VigorAP. Basically, VigorAP can be used as a mesh node only.



Mesh >> Mesh Setup

General Setup

Role ● Mesh Node

Wired Uplink □

Wireless Uplink Band: Auto

Log Level: Basic

Mesh Group

Index	Role	MAC Address	Model
1	Root	00:50:7F:F1:91:BC	VigorAP903
2	Node	00:1D:AA:3F:47:64	VigorAP802

Backup Mesh Config

Available settings are explained as follows:

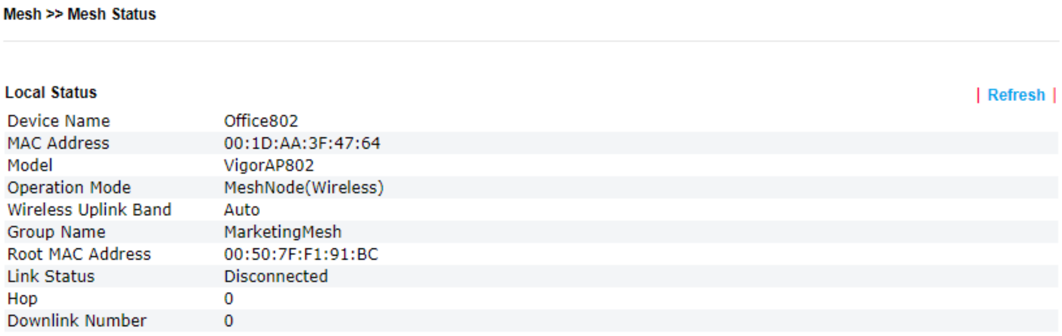
Item	Description

Role	**Mesh Node –** As a mesh node, the VigorAP can pass the wireless connection signal to other mesh node or a remote device (PC, CPE, mobile phone).
Wired Uplink	Check the box if the VigorAP connects to an uplinked mesh root or an uplinked mesh node with an Ethernet cable.
Wireless Uplink Band	Choose a wireless band for connecting with an uplinked mesh root or an uplinked mesh node.
Log Level	Choose **Basic** or **Detailed**. Related information will be shown on the **Diagnostics>>System Log.**
Mesh Group	When such VigorAP 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.
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.

II-4-2 Mesh Status

This page shows general information for the VigorAP.

In which, hop 0 means this node will use Ethernet cable to join the mesh group while others use the wireless link.



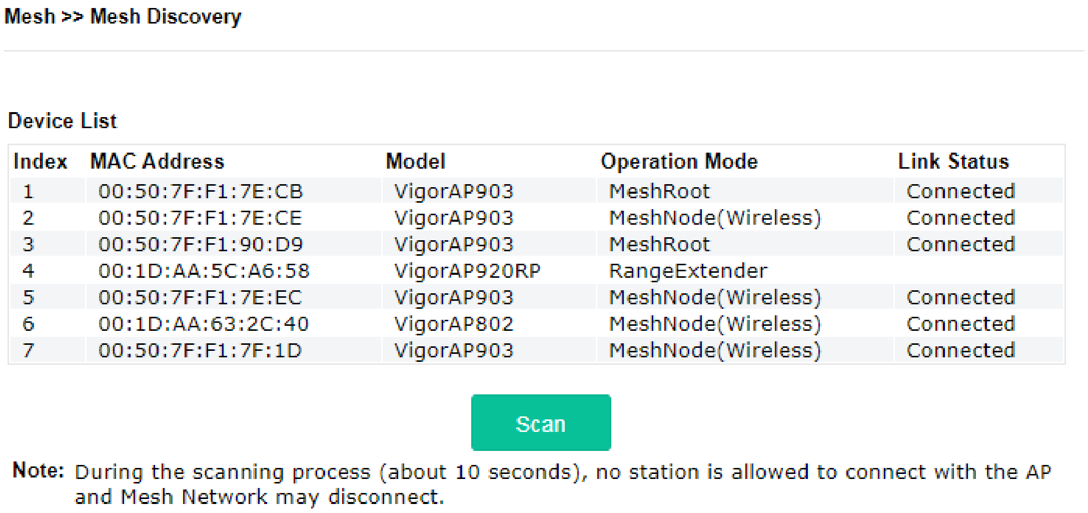
Mesh >> Mesh Status

Local Status

Device Name	Office802
MAC Address	00:1D:AA:3F:47:64
Model	VigorAP802
Operation Mode	MeshNode(Wireless)
Wireless Uplink Band	Auto
Group Name	MarketingMesh
Root MAC Address	00:50:7F:F1:91:BC
Link Status	Disconnected
Hop	0
Downlink Number	0

II-4-3 Mesh Discovery

This page helps discover all Mesh devices around and offer the Link Status and Operation Mode of each Mesh device.



Mesh >> Mesh Discovery

Device List

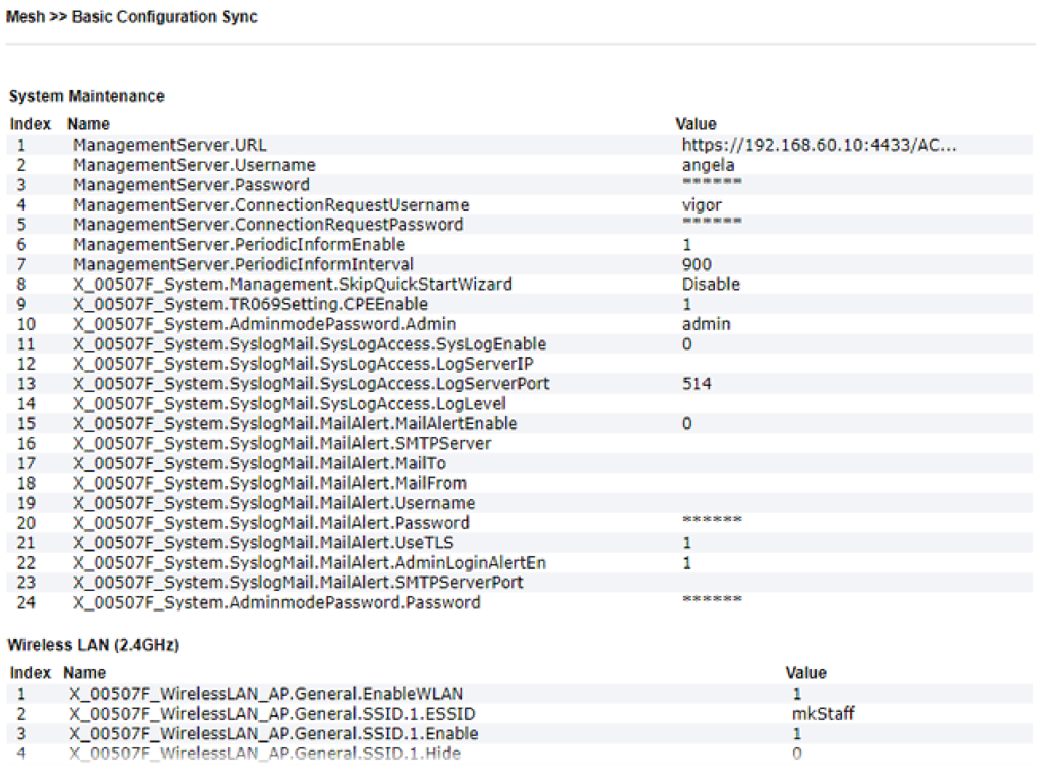
Index	MAC Address	Model	Operation Mode	Link Status
1	00:50:7F:F1:7E:CB	VigorAP903	MeshRoot	Connected
2	00:50:7F:F1:7E:CE	VigorAP903	MeshNode(Wireless)	Connected
3	00:50:7F:F1:90:D9	VigorAP903	MeshRoot	Connected
4	00:1D:AA:5C:A6:58	VigorAP920RP	RangeExtender	
5	00:50:7F:F1:7E:EC	VigorAP903	MeshNode(Wireless)	Connected
6	00:1D:AA:63:2C:40	VigorAP802	MeshNode(Wireless)	Connected
7	00:50:7F:F1:7F:1D	VigorAP903	MeshNode(Wireless)	Connected

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

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

II-4-4 Basic Configuration Sync

This page can display current configuration of VigorAP device.



Mesh >> Basic Configuration Sync

System Maintenance

Index	Name	Value
1	ManagementServer.URL	https://192.168.60.10:4433/AC...
2	ManagementServer.Username	angela
3	ManagementServer.Password	******
4	ManagementServer.ConnectionRequestUsername	vigor
5	ManagementServer.ConnectionRequestPassword	******
6	ManagementServer.PeriodicInformEnable	1
7	ManagementServer.PeriodicInformInterval	900
8	X_00507F_System.Management.SkipQuickStartWizard	Disable
9	X_00507F_System.TR069Setting.CPEEnable	1
10	X_00507F_System.AdminmodePassword.Admin	admin
11	X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable	0
12	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
13	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
14	X_00507F_System.SyslogMail.SysLogAccess.LogLevel	
15	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
16	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
17	X_00507F_System.SyslogMail.MailAlert.MailTo	
18	X_00507F_System.SyslogMail.MailAlert.MailFrom	
19	X_00507F_System.SyslogMail.MailAlert.Username	
20	X_00507F_System.SyslogMail.MailAlert.Password	******
21	X_00507F_System.SyslogMail.MailAlert.UseTLS	1
22	X_00507F_System.SyslogMail.MailAlert.AdminLoginAlertEn	1
23	X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	
24	X_00507F_System.AdminmodePassword.Password	******

Wireless LAN (2.4GHz)

Index	Name	Value
1	X_00507F_WirelessLAN_AP.General.EnableWLAN	1
2	X_00507F_WirelessLAN_AP.General.SSID.1.ESSID	mkStaff
3	X_00507F_WirelessLAN_AP.General.SSID.1.Enable	1
4	X_00507F_WirelessLAN_AP.General.SSID.1.Hide	0

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 node. **Note that this button is available only when such AP is in mesh root mode.**

Tips for Mesh Network Setup

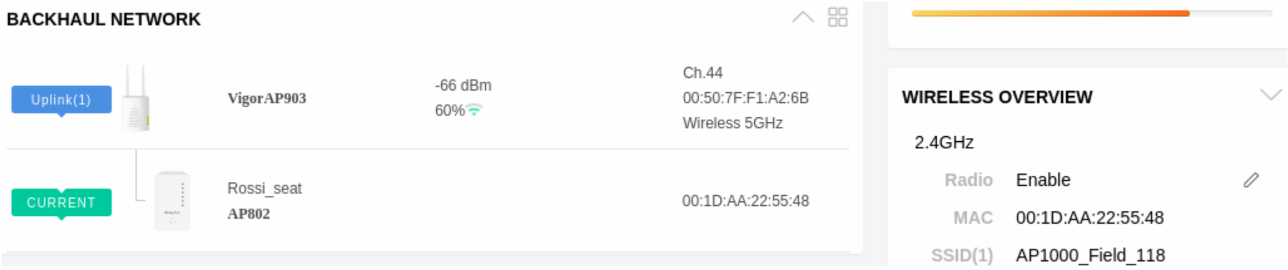
- Set up TWO mesh devices with uplink RSSI larger than -65dBm.
- Upgrade the firmware version of Mesh devices through Mesh link, starting from the mesh device with less hop number. For example, upgrade the firmware from the root, hop1 Mesh Node then hop2 Mesh Node, and so on.
- VigorMesh network supports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

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

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

iPad connects to Root	: 80Mbps
iPad connects to hop1 Node	: 49Mbps (Uplink RSSI : -55dBm)
iPad connects to hop2 Node	: 41Mbps (Uplink RSSI : hop2 -64dBm / hop1 -55dBm)
iPad connects to hop3 Node	: 26Mbps (Uplink RSSI : hop3 -62dBm / hop2 -68dBm / hop1 -55dBm)

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



BACKHAUL NETWORK

Uplink(1)	VigorAP903	-66 dBm 60%	Ch.44 00:50:7F:F1:A2:6B Wireless 5GHz
CURRENT	Rossi_seat AP802		00:1D:AA:22:55:48

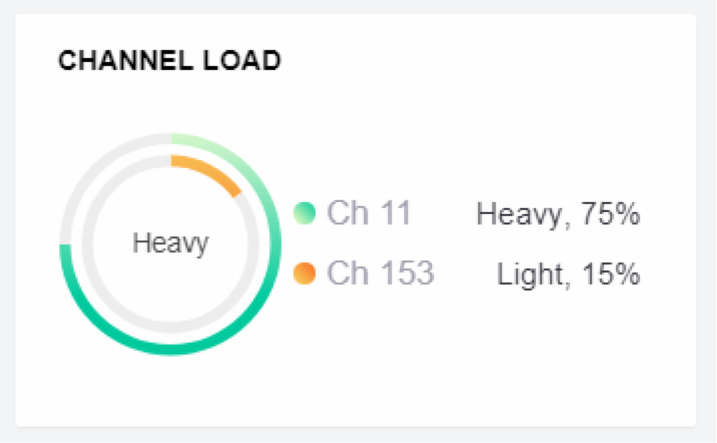
WIRELESS OVERVIEW

2.4GHz

Radio	Enable
MAC	00:1D:AA:22:55:48
SSID(1)	AP1000_Field_118

- If Mesh Search / Apply / Discover is worked too fast or is done with empty result, your request may be rejected. Please try again.

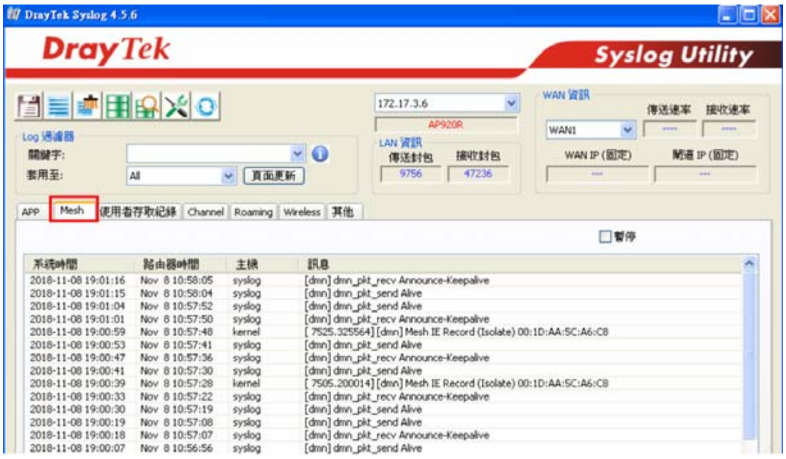
- Troubleshooting:
  - Check the firmware version. Please make sure all APs within the mesh group are in the newest firmware version.
  - Check the OP (operation) Mode. Make sure new Mesh Node doesn't accidentally get DHCP IP and becomes AP mode.
  - Check the country code and channels. For example, it is impossible for connecting a VigorAP 802 Mesh Node with 5G channel 36 to VigorAP920R Wireless Mesh Root in EU country code.
  - Check the channel load. Make sure it is not over 70%.



CHANNEL LOAD

● Ch 11	Heavy, 75%
● Ch 153	Light, 15%

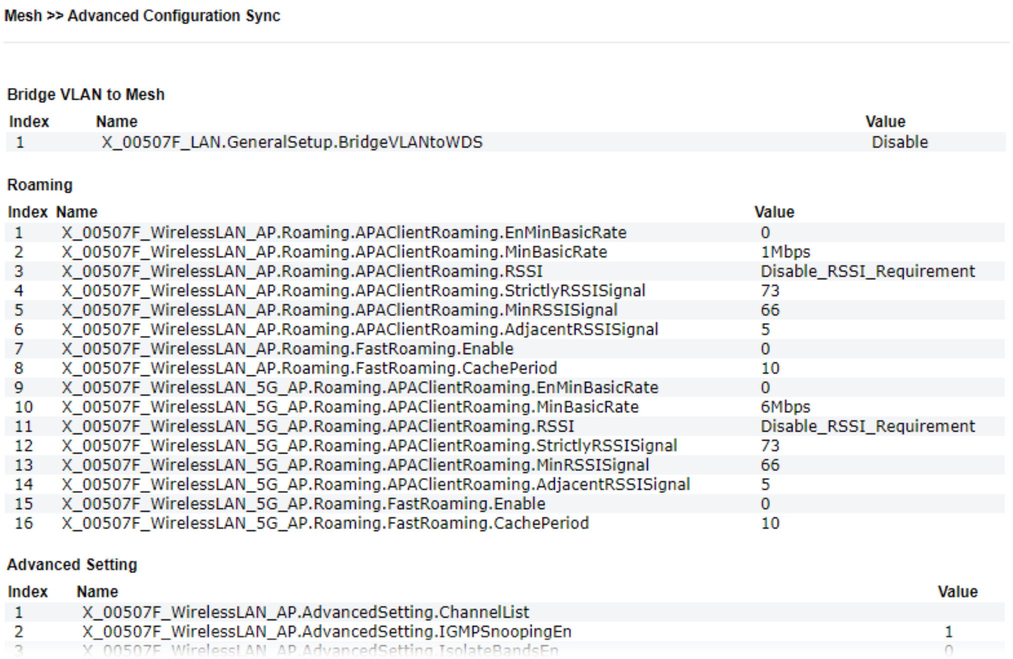
  - Collect some Mesh logs and send the result to DrayTek for analyzing.



```
系統時間              路由器時間        主機      訊息
2018-11-08 19:01:16  Nov  8 10:58:05  syslog   [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:01:15  Nov  8 10:58:04  syslog   [dmn] dmn_pkt_send Alive
2018-11-08 19:01:04  Nov  8 10:57:52  syslog   [dmn] dmn_pkt_send Alive
2018-11-08 19:01:01  Nov  8 10:57:50  syslog   [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:59  Nov  8 10:57:48  kernel   [ 7525.325564] [dmn] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8
2018-11-08 19:00:53  Nov  8 10:57:41  syslog   [dmn] dmn_pkt_send Alive
2018-11-08 19:00:47  Nov  8 10:57:36  syslog   [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:41  Nov  8 10:57:30  syslog   [dmn] dmn_pkt_send Alive
2018-11-08 19:00:39  Nov  8 10:57:28  kernel   [ 7505.200014] [dmn] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8
2018-11-08 19:00:33  Nov  8 10:57:22  syslog   [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:30  Nov  8 10:57:19  syslog   [dmn] dmn_pkt_send Alive
2018-11-08 19:00:19  Nov  8 10:57:08  syslog   [dmn] dmn_pkt_send Alive
2018-11-08 19:00:18  Nov  8 10:57:07  syslog   [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:07  Nov  8 10:56:56  syslog   [dmn] dmn_pkt_send Alive
```

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

Bridge VLAN to Mesh

Index	Name	Value
1	X_00507F_LAN.GeneralSetup.BridgeVLANtoWDS	Disable

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	73
5	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinRSSISignal	66
6	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	5
7	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.Enable	0
8	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.CachePeriod	10
9	X_00507F_WirelessLAN_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	73
13	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinRSSISignal	66
14	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	5
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	0

Available settings are explained as follows:

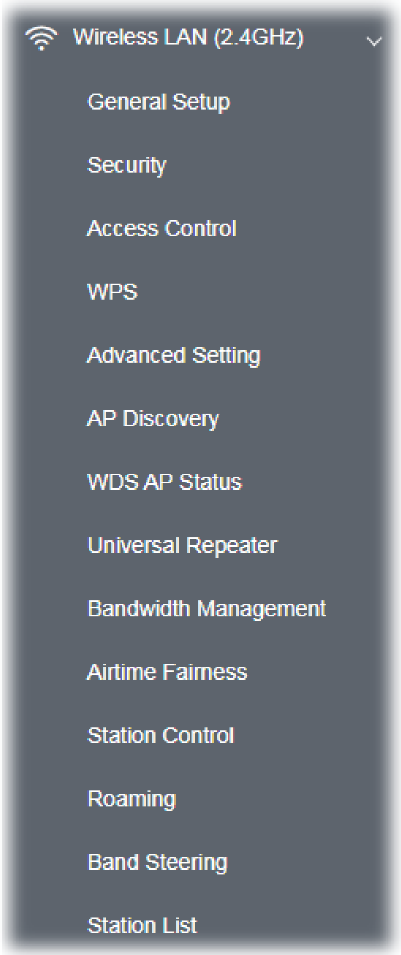
Item	Description
Select All	All item(s) will be selected for making configuration sync.
Bridge VLAN to Mesh	Check to transmit the packets with VLAN tag to mesh nodes.

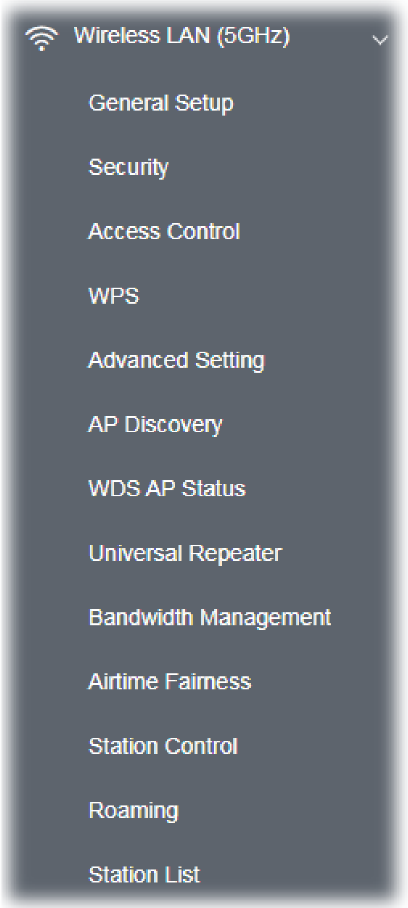
II-5 Universal Repeater Settings for Range Extender Mode

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

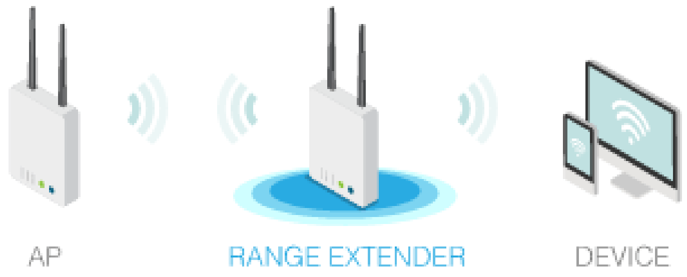
This section will introduce settings for Universal Repeater only.

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





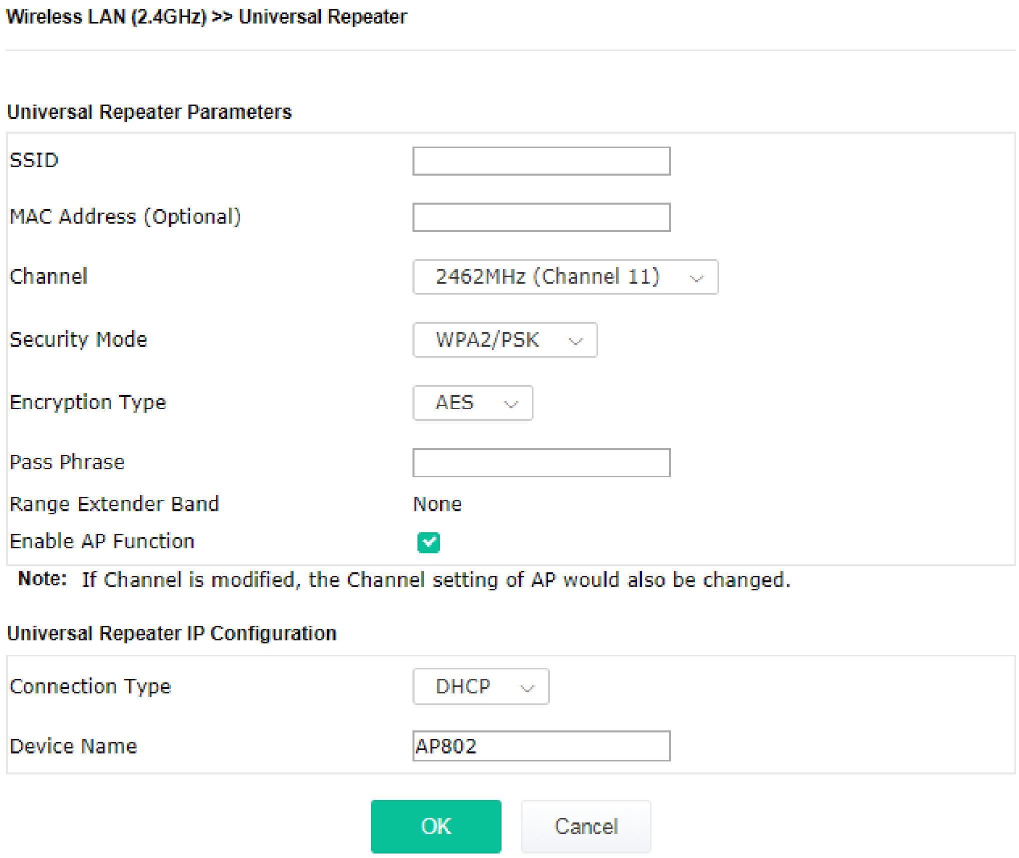
The following figure shows how VigorAP runs as Range Extender:



The access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a root AP and use AP function to serve all wireless stations within its coverage.

Note:

While using **Universal Repeater** mode, the access point will demodulate the received signal. Please check if this signal is noise for the operating network, then have the signal modulated and amplified again. The output power of this mode is the same as that of AP mode.



Wireless LAN (2.4GHz) >> Universal Repeater

Universal Repeater Parameters

SSID	
MAC Address (Optional)	
Channel	2462MHz (Channel 11)
Security Mode	WPA2/PSK
Encryption Type	AES
Pass Phrase	
Range Extender Band	None
Enable AP Function	☑

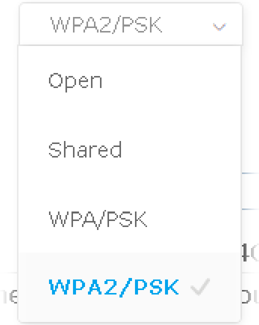
Note: If Channel is modified, the Channel setting of AP would also be changed.

Universal Repeater IP Configuration

Connection Type	DHCP
Device Name	AP802

Available settings are explained as follows:

Item	Description
Universal Repeater Parameters	
SSID	Display the SSID defined for Range Extender operation mode in Quick Start Wizard. Change the name of SSID whenever you want.
MAC Address (Optional)	Type the MAC address of access point that VigorAP 802 wants to connect to.
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to

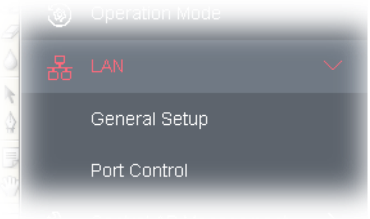
	let system determine for you.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure. 
Encryption Type for Open/Shared	This option is available when Open/Shared is selected as Security Mode. Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose **WEP**. **WEP Keys** - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.
Encryption Type for WPA/PSK and WPA2/PSK	This option is available when WPA/PSK or WPA2/PSK is selected as **Security Mode**. Select **TKIP** or **AES** as the algorithm for WPA.
Pass Phrase	Type **8~63** ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Range Extender Band	Display which wireless band (2.4G/5G) is currently used for Universal Repeater. **None** - No network connection.
Enable AP Function	If disabled, other stations cannot connect to this VigorAP even using the correct SSID. Thus, VigorAP can be used as range extender but not as an access point. In default, it is enabled.
Universal Repeater IP Configuration	
Connection Type	Choose DHCP or Static IP as the connection mode. **DHCP** – The wireless station will be assigned with an IP from VigorAP. **Static IP** – The wireless station shall specify a static IP for connecting to Internet via VigorAP.
Router Name	This setting is available when **DHCP** is selected as **Connection Type**. Type a name for the VigorAP as identification. Simply use the default name.
IP Address	This setting is available when **Static IP** is selected as **Connection**

	Type. Type an IP address with the same network segment of the LAN IP setting of VigorAP. Such IP shall be different with any IP address in LAN.
Subnet Mask	This setting is available when **Static IP** is selected as **Connection Type**. Type the subnet mask setting which shall be the same as the one configured in LAN for VigorAP.
Default Gateway	This setting is available when **Static IP** is selected as **Connection Type**. Type the gateway setting which shall be the same as the default gateway configured in LAN for VigorAP.

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

II-6 LAN

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

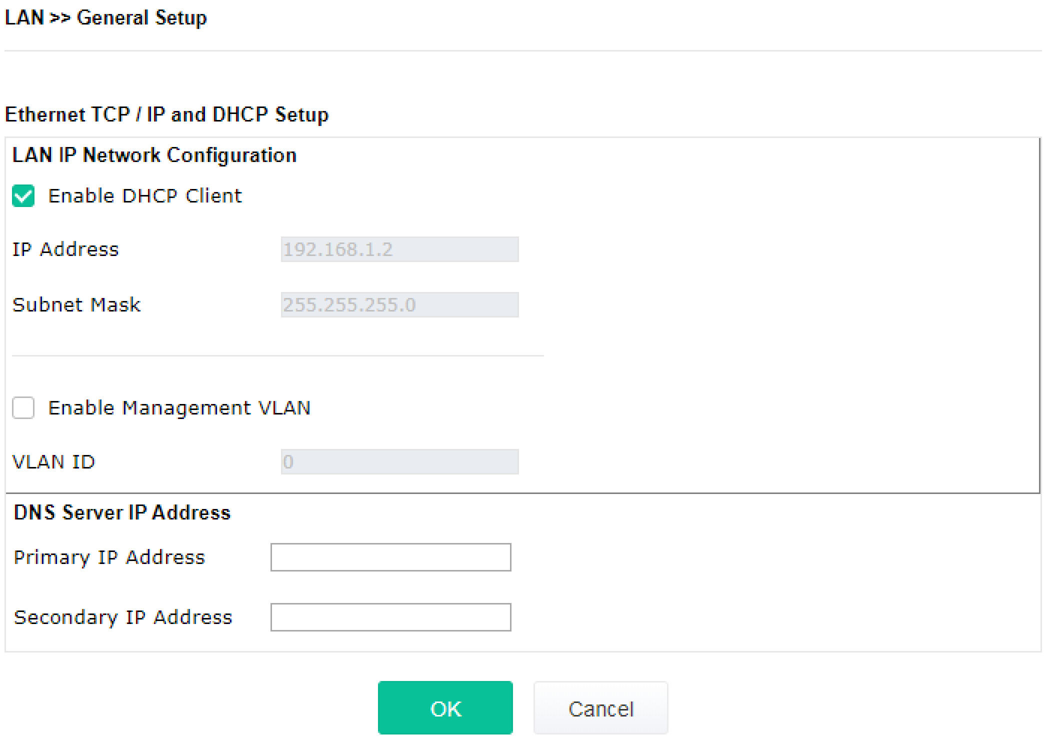


II-6-1 General Setup

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

Note:

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



LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

☑ Enable DHCP Client

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

□ Enable Management VLAN

VLAN ID: 0

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Available settings are explained as follows:

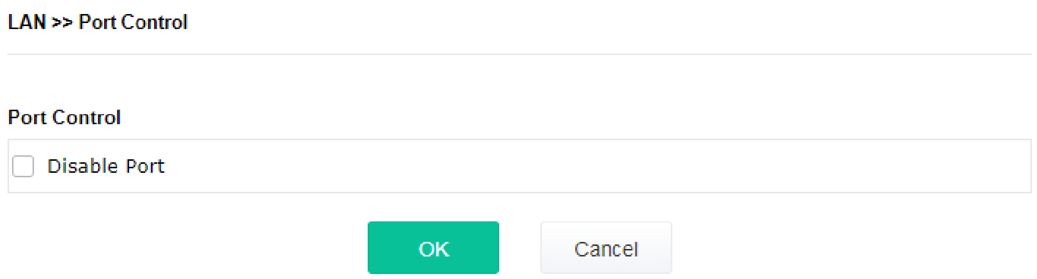
Item	Description
LAN IP Network	**Enable DHCP Client** – When it is enabled, VigorAP 802 will be treated

Configuration	as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2862). **IP Address** – Type in private IP address for connecting to a local private network (Default: 192.168.1.2). **Subnet Mask** – Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) **Enable Management VLAN** – VigorAP 802 supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 802. ● **VLAN ID** – Type the number as VLAN ID tagged on the transmitted packet. "0" means no VALN tag.
DNS Server IP Address	**Primary IP 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 IP Server -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

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

II-6-2 Port Control

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



LAN >> Port Control

Port Control

□ Disable Port

Available settings are explained as follows:

Item	**Description**
Disable Port	Check it to disable the LAN port.

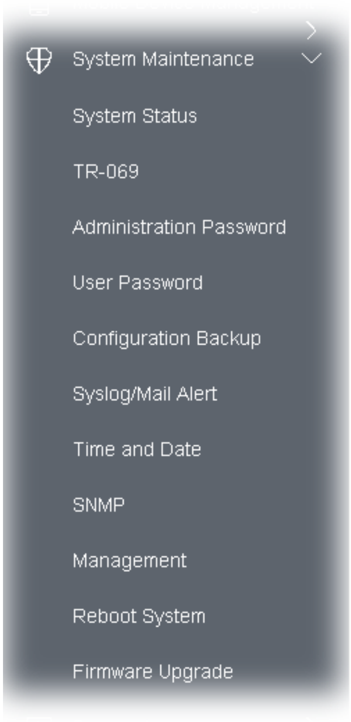
After finishing this web page configuration, please click **OK** to save the settings.

Chapter III Management

III-1 System Maintenance

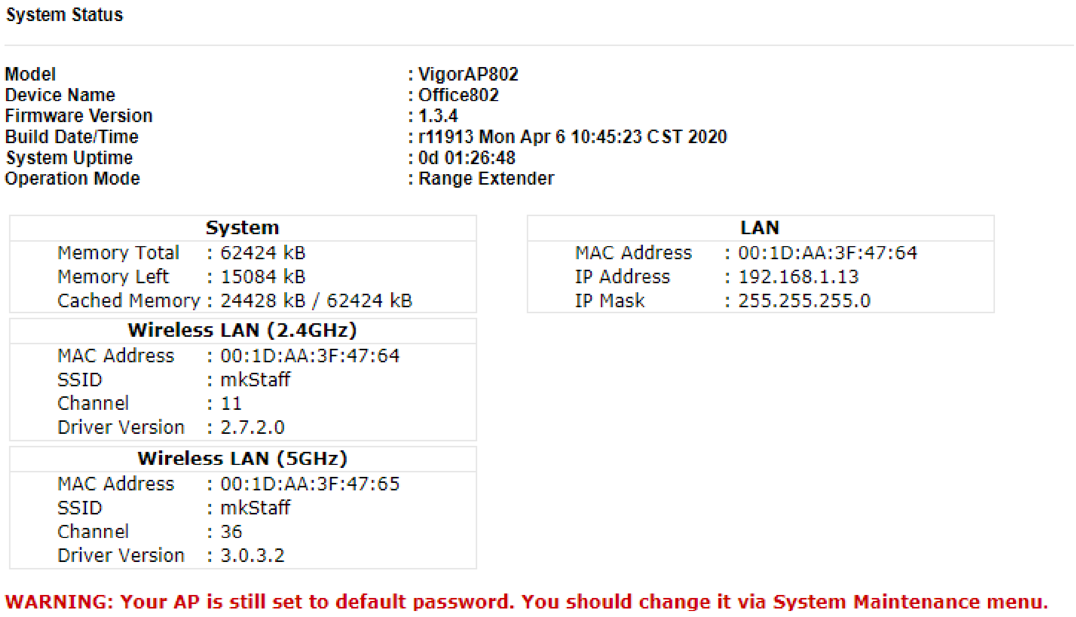
For the system setup, there are several items that you have to know the way of configuration: Status, TR-069, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



III-1-1 System Status

The **System Status** provides basic network settings of Vigor modem. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.



System Status

```
Model                          : VigorAP802
Device Name                    : Office802
Firmware Version               : 1.3.4
Build Date/Time                : r11913 Mon Apr 6 10:45:23 CST 2020
System Uptime                  : 0d 01:26:48
Operation Mode                 : Range Extender
```

```
System
Memory Total   : 62424 kB
Memory Left    : 15084 kB
Cached Memory  : 24428 kB / 62424 kB

Wireless LAN (2.4GHz)
MAC Address    : 00:1D:AA:3F:47:64
SSID           : mkStaff
Channel        : 11
Driver Version : 2.7.2.0

Wireless LAN (5GHz)
MAC Address    : 00:1D:AA:3F:47:65
SSID           : mkStaff
Channel        : 36
Driver Version : 3.0.3.2

LAN
MAC Address    : 00:1D:AA:3F:47:64
IP Address     : 192.168.1.13
IP Mask        : 255.255.255.0
```

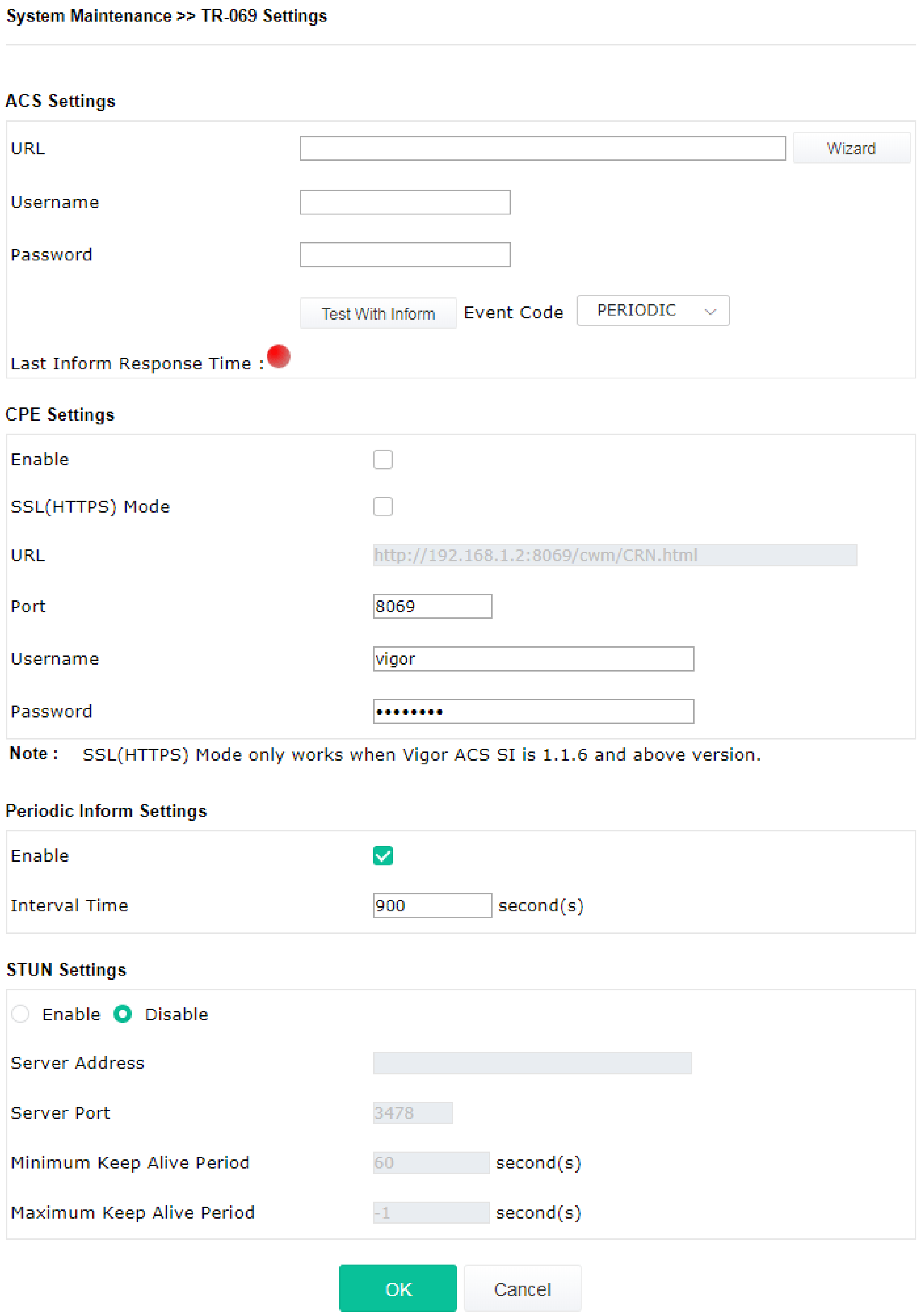
WARNING: Your AP is still set to default password. You should change it via System Maintenance menu.

Each item is explained as follows:

Item	Description
Model /Device Name	Display the model name of the modem.
Firmware Version	Display the firmware version of the modem.
Build Date/Time	Display the date and time of the current firmware build.
System Uptime	Display the period that such device connects to Internet.
Operation Mode	Display the operation mode that the device used.
System	
Memory total	Display the total memory of your system.
Memory left	Display the remaining memory of your system.
LAN	
MAC Address	Display the MAC address of the LAN Interface.
IP Address	Display the IP address of the LAN interface.
IP Mask	Display the subnet mask address of the LAN interface.
Wireless LAN (2.4GHz/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 device.

III-1-2 TR-069

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



System Maintenance >> TR-069 Settings

ACS Settings

URL	[ ] Wizard
Username	[ ]
Password	[ ]
	Test With Inform Event Code PERIODIC
Last Inform Response Time : ●	

CPE Settings

Enable	□
SSL(HTTPS) Mode	□
URL	http://192.168.1.2:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	••••••••

Note : SSL(HTTPS) Mode only works when Vigor ACS SI is 1.1.6 and above version.

Periodic Inform Settings

Enable	☑
Interval Time	900 second(s)

STUN Settings

○ Enable ● Disable

Server Address	
Server Port	3478
Minimum Keep Alive Period	60 second(s)
Maximum Keep Alive Period	-1 second(s)

Available settings are explained as follows:

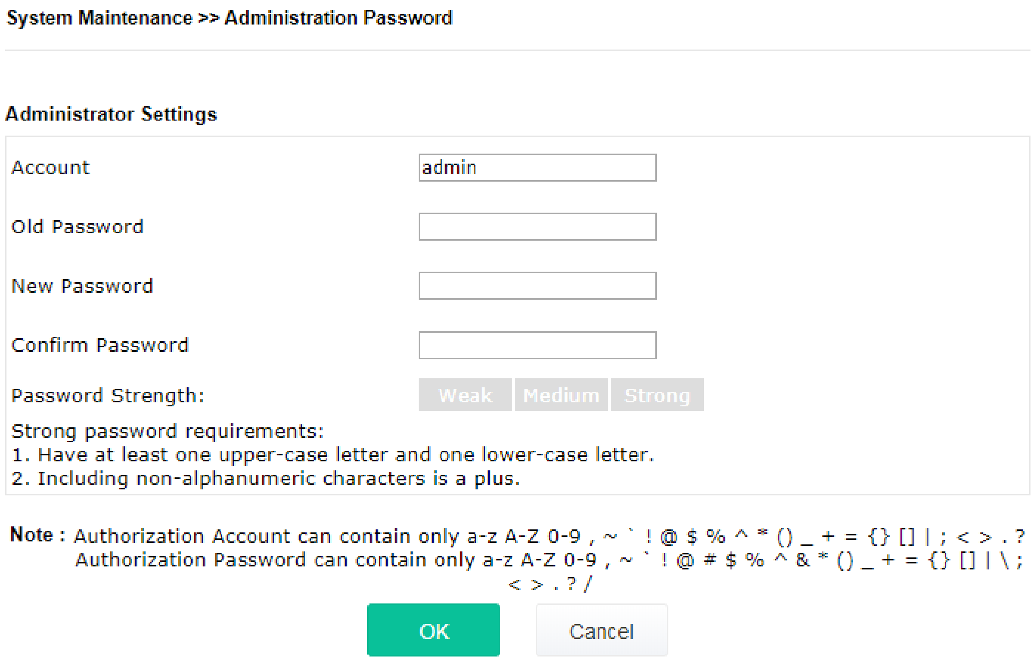
Item	Description
ACS Settings	**Wizard** – Click it to enter the IP address of VigorACS server host, port number and the handler. **URL/Username/Password –** Such data must be typed according to

	the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information. **Test With Inform** – Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server. **Event Cod**e – Use the drop down menu to specify an event to perform the test. **Last Inform Response Time** – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
CPE Settings	Such information is useful for Auto Configuration Server (ACS). **Enable**– Check the box to allow the CPE Client to connect with Auto Configuration Server. **SSL(HTTPS) Mode** - Check the box to allow the CPE client to connect with ACS through SSL. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. **Username/Password –** Type the username and password that VigorACS can use to access into such CPE.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the AP to send notification to 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 binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

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

III-1-3 Administrator Password

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



System Maintenance >> Administration Password

Administrator Settings

Account	admin
Old Password	
New Password	
Confirm Password	
Password Strength:	Weak Medium Strong

Strong password requirements:
1. Have at least one upper-case letter and one lower-case letter.
2. Including non-alphanumeric characters is a plus.

Note : Authorization Account can contain only a-z A-Z 0-9 , ~ ` ! @ $ % ^ * () _ + = {} [] | ; < > . ?
Authorization Password can contain only a-z A-Z 0-9 , ~ ` ! @ # $ % ^ & * () _ + = {} [] | \ ; < > . ? /

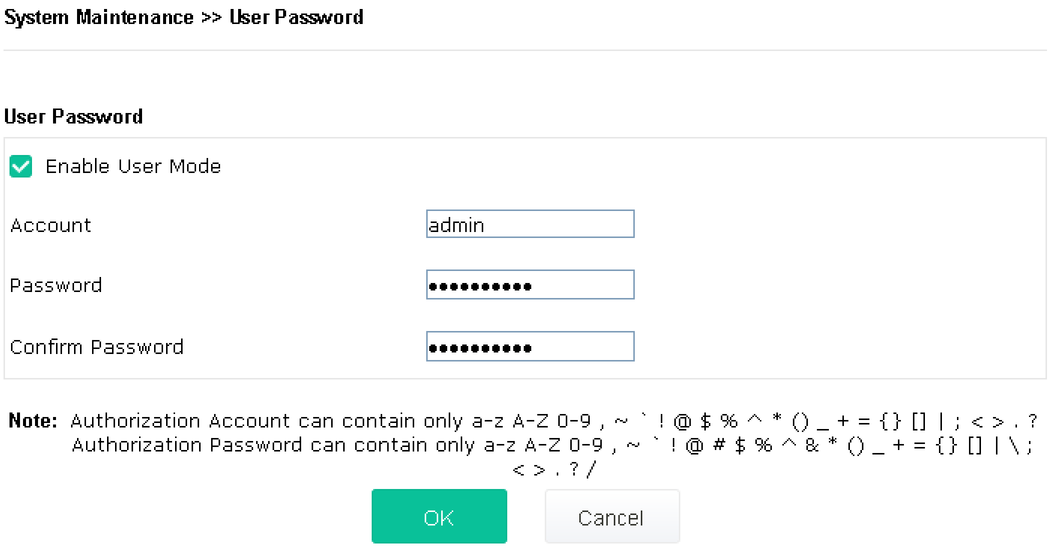
Available settings are explained as follows:

Item	Description
Account	Enter the name for accessing into web user Interface.
Old Password	Enter the old password for accessing into the web user interface.
New Password	Enter in new password in this filed.
Confirm Password	Enter the new password again for confirmation.
Password Strength	The system will display the password strength (represented with the word of weak, medium or strong) of the password specified above.

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

III-1-4 User Password

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



System Maintenance >> User Password

User Password

☑ Enable User Mode

Account: admin

Password: ●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●

Note: Authorization Account can contain only a-z A-Z 0-9 , ~ ` ! @ $ % ^ * () _ + = {} [] | ; < > . ?
Authorization Password can contain only a-z A-Z 0-9 , ~ ` ! @ # $ % ^ & * () _ + = {} [] | \ ; < > . ? /

Available settings are explained as follows:

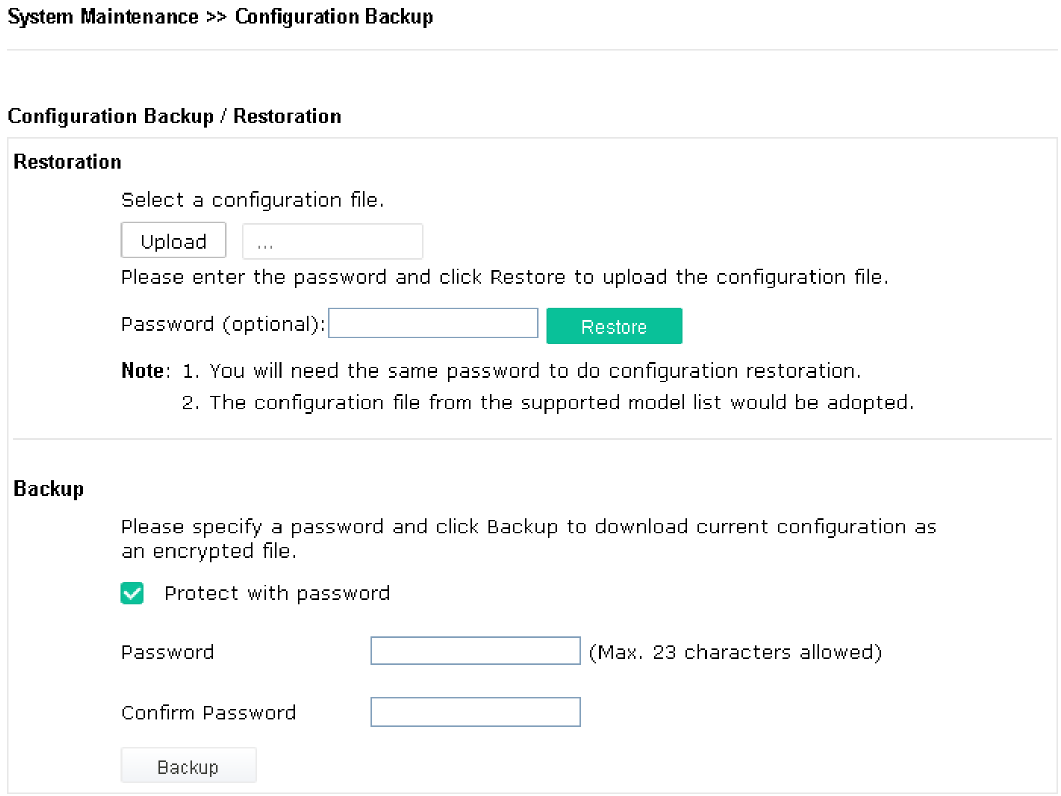
Item	Description
Enable User Mode	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Account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

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

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

III-1-5 Configuration Backup

Such function can be used to backup/restore the VigorAP 802 settings.



System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Upload ...

Please enter the password and click Restore to upload the configuration file.

Password (optional): Restore

Note: 1. You will need the same password to do configuration restoration.
2. The configuration file from the supported model list would be adopted.

Backup

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

☑ Protect with password

Password (Max. 23 characters allowed)

Confirm Password

Backup

Available settings are explained as follows:

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

Follow the steps below to backup your configuration.

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

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

ⓘ **Note:**

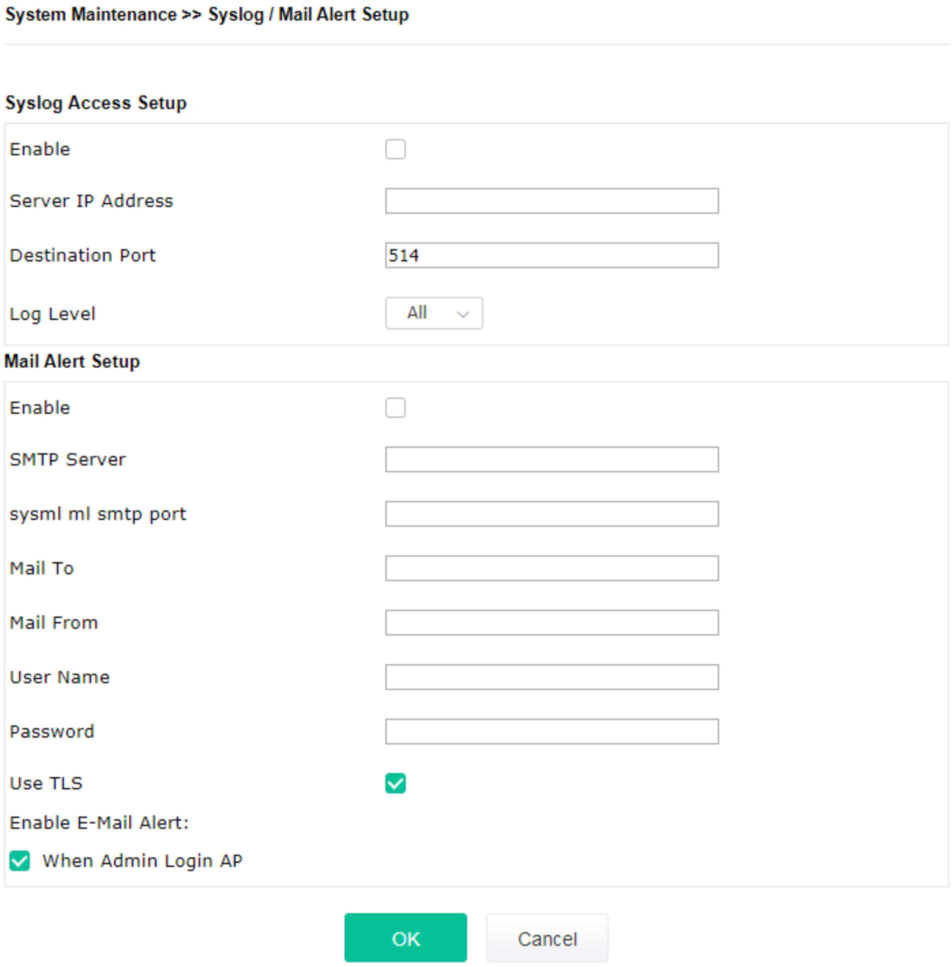
Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Follow the steps below to restore your configuration.

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

III-1-6 Syslog/Mail Alert

SysLog function is provided for users to monitor AP. There is no bother to directly get into the Web user interface of the AP or borrow debug equipments.



System Maintenance >> Syslog / Mail Alert Setup

Syslog Access Setup

Enable	□
Server IP Address	
Destination Port	514
Log Level	All

Mail Alert Setup

Enable	□
SMTP Server	
sysml ml smtp port	
Mail To	
Mail From	
User Name	
Password	
Use TLS	☑

Enable E-Mail Alert:

☑ When Admin Login AP

Available settings are explained as follows:

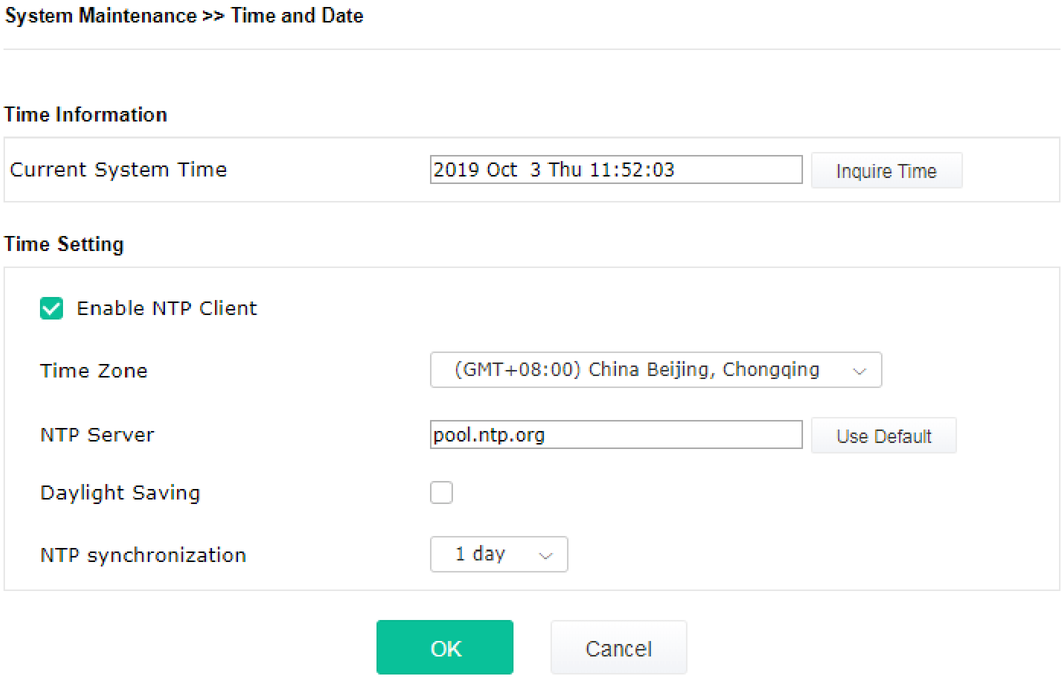
Item	Description
Syslog Access Setup	**Enable** - Check **Enable** to activate function of Syslog. **Server IP Address** -The IP address of the Syslog server. **Destination Port** -Assign a port for the Syslog protocol. The default setting is 514. **Log Level** - Specify which level of the severity of the event will be recorded by Syslog.
Mail Alert Setup	**Enable** - Check **Enable** to activate function of mail alert. **SMTP Server -** The IP address of the SMTP server. **Mail To -** Assign a mail address for sending mails out. **Mail From -** Assign a path for receiving the mail from outside. **User Name -** Type the user name for authentication. **Password -** Type the password for authentication. **Use TLS** – Check this box to encrypt alert mail. However, if the SMTP

	server specified here does not support TLS protocol, the alert mail with encrypted data will not be received by the receiver. **Enable E-Mail Alert** - VigorAP will send an e-mail out when a user accesses into the user interface by using web or telnet. **When Admin Login AP** – Enable/disable the function. When it is enabled, VigorAP will send out an e-mail to the recipient defined above when a user tries to access into VigorAP by entering login username and password.

Click **OK** to save the settings.

III-1-7 Time and Date

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



System Maintenance >> Time and Date

Time Information

Current System Time: 2019 Oct 3 Thu 11:52:03

Time Setting

☑ Enable NTP Client

Time Zone: (GMT+08:00) China Beijing, Chongqing

NTP Server: pool.ntp.org

Daylight Saving: □

NTP synchronization: 1 day

Available parameters are explained as follows:

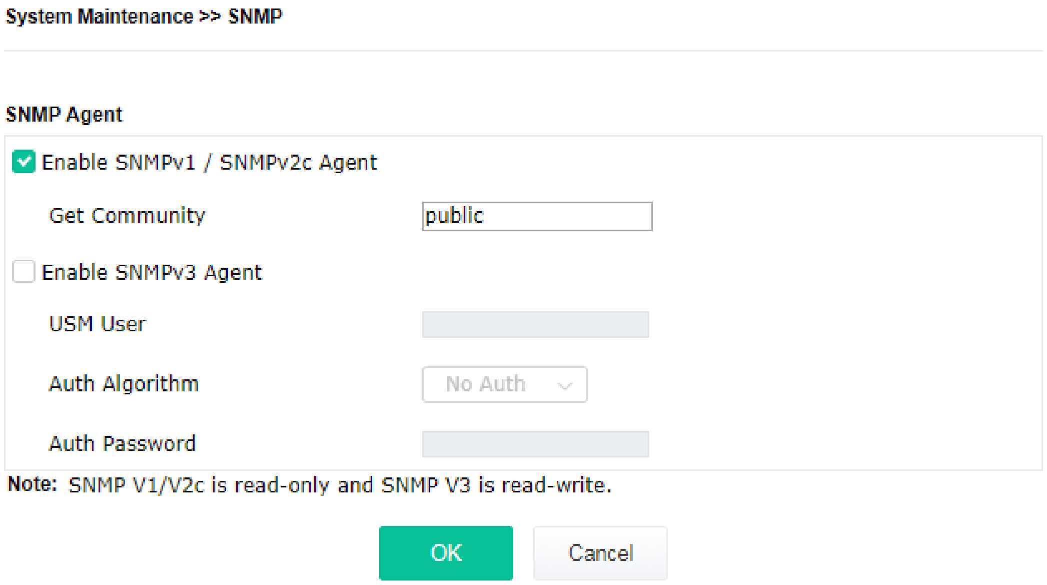
Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Enable NTP Client	Check it to inquire time information from Time Server on the Internet using assigned protocol.
Time Zone	Select a time protocol.
NTP Server	Type the IP address of the time server. **Use Default** – Click it to choose the default NTP server.
Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.
NTP synchronization	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

III-1-8 SNMP

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

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



System Maintenance >> SNMP

SNMP Agent

☑ Enable SNMPv1 / SNMPv2c Agent

Get Community: public

□ Enable SNMPv3 Agent

USM User:

Auth Algorithm: No Auth

Auth Password:

Note: SNMP V1/V2c is read-only and SNMP V3 is read-write.

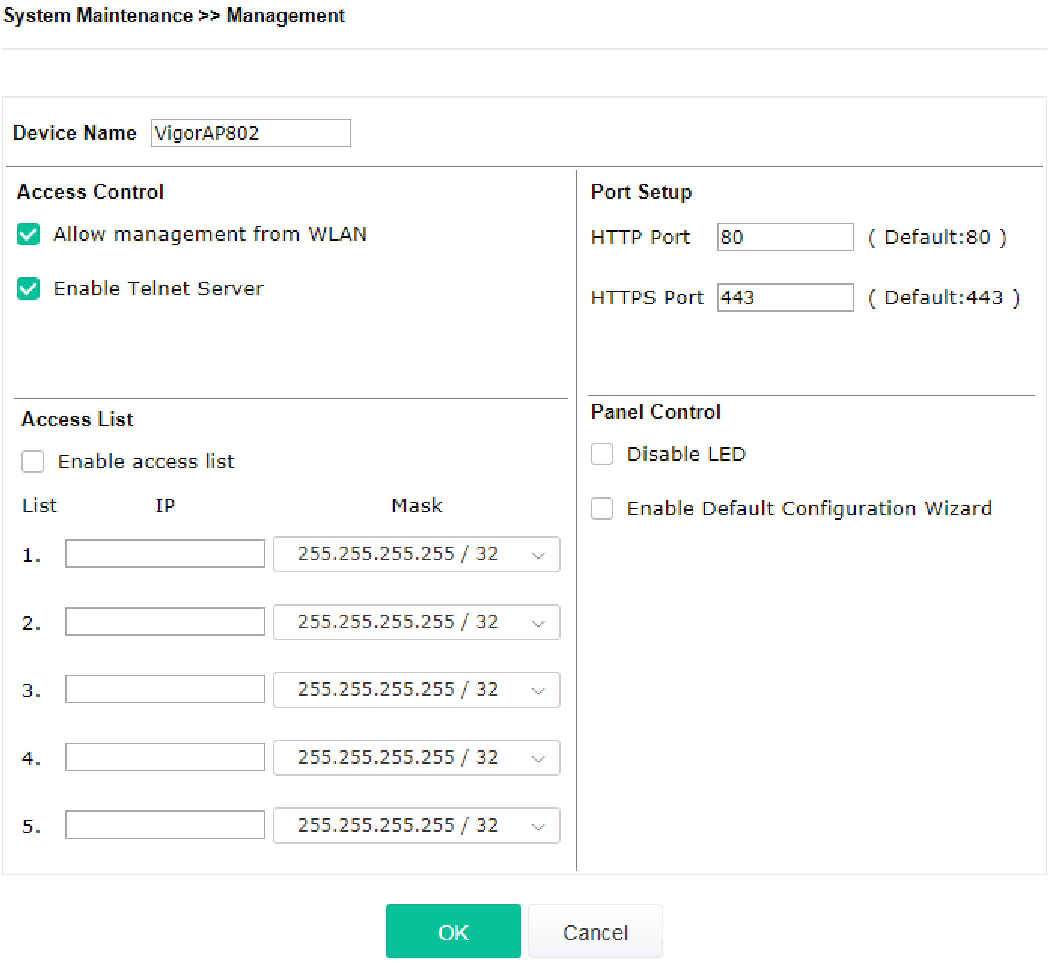
Available settings are explained as follows:

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 will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm.
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.

Click **OK** to save these settings.

III-1-9 Management

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



System Maintenance >> Management

Device Name: VigorAP802

Access Control

☑ Allow management from WLAN

☑ Enable Telnet Server

Port Setup

HTTP Port: 80 (Default:80)

HTTPS Port: 443 (Default:443)

Access List

□ Enable access list

List	IP	Mask
1.		255.255.255.255 / 32
2.		255.255.255.255 / 32
3.		255.255.255.255 / 32
4.		255.255.255.255 / 32
5.		255.255.255.255 / 32

Panel Control

□ Disable LED

□ Enable Default Configuration Wizard

Available parameters are explained as follows:

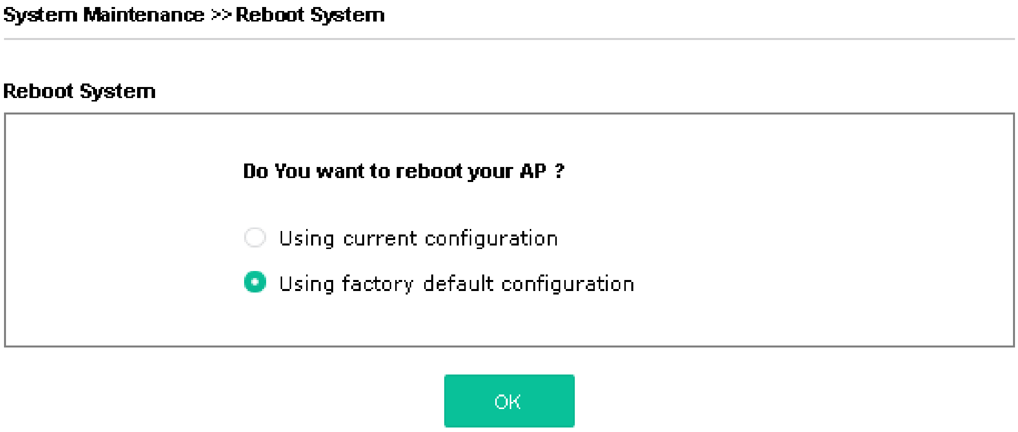
Item	Description
Device Name	The default setting is VigorAP 802. Change the name if required.
Access Control	**Allow management from WLAN** - Enable the checkbox to allow system administrators to login from wireless LAN. **Enable Telnet Server**– The administrator / user can access into the command line interface of VigorAP remotely for configuring settings.
Access List	**Enable access list** – Check the box to specify that the system administrator can only login from a specific host or network defined in the list. A maximum of five IPs/subnet masks is allowed.
Port Setup	**HTTP port/HTTPS port** -Specify user-defined port numbers for the HTTP and HTTPS servers.
Panel Control	**Disable LED** - The LEDs blink always since VigorAP is powered on. Some people might not like that. Therefore the function of LED is allowed to be disabled to make people feeling comfortable and undisturbed. After checking it, all the LEDs on VigorAP will light off immediately after clicking OK. **Enable Default Configuration Wizard** – Default setting is enabled.

	When it is enabled, you will be guided into **Quick Start Wizard** whenever clicking the DrayTek logo on the top of the web user interface. Such function will be disabled if you have configured Operation Mode, WLAN>>General Setup, WLAN>>Bandwidth Management, WLAN>>Station Control or System Maintenance>>Administration Password.

Click **OK** to save these settings.

III-1-10 Reboot System

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



System Maintenance >> Reboot System

Reboot System

Do You want to reboot your AP ?

○ Using current configuration

● Using factory default configuration

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

Note:

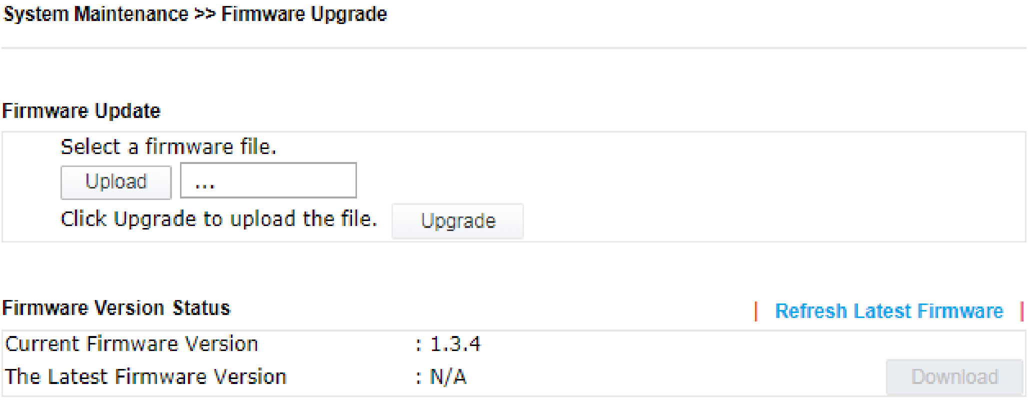
When the system pops up Reboot System web page after configuring the web settings, please click **OK** to reboot your device for ensuring normal operation and preventing unexpected errors of the modem in the future.

III-1-11 Firmware Upgrade

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

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

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



System Maintenance >> Firmware Upgrade

Firmware Update

Select a firmware file.

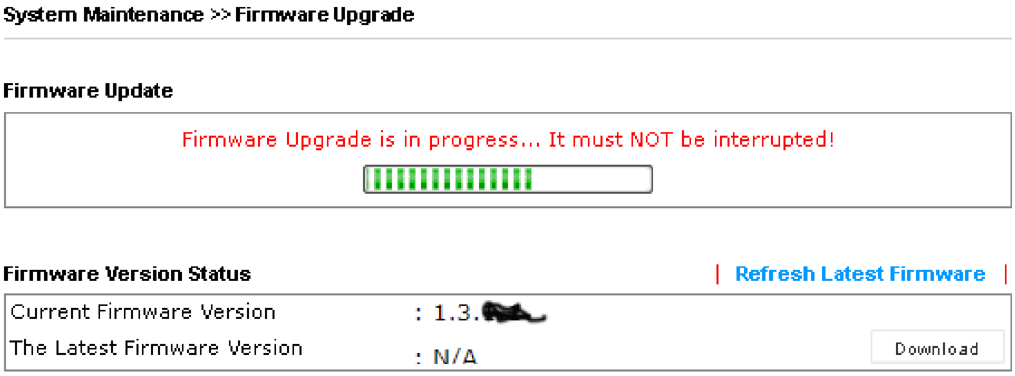
Upload ...

Click Upgrade to upload the file. Upgrade

Firmware Version Status | Refresh Latest Firmware |

Current Firmware Version	: 1.3.4	
The Latest Firmware Version	: N/A	Download

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



System Maintenance >> Firmware Upgrade

Firmware Update

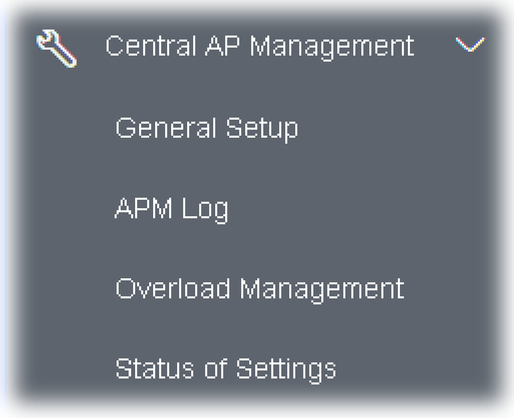
Firmware Upgrade is in progress... It must NOT be interrupted!

Firmware Version Status | Refresh Latest Firmware |

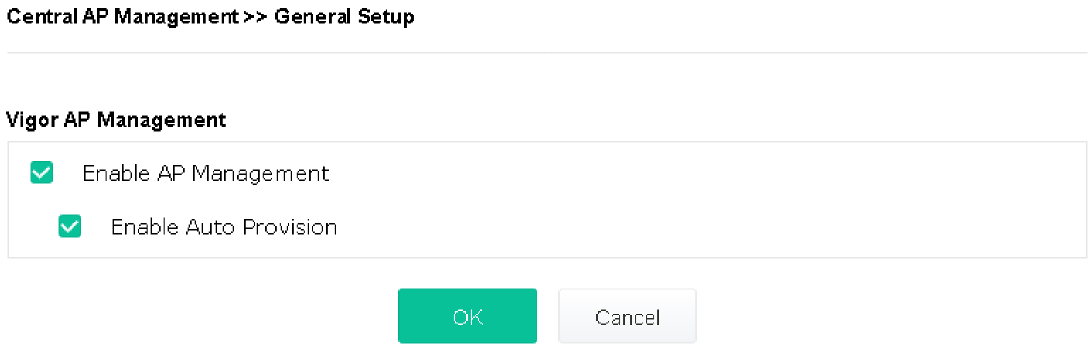
Current Firmware Version	: 1.3.[redacted]	
The Latest Firmware Version	: N/A	Download

III-2 Central AP Management

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



III-2-1 General Setup



Central AP Management >> General Setup

Vigor AP Management

☑ Enable AP Management

☑ Enable Auto Provision

Available settings are explained as follows:

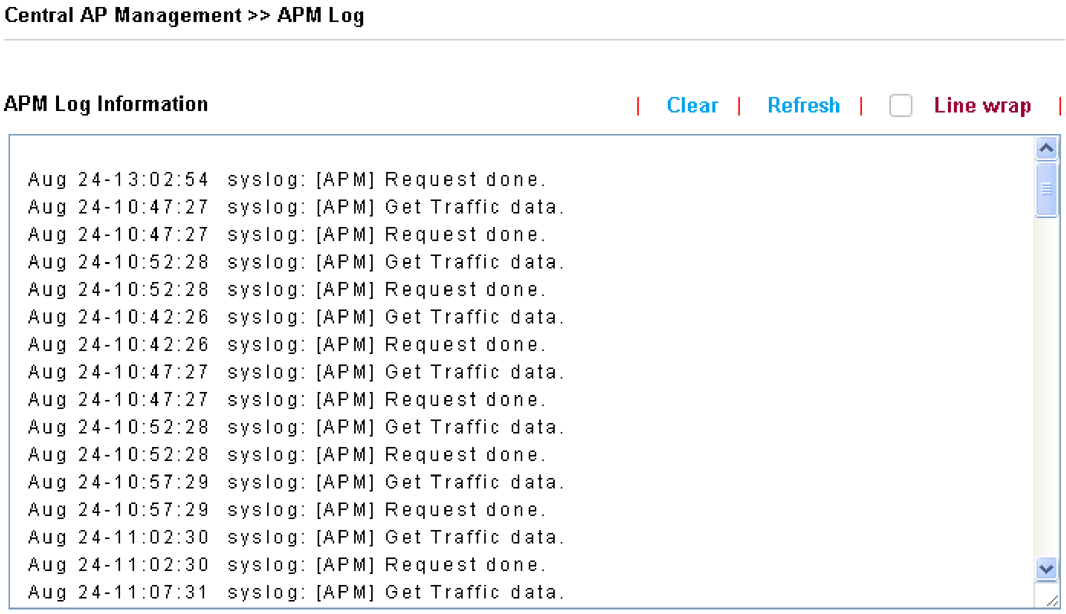
Item	Description
Enable AP Management	Check the box to enable the function of AP Management (APM).
Enable Auto Provision	VigorAP 802 can be controlled under Central AP Management in Vigor2862 series. When both Vigor2862 series and VigorAP 802 have such feature enabled, once VigorAP 802 is registered to Vigor2862 series, the **WLAN profile** pre-configured on Vigor2862 series will be applied to VigorAP 802 immediately. Thus, it is not necessary to configure VigorAP 802 separately.

Click **OK** to save these settings.

III-2-2 APM Log

This page will display log information related to wireless stations connected to VigorAP 802 and central AP management.

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


Central AP Management >> APM Log
APM Log Information
| Clear | Refresh | □ Line wrap |

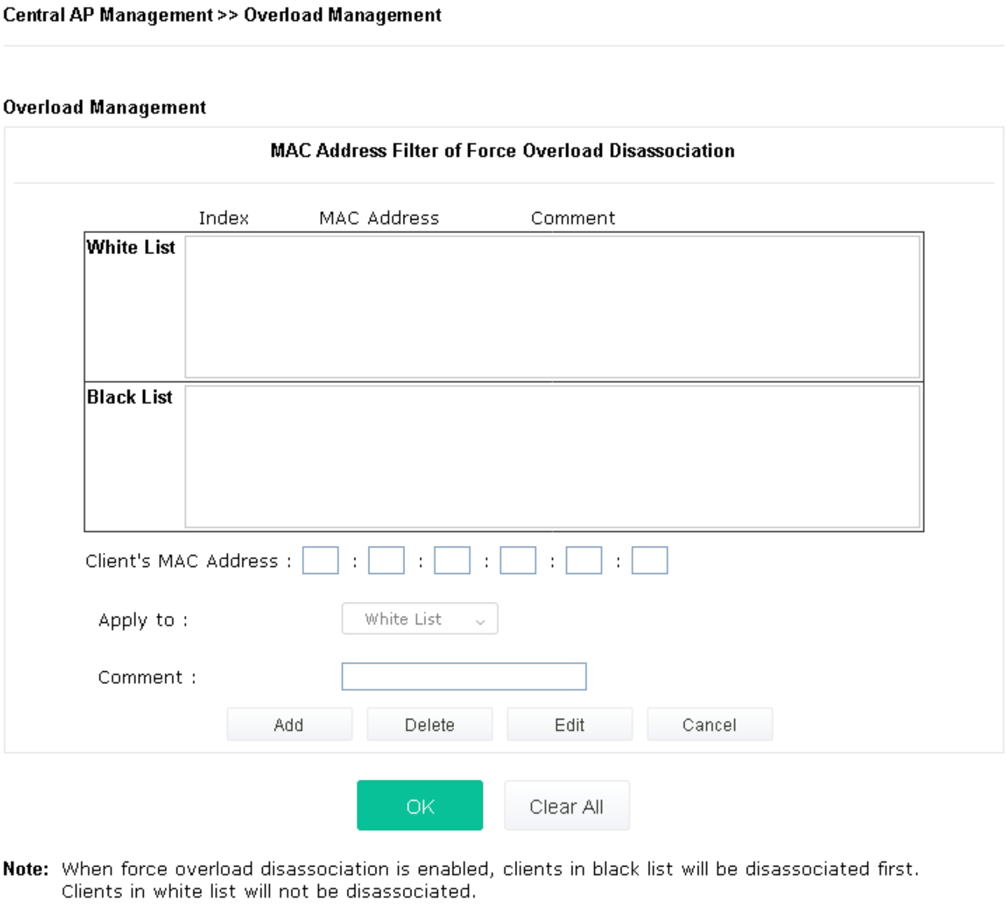
```
Aug 24-13:02:54  syslog: [APM] Request done.
Aug 24-10:47:27  syslog: [APM] Get Traffic data.
Aug 24-10:47:27  syslog: [APM] Request done.
Aug 24-10:52:28  syslog: [APM] Get Traffic data.
Aug 24-10:52:28  syslog: [APM] Request done.
Aug 24-10:42:26  syslog: [APM] Get Traffic data.
Aug 24-10:42:26  syslog: [APM] Request done.
Aug 24-10:47:27  syslog: [APM] Get Traffic data.
Aug 24-10:47:27  syslog: [APM] Request done.
Aug 24-10:52:28  syslog: [APM] Get Traffic data.
Aug 24-10:52:28  syslog: [APM] Request done.
Aug 24-10:57:29  syslog: [APM] Get Traffic data.
Aug 24-10:57:29  syslog: [APM] Request done.
Aug 24-11:02:30  syslog: [APM] Get Traffic data.
Aug 24-11:02:30  syslog: [APM] Request done.
Aug 24-11:07:31  syslog: [APM] Get Traffic data.
```

III-2-3 Overload Management

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 802) registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

However, traffic overload might be occurred if too many wireless stations connected to VigorAP 802 for data incoming and outgoing. Therefore, “Force Overload Disassociation” is required to terminate the network connection of the client’s station to release network traffic. When the function of “Force Overload Disassociation” in web user interface of Vigor router (e.g., Vigor2860 or Vigor2925 series) is enabled, wireless clients specified in **black list** of such web page will be disassociated to solve the problem of traffic overload.

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



Central AP Management >> Overload Management

Overload Management

MAC Address Filter of Force Overload Disassociation

Index	MAC Address	Comment

White List

Black List

Client's MAC Address : ___ : ___ : ___ : ___ : ___ : ___

Apply to : White List

Comment :

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

Available settings are explained as follows:

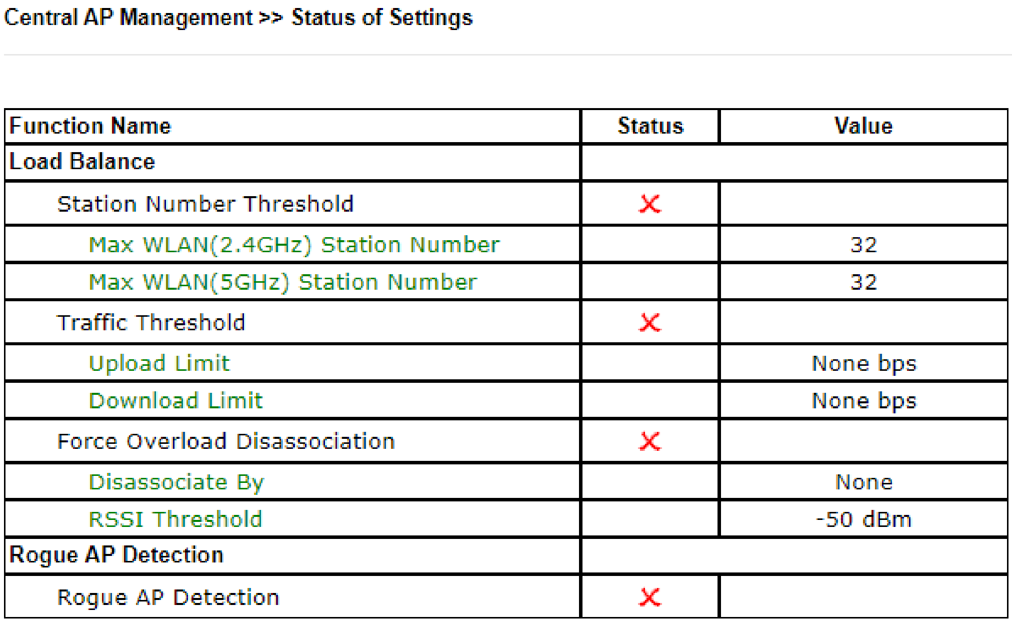
Item	Description
White List/Black List	Display the information (such as index number, MAC address and comment) for all of the members in White List/Black List. Wireless stations listed in Black List will be forcefully disconnected first when traffic overload occurs and “Force Overload Disassociation” is enabled.
Client’s MAC Address	Specify the MAC Address of the remote/local client.
Apply to	**White List** – MAC address listed inside Client’s MAC Address will be categorized as one of members in White List. **Black List** - MAC address listed inside Client’s MAC Address will be categorized as one of members in Black List.

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

Click **OK** to save these settings.

III-2-4 Status of Settings

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 802s) registered to Vigor 2862 or Vigor2926 series. This web page displays the settings related to Load Balance for VigorAP 802. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor 2862 or Vigor2926 series.

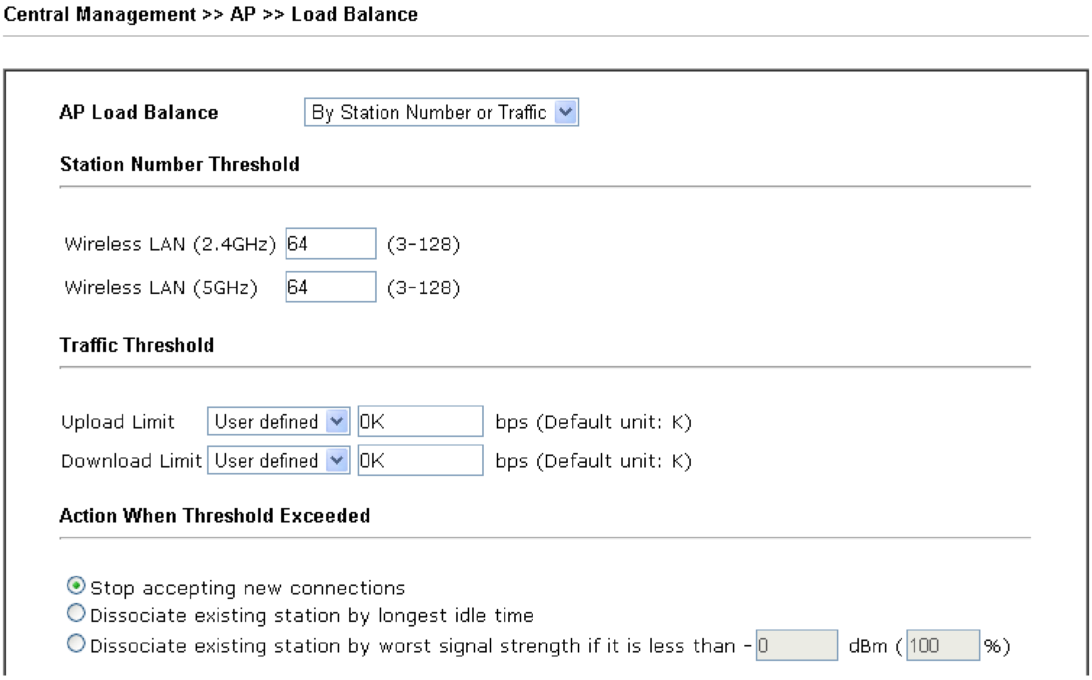


Central AP Management >> Status of Settings

Function Name	Status	Value
Load Balance		
Station Number Threshold	✗	
Max WLAN(2.4GHz) Station Number		32
Max WLAN(5GHz) Station Number		32
Traffic Threshold	✗	
Upload Limit		None bps
Download Limit		None bps
Force Overload Disassociation	✗	
Disassociate By		None
RSSI Threshold		-50 dBm
Rogue AP Detection		
Rogue AP Detection	✗	

"X" means the function is not enabled or VigorAP 802 has not registered to any Vigor router yet.

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



Central Management >> AP >> Load Balance

AP Load Balance: By Station Number or Traffic

Station Number Threshold

Wireless LAN (2.4GHz) 64 (3-128)

Wireless LAN (5GHz) 64 (3-128)

Traffic Threshold

Upload Limit: User defined 0K bps (Default unit: K)

Download Limit: User defined 0K bps (Default unit: K)

Action When Threshold Exceeded

● Stop accepting new connections

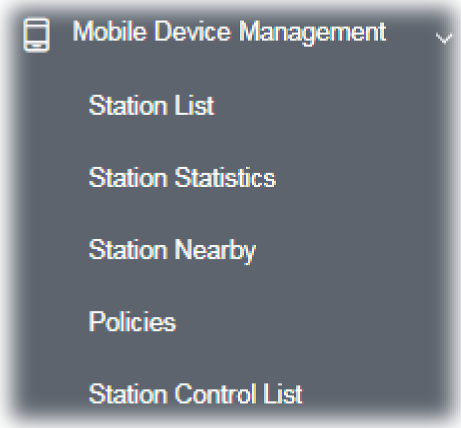
○ Dissociate existing station by longest idle time

○ Dissociate existing station by worst signal strength if it is less than - 0 dBm (100 %)

III-3 Mobile Device Management

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

Below shows the menu items for Mobile Device Management (MDM).

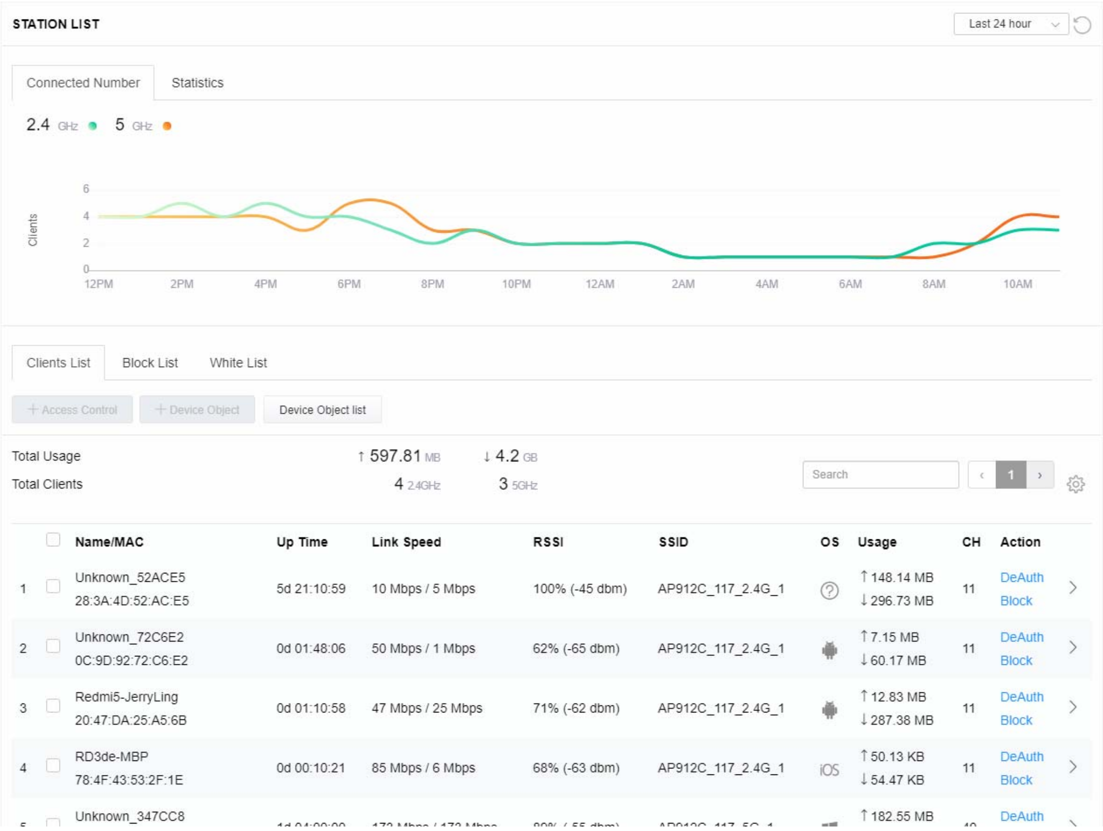


III-3-1 Station List

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

III-3-1-1 Connected Number

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



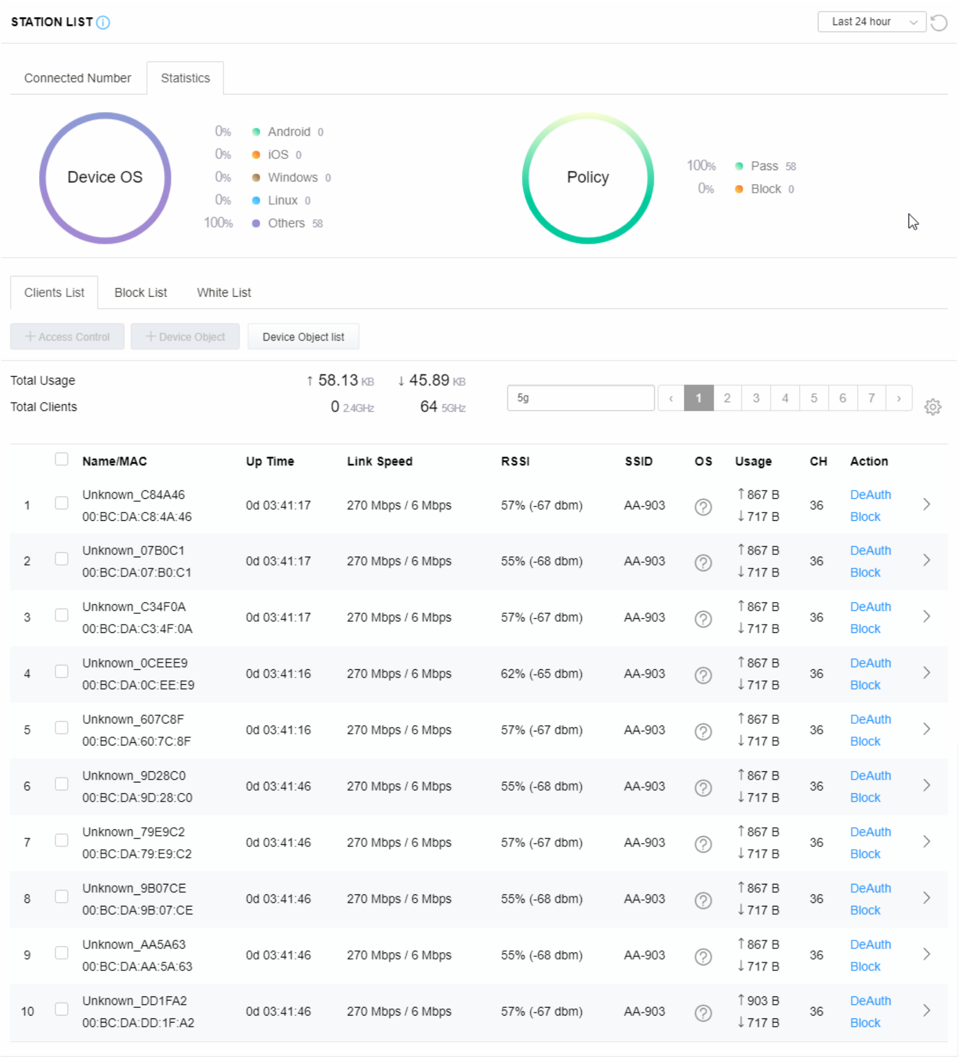
Total Usage ↑ 597.81 MB ↓ 4.2 GB

Total Clients 4 2.4GHz 3 5GHz

	□	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	□	Unknown_52ACE5 28:3A:4D:52:AC:E5	5d 21:10:59	10 Mbps / 5 Mbps	100% (-45 dbm)	AP912C_117_2.4G_1	?	↑148.14 MB ↓296.73 MB	11	DeAuth Block
2	□	Unknown_72C6E2 0C:9D:92:72:C6:E2	0d 01:48:06	50 Mbps / 1 Mbps	62% (-65 dbm)	AP912C_117_2.4G_1		↑7.15 MB ↓60.17 MB	11	DeAuth Block
3	□	Redmi5-JerryLing 20:47:DA:25:A5:6B	0d 01:10:58	47 Mbps / 25 Mbps	71% (-62 dbm)	AP912C_117_2.4G_1		↑12.83 MB ↓287.38 MB	11	DeAuth Block
4	□	RD3de-MBP 78:4F:43:53:2F:1E	0d 00:10:21	85 Mbps / 6 Mbps	68% (-63 dbm)	AP912C_117_2.4G_1	iOS	↑50.13 KB ↓54.47 KB	11	DeAuth Block
	□	Unknown_347CC8						↑182.55 MB		DeAuth

III-3-1-2 Statistics

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



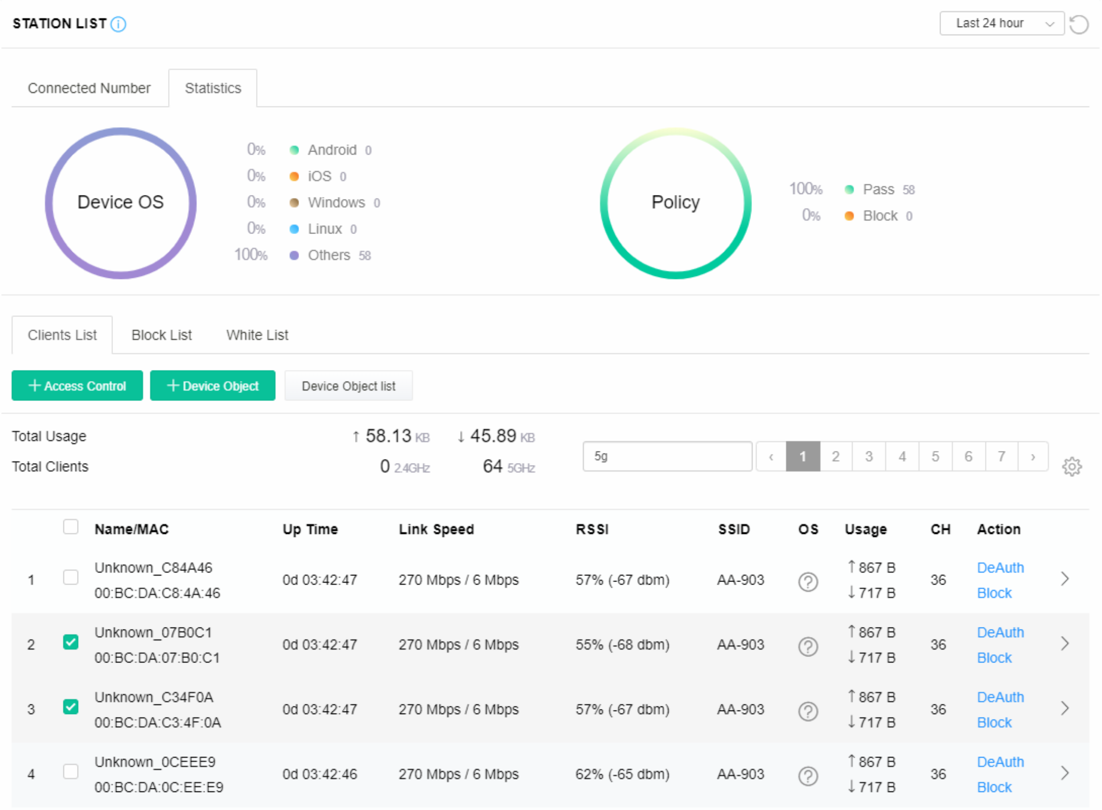
Total Usage ↑ 58.13 KB ↓ 45.89 KB

Total Clients 0 2.4GHz 64 5GHz

	□	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	›

III-3-1-3 Clients List

The client list displays all the stations connecting to VigorAP.



STATION LIST ⓘ

Last 24 hour

Device OS: 0% Android 0; 0% iOS 0; 0% Windows 0; 0% Linux 0; 100% Others 58

Policy: 100% Pass 58; 0% Block 0

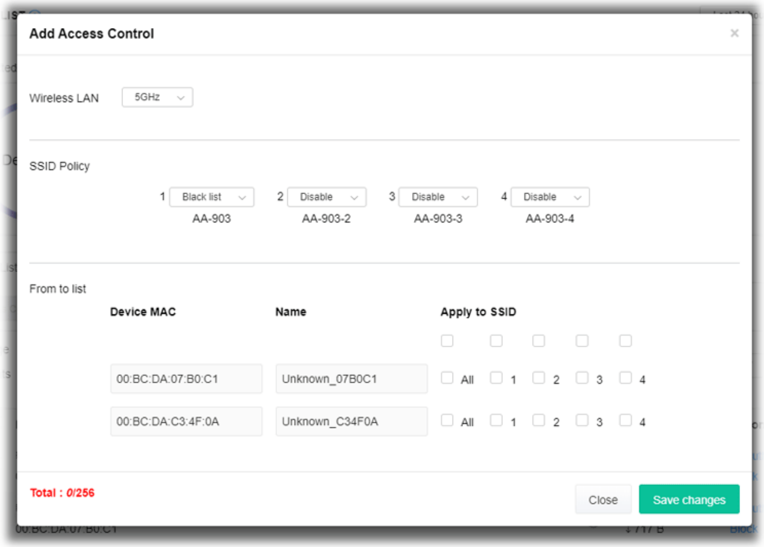
Total Usage ↑ 58.13 KB ↓ 45.89 KB

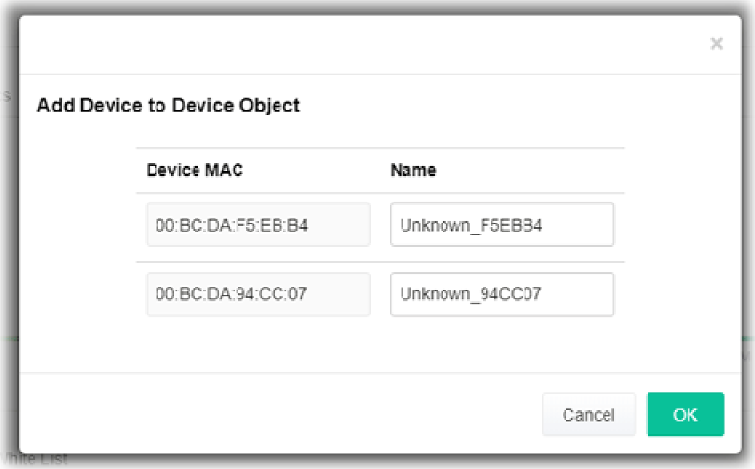
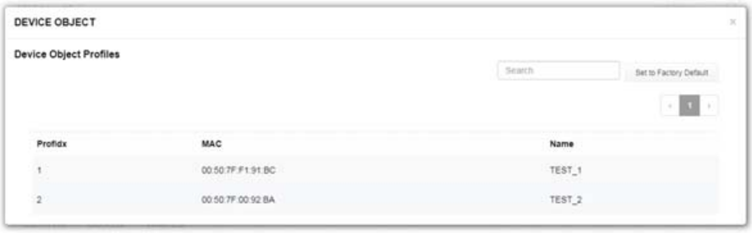
Total Clients 0 2.4GHz 64 5GHz

5g

	□	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	□	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:42:47	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 03:42:47	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 03:42:47	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 03:42:46	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	↑867 B ↓717 B	36	DeAuth Block

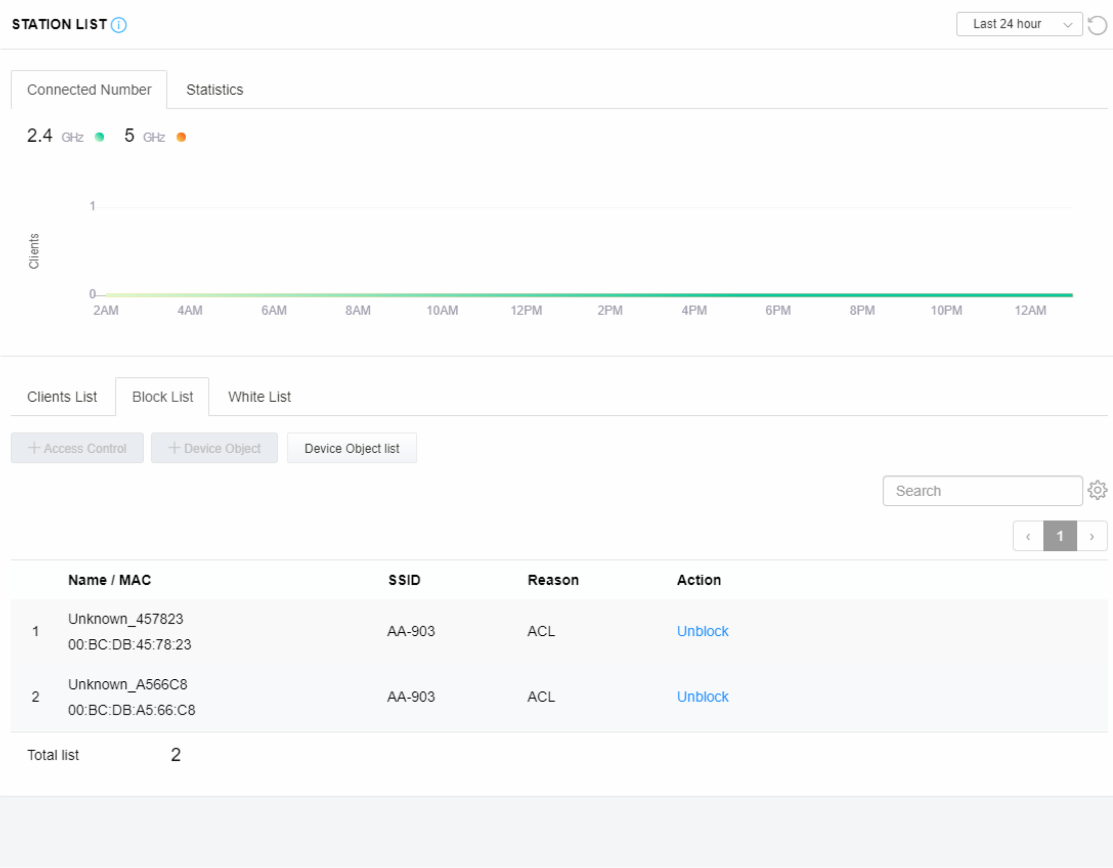
Available settings are explained as follows:

Item	Description
+Access Control	It is available after choosing one of the entries (clients) on Clients List.  Add Access Control Wireless LAN: 5GHz SSID Policy: 1 Black list AA-903; 2 Disable AA-903-2; 3 Disable AA-903-3; 4 Disable AA-903-4 From to list Device MAC / Name / Apply to SSID 00:BC:DA:07:B0:C1 / Unknown_07B0C1 / □ All □ 1 □ 2 □ 3 □ 4 00:BC:DA:C3:4F:0A / Unknown_C34F0A / □ All □ 1 □ 2 □ 3 □ 4 Total : 0/256 Close / Save changes **Wireless LAN** - Specify the bandwidth for the access control list. **SSID Policy** - Set the policy for each SSID as black list or white list 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 device object list, choose one of the entries (clients) on Clients List to enable the Device Object button. Click the button to open the following page.  Add Device to Device Object Device MAC: 00:BC:DA:F5:EB:B4 — Name: Unknown_F5EB34 Device MAC: 00:BC:DA:94:CC:07 — Name: Unknown_94CC07 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.  DEVICE OBJECT Device Object Profiles Profidx: 1 — MAC: 00:50:7F:F1:91:BC — Name: TEST_1 Profidx: 2 — MAC: 00:50:7F:00:92:BA — Name: TEST_2
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 block list or white list.

II-3-1-4 Block List

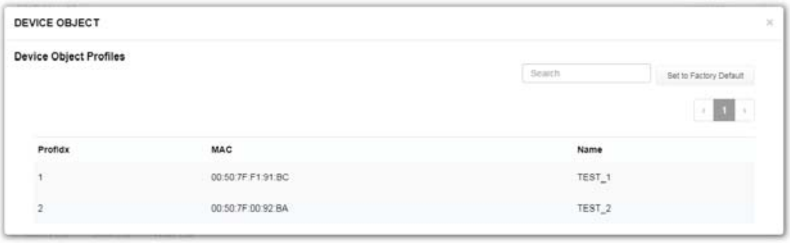
This page displays information of the stations under block list.



	Name / MAC	SSID	Reason	Action
1	Unknown_457823 00:BC:DB:45:78:23	AA-903	ACL	Unblock
2	Unknown_A566C8 00:BC:DB:A5:66:C8	AA-903	ACL	Unblock

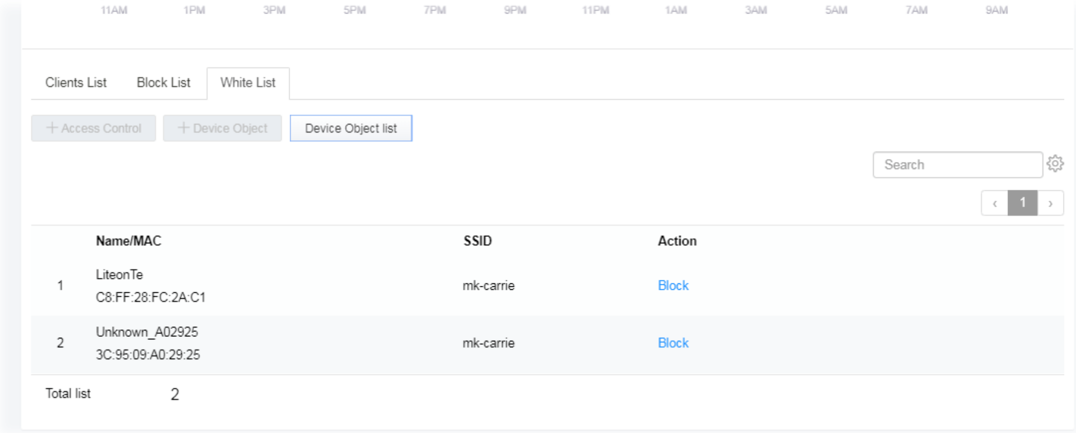
Total list 2

Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.  DEVICE OBJECT Device Object Profiles Search Set to Factory Default Profidx MAC Name 1 00:50:7F:F1:91:BC TEST_1 2 00:50:7F:00:92:BA TEST_2
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

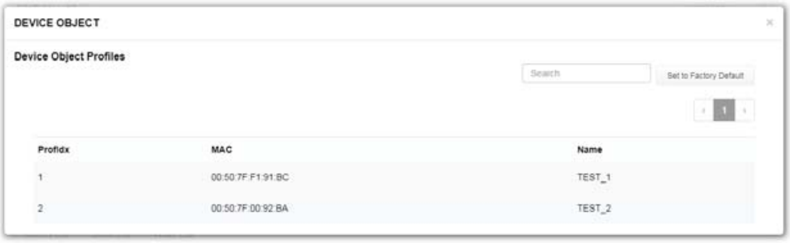
This page displays general information of the stations under white list.



	Name/MAC	SSID	Action
1	LiteonTe C8:FF:28:FC:2A:C1	mk-carrie	Block
2	Unknown_A02925 3C:95:09:A0:29:25	mk-carrie	Block

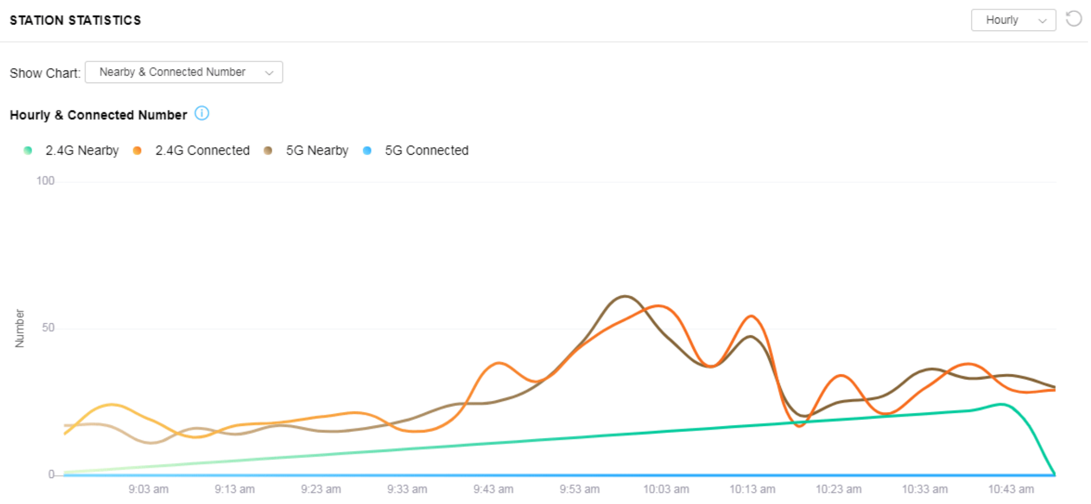
Total list 2

Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.  DEVICE OBJECT Device Object Profiles Search · Set to Factory Default Profidx · MAC · Name 1 · 00:50:7F:F1:91:BC · TEST_1 2 · 00:50:7F:00:92:BA · TEST_2
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 debug or for the user to observe network traffic and network quality.



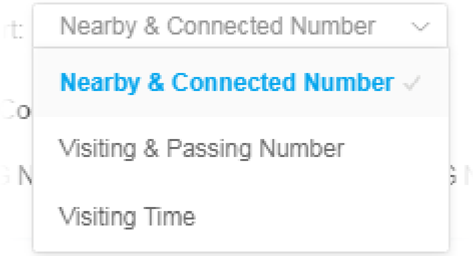
STATION STATISTICS

Hourly

Show Chart: Nearby & Connected Number

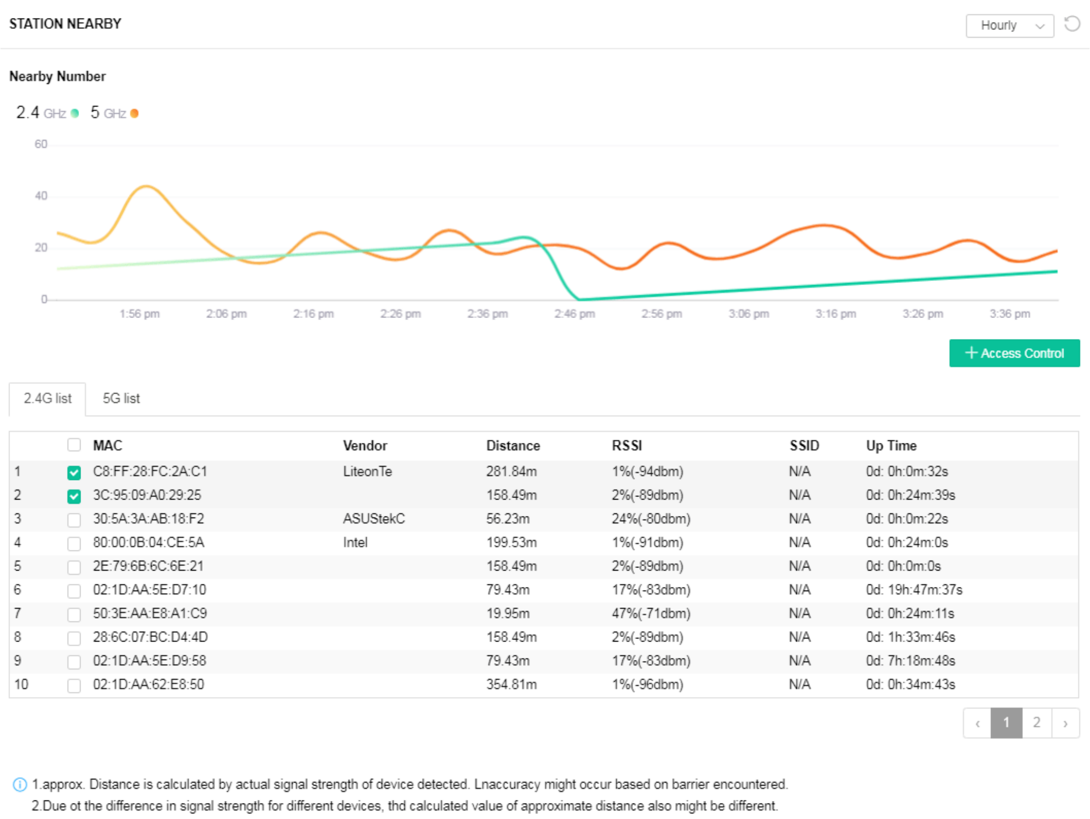
Hourly & Connected Number

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 Nearby & Connected Number ✓ Visiting & Passing Number Visiting Time **Nearby & Connected Number** – Choose it to have the statistics of the wireless stations which is nearby and connected to VigorAP 802. **Visiting & Passing Number** – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP 802. **Visiting Time** - Choose it to have the statistics of the wireless stations which is visiting VigorAP 802.

III-3-3 Station Nearby

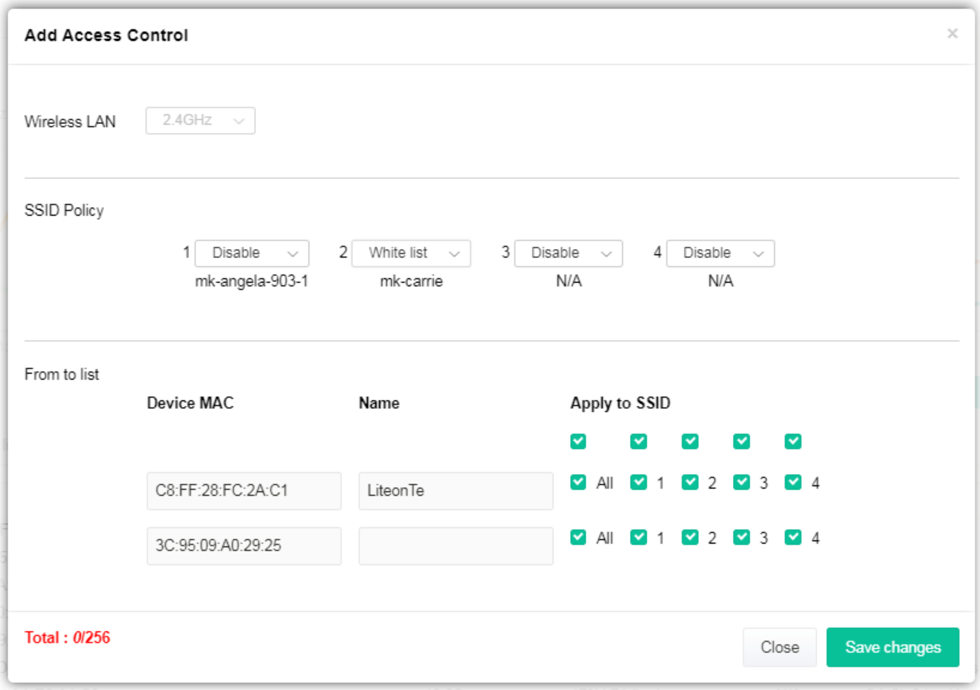
This page displays the general information for the nearby stations.



	□	MAC	Vendor	Distance	RSSI	SSID	Up Time
1	☑	C8:FF:28:FC:2A:C1	LiteonTe	281.84m	1%(-94dbm)	N/A	0d: 0h:0m:32s
2	☑	3C:95:09:A0:29:25		158.49m	2%(-89dbm)	N/A	0d: 0h:24m:39s
3	□	30:5A:3A:AB:18:F2	ASUStekC	56.23m	24%(-80dbm)	N/A	0d: 0h:0m:22s
4	□	80:00:0B:04:CE:5A	Intel	199.53m	1%(-91dbm)	N/A	0d: 0h:24m:0s
5	□	2E:79:6B:6C:6E:21		158.49m	2%(-89dbm)	N/A	0d: 0h:0m:0s
6	□	02:1D:AA:5E:D7:10		79.43m	17%(-83dbm)	N/A	0d: 19h:47m:37s
7	□	50:3E:AA:E8:A1:C9		19.95m	47%(-71dbm)	N/A	0d: 0h:24m:11s
8	□	28:6C:07:BC:D4:4D		158.49m	2%(-89dbm)	N/A	0d: 1h:33m:46s
9	□	02:1D:AA:5E:D9:58		79.43m	17%(-83dbm)	N/A	0d: 7h:18m:48s
10	□	02:1D:AA:62:E8:50		354.81m	1%(-96dbm)	N/A	0d: 0h:34m:43s

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

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



Wireless LAN: 2.4GHz

SSID Policy

1	2	3	4
Disable	White list	Disable	Disable
mk-angela-903-1	mk-carrie	N/A	N/A

From to list

Device MAC	Name	Apply to SSID
		☑ ☑ ☑ ☑ ☑
C8:FF:28:FC:2A:C1	LiteonTe	☑ All ☑ 1 ☑ 2 ☑ 3 ☑ 4
3C:95:09:A0:29:25		☑ All ☑ 1 ☑ 2 ☑ 3 ☑ 4

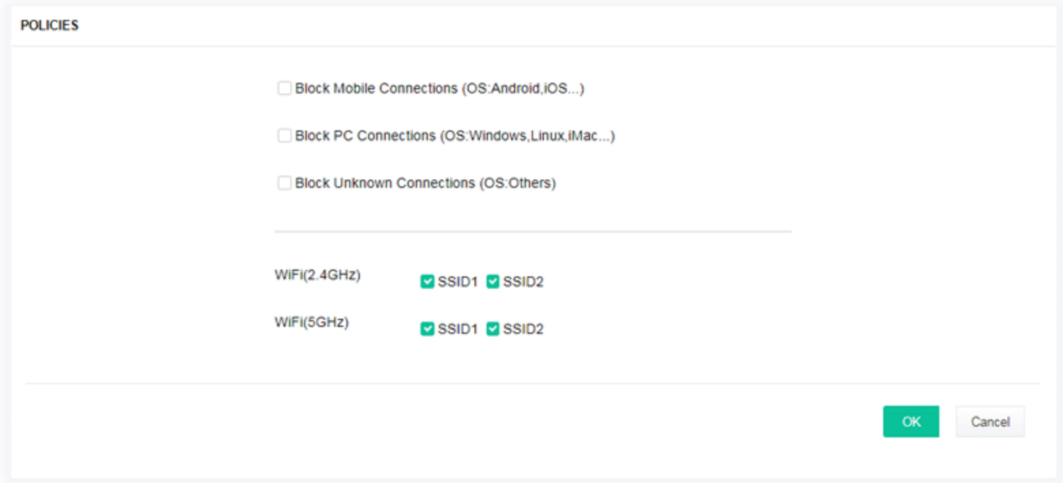
Total : 0/256

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

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



POLICIES

□ Block Mobile Connections (OS:Android,iOS...)

□ Block PC Connections (OS:Windows,Linux,iMac...)

□ Block Unknown Connections (OS:Others)

WiFi(2.4GHz) ☑ SSID1 ☑ SSID2

WiFi(5GHz) ☑ SSID1 ☑ SSID2

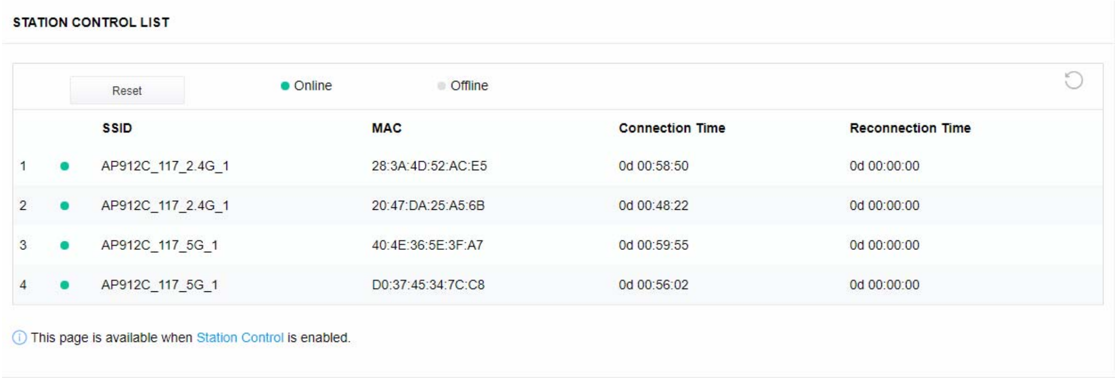
Each item is explained as follows:

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

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

III-3-5 Station Control List

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



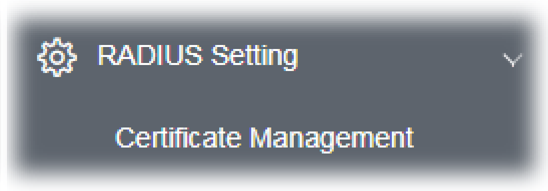
STATION CONTROL LIST

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

ⓘ This page is available when Station Control is enabled.

Chapter IV Others

IV-1 RADIUS Setting

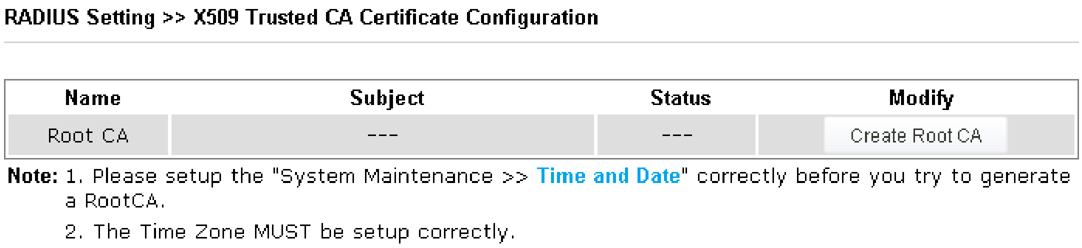


IV-1-1 Certificate Management

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

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

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



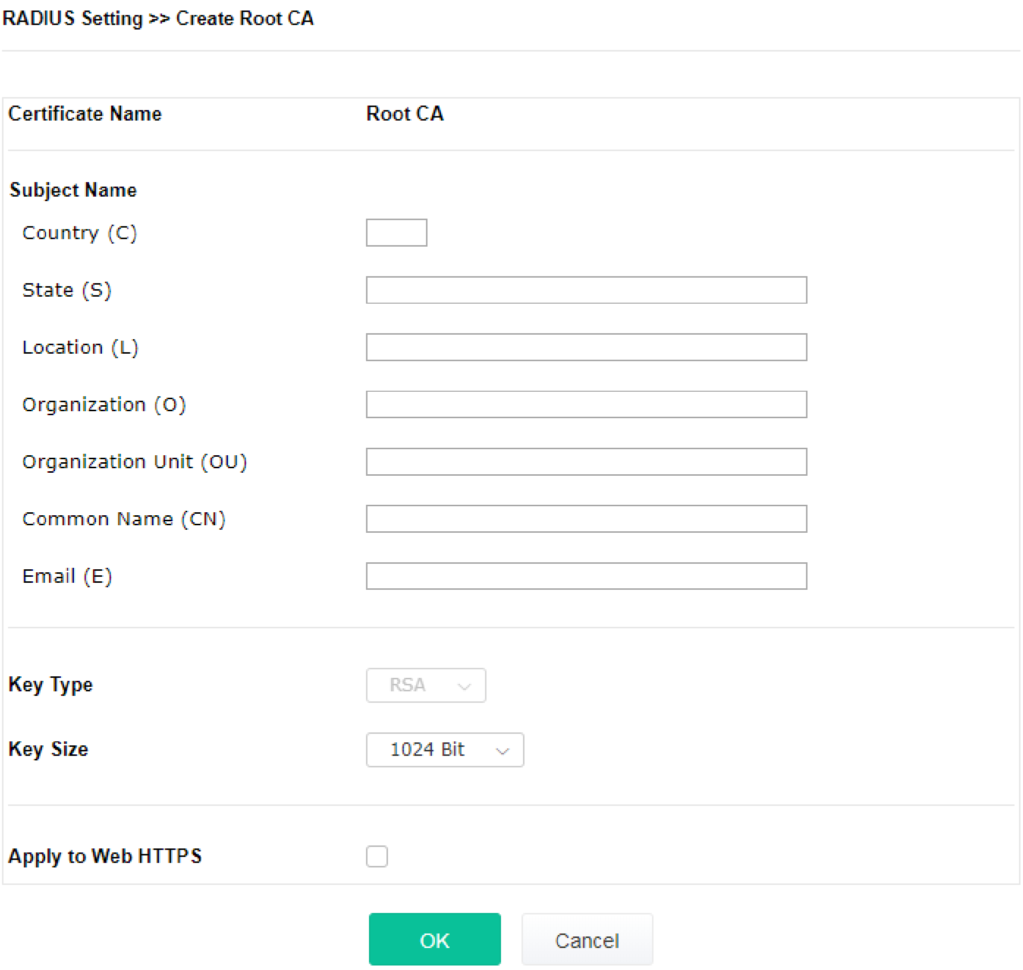
RADIUS Setting >> X509 Trusted CA Certificate Configuration

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

Note: 1. Please setup the "System Maintenance >> Time and Date" correctly before you try to generate a RootCA.

2. The Time Zone MUST be setup correctly.

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



RADIUS Setting >> Create Root CA

Certificate Name	Root CA
Subject Name	
Country (C)	
State (S)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Key Type	RSA
Key Size	1024 Bit
Apply to Web HTTPS	□

Available settings are explained as follows:

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

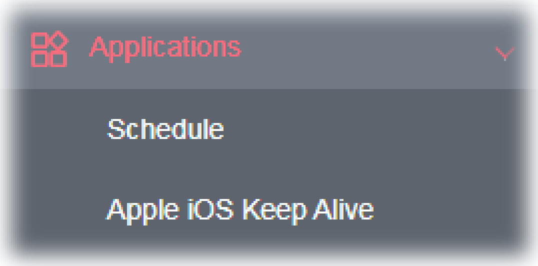
ⓘ **Note:**

“Common Name” must be configured with rotuer’s WAN IP or domain name.

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

IV-2 Applications

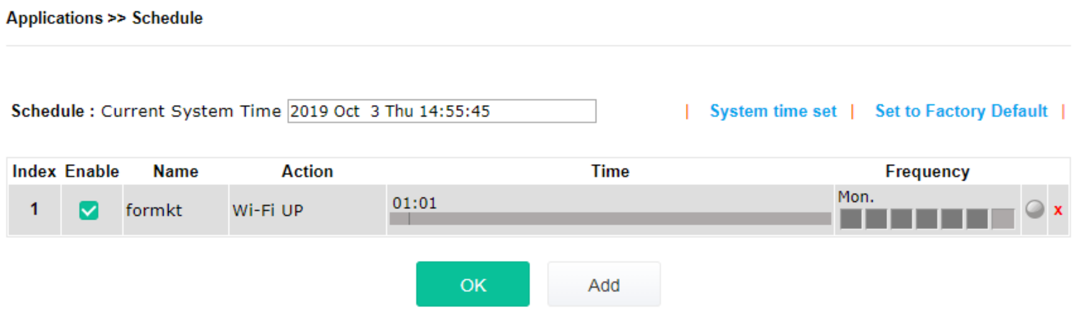
Below shows the menu items for Applications.



IV-2-1 Schedule

The VigorAP has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the AP to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the VigorAP's clock to current time of your PC. The clock will reset once if you power down or reset the AP. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the AP's clock. This method can only be applied when the WAN connection has been built up.


Applications >> Schedule

Schedule : Current System Time 2019 Oct 3 Thu 14:55:45 | System time set | Set to Factory Default |

Index	Enable	Name	Action	Time	Frequency
1	☑	formkt	Wi-Fi UP	01:01	Mon.

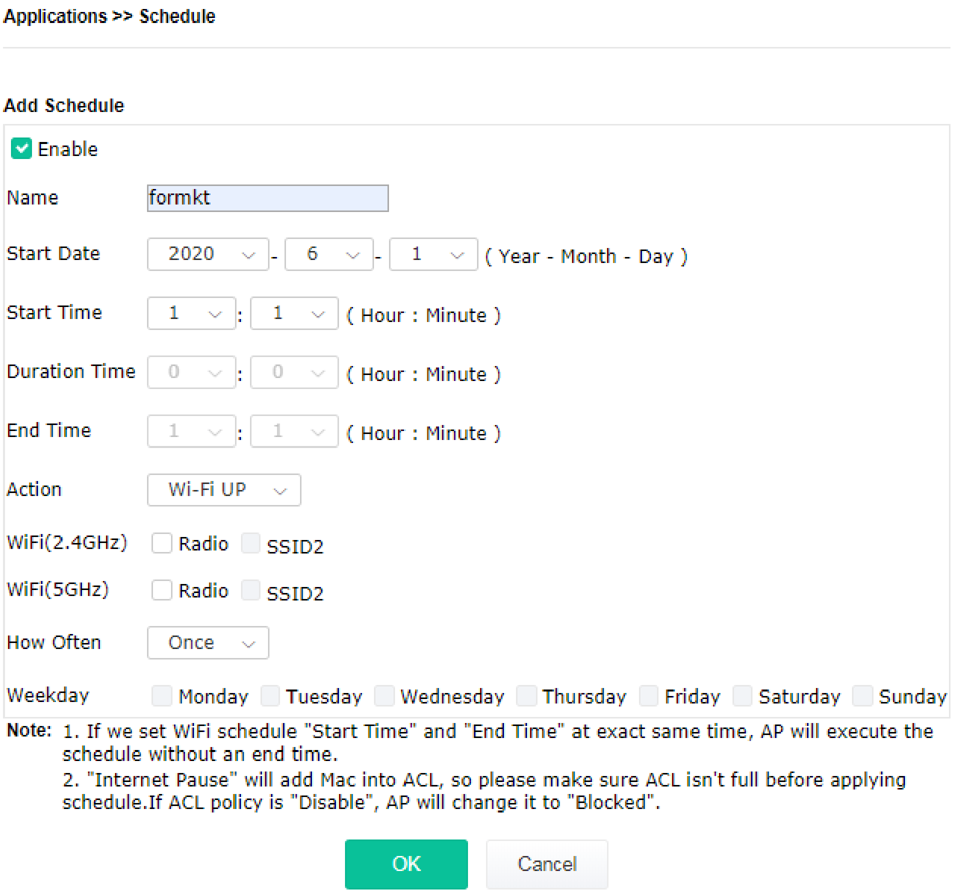
Available settings are explained as follows:

Item	Description
Schedule: Current System Time	Display current system time.
System time set	Click it to open **System Maintenance>>Time and Date** to configure time setting.
Set to Factory Default	Click it to restore the factory default settings for the schedule profile.
Index	Display the sort number of the schedule profile.
Enable	Display if the profile is enabled (V) or not (X).
Name	Display the name of the schedule profile.

Action	Display the action adopted by the schedule profile.
Time	Display the time duration.
Frequency	Display the day(s) selected for the schedule profile.
x	Click the icon to remove the profile.
OK	Save the settings.
Add	Create a new schedule profile.

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

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



Applications >> Schedule

Add Schedule

☑ Enable

Name: formkt

Start Date: 2020 - 6 - 1 (Year - Month - Day)

Start Time: 1 : 1 (Hour : Minute)

Duration Time: 0 : 0 (Hour : Minute)

End Time: 1 : 1 (Hour : Minute)

Action: Wi-Fi UP

WiFi(2.4GHz): □ Radio □ SSID2

WiFi(5GHz): □ Radio □ SSID2

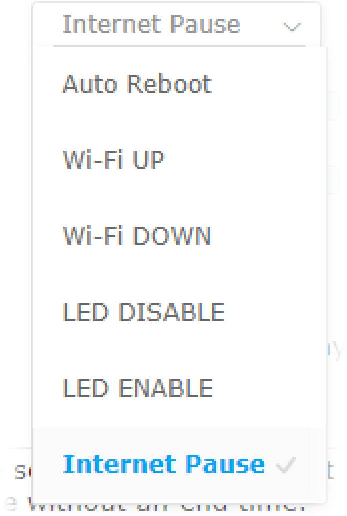
How Often: Once

Weekday: □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

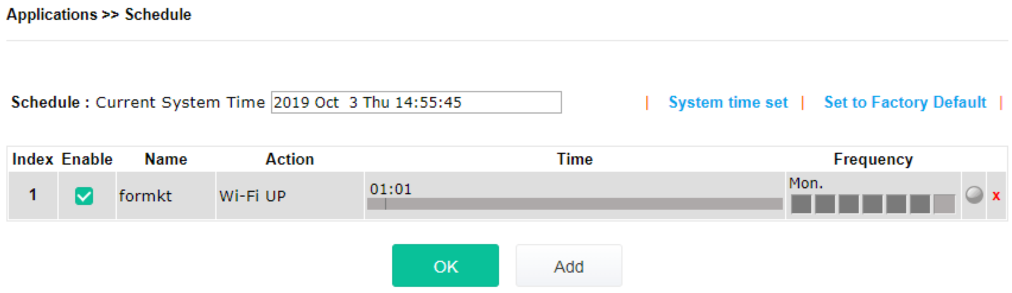
Note: 1. If we set WiFi schedule "Start Time" and "End Time" at exact same time, AP will execute the schedule without an end time.
2. "Internet Pause" will add Mac into ACL, so please make sure ACL isn't full before applying schedule.If ACL policy is "Disable", AP will change it to "Blocked".

Available settings are explained as follows:

Item	Description
Enable	Check to enable such schedule profile.
Name	Enter the name of the 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 when **Wi-Fi UP** or **Wi-Fi DOWN** is selected as **Action.**
End Time	Specify the ending time of the schedule.
Action	Specify which action should apply the schedule.

	 Internet Pause Auto Reboot Wi-Fi UP Wi-Fi DOWN LED DISABLE LED ENABLE Internet Pause 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 box to setup the network based on the schedule profile. **Note**: When Radio is selected, SSID2 is not available for choosing, vice versa. Moreover, SSID2 is not available for choosing if it is not enabled.
How Often	Specify how often the schedule will be applied. **Once -**The schedule will be applied just once **Weekdays -**Specify which days in one week should perform the schedule.
Weekday	Choose and check the day to perform the schedule. It is available when **Weekdays** is selected as **How Often**.

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.



Applications >> Schedule

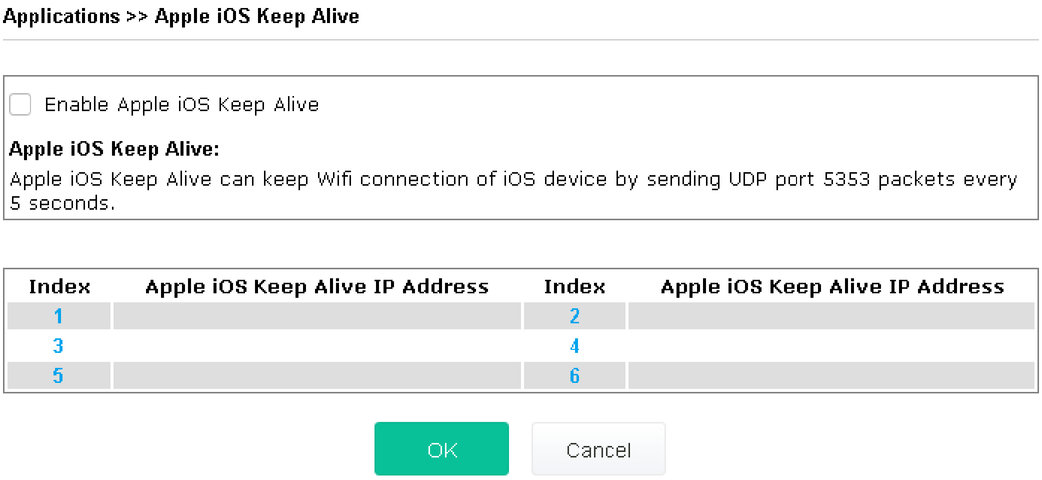
Schedule : Current System Time 2019 Oct 3 Thu 14:55:45 | System time set | Set to Factory Default |

Index	Enable	Name	Action	Time	Frequency		
1	☑	formkt	Wi-Fi UP	01:01	Mon.	○	x

OK Add

IV-2-2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 802 will send the UDP packets with 5353 port to the specific IP every five seconds.



Applications >> Apple iOS Keep Alive

□ Enable Apple iOS Keep Alive

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

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

Available settings are explained as follows:

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

Click **OK** to save the settings.

Chapter V Troubleshooting

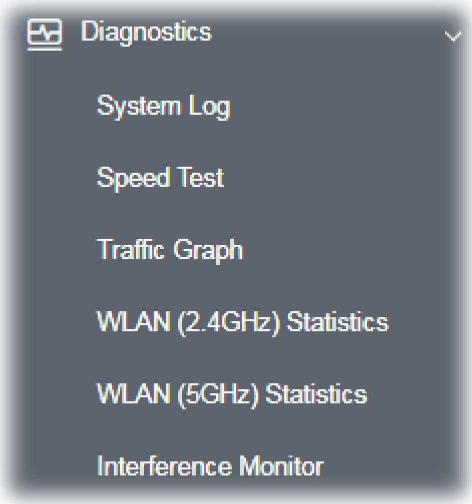
V-1 Diagnostics

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

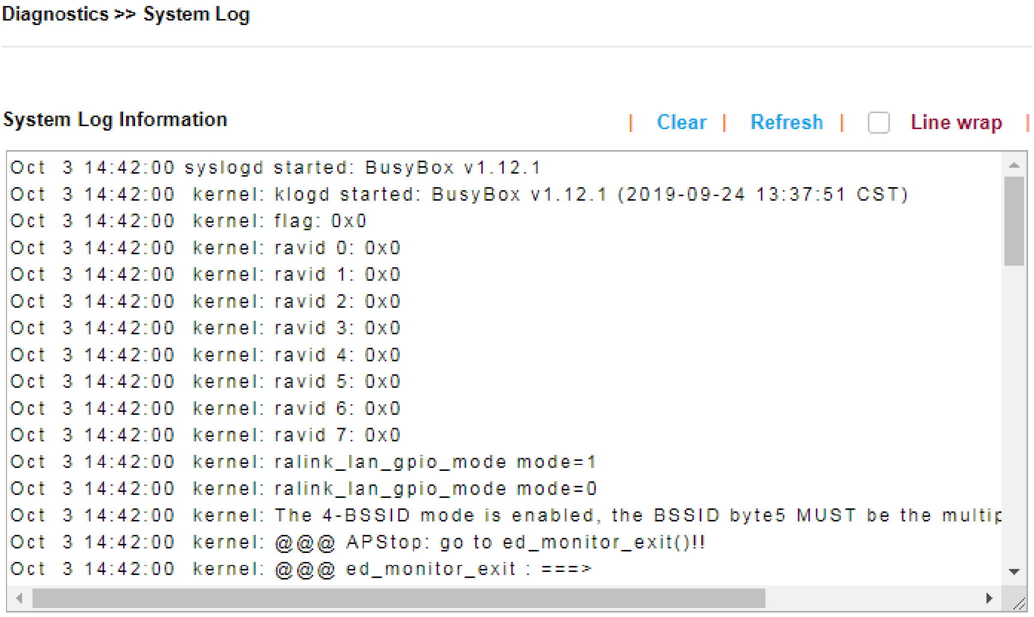
If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Diagnostic tools provide a useful way to **view** or **diagnose** the status of your VigorAP 802.



V-1-1 System Log

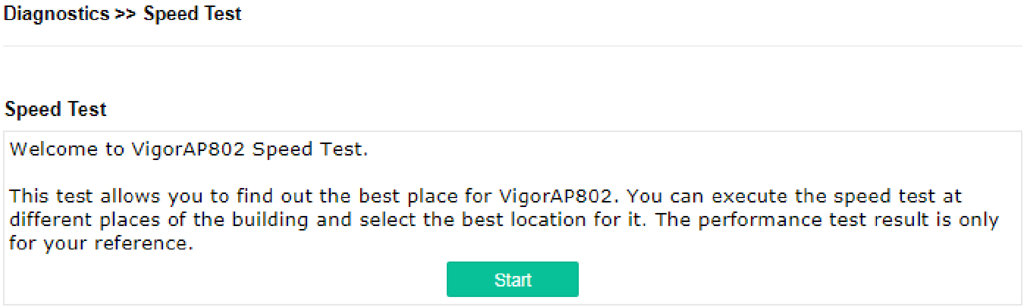
At present, only **System Log** is offered.



```
Oct  3 14:42:00 syslogd started: BusyBox v1.12.1
Oct  3 14:42:00  kernel: klogd started: BusyBox v1.12.1 (2019-09-24 13:37:51 CST)
Oct  3 14:42:00  kernel: flag: 0x0
Oct  3 14:42:00  kernel: ravid 0: 0x0
Oct  3 14:42:00  kernel: ravid 1: 0x0
Oct  3 14:42:00  kernel: ravid 2: 0x0
Oct  3 14:42:00  kernel: ravid 3: 0x0
Oct  3 14:42:00  kernel: ravid 4: 0x0
Oct  3 14:42:00  kernel: ravid 5: 0x0
Oct  3 14:42:00  kernel: ravid 6: 0x0
Oct  3 14:42:00  kernel: ravid 7: 0x0
Oct  3 14:42:00  kernel: ralink_lan_gpio_mode mode=1
Oct  3 14:42:00  kernel: ralink_lan_gpio_mode mode=0
Oct  3 14:42:00  kernel: The 4-BSSID mode is enabled, the BSSID byte5 MUST be the multip
Oct  3 14:42:00  kernel: @@@ APStop: go to ed_monitor_exit()!!
Oct  3 14:42:00  kernel: @@@ ed_monitor_exit : ===>
```

V-1-2 Speed Test

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

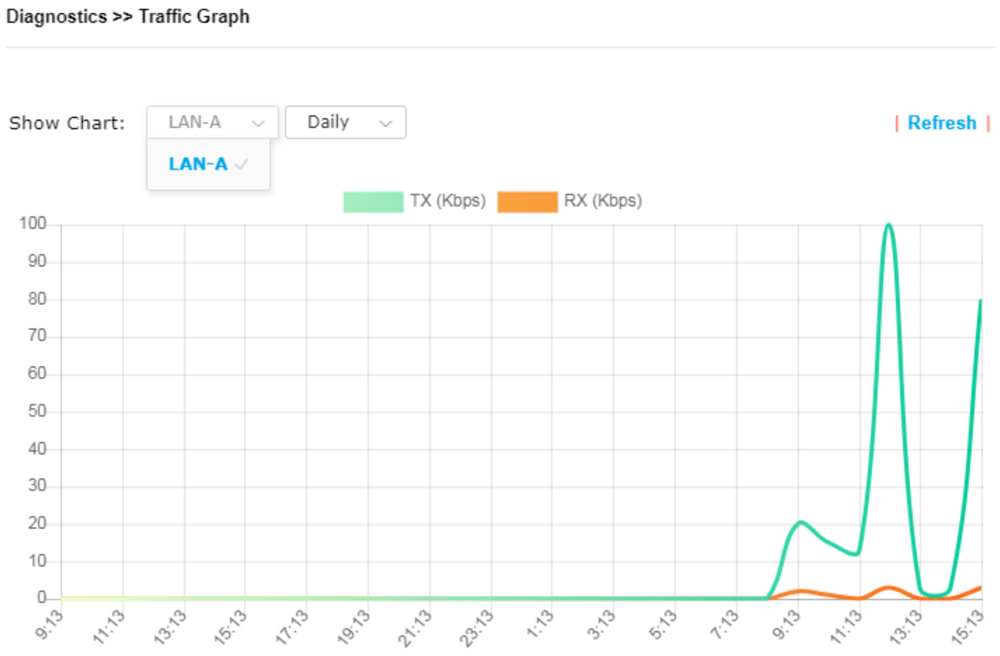


Welcome to VigorAP802 Speed Test.

This test allows you to find out the best place for VigorAP802. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference.

V-1-3 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.



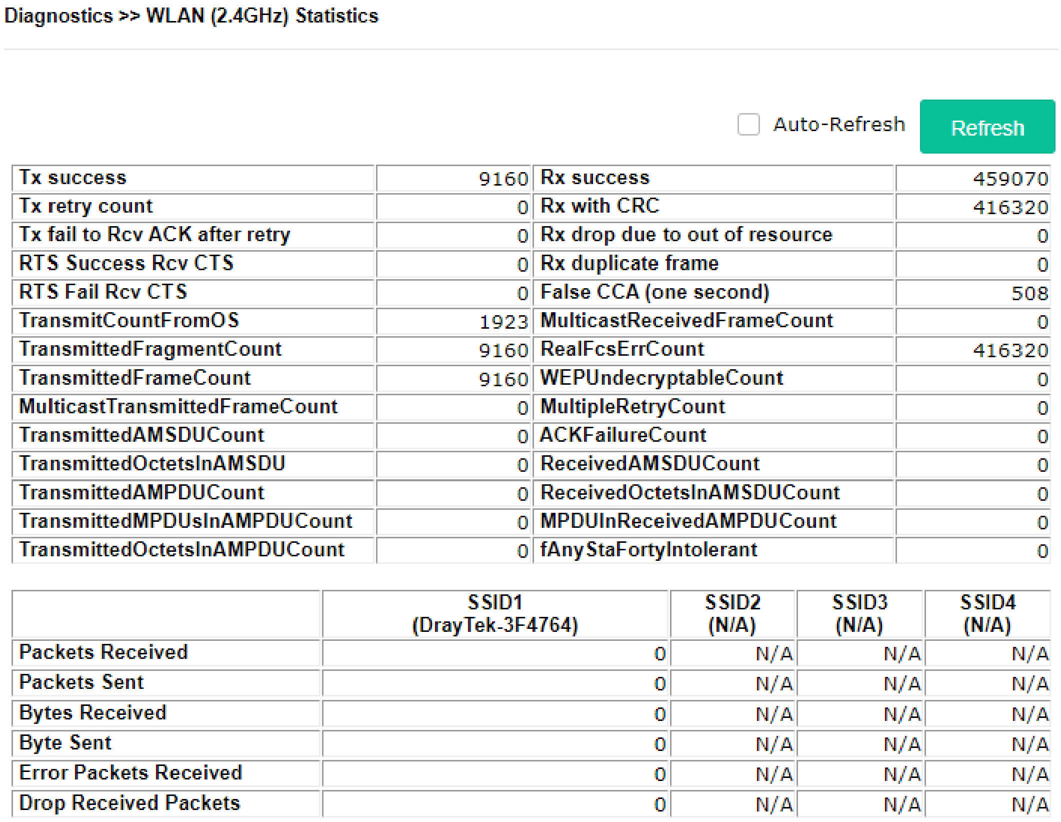
Diagnostics >> Traffic Graph

Show Chart: LAN-A Daily

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

V-1-4 WLAN (2.4GHz) Statistics

Such page is used for debug by RD only.



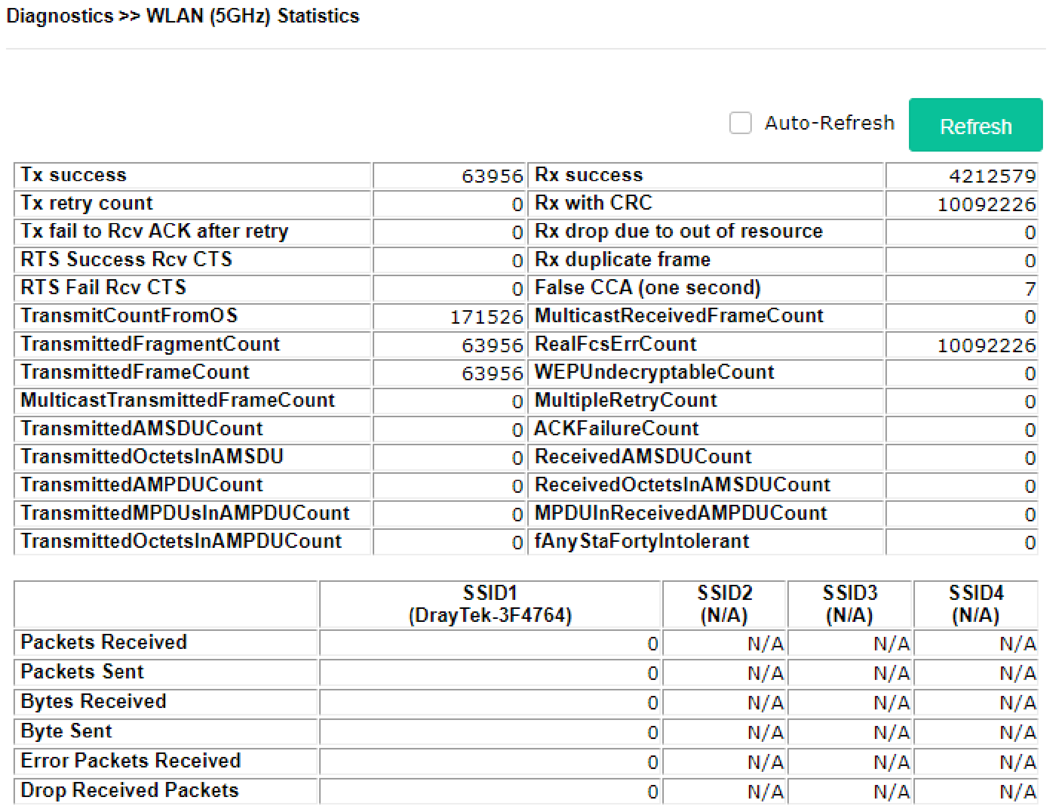
Diagnostics >> WLAN (2.4GHz) Statistics

Tx success	9160	Rx success	459070
Tx retry count	0	Rx with CRC	416320
Tx fail to Rcv ACK after retry	0	Rx drop due to out of resource	0
RTS Success Rcv CTS	0	Rx duplicate frame	0
RTS Fail Rcv CTS	0	False CCA (one second)	508
TransmitCountFromOS	1923	MulticastReceivedFrameCount	0
TransmittedFragmentCount	9160	RealFcsErrCount	416320
TransmittedFrameCount	9160	WEPUndecryptableCount	0
MulticastTransmittedFrameCount	0	MultipleRetryCount	0
TransmittedAMSDUCount	0	ACKFailureCount	0
TransmittedOctetsInAMSDU	0	ReceivedAMSDUCount	0
TransmittedAMPDUCount	0	ReceivedOctetsInAMSDUCount	0
TransmittedMPDUsInAMPDUCount	0	MPDUInReceivedAMPDUCount	0
TransmittedOctetsInAMPDUCount	0	fAnyStaFortyIntolerant	0

	SSID1 (DrayTek-3F4764)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Packets Received	0	N/A	N/A	N/A
Packets Sent	0	N/A	N/A	N/A
Bytes Received	0	N/A	N/A	N/A
Byte Sent	0	N/A	N/A	N/A
Error Packets Received	0	N/A	N/A	N/A
Drop Received Packets	0	N/A	N/A	N/A

V-1-5 WLAN (5GHz) Statistics

Such page is used for debug by RD only.



Diagnostics >> WLAN (5GHz) Statistics

Tx success	63956	Rx success	4212579
Tx retry count	0	Rx with CRC	10092226
Tx fail to Rcv ACK after retry	0	Rx drop due to out of resource	0
RTS Success Rcv CTS	0	Rx duplicate frame	0
RTS Fail Rcv CTS	0	False CCA (one second)	7
TransmitCountFromOS	171526	MulticastReceivedFrameCount	0
TransmittedFragmentCount	63956	RealFcsErrCount	10092226
TransmittedFrameCount	63956	WEPUndecryptableCount	0
MulticastTransmittedFrameCount	0	MultipleRetryCount	0
TransmittedAMSDUCount	0	ACKFailureCount	0
TransmittedOctetsInAMSDU	0	ReceivedAMSDUCount	0
TransmittedAMPDUCount	0	ReceivedOctetsInAMSDUCount	0
TransmittedMPDUsInAMPDUCount	0	MPDUInReceivedAMPDUCount	0
TransmittedOctetsInAMPDUCount	0	fAnyStaFortyIntolerant	0

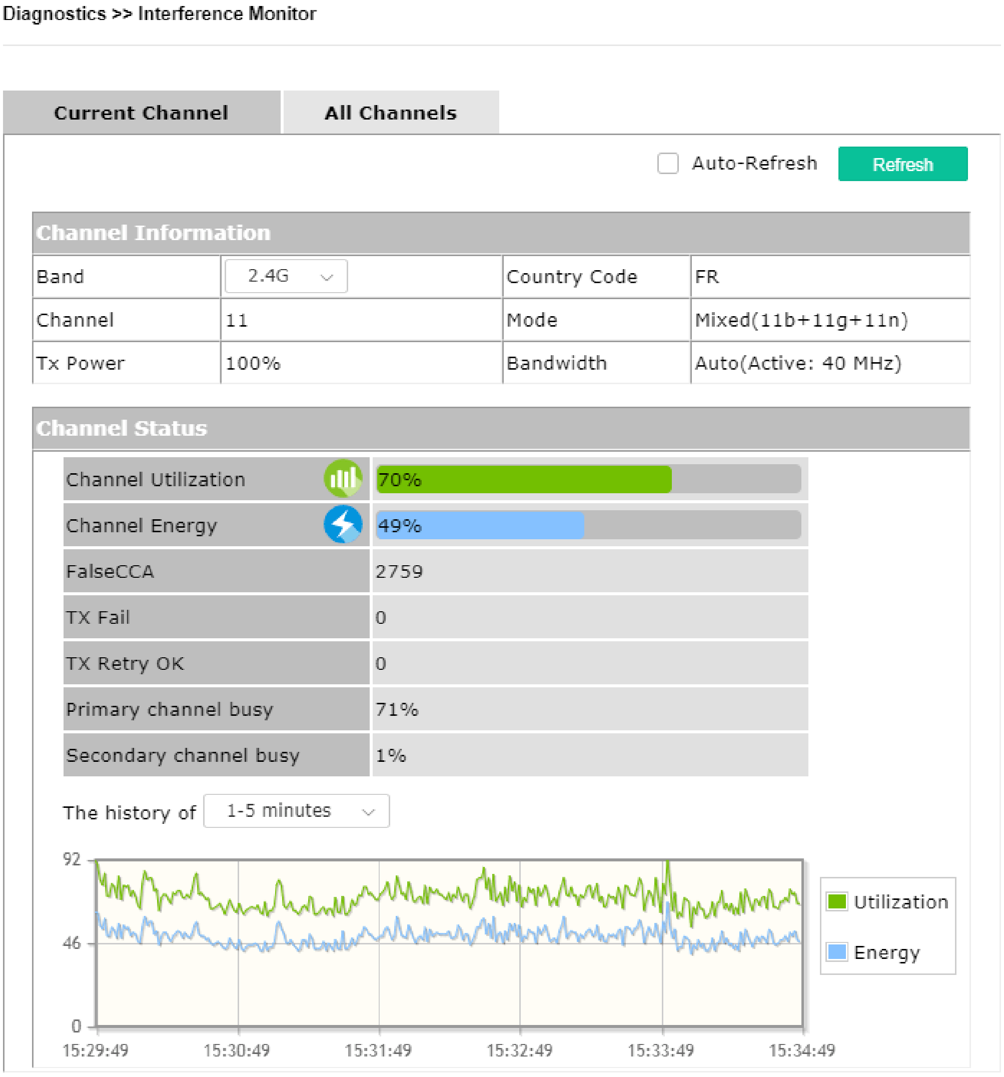
	SSID1 (DrayTek-3F4764)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Packets Received	0	N/A	N/A	N/A
Packets Sent	0	N/A	N/A	N/A
Bytes Received	0	N/A	N/A	N/A
Byte Sent	0	N/A	N/A	N/A
Error Packets Received	0	N/A	N/A	N/A
Drop Received Packets	0	N/A	N/A	N/A

V-1-6 Interference Monitor

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

Current Channel

The analysis page with information about wireless band, channel, transmission power, bandwidth, wireless mode, and country code chosen will be displayed on this page completely based on the wireless band (2.4G or 5G) selected. Also, channel status can be seen easily from this page.



Diagnostics >> Interference Monitor

Channel Information

Band	2.4G	Country Code	FR
Channel	11	Mode	Mixed(11b+11g+11n)
Tx Power	100%	Bandwidth	Auto(Active: 40 MHz)

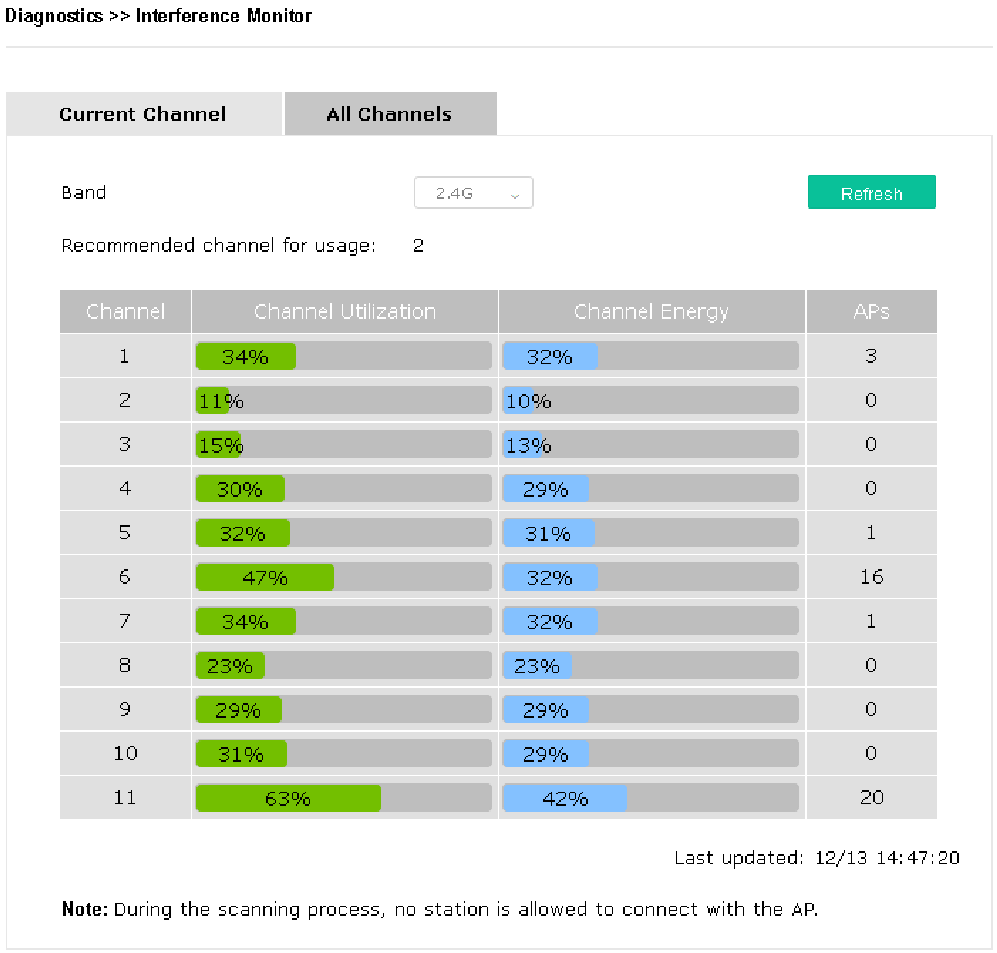
Channel Status

Channel Utilization	70%
Channel Energy	49%
FalseCCA	2759
TX Fail	0
TX Retry OK	0
Primary channel busy	71%
Secondary channel busy	1%

The history of 1-5 minutes

All Channels

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



Diagnostics >> Interference Monitor

Band 2.4G

Recommended channel for usage: 2

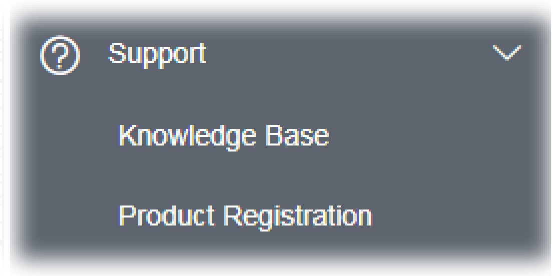
Channel	Channel Utilization	Channel Energy	APs
1	34%	32%	3
2	11%	10%	0
3	15%	13%	0
4	30%	29%	0
5	32%	31%	1
6	47%	32%	16
7	34%	32%	1
8	23%	23%	0
9	29%	29%	0
10	31%	29%	0
11	63%	42%	20

Last updated: 12/13 14:47:20

Note: During the scanning process, no station is allowed to connect with the AP.

V-1-7 Support Area

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



V-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.

V-3 Checking the Network Connection Settings

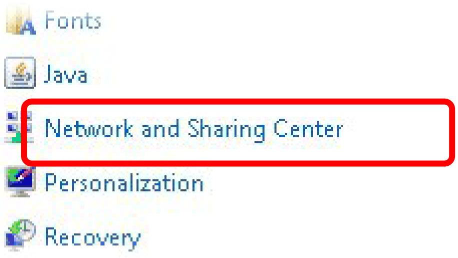
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

V-3-1 For Windows

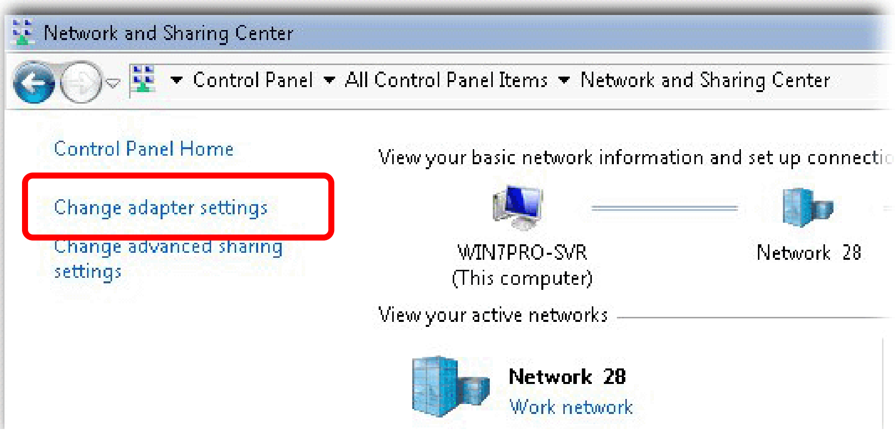
Note:

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

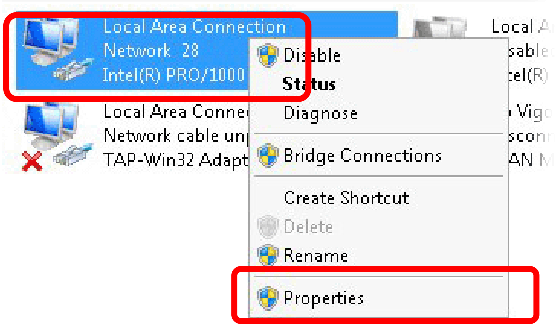
1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**



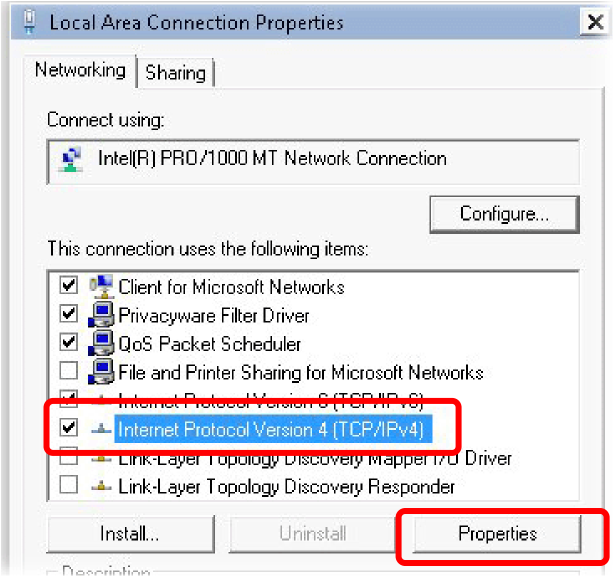
2. In the following window, click **Change adapter settings**.


Network and Sharing Center
Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connecti
WIN7PRO-SVR
(This computer)
Network 28
View your active networks
Network 28
Work network

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



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



Local Area Connection Properties

Networking | Sharing

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

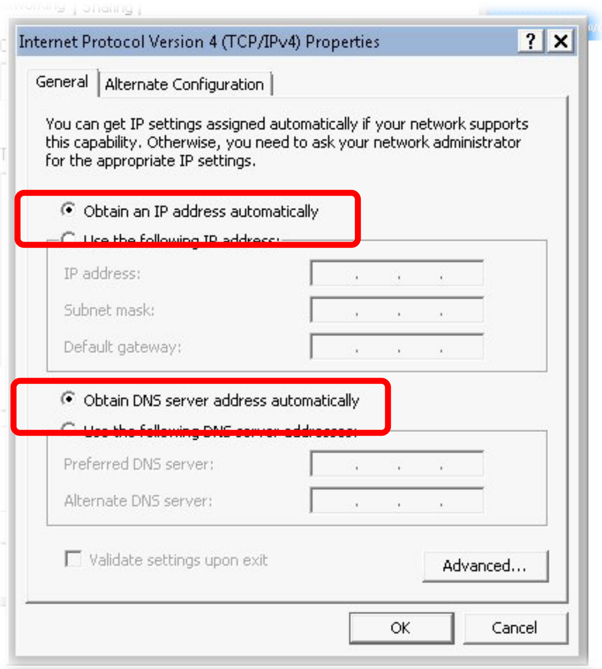
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Privacyware Filter Driver
- ☑ QoS Packet Scheduler
- □ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Link-Layer Topology Discovery Mapper I/O Driver
- □ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

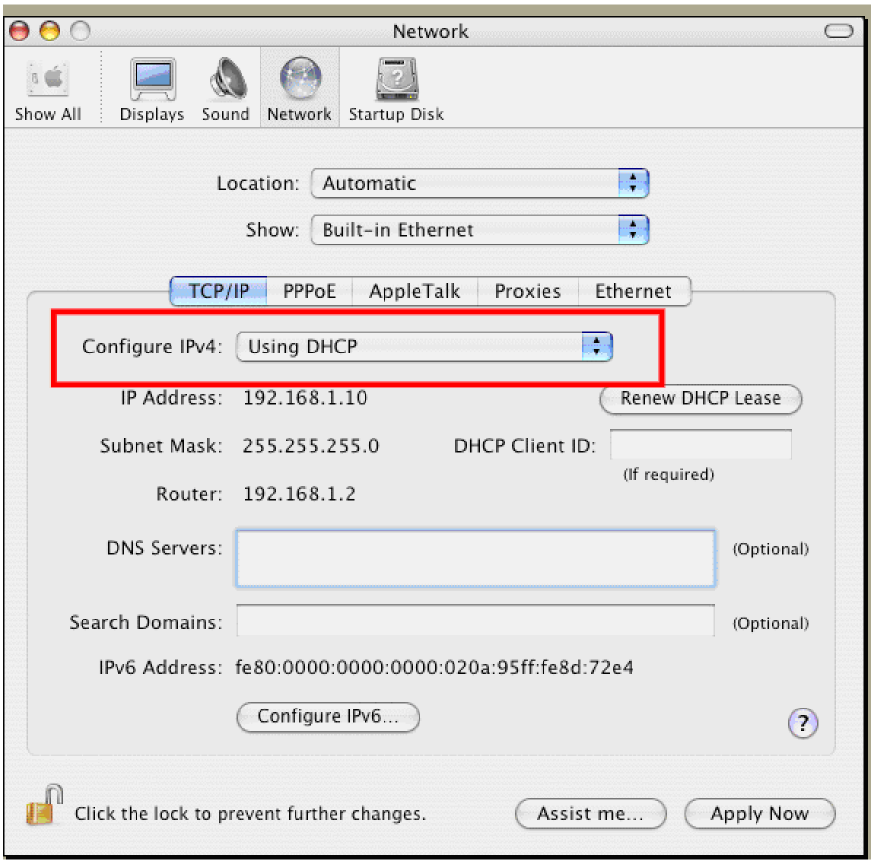
□ Validate settings upon exit

Advanced...

OK | Cancel

V-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.



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.2

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

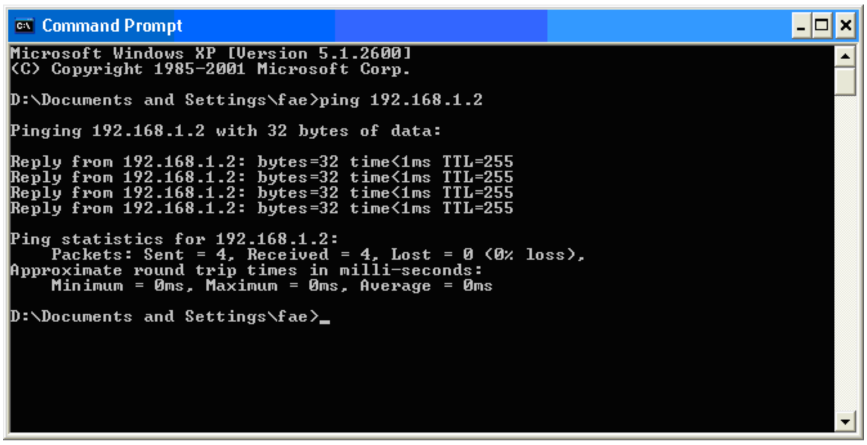
V-4 Pinging the Device

The default gateway IP address of the modem is 192.168.1.2. For some reason, you might need to use “ping” command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.2.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section V-2)

Please follow the steps below to ping the modem correctly.

V-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.

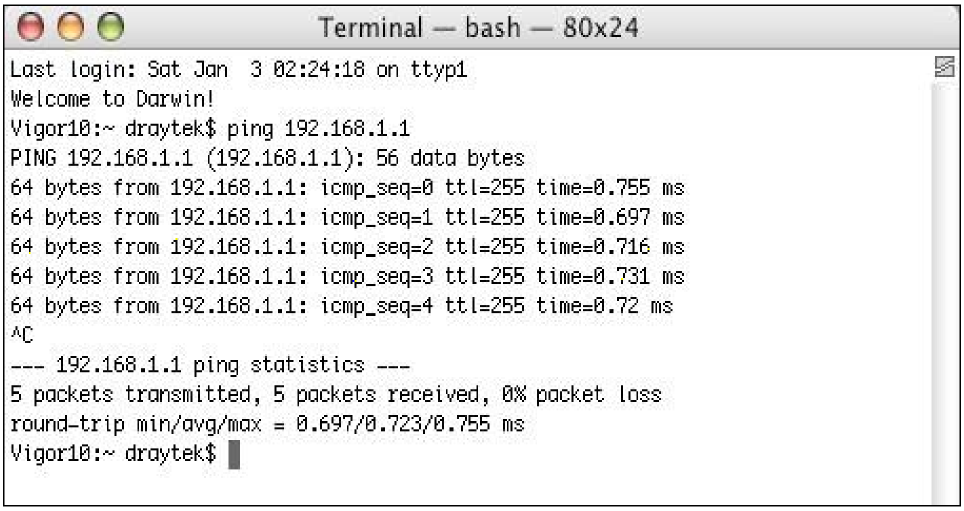


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.2 and press [Enter]. If the link is OK, the line of **“Reply from 192.168.1.2:bytes=32 time<1ms TTL=255”** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

V-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.



```
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$ 
```

V-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.

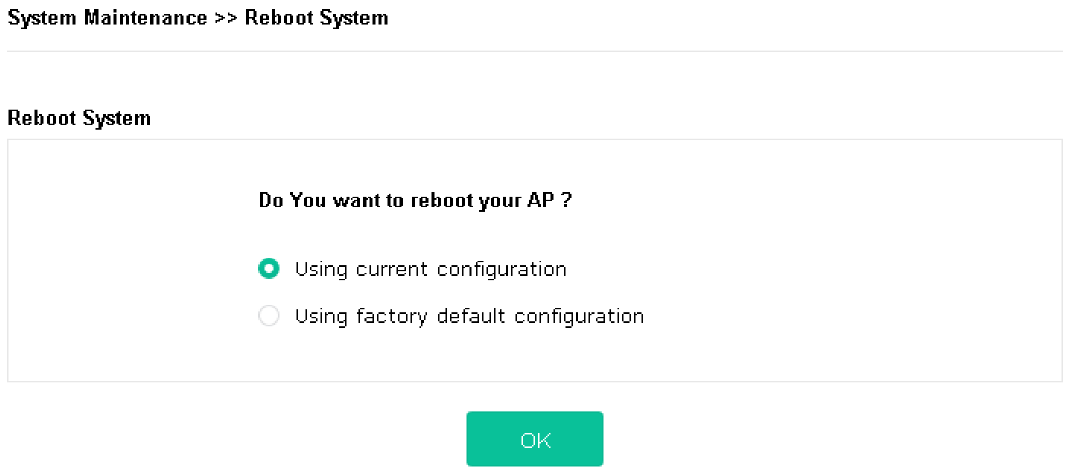
Warning:

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

V-5-1 Software Reset

You can reset the modem to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the modem will return all the settings to the factory settings.



System Maintenance >> Reboot System

Reboot System

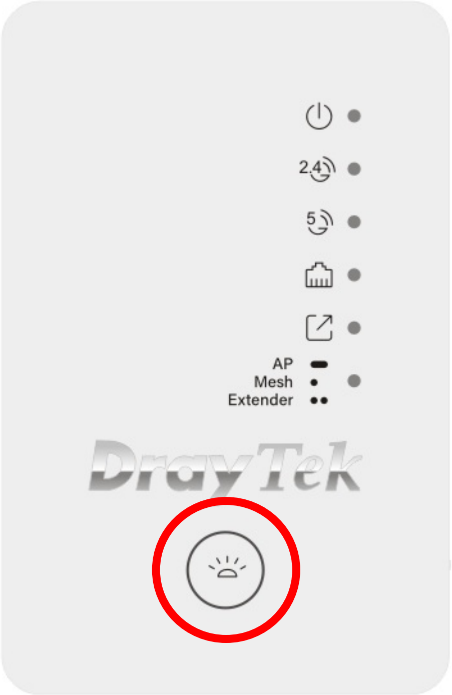
Do You want to reboot your AP ?

● Using current configuration

○ Using factory default configuration

V-5-2 Hardware Reset

Press the button for more than 15 seconds. When the ACT LED flashes rapidly, release the button. Then, the device will restart with the default configuration.



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

V-6 Contacting DrayTek

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

Index