VigorAP 962C

802.11ax Ceiling-mount Access Point

User's Guide

Version: 1.0

Firmware Version: V1.5.4

Date: June 12, 2024

Intellectual Property Rights (IPR) Information

Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

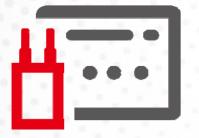
Safety Instructions	 Read the installation guide thoroughly before you set up the device. The device is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the device yourself. Do not place the device in a damp or humid place, e.g. a bathroom. The device should be used in a sheltered area, within a temperature range of +0 to +40 Celsius. Do not expose the device to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources. Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards. Do not power off the device when saving configurations or firmware upgrades. It may damage the data in a flash. Please disconnect the Internet connection on the device before powering it off when a TR-069/ ACS server manages the device. Keep the package out of reach of children. When you want to dispose of the device, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the device will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.
Be a Registered Owner	Web registration is preferred. You can register your Vigor router via https://myvigor.draytek.com.
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all devices will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents. https://www.draytek.com

Table of Contents

Chapter I Installation	v
I-1 Introduction	1
I-1-1 LED Indicators and Connectors	2
I-2 Hardware Installation	3
I-2-1 Ceiling-mount Installation (from A to C) I-2-2 Wall-mount Installation (from A to C) I-2-3 Notifications for Hardware Connection	3
I-3 Network IP Configuration	
I-3-1 Windows 10 IP Address Setup	
I-4 Accessing to Web User Interface	
I-5 Changing Password	
I-6 Dashboard	
Chapter II Connectivity	
II-1 Configuration	
II-1-1 Physical Interface	
II-1-2 LAN II-1-2-1 LAN Networks	
II-1-2-2 Bind IP to MAC	
II-1-2-3 DHCP Options	
II-1-2-4 VLAN List	
II-1-2-5 Interface VLAN	
II-1-3 Wireless LAN	
II-1-3-1 SSID	
II-1-3-2 Radio Settings II-1-3-3 Roaming	
II-1-3-4 AP Discovery	
II-1-3-5 WPS	
II-1-3-6 Range Extender	
II-1-3-7 WDS	
II-1-4 Objects	
II-1-4-1 Schedule	
II-1-5 Notification Services II-1-6 RADIUS	
II-1-6 RADIOS	
II-1-7-1 Local Certificates	
II-1-7-2 Trusted CA	
II-1-7-3 Local Services	54
II-1-7-4 Backup & Restore	55
II-2 Security	56
II-2-1 MAC Filtering Profile	56
II-2-1-1 MAC Filtering Profile	
II-2-1-2 Backup & Restore	58
II-3 Virtual Controller - Wireless	59
II-3-1 Role Setup	
II-3-2 Device	
II-3-2-1 Device List	
II-3-2-2 Mesh Status II-3-2-3 AP Adoption	
Chapter III Management	71

III-1 System Maintenance	
III-1-1 Device Settings	
III-1-1-1 Time	
III-1-1-2 Device Name	74
III-1-1-3 Syslog	
III-1-1-4 SNMP	
III-1-2 Management	
III-1-2-1 Service Control	
III-1-2-2 TR-069 III-1-2-3 System Information	
III-1-2-5 System Information	
III-1-4 Backup and Restore	
III-1-5 Accounts & Permission	
III-1-5-1 Local Admin Account	
III-1-5-2 Role & Permission	
III-1-6 System Reboot	
Chapter IV Others	92
IV-1 Monitoring	
IV-1-1 DHCP Table	
IV-1-1-1 IPv4 DHCP Subnet	
IV-1-1-2 IPv4 DHCP Lease	
IV-1-2 ARP Table	
IV-1-3 Web Syslog	
IV-1-4 Clients List	
IV-2 Utility	
IV-2-1 Ping Tool	
IV-2-2 Trace Tool	
IV-2-3 Web CLI	
Chapter V Mobile APP, DrayTek Wireless	100
V-1 Introduction of DrayTek Wireless	101
V-2 Create a New Network	
V-3 Wizard	
V-4 Login	
V-4-1 Setup	
Chapter VI Troubleshooting	110
VI-1 Checking the Hardware Status	
VI-2 Checking the Network Connection Settings	
VI-3-1 For Windows	
VI-3-2 For Mac Os	
VI-3 Pinging the Device	115
VI-3-1 For Windows	
VI-3-2 For Mac Os (Terminal)	115
VI-4 Backing to Factory Default Setting	
VI-4-1 Software Reset	117
VI-4-2 Hardware Reset	
VI-5 Contacting DrayTek	

Chapter I Installation



I-1 Introduction

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

Thank you for purchasing this VigorAP 962C!

VigorAP 962C can operate in standalone mode for your office network or a classroom; connected to your LAN and offering you wireless access.

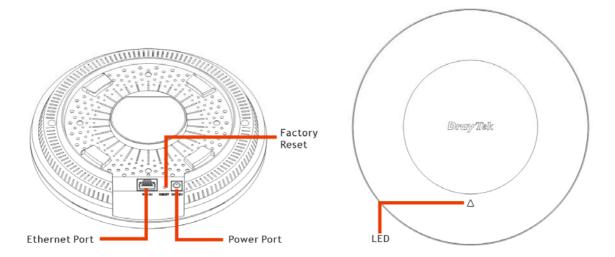
It makes high density with quality-performance be feasible for users as it is going to be implemented with DrayTek VigorACS supports configuration, firmware upgrade, status, and monitoring.

The Power of Ethernet (PoE) on VigorAP 962C relieves the installation of the power plug. The massive deployment of VigorAP 962C for hospitalities and school environment will be much easier.

With the optimized antennas built-in, DrayTek VigorAP 962C ceiling-mount wireless access point is ideal for hospitalities, small offices, and small campus.

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

I-1-1 LED Indicators and Connectors



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

LED	Status	Explanation
Orange LED	On	The system is in boot-loader mode.
	Blinking	The system is in TFTP mode.
Blue LED	Blinking	The system is in AP mode and work normally.
Red LED	Blinking	System error.
Off	Off	VigorAP is turned off or not functioning.
Interface		Explanation
Ethernet Port	:	Connects to LAN or router.
		Supports PoE power & Gigabit (2.5G).
Power Jack (D	DC IN)	Connecter for a power adapter.
Hole		Explanation
Factory Reset		Restores the unit back to factory default settings.
		To use, insert a small item such as an unbent paperclip into the hole. You will feel the button inside depress gently. Hold it for 5 seconds.
		The VigorAP will restart with the factory default configuration and the LED will blink blue.

I-2 Hardware Installation

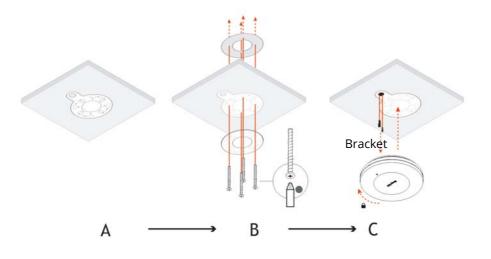
This section will guide you through installing the VigorAP.

VigorAP can be installed under certain locations: wooden ceiling, plasterboard ceilings, light-weighted steel frame and wall.

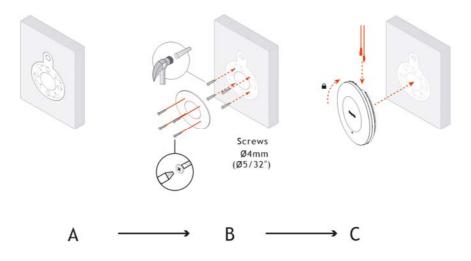
(i) Note:

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

I-2-1 Ceiling-mount Installation (from A to C)



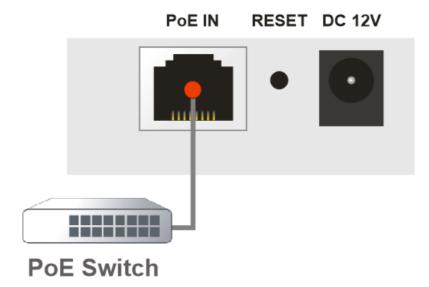
I-2-2 Wall-mount Installation (from A to C)



I-2-3 Notifications for Hardware Connection

- PoE IN RESET DC 12V
- Connect VigorAP to Vigor router (via LAN port) with Ethernet cable.

• Connect VigorAP to the PoE switch (via LAN port) with an Ethernet cable for getting the power from the switch directly. While connecting with a PoE switch, the power adapter is not necessary but optional.



I-3 Network IP Configuration

After the network connection is built, the next step you should do is setup VigorAP 962C with proper network parameters, so it can work properly in your network environment.

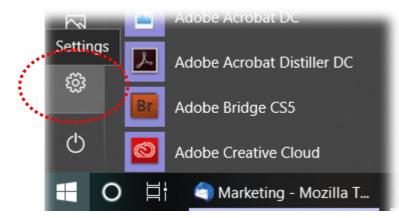
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address in the same subnet as this AP. If it's not connected to the same DHCP Server with the AP or you're unsure, please follow the following instructions to configure your computer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

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

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

I-3-1 Windows 10 IP Address Setup

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



Double-click Network & Internet.



Next, click Change adapter options.

Settings		- 0
	Windows Settings	
	Find a setting	
<- Settings		- 0
G Home	Status	
Find a setting	Network status	Do you have a question? Get help
Network & Internet	$\Box = \Box = \bigoplus$	
🕏 Status	3.135-1 Public network	Make Windows better
12 Ethernet	You're connected to the Internet	
한 Dial-up	If you have a limited data plan, you can make this network a metered connection or change other properties.	
% VPN	Change connection properties	
🕑 Data usage	Show a stillar activity	
Proxy	Change your network settings	
	Change adapter options View network adapters and change connection settings.	
	Sharing options For the networks that you consists the decide what you want to share.	
	Network troubleshooter Tanona and fin returns anothers	



Settings			- a
	Windows Settings		
	Find a setting P		
- Settings			- 0
⇔ Home	Status		0
Find a setting	Network status		Do you have a question? Get help
Network & Internet			Make Windows better
🔛 Ethernet	Public network	0	Give us feedback
🕾 Dial-up		Search Ne	<i>p</i>
% VPN		• 🖬	0
🕑 Data usage	Zod Bit 7 Minorit Cable unplugged Minorit Cab		
Proxy	and the second sec		

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

🖳 Local Area Connection Properties	x
Networking Sharing	
Connect using:	
Realtek RTL8139/810x Family Fast Ethernet NIC	
Configure	
This connection uses the following items:	
Client for Microsoft Networks	ן ך
🗹 📮 QoS Packet Scheduler	
File and Printer Sharing for Microsoft Networks	
Internet Protocol Version 6 (TCP/IP+6),	
 Internet Protocol Version 4 (TCP/IPv4) 	
Link-Layer Topology Discovery Resigneder	
	5
Install Uninstall Properties	.
Description	h
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
OK Cancel	

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

IP address: 192.168.1.9

Subnet Mask: 255.255.255.0

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

I-4 Accessing to Web User Interface

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

- 1. Make sure your PC connects to the VigorAP 962C 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.

	Username admin	
DrayTek VigorAP962C	Password	0
VigorAP962C		
	Log	m

(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 962C.**

- If there is no DHCP server on the network, then VigorAP 962C will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 962C will receive it's IP address via the DHCP server.
- 3. Next, the page will appear to guide you change the login password.

You **MUST** change the login password before accessing the web user interface. Please set a new password for network security.

LIGHT	admin / Set Password	
Change Password	Account	admin
	Current: Password	0
Your device is still using default password.	New Password	
For security reason please change password.	Confirm New Password	
		- Uppercase characters
		- Cowercase characters
Change password		 Formbers or Special characters -184/04/4/10, 47(0)
	Apply	

4. After clicking **Apply**, the Main Screen will pop up. When the homepage appears, view the configuration and modify the settings if you want.

DrayTek vs	orAP962C	Syste	VigorAP962C em Time : 2021-01-03 04:10:13	a admin 🗸
SearchQ	Dashboard			C Refresh
Device Menu Configuration > Security > Monitoring > 88 Utility >	WIRELESS CLIENTS OVERVIEW	CHANNEL LOAD		BC:51:89:48 11m: 54s
 Q. System Maintenance , Virtual Controller Jr. Wireless , 	PORT STATUS	SYSTEM USAGE CPU Usage 63% Memory Usage 41%		e DC:51:89:AB ek-5189AB
	LAN STATUS Name IP Address Subnet Mask	DHCP Primary DNS Secondary DNS		1 BC:61:89:AB Rk-5189AB

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

VigorAP962C System Time : 2021-01-01 00:11:15	a admin \vee	VigorAP962C System Time : 2021-01-01 00:11:35	a admin \vee
	Auto Logout off 🗸		Auto Logout off
SYSTEM	🔒 Set Password	SYSTEM	G Set Passwo 1 min 3 min
Device Name VigorAP	☐→ Log Out	Device Name VigorAP	→ Log Out 5 min 10 min

(i) Note:

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

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

I-5 Changing Password

- 1. Please change the password for the original security of the VigorAP.
- 2. Go to **System Maintenance** page and choose **Account & Permission.** Click **Edit** to open the modification page.

						×
ocal Admin	Account				Account ()	admin
+ Add					Current Password 🕢	
Account	Role	Status	Last Login at	Last Login	New Password ()	
admin	Administrator	Active	2021-01-01 02:32:00	192,168,1		Mediu
					Confirm New Password 💿	
					Role	Administrator 🗠
					Status	Active 🗠
					Account Info	
					Created Time	2021-01-01 00:02:
					CONTRACTOR OF THE	2021-01-01-00020

- 3. Enter the new login password on the fields of **New Password** and **Confirm New Password**. Then click **Apply** to continue.
- 4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this VigorAP.

	ے Er	nglish 🗸
Dray Tek VigorAP962C	Username admin Password	Ø
VigorAP962C	Login	

I-6 Dashboard

Dashboard shows port status, LAN status, LAN usage, system status, and wireless overview information.

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

Dashboard									C Refresh
WIRELESS CLIENT	S OVERVIEW		CHANN	EL LOAD			SYSTEM		٥
							Device Name	VigorAP962C	
							LAN MAC	14:49:BC:51:B9:AB	
0	● 2.4G	0		1 inte	h 9	Light, 11%	System Uptime	0d 0h: 46m: 13s	
Clients	• 5G	0		Light	h 104	Light, 1%	Firmware	1.5.4	
							ACS Server	•	
								See More +	
PORT STATUS			SYSTEM	I USAGE			WIRELESS OVERVIE	EW	
			CPU Us	age			2.4GHz		
			L —			38%	Radio	Enable	
			Memor	y Usage			MAC	14:49:BC:51:B9:AB	
	LAN		L —			39%	SSID(1)	DrayTek-51B9AB	
	10/100M = 1G	2.56					SSID(2)		
							5GHz		
							Radio	Enable	
LAN STATUS							MAC	16:49:BC:61:B9:AB	
Name	IP Address	Subnet Mask	DHCP	Primary DNS	Secondary DNS		SSID(1)	DrayTek-51B9AB	
[LAN] LAN1	192.168.1.2	255.255.255.0	off	8.8.8.8	8.8.4.4		SSID(2)		
[LAN] LAN1	192-168-1-2	255.255.255.0	off	9.9.9.9	0.0.4.4			See More +	

This page is left blank.

Chapter II Connectivity



II-1 Configuration

II-1-1 Physical Interface

Configure the general settings for LAN interface. Open **Configuration >> Physical Interface**.

Search Q	Configuration / Physica	l Interface					CRefresh
Device Menu	Setup the interface						
Dashboard Configuration Physical Interface LAN Wireless LAN Objects Notification Services RADNUS Certificates	Ethernet				AN 16 236		
Security >	Name		Function	Status		Speed	
Monitoring Monitoring Monitoring Monitoriance Monitoriance	P1 LED		LAN			Auto negotiation \sim	
Virtual Controller	Interface LED	Enabled	LED Sleep Schedule Disabled V				

ltem	Description				
	Ethernet				
Name	Displays the name of the Ethernet port.				
Function	Displays current function of the Ethernet port.				
Status	Switch the toggle to enable or disable the Ethernet port.				
Speed	Set the Ethernet port speed capabilities:				
	Port speed capabilities:				
	Auto negotiation: Auto speed with all capabilities.				
	Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.				
	LED				

Interface Displays the name of the LED.	
---	--

Enabled	In default, the LED on the device will be always on. However, the LED can be turned on or off after a specified number of minutes has elapsed to meet certain requirements. For this, switch the toggle to enable this setting.
LED Sleep Schedule	The LED can be turned on or off based on the settings configured in the selected schedule (defined under Configuration>>Objects) profile to fulfill specific requirements.
	When LED is slept, it can be woken up by pressing one of the following buttons:
	 Factory Reset on the front panel
	 Wake up LED on this configuration page
	Note that if the schedule is set with repeat type and applied here, the LED on the device will be turned on and turned off at specified time periodically and automatically.
Cancel	Click to discard the modification.
Apply	Click to save the settings.

(Note:

Switch these two icons by click the mouse cursor on them.



- means "Enable".

) - means "Disable".

II-1-2 LAN

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

II-1-2-1 LAN Networks

Open **Configuration>>LAN** and select the **LAN Networks** tab to open the following page.

Search	q	Configuration / LAN	③Reset C Refresh
		LAN Networks Bind IP to MAC DHCP Options VLAN List Interface VLAN	
Device Menu	-	LAN Networks	
(?) Dashboard			
E Configuration		Name [LAN] LÁN1	
Physical Interface		LAN Network Configuration	
Wireless LAN		LAN Network Configuration DHCP State IP	
Objects		IP Address () 192.168.1.2	
Notification Services RADIUS		Subnet Mask 255-255.0/24 ~	
Certificates		Default Gateway () 192.168.1.1	
Security	×S	Primary DNS Server () 8.8.8.8	
🖽 Monitoring	> ::	Secondary DNS Server ③ 8.8.4.4	
88 Utility	20	Management VLAN 📀 None 🗸	
🗞 System Maintenance	20	DHCP Server Configuration	
Virtual Controller		DHCP Server On Off Relay	
}+ Wireless	>		
		Cancel Apply	

ltem	Description
LAN Network Configurat	ion
LAN Network	Select the connection type for the LAN network.
Configuration	• DHCP - DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client.
	Static IP
	When DHCP is selected
Primary DNS Server	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISI does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS Server	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does no provide it, the device will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
Management VLAN	VigorAP 962C supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 962C.
	Select a number as VLAN ID tagged on the transmitted packet. "None" means no VALN tag.
	When Static IP is selected
IP Address	Enter a private IP address for connecting to a local private network

	(Default: 192.168.1.2).
Subnet Mask	Enter an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
Default Gateway	Enter a value of the gateway IP address for the DHCP server.
Primary DNS Server	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISF does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS Server	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the device will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
Management VLAN	VigorAP 962C supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 962C.
	Select a number as VLAN ID tagged on the transmitted packet. "None" means no VALN tag.

DHCP Server	• On - Lets the device assign IP address to every host in the LAN.
	 Off - Lets you manually or use other DHCP server to assign IP address to every host in the LAN.
	• Relay - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address	It is available when On is selected as the DHCP Server.
	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your device is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254.
IP Pool Counts	It is available when On is selected as the DHCP Server.
	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
Gateway IP Address	It is available when On is selected as the DHCP Server.
	Enter a value of the gateway IP address for the DHCP server.
Lease Time	It is available when On is selected as the DHCP Server.
	It allows you to set the leased time for the specified PC.
Primary DNS	It is available when On is selected as the DHCP Server.
	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS	It is available when On is selected as the DHCP Server.
	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

DHCP Server Configuration - Available when Static IP is selected

DHCP Server IP Address	It is available when Relay is selected as the DHCP Server. Enter a value of the IP address for the DHCP server.
Cancel	Click to discard the modification and return to the previous page.
Apply	Click to save the settings.

II-1-2-2 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

	q	Configuration / LAN					() Rese
		LAN Networks Bind IP to MA	C DHCP Options VLAN List I	nterface VLAN			
		Bind IP to MAC					
b Dashboard							
	1.45	+ Add				Search	Mate 3
Physical Interface		Comment :	MAC Address		IP Address		Option
				No Records Founds			
Wireless LAN							
Objects							
Notification Services							
RADIUS							
Certificates	10						
Security	25						
Monitoring	2						
Utility	>						
System Maintenance	51						
	-						
Wireless	*:						

Available settings are explained as follows:

ltem	Description				
+Add	Click to create a new profile.				
Comment	Displays a brief description for the entry.				
MAC Address	Displays the MAC address used by the entry.				
IP Address	Displays the IP address used by the entry.				
Option	Edit - Click to modify the selected profile. Delete - Click to delete the selected entry.				

To modify an existing profile, select a file and click **Edit.**

Configuration / LAN				
LAN Networks Bind IP to	MAC DHCP Options VLAN List	Interface VLAN		×
Bind IP to MAC			Comment	Bind_A_PC
+ Add			MAC Address (Input format is FF:FF:FF:FF:FF:FF)	08:BF:B8:D5:DD:A9
Comment ⇔	MAC Address 👙		IP Address ()	192.168.1.102
ooninent y	MAG AGIESS &			132110011102
		No Records Found		
				Cancel Apply

To add a new profile, click the **+Add** link to get the following page.

ltem	Description
Comment	This is an optional field to identify this IP Address – MAC Address pair.
MAC Address	Use the drop-down menu to select a MAC address
IP Address	Use the drop-down menu to select an IP address.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save the settings and return to the previous page.

II-1-2-3 DHCP Options

DHCP packets can be processed by adding option number and data information when such function is enabled and configured.

This page allows you to configure additional DHCP client options.

Dashboard		OHCP Options			
		+ Add		Sec	arch _{ee} Max
Physical Interface		Option Number	Data Type 👌	Data 🗉	Option
Wireless LAN					
Objects					
Notification Services					
RADIUS					
Certificates					
Security	2				
Monitoring	5				
Utility	5				
System Maintenance	>				
Wireless					

Available settings are explained as follows:

ltem	Description
+Add	Click to create a new profile.
Option Number	Displays the number used by this profile.
Data Type	Displays the data type.
Option	Edit - Click to modify the selected profile. Delete - Click to delete the selected entry.

To modify an existing profile, select a file and click **Edit.**

Configuration / LAN LAN Networks Bind IP to MAC DHCP Options VLAN List Interface VLAN × DHCP Options 0 Option Number (0-255) ASCII Character $\,\,\smallsetminus\,\,$ + Add Data Type Option Number Data Type Data ASCII Character Hexadecimal Digital Address List Note: 1. DHCP Option does NOT take affect when the configured option number conflicts with LAN or WAN settings. Cancel Apply

To add a new profile, click the **+Add** link to get the following page.

ltem	Description						
Option Number	Enter a number (0 to 255) for this function.						
Data Type	Choose the type (ASCII or Hex or Address List) for the data to be stored. Type of data in the Data field:						
	• ASCII Character - A text string. Example: /path.						
	 Hexadecimal Digit - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468. 						
	• Address List - One or more IPv4 addresses, delimited by commas.						
Data	Enter the content of the data to be processed by the function of DHCP option.						
Cancel	Discard the settings and return to the previous page.						
Apply	Click it to save the settings and return to the previous page						

II-1-2-4 VLAN List

Virtual Local Area Networks (VLANs) allow you to subdivide your LAN to facilitate management or to improve network security.

	Configuration / LAN			③ Reset C Refresh
	LAN Networks Bi	nd IP to MAC DHCP Options VLAN List	Interface VLAN	
	VLAN List			
 Dashboard 				
	+ Add			Max
Physical Interface	VLAN ID	Name	LAN Network	Option
Wireless LAN				
Objects				
Notification Services				
RADIUS				
Certificates				
Security				
88 Utility				
N System Maintenance				
>- Wireless	35			

Available settings are explained as follows:

ltem	Description
+Add	Click to create a new profile.
VLAN ID	Displays the number used by this profile.
Name	Displays the name of the VLAN profile.
LAN Network	Displays the LAN network used by the VLAN profile.
Option	Edit - Click to modify the selected profile. Delete - Click to delete the selected entry.

To modify an existing profile, select a file and click Edit.

Configuration / L	AN					
LAN Networks	Bind IP to MAC	DHCP Options	VLAN List	Interface VLAN		×
VLAN List					VLAN ID 0	100
+ Add					Name	100_VLAN
VLAN ID			Name	LAN N	LAN Network	Please select $$
				No Records Found		[LAN] LAN1
						Cancel Apply

To add a new profile, click the **+Add** link to get the following page.

ltem	Description
VLAN ID	Enter the value as the VLAN ID number.
Name	Enter a name to represent the VLAN profile.
LAN Network	Select the LAN network used by the VLAN profile.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

II-1-2-5 Interface VLAN

This page allows you to configure the LAN port settings to assure the VLAN profile can work normally.

Search	٩	Configuration / LAN						③ Reset	C Refresh
		LAN Networks Bind IP to MAC	DHCP 0	options	VLAN List Int	erface VLAN			
Device Menu	_	Interface VLAN Settings							
(2) Dashboard		and the rest strangs							
E Configuration		22440000							
Physical Interface		Ethernet							
LAN		Ethernet	Interface	Port Tune	Untagged VLAN	Tenned VI AN			
Wireless LAN									
Objects			Port 1	Trunk♀	None 🗸	ALVLANS	Select VLANs		
Notification Services									
RADIUS									
Certificates									
Security	>								
G Monitoring	>								
BS Utility	2								
🖏 System Maintenance	8								
Virtual Controller									
}+ Wireless	>								

ltem	Description				
Interface	Displays the Ethernet port number.				
Port Type	Trunk - A trunk port can transmit data from multiple VLANs.				
	Access - Transmits the data to and from a specific VLAN.				
	An access port is only assigned to a single VLAN, it sends and receives frames that aren't tagged and only have the access VLAN value.				
Untagged VLAN	Use the drop-down list to select a VLAN ID as the untagged VLAN.				
	The connected host sends its traffic without any VLAN tag on the frames. However, when the frame reaches this interface (LAN port), It will be added with the VLAN tag.				
Tagged VLAN	Select to enable 802.1Q tagging on this VLAN. The device will add specific VLAN number to all packets on the LAN while sending them out. All VLANs - All VLAN will be tagged.				
	Select VLANs - Only the selected VLAN will be tagged.				
	Tagged VLAN				
	All VLANs Select VLANs select your options				
	Select All				
	Search				
	00 (100_VLAN)				
Cancel	Discard the settings and return to the previous page.				

II-1-3 Wireless LAN

VigorAP 962C is a highly integrated wireless local area network (WLAN) for 2.4/5 GHz 802.11b/g/n/ax WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80/160 MHz at 5 GHz. VigorAP 962C can support data rates up to 2.4 Gbps/4.8Gbps in 802.11ax 80/160 MHz bandwidth.

(i) Note:

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

VigorAP 962C 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 962C.

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.

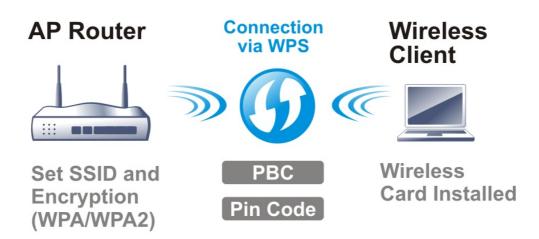
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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 962C 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 962C) with the encryption of WPA and WPA2.



It is the simplest way to build connection between wireless network clients and VigorAP 962C. 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 962C automatically.

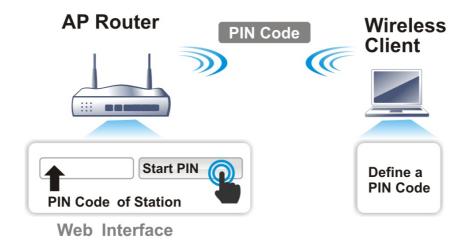
(i) Note:

This 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*.

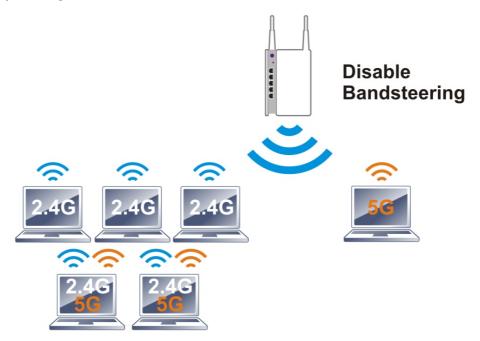
On the side of VigorAP 962C series which served as an AP, click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.

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 962C.

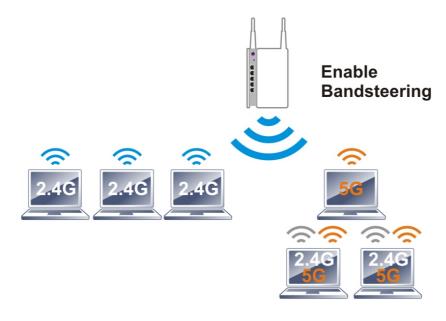


Band Steering

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



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



(i) Note:

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

Airtime Fairness

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

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

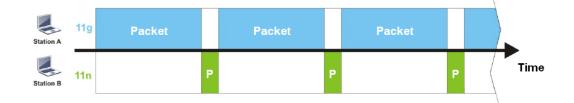
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

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

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

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



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



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

Suitable environment:

(1) Many wireless stations.

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

(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-1-3-1 SSID

By clicking the SSID tab, a web page will appear so that you could set the SSID, the security mode, and the password.

	SSID						
b Dashboard	3310						
	+Add						Ma
Physical Interface	SSID ()	Enabled	Security	Password 💿	Scheduled On	2.4GHz	5GHz Option
LAN Wireless GAN	DrayTek-5189AB		WPA3/WPA2 Personal V	••••••	Always On \vee	•	🖸 🥒 Edit
Objects							
Notification Services							
RADIUS							
Certificates							
Security							
Monitoring							
Utility	5						
System Maintenance	s.						

Available settings are explained as follows:

Item	Description	
+Add	Click to set a new SSID.	
SSID Name	Displays the name of the SSID.	
Enabled	Switch the toggle to enable or disable this entry.	
Security	Displays the security mode used by this entry. If required, use the drop-down list to select another mode.	
Password	Displays the password used by this entry.	
Scheduled On	 Select Always or any other schedule profile. Always - This WLAN profile will be active all the time. Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to Configuration>>Object to create schedule profiles (at least one). 	
2.4GHz	Switch the toggle to enable or disable this entry.	

	If enabled, this entry will be applied to 2.4GHz wireless network.	
5GHz	Switch the toggle to enable or disable this entry. If enabled, this entry will be applied to 5GHz wireless network.	
Option	Edit - Click to modify the selected profile. Delete - Click the selected entry. The default SSID can not be deleted.	
Cancel	Discard the settings and return to the previous page.	
Apply	Save and apply the settings.	

To edit an existing SSID, click the **Edit** link to get to the following page.

Configuration / Wireless LAN	
SSID 🕕	DrayTek-51B9AB
Enabled	
Security	WPA3/WPA2 Personal V
Password (j	····· ©
VLAN ()	None 🗸
Scheduled On	Always On 🗸 🗸
SSID Band	
2.4GHz	
5GHz	
SSID Settings	
MAC Filtering List	Disabled \checkmark
Isolate Client from Wireless	
Hide SSID	
WDA Cottings	

ltem	Description
SSID	Set a name for VigorAP to be identified.
Enabled	Switch the toggle to enable or disable the function.
Security	There are several modes provided for you to choose from. Below shows the modes with higher security:
	 WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2, or Auto as WPA mode.
	WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise - The

	WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	• OWE - WPA3 also introduces a new open and secure connection mode; "Opportunistic Wireless Encryption" (OWE). It allows the clients to connect without a password, ideal for hotspot networks, but the connection between each individual client is uniquely encrypted behind the scenes.
	Below shows the modes with basic security;
	 WPA Personal - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	 WPA Enterprise - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	• WEP Personal - Accepts only WEP clients and the encryption key should be entered in WEP Key.
	• None - The encryption mechanism is turned off.
Password	Enter 8~63 ASCII characters, such as "012345678". This feature is available for WPA Personal or WPA2 Personal or WPA2 / WPA Persona mode, WPA3 Personal or WPA3/WPA2 Personal .
RADIUS Server	This feature is available for WPA3 Enterprise , WPA2 Enterprise , WPA2/WPA Enterprise , and WPA Enterprise mode.
	Use the drop-down list to select a RADIUS server setting.
	Note : Before configuring the RADIUS server, go to Configuration>>RADIUS to create external RADIUS profiles (at least one) first.
VLAN	Select VLAN ID # for this SSID. Packets transferred from this 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 None by default, it means disabling the VLAN function for the SSID.
Scheduled On	Select Always or any other schedule profile.
Scheduled On	
Scheduled On	Always - This WLAN profile will be active all the time.
Scheduled Off	Or, use the drop-down list to select a preset schedule profile.
Scheduled On	
	Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to Configuration>>Object to create
2.4GHz/5GHz	Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to Configuration>>Object to create schedule profiles (at least one).
	Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to Configuration>>Object to create schedule profiles (at least one). SSID Band

	Before choosing, please go to Security>>MAC Filtering to create MAC filtering profiles (at least one).
Isolate Client from	Switch the toggle to enable or disable the function.
Wireless	Makes the wireless clients (stations) with the same SSID not access fo each other.
Hide SSID	Switch the toggle to enable or disable the function.
	Prevents 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 962C while site surveying. The system allows you to set four sets of SSID for different usage.
	WPA Settings
WPA Algorithm	This feature is available for WPA2 Personal, WPA2/WPA Personal, WPA2 Enterprise, WPA2/WPA Enterprise, WPA Personal, or WPA Enterprise mode.
	Select TKIP, AES, or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses a shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. This feature is available for WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal, WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise, WPA Personal, WPA Enterprise mode.

Default Key	This feature is available for WEP Personal mode.
	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 ','.
Кеу # Туре	Hex/ASCII - 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 ','. This feature is available for WEP Personal mode.
Key #	Enter 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. This feature is available for WEP Personal mode.
Cancel	Discard the settings and return to the previous page.
Apply	Save and apply the settings.

Click **Apply** to save the settings and return to the previous page.

II-1-3-2 Radio Settings

This page is to determine the wireless radio setting, like channel, physical mode, channel bandwidth, transmit power and etc.

Search	Q	Configuration / Wireless LAN		③ Reset
		SSID Radio Settings Ro	aming AP Discovery WPS Range Extender WDS	
Device Menu				
 Dashboard 		Radio Settings		
Configuration	14			Advanced Mode: OFF
Physical Interface		2.4GHz Radio		
LAN		Enabled		
Wireless LAN		Mode	Mixed (11b+11g+11n+11ax) 🗸	
Objects		Transmit Power	100%	
Notification Services				
RADIUS		Channel	Auto Select 🗸 🗸	
Certificates		Channel Bandwidth	Auto 20/40 MHz \sim	
Security	\$3	Current Channel	Channel 9	
🔛 Monitoring	\$ 2	Current Extension Channel	Channel 5	1
88 Utility	>	Update Channel	Scan and Update	
🖏 System Maintenance	•		Note: Execute a one-time channel optimization for this AP. This would result in wireless downtime for few minutes.	
		Updated Channel Result		
Virtual Controller				
>- Wireless	>	5GHz Radio		
		Enabled		
		Mode	Mixed(11a+11n+11ac+11ax) ~	

ltem	Description	
Advanced Mode	ON/OFF - Click the button to show or hide more settings.	
	2.4GHz Radio	
Enabled	Switch the toggle to enable or disable the function.	
Mode	At present, VigorAP can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n), Mixed (11b+11g+11n) and Mixed (11b+11g+11n+11ax) stations simultaneously. Simply choose Mixed (11b+11g+11n+11ax) mode.	
Transmit Power	The default setting is the maximum (100%). Lowering down the value may degrade the range and throughput of wireless.	
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto Select to let the system determine for you.	
Channel Bandwidth	Auto 20/40 MHz– The AP will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not.	
	20 MHz- The device will use 20MHz for data transmission and receiving between the AP and the stations.	
	40 MHz- The device will use 40MHz for data transmission and receiving between the AP and the stations.	
Current Channel	Displays current channel number.	
Current Extension Channel	Displays current extension channel.	

Update Channel	Scan and Update - Click to select the best channel again when Auto Select is selected as the Channel setting.	
Updated Channel Result	Displays the best channel after pressing the Scan and Update button.	
	Update Channel Scan and Update Note: Execute a one-time channel optimization for this AP. T	
	Updated Channel Result New Channel: 9	
	5GHz Radio	
Enabled	Switch the toggle to enable or disable the function.	
Mode	At present, VigorAP can connect to 11a only, 11n only (5G), Mixed (11a+11n), Mixed (11a+11n+11ac), and Mixed (11a+11n+11ac+11ax) stations simultaneously. Simply choose Mixed (11b+11g+11n+11ax) mode.	
Transmit Power	The default setting is the maximum (100%). Lowering down the value may degrade the range and throughput of wireless.	
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto Select to let the system determine for you.	
Channel Bandwidth	20 MHz- The device will use 20MHz for data transmission and receiving between the AP and the stations.	
	40 MHz- The device will use 40MHz for data transmission and receiving between the AP and the stations. It is for wireless LAN 2.4GHz only.	
	80 MHz- The device will use 80MHz for data transmission and receiving between the AP and the stations.	
	160 MHz- The device will use 160MHz for data transmission and receiving between the AP and the stations.	
Current Channel	Displays current channel number.	
Update Channel	Scan and Update - Click to scan current channel used.	
Updated Channel Result	Displays current channel used.	
	Update Channel Scan and Update Note: Execute a one-time channel optimization for this AP.	
	Updated Channel Result New Channel: 9	
	Band Steering Settings	
	If it is enabled MiserAD will detect if the wireless client is seable of	

5Ghz Client Minimum RSSI	If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit.	
	The wireless station has the capability of a 5GHz network connection, yet the signal performance might not be satisfied. Therefore, when the signal strength is below the value set here while the wireless station connecting to VigorAP, VigorAP will allow the client to connect to the 2.4GHz network.	
Below shows more settings if the Advance Mode is ON		
Antenna	Configure the number of antenna for transmission and reception.	

Fragment Length	Sets the Fragment threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2346.
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.
	Set the RTS threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2347.
Country Code	VigorAP broadcasts country codes by following the 802.11d standard However, some wireless stations will detect/scan the country code to prevent conflict occurred. If conflict is detected, the wireless station will be warned and is unable to make a network connection. Therefore, changing the country code to ensure a successful network connection will be necessary for some clients.
WMM Capable	To apply WMM parameters for wireless data transmission, switch the toggle to enable the function.
APSD Capable	APSD (Automatic Power-Save Delivery) is an enhancement over the power-saving mechanisms supported by Wi-Fi networks. It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption. Not all wireless clients support APSD properly, and the only way to find out if APSD is appropriate for your network is to experiment.
Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. Switch the toggle to enable the function.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

II-1-3-3 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.

Search	۹	Configuration / Wireless LAN	③Reset
Device Menu		SSID Radio Settings Roaming AP Discovery WPS Range Extender WDS Fast Roaming	
 Configuration Physical interface LAN Wireless LAN Objects 	*	Enabled 802.11r Enabled 802.11r Pre-Authentication for 802.1x	
Notification Services RADIUS Certificates	I	Assisted Client Roaming Assisted Roaming by Signal Strength (RSSI)	v
Security	>	Enubled	
	*	Assisted Reaming Signal Strength Threshold - (Hourning Signal range: -Bodttim - 42:000m) 65 dBm.(Default: -65) Assist reaming when adjacent AP signal is better than (adjacent AP signal range: 1db - 20:d0) 5 dB(,Default: 5)	
88 Utility	>	ester rommelt was induced to alban a neres runn induced to alban under rom a seres. a	
🖏 System Maintenance	>		
Virtual Controller			
≻ Wireless	. A	Cancel Apply	

ltem	Description	
Fast Roaming		
Enable 802.11r	Enable 802.11r - Switch the toggle to enable the 802.11r protocol(also known as Fast Basic Service Set (BSS) Transition. If enabled, the access point will improve the roaming experience for the wireless clients.	
802.11r Mode	Over the DS - Transmit the handshake messages between the client and the new AP using the distribution system. In response to signal strength change, the client can communicate with the other AP through the original AP with Action Frames (FT Request and FT Response).	
	Over the Air - Transmits the messages directly over the wireless network. In response to the needs of signal strength change, the clien can communicate directly with the other AP using a fast roaming authentication algorithm (without requiring reauthentication at every AP).	
	Note that both APs must ping each other via DS (Distribution System) WDS.	
Enabled 802.11k	Switch the toggle to enable the 802.11k protocol (also know as Radio Resource Management (RRM)). If enabled, the access point will optimize the performance of wireless networks.	
Pre-Authentication for 802.1x	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 handof delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)	
	Switch the toggle to enable/disable 802.11x Pre-Authentication.	
	Enable - Enable IEEE 802.1X Pre-Authentication.	
	Disable - Disable IEEE 802.1X Pre-Authentication.	
Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2 Enterprise mode.	

Assisted Client Roaming		
Assisted Roaming by Signal Strength	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 962C 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. Enabled – Enable the function.	
	Assisted Roaming Signal Strength Threshold – When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of Assist roaming when adjacent AP signal is better than) is detected by VigorAP 962C, VigorAP 962C will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI).	
	Assist roaming when adjacent AP signal is better than - Specify a value as a threshold.	
Cancel	Discard the settings and return to the previous page.	
Apply	Click it to save and apply the settings.	

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

II-1-3-4 AP Discovery

VigorAP 962C 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.

	۹	Configuration / Wirele							C Refresh
			s Roaming AP Discovery	WPS Range Extender V	VDS				
 Dashboard 		AP Discovery							
		Start AP Discovery	Scan						
Physical Interface			Note: Scanning proc	ess would result in wireless dow	ntime for few	minutes.			
LAN									
		Radio Information							
Objects Notification Services			2.4GHz	5GHz					
RADIUS Certificates		Mode	Mixed(11b+11g+11n+11ax)	Mixed(11a+11n+11ac+11ax)					
Security		Current Channel	9	44					
🖽 Monitoring		Channel Utilization	15%	6%					
88 Utility	•	Channel Width	20/40 MHz	160 MHz					
🖏 System Maintenance									
		Neighbor AP List							
}→ Wireless	•	SSID (BSSID	Signal Strength (RSSI)	Band	Channel ()	Mode .	Security	Encryption
		912C_Demo_2	0a 03.7f 15.15.13	73%	2.4GHz	1	11b/g/n	WPA2 Personal	AES
		guests_5F	16:49.bc 51.b9:b3	50%	2.4GHz	1	11b/g/n/ax	WP3/WPA2 Personal	AES

Each item is explained as follows:

ltem	Description
Start AP Discovery	Scan - Discover all the connected AP. The results will be shown on the

	have also us this button					
	box above this button					
	Radio Information					
Mode, Current Channel, Channel Utilization, Channel Width	A table lists the radio information for this VigorAP 962C.					
	Neighbor AP List					
SSID	Displays the SSID of the AP scanned by VigorAP 962C.					
BSSID	Displays the MAC address of the AP scanned by VigorAP 962C.					
Signal Strength (RSSI)	Displays the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.					
Band	Displays the wireless band(2.4GHz/5GHz) used by the AP.					
Channel	Displays the wireless channel used for the AP that is scanned by VigorAP 962C.					
Mode	Displays the physical mode used by the scanned AP.					
Security	Displays the security mode used by the scanned AP.					
Encryption	Displays encryption mode (None, WEP, TKIP, AES, etc.) of AP.					

II-1-3-5 WPS

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

Search	۹	Configuration / Wireless LAN		③ Reset	C Refresh
Device Menu	=	SSID Radio Settings Roar	ming AP Discovery WPS Range Extender WDS		
 Dashboard 		Enabled	-		
🚊 Configuration		Enabled			
Physical Interface			Note: only WPA2/WPA Personal security mode support WP5.		
LAN		Band	2.4GHs SGHs		
Wireless LAN		2.4GHz SSID	DrayTek-5189AB		
Objects					
Notification Services RADIUS		Method 1 : WPS Button			
Certificates		Enable WPS	Start PBC		
Security					
		Method 2 : Using PIN Code			
and the second sec		Generate PIN code from	Client		
88 Utility	2	Client PIN Code	73156788		
🖏 System Maintenance	2		Contract		
Virtual Controller	-				
5- Wireless		Connection Status	Idle		
,→ wireless	,				
		Cancel Apply			

Available settings are explained as follows:

ltem	Description					
Enabled	Switch the toggle to enable/disable the WPS setting.					
Band	Specify which wireless band (2.4G/5G) will be used for this connection mode.					
	• 2.4GHz					
	• 5GHz					
2.4GHz/5GHz SSID	Displays the SSID setting for 2.4GHz/5GHz.					
	Method 1: WPS Button					
Enable WPS	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 962C will wait for WPS requests from wireless clients about two minutes.					
	Method 2: Using PIN Code					
Generate PIN code from	Client - Use wireless client's PIN code to securely connect it to the Wi-Fi network.					
Client PIN Code	Enter a number as the PIN code from the wireless client.					
Connect	Click to build WPS connection between this AP and another station.					
Apply	Click it to save and apply the settings.					
Cancel	Discard the settings.					

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

II-1-3-6 Range Extender

VigorAP can act as a wireless repeater which will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use the Station function to connect to a Root AP and use the AP function to service all wireless clients within its coverage.

Search	Q	Configuration / Wireless LAN	③Reset CRefresh
		SSID Radio Settings Roan	ming AP Discovery WPS Range Extender WDS
Device Menu	-	Range Extender	
(?) Dashboard		nonge extender	
E Configuration	-	Enabled	
Physical Interface		Band	2.40Hz 50Hz
LAN		Peer SSID	Scan and Update
Wireless LAN			Note: Update the Peer SSID and MAC suggestion list by using the button to execute a one-time AP Discovery. This would result in wireless downtime for
Objects			few minutes,
Notification Services			
RADIUS		Updated Status	
Certificates		Peer MAC Address (Optional)	
⊘ Security	1911	Channel	Auto
표 Monitoring		Security Mode	WPA2 Personal 😪
88 Utility	: •:	WPA Algorithms	AS
🐁 System Maintenance	÷.	Password	•
Virtual Controller	-	Connection Status	Disconnect
> Wireless	167		
		Cancel Apply	

ltem	Description						
Enabled	 Switch the toggle to enable/disable the Range Extender setting. Specify which wireless band (2.4G/5G) will be used for this connection mode. 2.4GHz 5GHz 						
Band							
Peer SSID	Enter the SSID of the access point that VigorAP 962C wants to connect to. Scan and Update - Scan the peer SSID and connect to it again.						
	Update Status						
Peer MAC Address (Optional)	Enter the MAC address of the access point that VigorAP 962C wants to connect to.						
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference.At present, only Auto is available for selection which lets the system determine for you.						
Security Mode	 There are several modes provided for you to choose from. Each mod will bring up different parameters for you to configure. WPA3 Personal WPA2 Personal OPEN 						
WPA Algorithm	This option is available when WPA3 Personal or WPA2 Personal is selected as Security Mode . At present, only AES is available for selection.						
Password	This option is available when WPA3 Personal or WPA2 Personal is selected as Security Mode . Enter 8~63 ASCII characters, such as "012345678".						
Connection Status	Displays current connection status.						
Cancel	Discard the settings.						

Apply	Click it to save and apply the settings.
-------	--

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

II-1-3-7 WDS

Wireless Distribution System (WDS) is a protocol for linking access points (AP) wirelessly.

Search Q	Configuration / Wireless LAN SSID Radio Settings Roamin	AP Discovery WPS Range	Estandar MIN			() Reset	C Refresh
Device Menu	WDS	Ar Docovery WPS halige	EXENSE W03				
Configuration	Enabled Mode 2.4GHz WDS List	HE (11ax)					
Windess LAN Objects Notification Services	+Add Peer MAC Address 💿		Enabled	Security	Pessword 🕕		Max: 4
RADIUS Certificates Ø Security >	5GHz WDS List		ten Brennik, Enundi				~
B Monitoring , B Utility , System Maintenance ,	+ Add Peer MAC Address ③		Enabled	Security	Password 💿		Main 4
Virtual Controller							
	Cancel Apply						

ltem	Description					
Enabled	Switch the toggle to enable/disable the WDS setting.					
Mode	 Select the physical mode for this WDS setting. HE(11ax) VHT(11ac) HTMIX(11n) 					
	2.4GHz WDS List					
+Add	Creates a new WDS entry for wireless band 2.4GHz.					
Peer MAC Address	Displays the peer MAC addresses Enter the peer MAC addresses in these fields. Up to four peer MAC addresses may be entered in this page. Select the checkbox in front of a MAC address to enable it.					
Enabled	Switch the toggle to enable/disable this setting.					
Security	Displays the security type.					
Password	Displays the password for TKIP/AES mode.					
	5GHz WDS List					
+Add	Creates a new WDS entry for wireless band 5GHz.					
Peer MAC Address	Displays the peer MAC addresses Enter the peer MAC addresses in these fields. Up to four peer MAC addresses may be entered in this page.					
Enabled	Switch the toggle to enable/disable this setting.					

Security	Displays the security type.
Password	Displays the password for TKIP/AES mode.
Cancel	Discard the settings.
Apply	Click it to save and apply the settings.

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

II-1-4 Objects

II-1-4-1 Schedule

This page allows you to set schedule profiles that can be used for the VigorAP to dial up to the Internet at a specified time. It is especially useful for each WLAN SSID to access the Internet network at different time periods by assigning different schedule profiles.

The schedule is also applicable to other functions.

۹	composition	on / Objects							() Reset
	Schedule								
-	1.114								Max: 2
									100.0 × 2
	Name	Enabled (Start Date	Start Time (Hr: Min.)	End Time (Hr: Min.)	Repeat Used In a	In Use II	Option	
	For_LED	Enabled	2024-05-16	15:26	00:00	Daily	NO	@ Edt	2 Delete
2									
×									
*									
×									
2									
	2	Schedule + Add Name For_LED	Schedule + Add Name Enabled For_LED Enabled	Schedule + Add Name Enabled Start Date For_LED Enabled 2024-05-16	Schedule + Add Name Enabled Start Date Start Time (Hr: Min.) For_LED Enabled 2024-05-16 15:26	Schedule Add Name Enabled Start Date Start Time (Hr: Mn.) End Time (Hr: Min.) For_LED Enabled 2024-05-16 15:26 00:00	Schedule + Add Name Enabled Start Date Start Time (Hr: Min.) End Time (Hr: Min.) Repeat Used in (For_LED Enabled 2024-05-16 15:26 00:00 Daily	Schedule	Schedule * Add

To add a new schedule profile, click the **+Add** link to get the following page.

Configuration	n / Objects							
Schedule								×
+ Add					Name 🕕		Test_AP	
Name	Enabled 🖕	Start Date	Start Time (Hr: Min.) 🖕	End Time (Hr: Min.) 🔅	Enabled			
For_LED	Enabled	2024-05-16	15:26	00:00	Start Date	2024-05-2	24	۲
					Start Time (Hr: Min.)	03	~ : 07	\sim
					End Time (Hr: Min.)	22	~ : 00	\sim
					Repeat		Once	~
							Cancel	Apply

ltem	Description
Name	Enter the name of the schedule profile.
Enabled	Switch the toggle to enable/disable the schedule profile.
Start Date	Specify the starting date of the schedule.
Start Time (Hr:Min.)	Specify the starting time of the schedule.
End Time (Hr:Min.)	Specify the ending time of the schedule.
Repeat	Specify how often the schedule will be applied.
	Once - The schedule will be applied just once.
	Daily - The schedule will be applied every day based on the above settings.
	• End Repeat - Switch the toggle to enable/disable the daily functio
	• End Repeat Date - The schedule is valid until that day.
	Weekly - Specify which days in one week should perform the schedu
	• Every - Select the days in one week.
	• End Repeat - Switch the toggle to enable/disable the daily function
	• End Repeat Date - The schedule is valid until that day.
	Monthly - The schedule will be applied every month .
	• End Repeat - Switch the toggle to enable/disable the daily function
	• End Repeat Date - The schedule is valid until that day.
	Cycle - Enter a number as cycle duration. Then, any action applied th schedule will be executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined or

	the Start Date.
	• Every (days)- Enter a number.
	• End Repeat - Switch the toggle to enable/disable the daily function.
	• End Repeat Date - The schedule is valid until that day.
Cancel	 End Repeat Date - The schedule is valid until that day. Discard the settings.

II-1-5 Notification Services

VigorAP can send messages related to the system and the wireless LAN to DrayTek Wireless APP.

Search	a	Configuration / Notification Servic	es			(1) Reset	C Refresh
Device Menu		App Notifications					
 Device menu Dashboard 		Enabled					
		Connected Devices					
Physical Interface		connected Devices					
LAN		Devices					
Wireless LAN		No Records Fol					
Objects							
Notification Services RADIUS		Test Notifications	Send Test Notification				
Certificates		Send Status					
Security	2	Notification Message					
🖽 Monitoring	×	Category		Enable	Content		
88 Utility	2	System			WUUSSH/Telnet Login		
🐴 System Maintenance	2	Wireless LAN			Mesh Node online/offline		
Virtual Controller							
>- Wireless	5						
		Cancel Apply					

Available settings are explained as follows:

Item	Description
	App Notifications
Enabled	Switch the toggle to enable/disable the function of sending notification to the DrayTek Wireless APP.
	Connected Devices
Devices	Display the name (device ID) of the mobile phone(s) connected and submitted to DrayTek Wireless APP. Note that the little bell on the top-right corner of the APP must be turned on to receive the message from VigorAP 962C.
Test Notifications	Send Test Notification – Press to send a message to DrayTek Wireless APP.
Send Status	Display the test result after pressing the Send Test Notification button.
	Notification Message
Category	At present, only two categories are available.
Enable	Switch the toggle to enable/disable the category.
Content	Display the detailed information for the selected category.

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

II-1-6 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

This web page is used to configure settings for external RADIUS server. Then WLAN users of VigorAP will be authenticated and accounted by such server for network application.

Search	۹	Configuration	n / RADIUS		
		External RAI	DIUS		
 Dashboard 		+ Add			Max: 4
	141	Name	Primary Authentication Server	Secondary Authentication Server	Option
Physical Interface LAN Wireless LAN Objects Notification Services RADRUS Certificates					
Security					
	•				
88 Utility					
🌯 System Maintenance	2				
}⊷ Wireless					

To edit an existing profile, click the **Edit** link of the selected profile to make modifications.

e DrayTek-366100 Intentication US Authentication entication Server +Add Max 2 Priority Server IP Secret Authentication Port Option
entication US Authentication entication Server +Add Max: 2
US Authentication Authentication Server +Add Max: 2
entication Server +Add Max: 2
Priority Server IP Secret Authentication Port Option
0 172.16.3.62 ····· @ 1812 @ Delete

To add a new profile, click the **+Add** link to get the following page.

ltem	Description
Name	Enter the name of the server profile.

	Authentication					
RADIUS Authentication	Switch the toggle to enable/disable the function.					
Authentication Server	+Add - Click to create a new server profile.					
	• Priority - Only two external server can be used.					
	• Server IP - Enter the IP address of the external RADIUS server.					
	 Secret - Enter the password for the user to be authenticated by VigorAP 962C while the user tries to use VigorAP 962C as the RADIUS server. 					
	• Authentication Port - Enter a port number for the RADIUS server.					
	• Option - Click Delete to remove the selected entry.					
Cancel	Discards the settings and exits the page.					
Apply	Click it to save the settings and exit the page.					

II-1-7 Certificates

A digital certificate is an electronic document issued by a certification authority (CA) to an entity to prove ownership of a public key. It contains identifying information including the issued-to party's name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Vigor AP supports digital certificates that conform to the X.509 standard.

In this section, you can generate and manage local digital certificates, and import trusted CA certificates. Be sure that the system time is correct on the access point so that certificates will not be erroneously considered to be invalid because of an incorrect system time falling outside of the certificate's valid time period. The easiest way to accomplish this is by periodically synchronizing the system time to a Network Time Protocol (NTP) server.

II-1-7-1 Local Certificates

You can generate, import or view local certificates on this page.

evice Menu ስ Dashboard		Local Certificates						
Cinfiguration		+ Add					100	arch Max
	12	Certificate Name	Status	Source	CA Imported	Valid From	Valid Until	Option
Physical Interface		Default_Certificate	Valid	internal	~	2021/01/01 01:00:03	2022/01/31 01:00:03	⊕ View ⊙ Regenerate
Wireless LAN Objects								
Notification Services								
RADIUS								
	5 0							
Security	2° 3°							
Security Monitoring								
Security Monitoring Utility	3 7							
Certificates Security Monitoring Utility System Maintenance ual Controller	3° 3°							

Available settings are explained as follows:

ltem	Description
+Add	Creates a new certificate.
View	Displays the content of the certificate.

	Configuration / Certificates Local Certificates Local Certificates		nices Backup &	Restore		Ceroficate Name 💿	X Default_Certificate
	+ Add					Version	V3
	Certificate Name	Status +	Source	CA Imported	Valid F	Status	Valid
	Default_Certificate	yalid -	Internal	~	2021/5	Source	Internal
						CA Imported	×
						Subject_Name	~
						Country (C)	TW
						State (11)	Hsinchu
						Locations (L)	Hsinchu
						Organization (0)	DrayTek
						Organization Unit (180)	DrayTek
						Common Name (CH)	www.draytek.com
						Email (I)	
						Issuer	×
						Common Name (CH)	www.draytek.com
Regenerate	Regenerate	tho co	rtificato	`			

To add a new local certificate profile, click the **+Add** link to get the following page.

Configuration / Certificates		
Certificate Name 🕕		
Method	Generate CSR Import Certificate & Keys	
Кеу Туре	RSA-2048 Bit	
Algorithm	SHA-256	
Subject Alternative Name		`
Туре	IP Address Domain Name Email	
IP Address ()		
Subject Name		
Country (C) 🛈		
State (ST) (j)		
Location (L) 🚺		
Organization (O) (i)		
Organization Unit (OU) 🕕		
Common Name (CN) 🕕		
Email (E)		
Cancel Apply		

ltem	Description
Certificate Name	Enter the name that identifies the certificate.
Method	Generate CSR - Generate a new local certificate. Import Certificate & Keys - Vigor access point allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.
	Method - Generate CSR
Кеу Туре	Displays the key type used by the certificate.
Algorithm	Displays the algorithm for generating the certificate.

Туре	 Select the type of Subject Alternative Name and enter its value. IP Address Domain Name
	Email
Country (C)	Enter the country name (code) in which your organization is located.
State (ST)	Enter the state or province where your organization is located.
Location (L)	Enter the city where you're your organization is located.
Organization (O)	Enter the legal name of your organization.
Organization Unit (OU)	Enter the department within your organization that you wish to be associated with this certificate.
Common Name (CN)	Enter the fully-qualified domain name / WAN IP that will be used to reach your server.
Email (E)	Enter the email address of the entry.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.
	Method - Import Certificate & Keys
File Type	 Vigor AP allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key. Certificate Only - Local certificate. Upload Certificate - Click Choose a file to select a local certificate file. PKCS12 - Users can import the certificates usually need passwords. PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options. Upload PKCS12 File - Click Choose a file to select a PKCS12 certificate file. Password - Enter the password associated with the certificates and key files. Certificate & Keys - It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted. Upload Certificate - Click Choose a file to select a local certificate file. Password - Enter the password associated with the certificate and key files. Upload Certificate - Click Choose a file to select a local certificate file. Upload Certificate - Click Choose a file to select a local certificate file. Upload Certificate - Click Choose a file to select a local certificate file. Upload Certificate - Click Choose a file to select a local certificate file. Upload Certificate - Click Choose a file to select a local certificate file. Upload Certificate - Click Choose a file to select a local certificate file. Upload Key - Click Choose a file to select a key file. Password - Enter the password associated with the certificate and key files.
Cancel	Discards current settings and return to the previous page.

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

II-1-7-2 Trusted CA

The user can build RootCA certificates (up to three) if required.

When the local client and remote server are required to make certificate authentication (e.g., Radius EAP-TLS authentication) for wireless connection and avoid 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 for digital certificates from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor AP offers a mechanism that allows you to generate root CA to save time and provide convenience for general users. Later, such root CA generated by the DrayTek server can perform the issuing of the 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.

Search	۹	Configuration / Certificates					
Device Menu		Local Certificates Trusted C	Local Services Backu	p & Restore			
	-	Trusted Certificate Authorities	F.				
 Dashboard 							
E Configuration		+ Add				Search	Max: 20
Physical Interface		Certificate Name	Status	Common Name	Valid From	Valid Until #	Option
LAN		Root CA	Empty				2 Create
Wireless LAN							
Objects							
Notification Services							
RADIUS							
Certificates							
Security	>						
Monitoring	>						
88 Utility	•						
🖏 System Maintenance	•						
Virtual Controller							
>+ Wireless	,						

Available settings are explained as follows:

ltem	Description
+Add	Creates a new trusted certificate.
Option	Create - Click to open the configuration page.

To create a new RootCA, click **Create** to get the following page.

Configuration / Certificates	
Local Certificates Trusted CA Local Services Backup & Restore	×
Trusted Certificate Authorities	Key Type RSA-2048 Bit
+ Add	Algorithm SHA-256
Certificate Name Status Common Name	Subject Alternative Name
Root CA Empty	Туре
	None IP Address Domain Name Email
	IP Address ()
	Subject Name 🗸 🗸
	Country (C) 0 TW
	Common Name (CN) 🕐
	State (ST) ()
	Location (L) ()
	Organization (O) ()
	Organization Unit (OU) () Email (E)
	Cancel Apply

Available settings are explained as follows:

ltem	Description
Кеу Туре	Displays the key type (set to RSA).
Algorithm	Displays the algorithm.
	Subject Alternative Name
Туре	Select the type of Subject Alternative Name and enter its value.
	Subject Name
Country (C)	Enter the country name (code) in which your organization is located
Common Name (CN)	Enter the fully-qualified domain name / WAN IP that will be used to reach your server.
State (ST)	Enter the state or province where your organization is located.
Location (L)	Enter the city where you're your organization is located.
Organization (O)	Enter the legal name of your organization.
Organization Unit (OU)	Enter the department within your organization that you wish to be associated with this certificate.
Email (E)	Enter the email address of the entry.
Cancel	Discard current settings and return to the previous page.
Apply	Click to submit generate request to the CA server.

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

To upload a certificate, click the **+Add** link to get the following page.

Configuration / Certificates	ionfiguration / Certificates		
		×	
Upload Certificate	C Choose a file		

Available settings are explained as follows:

ltem	Description
Upload Certificate	Choose a file - Select an existing certificate.
Cancel	Discards the settings and exits the page.
Apply	Click it to save the settings and exit the page.

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

II-1-7-3 Local Services

This page allows you to set different categories and services for the local certificate(s) to prevent security warning messages popped up due to using different browsers.

	Q Local Cartificator	CA Local Services Backup & Restore		
		LOCAL SERVICES BACKUP & RESURE		
Dashboard	Local Services			
	Categories	Services	Local Certificate	
Physical Interface	Web Server	HTTPS		
LAN	web Server	HUPS	Default_Certificate ~	
Wireless LAN	Web Server	TR069	Default_Certificate ~	
Objects				
Notification Services	The second s			
RADIUS	Note:			
	Certificate only and CSR cannot	t be applied to local services.		
🦻 Security	(9 .)			
Monitoring	3-S			
g Utility				
🖁 System Maintenance	- 90°			
lirtual Controller ⊷ Wireless				

Available settings are explained as follows:

ltem	Description
Local Certificate	Select a local certificate (has been imported to Vigor device) with full key and authentication information.
	Certificate without key phrase or CSR (certificate signing request) file cannot be selected as local certificate.
Cancel	Discards the settings and exits the page.
Apply	Click it to save the settings and exit the page.

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

II-1-7-4 Backup & Restore

You can back up or restore the Local and Trusted CA certificates on the access point to a file.

	Q. Configuration / Certificates	
	Local Certificates Trusted	CA Local Services Backup & Restore
	Backup & Restore	
 Dashboard 	basing or ressore	
Physical Interface	Backup	
LAN	Selected Item	Select All
Wireless LAN		Local Certificates
Objects		🕑 Trusted Certificate Authorities
Notification Services	Password Protection	
RADIUS	Password	•
	Confirm Password	0
Security	3	
	,	Backup
28 Utility	Restore	
System Maintenance	Restore from Backup File	E Restore
	File has Password Protection	
	A Design of the second second second	
→ Wireless	Password	0

Item	Description						
Backup							
Selected Item	Select All						
	 Local Certificates 						
	Trusted Certificate Authorities						
Password Protection	Enabled - Switch the toggle to enable or disable the function.						
	 Password - Enter the password with which you wish to encrypt the certificate. 						
	• Confirm Password - Enter the password again.						
	Backup - Click to download the certificate.						
	Restore						
Restore from Backup	Click to select the backup file you wish to restore.						
File	Restore - Click to retrieve the certificate.						
File has Password	Enabled - Switch the toggle to enable or disable the function.						
Protection	Password - Enter the password that was used to encrypt the certificates.						

II-2 Security

II-2-1 MAC Filtering Profile

II-2-1-1 MAC Filtering Profile

Users can create access control policies and set black & white lists.

Search	q	Security / MAC Filtering	Profile		③Reset CRefresh
		MAC Filtering Profile	Backup & Restore		
Device Menu		MAC Filtering Profile			
(🕗 Dashboard		MAC Pittering Prome			
	*	+ Add			Max: TD
Security		Name	Policy	Included Devices	Option
MAC Filtering Profile					
🔂 Monitoring	2				
BS Utility	>				
🖏 System Maintenance	>				
Virtual Controller					
≻ Wireless	>				

ltem	Description
+Add	Click to create a new entry.
Edit	Click to modify the selected entry.
Delete	Click to remove the selected entry.

Security / MAC Filtering Profile					
					×
Name	0				
Policy	Disabled Allow List B	lock List			
Device List	+Add		Search	Max: 128	
	Name	MAC Address ()			
		No Records Found!			
Cancel Apply					

To add a new MAC filtering profile, click the **+Add** link to get the following page.

ltem	Description									
Name	Enter the name of the pro	ofile.								
Policy	Disabled - Disable this pro	ofile.								
	If enabled, set Allow List o	or Block List.								
	Allow List - Specify only the list can access this VigorA		he MAC addı	ress defined in the						
		Block List - Specify only the name with the MAC address defined in the list will be blocked to access this VigorAP.								
Device List	It is available when Allow +Add - Create a new entry			-						
	Device List									
	+Add		Search	Max: 128						
	Name	Name MAC Address								
	TE_ST	TE_ST 14:49:BC:5D:68:92 💼 Delete								
Cancel	Discard the settings.									
Apply	Click it to save the setting	s and exit the	page.							

II-2-1-2 Backup & Restore

This page allows you to save the access control policies and black & white lists as a profile, which can be used for restoration purposes.

Search	Q	Security / MAC Filtering Profile			
		MAC Filtering Profile Backu	ip & Restore		
Device Menu	_	Backup & Restore			
 Dashboard 					
	2	Download Backup File	Download		
 security 		Restore from Backup File	D	Restore	
MAC Filtering Profile					
🖽 Monitoring	•				
BS Utility	20				
🐁 System Maintenance	2				
Virtual Controller					
}+ Wireless	>				

ltem	Description
Download Backup File	Download - Click to save the MAC filtering profile.
Restore from Backup File	Click to select the backup file (MAC filtering profile) you wish to restore. Restore - Click to retrieve the MAC filtering profile.

II-3 Virtual Controller - Wireless

This feature allows users to establish and manage a network of DrayTek devices connected by Wireless or Wired links.

The network consists of one Root and multiple Nodes. Root controls this network and syncs configurations to Nodes. Normally Root and Nodes use the same Wireless SSID/security, and Wireless clients can connect to any of them.

For Mesh networks, Root is also the outlet to the Internet. All devices of a network are in the same Group. The root can add a new Node to its Group or delete members from its Group. Users can choose VigorMesh or EasyMesh to establish the Mesh network. If Mesh is disabled, a network with wired links alone could still be established as long as AP Management is enabled.

Mesh Root and Mesh Node

Mesh Root indicates that this device would be another device's uplink connection.

As a Mesh Root, the device must connect to a gateway with an Ethernet cable first to have an Internet connection.

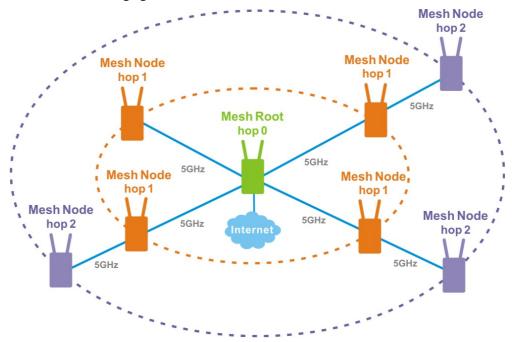
As a Mesh Node, the device can connect to the Mesh Root or Mesh Node within the same Mesh Group via Wireless or Wired links.

VigorMesh

VigorMesh is a DrayTek proprietary Mesh function. Pleae note that, within VigorMesh network,

- The total number allowed for Group members is 8 (including the Mesh Root).
- The maximum number of hop is 3.

Refer to the following figure:



EasyMesh

EasyMesh is a standard Mesh protocol of Wi-Fi Alliance.

II-3-1 Role Setup

This page can determine the role of the VigorAP connecting to the computer physically. And set up its Mesh function and AP Management function.

	۹	Wireless / Role Setup		③ Reset C Ref
	=	Role Setup		
 Dashboard 		Device Role	Auto 🗸	Advanced Mode: 0
🚊 Configuration	>	Current Device Role	Node	
Security	>	Group Admin Account	admin	
E Monitoring	5	Group Admin Password 🕕	······ •	
88 Utility	5	Password Status	Use random password	
🖏 System Maintenance	×	Mesh Setup		
		Enable Mesh		
	÷.	Mesh Protocol	Vigor Mesh EasyMesh	
		Current Uplink	Wireless	
Device		Group Name	DrayTekMesh	
		AP Management Setup		
		Enable AP Management		
		Cancel Apply		

ltem	Description					
	Role Setup					
Device Role	Auto - The device can switch between a Root and a Node based on the actual situation.					
	Root – The device is a Root. It controls the network and syncs configurations to the Nodes of its Group.					
	If Mesh is enabled, the device must connect to a gateway with an Ethernet cable to have an Internet connection.					
	Node – The device is a Node. It is managed by a Root if it has joined a Group.					
	If Mesh is enabled, the device can connect to the network through wireless.					
	Auto ~					
	Auto					
	Root Node					
Current Device Role	Displays the current role of the device.					
Group Admin Account	Set an account for the system administrator to manage the mesh nodes. The account configured here will replace the account name defined					
	for each node to ensure the mesh node's account security.					
Group Admin Password	Set a password for the system administrator to manage the mesh					

	nodes.
	The password configured here will replace the password defined for each node to ensure the mesh node's account security.
	Mesh Setup
Enable Mesh	Switch the toggle to enable/disable the mesh function.
Mesh Protocol	Select the mesh protocol to manage the mesh network.
	• Vigor Mesh - A protocol developed by DrayTek.
	• EasyMesh - A protocol defined by WiFi alliance.
Uplink	It is available only when Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Set the uplink of the device.
	 Auto - If the Ethernet port is connected and the device can access its gateway, use Wired uplink. Otherwise, use the Wireless uplink.
	• Wired - Fixed on the Wired uplink.
	• Wireless - Fixed on the Wireless uplink.
Current Uplink	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Displays the current uplink.
Group Name	Displays the name of the current Mesh Group. It is available only when Auto or Root / VigorMesh is selected as Device Role / Mesh Protocol.
	If required, change the name.
Mesh Onboarding Mode	It is available only when EasyMesh is selected as Mesh Protocol.
	• PBC - Means the push-button configuration.
Start PBC Onboarding	It is available only when EasyMesh is selected as Mesh Protocol and PBC is selected as Mesh Onboarding Mode.
	• Start PBC - Triggers the WPS connection to build network between node backhaul and the root fronthaul.
	AP Management Setup
Enable AP Management	Switch the toggle to enable/disable the AP Management.
Default AP Profile	Follow Root - Click to synchronize the same configuration to the nodes managed by root AP.
	Advanced Mode: On
Wireless Uplink Band	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Select available Wireless bands for connecting with uplink
Wireless Downlink Band	It is available only when VigorMesh is selected as Mesh Protocol.
	Select available Wireless bands for connecting with downlink.
Preferred Wireless Uplink Device	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Select a Mesh member as the first priority when choosing Wireless uplink.

Preferred Wireless Uplink Timeout(min)	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Set the time period (1 to 10 minutes) to wait for the Preferred Wireless Uplink Device.
Auto Wireless Uplinks Optimization	It is available only when Auto or Root / VigorMesh is selected as Device Role / Mesh Protocol.
	It is selected in default.
	If enabled, after changing the environment of the Mesh network, Root will perform reselect to reconstruct the Mesh network.
Log Level	It is available only when VigorMesh is selected as Mesh Protocol.
	Select Basic or Detailed. Related information will be shown on Syslog.
Cancel	Discard the settings.
Apply	Click it to save the settings.

II-3-2 Device

II-3-2-1 Device List

This page displays general information about the belonging group.

	٩	ss / Device	- ID Martin							(C) H	eset C Refresh
		List Mesh Statu	s AP Adoption								
) Dashboard	Device	e List									
Configuration										Search	Marc 2
Security		Name ::	MAC	IP Address	SSID	Status =	Role	WLAN Clients (2.4G/5G)	Firmware Version	System Uptime	Option
Monitoring		VigorAP962C	1449BC51B9AB	192.168.1.2		Online	Node	0/0	1.5.4	0d 23h 45m 23s	ØEdit
Utility											
System Maintenance	¥.										
	-										
Role Setup Device											

ltem	Description
Edit	Click to modify the settings of the selected device. The settings for the APs are slightly different based on the role of the Root and Node. Settings for the AP (as the Node):

×		
VigorAP962C	Name	
1449BC51B9A6	MAC	
192.168.1.2	IP Address	AN
	SSID	
Online	Status	
VigorAP9620	Model	
Node	Role	
0/0	WLAN Clients (2.4G/5G)	
1.5.4	Firmware Version	
0d 23h 45m 23:	System Uptime	

II-3-2-2 Mesh Status

Displays general information of the Mesh network.

This page is available only when **Mesh** is enabled (Virtual Controller>>Role Setup).

	Wireless	/ Device								C Refresh
	Device L	Ist Mesh Status	AP Adopt	tion						
	Mesh St	tatus								
b Dashboard										
Configuration	*								Search	Max: 25
Security	Name	MAC Address	Role	Hop :	Uplink Device	Uplink Interface	Signal Strength	Uplink Rate (TX/RX)	Uplink Uptime	Option
Monitoring										
Utility										
System Maintenance	*									
Role Setup										

Available settings are explained as follows:

ltem	Description
Name	Displays the name of the device (for identification).
MAC Address	Displays the MAC address of the device.
Role	Displays the role of the device.
Нор	Displays the number of Wireless links from the device to Root. "0" means the device is using a Wired uplink.
Uplink Device	Displays the MAC address of the device that this device connects to.
Uplink Interface	Displays the interface which the device is using to connect to uplink.
Signal Strength	Displays the signal strength of the device to its uplink.
Uplink Rate(Tx/RX)	It is available only when VigorMesh is selected as Mesh Protocol. Displays the link rate of the device to its uplink.
Uplink Uptime	It is available only when VigorMesh is selected as Mesh Protocol. Displays how long the device is online.
Option	Click View to modify the selected mesh device.

Mesh Status Mac Address Role Hop Uplink Device Uplink Device Oo:1D:AA:10:27:22 Oo:1D:AA:10:27:22 Name MAC Address Role Hop Uplink Device Uplink Interface Wireless SGHz (Ch36) VigorAP1062C 00:1D:AA:64:10:15 Node 1 00:1D:AA:10:27:22 Signall Strength -56dBmr/864 N1 00:1D:AA:64:10:15 Node 1 00:1D:AA:10:27:22 Signall Strength -56dBmr/864 Uplink Rate (TO/700) 1755M/1755MI Uplink Rate (TO/700) 1755M/1755MI Uplink Rate (TO/700) 1755M/1755MI Uplink Rate (TO/700) 1755M/1755MI Uplink Rate (TO/700) 1755M/1755MI Uplink Device NA Signall Strength -56dBmr/864 Uplink Rate (TO/700) 1755M/1755MI Uplink Device NA Signall Strength -56dBmr/864 Uplink Device -56dBmr/864	Device List	Mesh Status AP	Adopti	ion			C Refresh
Name MAC Address Ref Hop Uplink Device Uplink Device 00:10:AA:10:27:22 OD:10:AA:10:27:22 OD:10:AA:10:27:27 OD:10:AD:10:27:27 OD:10:AD:10:2	Mesh Status						>
VigorAP1062C 00:1D:AA:10:27:22 Root 0 N/A VigorAP1062C 00:1D:AA:10:17 Node 1 00:1D:AA:10:27:22 Signal Strength -56dBm/869 Uplink Rate (DV/R0) 1755M/1755M Uplink Rate (DV/R0) 1755M/1755M Uplink Upline 0d 02:11:22 Mesh Action Optimize Uplink Preferred Wireless Uplink Device NA	Name	MAC Address	Role	Нор	Uplink Device	Uplink Device	
N1 00:1D:AA:64:10:15 Node 1 00:1D:AA:10:27:22 Signal Strength -S6dBm/869 UpInk Rate (10/300) 1255M/1255M UpInk Uplime 0d 02:11:22 Mesh Action Optimize Uplink Preferred Wireless Uplink Device NA Set Preferred Wireless Uplink Device	VigorAP1062C	00:1D:AA:10:27:22					Wireless 5GHz (Ch36)
Uplink Uplime 0d 02:11:22 Mesh Action Optimize Uplink Optimize Uplink Preferred Wireless Uplink Device NA Set Preferred Wireless Uplink Device	NT	00:1D:AA:64:10:15	Node	15	00:1D:AA:10:27:22		-56dBm/86%
Mesh Action Optimize Uplink Optimize Uplink Preferred Wireless Uplink Device NA Set Preferred Wireless Uplink Device						Uplink Rate (TX/RX)	1755M/1755M
Optimize Uplink Optimize Preferred Wireless Uplink Device NIA Set Preferred Wireless Uplink Device						Uplink Uptime	0d 02:11:22
Preferred Wireless Uplink Device NA Set Preferred Wireless Uplink Device						Mesh Action	
Set Preferred Wireless Uplink Device						Optimize Uplink	Optimize
							N/A
						Set Preferred Wireless Uplink Device	Set

Optimize All Mesh Links - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Root.

Press the **Optimize** button to perform reselect to reconstruct the Mesh network.

Optimize Uplink - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Wireless Node.

Press the **Optimize** button to disconnect the device from Mesh network. The device might connect to a better uplink later.

Preferred Wireless Uplink Device - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Node.

Displays the Preferred Wireless Uplink of the device.

Set Preferred Wireless Uplink Device - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Node.

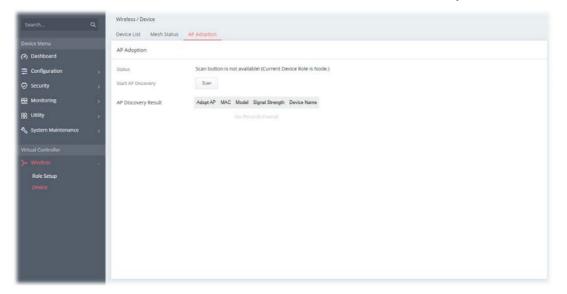
Select a Mesh member and press the **Set** button to set the Preferred Wireless Uplink Device of the device.

II-3-2-3 AP Adoption

Search and add new Nodes to the device's Group.

This page is available when Current Device Role is Root.

It is also available when Device Role is Auto and Device List contains only the device itself.



Available settings are explained as follows:

Item	Description			
Status	Displays whether the Scan button is available now.			
Start AP Discovery	Press the Scan button to search new Nodes.			
AP Discovery Result	Displays the scanned result.			
	Adopt AP - Select the checkbox if you want to add the device into a Group.			
	MAC - Displays the MAC address of the device.			
	Model - Displays the model of the device.			
	Signal Strength - Displays the signal strength of the device if it was found through the Wireless.			
	Device Name - Insert the name of the device for identification.			
Cancel	Discard current settings.			
Apply	Click to add the selected device(s) into the Group.			

Tips for VigorMesh Network Setup

 VigorMesh supports auto uplink. If a device could not access its gateway, it becomes a Wireless Node automatically.

A Mesh Root or a Wired Mesh Node should be able to ping its gateway through Ethernet.

• VigorMesh can add new Mesh Nodes into Mesh Group through both Wireless and Wired. However, we recommend to connect new Nodes to the Root by Ethernet cables and add them into Mesh Group first. Wait until the configuration sync finishes. And then move the Nodes to their destinations.

- VigorMesh supports up to 3 hops. However, it is suggested to connect the Mesh network with less than or equal to 2 hops.
- It is suggested to make the Uplink Signal Strengths of all Wireless Mesh Nodes be larger than -65 dBm.
- A Wireless Mesh Node with an Ethernet cable should not loop to another Node.
- If the Mesh Root disappears and there are online Wired Mesh Nodes with Device Role Auto, one of the Wired Mesh Nodes will become a Mesh Root automatically.
- A VigorMesh Group can be reset by the "Reset" button on Virtual Controller >> Wireless >> Device >> Device List.
 - If resetting a Mesh Root,
 - All online Mesh Nodes will be informed to reset.
 - For those Mesh Nodes unable to reset, reset them manually.
 - If resetting a Mesh Node,
 - The device will become a New Node again.
 - The Wireless SSID settings of the device will be reset, too.

Troubleshooting:

- Check the country code and Wireless channels.
- Check the firmware version. Please make sure all Mesh members are in the newest firmware version.
- Check the Current Device Role and Current Uplink of the device.
- Please make sure that the device is not in DFS CAC detection.
- Check the channel load. Make sure it is not over 70%.

Tips for EasyMesh Network Setup

- Set up multiple mesh devices with uplink RSSI larger than -65dBm.
- Setup is recommended to use wired connection and device list to add devices.
- EasyMesh network supports up to 3 hops of devices. However, it is suggested to connect with less than or equal to 2 hops.
- EasyMesh is not suggested to join existing VigorMesh Environment.
- The maximum of devices number is (ssid_num * device_num <= 56) -> device_num is the max device number

How to set up a VigorMesh group?

The following steps will guide you how to setup a VigorMesh Group.

Please access the web of the device which you want to use it as the Root.

1. (Optional) Open Virtual Controller>>Wireless>>Role Setup.

Set **Group Admin Password**. This value will be the Administrator Password of the Nodes after they join the Mesh Group and complete configuration sync.

Wireless / Role Setup		🕄 Reset 🔿 Refresh
Role Setup		
Device Role	Auto 🗸	Advanced Mode: OFF
Current Device Role	Node	
Group Admin Account 🕕	admin	
Group Admin Password (j)		
Password Status	Use random password	
Mesh Setup		
Enable Mesh		
Mesh Protocol	Vigor Mesh EasyMesh	
Current Uplink	Wireless	
Group Name	DrayTekMesh	
AP Management Setup		
Enable AP Management		
Cancel Apply		

2. Open Virtual Controller>>Wireless>>Device>>AP Adoption. Click the Scan button.

Device List Mesh Status AP Adoption AP Adoption
Status Scan button is not available! (Current Device Role is Node.)
Start AP Discovery Scan
AP Discovery Result Adopt AP MAC Model Signal Strength Device Name
No Records Found!

3. Wait until the searching result appears.

Choose the device(s) you want to add to the Group and set the names for identification.

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

Wireless / Device					
Device List Mesh Status A	P Adoption	_			
AP Adoption					
Status	Ready				
Start AP Discovery	Scan				
AP Discovery Result	Adopt AP	MAC	Model	Signal Strength	Device Name
		14:49:BC:51:B7:9F	VigorAP1062C	-92dBm(weak)	
		00:1D:AA:66:44:66	VigorAP1062C	-94dBm(weak)	
		00:1D:AA:64:10:15	VigorAP1062C	-61dBm(good)	N1
Cancel Apply					

4. Refer to Virtual Controller>>Wireless>>Device>>Device List and Virtual Controller>> Wireless >> Device >>Mesh Status for viewing the result.

Wireless / Devic	e											
Device List	Mesh Status 🛛 🗚	AP Adoptio	on							U) Reset C	Refresh
Device List												
												Max: 50
Name	MAC	IP Address	5	SSID	Status	Role	WLAN Clients (2.4G/5G)	Firm	ware Version	System Uptime	Option	
VigorAP1062C	001DAA102722	192.168.1	.10	DrayTek- 102722	Online	Root	0/0	1.5.1	_RC8	0d 4h 58m	24s 🧷 Edit	
VigorAP1062C	001DAA641015	192.168.1	.11	DrayTek- 102722	Online	Node	0/0	1147	.8df8de432f_Be	eta Od 1h 00m	45s 🧷 Edit	ሰ Delete
Wireless / Devic	:e											
Device List	Mesh Status	AP Adopti	on								C	Refresh
Mesh Status												
Name	MAC Address	Role	Нор	Uplink D	evice	Uplir	nk Interface		Signal Strength	Uplink Rate (TX/RX)	Uplink Uptime	Option
VigorAP1062C	00:1D:AA:10:27:2	2 Root	0	N/A							0d 02:15:33	© View
N1	00:1D:AA:64:10:1	5 Node	1	00:1D:A/	A:10:27:22	2 Wire	eless 5GHz (C	:h36)	-56dBm/86%	1755M/1755M	0d 02:11:22	@ View

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: Device Settings, Management, Firmware, Backup & Restore, Accounts & Permission, System Reboot, and Registration & Services.

III-1-1 Device Settings

The user can modify the time, device name, and Syslog for the device.

III-1-1-1 Time

Open System Maintenance>>Device Settings and click the Time tab.

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

Search Q	System Maintenance / Device	Settings	③Reset CRefresh
1000000000 2250	Time Device Name Sys	log SNMP	
Device Menu	Time and Date		
(?) Dashboard			
🛬 Configuration 🛛 >	System Time	2021-01-02 00:18:22	
⊘ Security →	Time Setting		
🔂 Monitoring >	Set Time	Automatically with Time Server Manually	
BS ∪tility →	Time Server	time.google.com	
🔦 System Maintenance 🚽 🚽	Time Zone	(UTC) Greenwich Mean Time : Dublin	
Device Settings	Interface	Auto	
Management			
Firmware	Daylight Saving		
Backup & Restore		Test Time Server Connection	
Account & Permission	Server Status		
System Reboot			
Registration & Services	More settings 💛		
Virtual Controller			
≻ Wireless >			
	Cancel Apply		

Available parameters are explained as follows:

ltem	Description
	Time and Date
System Time	Display current time.
	Time Setting
Set Time	 Determine the method (automatically or manually) to set the time. Automatically with Time Server - Set the system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP). Manually - Set the system time using the time reported by the web browser.
When Automatically with Time Server is	Time Server - Enter the web site of the primary time server.Time Zone - Select the time zone where the access point is located.

Daylight Saving - Enable Daylight Saving Time (DST) if it is applicable your location.Update Time - Force to renew current time setting. Connection Status - Displays last update time status.More Settings - Click to open advanced settings for the time server• Auto Update Interval - Select the time interval (30min or 60m at which the AP updates the system time periodically.• Secondary Server - For having a backup time server, please enter the URL/IP address in the field of Secondary Server.• Secondary Interface - Backup interface for renewing the time automatically.• Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date.When Manually is selected as Set Time2021-04-26 </th <th>selected as Set Time</th> <th>Interfa autom</th> <th></th> <th></th> <th>the t</th> <th>time t</th> <th>hroug</th> <th>gh the</th> <th>inter</th> <th>face selected by VigorAP</th>	selected as Set Time	Interfa autom			the t	time t	hroug	gh the	inter	face selected by VigorAP
Connection Status - Displays last update time status. More Settings - Click to open advanced settings for the time server Auto Update Interval - Select the time interval (30min or 60m at which the AP updates the system time periodically. Secondary Server - For having a backup time server, please enter the URL/IP address in the field of Secondary Server. Secondary Interface - Backup interface for renewing the time automatically. Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date. When Manually is selected as Set Time Time Zone - Select the time zone where the AP is located. Date - Use the drop-down calendar to specify correct date. 2021 APR = 2021 APR = S M T With 12 2 3 4 5 6 7 8 9 11 12 13 12 2 2 2021 APR = > 13 19 20 21 22 23 24 5 6 7 8 9 10 11 12 13 14 15 16 17 <th></th> <th colspan="8">Daylight Saving - Enable Daylight Saving Time (DST) if it is applicable to your location.</th>		Daylight Saving - Enable Daylight Saving Time (DST) if it is applicable to your location.								
 More Settings - Click to open advanced settings for the time server Auto Update Interval - Select the time interval (30min or 60m at which the AP updates the system time periodically. Secondary Server - For having a backup time server, please enter the URL/IP address in the field of Secondary Server. Secondary Interface - Backup interface for renewing the time automatically. Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date. When Manually is selected as Set Time Time Zone - Select the time zone where the AP is located. Date - Use the drop-down calendar to specify correct date. 2021-04-26 2021-04-26 2021-04-26 2021-04-26 2021-04-26 3 M T W T F S APR 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser. 		Update Time - Force to renew current time setting.								
 Auto Update Interval - Select the time interval (30min or 60m at which the AP updates the system time periodically. Secondary Server - For having a backup time server, please enter the URL/IP address in the field of Secondary Server. Secondary Interface - Backup interface for renewing the time automatically. Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date. When Manually is selected as Set Time Time Zone - Select the time zone where the AP is located. Date - Use the drop-down calendar to specify correct date. 2021-04-26 2021-04-26 S M T W T F S APR 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser. 		Conne	ection	Statu	s - Di	splay	s last	updat	te tim	e status.
at which the AP updates the system time periodically. Secondary Server - For having a backup time server, please enter the URL/IP address in the field of Secondary Server. Secondary Interface - Backup interface for renewing the time automatically. Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date. When Manually is selected as Set Time Time Zone - Select the time zone where the AP is located. Date - Use the drop-down calendar to specify correct date. 2021-04-26 2021-04-26 S M T W APR 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 25 27 28 29 30 Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser.		More	Settin	ngs - C	lick to	o opei	n adva	anced	settir	ngs for the time server.
 enter the URL/IP address in the field of Secondary Server. Secondary Interface - Backup interface for renewing the time automatically. Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date. When Manually is selected as Set Time Time Zone - Select the time zone where the AP is located. Date - Use the drop-down calendar to specify correct date. 2021-04-26 Image: Correct date. Image: Correct date. Image: Correct date. 2021-04-26 Image: Correct date. Image: Correct date. Image: Correct date. 2021-04-26 Image: Correct date. Image: Correct date. Image: Correct date. Image: Correct date. Image: Correct date. Image: Correct date.				•						
automatically. Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date. When Manually is selected as Set Time Selected as Set Time Time Zone - Select the time zone where the AP is located. Date - Use the drop-down calendar to specify correct date. 2021-04-26 2021 APR → S M T W T F S M T V S M T V Y F S M T V Y T F S APR 1 2 1 1 1 1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 <td< th=""><th></th><th></th><th>-</th><th></th><th></th><th></th><th>-</th><th>-</th><th>-</th></td<>				-				-	-	-
enabled. Enter a custom schedule to enable the DST - Defaul by Week and by Date. When Manually is selected as Set Time 2021-04-26 2021 APR - 2021-04-26 2021 APR - 2021 AP				-		ace -	Backu	ıp inte	erface	for renewing the time
selected as Set Time Date - Use the drop-down calendar to specify correct date. Date - Use the drop-down calendar to specify correct date. Date - Use the drop-down calendar to specify correct date. Date - Use the drop-down calendar to specify correct date. Date - Use the drop-down calendar to specify correct date. Date - Use the drop-down calendar to specify correct date. Date - Use the drop-down calendar to specify correct date. Date - Use the time by specify a specify correct date. Time - Set the time by specify in hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser.			enabl	ed. En	iter a	custo				
Date - Ose the diop-down calendar to spechy correct date. 2021-04-26 $3 M T W T F S$ $APR 1 2 3$ $4 5 6 7 8 9 10$ $11 12 13 14 15 16 17$ $18 19 20 21 22 23 24$ $25 26 27 28 29 30$ Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser.	When Manually is	Time 2	Zone ·	- Selec	t the	time	zone	wher	e the /	AP is located.
$2021 \text{ APR} \rightarrow \qquad \qquad \checkmark \qquad \checkmark \qquad \checkmark \qquad \checkmark \qquad \land \qquad \checkmark \qquad \land \qquad \land \qquad \land \qquad$	selected as Set Time	Date -	Use t	the dr	op-do	own c	alend	ar to :	specif	y correct date.
$2021 \text{ APR} \rightarrow \qquad $		2	2021-0	4-26			Ē	1		
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$										t
APR123456789101112131415161718192021222324252627282930Time - Set the time by specifying hours, minutes, and seconds.Synchronize with Browse - Click Sync now to sync the time setting the browser.			202	1 APR	*			<	>	~
456789101112131415161718192021222324252627282930Time - Set the time by specifying hours, minutes, and seconds.Synchronize with Browse - Click Sync now to sync the time setting the browser.			S	М	Т	W	Т	F	S	
1112131415161718192021222324252627282930Time - Set the time by specifying hours, minutes, and seconds.Synchronize with Browse - Click Sync now to sync the time setting the browser.			APF	2			1	2	3	
18 19 20 21 22 23 24 25 26 27 28 29 30 Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser.			4	5	6	7	8	9	10	
25 26 27 28 29 30 Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser.			11	12	13	14	15	16	17	
Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting the browser.			18	19	20	21	22	23	24	
Synchronize with Browse - Click Sync now to sync the time setting the browser.			25	26	27	28	29	30		
Synchronize with Browse - Click Sync now to sync the time setting the browser.										
ApplySave the current settings and renew the system time.		Synch	ronizo	e with	-	-				
	Apply	Save t	he cu	rrent	settir	ngs an	d ren	ew th	e syst	em time.
Cancel Discard current settings and return to the previous page.						-			-	

After finishing this web page configuration, please click **Apply** to renew the system time.

III-1-1-2 Device Name

Display the device name. Change the name if you want.

Open System Maintenance>>Device Settings and click the Device Name tab.

	System Maintenance / Device	Settings	③ Reset
Device Menu	Time Device Name Sy	slog SNMP	
 Dashboard 	Device Name		
	> Device Name ()	VigorAP962C	
Security	5		
G Monitoring			
88 Utility	5		
Management			
Firmware Backup & Restore			
Account & Permission			
System Reboot			
Registration & Services			
≻ Wireless	s		
	Cancel Apply		

III-1-1-3 Syslog

SysLog function is provded for users to monitor the device.

Open **System Maintenance>>Device Settings** and click the **Syslog** tab.

Search Q	System Maintenance / Devi	ce Settings		() Reset
Device Menu	Time Device Name Syslog Settings	 SNMP External Server User Access Log LAN Log System Log WiFi Basic Log Mesh Log APM Log 		
Firmware Backup & Restore Account & Permission System Reboot Registration & Services Virtual Controller J+ Wireles >	+Add Server IP () 192.168.1.10	Port () 514	Max: 3 Option	
	Cancel Apply			

Available parameters are explained as follows:

Item Description					
Syslog Settings					
Logging Destinations Select External Server to display Log Message and Syslog Servers for					

	detailed configuration.
Log Message	Select to send the corresponding message of user access, interface, and system information to Syslog.
	Syslog Servers
+Add	Click to display new entry boxes for creating a new Syslog server profile.
	The maximum number of Syslog servers to be added is "3".
Server IP	Enter the IP address of the Syslog Server.
Port	Enter the port number of the Syslog Server.
Option	Delete - Click it to remove the selected server profile.
Apply	Save the current settings and exit the page.

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

III-1-1-4 SNMP

This section allows you to configure settings for SNMP services.

The SNMPv3 is more secure than SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.

	System Maintenance / Device	e Settings	D Reset
	Time Device Name Sy	/slog	
	SNMP		
 Dashboard 	State		
🛱 Configuration 🔊	Enabled		
Security >	Manager		
Monitoring >	Manager Host	Any Specific Hast	
BS Utility >			
	Query		
	Get Community ()	public	
Management	Set Community ()	private	
Firmware	Query Port	161	
Backup & Restore	1910610101		
Account & Permission	Agent		
System Reboot			
Registration & Services	SNMPv3 Agent Enabled		
Virtual Controller	SNMPv2c Agent Enabled		
	SNMPv1 Agent Enabled		
> Wireless			
	Cancel Apply		

Available parameters are explained as follows:

ltem	Description		
	SNMP		
Enabled	Switch the toggle to enable/disable the SNMP function. If enabled, Manager, Query, Agent and Trap settings will be valid for you to configure.		
	Manager		
Manager Host	Any - Any IP can be set as the manager host. Specific Host - Specify a host (IPv4 or IPv6) or hosts (both IPv4 and		

IPv6). Enter the IPv4 address with subnet mask / IPv6 address with specified prefix length of hosts that are allowed to issue SNMP commands. If these field are left blank, any IPv4/IPv6 LAN host is allowed to issue SNMP commands. Query
prefix length of hosts that are allowed to issue SNMP commands. If these field are left blank, any IPv4/IPv6 LAN host is allowed to issue SNMP commands.
Query
Enter the Get Community string. The default setting is public . Devices that send requests to retrieve information using get commands must pass the correct Get Community string. The maximum allowed length is 23 characters.
Enter the Set Community string. The default setting is private . Devices that send requests to change settings using set commands must pass the correct Set Community string. The maximum length of the text is 23 characters.
Displays the port number used by the query server.

Agent

		-gent						
SNMPv3 Agent Enabled	Switch the toggle to	o enable/d	isable the SNMPv3	8 function.				
	If enabled, specify corresponding settings.							
	SNMPv3 Agent Enabled							
	+Add M.							
	Username (USM)	Authentication	Authentication Password	Privacy	Privacy Password			
		sha \sim	٢	Disabled \vee				
	SNMPv2c Agent Enabled	Disabled						
	SNMPv1 Agent Enabled	MD5						
		SHA						
	Username(USM) - USM means user-based security mode.							
	Enter the username to be used for authentication. The maximum allowed length is 23 characters.							
	Authentication - Select one of the hashing methods to be used with the authentication algorithm.							
	Authentication Password - Enter a password for authentication. The maximum allowed length is 23 characters.							
	Privacy - Select an encryption method as the privacy algorithm.							
	Privacy Password - Enter a password for privacy. The maximum allowed length is 23 characters.							
SNMPv2c Agent Enabled	Switch the toggle to	enable/d	isable the SNMPv2	function.				
SNMPv1 Agent Enabled	Switch the toggle to	o enable/d	isable the SNMPv1	function.				
		Trap						
	1							

Пар		
Enabled Switch the toggle to enable/disable the Trap function.		
Trap Version	Select the trap version. V1	

	• V2c
	• V3
Trap Community	Enter the Trap Community string. The default setting is public. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string. The maximum length of the text is 23 characters.
Trap Port	Enter the port number used for the Trap server.
Notification Host IP Type	 Select the type of the notification host. Both IPv4 IPv6
Notification Host(IPv4)	+Add - Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
Notification Host(IPv6)	+Add - Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
Trap Events	Select the event(s) to apply the settings configured in this page.
Apply	Save the current settings and exit the page.

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

III-1-2 Management

III-1-2-1 Service Control

This page allows you to manage the general settings, management services, and TLS/SSL Encryption setup.

	System N	Aaintenance / I	Management		
	-	ontrol TR-0	069 System	n information	
 Dashboard 	General				
출 Configuration >	Auto Log	out	0	ff	
🤉 Security 💦 💡	Manage	ment Services			
a Monitoring		ITTPS Access			
g Utility >		ITTPS Access			
	ANOW PIN	IG HOM DAN			
Device Settings		Port ()	(default)	LAN Access	
	HTTP	80	(80)	•	
Firmware	HTTPS	443	(443)	٠	
Backup & Restore Account & Permission	SSH	22	(22)	•	
System Reboot	Telnet	23	(23)		
Registration & Services					
	SNMP	161	(161)		
⊷ Wireless >	TLS/SSL	Encryption			
	TLS 1.3			D	
	Cancel	Apply			

lé a ma	Description
item	Description

	General
Auto Logout	If "off" is selected, the function of auto-logout for the web user interface will be disabled. The web user interface will be open until you click the Logout icon manually.
	off ~
	off
	1 min
	3 min
	5 min
	10 min

	Management Services
Enforce HTTPS Access	Enable the checkbox to allow system administrators to login Vigor device via HTTPS.
Allow PING from LAN	Allow all PING packets from LAN.
Port	Specify user-defined port numbers for the HTTP, HTTPS, SSH, Telnet and SNMP servers.
LAN Access	Select the checkbox to allow system administrators to login from LAN interface.
	TLS/SSL Encryption
TLS 1.3/TLS 1.2	Switch the toggle to enable the function of TLS 1.3/1.2 if required.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

(i) Note:

Switch these two icons by click the mouse cursor on them.

) - means "Enable".

- means "Disable".

III-1-2-2 TR-069

Vigor device supports the TR-069 standard for remote management of customer-premises equipment (CPE) through an Auto Configuration Server, such as VigorACS.

Search Q	System Maintenance / Management	③ Reset C Refresh
	Service Control TR-069 System Information	
Device Menu	ACS and CPE Settings	
 Dashboard 	ACS and CPE Settings	
🛱 Configuration >	TR 069	
Security >	ACS Server	
🔂 Monitoring 🧼 🥠	ACS Server On None V	
B Utility	URL () http:// Witard	
🐴 System Maintenance 🧠	Username 💿	
Device Settings	Password ()	
Management		
Firmware	Event Code PERIODIC V	
Backup & Restore	Test With Inform	
Account & Permission	Last inform Response Time	
System Reboot		
Registration & Services	More settings 💛	
Virtual Controller		
}⊷ Wireless >		
	Cancel Apply	

ltem	Description			
TR-069	Switch the toggle to enable or disable the function.			
	If enabled, settings available for TR-069 will be shown below.			
	ACS Server			
ACS Server On	Choose the interface for connecting the AP to the Auto Configuration Server.			
URL	Enter the URL for connecting to the ACS.			
	Wizard - Click it to enter the IP address of VigorACS server, port number and the handler.			
Username/Password	Enter the credentials required to connect to the ACS server.			
Event Code	Use the drop down menu to specify an event to perform the test.			
	Test With Inform - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS server.			
Last Inform Response Time	Display the time that VigorACS server made a response while receiving Inform message from CPE last time.			
	More settings			
CPE Client	This section specifies the settings of the CPE Client.			
	Protocol - Select Https if the connection is encrypted; otherwise selec Http.			
	Port - In the event of port conflicts, change the port number of the CPE.			
	Username / Password - Enter the username and password that the			

	VigorACS will use to connect to the CPE.
Periodic Inform Settings	 Enable / Disable - Switch the toggle to enable or disable the function. The default setting is Enable, which means the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field. Time Interval - Set interval time or schedule time for the device to send notification to CPE.
STUN Settings	Enabled / Disabled - Select to enable or disable the function.
	If select Enabled , please enter the relational settings listed below:
	• Server Address - Enter the IP address of the STUN server.
	• Server STUN Port - Enter the port number of the STUN server.
	 Minimum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	 Maximum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Apply	Save the current settings and exit the page.
Cancel	Discard current settings and return to the previous page.

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

III-1-2-3 System Information

The System Information displays basic information (e.g., device name, LAN MAC, firmware version, build date/time, ACS server and etc.) of Vigor device.

Search Q	System Maintena	nce / Management	C Refresh
	Service Control	TR-069 System Information	
Device Menu	System_Informa	tion	
 Dashboard 	System		
	Device Name	VigorAP962C	
⊘ security >	LAN MAC	14:49:BC:51:B9:AB	
🔂 Monitoring 🔋	System Uptime	1d 0h: 50m: 195	
😫 Utility 🕠	Firmware	1.5.4	
🔦 System Maintenance 🔍	ACS Server	•	
Device Settings		See More +	
Management			
Firmware			
Backup & Restore			
Account & Permission			
System Reboot			
Registration & Services			
Virtual Controller			
γ+ Wireless א			

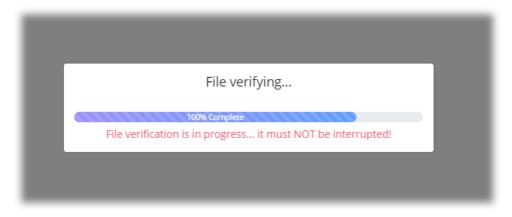
III-1-3 Firmware

Before firmware upgrade, please **download** the newest firmware from the DrayTeks website or FTP site **first**. The DrayTek website is www.draytek.com (or local DrayTeks website) and the FTP site is ftp.draytek.com.

Open **System Maintenance>>Firmware**. 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).

Search	Q.	System Maintenance / Firmware
		Firmware
Device Menu	_	
(?) Dashboard		Current Firmware Version 1.5.4
	•	Firmware for upload D Upload
Security		
🔂 Monitoring		
88 Utility	20	
	14	
Device Settings		
Management		
Backup & Restore		
Account & Permission		
System Reboot		
Registration & Services		
≻ Wireless	- 22	

Then click **Upload** and wait for a few seconds.



When the upload is finished, please click the **Restart** button.

ad		×
	Congratulations	
	File Uploaded	
	Please restart to apply changes.	

Wait for a while until the system finishes the rebooting.

	×
Rebooting	
Web UI will be redirected in few seconds.	
65 4 SECONDS	
Or Access Now \rightarrow	

III-1-4 Backup and Restore

This function can be used to backup/restore the **VigorAP** settings.

SearchQ.	System Maintenance / Backup & Restore
Device Menu	Download Configuration Backup
🔿 Dashboard	Download Configuration Backup
 ⇒ Configuration → ⊘ Security → 	Password Drotection
Monitoring >	Dewnlead Dewnlead
😵 Utility 🥎	Restore from a Configuration Backup
Device Settings	Restore from Backup File
Management Firmware Backup & Restore Account & Permission	Restore Password ()
System Reboot Registration & Services	
> Wireless >	

ltem	Description						
Download Configuration Backup							
Password Protection	For the sake of security, the configuration file for the access point can be encrypted. Switch the toggle to enable or disable the function.						
Password	Enter several characters as the password for encrypting the configuration file.						
Download	Click it to backup the configuration file.						
	Restore from a Configuration Backup						
Restore from Backup File	Click to locate the file for restoring. Restore - Click to execute the restoration.						
Restore except the login password	Switch the toggle to enable or disable the function.						
File has Password Protection	Switch the toggle to enable or disable the function. If enabled, a password will be required for restoring the configuration.						
Restore Password	Enter a password for configuration restoration.						

III-1-5 Accounts & Permission

This page allows you to modify current administration account and password.

Search Q	seteration.	ntenance / Account &					() Res	et C Refresh
evice Menu	Local Admin		ermission					
ት Dashboard	Local Admi	n Account						
Configuration	+ Add							Max
Security >	Account	Role	Status	Last Login at	Last Login IP	Created Time	Option	
Monitoring	admin	Administrator	Active	2021-01-01 19:57:19	192.168.1.10	51	Ø Edit	🖄 Delete
Utility >								
System Maintenance								
Device Settings								
Management								
Firmware								
Backup & Restore								
Account & Permission								
System Reboot								
Registration & Services								
rtual Controller								
Wireless								

III-1-5-1 Local Admin Account

Available settings are explained as follows:

ltem	Description			
+Add	Create a new account profile.			
Edit	Modify the selected account profile.			
Delete	Remove the selected account profile.			

To modify an existing profile, select the one and click the **+Edit** link to open the setting page.

To add a new profile, Click **+Add**.

System Maintenance / Account	& Permission	
Account 🕕	admin	
New Password 🕕		0
		Medium
Confirm New Password 🕕		٢
Role	None	~
Status	Active	~
Account Info		
Created Time		
Cancel Apply		

Available settings are explained as follows:

ltem	Description					
	Local Admin Account					
Account	Display the name of the account.					
New Password	Enter a new password in this field. The length of the password is limited to 83 characters.					
Confirm New Password	Enter the new password again.					
Role	Specify the role of the account.					
	Administrator					
	Guest					
	 User-defined role (created on the Role & Permission page) 					
Status	Active - Enable the selected account profile.					
	Inactive - Disable the selected account profile.					
Cancel	Discard current settings and return to the previous page.					
Apply	Save the current settings and exit the page.					

Click **Apply** to save the settings.

III-1-5-2 Role & Permission

This page allows to create new roles which can be applied to local admin account.

The default roles are Administrator and Guest.

Search Q	System Maintenance / Account & P	ermission		3 Rese
	Local Admin Account Role & Pe	ermission		
	Role & Permission			
🛛 Dashboard				
🛱 Configuration >	+Add		Max: 64	
Security >				
G Monitoring	Role	Administrator	Guest	
B Utility	Left Menu Path			
	 Device Menu 	Read-write	Read-only	
Device Settings	 Dashboard 	Read-write	Read-only	
Management	 Configuration 	Read-write	Read-only	
Firmware	▶ Security	Read-write	Read-only	
Backup & Restore	 Monitoring 	Read-write	Read-only	
Account & Permission System Reboot	▶ Utility	Read-write	Read-only	
Registration & Services	 System Maintenance 	Read-write	Read-only	
irtual Controller	 Virtual Controller 	Read-write	Read-only	

Available settings are explained as follows:

Item	Description		
+Add	Create a new role profile.		
Role	Lists all of the features that a role can have.		

To create a new role profile, click **+Add**. A new role will be added on to the page.

ystem Maintenance / /	Account & Permission			3
ocal Admin Account	Role & Permission			
Role & Permission				
FAdd			Max: 64	
Role	Administrator	Guest	Role_1	
Left Menu Path			逾 Delete	
Device Menu	Read-write	Read-only	Read-only 🖌	
Dashboard	Read-write	Read-only	Read-only 👻	
 Configuration 	Read-write	Read-only	Read-only 👻	
Security	Read-write	Read-only	Read-only 👻	
 Monitoring 	Read-write	Read-only	Read-only 👻	
▶ Utility	Read-write	Read-only	Read-only 👻	
 System Maintenar 	nce Read-write	Read-only	Read-only 🗸	
Virtual Controller	Read-write	Read-only	Read-only 🗸	

ltem	Description					
+Add	Create a new role profile.					
Role_1	The field of profile name. New added profile will be named as Role_# To modify the name, simply click the name and enter a new string (e.g., Role_MKT).					
	System Maintenance / Account & Permission					
	Local Admin Account Role & Permission					
	Role & Permission					
	+Add					
	Role Administrator Guest Role_MKT ×					
	Left Menu Path					
Left Menu Path	Lists all of the features that a role can have.					
	The role of Administrator have the highest authority for accessing VigorAP.					
	The role of Guest have the lowest authority for accessing VigorAP.					
	The authority of the user-defined roles must be based on the conditions selected respectively.					
Delete	Remove the selected user-defined role profile.					

Read-only 🗸	Specify the permission for each menu item for the user-defined role. Deny - The permission for the menu item on the left side is not allowed for the user-defined role profile.
 Deny	Read-only - The permission for the menu item on the left side allowed for the user-defined role profile to be read-only.
Read-only Read-write	Read-write - The permission for the menu item on the left side allowed for the user-defined role profile to be both read-only and written.
Apply	Save the current settings and exit the page.

After finished the settings, click **Apply.** The new role can be seen and selected on **System Maintenance>>Account & Permission>>Local Admin Account**.

	intenance / Accoun n Account Role				>
Local Adm	in Account			Account ()	admin
+ Add				Current Password ()	4
Account	Role	Status	Last Login at	New Password 🕕	4
admin	Administrator	Active	2021-01-01 19:57:19		We
				Confirm New Password ()	
				Role	Administrator
				Status	None
				Account Info	Administrator
				Created Time	Guest
					Role_MKT
				New role	/

III-1-6 System Reboot

The Web user interface may be used to restart your VigorAP. Open **System Maintenance >> System Reboot** to get the following page.

Search Q	System Maintenance / System R	eboot
Device Menu	System Reboot	
(?) Dashboard	Reboot With	Current Configuration Factory Default
🔹 Configuration 🔋		Reboot
Security	Auto Reboot Time Schedule	
🛃 Monitoring >	Enable Auto Reboot Schedule	
路 Utility ,	Schedule Profile	select your options
🔦 System Maintenance 💪		
Device Settings		
Management Firmware		
Backup & Restore		
Account & Permission		
System Reboot		
Registration & Services		
Virtual Controller		

Item	Description
Reboot With	Select one of the following options, and press the Reboot button to reboot the VigorAP.
	Current Configuration – Select this option to reboot the VigorAP. using the current configuration.
	Factory Default – Select this option to reset the VigorAP's configuration to the factory defaults before rebooting.
Reboot	Reboot the device immediately.
Enable Auto Reboot Schedule	Switch the toggle to enable/disable the auto reboot schedule function. If it is enabled, select the schedule profile as the basis to reboot the router.
Schedule Profile	Select up to 4 user-configured schedules.

This page is left blank.

Chapter IV Others



IV-1 Monitoring

IV-1-1 DHCP Table

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

Click **Refresh** to reload this page with the most up-to-date information.

IV-1-1-1 IPv4 DHCP Subnet

Search	۹	Monitoring / Di	HCP Table					C Refresh
Device Menu		IPv4 DHCP Sul	ppat					
(?) Dashboard		inverbiter but	onec					
🚔 Configuration	2						Search	Max: 255
Security	•	Name 🕤	DHCP Server Status	IP Range	IP Pool	Used IP	Utilization 🕘	
🖽 Monitoring		[LAN] LAN1	Disabled					0%
DHCP Table								
ARP Table								
Web Syslog								
Clients List								
88 Utility	->							
🖏 System Maintenance	*							
Virtual Controller								
}- Wireless	*							

IV-1-1-2 IPv4 DHCP Lease

	Q	Monitoring / D	HCP Table					C Refresh
		IPv4 DHCP Sub	onet IPv4 DHCP Lea	ise				
		IPv4 DHCP Le	200					
ව Dashboard		Inve brief be	a3e					
E Configuration						Sea	irch	Max: 25
Security	*	Subnet	IP Address	MAC Address	Host Name	Туре 👳	Leased Time	
				No R				
ARP Table								
Web Syslog								
Web Syslog Clients List								
Clients List	,							
	> >							
Clients List								

IV-1-2 ARP Table

The table shows the contents of the ARP (Address Resolution Protocol) cache held in the router and shows the mappings between Ethernet hardware addresses (MAC Addresses) and IP addresses.

Click **Refresh** to reload this page with the most up-to-date information.

Search	a	Monitoring / AF	RP Table			C Refresh
Device Menu		LAN Ethernet	ARP Table			
 Dashboard 		🗇 Clear All			Search	Max: 255
😅 Configuration		Interface	IP Address	MAC Address	Host Name	Port 🗧
Security	>	LAN1	192.168.1.10	08:8F:88:D5:DD:A9	A 1	P1
S Monitoring	*					
DHCP Table						
ARP Table						
Web Syslog						
Clients List						
88 Utility	2					
🖏 System Maintenance	2					
Virtual Controller						
≻ Wireless	>					

IV-1-3 Web Syslog

Log related to setting configuration and/or actions performed by this device can be stored on web Syslog.

Search	Q	Monitoring / Web Syslog			C Refresh
Device Menu		Web Syslog			
 Dashboard 		Enabled Web Syslog			
😴 Configuration	>	Loop Logging Option	Override Oldest Logs Stop when Full]	
⊘ Security	>				
		🗹 Export 🛛 🗎 Clear All		Filter: All Type 🗸 Search	Max: 200
DHCP Table		Time 🕁	Туре 🝵	Content	
ARP Table			No Records F		
Web Syslog					
Clients List					
路 Utility	>				
🖏 System Maintenance	×				
Virtual Controller					
> Wireless	>				
		Cancel Apply			

Available settings are explained as follows:

ltem	Description
Enabled Web Syslog	Switch the toggle to enable or disable the function. If enabled, Loop Logging Option will be shown as follows.
Loop Logging Option	Override Oldest Logs - Vigor router system will backup all existed information on the flash onto the host and clean up the information from the flash. Later, it will start a new record.
	Stop when Full - Vigor router system will stop to record the user information onto the flash.
Export	Click it to export the log records as a file (.json).
Clear All	Click it to clear all log records on this page.
Filter	Select the type of log to display on this page.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

Click **Apply** to save the settings.

IV-1-4 Clients List

It provides the information related to the wireless clients connecting to the VigorAP 962C.

Search	Q	Monitoring	/ Clients	List											CRef	resh
		Clients List														
 Dashboard 		Se Add MA	C Filteri	ng from Cl	ients Ma	x: 512							Searc	h	3	٠
	•	Name :	MAC :	Up Time	Link Speed	RSSI S	SID Usag	e Usage Down	СН	Band	BW :	PSM :	Physical Mode	Auth Mode	Encryp Type	
Security																
DHCP Table																
ARP Table																
Web Syslog																
88 Utility																
🖏 System Maintenance																
⊁ Wireless	>															

IV-2 Utility

IV-2-1 Ping Tool

The user can perform the ping job for specified IP (host) to diagnose if the data transmission via the Vigor system is well or not.

Search	Utility / Ping Tool						
	Ping Tool						
Device Menu	Ping from Auto 🗸						
🛱 Configuration	Pling to Host/IP Address () 192.168.1.10						
Security	Packet Size (byte) 64						
G Monitoring	Ping Count 4 V						
88 Unity	Ping Interval (sec.) 1 V						
	Clear Run						
Trace Tool							
Web CLI							
🗞 System Maintenance							
≻ Wireless							

ltem	Description
Ping from	Choose Auto for the router to select the WAN interface.
Ping to Host/IP Address	Enter the host / IP address that you want to ping.
Packet Size (byte)	Select the packet size for the ping job.
Ping Count	Select the quantity of the packet being pinged.
Ping Interval (sec.)	Select a time interval (unit:second) for the system to ping the IP address specified above.
Clear	Remove the settings and return to the factory settings.
Run	Perform the ping job.

IV-2-2 Trace Tool

The user can perform the traceroute job for specified IP (host) to diagnose if the data transmission via the Vigor system is well or not.

Security Protocol Monitoring Host / IP Address Utality Trace Count Ping Tool Max Hop Max Hop 30 Trace Tool Ctear Web CLI Host / IP Address system Maintenance Host / IP Address	iearch Q	Utility / Trace Tool	
Dashboard IP Version Configuration Trace Through Security Protocol Monitoring Hott / IP Address Unlity Trace Count Ping Tool Max Hop Trace Tool Clear Run Web CLI System Maintenance		Trace Tool	
Configuration Trace Through Security Protocol Monitoring Hott / IP Address Lutity Trace Count Ping Tool Max Hop Trace Tool Clear Web CLI system Maintenance autor		-	
Security Protocol Monitoring Host / IP Address Unitry Trace Count Ping Tool Max Hop 30 Trace Tool Web CLI Clear system Maintenance stual Controller	Dashboard	IP Version	(Pod
Monitoring Host / IP Address Unitity Trace Count Ping Tool Max Hop Trace Tool Cear Web CLI System Maintenance	Configuration >	Trace Through	Auto 🗸
Initiv Trace Count Initiv Trace Count Initiv Initiv Ping Tool Max Hop Inite Cool Clear Web CLI System Maintenance	Security >	Protocol	ICMP UDP
Ping Tool Max Hop Trace Tool Clear Web CLI Run system Maintenance	Monitoring >	Host / IP Address	
Trace Tool Clear Num Web CLI System Maintenance	untry	Trace Count	3 ~
Web CLI System Maintenance tual Controller	Ping Tool	Max Hop	30 🗸
System Maintenance	Trace Tool		Clear Run
tual Controller	Web CLI		
	System Maintenance 3		
Wireless >	tual Controller		
	Wireless		

ltem	Description				
IP Version	Select the IP version. At present, only IPv4 is available for selection.				
Trace Through	Trace through specific interface. Only Auto is available for selection.				
Protocol	Select ICMP or UDP protocol.				
Host/IP Address	Enter the host / IP address that you want to traceroute.				
Trace Count	Select the max hops for traceroute, select none for unlimited.				
Мах Нор	Set the maximum number of hops to search for the target.				
Clear	Remove the settings and return to the factory settings.				
Run	Perform the ping job.				

IV-2-3 Web CLI

It is not necessary to use the telnet command via DOS prompt. The changes made by using web console have the same effects as modified through web user interface. The functions/settings modified under Web Console also can be reviewed on the web user interface.

Click the Web Console icon on the top of the main screen to open the following screen.

Open the page of **Utility>>Web CLI**.

Search Q	Utility / Web CLI Web CLI
Device Menu	
 Dashboard 	
	, Username: admin Password:
Security	Passworu:
🔂 Monitoring	, vigor>
BS Ottility	help Show available commands quit Disconnect
Ping Tool	history Show a list of previously run commands
Trace Tool	enable Turn on privileged commands
	exit Exit from current mode config Configure
🖏 System Maintenance	exec execute
Virtual Controller	vigor>
}⊷ Wireless	

Chapter V Mobile APP, DrayTek Wireless



V-1 Introduction of DrayTek Wireless

VigorAP 962C supports Android/iOS APP : DrayTek Wireless. The mobile user can find the APP through Apple App Store / Google Play Store.

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

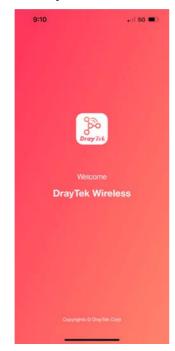
(i) Note:

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

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

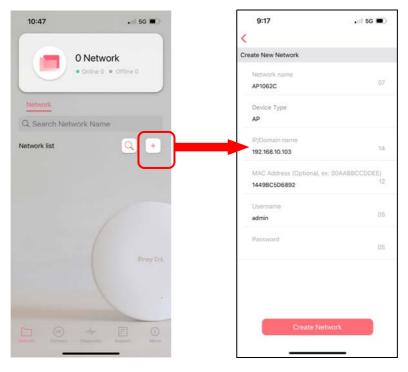
V-2 Create a New Network

1. Run DrayTek Wireless APP.

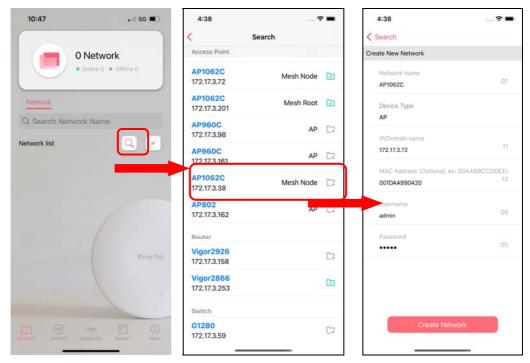


- 2. The system will open the NETWORK page to ask you create a new network first.
- 3. There are two methods for creating a new network. Click "+" or press the search button

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



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



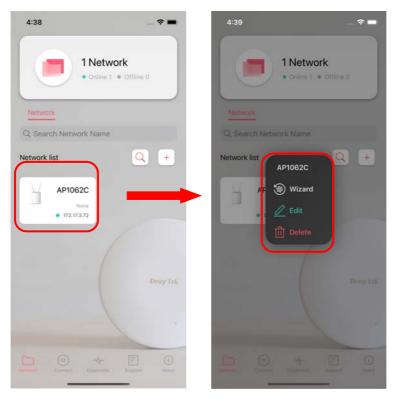
4. After clicking **Create Network**, a new network will be shown on the screen.

4:38	
	letwork
Network	
Q Search Network N	lame
Network list	Q +
AP1062C Norm	
	DrayTek
	nder 🗊 🕕



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

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



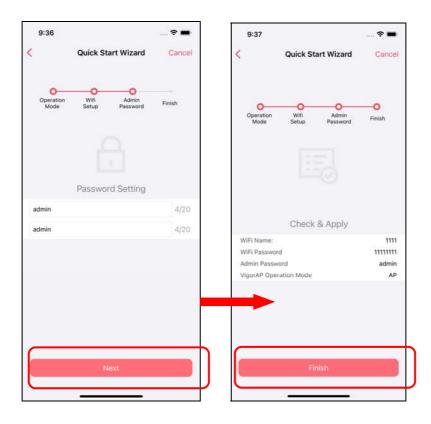
2. On the next page, enter the SSID and the password for VigorAP and click **Connect.** When a summary page appears, click the **Next** button.

9:25	🗢 🔳	9:25	🕈 🔳
Establish con	nection	K Establ	ish connection
1		SSID	Dray920
LPm		Device MAC	00:1D:AA:99:04:20
		Assigned IP	172.17.3.103
Enter your SSID &	k Password		
Scan QR Code	[38]		
SSID Dray920	0/32		
Password ••••••	0/64		
Connec	t		Next
	F	Conn	ect to another
Network Connect Diagnostic			

3. Enter the username and the password of VigorAP, click **OK**. On the WiFi Name & Password page, define the WiFi Name and the Password. Then click the **Next** button.

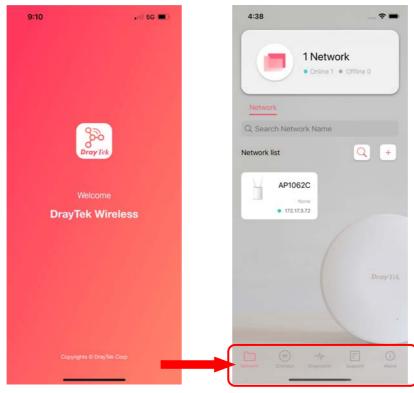
9:25	🗢 🔳	9:36		🕈 🔳
< Establis	sh connection	< Back	Quick Start Wizard	Cancel
SSID Device MAC Assigned IP	Dray920 00:1D:AA:99:04:20 172.17.3.103	Operation	Wifi Admin Setup Password	Finish
Enter Userr	name and Password	V	Vifi Name & Password	3/32
Cancel	ОК	1111111		7/64
	Next			
Conne	ct to another		Next	

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





Run DrayTek Wireless APP.



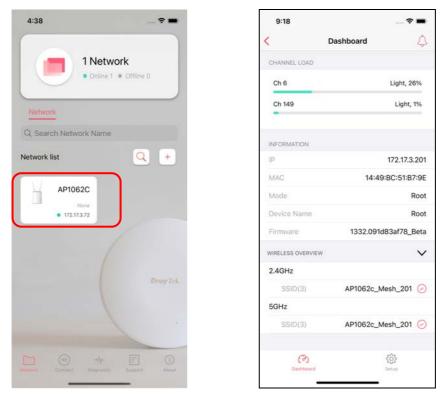
Available settings are explained as follows:

ltem	Description
Network	Create a new network.
Connect	Connect to a device (AP/CPE).
Diagnostic	Analyze the current Wi-Fi network to check the network quality.

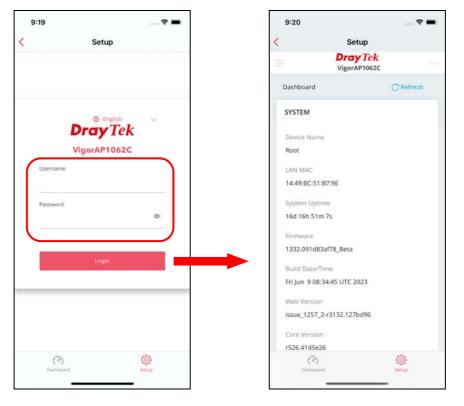
Support	Display a list of models supported by this APP.
About	Display the version information of this APP.

V-4-1 Setup

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



Click **Setup** to access into the web user interface of VigorAP 962C. On the following page, enter the username and the password. Click **Login** to get the dashboard of the access point.



Chapter VI Troubleshooting



VI-1 Checking the Hardware Status

Follow the steps below to verify the hardware status.

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

VI-2 Checking the Network Connection Settings

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

VI-3-1 For Windows

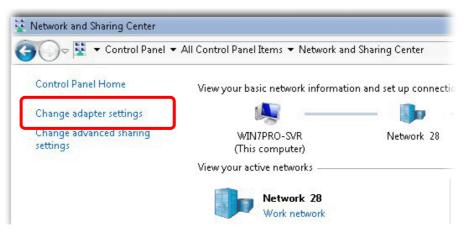
(Note:

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

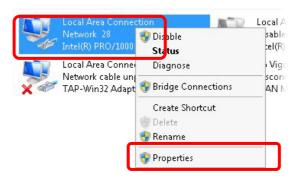
1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



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



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



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

Mahuarking Cot	
Networking Sharing	
Connect using:	
1ntel(R) PR0/1000 MT Network Connection	_
, Configure	٦
This connection uses the following items:	-
🗹 🍨 Client for Microsoft Networks	
🗹 📕 Privacyware Filter Driver	
☑ ➡ ➡ QoS Packet Scheduler □ ➡ ➡ File and Printer Sharing for Microsoft Networks	
Internet Protocol Version 6 (TCP //P -6)	
✓ Internet Protocol Version 4 (TCP/IPv4)	
Link-Layer Topology Discovery Mapper 170 Driver Link-Layer Topology Discovery Responder	
Install Uninstall Properties	1

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

'ou can get IP settings assigned his capability. Otherwise, you r					
or the appropriate IP settings.	1000 00 001	(your i	10011101	it dann	
Obtain an IP address auto	matically	ר			
- C Use the following IR addre		┛			
IP address:					
Subnet mask:					
Default gateway;	Γ		5		
Obtain DNS server addres	is automati	cally	٦		
C Use the following DNC com	ver eddree		J		
Preferred DNS server:		8	4	Ч. Т	
Alternate DNS server:	Γ	12			
🗖 Validate settings upon ex	it			Adv	vanced

VI-3-2 For Mac Os

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

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

VI-3 Pinging the Device

The default gateway IP address of the device is 192.168.1.2. For some reason, you might need to use "ping" command to check the link status of the device. **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 device correctly.

VI-3-1 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.

🐼 Command Prompt	- 🗆 X
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 = Oms, Maximum = Oms, Average = Oms	
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.

VI-3-2 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.

- 2014ch-2010ch-2020 cbi - 02 - 02 - 02 - 02 - 02 - 02 - 02 - 0	000	Terminal — bash — 80x24	
/igor10:~ draytek\$ ping 192.168.1.1 PING 192.168.1.1 (192.168.1.1): 56 data bytes 54 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms 54 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms 54 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms 54 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms 54 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms 54 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms	그는 성상 것이 이렇게 깨끗 생각하는 것이 가지 않았다. 이 것 같아요.	3 02:24:18 on ttyp1	8
PING 192.168.1.1 (192.168.1.1): 56 data bytes 54 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms 54 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms 54 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms 54 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms 54 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms 56	142 - 2686 - 66 - 2040-00 - 1		
54 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms 54 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms 54 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms 54 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms 54 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms 54 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms			
54 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms 54 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms 54 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms 54 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms 50			
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 ℃	64 bytes from 192.16	68.1.1: icmp_seq=0 ttl=255 time=0.755 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 MC	64 bytes from 192.16	68.1.1: icmp_seq=1 ttl=255 time=0.697 ms	
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms C	64 bytes from 192.16	68.1.1: icmp_seq=2 ttl=255 time=0.716 ms	
Ċ	64 bytes from 192.16	68.1.1: icmp_seq=3 ttl=255 time=0.731 ms	
- 2014ch-2010ch-2020 cbi - 02 - 02 - 02 - 02 - 02 - 02 - 02 - 0	64 bytes from 192.16	68.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
102 169 1 1 pipe statistics	^C		
172.100.1.1 ptny stutistics	192.168.1.1 ping	g statistics	
5 packets transmitted, 5 packets received, 0% packet loss	그 모든 물질에서 가지 않아? 이 것 같아. 그 말 안 가지 않는 것 같아. 가지 않아?	그는 사람이 가슴을 많은 것이 없다. 것은 것은 것이 많은 것에서 사람들은 것이 가지 않는 것이 같아요. 것은 것은 것은 것은 것은 것은 것은 것은 것이 없는 것이 같이 없다. 것은 것은 것은 것이 없는 것이 없다. 것은 것은 것이 없는 것이 없는 것이 없다. 것은 것은 것이 없는 것이 없는 것이 없다. 것은 것이 없는 것이 없는 것이 없는 것이 없다. 것은 것이 없는 것이 없는 것이 없는 것이 없다. 것은 것이 없는 것이 없는 것이 않는 것이 없다. 것은 것이 없는 것이 없는 것이 없는 것이 없다. 것은 것이 없는 것이 없는 것이 없다. 것은 것이 없는 것이 없는 것이 없다. 것은 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 없다. 것이 없는 것이 없다. 것이 없는 것이 없다. 것이 것이 없다. 것이 없다. 것이 없다. 것이 없다. 것이 없다. 것이 않다. 것이 것이 없다. 것이 없다. 것이 없다. 것이 않다. 것이 않다. 것이 않다. 것이 않다. 것이 없다. 것이 않다. 것이 없다. 것이 없다. 것이 없다. 것이 없다.	
round-trip min/avg/max = 0.697/0.723/0.755 ms	round_trip min/ava/m	max = 0.697/0.723/0.755 ms	
양한 일을 통하는 것 이렇게 다 같았는 것 같은 것 같은 것 같은 것 같아요. 것 같아요. 것 같아요. 것 같아요. 것 같아요. 같아요. 같아요. 같아요. 같아요. 같아요. 같아요. 같아요.	Vigor10:~ draytek\$	그는 방법은 이상에 가장하는 것 수 있는 것 수 있는 것 수 있는 것 같은 것을 수 있는 것 같은 것을 하는 것 같이 없다.	

VI-4 Backing to Factory Default Setting

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

(i) Warning:

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

VI-4-1 Software Reset

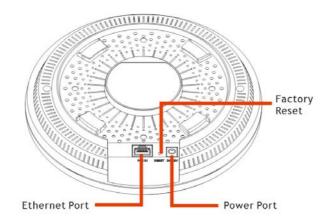
You can reset the device to factory default via Web page.

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 device will return all the settings to the factory settings.

System Maintenance / Syster	m Reboot
System Reboot	
Reboot With	Current Configuration Factory Default
	Reboot

VI-4-2 Hardware Reset

While the AP is running, press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the AP will restart with the default configuration.



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

VI-5 Contacting DrayTek

If the AP 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.