

# DrayTek

## VigorAP 802

11ac Dual-band Wall Plug AP



### USER'S GUIDE

V1.0

# **VigorAP 802**

---

802.11ac Access Point

User's Guide

Version: 1.0

Firmware Version: V1.3.1.1

Date: October 1, 2019

# Intellectual Property Rights (IPR) Information

---

## Copyrights

© All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

## Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista, 7 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

# Safety Instructions and Approval

---

## Safety Instructions

- 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 to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

## Be a Registered Owner

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

## Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents. <http://www.draytek.com>



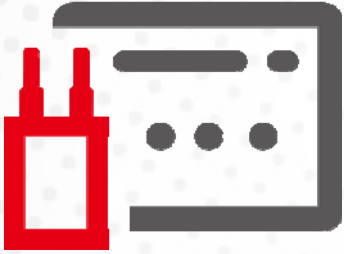
# Table of Contents

---

<b>Chapter I Installation .....</b>	<b>VII</b>
I-1 Introduction .....	1
I-1-1 LED Indicators and Connectors .....	3
I-2 Hardware Installation .....	5
I-3 Network IP Configuration .....	6
I-3-1 Windows 7 IP Address Setup .....	6
I-4 Accessing to Web User Interface .....	8
I-5 Changing Password .....	11
I-6 Dashboard .....	12
I-7 Quick Start Wizard .....	13
I-7-1 Settings for Access Point .....	14
I-7-2 Settings for Mesh Node .....	17
I-7-3 Settings for Range Extender .....	18
<b>Chapter II Connectivity .....</b>	<b>23</b>
II-1 Operation Mode .....	24
II-2 General Concepts for Wireless LAN (2.4GHz/5GHz) .....	26
II-3 Wireless LAN (2.4GHz/5GHz) Settings for AP Mode .....	29
II-3-1 General Setup .....	30
II-3-2 Security .....	32
II-3-3 Access Control .....	35
II-3-4 WPS .....	36
II-3-5 Advanced Setting .....	37
II-3-6 AP Discovery .....	40
II-3-7 WDS AP Status .....	41
II-3-8 Bandwidth Management .....	41
II-3-9 Airtime Fairness .....	42
II-3-10 Station Control .....	44
II-3-11 Roaming .....	46
II-3-12 Band Steering (for Wireless LAN (2.4GHz)) .....	48
II-3-13 Station List .....	53
II-4 Mesh Settings for Mesh Node Mode .....	55
II-4-1 Mesh Setup .....	57
II-4-2 Mesh Status .....	59
II-4-3 Mesh Discovery .....	59
II-4-4 Configuration Sync .....	60
II-5 Universal Repeater Settings for Range Extender Mode .....	63
II-6 LAN .....	67
II-6-1 General Setup .....	67
II-6-2 Port Control .....	69
<b>Chapter III Management .....</b>	<b>71</b>
III-1 System Maintenance .....	72
III-1-1 System Status .....	73
III-1-2 TR-069 .....	74
III-1-3 Administrator Password .....	76
III-1-4 User Password .....	77
III-1-5 Configuration Backup .....	78

III-1-6 Syslog/Mail Alert.....	80
III-1-7 Time and Date .....	81
III-1-8 SNMP.....	82
III-1-9 Management.....	83
III-1-10 Reboot System .....	85
III-1-11 Firmware Upgrade.....	86
III-2 Central AP Management.....	87
III-2-1 General Setup .....	87
III-2-2 APM Log.....	88
III-2-3 Overload Management .....	89
III-2-4 Status of Settings.....	90
III-3 Mobile Device Management .....	92
III-3-1 Detection .....	92
III-3-2 Policies .....	93
III-3-3 Statistics.....	94
<b>Chapter IV Others .....</b>	<b>95</b>
IV-1 RADIUS Setting.....	96
IV-1-1 Certificate Management .....	96
IV-2 Applications.....	99
IV-2-1 Schedule .....	99
IV-2-2 Apple iOS Keep Alive.....	101
<b>Chapter V Troubleshooting.....</b>	<b>103</b>
V-1 Diagnostics .....	104
V-1-1 System Log.....	105
V-1-2 DHCP Table List .....	105
V-1-3 Speed Test.....	106
V-1-4 Traffic Graph.....	106
V-1-5 Data Flow Monitor .....	107
V-1-6 WLAN (2.4GHz) Statistics.....	108
V-1-7 WLAN (5GHz) Statistics .....	109
V-1-8 Station Statistics .....	110
V-1-9 Interference Monitor .....	112
V-1-10 Station Airtime.....	114
V-1-11 Station Traffic Graph .....	115
V-1-12 Station Link Speed .....	116
V-1-13 Support Area .....	116
V-2 Checking the Hardware Status .....	117
V-3 Checking the Network Connection Settings .....	118
V-3-1 For Windows .....	118
V-3-2 For Mac Os .....	120
V-4 Pinging the Device .....	121
V-4-1 For Windows .....	121
V-4-2 For Mac Os (Terminal) .....	121
V-5 Backing to Factory Default Setting.....	123
V-5-1 Software Reset.....	123
V-5-2 Hardware Reset.....	124
V-6 Contacting DrayTek .....	125
Index .....	126

# Chapter I Installation







# I-1 Introduction

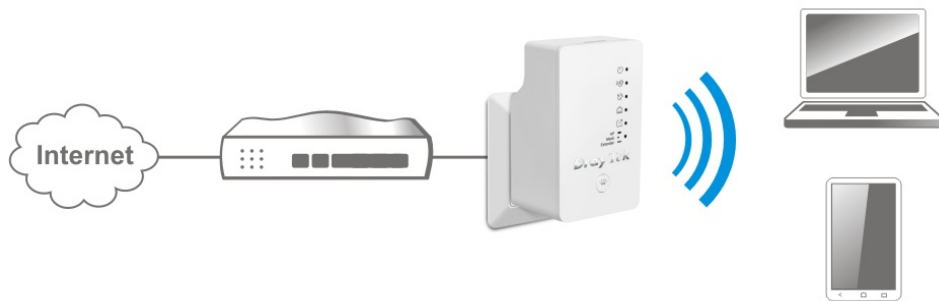
---

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.

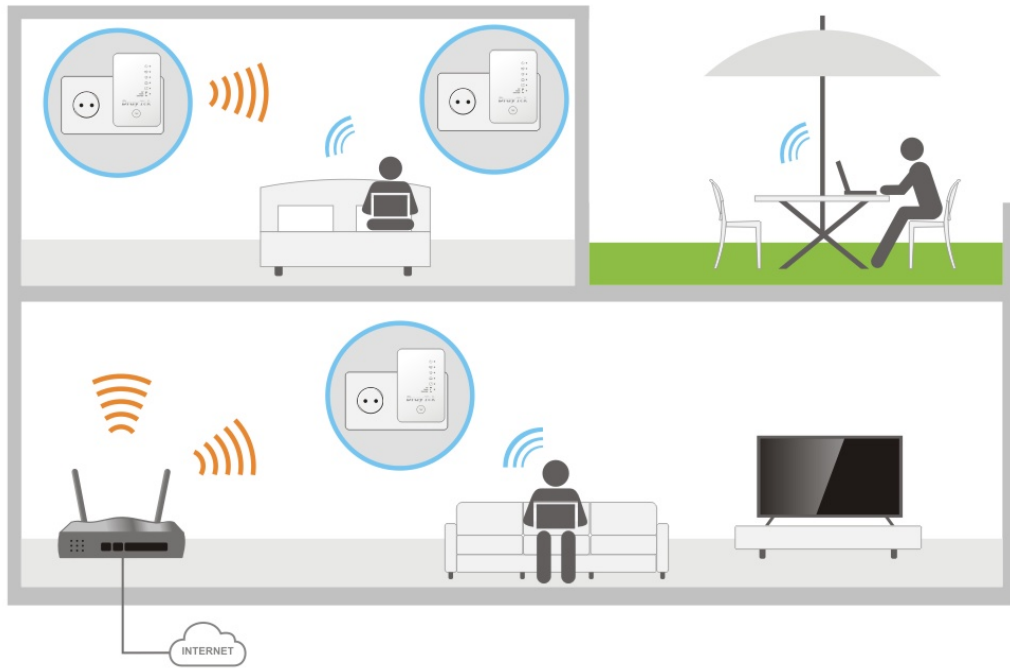
Without any cable, the plug design of VigorAP brings an easy hardware installation (by plugging to a wall outlet) for any computer users to set up a network environment in a very short time - within minutes, even inexperienced users.



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.



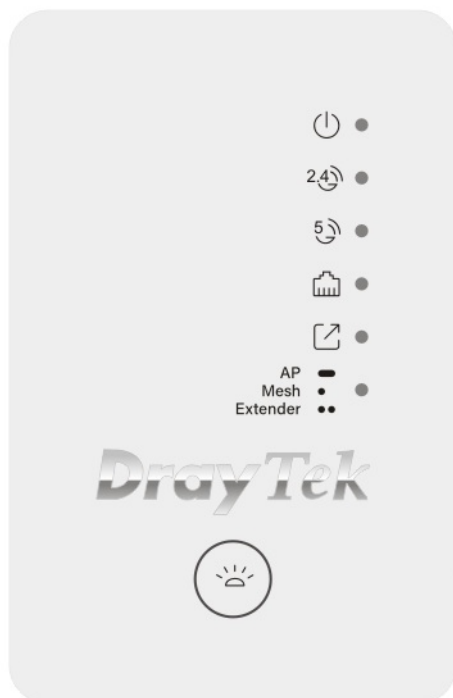
VigorAP supports AP, Mesh Node and Range Extender mode. In which, the Range Extender mode can extend the wireless coverage for wireless network.






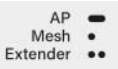



Follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

## 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 	On	Wireless function (2.4G) is ready.
	Off	Wireless function (2.4G) is not ready.
	Blinking	Data is transmitting (sending/receiving).
5G 	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 	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	Connector 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.

**i** Note:

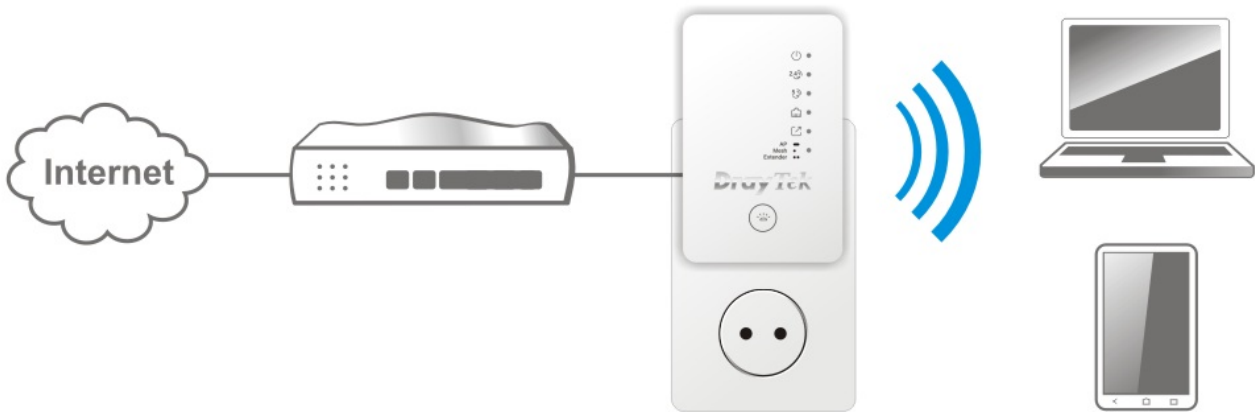
For the sake of security, make the accessory kit away from children.

## 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:

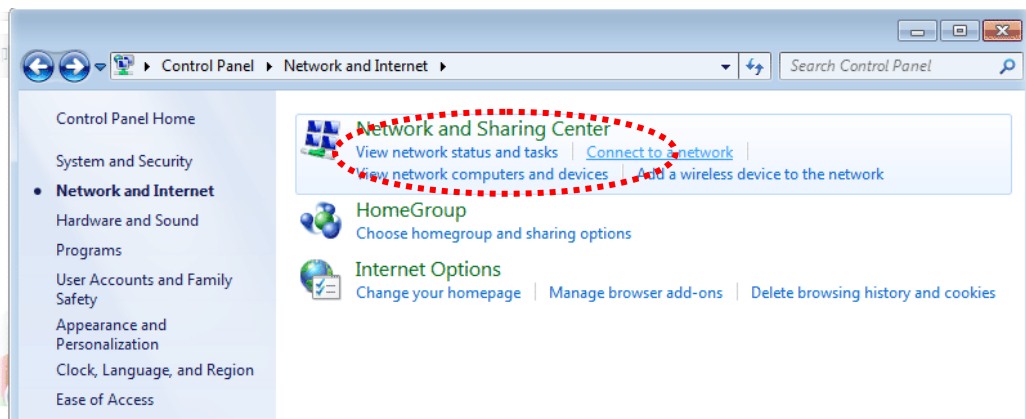
For the default IP address of this AP is set "192.168.1.2", we recommend you to use "192.168.1.X (except 2)" in the field of IP address on this section for your computer.

***If the operating system of your computer is...***

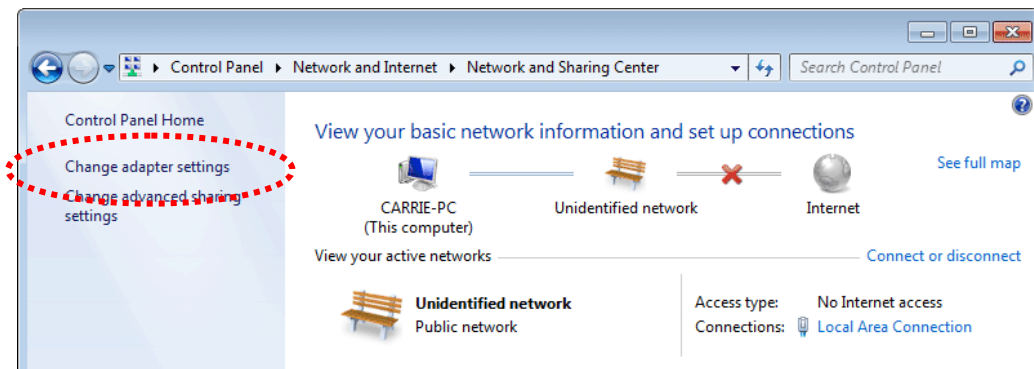
**Windows 7** - please go to section I-3-1

## I-3-1 Windows 7 IP Address Setup

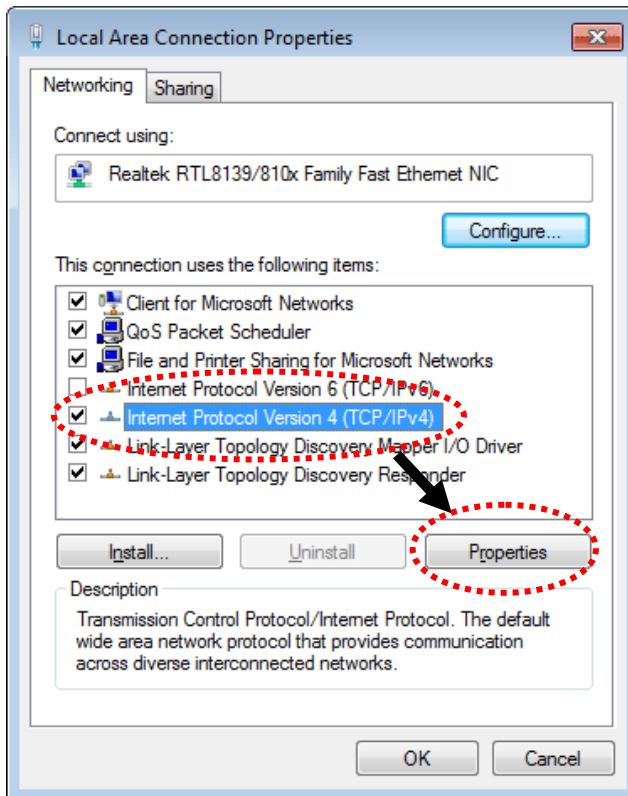
Click **Start** button (it should be located at lower-left corner of your computer), then click Control Panel. Double-click **Network and Internet**, and the following window will appear. Click **Network and Sharing Center**.



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



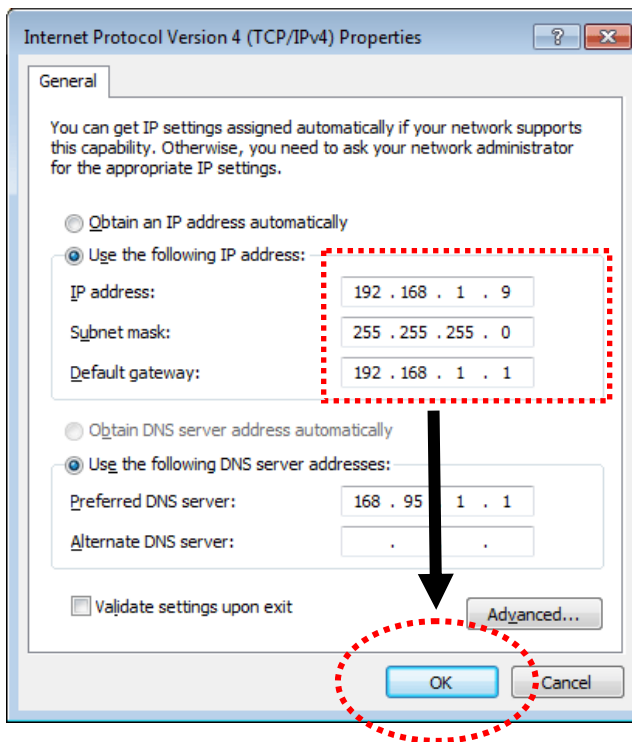
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



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

IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**

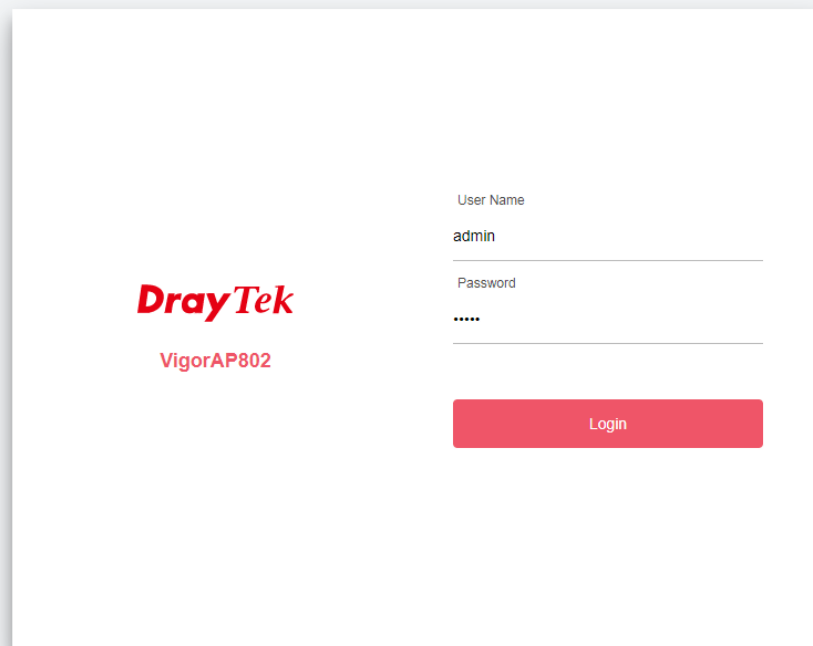


## I-4 Accessing to Web User Interface

---

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. Please type "admin/admin" on Username/Password and click **OK**.



The screenshot shows the login page for the DrayTek VigorAP802. On the left side, the DrayTek logo is displayed in red, with "VigorAP802" written below it in a smaller red font. On the right side, there is a login form with two input fields: "User Name" containing the text "admin" and "Password" containing five dots. Below the password field is a red "Login" button. At the bottom center of the page, there is a small copyright notice: "Copyright © 2018 DrayTek Corp".

---

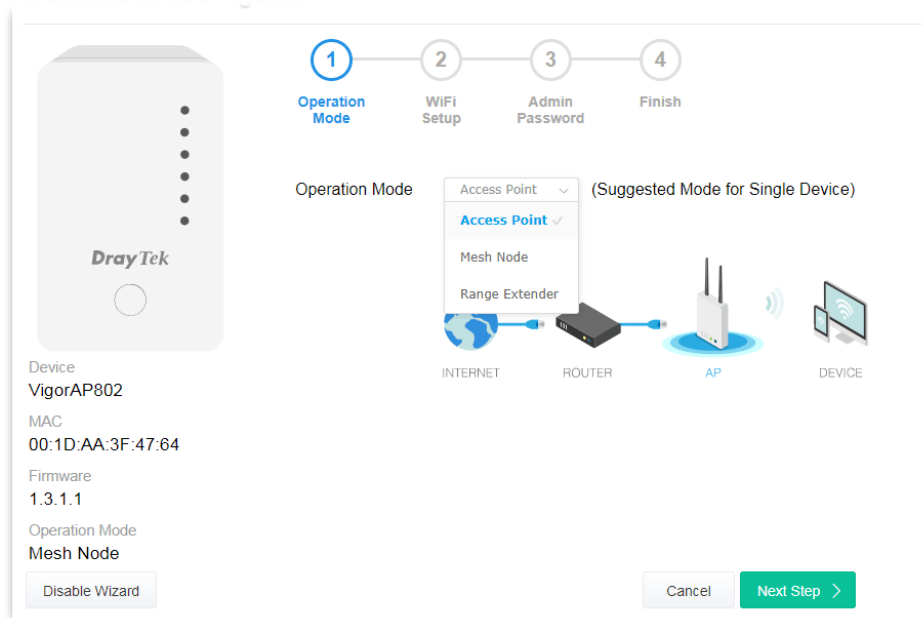
### **i** Note:

You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as **the IP address of VigorAP 802**.

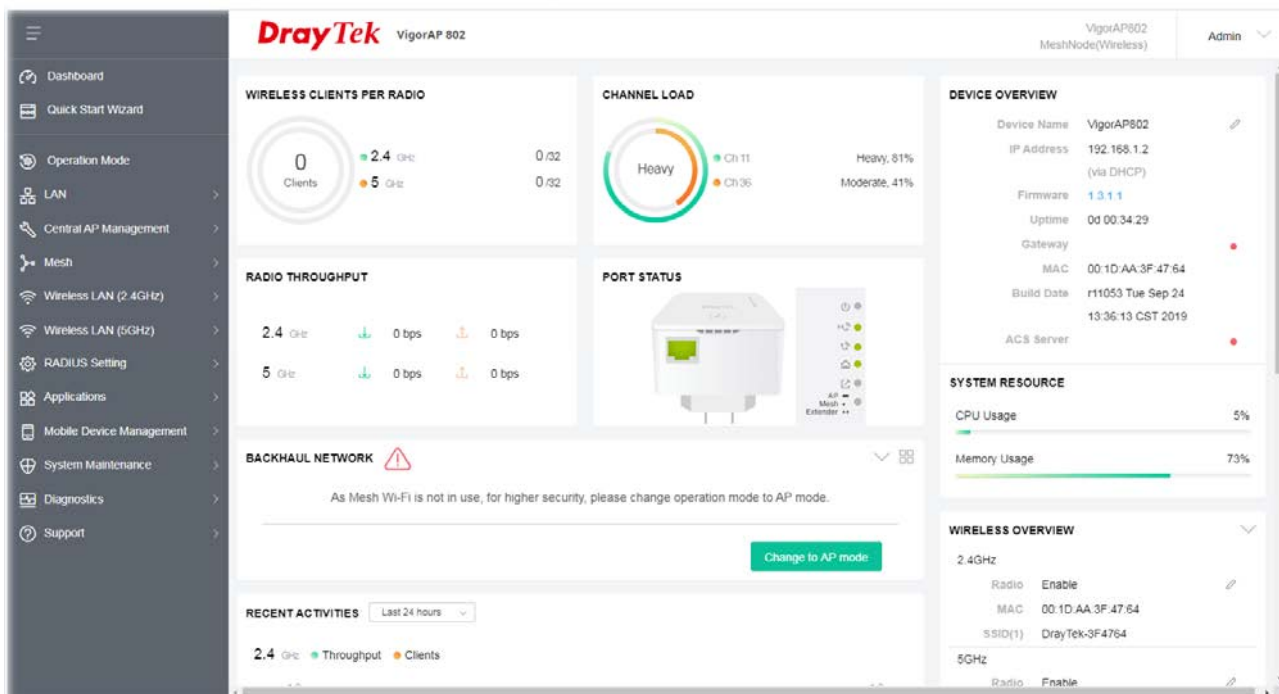
- If there is no DHCP server on the network, then VigorAP 802 will have an IP address of 192.168.1.2.
  - If there is DHCP available on the network, then VigorAP 802 will receive its IP address via the DHCP server.
  - If you connect to VigorAP by wireless LAN, you could try to access the web user interface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



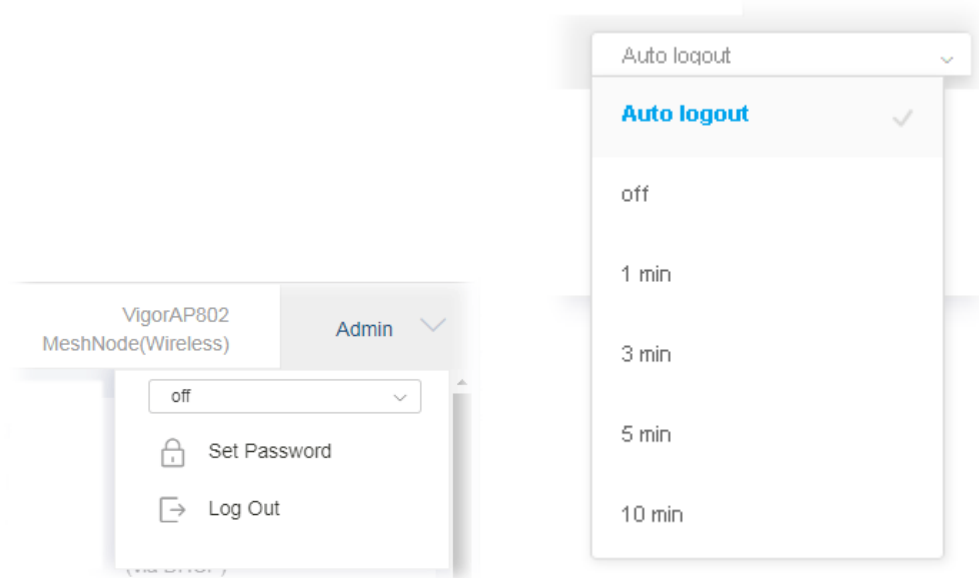
- For the first time accessing VigorAP, the **Quick Start Wizard** for configuring wireless settings will appear as follows. Refer to [Section I-7 Quick Start Wizard for detailed information](#).



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



- 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.



---

**i** Note:

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

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

---

# I-5 Changing Password

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

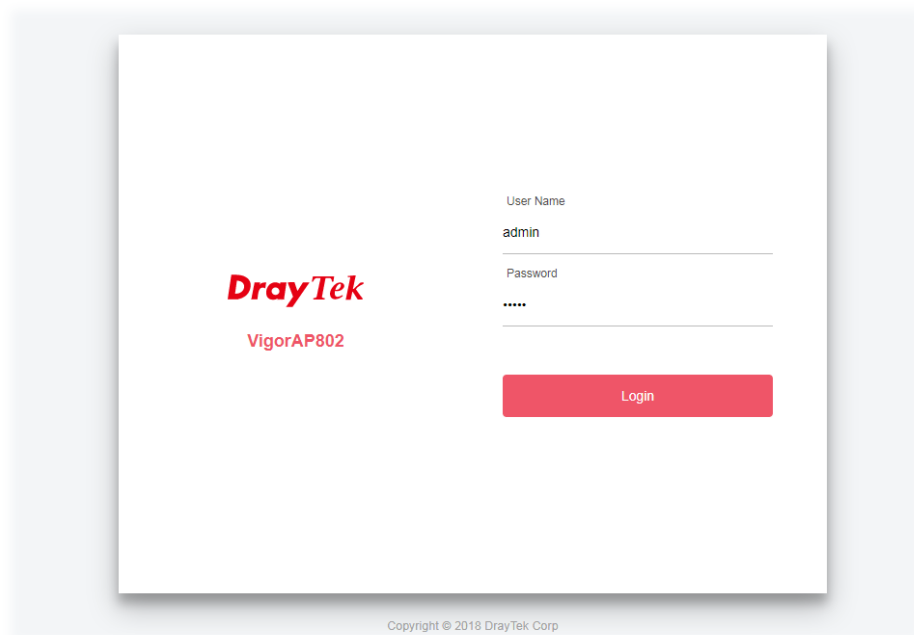
**System Maintenance >> Administration Password**

### Administrator Settings

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

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

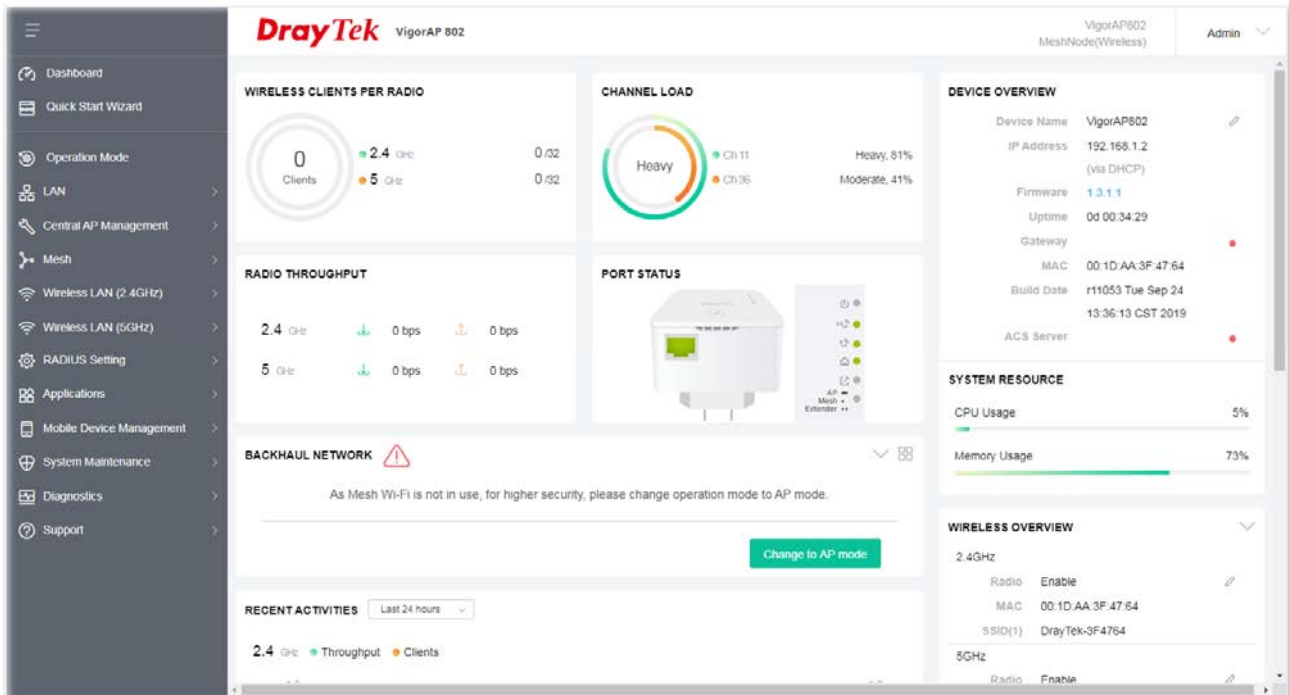
3. Enter the new login password on the field of **Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.



# I-6 Dashboard

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

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



# I-7 Quick Start Wizard

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

1 Operation Mode 2 WiFi Setup 3 Admin Password 4 Finish

Operation Mode  (Suggested Mode for Single Device)

INTERNET ROUTER AP DEVICE

Device  
VigorAP802  
MAC  
00:1D:AA:3F:47:64  
Firmware  
1.3.1.1  
Operation Mode  
Mesh Node

Disable Wizard Cancel Next Step >

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  
1.3.1.1

Operation Mode  
Mesh Node

Disable Wizard

Cancel

Next Step >

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

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.

< Back

Cancel

Next Step >

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

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

Device  
VigorAP802

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

Firmware  
1.3.1.1

Operation Mode  
Mesh Node

< Back

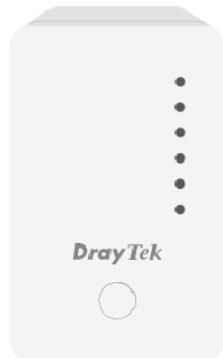
Cancel **Next Step** >

Available settings are explained as follows:

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

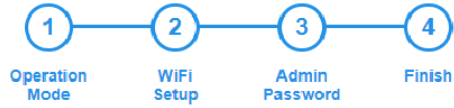
<b>Admin Password</b>	Enter a new password.
<b>Confirm Password</b>	Enter the new password again for confirmation.

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



Device  
VigorAP802  
MAC  
00:1D:AA:3F:47:64  
Firmware  
1.3.1.1  
Operation Mode  
**Mesh Node**

< Back



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

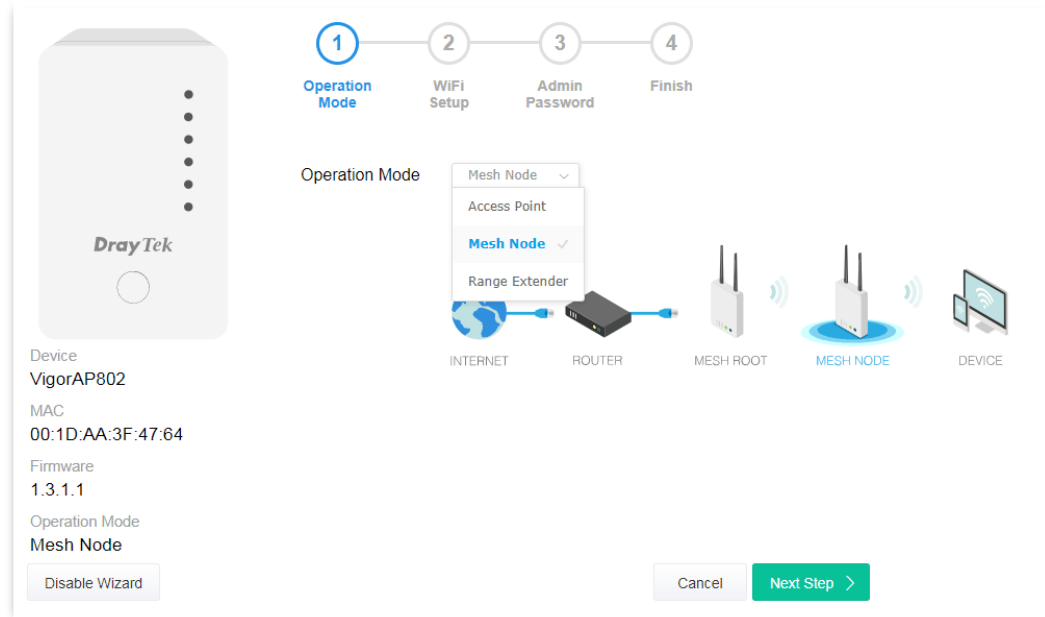
Cancel

Finish

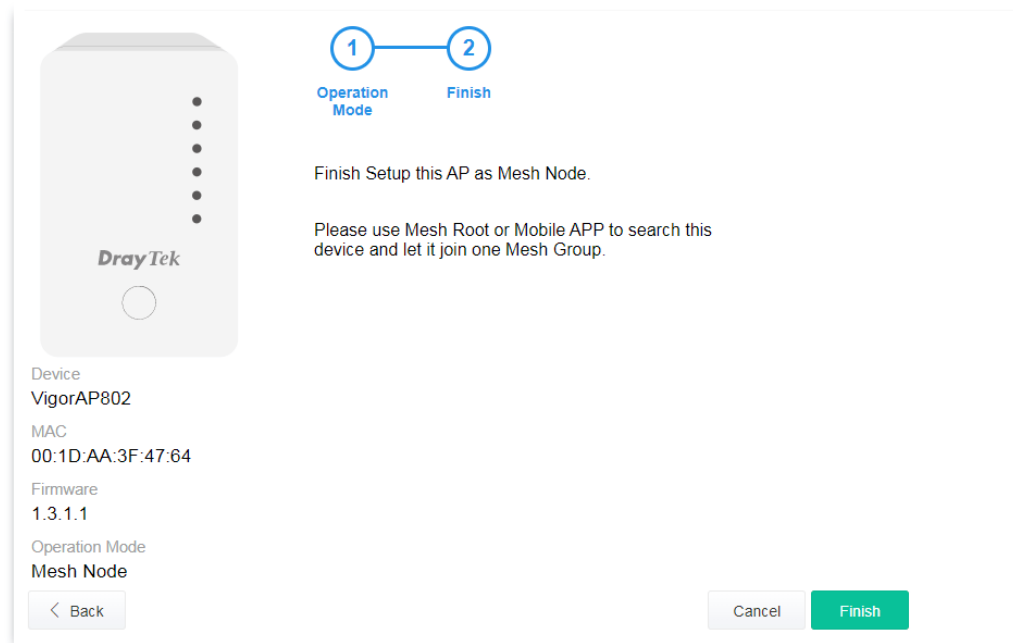


## I-7-2 Settings for Mesh Node

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



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



## I-7-3 Settings for Range Extender

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

Device  
VigorAP802  
MAC  
00:1D:AA:3F:47:64  
Firmware  
1.3.1.1  
Operation Mode  
Mesh Node

Disable Wizard

Cancel Next Step >

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

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.

< Back Cancel Next Step >

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

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

1 — 2 — 3 — 4 — 5  
 Operation Mode WiFi Setup Admin Password Range Extender Finish

Your AP is under default config. Please setup first.

Admin Password:

Confirm Password:

Device  
 VigorAP802  
 MAC  
 00:1D:AA:3F:47:64  
 Firmware  
 1.3.1.1  
 Operation Mode  
 Mesh Node

< Back Cancel Next Step >

Available settings are explained as follows:

Item	Description
<b>Admin Password</b>	Enter a new password.
<b>Confirm Password</b>	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**.

Available settings are explained as follows:

Item	Description
<b>SSID/Security Key</b>	Once the access point specified above, the name / security key of the AP will be shown automatically in these fields.
<b>Channel</b>	Means the channel frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference.
<b>Security Mode</b>	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.
<b>Encryption Type</b>	Available options will vary according to the selected <b>Security Mode</b> . <b>When Open is selected:</b> <ul style="list-style-type: none"> <li>Choose <b>None</b> to disable the WEP Encryption. Data sent to the AP will not be encrypted.</li> <li><b>WEP Keys</b> –To enable WEP encryption for data transmission, please choose <b>WEP</b>. 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 '':</li> </ul> <b>When Shared is selected:</b>

- **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 ';\n

**When WPA/PSK or WPA2/PSK is selected:**

- Select **TKIP** or **AES** as the algorithm for WPA.
- **Security Key** - Select WEP, TKIP or AES as the encryption algorithm.

Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

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

1 — 2 — 3 — 4 — 5  
 Operation Mode — WiFi Setup — Admin Password — Range Extender — Finish

Basic settings are completed. Press Finish button apply changes.

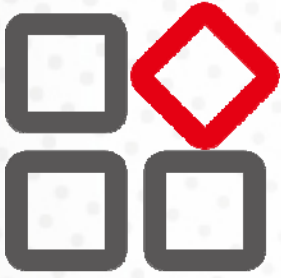
Operation Mode	Range Extender (2.4GHz WLAN)
Peer SSID	guests
WiFi Name	DrayTek-3F4764
2nd WiFi Name	Disabled
Bandwidth Limit	Disabled
Station Control	Disabled

Device  
 VigorAP802  
 MAC  
 00:1D:AA:3F:47:64  
 Firmware  
 1.3.1.1  
 Operation Mode  
 Mesh Node

< Back Cancel **Finish**

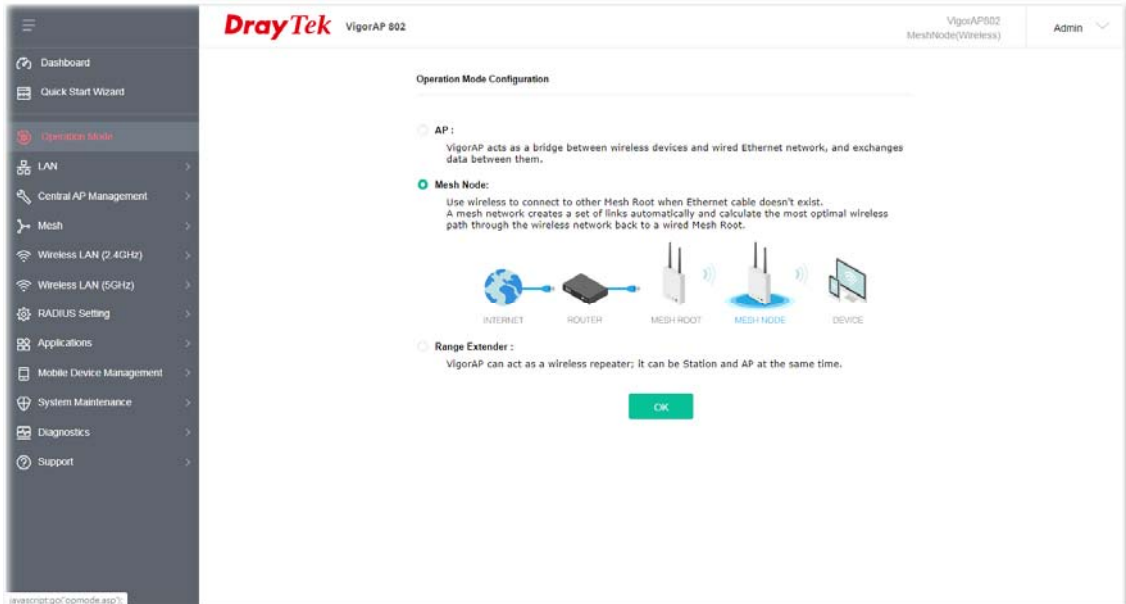
This page is left blank.

# Chapter II Connectivity



# II-1 Operation Mode

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



Available settings are explained as follows:

Item	Description
<b>AP</b>	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
<b>Mesh</b>	<p><b>Mesh Root</b> – VigorAP must connect to a gateway with an Ethernet cable.</p> <p><b>Mesh Node</b> – 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.</p>
<b>Range Extender</b>	VigorAP can act as a wireless repeater which will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.



---

**i** Note:

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

---

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

---

VigorAP 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.



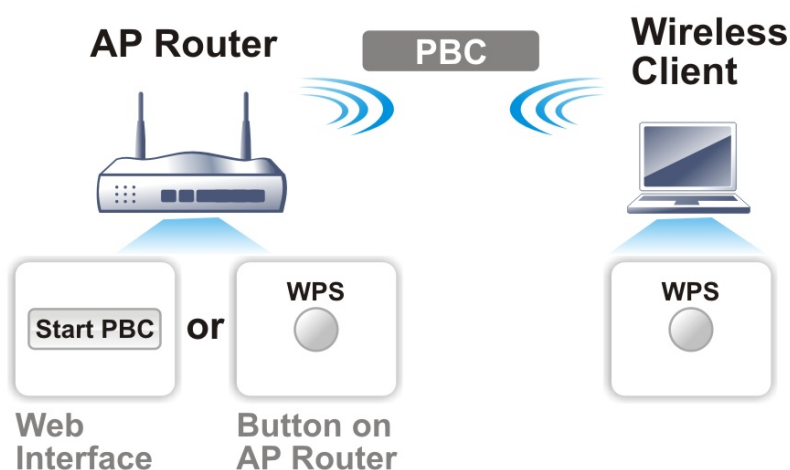
It is the simplest way to build connection between wireless network clients and VigorAP 802. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

**i** Note:

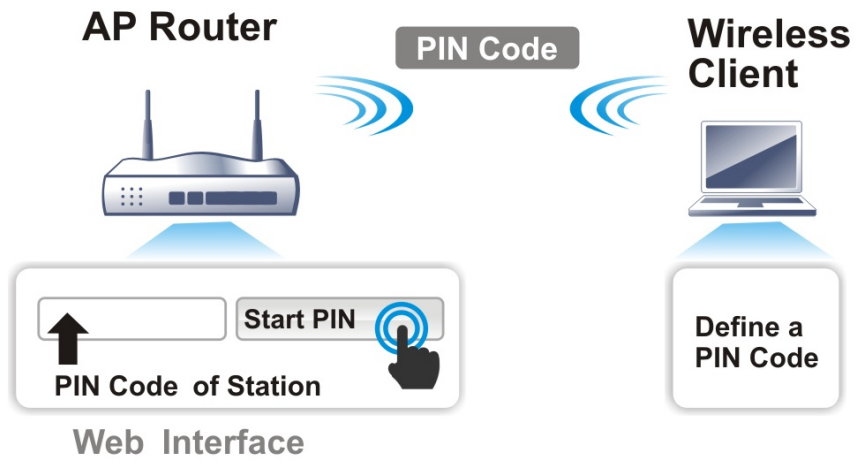
Such function is available for the wireless station with WPS supported.

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

On the side of VigorAP 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.



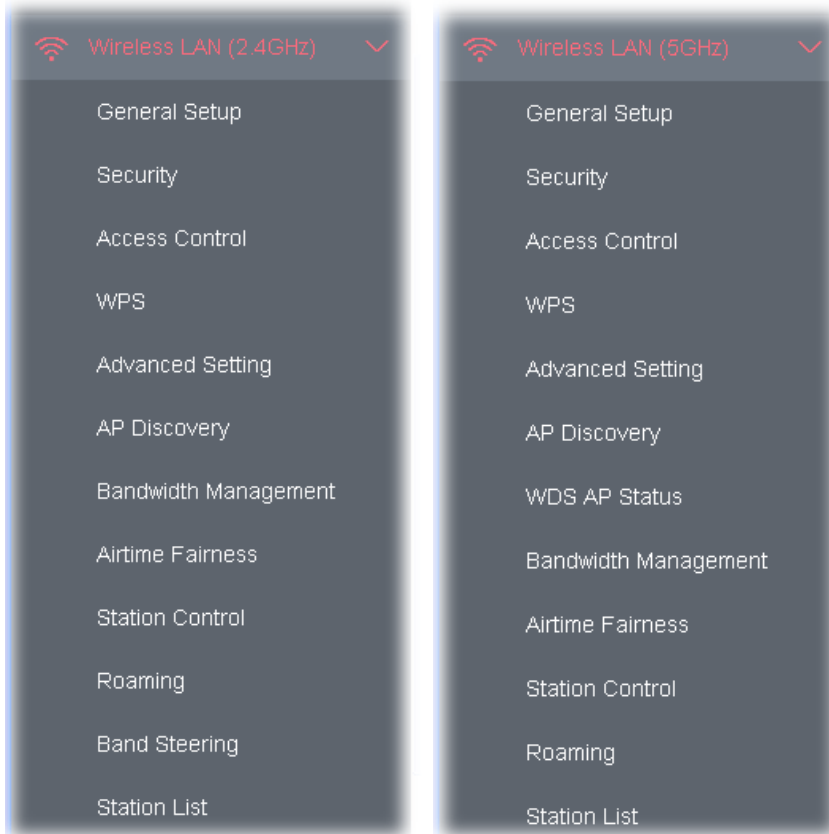
If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 802.



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

---

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



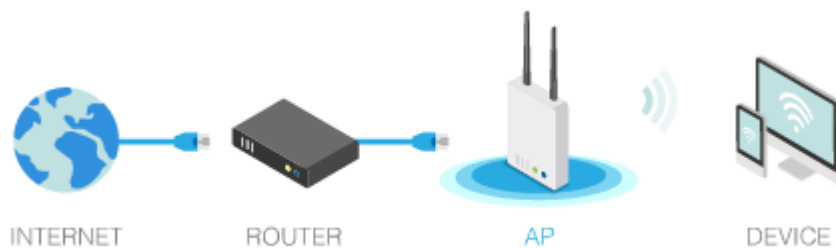
---

**i** Note:

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

---

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



## II-3-1 General Setup

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

Wireless LAN (5GHz) >> General Setup

General Setting ( IEEE 802.11 )

Enable Wireless LAN

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

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

---

Mode :

Channel :  (Active Channel: 36)

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

---

	Enable	Hide SSID	SSID	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek-3F4764"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Hide SSID: Prevent SSID from being scanned.  
Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

---

WDS Settings (PHY Mode : HTMIX)

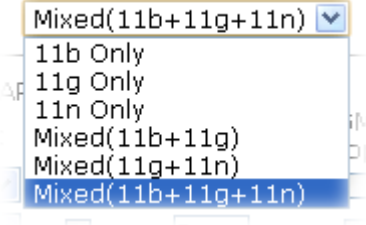
<p>1. Subnet <input type="text" value="LAN-A"/></p> <p>Security : <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p>Peer MAC Address : <input type="text"/></p>	<p>3. Subnet <input type="text"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

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
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Client Limit</b>	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.

<b>Enable Client Limit per SSID</b>	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.
<b>Mode</b>	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.  
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above. Configure the extension channel you want.
<b>Hide SSID</b>	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.
<b>SSID</b>	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.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not access for each other.
<b>VLAN ID</b>	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.
<b>PHY Mode</b>	Data will be transmitted via HTMIX mode.  Each access point should be setup to the same <b>Phy Mode</b> for connecting with each other.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm.  Type <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
<b>Peer MAC Address</b>	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 1
SSID 2

SSID DrayTek-3F4764

Mode WPA2/PSK v

Set up [RADIUS Server](#) if 802.1x is enabled.

**WPA**

WPA Algorithms  TKIP  AES  TKIP/AES

Pass Phrase

Key Renewal Interval  seconds

EAPOL Key Retry  Enable  Disable

**WEP**

Key 1 :  Hex v

Key 2 :  Hex v

Key 3 :  Hex v

Key 4 :  Hex v

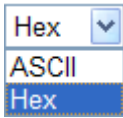
802.1x WEP  Disable  Enable

OK
Cancel

Available settings are explained as follows:

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



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

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

**RADIUS Server**

IP Address: 0

Port: 1812

Shared Secret: DrayTek

Session Timeout: 0 second(s)

OK

Available settings are explained as follows:

Item	Description
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	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.
<b>Session Timeout</b>	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 v

**MAC Address Filter**

Index	MAC Address

Client's MAC Address :  :  :  :  :  :

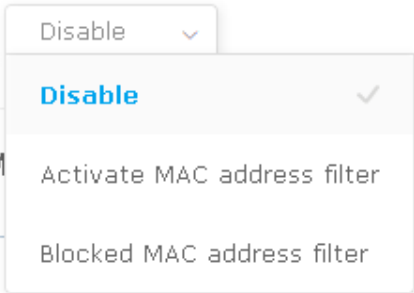
Add
Delete
Edit
Limit: 256 entries

OK
Cancel

Backup ACL Cfg : Backup

Upload From File: Upload ... Restore

Available settings are explained as follows:

Item	Description
<b>Policy</b>	<p>Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b>, 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.</p> <div style="margin-top: 10px;">  </div>


<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>Client's MAC Address</b>	Manually enter the MAC address of wireless client.
<b>Add</b>	Add a new MAC address into the list.
<b>Delete</b>	Delete the selected MAC address in the list.
<b>Edit</b>	Edit the selected MAC address in the list.
<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	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


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


### Device Configure


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

Status: Idle

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 802 is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 802. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 802.

<b>Configure via Push Button</b>	Click <b>Start PBC</b> 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)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> 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

Antenna  2T2R  1T1R

Tx Power  100%  80%  60%  30%  20%  
 10%

Fragment Length (256 - 2346)  bytes

RTS Threshold (1 - 2347)  bytes

Country Code  (Reference)

Auto Channel Filtered Out List  1  2  3  4  5  6  7  8  9  10  
 11

IGMP Snooping  Enable  Disable

Isolate 2.4GHz and 5GHz bands  Enable  Disable

Isolate members with IP  Enable  Disable

WMM Capable  Enable  Disable

APSD Capable  Enable  Disable

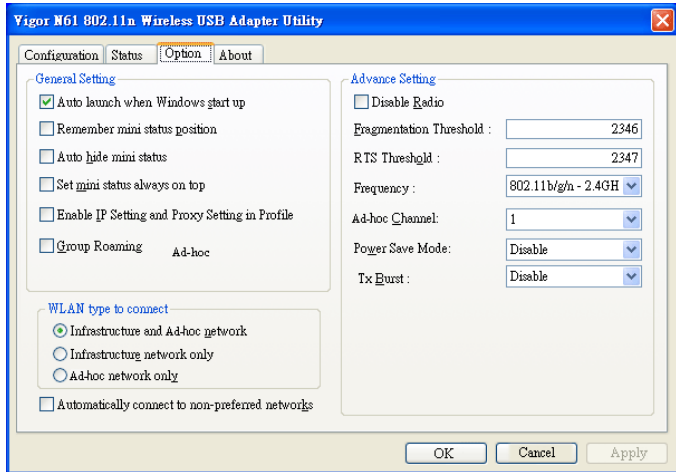
MAC Clone  Enable  Disable

**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.

**Note:** Fragment Length takes effect when mode is "11b Only" or "Mixed(11b+11g)".

Available settings are explained as follows:

Item	Description
<b>Channel Width</b>	<p><b>20 MHz-</b> The device will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHz-</b>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.</p>

	<p><b>40 MHz-</b> The device will use 40MHz for data transmission and receiving between the AP and the stations. It is for wireless LAN 2.4GHz only.</p> <p><b>Auto 20/40 /80 MHz -</b> The device will use 20/40/80 MHz channel bandwidth for data transmission and receiving between the AP and the stations.</p>
<p><b>Packet-OVERDRIVE (for 2.4GHz only)</b></p>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). 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.</p> <p>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 <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b>).</p> 
<p><b>Antenna (for 2.4GHz only)</b></p>	<p>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.</p>
<p><b>Tx Power</b></p>	<p>The default setting is the maximum (100%). Lowering down the value may degrade range and throughput of wireless.</p>
<p><b>Rate Adaptation Algorithm</b></p>	<p>Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old".</p>
<p><b>Fragment Length</b></p>	<p>Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.</p>
<p><b>RTS Threshold</b></p>	<p>Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.</p> <p>Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.</p>
<p><b>Country Code</b></p>	<p>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.</p>
<p><b>Auto Channel Filtered Out List</b></p>	<p>The selected wireless channels will be discarded if <b>AutoSelect</b> is selected as <b>Channel</b> selection mode in <b>Wireless LAN&gt;&gt;General</b></p>

	<b>Setup.</b>
<b>IGMP Snooping</b>	Click <b>Enable</b> 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.
<b>Isolate 2.4GHz and 5GHz bands</b>	<p>The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.</p> <p>For WLAN 2.4GHz and 5GHz set with the same SSID name:</p> <ul style="list-style-type: none"> <li>● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is NOT enabled for such SSID.</li> <li>● Yet, if the function of <b>Isolate Member</b> (in <b>Wireless LAN&gt;&gt;General Setup</b>) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.</li> </ul>
<b>Isolate members with IP</b>	<p>The default setting is "Disable".</p> <p>If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).</p>
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>APSD Capable (for 5GHz only)</b>	<p>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.</p> <p>The default setting is <b>Disable</b>.</p>
<b>MAC Clone (for 2.4GHz only)</b>	Click <b>Enable</b> 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

Scan

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
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 802.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 802.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 802.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Mode</b>	Display the wireless connection mode that the scanned AP used.
<b>Ch. Width</b>	Display the channel width that the scanned AP used.
<b>Scan</b>	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
-----	-------------	----------------------	------------	-----------

Refresh

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

## II-3-8 Bandwidth Management

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

Wireless LAN (5GHz) >> Bandwidth Management

SSID 1	SSID 2
SSID	DrayTek-3F4764
Per Station Bandwidth Limit	
Enable	<input checked="" type="checkbox"/>
Upload Limit	User defined <input type="text" value="K"/> bps (Default unit : K)
Download Limit	2M <input type="text" value=""/> bps
Auto Adjustment	<input checked="" type="checkbox"/>
Total Upload Limit	User defined <input type="text" value="K"/> bps (Default unit : K)
Total Download Limit	User defined <input type="text" value="K"/> bps (Default unit : K)

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

OK

Cancel

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the specific SSID name.
<b>Enable</b>	Check this box to enable the bandwidth management for clients.
<b>Upload Limit</b>	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 <b>User defined</b> , you have to specify the rate manually.
<b>Download Limit</b>	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 <b>User defined</b> , you have to specify the rate manually.
<b>Auto Adjustment</b>	Check this box to have the bandwidth limit determined by the system automatically.
<b>Total Upload Limit</b>	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.
<b>Total Download Limit</b>	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.

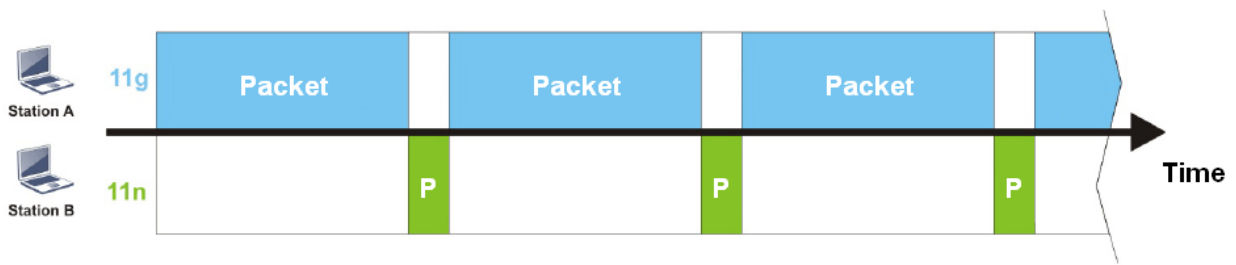
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

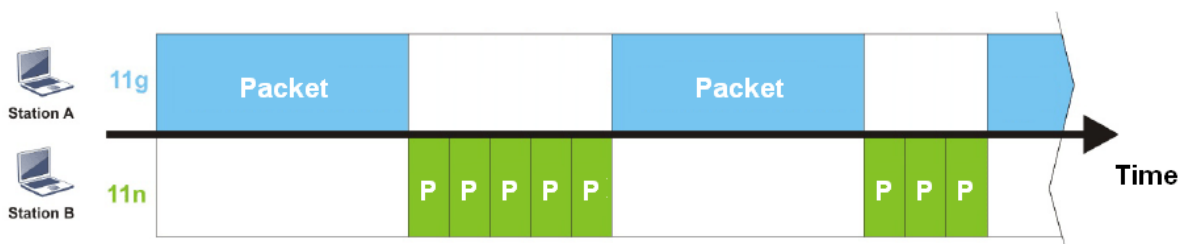
The principle behind the IEEE802.11 channel access mechanisms is that each station has **equal probability** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

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

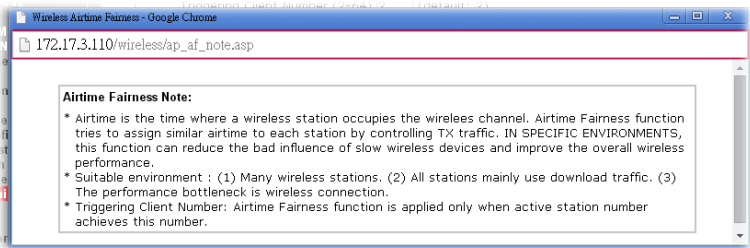
Enable [Airtime Fairness](#)

Triggering Client Number  (2 ~ 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.

Available settings are explained as follows:

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



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

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

**i** Note:

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

## II-3-10 Station Control

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

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

**i** Note:

Up to 300 Wireless Station records are supported by VigorAP.

## Wireless LAN (5GHz) >> Station Control

SSID 1	SSID 2
SSID	DrayTek-3F4764
Enable	<input type="checkbox"/>
Connection Time	1 hour ▾
Reconnection Time	1 day ▾
<a href="#">Display All Station Control List</a>	

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

OK

Cancel

Available settings are explained as follows:

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

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

#### Fast Roaming(WPA2/802.1x)

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

OK Cancel

Available settings are explained as follows:

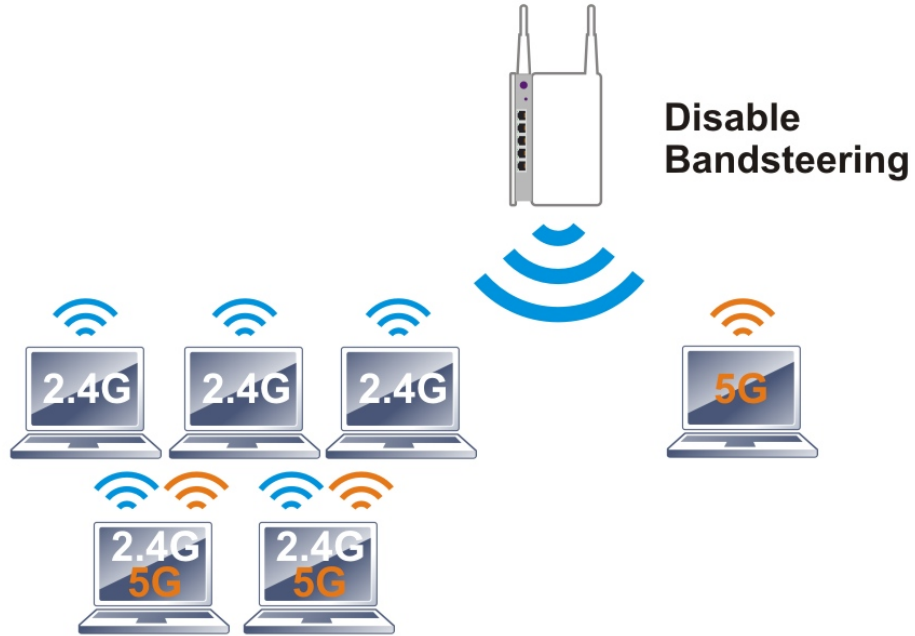
Item	Description
<b>AP-assisted Client Roaming Parameters</b>	<p>When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 802 will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal.</p> <p><b>Minimum Basic Rate</b> - Check the box to use the drop down list to specify a basic rate (<b>Mbps</b>). When the link rate of the wireless station is below such value, VigorAP 802 will terminate the network connection for that wireless station.</p> <p><b>Disable RSSI Requirement</b> - If it is selected, VigorAP will not terminate the network connection based on RSSI.</p> <p><b>Strictly Minimum RSSI</b> - 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 (<b>dBm</b>) set here, VigorAP 802 will terminate the network connection for that wireless station.</p> <p><b>Minimum RSSI</b> - When the signal strength of the wireless station is below the value (<b>dBm</b>) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value</p>

	<p>(defined in the field of <b>With Adjacent AP RSSI over</b>) 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).</p> <ul style="list-style-type: none"> <li>● <b>With Adjacent AP RSSI over</b> – Specify a value as a threshold.</li> </ul>
<p><b>Fast Roaming (WPA2/802.1x)</b></p>	<p><b>Enable</b> – Check the box to enable fast roaming configuration.</p> <p><b>PMK Caching</b> - 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 <b>WPA2/802.1</b> mode.</p> <p><b>Pre-Authentication</b> - Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)</p> <p><b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.</p> <p><b>Disable</b> - Disable IEEE 802.1X Pre-Authentication.</p>

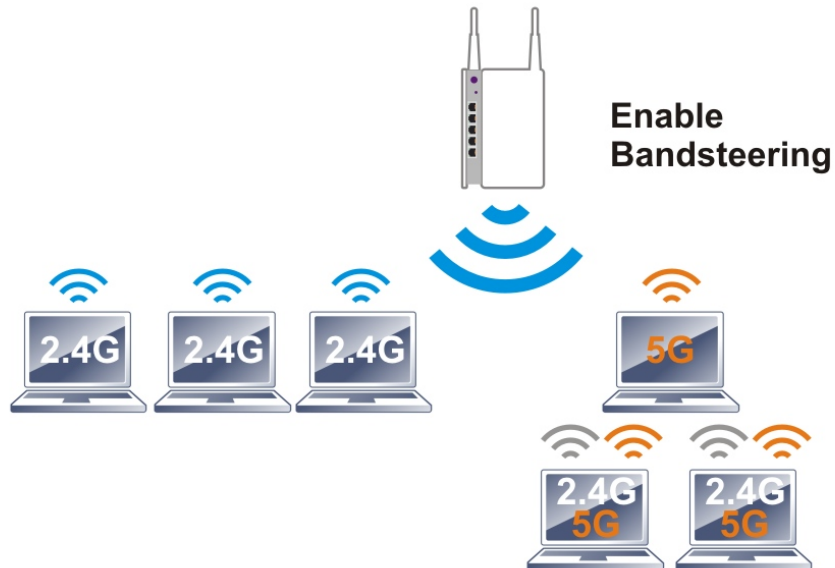
After finishing this web page configuration, please click **OK** to save the settings.

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

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



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



---

**i** Note:

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

---



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

#### Wireless LAN (2.4GHz) >> Band Steering

Enable **Band Steering**  
  
Check Time for WLAN Client 5G Capability  seconds (1 ~ 60, Default: 15)  
  
 5GHz Minimum RSSI  dBm ( %) (Default: -78)  
  
(Only do band steering when 5GHz signal is better than Minimum RSSI)

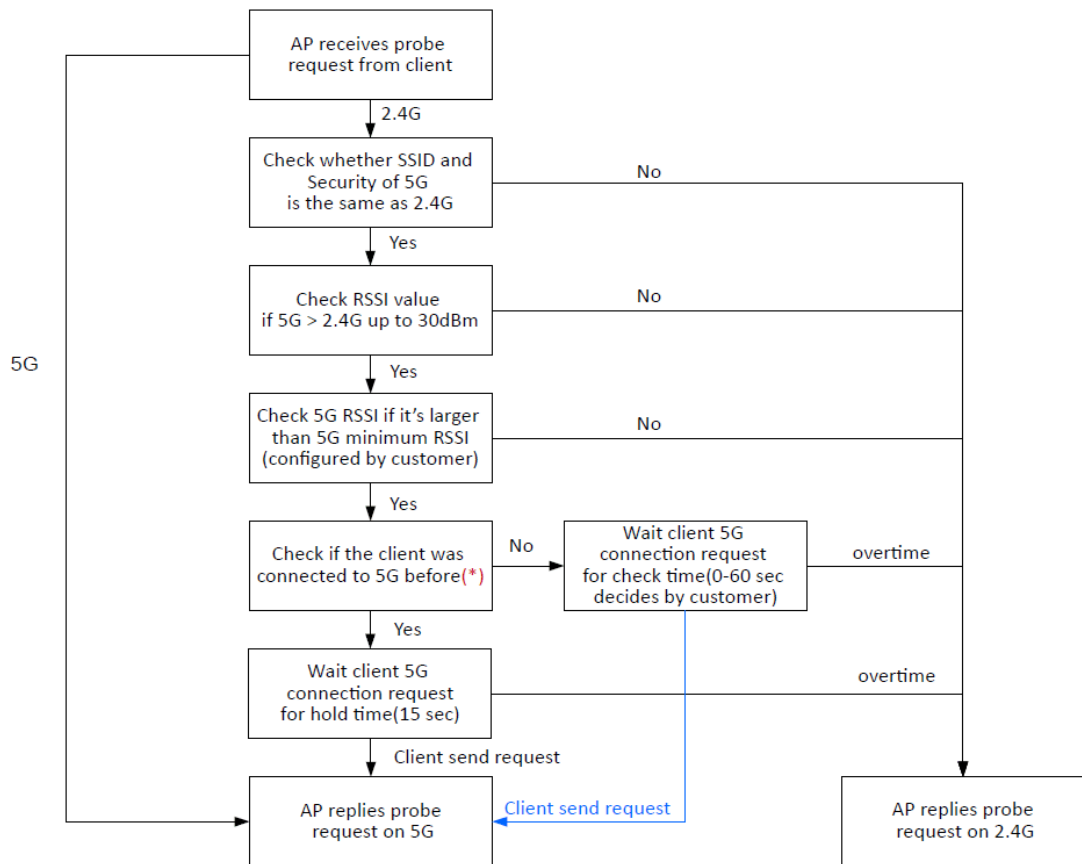
**Note:** Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
<b>Enable Band Steering</b>	<p>If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit.</p> <p><b>Check Time....</b> – If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for VigorAP to detect the wireless client.</p> <p><b>5GHz Minimum RSSI</b> – 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.</p>

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

Below shows how Band Steering works.



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

## How to Use Band Steering?

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

### Wireless LAN (2.4GHz) >> Band Steering

Enable **Band Steering**

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

5GHz Minimum RSSI  dBm ( %) (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.

OK
Cancel

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  (3 ~ 64, default: 64)

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

---

Mode :

Channel :

Extension Channel :

---

Enable 2 Subnet (Simulate 2 APs)

	Enable	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0: Untagged)
1	<input type="checkbox"/>	<input type="checkbox"/>	ap903-BandSteering	LAN-A	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DrayTek-LAN-B	LAN-A	<input type="checkbox"/>	<input type="text" value="0"/>

### Wireless LAN (5GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

Enable Wireless LAN

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

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

---

Mode :

Channel :

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	<input type="checkbox"/>	<input type="checkbox"/>	ap903-BandSteering	LAN-A	<input type="checkbox"/>	<input type="text" value="0"/>

Same value for 2.4GHz and 5GHz

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

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
ap903-BandSteering			
Mode			
Mixed(WPA+WPA2)/802.1x			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
<input type="text" value="....."/>			
Key Renewal Interval			
<input type="text" value="3600"/> seconds			
EAPOL Key Retry			
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<b>WEP</b>			

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 <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
<input type="text" value="....."/>			
Key Renewal Interval			
<input type="text" value="3600"/> seconds			
EAPOL Key Retry			
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<b>WEP</b>			

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

### General

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

Wireless LAN (2.4GHz) >> Station List

#### Station List

							General	Advanced	Control	Neighbor
Index	MAC Address	Vendor	RSSI	Approx. Distance	SSID	Visit Time				
1	DA:75:55:94:AD:C3		34% (-76dBm)	35.48m	N/A	0d:0h:0m:0s				
2	02:1D:AA:62:E4:30		24% (-80dBm)	56.23m	N/A	4d:22h:33m:55s				
3	DA:A1:19:38:16:4A	Google	0% (-90dBm)	177.83m	N/A	0d:0h:0m:0s				
4	CB:FF:28:FC:2A:C1	LiteonTe	0% (-92dBm)	223.87m	N/A	0d:0h:0m:0s				
5	A6:3F:F4:6E:5E:55		36% (-75dBm)	31.62m	N/A	0d:0h:0m:0s				
6	02:1D:AA:62:E7:38		12% (-85dBm)	100.00m	N/A	4d:22h:34m:7s				
7	02:1D:AA:62:FF:20		29% (-78dBm)	44.67m	N/A	4d:22h:34m:13s				
8	02:1D:AA:69:ED:38		12% (-85dBm)	100.00m	N/A	4d:22h:34m:12s				

[Refresh](#)

Add to [Access Control](#) :

Client's MAC Address :  :  :  :  :  :

- Note:**
1. Approx. Distance is calculated by actual signal strength of device detected. Inaccuracy might occur based on barrier encountered.
  2. Due to the differences in signal strength for different devices, the calculated value of approximate distance also might be different.
  3. Trademarks and brand names are the properties of their respective owners.

[Add](#)

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>Hostname</b>	Display the host name of the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - 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.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

**Advanced**

Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

**Control**

Display connection and reconnection time of the wireless stations.

**Neighbor**

Display more information for the neighboring wireless stations.

## 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.

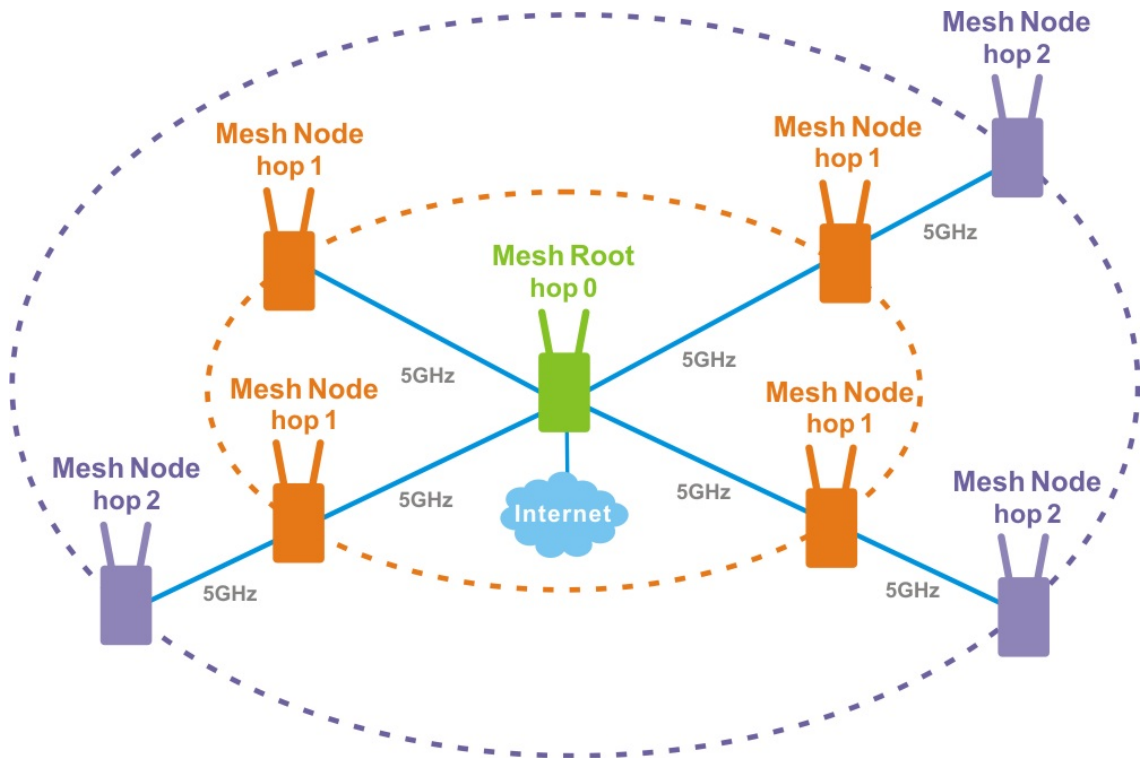
OK



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,

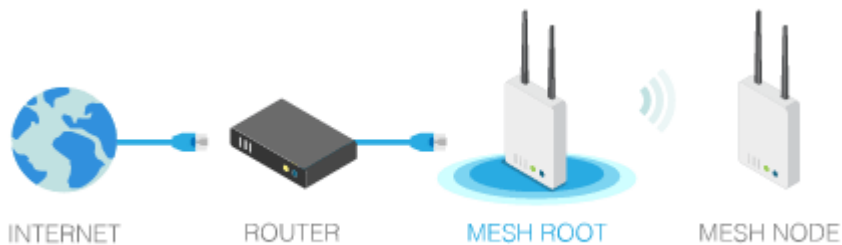
- It must be composed by "1" Mesh Root and "0~7" mesh nodes
- (Roaming) Normally members in a mesh group use the same Wireless SSID/security
- (Add) Only the mesh root can add a new mesh node into the mesh group
- (Recover) A disconnected mesh node will automatically try to connect to another connected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





**i 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	<input checked="" type="radio"/> Mesh Node		
Wired Uplink	<input type="checkbox"/>		
Wireless Uplink Band	Auto <input type="button" value="v"/>		
Log Level	Basic <input type="button" value="v"/>		
<b>Mesh Group</b>			
Index	Role	MAC Address	Model
<input type="button" value="Reset"/>			

### Backup Mesh Config

<input type="button" value="Backup"/>	<input type="button" value="Upload"/>	<input type="text" value="..."/>	<input type="button" value="Restore"/>
---------------------------------------	---------------------------------------	----------------------------------	--

Available settings are explained as follows:

Item	Description
<b>Role</b>	<b>Mesh Node</b> – As a mesh node, the VigorAP can pass the wireless connection signal to other mesh node or a remote device (PC, CPE, mobile phone).
<b>Wired Uplink</b>	Check the box if the VigorAP connects to an uplinked mesh root or an uplinked mesh node with an Ethernet cable.
<b>Wireless Uplink Band</b>	Choose a wireless band for connecting with an uplinked mesh root or an uplinked mesh node.
<b>Log Level</b>	Choose <b>Basic</b> or <b>Detailed</b> . Related information will be shown on the <b>Diagnostics&gt;&gt;System Log</b> .
<b>Mesh Group</b>	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.
<b>Reset</b>	Click it to clear the Mesh Group information.
<b>Backup Mesh Config</b>	<b>Backup</b> – Click the button to save the configuration as a file. <b>Upload/Restore</b> – 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

| [Refresh](#) |

Device Name	VigorAP802
MAC Address	00:1D:AA:3F:47:64
Model	VigorAP802
Operation Mode	MeshNode(Wireless)
Wireless Uplink Band	Auto
Link Status	New
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

Scan

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

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

## II-4-4 Configuration Sync

This page can display current configuration of VigorAP device.

Mesh >> Configuration Sync

### System Maintenance

Index	Name	Value
1	X_00507F_System.Management.SkipQuickStartWizard	Enable
2	X_00507F_System.TR069Setting.CPEEnable	0
3	ManagementServer.URL	
4	ManagementServer.Username	
5	ManagementServer.Password	*****
6	ManagementServer.ConnectionRequestUsername	vigor
7	ManagementServer.ConnectionRequestPassword	*****
8	X_00507F_System.AdminmodePassword.Admin	admin
9	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	DrayTek-3F4764
3	X_00507F_WirelessLAN_AP.General.SSID.1.Enable	1
4	X_00507F_WirelessLAN_AP.Security.1.WPAPSK	*****
5	X_00507F_WirelessLAN_AP.Security.1.Mode	WPA2/PSK
6	X_00507F_WirelessLAN_AP.Security.1.WPAEncMode	AES
7	X_00507F_WirelessLAN_AP.Security.1.KeyRenewalInterval	3600
8	X_00507F_WirelessLAN_AP.General.SSID.2.ESSID	
9	X_00507F_WirelessLAN_AP.General.SSID.2.Enable	0
10	X_00507F_WirelessLAN_AP.Security.2.WPAPSK	*****
11	X_00507F_WirelessLAN_AP.Security.2.Mode	WPA2/PSK
12	X_00507F_WirelessLAN_AP.Security.2.WPAEncMode	AES
13	X_00507F_WirelessLAN_AP.Security.2.KeyRenewalInterval	3600
14	X_00507F_WirelessLAN_AP.StationControl.2.Enable	0
15	X_00507F_WirelessLAN_AP.StationControl.2.ConnectTime	0_days,1_hours,0_mins
16	X_00507F_WirelessLAN_AP.StationControl.2.ReconnectTime	1_days,0_hours,0_mins
17	X_00507F_WirelessLAN_AP.BandwidthManagement.SSID.2.Enable	0
18	X_00507F_WirelessLAN_AP.BandwidthManagement.SSID.2.UploadLimit	K
19	X_00507F_WirelessLAN_AP.BandwidthManagement.SSID.2.DownloadLimit	K
20	X_00507F_WirelessLAN_AP.General.SSID.3.ESSID	Error
21	X_00507F_WirelessLAN_AP.General.SSID.3.Enable	Error
22	X_00507F_WirelessLAN_AP.Security.3.WPAPSK	*****
23	X_00507F_WirelessLAN_AP.Security.3.Mode	Error
24	X_00507F_WirelessLAN_AP.Security.3.WPAEncMode	Error
25	X_00507F_WirelessLAN_AP.Security.3.KeyRenewalInterval	Error
26	X_00507F_WirelessLAN_AP.General.SSID.4.ESSID	Error
27	X_00507F_WirelessLAN_AP.General.SSID.4.Enable	Error
28	X_00507F_WirelessLAN_AP.Security.4.WPAPSK	*****
29	X_00507F_WirelessLAN_AP.Security.4.Mode	Error
30	X_00507F_WirelessLAN_AP.Security.4.WPAEncMode	Error
31	X_00507F_WirelessLAN_AP.Security.4.KeyRenewalInterval	Error

### Wireless LAN (5GHz)

Index	Name	Value
1	X_00507F_WirelessLAN_5G_AP.General.EnableWLAN	1
2	X_00507F_WirelessLAN_5G_AP.General.SSID.1.ESSID	DrayTek-3F4764
3	X_00507F_WirelessLAN_5G_AP.General.SSID.1.Enable	0
4	X_00507F_WirelessLAN_5G_AP.Security.1.WPAPSK	*****
5	X_00507F_WirelessLAN_5G_AP.Security.1.Mode	WPA2/PSK
6	X_00507F_WirelessLAN_5G_AP.Security.1.WPAEncMode	AES
7	X_00507F_WirelessLAN_5G_AP.Security.1.KeyRenewalInterval	3600
8	X_00507F_WirelessLAN_5G_AP.General.SSID.2.ESSID	
9	X_00507F_WirelessLAN_5G_AP.General.SSID.2.Enable	0
10	X_00507F_WirelessLAN_5G_AP.Security.2.WPAPSK	*****
11	X_00507F_WirelessLAN_5G_AP.Security.2.Mode	WPA2/PSK
12	X_00507F_WirelessLAN_5G_AP.Security.2.WPAEncMode	AES
13	X_00507F_WirelessLAN_5G_AP.Security.2.KeyRenewalInterval	3600
14	X_00507F_WirelessLAN_5G_AP.StationControl.2.Enable	0
15	X_00507F_WirelessLAN_5G_AP.StationControl.2.ConnectTime	0_days,1_hours,0_mins
16	X_00507F_WirelessLAN_5G_AP.StationControl.2.ReconnectTime	1_days,0_hours,0_mins
17	X_00507F_WirelessLAN_5G_AP.BandwidthManagement.SSID.2.Enable	0
18	X_00507F_WirelessLAN_5G_AP.BandwidthManagement.SSID.2.UploadLimit	K
19	X_00507F_WirelessLAN_5G_AP.BandwidthManagement.SSID.2.DownloadLimit	K
20	X_00507F_WirelessLAN_5G_AP.General.SSID.3.ESSID	Error
21	X_00507F_WirelessLAN_5G_AP.General.SSID.3.Enable	Error
22	X_00507F_WirelessLAN_5G_AP.Security.3.WPAPSK	*****
23	X_00507F_WirelessLAN_5G_AP.Security.3.Mode	Error
24	X_00507F_WirelessLAN_5G_AP.Security.3.WPAEncMode	Error
25	X_00507F_WirelessLAN_5G_AP.Security.3.KeyRenewalInterval	Error
26	X_00507F_WirelessLAN_5G_AP.General.SSID.4.ESSID	Error
27	X_00507F_WirelessLAN_5G_AP.General.SSID.4.Enable	Error
28	X_00507F_WirelessLAN_5G_AP.Security.4.WPAPSK	*****
29	X_00507F_WirelessLAN_5G_AP.Security.4.Mode	Error
30	X_00507F_WirelessLAN_5G_AP.Security.4.WPAEncMode	Error
31	X_00507F_WirelessLAN_5G_AP.Security.4.KeyRenewalInterval	Error

**Note:** 1. Please wait for about 5 ~ 10 secs to load TR-069 parameters.  
2. Mesh Root can apply above TR-069 parameters to Mesh Nodes.

Available settings are explained as follows:

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

## 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)

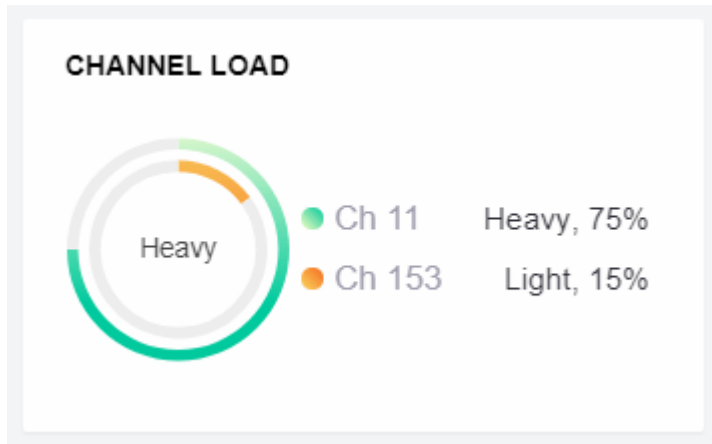
iPad connects to hop3 Node : 26Mbps (Uplink RSSI : hop3 -62dBm / hop2 -68dBm / hop1 -55dBm)

- 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.

The screenshot displays the 'BACKHAUL NETWORK' dashboard. On the left, a diagram shows a mesh topology with 'Uplink(1)' connected to 'VigorAP903' (Root) and 'Rossi\_seat AP802' (Current Node). The root node shows a signal strength of -66 dBm and 60% battery. The current node shows MAC address 00:1D:AA:22:55:48. On the right, the 'WIRELESS OVERVIEW' panel shows settings for 2.4GHz: Radio is 'Enable', MAC is 00:1D:AA:22:55:48, and SSID(1) is 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%.



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

**DrayTek Syslog Utility**

Log 過濾器  
 關鍵字:   
 表用至: All

172.17.3.6 AP920R  
 LAN 資訊 傳送封包 接收封包  
 9756 47236

WAN 資訊  
 WAN1 傳送速率 接收速率  
 WAN IP (固定) 網橋 IP (固定)

APP Mesh 使用者存取紀錄 Channel Roaming Wireless 其他

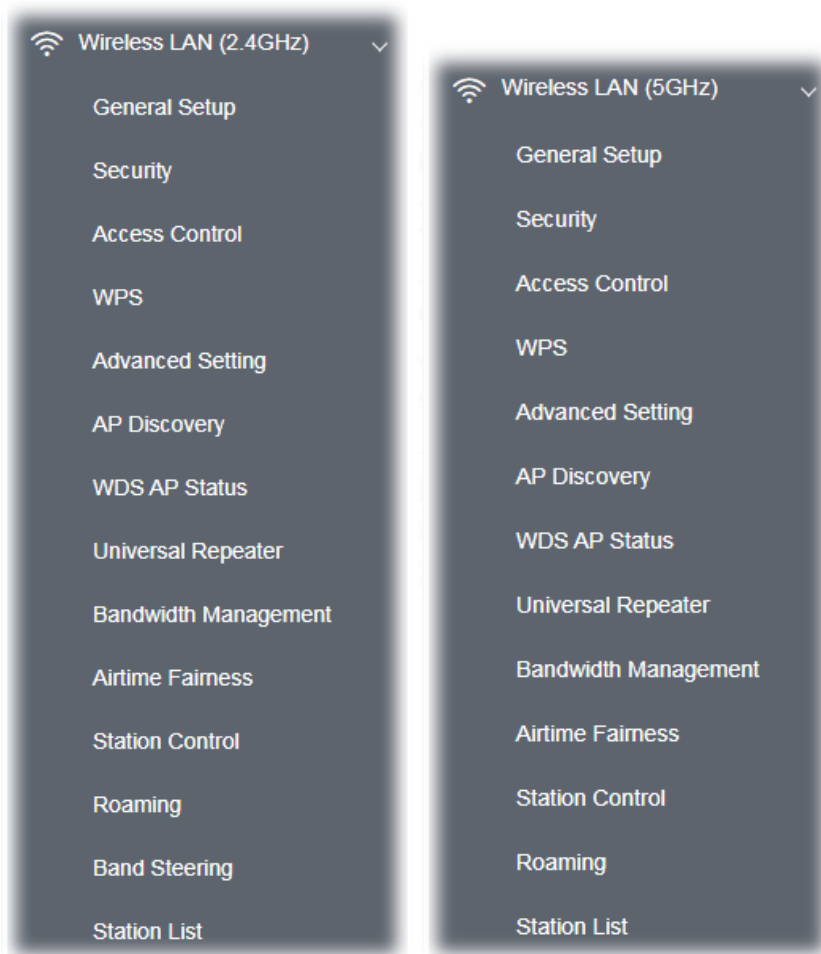
系統時間	路由器時間	主機	訊息
2018-11-08 19:01:16	Nov 8 10:58:05	syslog	[dnn] dnn_pkt_recv Announce-Keepalive
2018-11-08 19:01:15	Nov 8 10:58:04	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:01:04	Nov 8 10:57:52	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:01:01	Nov 8 10:57:50	syslog	[dnn] dnn_pkt_recv Announce-Keepalive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

## 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.

**i** Note:

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

Wireless LAN (5GHz) >> Universal Repeater

Universal Repeater Parameters

SSID	<input type="text"/>
MAC Address (Optional)	<input type="text"/>
Channel	5180MHz (Channel 36) ▾
Security Mode	WPA2/PSK ▾
Encryption Type	AES ▾
Pass Phrase	<input type="text"/>
Range Extender Band	None

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

Universal Repeater IP Configuration

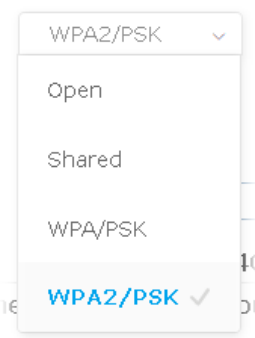
Connection Type	DHCP ▾
Router Name	AP802

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Universal Repeater Parameters</b>	
<b>SSID</b>	Display the SSID defined for Range Extender operation mode in Quick Start Wizard. Change the name of SSID whenever you want.
<b>MAC Address (Optional)</b>	Type the MAC address of access point that VigorAP 802 wants to connect to.
<b>Channel</b>	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 <b>AutoSelect</b> to let system determine for you.
<b>Security Mode</b>	There are several modes provided for you to choose. Each mode will



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

---

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	
<input checked="" type="checkbox"/> Enable DHCP Client	
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
<hr/>	
<input type="checkbox"/> Enable Management VLAN	
VLAN ID	0
<hr/>	
DNS Server IP Address	
Primary IP Address	<input type="text"/>
Secondary IP Address	<input type="text"/>

OK

Cancel

Available settings are explained as follows:

Item	Description
LAN IP Network	<b>Enable DHCP Client</b> - When it is enabled, VigorAP 802 will be treated

<b>Configuration</b>	<p>as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2862).</p> <p><b>IP Address</b> – Type in private IP address for connecting to a local private network (Default: 192.168.1.2).</p> <p><b>Subnet Mask</b> – Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p><b>Enable Management VLAN</b> – 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.</p> <ul style="list-style-type: none"> <li>● <b>VLAN ID</b> – Type the number as VLAN ID tagged on the transmitted packet. “0” means no VALN tag.</li> </ul>
<b>DNS Server IP Address</b>	<p><b>Primary IP Server</b> - 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.</p> <p><b>Secondary IP Server</b> - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.</p>

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

OK

Cancel

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.

This page is left blank.

# Chapter III Management

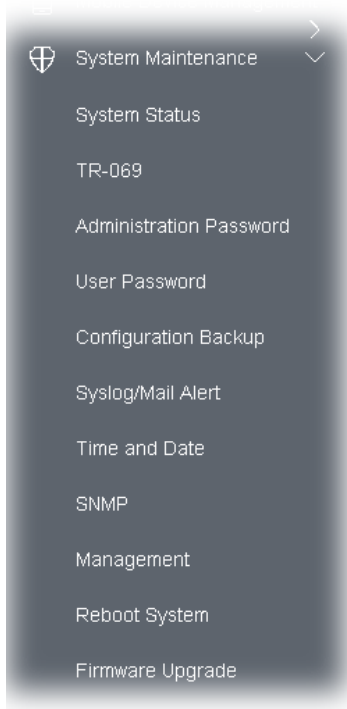


# III-1 System Maintenance

---

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          : VigorAP802
Firmware Version     : 1.3.1.1
Build Date/Time      : r11053 Tue Sep 24 13:36:13 CST 2019
System Uptime        : 0d 02:52:54
Operation Mode       : Range Extender
  
```

System	
Memory Total	: 62424 kB
Memory Left	: 16392 kB
Cached Memory	: 23876 kB / 62424 kB

LAN	
MAC Address	: 00:1D:AA:3F:47:64
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

Wireless LAN (2.4GHz)	
MAC Address	: 00:1D:AA:3F:47:64
SSID	: DrayTek-3F4764
Channel	: 11
Driver Version	: 2.7.2.0

Wireless LAN (5GHz)	
MAC Address	: 00:1D:AA:3F:47:65
SSID	: DrayTek-3F4764
Channel	: 36
Driver Version	: 3.0.3.2

**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
<b>Model /Device Name</b>	Display the model name of the modem.
<b>Firmware Version</b>	Display the firmware version of the modem.
<b>Build Date/Time</b>	Display the date and time of the current firmware build.
<b>System Uptime</b>	Display the period that such device connects to Internet.
<b>Operation Mode</b>	Display the operation mode that the device used.
<b>System</b>	
<b>Memory total</b>	Display the total memory of your system.
<b>Memory left</b>	Display the remaining memory of your system.
<b>LAN</b>	
<b>MAC Address</b>	Display the MAC address of the LAN Interface.
<b>IP Address</b>	Display the IP address of the LAN interface.
<b>IP Mask</b>	Display the subnet mask address of the LAN interface.
<b>Wireless LAN (2.4GHz/5GHz)</b>	
<b>MAC Address</b>	Display the MAC address of the WAN Interface.
<b>SSID</b>	Display the SSID of the device.
<b>Channel</b>	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	<input type="text"/>	Wizard
Username	<input type="text"/>	
Password	<input type="text"/>	
	Test With Inform	Event Code PERIODIC <input type="text"/>
Last Inform Response Time : <span style="color: red;">●</span>		

#### CPE Settings

Enable	<input type="checkbox"/>
SSL(HTTPS) Mode	<input type="checkbox"/>
URL	<input type="text" value="http://192.168.1.2:8069/cwm/CRN.html"/>
Port	<input type="text" value="8069"/>
Username	<input type="text" value="vigor"/>
Password	<input type="password" value="*****"/>

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

#### Periodic Inform Settings

Enable	<input checked="" type="checkbox"/>
Interval Time	<input type="text" value="900"/> second(s)

#### STUN Settings

<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Server Address	<input type="text"/>
Server Port	<input type="text" value="3478"/>
Minimum Keep Alive Period	<input type="text" value="60"/> second(s)
Maximum Keep Alive Period	<input type="text" value="-1"/> second(s)

OK Cancel

Available settings are explained as follows:

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

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

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

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

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

Available settings are explained as follows:

Item	Description
<b>Account</b>	Enter the name for accessing into web user Interface.
<b>Old Password</b>	Enter the old password for accessing into the web user interface.
<b>New Password</b>	Enter in new password in this filed.
<b>Confirm Password</b>	Enter the new password again for confirmation.
<b>Password Strength</b>	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

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
<b>Enable User Mode</b>	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.
<b>Account</b>	Enter a user name.
<b>Password</b>	Enter in new password in this field. The length of the password is limited to 31 characters.
<b>Confirm Password</b>	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.

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

Password (optional):

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

---

**Backup**

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

Protect with password

Password  (Max. 23 characters allowed)

Confirm Password

Available settings are explained as follows:

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

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	<input type="checkbox"/>
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="514"/>
Log Level	<input type="button" value="All"/> ▾

#### Mail Alert Setup

Enable	<input type="checkbox"/>
SMTP Server	<input type="text"/>
sysml ml smtp port	<input type="text"/>
Mail To	<input type="text"/>
Mail From	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Use TLS	<input checked="" type="checkbox"/>
Enable E-Mail Alert:	
<input checked="" type="checkbox"/> When Admin Login AP	

Available settings are explained as follows:

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



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	Inquire Time
---------------------	-------------------------	--------------

#### Time Setting

<input checked="" type="checkbox"/> Enable NTP Client	
Time Zone	(GMT+08:00) China Beijing, Chongqing
NTP Server	pool.ntp.org <span>Use Default</span>
Daylight Saving	<input type="checkbox"/>
NTP synchronization	1 day

**OK** Cancel

Available parameters are explained as follows:

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

<input checked="" type="checkbox"/>	Enable SNMP Agent
<input checked="" type="checkbox"/>	Enable SNMPV3 Agent
USM User	<input type="text"/>
Auth Algorithm	<input type="text" value="No Auth"/>
Auth Password	<input type="password"/>

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

OK

Cancel

Available settings are explained as follows:

Item	Description
<b>Enable SNMP Agent</b>	Check it to enable this function.
<b>Enable SNMPV3 Agent</b>	Check it to enable this function.
<b>USM User</b>	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.
<b>Auth Algorithm</b>	Choose one of the encryption methods listed below as the authentication algorithm.
<b>Auth Password</b>	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

---

**Access Control**

Allow management from WLAN

Enable Telnet Server

---

**Access List**

Enable access list

List	IP	Mask
1.	<input type="text"/>	255.255.255.255 / 32 <span style="float: right;">v</span>
2.	<input type="text"/>	255.255.255.255 / 32 <span style="float: right;">v</span>
3.	<input type="text"/>	255.255.255.255 / 32 <span style="float: right;">v</span>
4.	<input type="text"/>	255.255.255.255 / 32 <span style="float: right;">v</span>
5.	<input type="text"/>	255.255.255.255 / 32 <span style="float: right;">v</span>

**Port Setup**

HTTP Port  ( Default:80 )

HTTPS Port  ( Default:443 )

---

**Panel Control**

Disable LED

Enable Default Configuration Wizard

Available parameters are explained as follows:

Item	Description
<b>Device Name</b>	The default setting is VigorAP 802. Change the name if required.
<b>Access Control</b>	<p><b>Allow management from WLAN</b> - Enable the checkbox to allow system administrators to login from wireless LAN.</p> <p><b>Enable Telnet Server</b>- The administrator / user can access into the command line interface of VigorAP remotely for configuring settings.</p>
<b>Access List</b>	<b>Enable access list</b> – 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.
<b>Port Setup</b>	<b>HTTP port/HTTPS port</b> -Specify user-defined port numbers for the HTTP and HTTPS servers.
<b>Panel Control</b>	<p><b>Disable LED</b> - 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.</p> <p><b>Enable Default Configuration Wizard</b> – Default setting is enabled.</p>

---

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

OK

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

---

**i** Note:

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

---

## III-1-11 Firmware Upgrade

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

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

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

**System Maintenance >> Firmware Upgrade**

### Firmware Update

Select a firmware file.

Click Upgrade to upload the file.

### Firmware Version Status

[Refresh Latest Firmware](#)


Current Firmware Version	: 1.3.1.1	
The Latest Firmware Version	: N/A	<input type="button" value="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!



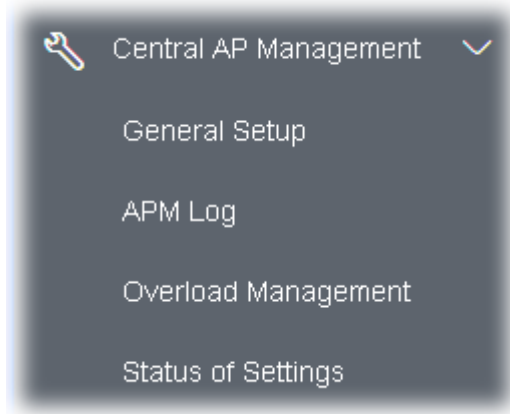
### Firmware Version Status

[Refresh Latest Firmware](#)

Current Firmware Version	: 1.3.1.1	
The Latest Firmware Version	: N/A	<input type="button" value="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

OK

Cancel

Available settings are explained as follows:

Item	Description
<b>Enable AP Management</b>	Check the box to enable the function of AP Management (APM).
<b>Enable Auto Provision</b>	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 <b>WLAN profile</b> 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
<b>White List</b>		
<b>Black List</b>		

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

<b>Comment</b>	Type a brief description for the specified client's MAC address.
<b>Add</b>	Add a new MAC address into the White List/Black List.
<b>Delete</b>	Delete the selected MAC address in the White List/Black List.
<b>Edit</b>	Edit the selected MAC address in the White List/Black List.
<b>Cancel</b>	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
<b>Load Balance</b>		
Station Number Threshold	X	
Max WLAN(2.4GHz) Station Number		32
Max WLAN(5GHz) Station Number		32
Traffic Threshold	X	
Upload Limit		None bps
Download Limit		None bps
Force Overload Disassociation	X	
Disassociate By		None
RSSI Threshold		-50 dBm
<b>Rogue AP Detection</b>		
Rogue AP Detection	X	

"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.

**AP Load Balance**

By Station Number or Traffic

**Station Number Threshold**

---

Wireless LAN (2.4GHz)  (3-128)

Wireless LAN (5GHz)  (3-128)

**Traffic Threshold**

---

Upload Limit   bps (Default unit: K)

Download Limit   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 -  dBm (  %)

## 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 Detection


Such page displays mobile device(s) detected by VigorAP. Detected device(s) with Policy – **Pass** can access into the wireless LAN offered by VigorAP. Detected device(s) with Policy – **Block** are not allowed to access into Internet via VigorAP's WLAN.

Mobile Device Management >> Detection

Refresh Seconds:  Page:  | [Refresh](#) |

Index	OS	MAC	Vendor	Model	Policy
1		40:49:0F:06:E0:0D	HonHaiPr	PC	Pass
2		8C:3A:E3:40:F6:73	LgElectr	LG	Block
3		F8:95:EA:EA:45:93	Apple	iPad	Block
4		7C:1D:D9:64:5C:4C	Xiaomi	HM NOTE	Block

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

 iOS  Android  Windows  Linux  Others

#### Trademark Notice and Attribution:

- The Android robot is reproduced or modified from work created and shared by Google and used according to the terms described in the [Creative Commons 3.0 Attribution License](#).
- Android is a trademark of Google Inc..
- Tux logo was created by [Larry Ewing](#) and [The GIMP](#) in 1996.
- Windows and windows logo are registered trademark of Microsoft Corporation in the United States and/or other countries.
- Apple, Apple logo, iPad, iPhone, iPod, Mac OS and iTunes are trademarks of Apple Inc., registered in the U.S. and other countries.
- IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- All other brands and trademarks are the properties of their respective owners.

Once you check/uncheck the box of **Enable Mobile Device Management** and click **OK**, VigorAP will reboot automatically to activate MDM.

At present, OS (for mobile device) categories supported by VigorAP include:

- Windows
- Linux
- iOS
- Andorid
- WindowsPhone
- BlackBerry
- Symbian

### III-3-2 Policies

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

#### Mobile Device Management >> Policy

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

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

Block Unknown Connections (OS:Others)

---

WiFi(2.4GHz)  SSID1  SSID2

WiFi(5GHz)  SSID1  SSID2

Each item is explained as follows:

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

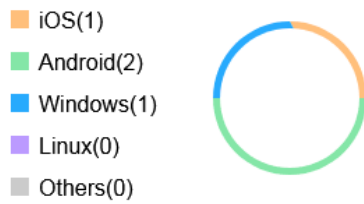
After finished the policy selection, click **OK**. VigorAP will *reboot* to activate the new policy automatically.

### III-3-3 Statistics

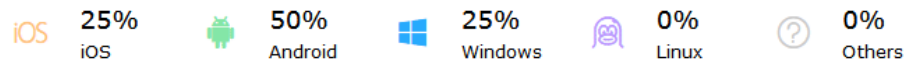
The number of detected devices and the number of device(s) passed/blocked according to the policy specified in **Mobile Device Management>>Policy** can be illustrated as doughnut chart.

Mobile Device Management >> Statistics

#### Device OS Statistics



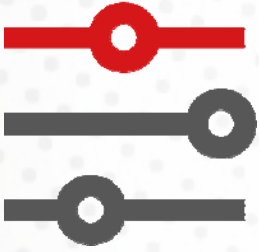
#### Policy Statistics



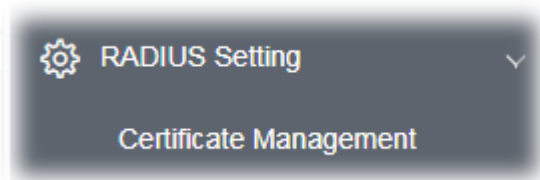
#### Trademark Notice and Attribution:

- The Android robot is reproduced or modified from work created and shared by Google and used according to the terms described in the [Creative Commons 3.0 Attribution](#) License.
- Android is a trademark of Google Inc..
- Tux logo was created by [Larry Ewing](#) and [The GIMP](#) in 1996.
- Windows and windows logo are registered trademark of Microsoft Corporation in the United States and/or other countries.
- Apple, Apple logo, iPad, iPhone, iPod, Mac OS and iTunes are trademarks of Apple Inc., registered in the U.S. and other countries.
- IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- All other brands and trademarks are the properties of their respective owners.

# 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.



<b>Certificate Name</b>	Root CA
<b>Subject Name</b>	
Country (C)	<input type="text"/>
State (S)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
<b>Key Type</b>	RSA <input type="button" value="v"/>
<b>Key Size</b>	1024 Bit <input type="button" value="v"/>
<b>Apply to Web HTTPS</b>	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
<b>Subject Name</b>	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.
<b>Key Type</b>	At present, only RSA (an encryption algorithm) is supported by such device.
<b>Key Size</b>	To determine the size of a key to be authenticated, use the drop down list to specify the one you need.
<b>Apply to Web HTTPS</b>	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:

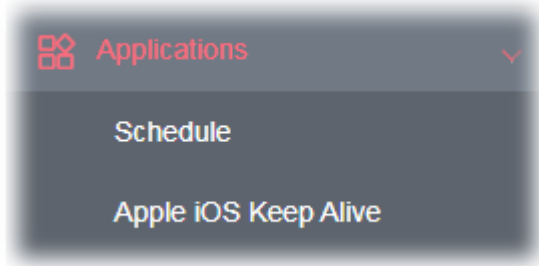
“Common Name” must be configured with router’s WAN IP or domain name.

---

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

# IV-2 Applications

Below shows the menu items for Applications.

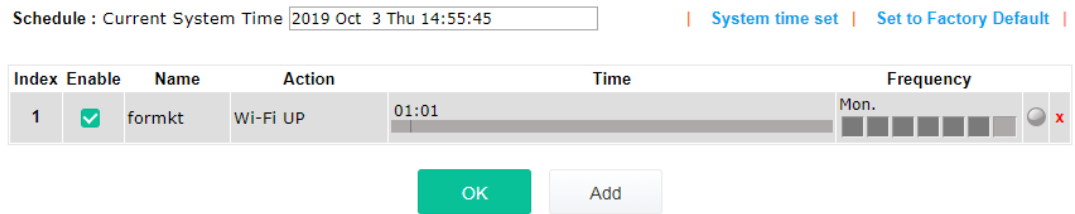


## IV-2-1 Schedule

The VigorAP has a built-in clock 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



Available settings are explained as follows:

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

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

Start Date  -  -  ( Year - Month - Day )

Start Time  :  ( Hour : Minute )

Duration Time  :  ( Hour : Minute )

End Time  :  ( Hour : Minute )

Action

WiFi(2.4GHz)  Radio  SSID2

WiFi(5GHz)  Radio  SSID2

Acts

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.

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check to enable such schedule profile.
<b>Name</b>	Enter the name of the profile.
<b>Start Date</b>	Specify the starting date of the schedule.
<b>Start Time</b>	Specify the starting time of the schedule.
<b>Duration Time</b>	Specify the duration (or period) for the schedule. It is available when <b>Wi-Fi UP</b> or <b>Wi-Fi DOWN</b> is selected as <b>Action</b> .
<b>End Time</b>	Specify the ending time of the schedule.

<b>Action</b>	Specify which action (Auto Reboot, Wi-Fi UP, Wi-Fi DOWN, LED DISABLE, LED ENABLE) should apply the schedule.
<b>WiFi(2.4GHz)/ WiFi(5GHz)</b>	When <b>Wi-Fi UP</b> or <b>Wi-Fi DOWN</b> is selected as <b>Action</b> , you can check the Radio or SSID 2 box to setup the network based on the schedule profile. <b>Note:</b> When Radio is selected, SSID2 is not available for choosing, vice versa. Moreover, SSID2 is not available for choosing if it is not enabled.
<b>Acts</b>	Specify how often the schedule will be applied. <b>Once</b> -The schedule will be applied just once <b>Routine</b> -Specify which days in one week should perform the schedule.
<b>Weekday</b>	Choose and check the day to perform the schedule. It is available when <b>Routine</b> is selected as <b>Acts</b> .

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  | [System time set](#) | [Set to Factory Default](#) |

Index	Enable	Name	Action	Time	Frequency
1	<input checked="" type="checkbox"/>	formkt	Wi-Fi UP	01:01	Mon. <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

## 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
<b>Enable Apple iOS Keep</b>	Check to enable the function.

<b>Alive</b>	
<b>Index</b>	Display the setting link. Click the index link to open the configuration page for setting the IP address.
<b>Apple iOS Keep Alive IP Address</b>	Display the IP address.

Click **OK** to save the settings.

# Chapter V Troubleshooting



# V-1 Diagnostics

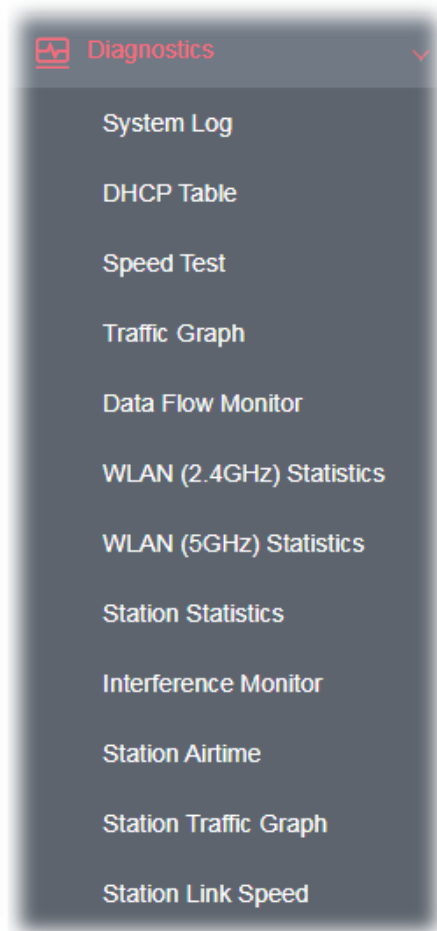
---

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.

Dagnostic 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.

[Diagnostics >> System Log](#)

System Log Information

| [Clear](#) | [Refresh](#) |  [Line wrap](#) |

```
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 DHCP Table List

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics >> DHCP Table** to open the web page.

[Diagnostics >> DHCP Table List](#)

DHCP Table

| [Refresh](#) |

Host Name (optional)	IP Address	MAC Address	Expire Time
----------------------	------------	-------------	-------------

## V-1-3 Speed Test

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

Diagnostics >> Speed Test

### Speed Test

Welcome to VigorAP802 Speed Test.

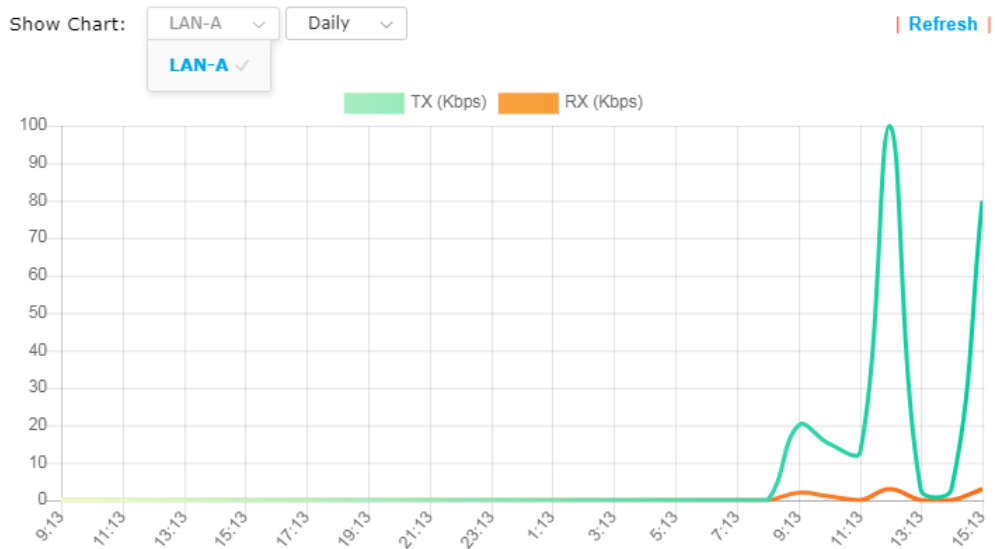
This test allows you to find out the best place for VigorAP802. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference.

Start

## V-1-4 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



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

# V-1-5 Data Flow Monitor

This page displays general information for the client connecting to VigorAP 802.

Diagnostics >> Data Flow Monitor

Page: 1 Auto-refresh  Refresh

Index	MAC Address	Station	TX rate(Kbps)	RX rate(Kbps)	2.4G / 5G	Action
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Total			0	0	0 / 0	

Available parameters are explained as follows:

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

## V-1-6 WLAN (2.4GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (2.4GHz) Statistics

Auto-Refresh **Refresh**

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

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

## V-1-7 WLAN (5GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (5GHz) Statistics

Auto-Refresh

Refresh

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

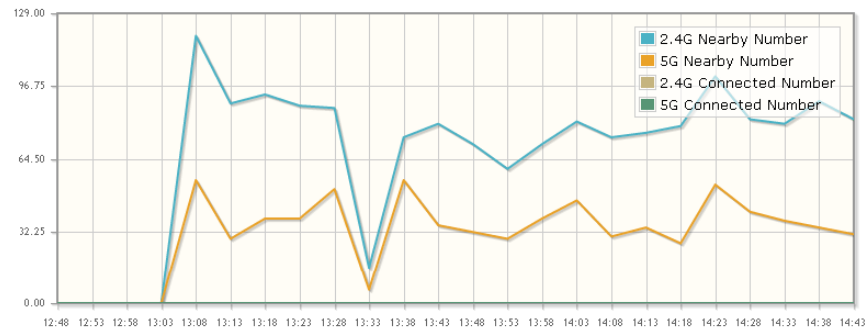
## V-1-8 Station Statistics

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

Diagnostics >> Station Statistics

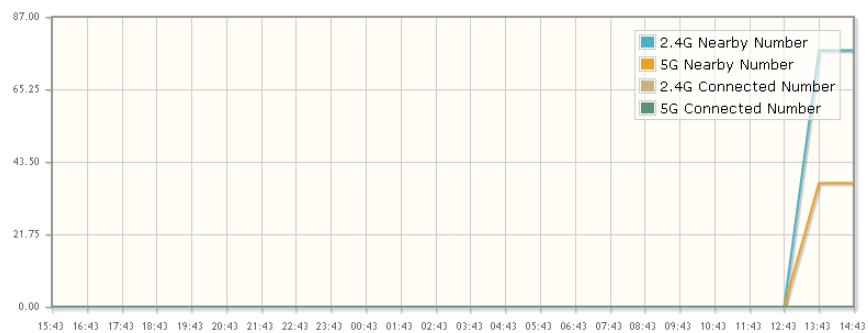
Show Chart:  | Refresh |

### Hourly Nearby & Connected Number



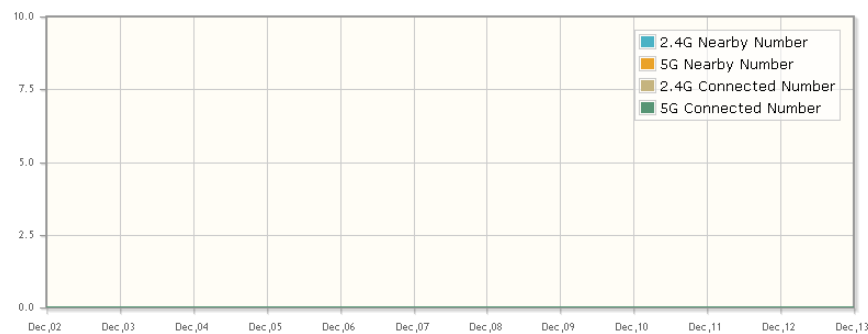
### Daily Nearby & Connected Number

[Daily Connected Number Analysis](#)



### Weekly Nearby & Connected Number

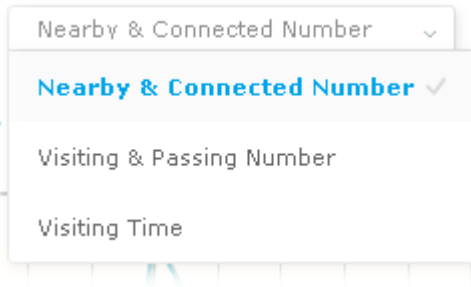
[Weekly Connected Number Analysis](#)



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

Available parameters are explained as follows:

Item	Description
Show Chart	Choose one of the items to display the statistics chart for wireless stations.



**Nearby & Connected Number** – Choose it to have the statistics of the wireless stations which is nearby and connected to VigorAP 802.

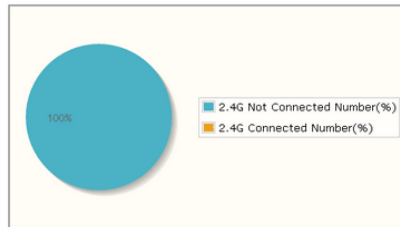
**Visiting & Passing Number** – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP 802.

**Visiting Time** - Choose it to have the statistics of the wireless stations which is visiting VigorAP 802.

**Daily Connected Number Analysis / Daily Visiting Number Analysis**

Click this button to get analysis pie chart for daily connected wireless stations / daily visiting wireless station.

Daily 2.4G Connected & Not Connected Number Analysis



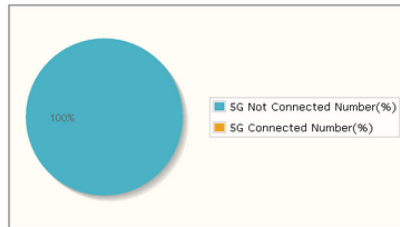
**Peak of Connected Station Number:**  
Time: 14:58-13:58 Number: 0

**Off-peak of Connected Station Number:**  
Time: 14:58-13:58 Number: 0

**Peak of Nearby Station Number:**  
Time: 19:58-20:58 Number: 12

**Off-peak of Nearby Station Number:**  
Time: 14:58-17:58 Number: 0

Daily 5G Connected & Not Connected Number Analysis



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

**Off-peak of Connected Station Number:**  
Time: 14:58-13:58 Number: 0

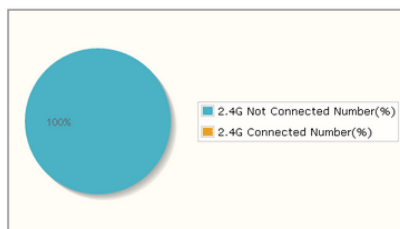
**Peak of Nearby Station Number:**  
Time: 19:58-20:58 Number: 3  
Time: 13:58 Number: 3

**Off-peak of Nearby Station Number:**  
Time: 14:58-17:58 Number: 0

**Weekly Connected Number Analysis / Weekly Visiting Number Analysis**

Click this button to get analysis pie chart for weekly connected wireless stations / weekly visiting wireless station.

Weekly 2.4G Connected & Not Connected Number Analysis



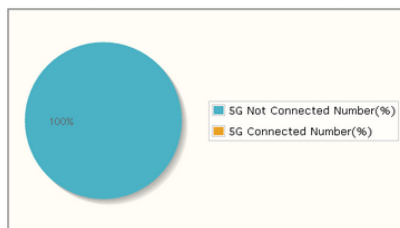
**Peak of Connected Station Number:**  
Time: 2015-8-22(Sun)-2015-9-3(Thu) Number: 0

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

**Peak of Nearby Station Number:**  
Time: 2015-9-2(Wed) Number: 4

**Off-peak of Nearby Station Number:**  
Time: 2015-8-22(Sun)-2015-9-2(Wed) Number: 0  
Time: 2015-9-3(Thu) Number: 0

Weekly 5G Connected & Not Connected Number Analysis



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

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

**Peak of Nearby Station Number:**  
Time: 2015-9-2(Wed) Number: 1

**Off-peak of Nearby Station Number:**  
Time: 2015-8-22(Sun)-2015-9-2(Wed) Number: 0  
Time: 2015-9-3(Thu) Number: 0

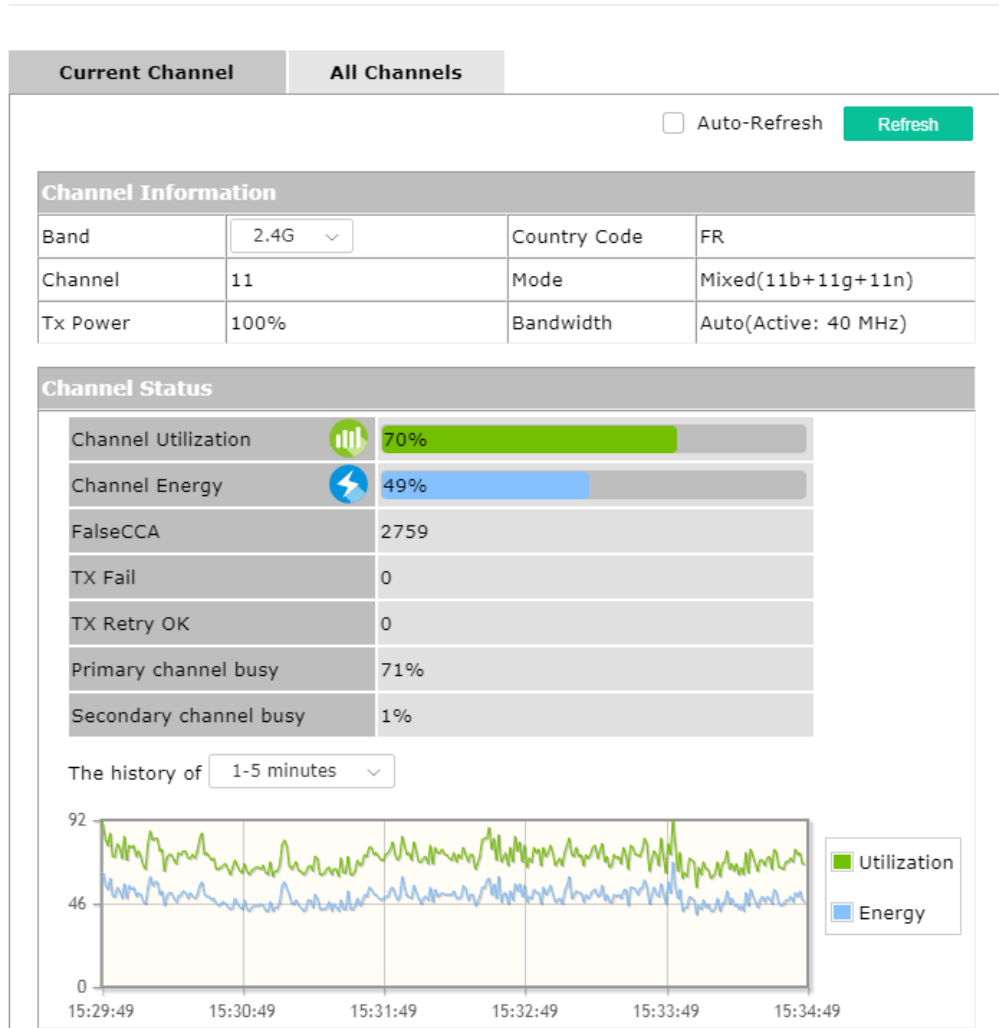
## V-1-9 Interference Monitor

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

### Current Channel

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

Diagnostics >> Interference Monitor





## All Channels

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

**Diagnostics >> Interference Monitor**

**Current Channel** | **All Channels**

Band:  Refresh

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.

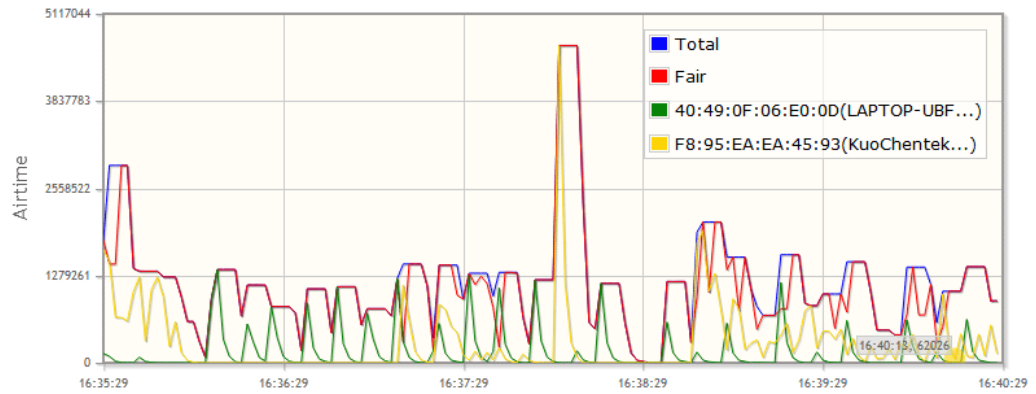
# V-1-10 Station Airtime

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

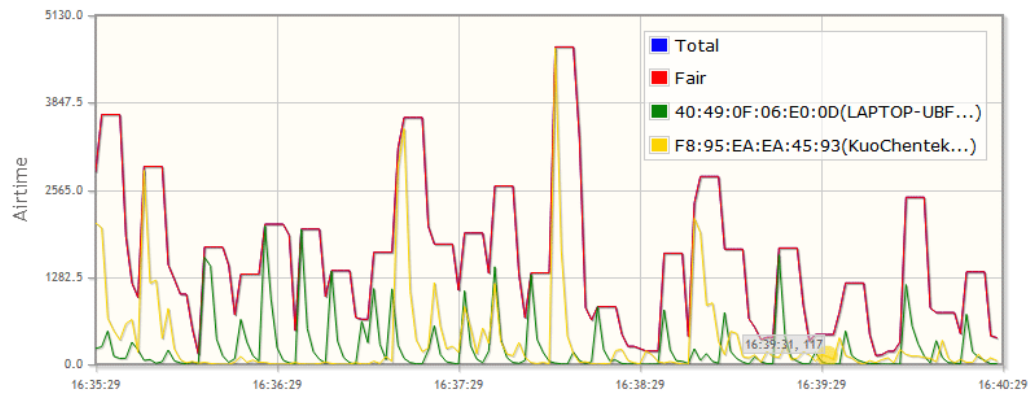
Diagnostics >> Station Airtime

Display:  and the history of  Airtime [Refresh](#)

## 5GHz Tx Airtime



## 5GHz Rx Airtime



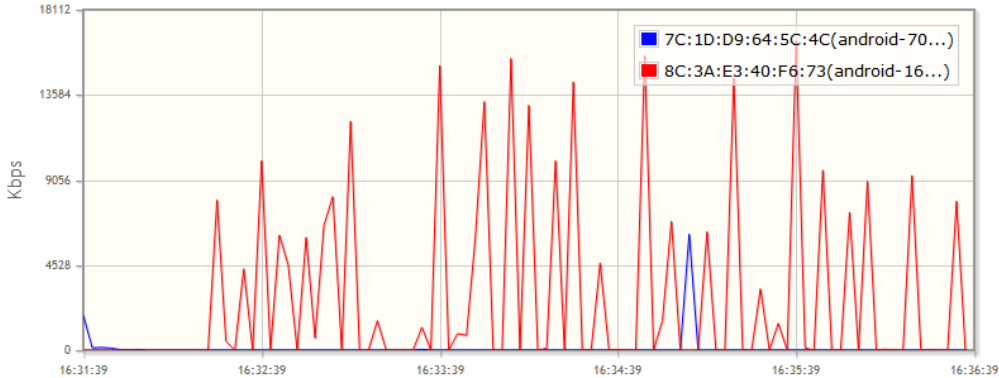
# V-1-11 Station Traffic Graph

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

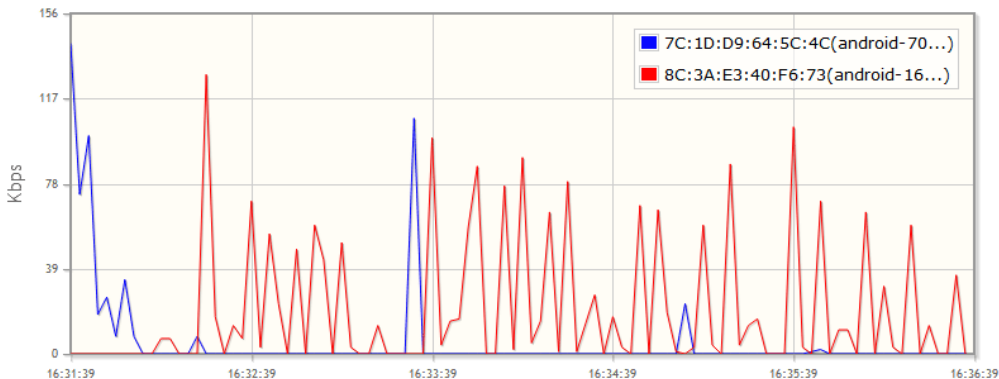
Diagnostics >> Station Traffic Graph

Display:   and the history of  Throughput [Refresh](#)

### 2.4GHz Tx Throughput



### 2.4GHz Rx Throughput



## V-1-12 Station Link Speed

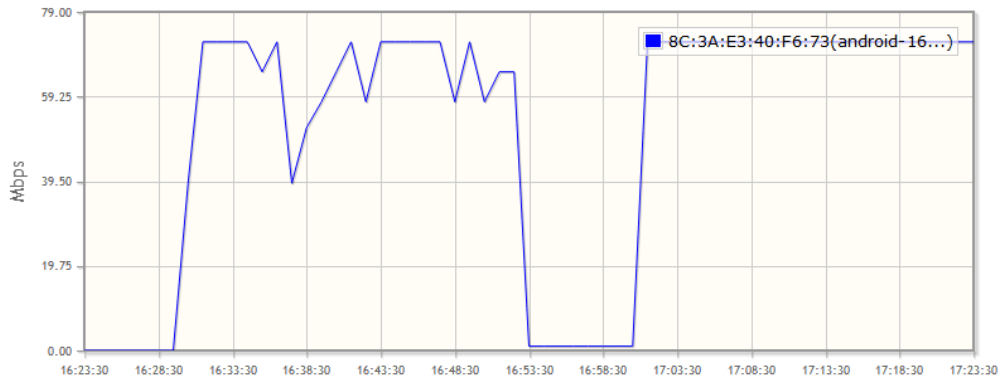
This page displays the link rate status for 2.4GHz/5GHz wireless stations within one hour with a run chart.

Diagnostics >> Station Link Speed

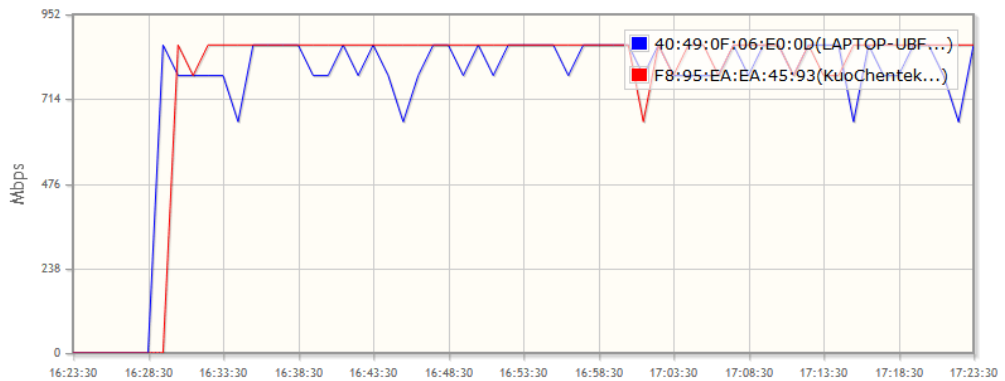
Display:  link rate

[Refresh](#)

### 2.4GHz Link Speed

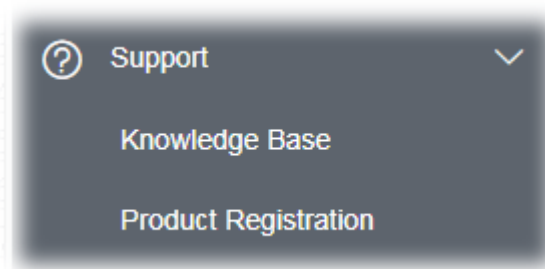


### 5GHz Link Speed



## V-1-13 Support Area

When you click **Support Area**, you will be guided to visit [www.draytek.com](http://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 still failed, please do the steps listed below to make sure the network connection settings is OK.

### V-3-1 For Windows

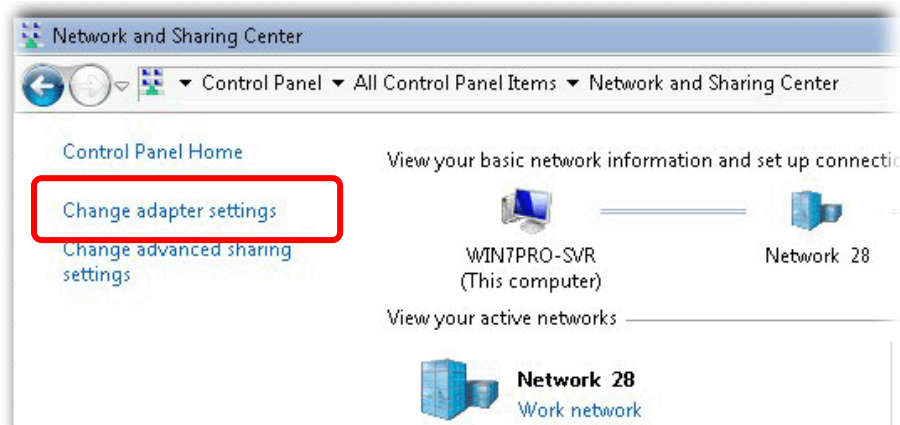
**Note:**

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](http://www.draytek.com).

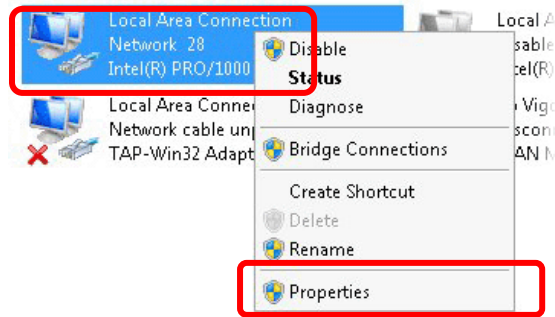
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



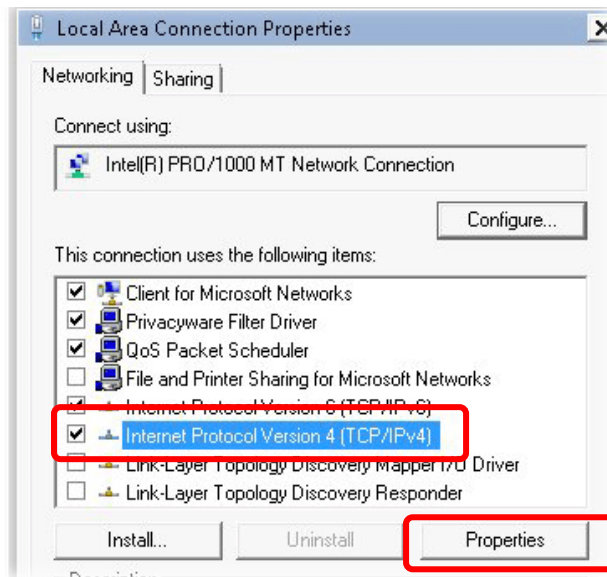
2. In the following window, click **Change adapter settings**.



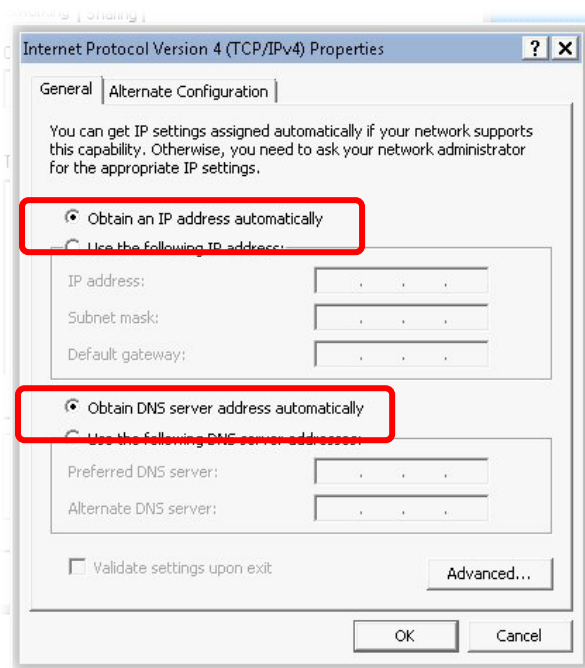
- Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

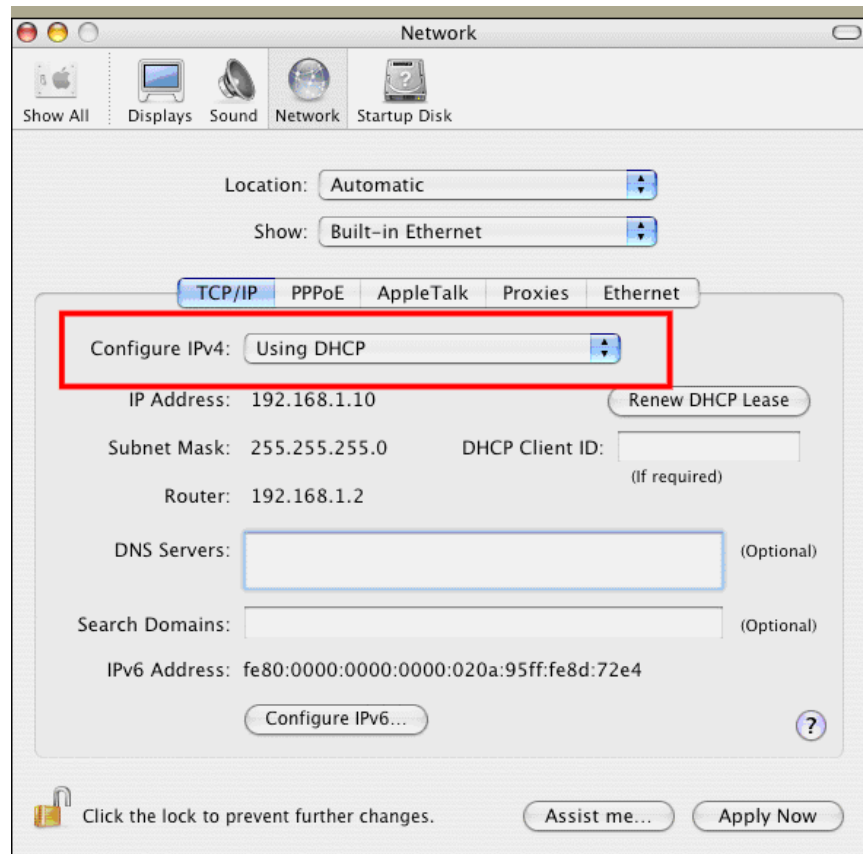


- Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



## 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.





## V-4 Pinging the Device

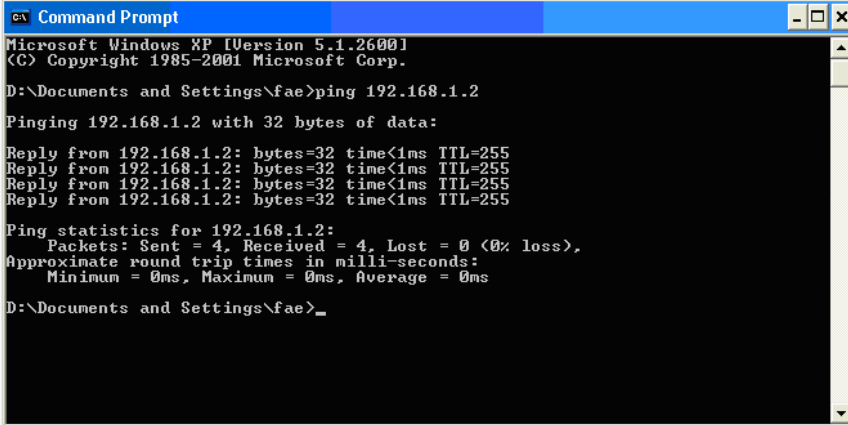
---

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.



```
ex Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
D:\Documents and Settings\fae>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
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.

```
Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttty1
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 lose 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

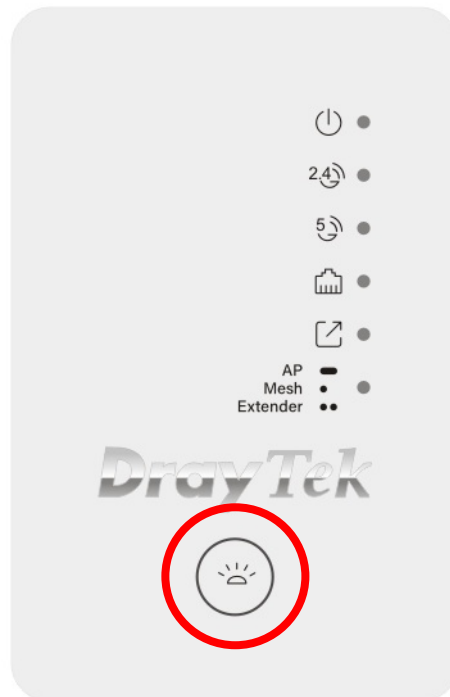
Using factory default configuration

**OK**

## 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](mailto:support@draytek.com).

# Index

## 8

802.11n, 33

802.1x, 35

## A

Access Control, 37

Action, 103

Advanced Setting, 39

AES, 23

Airtime Fairness, 44

Antenna, 40

AP Discovery, 42

AP Management, 1, 89

AP Mode, 31, 57, 65

AP Operation Mode, 17

APM Log, 90

Apple iOS Keep Alive, 103

Applications, 101

Auth Mode, 38

Auto Adjustment, 44

Auto Channel Filtered Out List, 40

Auto Logout, 13

Auto Provision, 89

AutoSelect, 66

## B

Band Steering, 50

Bandwidth Limit, 18, 22

Bandwidth Management, 43

Black List, 91

## C

Central AP Management, 89

Certificate Management, 98

Changing Password, 14

Channel, 33, 66

Channel Width, 39

Client PinCode, 39

Client's MAC Address, 91

Configuration Backup, 79, 80

Connection Time, 47

Connection Type, 67

Country Code, 40

## D

Data Flow Monitor, 109

Daylight Saving, 83

Default Gateway, 67

Detection, 94

DHCP Client, 69

DHCP server, 11

DHCP Table, 107

Download Limit, 44

## E

Encryp Type, 38

End Time, 102

Extension Channel, 33

## F

Factory Default Setting, 125

Fast Roaming, 49

Firmware Upgrade, 88

Force Overload Disassociation, 91

Fragment Length, 40

## G

General Setup, LAN, 69

## H

Hardware Reset, 126

Hide SSID, 33

HTTP port, 85

HTTPS, 99

HTTPS port, 85

## I

Interference Monitor, 114

IP Address, 67, 69

Isolate Member, 33

## **K**

Keep Alive Period, 77

Key Renewal Interval, 35

Key Size, 99

Key Type, 99

## **L**

LAN, 69

LED Indicators and Connectors, 3

Limit Client, 32

Limit Client per SSID, 33

Load Balance, 91

## **M**

MAC Address, 66

MAC Address Filter, 38

MAC Clone, 41

Main SSID, 17, 21

Management, 85

Management VLAN, 69

Mobile Device Management, 94

Mode, 33, 34

## **N**

NTP, 101

NTP Client, 83

NTP Server, 83

NTP synchronization, 83

## **O**

Once, 103

Open/Shared, 23, 67

Operation Mode, 26

Overload Management, 91

## **P**

Packet-OVERDRIVE, 40

Pass Phrase, 35, 67

Password, 14

Password Strength, 78

Periodic Inform Settings, 77

PIN Code, 29

PMK Cache Period, 49

Policy, 37, 95

Port, 36

Port Control, 71

Pre-Authentication, 49

PSK, 28

Push Button, 39

## **Q**

Quick Start Wizard, 16

## **R**

RADIUS Server, 35

RADIUS Setting, 98

Reboot System, 87

Reconnection Time, 47

Restore, 38

Roaming, 48

Router Name, 67

Routine, 103

RSSI, 48

RTS Threshold, 40

## **S**

Schedule, 101

Security, 34

Security Mode, 66

Security Overview, 28

Security Settings, 34

Session Timeout, 36

Shared Secret, 36

Show Chart, 112

Software Reset, 125

Speed Test, 107, 108

SSL(HTTPS), 77

Start Date, 102

Start PBC, 29

Start Time, 102

Station Airtime, 116

Station Control, 18, 22, 46

Station Link Speed, 118

Station List, 55

Station Statistics, 112

Station Traffic Graph, 117  
Statistics, 96  
Status of Settings, 92  
STUN, 77  
Subject Name, 99  
Subnet Mask, 67, 69  
Support Area, 118  
Syslog/Mail Alert, 82  
System Log, 107  
System Maintenance, 74  
System Status, 75

## **T**

Time and Date, 83  
Time Zone, 83  
TKIP, 23, 28  
Total Download Limit, 44  
Total Upload Limit, 44  
TR-069, 76  
Traffic Graph, 108  
traffic overload, 91

Triggering Client Number, 45  
Tx Power, 40

## **U**

Upload Limit, 43

## **V**

VLAN ID, 33, 69

## **W**

WEP, 23  
WEP (Wired Equivalent Privacy), 28  
White List, 91  
Wi-Fi DOWN, 102, 103  
Wi-Fi UP, 102, 103  
Wireless LAN (2.4GHz/5GHz), 28  
WLAN (2.4GHz) Statistics, 110  
WLAN (5GHz) Statistics, 111  
WPA (Wi-Fi Protected Access), 28  
WPA Algorithms, 35  
WPS, 38  
WPS (Wi-Fi Protected Setup), 28