Vigor C410/C510 Series

VPN Router with WLAN/LTE/5G-NR

User's Guide

Version: 1.02

Firmware Version: V5.3.1.3

Date: June 2, 2025

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

Table of Contents

Chapter I Installation	IX
I-1 Introduction	1
I-1-1 LED Indicators and Connectors for Vigor C410	1
I-1-2 LED Indicators and Connectors for Vigor C510	3
I-1-3 LED Indicators and Connectors for Vigor C410ax	4
I-1-4 LED Indicators and Connectors for Vigor C510ax	6
I-2 Hardware Installation	8
I-2-1 Network Connection	8
I-2-2 Wall-Mounted Installation	9
I-2-3 Antenna Installation	10
I-3 Accessing to Web User Interface	
I-4 Dashboard	
Chapter II Connectivity	17
II-1 Configuration	
II-1-1 Physical Interface	
II-1-2 WAN	
II-1-2-1 WAN Connections	20
II-1-2-2 WAN AutoHunt	
II-1-2-3 Virtual WAN	
II-1-2-4 Dynamic DNS	41
II-1-2-5 WAN Budget	
II-1-2-6 DHCP Options	
II-1-2-7 Failover	
II-1-2-8 Link Health Check	
II-1-2-9 Performance SLA	
II-1-2-10 PPPoE Pass Through	
II-1-3 LAN	
II-1-3-1 LANs	
II-1-3-2 Bind IP to MAC	
II-1-3-3 DHCP Options	
II-1-3-4 Inter-LAN Routing II-1-3-5 VLAN List	
II-1-3-6 Interface VLAN	
II-1-3-7 LAN Port 802.1x	
II-1-4 DNS	
II-1-4-1 DNS Security	
II-1-4-2 LAN DNS/Forwarding	
II-1-5 Wireless LAN	
II-1-5-1 SSID	
II-1-5-2 Radio Settings	
II-1-5-3 Roaming	
II-1-5-4 AP Discovery	
II-1-5-5 WPS	86
II-1-5-6 WDS	
II-1-6 Routing	

II-1-6-1 Route Policy	
II-1-6-2 IPv4 Static Route	
II-1-6-3 IPv6 Static Route	
II-1-7 RIP	
ll-1-7-1 General Setup	
II-1-7-2 RIP Network	
II-1-7-3 RIPng Network	
II-1-8 BGP	
ll-1-8-1 General Setup	
II-1-8-2 IPv4 Neighbors	
II-1-8-3 IPv4 Networks	
II-1-8-4 IPv6 Neighbors	
II-1-8-5 IPv6 Networks	
II-1-9 OSPF	
II-1-9-1 General Setup	
II-1-9-2 OSPFv2 Networks	
II-1-9-3 OSPFv3 Networks	
II-1-10 Bandwidth Management	
II-1-10-1 Traffic Shaping Policy	
II-1-10-2 Bandwidth Limit	
ll-1-10-3 QoS Setup	
II-1-10-4 APP QoS	
II-1-10-5 Default Policy	
II-1-11 NAT	
II-1-11-1 Port Forwarding	
II-1-11-2 DMZ Host	
II-1-11-3 Port Triggering	
II-1-11-4 ALG	
II-1-11-5 UPnP	
II-1-12 IGMP	
ll-1-12-1 General Setup	
II-1-12-2 IGMP Status	
II-1-13 Objects	
II-1-13-1 IP Object	135
II-1-13-2 IP Group	
II-1-13-3 MAC Object	
II-1-13-4 MAC Group	
II-1-13-5 Schedule	141
II-1-13-6 Service Type Object	
II-1-13-7 Country Object	
II-1-13-8 Keyword Object	
II-1-13-9 Backup & Restore	
II-1-14 LTE	
II-1-14-1 SIM Inbox	
II-1-14-2 Send SMS	
II-1-14-3 SMS Outbox	
II-1-15 Wake on LAN	
II-1-16 Notification Services	
II-1-16-1 Services & Providers	
II-1-16-2 SMTP Server	
II-1-16-3 SMS Provider	

II-1-16-4 Webhook	
II-1-16-5 Notification	
II-1-16-6 Backup & Restore	
II-1-17 RADIUS/TACACS+	
II-1-17-1 External RADIUS	
II-1-17-2 Internal RADIUS	
II-1-17-3 External TACACS+	
II-1-18 Certificates	
II-1-18-1 Local Certificates	
II-1-18-2 Trusted CA	
II-1-18-3 Local Services	
II-1-18-4 Backup & Restore	
II-2 Security	
II-2-1 Firewall Filters	
II-2-1-1 IP Reputation Filters	
II-2-1-2 IP Filters	
II-2-1-3 Content Filters	
II-2-1-4 Default Filters	
II-2-1-5 Backup & Restore	
II-2-2 Defense Setup	
II-2-2-1 DoS Defense	
II-2-2-2 BFP Settings	
II-2-2-3 Allow/Block List	
II-2-2-4 Defense Syslog	
II-2-3 MAC Filtering Profile	
II-2-3-1 MAC Filtering Profile	
II-2-3-2 Backup & Restore	
II-2-4 IPv6 Address Security	
II-2-5 Security Defense Status	
II-2-5-1 BFP Status	
II-2-5-2 IP Reputation	
II-2-6 URL/IP Lookup	
II-3 IAM	
II-3-1 Users & Groups	
II-3-1-1 Users	
II-3-1-2 User Groups	
II-3-1-3 Authentication Server	
II-3-2 IAM Policies	
II-3-2-1 Apply Policies to LAN	
II-3-2-2 Access Policies	
II-3-2-3 Group Policies	
II-3-2-4 Conditional Access Policy	
II-3-3 Resources	
II-3-4 Hotspot Web Portal	
II-3-4-1 Profile Setup	
II-3-4-2 Quota Policy Profile	
II-3-4-3 User Information	
II-3-5 Account Status	
II-3-6 Backup & Restore	
II-4 VPN	

	II-4-1 General Setup	
	II-4-1-1 Access Control	
	II-4-1-2 EasyVPN	
	II-4-1-3 IPsec	
	II-4-1-4 WireGuard	
	II-4-1-5 OpenVPN	
	II-4-1-6 VPN MSS	
	II-4-2 Site-to-Site VPN	
	II-4-2-1 VPN Type - IPsec	
	II-4-2-2 VPN Type - WireGuard	
	II-4-2-3 VPN Type - OpenVPN	
	II-4-3 Teleworker VPN	
	II-4-4 VPN Connection Status	
	II-4-5 Backup & Restore	
I	II-5 Virtual Controller - Wireless	
	II-5-1 Role Setup	
	II-5-2 Device	
	II-5-2-1 Device List	
	II-5-2-2 Mesh Status	
	II-5-2-3 AP Adoption	
I	II-6 Virtual Controller - Switch	
	II-6-1 General Setup	
	II-6-2 Device	
	II-6-3 Port Profile	
	II-6-4 Maintenance	
Chapter III	Management	201
•	-	
I	III-1 System Maintenance	
	III-1-1 Device Settings	
	III-1-1 Time	
	III-1-1-2 Device Name	
	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-1-3 System Upgrade	
	III-1-3-1 Firmware	
	III-1-3-2 Country Object Database	
	III-1-4 Backup & 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	
Ι	IV-1 Monitoring	
	IV-1-1 Clients List	
	IV-1-2 Log Center	
	IV-1-2-1 Log Center	

	IV-1-2-2 DDNS Log	
١v	/-1-3 Wireless Information	
	IV-1-3-1 Wireless Information	
	IV-1-3-2 Recent Activities	
	IV-1-3-3 Real Time Throughput 2.4G	
	IV-1-3-4 Real Time Throughput 5G	
١v	/-1-4 WAN	
	IV-1-4-1 WAN Utilization	
	IV-1-4-2 WAN Status	
١v	/-1-5 ARP Table	
	IV-1-5-1 LAN	
	IV-1-5-2 WAN	
١v	/-1-6 Route Table	
	IV-1-6-1 IPv4	
	IV-1-6-2 IPv6	
١v	/-1-7 DHCP Table	
	IV-1-7-1 IPv4 DHCP Subnet	
	IV-1-7-2 IPv4 DHCP Lease	
	IV-1-7-3 IPv6 Assignment	
	/-1-8 IPv6 TSPC Status	
	/-1-9 IPv6 Neighbor Table	
	/-1-10 LLDP Neighbors Information	
IV	/-1-11 DNS Cache Table IV-1-11-1 IPv4	
	IV-1-11-2 IPv6	
N	/-1-12 LTE Status	
	/-1-12 ETE Status	
	/-1-14 PPPoE Pass-Through	
	/-1-15 Session Table	
		-
-	y	
١v	/-2-1 Network Tools	
	IV-2-1-1 Ping Tool	
	IV-2-1-2 Traceroute	
	IV-2-1-3 DNS	
IV	/-2-2 Web CLI	
Chapter V Troubles	shooting	
-	sing the Hardware Status	
	ing the Network Connection Settings	
	-	
	-2-1 For Windows -2-2 For Mac Os	
V-3 Pingir	ng the Device	
V	-3-1 For Windows	
V	-3-2 For Mac Os (Terminal)	
V-4 Backir	ng to Factory Default Setting	
V	-4-1 Software Reset	
V	-4-2 Hardware Reset	
V-5 Conta	cting 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.

I-1-1 LED Indicators and Connectors for Vigor C410

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

LED

U	22	2	5	3	2	1	

LED	Status	Explanation
	Blinking	The router is powered on and running normally.
0	Off	The router is powered off.
	On	Internet connection (via Ethernet WAN) is ready.
72.	Blinking	The data is transmitting.
	Off	Internet connection is not ready.
2011 - 500 ·	On	SIM card is inserted into the slot and detected by Vigor device.
2 1	Blinking Quickly	The data is transmitting.
	Blinking Slowly	The LTE connection is being activated.
	Off	SIM errors or no SIM card in detected.
	On	The Ethernet port is connected.
54321	Blinking	The data is transmitting.
	Off	The Ethernet port is disconnected.

Factory Reset	WAN P1 P2 P3 P4 P5 SIM Image: PWR				
Interface	Explanation				
Factory Reset	Restore the default settings. Usage: Turn on the router (²² LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ²² LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.				
WAN	Connector for remote networked devices (by Ethernet cable).				
P1~P5	Connectors for local networked devices.				
SIM	Slots for installing SIM card(s).				
ON/OFF	Power switch.				
PWR	Connector for a power adapter.				

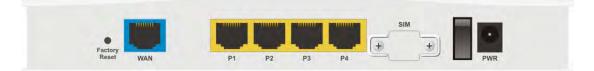
I-1-2 LED Indicators and Connectors for Vigor C510

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

LED



LED	Status	Explanation		
ds	Blinking	The router is powered on and running normally.		
0	Off	The router is powered off.		
	On	Internet connection (via Ethernet WAN) is ready.		
72	Blinking	The data is transmitting.		
00	Off	Internet connection is not ready.		
3-37 539	On	SIM card is inserted into the slot and detected by Vigor device.		
2 1	Blinking Quickly	The data is transmitting.		
	Blinking Slowly	The LTE connection is being activated.		
	Off	SIM errors or no SIM card in detected.		
	On	The Ethernet port is connected.		
4 3 2 1	Blinking	The data is transmitting.		
	Off	The Ethernet port is disconnected.		



Interface	Explanation				
Factory Reset	Restore the default settings. Usage: Turn on the router (🔀 LED is blinking). Press the hole and keep for more than 5 seconds. When you see the 🔀 LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.				
WAN	Connector for remote networked devices (by Ethernet cable).				
P1~P4	Connectors for local networked devices.				
SIM	Slots for installing SIM card(s).				
ON/OFF	Power switch.				
PWR	Connector for a power adapter.				

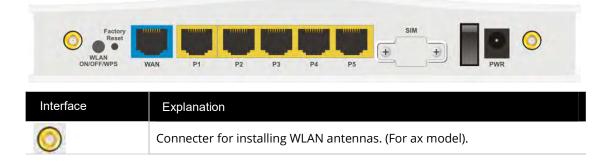
I-1-3 LED Indicators and Connectors for Vigor C410ax

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

LED



LED	Status	Explanation
	Blinking	The router is powered on and running normally.
0	Off	The router is powered off.
14114	On	Internet connection (via Ethernet WAN) is ready.
72	Blinking	The data is transmitting.
	Off	Internet connection is not ready.
	On	SIM card is inserted into the slot and detected by Vigor device.
2 1	Blinking Quickly	The data is transmitting.
	Blinking Slowly	The LTE connection is being activated.
	Off	SIM errors or no SIM card in detected.
	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless network.
2.43) 5.3	Blinking (quickly)	When both \bigotimes and \bigotimes \bigotimes LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection.
	Off	The wireless function is inactive.
	On	The Ethernet port is connected.
54321	Blinking	The data is transmitting.
	Off	The Ethernet port is disconnected.



	WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on.
WLAN ON/OFF/WPS	WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off.
010/077/073	WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS.
Factory Reset	Restore the default settings.
	Usage: Turn on the router (\gtrsim LED is blinking). Press the hole and keep for more than 5 seconds. When you see the \gtrsim LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WAN	Connector for remote networked devices (by Ethernet cable).
P1~P5	Connectors for local networked devices.
SIM	Slots for installing SIM card(s).
ON/OFF	Power switch.
PWR	Connector for a power adapter.

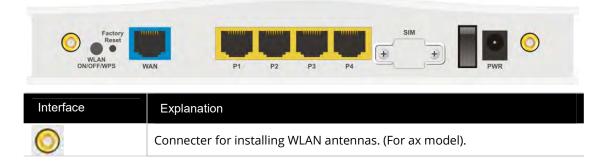
I-1-4 LED Indicators and Connectors for Vigor C510ax

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

LED



LED	Status	Explanation
	Blinking	The router is powered on and running normally.
0	Off	The router is powered off.
	On	Internet connection (via Ethernet WAN) is ready.
72.	Blinking	The data is transmitting.
	Off	Internet connection is not ready.
	On	SIM card is inserted into the slot and detected by Vigor device.
2 1	Blinking Quickly	The data is transmitting.
	Blinking Slowly	The LTE connection is being activated.
	Off	SIM errors or no SIM card in detected.
	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless network.
2.4 5 5	Blinking (quickly)	When both \bowtie and \bowtie \bowtie LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection.
	Off	The wireless function is inactive.
	On	The Ethernet port is connected.
4 3 2 1	Blinking	The data is transmitting.
	Off	The Ethernet port is disconnected.



	WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on.
WLAN ON/OFF/WPS	WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off.
010/077/073	WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS.
Factory Reset	Restore the default settings.
	Usage: Turn on the router (\gtrsim LED is blinking). Press the hole and keep for more than 5 seconds. When you see the \gtrsim LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WAN	Connector for remote networked devices (by Ethernet cable).
P1~P4	Connectors for local networked devices.
SIM	Slots for installing SIM card(s).
ON/OFF	Power switch.
PWR	Connector for a power adapter.

I-2 Hardware Installation

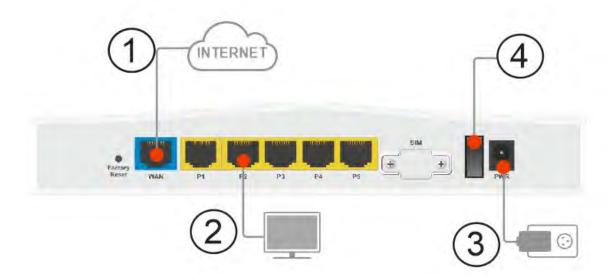
This section will guide you to install the Vigor C410/C510 through a hardware connection and configure the device's settings through the web browser.

I-2-1 Network Connection

- 1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
- 2. Connect one end of an Ethernet cable (RJ-45) to one of the LAN ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
- 3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
- 4. Power on the router. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connection.

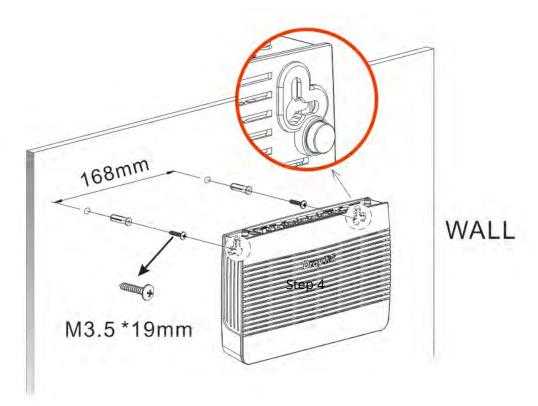
(For the detailed information of LED status, please refer to section 2. Panel Explanation)

Here we take Vigor C410 as an example.



I-2-2 Wall-Mounted Installation

- 1. Drill the holes on the wall according to the recommended instruction. The distance between the holes shall be 168mm.
- 2. Fit screws into the wall using the appropriate type of wall plug.
- 3. With the screws installed, the router can be slotted into place.



(i) Note

The recommended drill diameter shall be 6.5mm (1/4").

4. When you finished the above procedure, the modem has been mounted on the wall firmly.

I-2-3 Antenna Installation

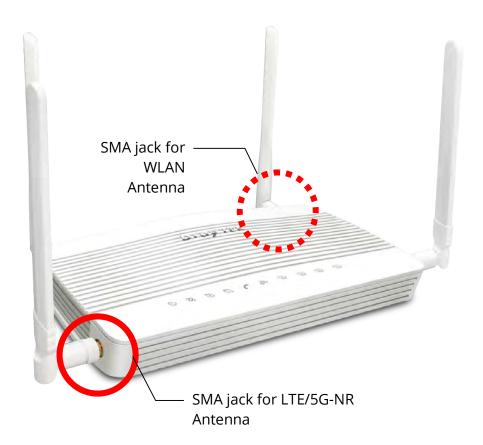
Antenna must be installed on Vigor router correctly to obtain the transmission signal.



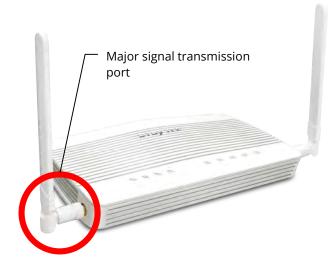
For model with SIM installed

For ax models

There are two types of antennas provided for Vigor C410ax / C510ax, which must be installed in different locations carefully and correctly. Wrong installation might cause bad signal of wireless connection. Therefore, pay attention to the installation of antennas by referring to the following illustration.



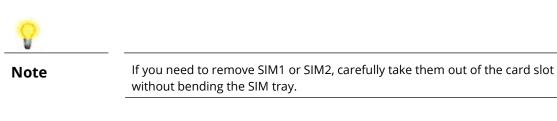
Note: The antennas for Vigor C410 must be installed on both sides of the device. If only one antenna will be used, please install on the left side of Vigor router.



For installing the SIM card into the card slot,

- (1) While installing the SIM card into the card slot, note that the back plate of the SIM card slot must be removed first.
- (2) Assemble the SIM1 and SIM2 with the SIM tray. Then insert the SIM tray into the SIM card slot of the router.







I-3 Accessing to Web User Interface

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

- 1. Make sure your PC connects to the Vigor router correctly.
- 2. Open a web browser on your PC and type http://192.168.1.1. A pop-up window will open to ask for a username and password. Pease type "admin/admin" on Username/Password and click Login.

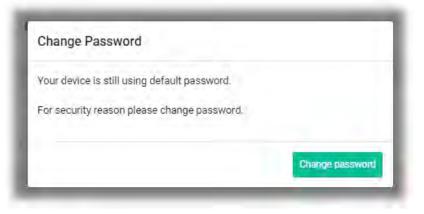
	Username
Dray Tek VigorC410	Password
VigorC410	
	Login

(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 the same subnet as **the default IP address of Vigor router 192.168.1.1**.

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

3. Next, the page will appear to guide you change the login password.



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

nin / Set Password	
Account	admin
Current Password	····· ©
New Password	······ ©
Confirm New Password	······ ©
	At least 8 characters
	Uppercase characters
	Zowercase characters
	Vumbers or Special characters ~!@#\$%*&*()_=/?[]{<>\

5. After clicking **Apply**, the Main Screen will pop up.

Search Q	Dashboard	CRefresh
Device Menu Device Menu Configuration Security LM VPN Monitoring	Vian P1 P2 P3 P4 P5 Sim. ■ 10/100M ■ 1G	SYSTEM C Device Hame DrayTek-86FAB8 LAN MAC 14:49:8C:86:FAB8 System Uptime 6d 6hr: 44m: 45 Pirmware 5.3.1_8C3 ACS Server • See More
88 Utility System Maintenance Virtual Controller Hireless Switch	WAN STATUS IPu6 Name MAC Address Connection IP Gateway Primary Secondary Uptime Address DNS DNS Uptime	LTE INFORMATION Status No SIM Card Bridge mode Disabled Access Tech Band Operator Signal Current using SIM Unknown WIRELESS OVERVIEW

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

DrayTek-86FAB8 21-10-30 16:31:43	a admin	× -	6FAB8 :31:23	а	admin 💛
	Auto Logout off	• луті		Auto Logout	off 🗸
E M	 Get Password Get Password Get Log Out 	.0-3	1	合 Set Passwo⊡ Log Out	off 1 min 3 min 5 min
1AC 1.	4:49:BC:86:FA:B8		14	:49:BC:86;FA:B8	10 min

(i) Note:

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

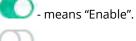
I-4 Dashboard

Dashboard shows port status, LAN status, system status, LAN/WAN Usage and DSL information. Click **Dashboard** from the main menu on the left side of the main page.

Dashboard								C Refres
PORT STATUS						SYSTEM		(
						Device Name	DrayTek-86FAB8	
						LAN MAC	14:49:BC:86:FA:B8	
						System Uptime	6d 6h: 56m: 38s	
	WAN P1	P2 P3	P4 P5	SIM		Firmware	5.3.1_RC3	
						ACS Server	•	
	10/100	I G					See More +	
WAN STATUS						LTE INFORMATION		
VAN STATUS						Status	No SIM Card	
	Connection Type IP Addr	ess Gateway	Primary DNS	Secondary DNS	Uptime			
IPv4 IPv6	Connection Type IP Addr DHCP	sss Gateway	Primary DNS 8.8.8.8	Secondary DNS 8.8.4.4	Uptime 00:00:00	Status Bridge mode	No SIM Card	
IPv6 Name MAC Address		ass Gateway				Status Bridge mode Access Tech	No SIM Card	
IPv6 Name MAC Address [WAN] WAN1 14:49:BC:86:FA:B9	DHCP	ess Gateway	8.8.8.8	8.8.4.4	00:00:00	Status Bridge mode Access Tech Band	No SIM Card	
IPv6 Name MAC Address [WAN] WAN1 14:49:BC:86:FA:B9	DHCP	ess Gateway	8.8.8.8	8.8.4.4	00:00:00	Status Bridge mode Access Tech Band Operator	No SIM Card	



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



- means "Disable".

This page is left blank.

Chapter II Connectivity



II-1 Configuration

II-1-1 Physical Interface

Configure the general settings for available interfaces. Open **Configuration >> Physical Interface**.

😂 Configuration	Configuration / Ph	ysical Interface			C Refresh
Physical Interface WAN	Physical Interfac	e			
LAN DNS					
Wireless LAN					
Routing RIP				WAN P1 P2 P3 P4 P5 SIM	
BGP OSPF				📕 10/100M 📕 1G	
Bandwidth Management	- A.				
IGMP	Ethernet				
Objects	Interface	Function	Enabled	Speed	
LTE Wake on LAN	Ethernet WAN	wan \sim		Auto negotiation \checkmark	
Notification Services RADIUS/ TACACS+	Port 1	$_{\rm LAN} \sim$		Auto negotiation \sim	
Certificates					

Available settings are explained as follows:

Item	Description						
Ethernet							
Interface	Displays the available interfaces of this device.						
Function	Displays the type (WAN or LAN) of the interface. Except Ethernet WAN is fixed to WAN, Port 1 can be set as WAN o LAN to meet different requirements. Use the drop-down menu to the specified interface as LAN or WAN.						
Enabled	Switch the toggle to enable or disable the interface.						
Speed	Set the port speed capabilities for each interface.						

Port speed capabilities: Auto negotiation - Auto speed with all capabilities. 10M half duplex - Force speed with 10M ability. 10M full duplex - Force speed with 10M ability. **100M half duplex -** Force speed with 100M ability. 100M full duplex - Force speed with 100M ability. 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.

(i) Note:

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

- means "Enable".
- means "Disable".

II-1-2 WAN

II-1-2-1 WAN Connections

This page is to configure the general settings for WAN connection.

Physical Interface											
	WAN Connect	ONS WAN AutoHur	it Virti,	ial WAN Dynan	nic DNS WAN	Budget	DHCP Options	Fallover	Link Health	Check P	erformance SLA
LAN	WAN Connec	tions									
DNS											
Wireless LAN	_					Active	IPv4		IPv6		
Routing	Index +	Profile Name	Enabled	Mode	Physical Type	WAN	Connection	IPv4 Address	Connection	Link Local Address	Option
RIP	1.000					Profile	Туре		Туре		
BGP	WAN1	Wired WAN	Enabled	Failover (Manual)	Ethernet		DHCP		Offline		Ø Edit
OSPF	WANZ	Wired WAN	Dirablad	Failover (Manual)	Ethornat		DHCP		Offline		@ Edit
Bandwidth Management	WANZ.	wined ware	Ursabileo	Pallover (Manual)	ethernet		UNCP		Ortune		0/ Eur
NAT	WAN3	Wireless WAN 2.4GHz	Disabled	Failover (Manual)	Wireless 2.4GHz		DHCP		Offline		/ Edit
IGMP	WAN4	Wireless WAN 5GHz	Disabled	Failover (Manual)	Wireless SGH7		DHCP		Offline		/ Edit
Objects	1009	THE BESS WAR JUNE	Ursauleu	Panover (manual)	Wileless Jane		DHCF		Chinine		er som
LTE	WAN5	Cellular WAN	Enabled	Primary (Manual)	LTE		DHCP		Offline		d Edit
Wake on LAN											
Notification Services											
RADIUS/ TACACS+											
Certificates											

Available settings are explained as follows:

ltem	Description
Profile Name	Displays the name of the interface.
Enabled	Displays if the WAN interface is enabled or disabled.
Mode	Displays if the WAN interface is primary or failover interface.
Physical Type	Displays the physical type (e.g., Ethernet, Wireless 2.4GHz, Wireless 5GHz or USB) of the WAN interface.
IPv4 Connection Type	Displays the IPv4 connection type (e.g, Static IP, DHCP and etc.) used by the WAN interface.
IPv4 Address	Displays the IP address assigned by the DHCP server or the static IP address specified manually.
IPv6 Connection Type	Displays the IPv6 connection type used by the WAN interface.
Link Local Address	Displays the IPv6 address for the IPv6 connection type – Static.
Option	Edit - Click to modify the interface name and physical mode.

To configure the detailed settings (varied by physical type) for the selected WAN interface, click the **Edit** link to the right side of the WAN interface.

For Physical Type with Ethernet

Click the **Edit** link of WAN1 or WAN2 to open the following page.

		×
		Advanced Mode: OFF
ndex	WÄN1	
Profile Name 🕕	Wired WAN	
nabled		
General Setup		Ý
Physical Type	Ethernet	
Bind to Physical Interface	Ethernet WAN	
	Note: To bind more Interfaces, alter the interface functionality on Physical Interface	
etup Mode	Manual AutoHunt	
Version	Both IPv4 IPv6	
/LAN Settings		~
ustomer VLAN		
ervice VLAN		

Available settings are explained as follows:

Item	Description	
Advanced Mode:ON/OFF	Click to show or hide the advanced settings (IP Alias and WAN MAC Address) for the WAN interface.	
Index	Displays current WAN interface.	
Profile Name	Displays the name of the profile.	
Enabled	Switch the toggle to enable or disable the function.	
	General Setup	
Physical Type	Displays the physical type used by this interface.	
Bind to Physical Interface	Select a physical interface (Ethernet).	
Setup Mode	Determine the WAN connection established on the settings page or automatically based on the AutoHunt profiles, processed one by one. Manual – If selected, the WAN connection will be performed according to the settings configured in this page.	
	AutoHunt – The Vigor router will automatically connect to Ethernet WAN connection. Once connected and powered on, the router will run through a list of network connection settings (based on the autohunt profiles) to determine if it can establish a connection. If it is unable to connect, the mechanism will proceed to the next ISP setting until it receives an IP address.	
	If Auto Hunt is selected, configure the following:	
	AutoHunt Profile – Select the AutoHunt profile(s).	
	+Add – Click to specify the autohunt profile(s).	

IP Version	Set the protocol (IPv4 or IPv6 or both) that this WAN interface used.
	VLAN Settings
Customer VLAN	Switch the toggle to enable or disable the function of VLAN with tag. I enabled, enter the values for the tag and priority.
	Tag - Enter the value as the VLAN ID number. The range is from 0 to 4094.
	Priority - Enter the packet priority number for such VLAN. The range i from 0 to 7.
Service VLAN	Switch the toggle to enable or disable the function of VLAN with tag. I enabled, enter the values for the tag and priority.
	Tag - Enter the value as the VLAN ID number. The range is from 0 to 4094.
	Priority - Enter the packet priority number for such VLAN. The range i from 0 to 7.
	IPv4
IPv4 Connection Type	It is available when Both or IPv4 is selected as IP Version.
	PPPoE – Set the access mode as PPPoE.
	 Username – Username provided by the ISP for PPPoE authentication.
	 Password – Password provided by the ISP for PPPoE authentication.
	• WAN DNS – Select Auto or Manual.
	If Manual is selected, specify the primary and secondary DNS servers.
	IPv4 Primary DNS – IP address of primary DNS server.
	IPv4 Secondary DNS - IP address of secondary DNS server.
	DHCP – The router receives IP configuration information from a DHC server.
	• WAN DNS – Select Auto or Manual.
	If Manual is selected, specify the primary and secondary DNS servers.
	IPv4 Primary DNS – IP address of primary DNS server.
	IPv4 Secondary DNS - IP address of secondary DNS server.
	Static IP – Set the access mode as Static IP.
	• IP Address – WAN IP address assigned by the ISP.
	• Subnet Mask – WAN subnet mask.
	• Gateway IP – IP address of the WAN Gateway.
	• IPv4 Primary DNS – IP address of primary DNS server.
	• IPv4 Secondary DNS - IP address of secondary DNS server.
	WAN Connection Detection
Mode	Configures how the WAN connection is monitored.
	Always On - The router assumes the WAN connection is always active
	ARP Detect - The router broadcasts an ARP request every 5 seconds. no response is received within 30 seconds, the WAN connection is deemed to have failed.
	Ping Detect - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is

	specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.	
	If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.	
	 Ping Gateway IP - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. 	
	• TTL –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.	
	• Ping Interval (Sec, 5-3600) – Enter the interval for the system to execute the PING operation.	
	 Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. 	
IP Alias	IPv4 Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.	
	+Add – Click to add an IPv4 address as the IPv4 alias.	
	IPv6	
IPv6 Connection Type	It is available when Both or IPv6 is selected as IP Version.	
	Offline – When Offline is selected, the IPv6 connection will be disabled	
	PPP – IPv6 WAN address is assigned along with the IPv4 WAN address during PPPoE negotiation. This IPv6 access mode requires that the IPv4 uses PPPoE.	
	Static – Configure an ISP-assigned static IPv6 setup.	
	 +Add –Click this button to add the values in the IPv6 Address and Prefix Length fields to the Global Address Table. 	
	 IPv6 Global Address – WAN IPv6 address assigned by the ISP. 	
	 Prefix Length – Length of the IPv6 prefix. 	
	• Gateway Address - IPv6 address of the ISP gateway.	
	DHCPv6 – Use DHCPv6 protocol to obtain IPv6 address from server.	
	 DUID – Displays the DHCP unique ID used by this WAN interfac 	
	• IAID – Unique integer that identifies this WAN interface.	
	 Authentication Protocol - This protocol will be used for the clier to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, Reconfigure Key, Delayed and None. In general, the default setting is None. 	
	 Reconfigure Key – During the connection process, DHCPv6 server will authenticate the client automatically. 	
	 Delayed - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields. Key ID – Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value. Realm – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value. Secret – Type a text (1 to 31 characters) as s a unique 	

identifier for each client on each DHCP server.

	TSPC - Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.
	 Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (http://gogonet.gogo6.com/page/freenet6-account) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background. After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet. Tunnel Broker Address – Enter the address for the tunnel broker IP, FQDN or an optional port number. Username – It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account. Password - Enter the password assigned with the user name.
	6in4 – Setup 6in4 Static Tunnel for WAN interface.
	However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than any cast endpoint. The mode has more reliability.
	6rd - Setup 6rd for WAN interface.
	IPv6 WAN Connection Detection
Mode	Configures how the WAN connection is monitored.
	Always On - The router assumes the WAN connection is always active.
	NS Detect - The router verifies connectivity by issuing Neighbor Solicitation packets.
	Ping Detect - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.
	If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.
	• Primary Ping IP – Enter an IP address in this field for pinging.
	• Secondary Ping IP - Enter an IP address in this field for pinging.
	• TTL –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
	• Ping Interval (Sec, 10-3600) – Enter the interval for the system to execute the PING operation.
	 Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
	MTU
MTU	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492.

WAN MAC Address	
Mode	Default – Use the default MAC address for the WAN port.
	Customized - Select this option if your ISP authenticates by MAC addresses.
	• MAC - Specify a MAC address for the WAN Ethernet port.
MAC	Displays the MAC address of this device.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

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

For Physical Type with Wireless 2.4GHz

When Wireless 2.4G is selected as Physical Type, WAN interface uses wireless station mode to access Internet. The Router acts as a 2.4GHz wireless station and connects to the specific Wireless AP.

		×
		Advanced Mode: OFF
Index	WAN3	
Profile Name 🛈	Wireless WAN 2.4GI	
Enabled		
General Setup		×
Physical Type	Wireless 2.4GHz	
Bind to Physical Interface	Please Select \sim	
	Note: To bind more interfaces, alter the interface functionality on Physical Interface	
IPv4		~
IPv4 Connection Type	рнср 🗸	
WAN DNS	- Auto Manual	
WAN Connection Detectior		
Möde	ARP Detect \sim	

Click the **Edit** link for WAN3 or WAN4 to open the following page.

Available settings are explained as follows:

Item	Description		
Advanced Mode:ON/OFF	Click to show or hide the advanced settings (WAN MAC Address) for the WAN interface.		
Index	Displays current WAN interface.		
Profile Name	Displays the name of the profile.		
Enabled	Switch the toggle to enable or disable the function.		
	General Setup		
Physical Type	Displays the physical type used by this interface.		
Bind to Physical Interface	At present, only Wireless 2.4GHz 5GHz for WAN4.	is available for WAN3 and Wireless	
	Bind to Physical Interface	Please Select	
		Wireless 2.4GHz	
Peer SSID	Enter the identification of the wi	Enter the identification of the wireless device.	
Channel	Select the channel of frequency of the device.		

Security Mode	There are several modes provided for you to choose from. Each mode will bring up different parameters (e.g., Pass Phrase) for you to configure.
	WPA3 Personal – The Router connects to the wireless AP as a WPA3 client and the encryption key should be entered in PSK.
	WPA2 Personal – The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.
	OPEN – The encryption mechanism is turned off.
WPA Algorithms	Select AES as the algorithm for WPA.
Password	Enter 8~64 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
	IPv4
IPv4 Connection Type	It is available when Both or IPv4 is selected as IP Version.
51	DHCP – The router receives IP configuration information from a DHCP server.
	• WAN DNS – Select Auto or Manual.
	If Manual is selected, specify the primary and secondary DNS servers.
	• IPv4 Primary DNS –IP address of primary DNS server.
	• IPv4 Secondary DNS - IP address of secondary DNS server.
	Static IP – Set the access mode as Static IP.
	• IP Address – WAN IP address assigned by the ISP.
	• Subnet Mask – WAN subnet mask.
	• Gateway IP – IP address of the WAN Gateway.
	• IPv4 Primary DNS – IP address of primary DNS server.
	• IPv4 Secondary DNS - IP address of secondary DNS server.
	WAN Connection Detection
Mode	Configures how the WAN connection is monitored.
	Always On - The router assumes the WAN connection is always active.
	ARP Detect - The router broadcasts an ARP request every 5 seconds. I no response is received within 30 seconds, the WAN connection is deemed to have failed.
	Ping Detect - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN
	connection is deemed to have failed.
	If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.
	 Ping Gateway IP - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.
	• TTL –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
	• Ping Interval (Sec, 5-3600) – Enter the interval for the system to execute the PING operation.
	• Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN

	disconnection is judged.
	MTU
MTU	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492.
	WAN MAC Address
Mode	 Default – Use the default MAC address for the wireless WAN. Customized - Select this option to use customized MAC addresses. MAC - Specify a MAC address for the wireless WAN.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

For Physical Type with Wireless 5GHz

When Wireless 5G is selected as Physical Type, WAN interface uses wireless station mode to access Internet. The Router acts as a 5GHz wireless station and connects to the specific Wireless AP.

		×
		Advanced Mode: ON
Index	WAN4	
Profile Name 🕕	Wireless WAN 5GH2	
Enabled		
General Setup		~
Physical Type	Wireless 5GHz	
Bind to Physical Interface	Please Select 😒	
	Note: To bind more interfaces, alter the interface functionality on Physic	cal Interface
Peer SSID 🕧		
Channel	Auto 🗸	
Security Mode	WPA2 Personal 🗸	
WPA Algorithms	AES	
Password	\$	
IPv4		\vee

ltem	Description
Advanced Mode:ON/OFF	Click to show or hide the advanced settings (WAN MAC Address) for the WAN interface.
Index	Displays current WAN interface.
Profile Name	Displays the name of the profile.
Enabled	Switch the toggle to enable or disable the function.

General Setup							
Physical Type	Displays the physical type used by this interface.						
Bind to Physical Interface	At present, only Wireless 2.4GHz is available for WAN3 and Wireless 5GHz for WAN4.						
Peer SSID	Enter the identification of the wireless device.						
Channel	Select the channel of frequency of the device.						
Security Mode	There are several modes provided for you to choose from. Each mode will bring up different parameters (e.g., Pass Phrase) for you to configure. WPA3 Personal – The Router connects to the wireless AP as a WPA3 client and the encryption key should be entered in PSK.						
	WPA2 Personal – The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.						
	OPEN – The encryption mechanism is turned off.						
WPA Algorithm	Select AES as the algorithm for WPA.						
Password	Enter 8~64 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").						
	IPv4						
IPv4 Connection Type	 It is available when Both or IPv4 is selected as IP Version. DHCP - The router receives IP configuration information from a DHCP server. WAN DNS - Select Auto or Manual. If Manual is selected, specify the primary and secondary DNS servers. IPv4 Primary DNS - IP address of primary DNS server. IPv4 Secondary DNS - IP address of secondary DNS server. Static IP - Set the access mode as Static IP. IP Address - WAN IP address assigned by the ISP. Subnet Mask - WAN subnet mask. Gateway IP - IP address of the WAN Gateway. IPv4 Primary DNS - IP address of primary DNS server. WAN Connection Detection 						
Mada							
Mode	 Configures how the WAN connection is monitored. Always On - The router assumes the WAN connection is always active. ARP Detect - The router broadcasts an ARP request every 5 seconds. In no response is received within 30 seconds, the WAN connection is deemed to have failed. 						

	Ping Detect - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is
	specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.
	If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.
	 Ping Gateway IP - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.
	 TTL –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
	 Ping Interval (Sec, 10-3600) – Enter the interval for the system to execute the PING operation.
	 Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
	MTU
MTU	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492.
	WAN MAC Address
Mode	 Default – Use the default MAC address for the wireless WAN. Customized - Select this option to use customized MAC addresses. MAC - Specify a MAC address for the wireless WAN.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

For Physical Type with LTE

It is available for SIM connection only.

Click the **Edit** link for WAN5 to open the following page.

Index Profile Name ①	WAN5 Cellular WAN	Advanced Mode: ON
Enabled		
General Setup		~
Physical Type	LTE	
IP Version	Both IPv4 IPv6	
USB/LTE Settings		~
Enable SIM1		
USB Mode	DHCP \checkmark	
USB/SIM1 PIN Code	@	
Enable Username/Password Authentication		
Authentication	PAP or CHAP 🛛 🗸	
Username 🕕		
Password ()	۵	
Cancel Apply		

ltem	Description				
Advanced Mode:ON/OFF	Click to show or hide the advanced settings (WAN MAC Address) for the WAN interface.				
Index	Displays current WAN interface.				
Profile Name	Displays the name of the profile.				
Enabled	Switch the toggle to enable or disable the access mode.				
	General Setup				
Physical Type	Displays the physical type used by this interface.				
IP Version	Set the protocol (IPv4 or IPv6 or both) that this WAN interface used.				
	USB/LTE Settings				
Enable SIM1	Click to enable or disable the SIM settings.				
USB Mode	DHCP – Dynamic Host Configuration Protocol is used to establish a connection.				
	PPP - Point-to-Point Protocol is used to establish a connection.				
USB/SIM1 PIN Code	PIN code of the SIM card in the modem. The maximum length of the PIN is 15 characters.				
Enable	Switch the toggle to enable or disable the function.				
Username/Password	Authentication – Select the protocol used for PPP authentication.				
Authentication	• PAP only - Only PAP (Password Authentication Protocol) is used.				
	• PAP or CHAP - Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use.				

	Username – Username provided by the ISP for authentication (optional).					
	Password - Password provided by the ISP for authentication (optional).					
Auto APN Name	Access Point Name to be used for the connection. Please contact you ISP or carrier for the appropriate value.					
Network Mode	Force Vigor router to connect Internet with the mode specified he you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.					
	SIM2 Settings					
Enable SIM2	Click to enable or disable the SIM2 settings.					
SIM2 PIN Code	PIN code of the SIM card in the modem. The maximum length of the PIN is 15 characters.					
Enable	Switch the toggle to enable or disable the function.					
Username/Password	Authentication – Select the protocol used for PPP authentication.					
Authentication	• PAP only - Only PAP (Password Authentication Protocol) is used					
	• PAP or CHAP - Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use.					
	Username – Username provided by the ISP for authentication (optional).					
	Password - Password provided by the ISP for authentication (optional).					
Auto APN Name	Access Point Name to be used for the connection. Please contact you ISP or carrier for the appropriate value.					
Network Mode	Force Vigor router to connect Internet with the mode specified here. you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.					
SIM Failover Settings	Dial-up timeout – Set the time out interval (50 to 255 seconds).					
	Fail Count Threshold - Set the maximum times (2 to 20) of failed dial-ups. After that, the system will stop dial-up and use another SIM card for dial-up instead.					
	Bridge Mode					
Enabled	Click to enable or disable the bridge mode settings.					
	If the function is enabled, the router will work as a bridge modem.					
	Bridge Specific MAC Address – Vigor router will forward incoming packets to the client with specific MAC address.					
	MAC Address – Enter a MAC address of the client.					
	Keep WAN Connection					
Enable Ping To Keep Alive LTE	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time.					
	Click to enable or disable the function.					
	click to chable of disable the function.					

Interval	Enter the interval for the system to execute the PING operation.				
Timeout	Maximum length of time, in seconds, of idling allowed (no traffic before the connection is dropped. Vigor system will send a pack "interval time" to the specified IP address. If the system does not receive any reply from that IP within specified (e.g., 10) seconds, system will reboot LTE module until successfully set LTE connect				
	IPv4 - WAN Connection Detection				
WAN DNS	Select Auto or Manual.				
	If Manual is selected, specify the primary and secondary DNS servers.				
	• IPv4 Primary DNS – IP address of primary DNS server.				
	• IPv4 Secondary DNS - IP address of secondary DNS server.				
Mode	Configures how the WAN connection is monitored.				
	Always On - The router assumes the WAN connection is always active				
	Ping Detect - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.				
	If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.				
	 Ping Gateway IP - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. 				
	• TTL –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.				
	 Ping Interval (Sec, 10-3600) – Enter the interval for the system to execute the PING operation. 				
	 Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. 				
	MTU				
MTU	Maximum Transmission Unit, the size of the largest packet, in bytes that can be transmitted to the WAN. The maximum value is 1500. F PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492.				
	WAN MAC Address				
Mode	Default – Use the default MAC address for the WAN port.				
	Customized - Select this option if your ISP authenticates by MAC addresses.				
	• MAC - Specify a MAC address for the WAN Ethernet port.				
Cancel	Discard current settings and return to previous page.				
Apply	Save the current settings and exit the page.				

II-1-2-2 WAN AutoHunt

The Vigor router will automatically connect to Ethernet WAN connection. Once connected and powered on, the router will run through a list of network connection settings (based on the autohunt profiles) to determine if it can establish a connection. If it is unable to connect, the mechanism will proceed to the next ISP setting until it receives an IP address.

	Configuration / WAN								Chene	sh ③Re	ser
	WAN Connections	WAN AutoHunt	Virtual WAN	Dynamic DNS	WAN Budget	DHCP Options	Failover	Link Health Check	Performan	nce SLA	3
evice Menu	WAN AutoHunt										
b Dashboard	Then Automatic										
	+ Add									Max	c.20
Physical Interface	Profile Name	Physical	1 Туре	IPv4 Connection	on Type	IPv6 C	Connection Typ	e .	Option		
	Auto_Hunt_1	Etherne	et.	PPPoE		Offline			J Edit	Delete	6
LAN				1.1.1.1.1.1							
DNS	Auto_Hunt_DH	Etherne	it.	DHCP		Offline	2		d Edit	1 Delete	
Wireless LAN											
Routing											
RIP											
BGP											
OSPF											
Bandwidth Management											
NAT											
IGMP											
Objects											
Wake on LAN											
Notification Services											
RADIUS/ TACACS+											

ltem	Description			
Reset	Click to clear all profiles to factory settings.			
+Add	Click to bring up the configuration page of the virtual WAN profile (max. 5).			

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

		×
		Advanced Mode: ON
Profile Name 🛈	Auto_Hunt_3	
Physical Type	Ethernet 🗸	
IP Version	Both IPv4 IPv6	
VLAN Settings		~
Customer VLAN		
Service VLAN		
IPv4		~
IPv4 Connection Type	PPPoe 🗸	
Username 🛈		
Password ()	•	
Service Name (Optional)		
PPP Authentication	PAP or CHAP 🛛 🗠	
IP Assignment	DHCP: Static IP	
Cancel Apply		

Item	Description

Advanced Mode:ON/OFF	Click to show or hide the advanced settings (IP Alias and WAN MAC Address) for the WAN interface.			
Physical Type	Displays the physical type used by this interface.			
IP Version	Set the protocol (IPv4 or IPv6 or both) that this WAN interface used.			
	VLAN Settings			
Customer VLAN	Switch the toggle to enable or disable the function of VLAN with tag. If enabled, enter the values for the tag and priority.			
	Tag - Enter the value as the VLAN ID number. The range is from 0 to 4094.			
	Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.			
Service VLAN	Switch the toggle to enable or disable the function of VLAN with tag. Is enabled, enter the values for the tag and priority.			
	Tag - Enter the value as the VLAN ID number. The range is from 0 to 4094.			
	Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.			
	IPv4			
IPv4 Connection Type	It is available when Both or IPv4 is selected as IP Version.			
	PPPoE – Set the access mode as PPPoE.			
	 Username – Username provided by the ISP for PPPoE authentication. 			
	 Password – Password provided by the ISP for PPPoE authentication. 			
	• Service Name – PPP service name tag. Required by some ISPs. Leave blank unless instructed otherwise by your ISP.			
	• PPP Authentication – The protocol used for PPP authentication.			
	PAP or CHAP - Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use.			
	 IP Assignment – It is available when PPPoE is selected as IPv4 Connection Type. 			
	DHCP - WAN IP address is dynamically allocated.			
	Static IP - ISP has assigned a fixed WAN IP address. Enter an IP address.			
	• WAN DNS – Select Auto or Manual.			
	If Manual is selected, specify the primary and secondary DNS servers.			
	IPv4 Primary DNS – IP address of primary DNS server.			
	IPv4 Secondary DNS - IP address of secondary DNS server.			
	DHCP – The router receives IP configuration information from a DHCF server.			
	• WAN DNS – Select Auto or Manual.			
	If Manual is selected, specify the primary and secondary DNS servers.			
	IPv4 Primary DNS – IP address of primary DNS server.			
	IPv4 Secondary DNS - IP address of secondary DNS server.			

	Static IP – Set the access mode as Static IP.				
	• IP Address – WAN IP address assigned by the ISP.				
	• Subnet Mask – WAN subnet mask.				
	• Gateway IP – IP address of the WAN Gateway.				
	• IPv4 Primary DNS – IP address of primary DNS server.				
	 IPv4 Secondary DNS - IP address of secondary DNS server. 				
	WAN Connection Detection				
Mode	Configures how the WAN connection is monitored. Select PPP Detect or Ping Detect .				
	Ping Detect - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.				
	If you choose Ping Detect as the detection mode, you have to enter required settings for the following items.				
	 Ping Gateway IP - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. 				
	• TTL –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.				
	• Ping Interval (Sec, 5-3600) – Enter the interval for the system to execute the PING operation.				
	 Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. 				
	IPv6				
IPv6 Connection Type	It is available when Both or IPv6 is selected as IP Version.				
	Offline – When Offline is selected, the IPv6 connection will be disabled				
	PPP – IPv6 WAN address is assigned along with the IPv4 WAN address during PPPoE negotiation. This IPv6 access mode requires that the IPv4 uses PPPoE.				
	Static – Configure an ISP-assigned static IPv6 setup.				
	 +Add –Click this button to add the values in the IPv6 Address and Prefix Length fields to the Global Address Table. 				
	 IPv6 Global Address – WAN IPv6 address assigned by the ISP. 				
	 Prefix Length – Length of the IPv6 prefix. 				
	 Gateway Address - IPv6 address of the ISP gateway. 				
	DHCPv6 – Use DHCPv6 protocol to obtain IPv6 address from server.				
	 DUID – Displays the DHCP unique ID used by this WAN interface 				
	 IAID – Unique integer that identifies this WAN interface. 				
	 Authentication Protocol - This protocol will be used for the clien to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, Reconfigure Key, Delayed and None. In general, the default setting is None. 				
	 Reconfigure Key – During the connection process, DHCPv6 server will authenticate the client automatically. 				
	- Delayed During the connection process DHCDy6 converting				

- Delayed - During the connection process, DHCPv6 server will

	 authenticate and identify the client based on the key ID, realm and secret information specified in these fields. Key ID - Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value. Realm - The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value. Secret - Type a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server. TSPC - Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily. Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (http://gogonet.gogo6.com/page/freenet6-account) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background. After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.
	 Iunnel Broker Address – Enter the address for the tunnel broke IP, FQDN or an optional port number. Username – It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account.
	 Password - Enter the password assigned with the user name.
	6in4 – Setup 6in4 Static Tunnel for WAN interface.
	However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than any cast endpoint. The mode has more reliability.
	6rd - Setup 6rd for WAN interface.
	IPv6 WAN Connection Detection
Mode	Configures how the WAN connection is monitored. Always On - The router assumes the WAN connection is always active NS Detect - The router verifies connectivity by issuing Neighbor Solicitation packets.
	Ping Detect - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is
	specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.
	specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN
	 specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. If you choose Ping Detect as the detection mode, you have to enter required settings for the following items. Primary Ping IP – Enter an IP address in this field for pinging.
	 specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. If you choose Ping Detect as the detection mode, you have to enter required settings for the following items. Primary Ping IP – Enter an IP address in this field for pinging. Secondary Ping IP - Enter an IP address in this field for pinging.
	 specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. If you choose Ping Detect as the detection mode, you have to enter required settings for the following items. Primary Ping IP – Enter an IP address in this field for pinging.
	 specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. If you choose Ping Detect as the detection mode, you have to enter required settings for the following items. Primary Ping IP – Enter an IP address in this field for pinging. Secondary Ping IP - Enter an IP address in this field for pinging. TTL –Time To Live, the maximum allowed number of hops to the following items.

	disconnection is judged.	
	MTU	
MTU	Maximum Transmission Unit, the size of the largest packet, in by that can be transmitted to the WAN. The maximum value is 1500 PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492.	
	WAN MAC Address	
Mode	Default – Use the default MAC address for the WAN port.	
	Customized - Select this option if your ISP authenticates by MAC addresses.	
	• MAC - Specify a MAC address for the WAN Ethernet port.	
MAC	Displays the MAC address of this device.	
Cancel	Discard current settings and return to previous page.	
Apply	Save the current settings and exit the page.	

II-1-2-3 Virtual WAN

Up to five virtual WAN profiles can be set for applying to different applications.

Each profile can be specified with VLAN and binding interfaces according to the requirements of the practical network environment.

	Q Confi	guration / WAN								③Reset CRef	resh
		Connections	WAN AutoHunt	Virtual WAN	Dynamic DNS	WAN Budget	DHCP Options	Failover	Link Health Check	Performance SLA	
evice Menu					-						
Dashboard	Virtu	al WAN									
	+ Ad	bb								4	Asc :
Physical Interface	Nam	e IP Addre	ss Uptime	Enabled	WAN Type	WAN Interface	Port Based Bridg	e	IPv4 Connection Type	Option	
LAN											
DNS											
Wireless LAN											
Routing											
RIP											
BGP											
OSPF											
Bandwidth Management											
NAT											
IGMP											
Objects											
Wake on LAN											
Notification Services											
RADIUS/ TACACS+											
Certificates											

ltem	Description	
Reset	Click to clear all profiles to factory settings.	
+Add	Click to bring up the configuration page of the virtual WAN profile (max. 5).	

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

		×
		Advanced Mode: ON
Name 🕕		
Enabled		
General		~
WAN Type	Ethernet 🗸	
WAN Interface	WAN1 ~	
	Note: The value of the 'Service Tag' is determined by the settings applied	to the chosen WAN Interface
Port-Based Bridge		~
Port Based Bridge		
VLAN Settings		V
Customer VLAN		
IPv4		Ŷ
IPv4 Connection Type	РРРоЕ	
Cancel Apply		

Available settings are explained as follows:

Trans

ltem	Description		
Advanced Mode: ON/OFF	Click to show or hide the advanced settings for virtual WAN.		
Name	Enter a name as the profile name.		
Enabled	Switch the toggle to enable or disable the function.		
	General		
WAN Type	Displays the type (e.g., Ethernet) of the physical interface.		
WAN Interface Select one of the available WAN interfaces (enabled on WAN>>WA Connections). Connections			
	Port-Based Bridge		
Port Based Bridge Switch the toggle to enable or disable the function.			
	Binding Interface - Select an interface for binding.		
Multicast Stream VLAN Switch the toggle to enable or disable the function.			

In some areas, the multicast VLAN tag value might be different from
the IGMP VLAN tag. That might cause data transfer issues for IPTV
packets flooding to other VLAN ports while watching the IPTV
program.
Configure the IGMP VLAN tag and the multicast VLAN tag with the

Configure the IGMP VLAN tag and the multicast VLAN tag with the same value if required.

Downstream Multicast VLAN Tag – Enter the value for tagging the multicast packet. The range is from 0 to 4094.

Upstream IGMP VLAN Tag – Enter the value for tagging the IGMP packet. The range is from 0 to 4094.

VLAN Settings

Customer VLAN	It is available when a WAN Type is selected.
	Switch the toggle to enable or disable the function of VLAN with tag.
	Tag - Enter the value as the VLAN ID number. The range is from 0 to 4094.
	Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.
	Note if Multicast Stream VLAN Trans is enabled, the VLAN Settings will be ignored and disabled.

Options under the Advanced Mode

	IPv4
IPv4 Connection Type	 There are several types for network connection: PPPoE DHCP Static IP
Username/Password	It is available when PPPoE is selected as IPv4 Connection Type.
PPP Authentication	It means the protocol used for PPP authentication. Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use.
IP Assignment	It is available when PPPoE is selected as IPv4 Connection Type. DHCP - WAN IP address is dynamically allocated. Static IP - ISP has assigned a fixed WAN IP address. Enter an IP address.
IP Address	It means the WAN IP address assigned by the ISP. It is available when Static IP is selected as IPv4 Connection Type.
Subnet Mask	It means the WAN subnet mask. It is available when Static IP is selected as IPv4 Connection Type.
Gateway IP	It means the IP address of the WAN Gateway. It is available when Static IP is selected as IPv4 Connection Type.
Router Name	Set a name for the router. It is available when DHCP is selected as IPv4 Connection Type.
Domain Name	Enter the domain name used for the router. It is available when DHCP is selected as IPv4 Connection Type.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

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

II-1-2-4 Dynamic DNS

Most ISPs assigns dynamic WAN IP addresses to their customers. Dynamic IP addresses presents challenges to users who would like to accept remote connections to their LANs from the Internet, as service could be disrupted due to the IP address changing without notice. By setting up service with a Dynamic DNS (DDNS) provider, and configuring Dynamic DNS updates on the Vigor router, you can have reliable access to your network by means of an easy-to-remember domain address that resolves to the most current WAN IP address.

The Vigor router supports a wide range of DDNS providers. Please contact the DDNS provider of your choice to set up service before configuring DDNS on the router.

Jevice Menu	WAN Connecti	ons WAN AutoHun	t Virtual WAN Dynamic ONS	WAN Budget DHCP Options Failo	ver Link Health Check Performan	ce SLA PPPoE Pass-Through
	Dynamic DNS	5				
Dashboard						
	+ Add CLF	orce Update				Search
Physical Interface	Name	Enabled	Service Provider	Domain Name	Enable ACME Client	Option
				And Street own (Contract)		
LAN						
ONS						
Wireless LAN						
Routing						
OSPF						
Bandwidth Management						
NAT						
IGMP						
Objects						
Wake on LAN						
Notification Services						
RADIUS/ TACACS+						
Certificates						

ltem	Description
Reset	Click to clear all profiles to factory settings.
+Add	Click to bring up the configuration page of the DDNS profile (max. 6).
Force Update	Click to connect immediately to DDNS servers to update IP address information.

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

		×
Name 🕦		
Enabled		
Service Provider	DrayDDNS 🗸	
Service Status		
	Activate	
	Note: To use DrayDDNS, activate license and set up domain name on MyVigor. Use Activate button to link to MyVigor page.	
Expire Date		
Domain Name	.drayddns.com	
	Sync Domain	
Let's Encrypt Certificate		
Enable ACME Client	0	
Status		
	Note: Enable ACME Client to create and allow certificate to be auto-renewed before expire date.	
Cancel Apply		

ltem	Description						
Name	Enter a name as the profile name.						
Enabled	Switch the toggle to enable or disable the function.						
Service Provider	 Select the DDNS provider. If your DDNS provider is not listed, select User-Defined and manually configure the profile. DrayDDNS NO-IP Dyn.com 58DDNS User-Defined 						
If DrayDDNS is selected as Service Provider	 Service Status - Click Activate to activate the service. Expire Date - Display the expired date of the service. Domain Name - Display the domain and sub-domain to be updated. Sync Domain – The domain name for DrayDDNS is set on the MyVigor server. Click this button to load and obtain the domain name if it is available. 						
If NO-IP, Dyn.com, 58DDNS is selected as Service Provider	Domain Name - The domain and sub-domain to be updated. Account Name - Enter the login name of the DDNS account. Password - Enter the password of the DDNS account.						
If User-Defined is selected as Service Provider	 Provider Host URL - Enter the IP address or the domain name of the host which provides related service. Service API - Enter the IP address or the domain name of the host which provides related service. Server Response - Enter any text that you want to receive from the DDNS server. Account Name - Enter the login name of the DDNS account. Password - Enter the password of the DDNS account. 						

	Auth Type – Two types can be used for authentication.
	• Basic – Username and password defined later can be shown from the packets captured.
	 URL - Username and password defined later can be shown in URL.
	Enable ACME Client – Switch the toggle to generate a certificate issued by Let's Encrypt for applying to such DDNS account.
Let's Encrypt Certificate	It is available when DrayDDNS is selected as the service provider.
	Enable ACME Client – Switch the toggle to generate a certificate issued by Let's Encrypt for applying to such DDNS account.
	Status – Display the information related to Let's Encrypt certificate.
More settings	
Update DDNS with	If a Vigor router is installed behind any NAT router, you can enable this function to locate the real WAN IP.
	When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update.
	There are two methods offered for you to choose:
	Internet IP –The real public IP address will be used. Select this option the IP address assigned to the router's WAN interface is not the actual external IP address.
	WAN IP – The IP address of the router's WAN interface will be used.
	+Add – Click to create a new group of Binding Interface and Interface IP. Up to 6 sets can be created.
	Binding Interface – Select the WAN interface associated with the DDN profile.
	Interface IP – Select a WAN IP. If not, the default WAN IP will be used instead.
Update WAN IP Mode	It is available when DrayDDNS is set as the Service Provider.
	Update All Selected WAN IPs – Vigor router system will obtain the multiple WAN IPs based on the following table and upload to the service provider.
	Update Single WAN IP by Sequence – Vigor system will use the first selected WAN IP from the following table and upload to the service provider.
Auto Update Interval	The frequency, in minutes, at which the router connects to DDNS servers to update IP address information.
	The default is 14400.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

DrayDDNS Settings

DrayDDNS, a DDNS service developed by DrayTek, can record multiple WAN IP (IPv4/IPv6) on single domain name. It is convenient for users to use and easily to set up with MyVigor. Each Vigor Router is available to register one domain name to MyVigor for one year license.

DDNS updates take place when:

- The router is powered on or rebooted.
- The public IP address of any WAN interface changes.
- The online status of a WAN interface changes (going from online to offline or vice versa).
- The DDNS function is changed from "disabled" to "enabled".
- A DDNS entry is modified and enabled.
- The Auto Update Interval has elapsed.
- Pressing the Force Update.

II-1-2-5 WAN Budget

This function is used to determine the data *traffic volume* for each WAN interface respectively to prevent overcharges for data transmission by the ISP. Please note that the Quota Limit and Billing cycle day of month settings will need to be configured correctly first in order for some period calculations to be performed correctly.

The WAN Budget feature allows you to conveniently keep track of Internet traffic volume. You can:

- set up calendar cycles to monitor;
- limit your Internet usage according to your ISP's quota;
- set up action(s) to take when the quota is exceeded.

Search Q	Configuration / WAN								0	Reset C Refresh
	WAN Connections	WAN AutoHun	t Virtual WAN	Dynamic DNS	WAN Budget	DHCP Option	s Fallover	Link Health Check	Perfo	rmance SLA PP
evice Menu	WAN Budget									
h Dashboard	WAN budget									
Physical Interface	Interface ·	Enabled	Quota	Utilization			Time cycle	Email Alert	Option	
	[WAN] WAN1	Disable	MB			0%	Monthly	Disable	@ Edit	Reset Utilization
LAN	[WAN] WAN2	Disable	MB			0%	Monthly	Disable	/ Edit	Reset Utilization
DNS		and a second							P. Ser	
Wireless LAN	[WAN] WAN3	Disable	MB			0%	Monthly	Disable	/ Edit	Reset Utilization
Routing	[WAN] WAN4	Disable	MB			0%	Monthly	Disable	/ Edit	Reset Utilization
RIP	Contraction of the second									
BGP	[WAN] WANS	Disable	MB			0%	Monthly	Disable	2 Edit	Reset Utilization
OSPF										
Bandwidth Management										
NAT										
IGMP										
Objects										
Wake on LAN										
Notification Services										
RADIUS/ TACACS+										
Certificates										

To edit a profile, click the **Edit** link to get the following page.

		Dynamic DNS WAN Bu	unt Virtual WAN	WAN AutoHu	WAN Connections
					WAN Budget
[WAN] W	Interface				
	Enabled	Utilization	Quota	Enabled	Interface *
	Quota 🕕		MB	Disable	WAN] WAN1
MB GB			MB	Disable	[WAN] WAN2
Shutdown WAN inter	When quota exceeded		MB	Disable	WAN] WAN3
Monthly Custo	Time cycle				
your (cellular) data resets.	Select the day of a month when your (cellula		MB	Disable	WAN] WAN4
Select Day	Data quota resets on day		MB	Disable	WAN] WAN5
Select Time	bita quota rescu on day				
	SMS Alert				
(Email Alert				

Item	Description
Enabled	Switch the toggle to enable or disable the profile. When enabled, the WAN Budget is enabled for this WAN.
Quota	Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify.
When quota exceed	Shutdown WAN interface - All the outgoing traffic through such WAN interface will be halted when the traffic has exceeded the budget limiter
Time Cycle	Monthly – Some ISP might apply for the network limitation based on the traffic limit per month. This setting is to offer a mechanism of resetting the traffic record every month.
	Custom - This setting allows the user to define the billing cycle according to his request. The WAN budget will be reset with an interval of billing cycle.
When Monthly is selected as the Time Cycle	Data quota resets on day - You can determine the starting day in one month.
When Custom is selected as the Time Cycle	Monthly is default. If long period or a short period is required, use Custom . The period of cycle duration is between 1 day and 30 days. You can determine the cycle duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.
	Cycle duration (Days) – Specify the days (1~31) to reset the traffic record.
	Cycle duration (Hours) – Specify the hours (0~23) to reset the traffic record.
	Start Date – Specify the day in the cycle as the starting point which Vigor router will reset the traffic record.
	Start Time (Hr:Min.) - Specify the time for data quota rest in the cycle as the starting point which Vigor router will reset the traffic record.
SMS Alert	Switch the toggle to enable or disable the function.
	Send Alert SMS to – The system will send out SMS message to the use specified here when the quota is running out (less than 10%).
Email Alert	Switch the toggle to enable or disable the function.
	Send Alert Email to – The system will send out a warning message to the user specified here when the quota is running out (less than 10%)
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

II-1-2-6 DHCP Options

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

This page allows to configure additional DHCP client options.

SearchQ	Configuration / WAN									() Reset
Xivice Menu	WAN Connections	Virtual WAN	Dynamic DNS	WAN Budget	DHCP Options	Failover Lini	Health Check	Performance SLA	PPPoE Pass-Through	
Dashboard	DHCP Options									
	+ Add								Searchim	Max: 5
Physical Interface	Option Number			Data Type		D	ata	Apply to		Option
LAN										
DNS										
Wireless LAN										
Routing										
RIP										
BGP										
OSPF										
Bandwidth Management										
NAT										
IGMP										
Objects										
USB Application										
Wake on LAN										
Notification Services										
RADIUS/ TACACS+										
Certificates										

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

Connections Virtual WAN E	Dynamic DNS WAN Budget D	HCP Options Failover		×
CP Options			Option Number (0-255)	150
add			Data Type	ASCII Character \sim
tion Number	Data Type		Data 🕕	
			Apply to Note: 1. DHCP Option does NOT take effect w LAN or WAN settings.	All WANS v when the configured option number conflicts with

ltem	Description
Option Number	Each DHCP option is composed by an option number with data. Enter a number.
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.
Apply to	Select WAN interface(s) to which this entry is applicable.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

II-1-2-7 Failover

This page allows to configure settings for failover WAN.

When the primary WAN of the router goes down the other available WAN interfaces will take over for network connection sequentially.

search Q	Configuration / WAN					3	Reset
and and a set	WAN Connections WAN Auto	Hunt Virtual WAN Dynamic DNS WAN	Budget DHCP Option	ns Failover	Link Health Check	Performance SLA	pp >
Device Menu	Failover						- 1
 Dashboard 	Failover						
a Configuration	Primary WAN Members			Max: 1			
Physical Interface	Primary WAN Members	Interface		Max, 1			- 1
WAIL		internace					
LAN		[WAN] WANS (Cellular WAN) V					- 1
DNS							- 1
Wireless LAN							- 1
Routing	Failover WAN Members			Micc-4			- 1
RIP		Interface	Priority 🕕	Option			- 1
BGP		[WAN] WAN1 (Wired WAN) ~	1	Delete			
OSPF		December and stimic of					
Bandwidth Management		[WAN] WAN2 (Wired WAN) ~	2	Delete			
NAT		[WAN] WAN3 (Wireless WAN 2.4GHz) \sim	3	1 Delete			
IGMP							
Objects		[WAN] WAN4 (Wireless WAN 5GHz) ~	4	@ Delete			
LTE							
Wake on LAN							
Notification Services	Advanced Settings. V						
RADIUS/ TACACS+							
Certificates							- 1

ltem	Description		
Primary WAN Members	Interface – Select a WAN interface. This WAN will be used for network connection in default. However, if it loses connection, the failover WAN members will take over the network connection based on priority.		
Failover WAN Members	Display all the active WAN interfaces which will run as failover WAN. If the interface specified in this field loses connection or is detected unsuccessfully, traffic can be forwarded to an alternate interface.		
	Interface – Select a WAN interface. This WAN is intended to serve as a backup when other WAN ports specified have lost connection.		
	Priority – Determine the priority of the failover WAN. The less the number is, the more it is used first as a backup WAN.		
	Option (Delete) – Remove the entry settings (active WAN).		
	Advanced Settings		
Failback	Packets will be sent through another Interface or follow another polic when the original interface goes down (Failover to). Once the original interface resumes service (Failback), the packets will be returned to it immediately.		
	Switch the toggle to enable / disable the function.		
Restore Link Checks	It is available if Failback is enabled.		
	Enter a value that will enable the system to determine the number of checks required for the link. Once the link is successfully checked, the connection will be restored.		
Link Health Check and SLA	Switch the toggle to enable the function. If disabled, the active WAN interface will be determined based on		

	WAN connection detection mode defined in the WAN Connections Profile.				
	If enabled, the WAN connection detection defined in the WAN Connections Profile will be ignored. The router will measure the performance of interface members, and active interfaces will be determined using Link Health Check and Performance SLA.				
	Interface Link Health & SLA – List the available WAN interfaces for setting different health check methods.				
	• Interface – Display the WAN interfaces.				
	• Link Health Check Profile – Select one of the available check profiles (defined on Configuration>>WAN>>Link Health Check) for the interface.				
	Link Health Check Profile				
	Off 😒				
	Off				
	Google DNS				
	CloudFlare DNS				
	Quad9 DNS				
	 Performance SLA – Select one of the available check profiles (defined on Configuration>>WAN>>Performance SLA) for the interface. 				
Failure Retry Checks	Specify how many times for the system to check the connections. If all attempts fail, the system will determine that the connection is unstable.				
Cancel	Discard current settings and return to previous page.				
Apply	Save the current settings and exit the page.				

II-1-2-8 Link Health Check

Link Health Check is used for specifying the IPs (IPv4 and IPv6) that need to be verified to ensure network connectivity via ping/httping.

This page allows you to create profiles for executing the link health of the WAN interface.

By default, the system offers standard health check options such as Google DNS, CloudFlare DNS, and Quad9 DNS.

Take Google DNS as an example. This profile indicates that primary/secondary IPv4 target (8.8.8.8/8.8.4.4) is used for checking IPv4 network connection, while primary/secondary IPv6 target (2001:4860:4860::8888, 2001:4860:4860::8844) is used for checking IPv6 network connection. Network connection detection is performed per 10 seconds. If one of the IPv4 and IPv6 addresses is detected connection unsuccessfully, it will be judged as checking network connection failure.

Search Q	Configuration / WAN					0	set C Refres
	WAN Connections	WAN AutoHunt Virtu	al WAN Dynamic DNS	WAN Budget DHCP Options	Failover Link Health Check	Performa	nce SLA PP
Jevice Menu	Link Health Check						
Dashboard	Link freditir creek						
	+ Add						Max:
Physical Interface	Profile Name	Primary IPv4 Target	Secondary IPv4 Target	Primary IPv6 Target	Secondary IPv6 Target	Interval	Option
	Google DNS	8.8.8.8	8.8.4.4	2001:4860:4860::8888	2001:4860:4860::8844	10	/ Edt
LAN	CloudFlare DNS	1.1.1.1	1.0.0.1	2605:4700:4700::1111	2605:4700:4700::1001	10	/ Lot
DNS							
Wireless LAN	Quad9 DNS	9.9.9.9	149.112.112.112	2620:fe::fe	2620:fe::9	10	/ Edit
Routing							
RIP							
BGP							
OSPF							
Bandwidth Management							
NAT							
IGMP							
Objects							
Wake on LAN							
Notification Services							
RADIUS/ TACACS+							
Certificates							

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

				Profile Name 🕕	Google DNS
Add					doogle Divs
Profile Name	Primary IPv4 Target	Secondary IPv4 Target	Prima	Detection Method	Ping Detect 🗸 🗸
Google DNS	8.8.8.8	8.8.4.4	2001:	Primary IPv4 Target 🕧	8.8.8
CloudFlare DNS	1.1.1.1	1.0.0.1	2606:4	Secondary IPv4 Target 🕦	8.8.4.4
				Primary IPv6 Target 🕧	2001:4860:4860::8888
Quad9 DNS	9.9.9.9	149.112.112.112	2620:1	Secondary IPv6 Target 🕕	2001:4860:4860::8844
				Interval (Seconds)	10
			l		
			l		

ltem	Description
Profile Name	Enter a name as the Link Health Check profile.
Detection Method	 Select the protocol for ping detection. HTTP Detect Ping Detect
Primary IPv4 Target	Enter the first IPv4 address as the primary target for health check.
Secondary IPv4 Target	Enter the second IPv4 address as the secondary target for health check.
Primary IPv6 Target	Enter the first IPv6 address as the primary target for health check.

Secondary IPv6 Target	Enter the second IPv6 address as the secondary target for health check.
Interval	Set the time interval (unit is second) for network detection or checking.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

II-1-2-9 Performance SLA

This page allows you to set the thresholds for jitter, latency, and loss for Performance SLA (Service Level Agreement), which will be used for detecting the health status of the WAN connection.

Search Q	Configuration / WAN				TReset C Refres
	WAN Connections WAN AutoHunt	Virtual WAN Dynamic DNS	WAN Budget DHCP Options	Failover Link Health Check	Performance SLA PP
evice Menu	Performance SLA				
) Dashboard					
	+ Add				Max
Physical Interface	Profile Name	Jitter Thres	hold Latency Thr	eshold Loss R	ate Option
	Wired Default Performance SLA	30	30	2	/ Edit
LAN	Wireless Default Performance SLA	80	80	2	@ Edit
DNS	Wireless belaut Performance Str	00	60	-	D. stat
Wireless LAN					
Routing					
RIP					
BGP					
OSPF					
Bandwidth Management					
NAT					
IGMP					
Objects					
LTE Wake on LAN					
Wake on LAN					

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

WAN Connections WAN AutoHunt Virtual	WAN Dynamic DNS WAN Budget		×
Performance SLA		Profile Name 🕕	Wired Default Performance SLA
+ Add		Jitter	
Profile Name	Jitter Threshold	Juce	
Wired Default Performance SLA	30	Jitter Threshold (IRIS) 🕡	30
Wireless Default Performance SLA	80	Latency	
		Latency Threshold (ms) 🕧	30
		Packet Loss	
		Loss Rate (%) 🕥	2
			Cancel Apply

ltem	Description
Profile Name	Enter a name as the Link Health Check profile.
Jitter	Switch the toggle to enable or disable the jitter function. Jitter Threshold - It defines the change rate of latency. For stable session, small jitter value will be better. When the detected value is greater than the value set here, the connection will be regarded as unstable and connection failure.
Latency	Switch the toggle to enable or disable the latency function. Latency Threshold - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. When the detected value is greater than the value set here, the connection will be regarded as unstable and connection failure.
Packet Loss	Switch the toggle to enable or disable the packet loss function. Loss Rate - It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection. When the detected value is greater than the value set here, the connection will be regarded as unstable and connection failure.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

II-1-2-10 PPPoE Pass Through

The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. According to the WAN Connection Type, this feature will encapsulate the PPPoE package of local clients and send it to the WAN Server.

Search Q	Configuration / WAN ③Re	iset
	WAN AutoHunt Virtual WAN Dynamic DNS WAN Budget DHCP Options Failover Link Health Check Performance SLA PPPoE Pass-Thro	ough
Device Menu	PPPoE Pass-Through	
 Dashboard 	The resolution of the second se	
😑 Configuration —	Selected WAN Pieuse select 5	
Physical Interface		
WAN	PPPoE Pass-through	
LAN	To Wired LAN	
DNS	To Wired DAN	
Wireless LAN	Pass-through to All Clients Selected LAVis Specific LAV Clients	
Routing		
RIP	Specific Pass-through Clients + Add Macc 6	
BGP	MAC Address	
OSPF		
Bandwidth Management		
NAT		
IGMP		
Objects		
LTE Wake on LAN		
Notification Services		
RADIUS/ TACACS+		
Certificates		
	Cancel Apply	

Thus, the PC can access Internet through such direction.

Available settings are explained as follows:

Item	Description	Description				
Selected WAN	Select a WAN interface for	Select a WAN interface for applying the PPPoE pass-through.				
To Wired LAN		Switch the toggle to enable or disable the function. If enabled, wired LAN clients can initiate PPPoE dial-up connections to the selected WAN.				
Pass-through to	All Clients – All the wired L connections to the selecte		ate PPPoE dial-up			
	Selected LANs – One or more LAN clients can initiate PPPoE dial-up connections to the selected WAN.					
	Specific LAN Clients – Up to six specific LAN clients can initiate PPPoE dial-up connections to the selected WAN.					
	• +Add –Click to add a	new client.				
	Specific Pass-through Clients	+ Add	Max: б			
		MAC Address	Option			
			面 Delete			
Cancel	Discard current settings.	Discard current settings.				
Apply	Save the current settings.					

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

II-1-3 LAN

A LAN(Local Area Network) comprises a collection of LAN clients, which are networked devices on your premises. A LAN client can be a computer, a printer, a Voice-over-IP (VoIP) phone, a mobile phone, a gaming console, an Internet Protocol Television (IPTV), etc, and can have either a wired (using Ethernet cabling) or wireless (using Wi-Fi) network connection.

LAN clients within the same LAN are normally able to communicate with one another directly, as they are peers to one another, unless measures, such as firewalls or VLANs, have been put in place to restrict such access. Nowadays the most common LAN firewalls are implemented on the LAN client itself. For example, Microsoft Windows since Windows XP and Apple OS X have built-in firewalls that can be configured to restrict traffic coming in and going out of the computer. VLANs, on the other hand, are usually set up using network switches or routers.

To communicate with the hosts outside of the LAN, LAN clients have to go through a network gateway, which in most cases is a router that sits between the LAN and the ISP network, which is the WAN. The router acts as a director to ensure traffic between the LAN and the WAN reach their intended destinations.

IP Address

On most broadband networks, the ISP assigns a single WAN IP address to the subscriber. All LAN clients have to share this WAN IP address when accessing the Internet. To achieve this, a technique called Network Address Translation (NAT) is used. Under NAT, a private block of IP addresses is assigned to the LAN clients, which communicate with WAN hosts through the router, also known as the gateway.

On outgoing traffic to the WAN, the router makes note that a LAN client has attempted to reach a WAN host, and forwards the request to the intended WAN recipient.

On traffic incoming to the LAN from a WAN host, the router checks its records to see if a matching outstanding request from a LAN client to this WAN host exists, and if so, forwards it to the LAN client. Otherwise, the traffic is dropped.

There are 3 distinct blocks of IPv4 address that are reserved for use as private IP addresses on a LAN.

Name IP Address Range	Number of Available Addr	esses Largest Subnet Mask
24-bit Block 10.0.0.0 to 10.25	55.255.255 16,777,216 255	5.0.0.0
20-bit Block 172.16.0.0 to 17	2.31.255.255 1,048,576	5 255.240.0.0
16-bit Block 192.168.0.0 to 1	92.168.255.255 65,536	255.255.0.0

The default beginning IP Address of LAN 1 is 192.168.1.1, and the Subnet Mask is 255.255.255.0, for a total of 254 assignable IP addresses, from 192.168.1.1 to 192.168.1.254. The final IP address of the selected range is reserved for routing and cannot be assigned to a LAN client.

In most cases, the default IP address block should work satisfactorily. However, there are situations where you need to select a different address block, such as when you need to communicate with other LANs that already use the same address block.

Private IP addresses can be assigned automatically to LAN clients using Dynamic Host Configuration Protocol (DHCP), or manually assigned. The DHCP server can either be the router (the most common case), or a separate server, that hands out IP addresses to DHCP clients.

Alternatively, static IP addresses can be manually configured on LAN clients as part of their network settings. No matter how IP addresses are configured, it is important that no two devices get the same IP address. If both DHCP and static assignment are used on a network, it is important to exclude the static IP addresses from the DHCP IP pool. For example, if your LAN uses the 192.168.1.x subnet and you have 20 DHCP clients and 20 static IP clients, you could configure 192.168.1.10 as the Start IP Address, 50 as the IP Pool Counts (enough for the current number of

DHCP clients, plus room for future expansion), and use addresses greater than 192.168.1.100 for static assignment.

II-1-3-1 LANs

This page provides you the general settings for LAN.

Open **Configuration>>LAN** and click the **LANs** tab to open the following page.

SearchQ	LANS	Bind IP t	MAC DHCP	Options Inter-LAN	Routing VLAN List	Interface VLAN	LAN Port 802.1X			
Device Menu										
Dashboard	LANs									
	+ Add									Max
Physical Interface	Name	Usage	IPv4 Address	Subnet Mask	IPv4 DHCP Server	Primary DNS	IPv6 Assignment	Router IPv6 Address Table	Option	
WAN	LAN1	NAT	192.168.1.1	255.255.255.0/24	On	8.8.8.8	Stateless	[fe80::1649:bcff:fe86:fab8/64]	@ Edit	
DNS										
Wireless LAN										
Routing										
RIP										
BGP										
OSPF										
Bandwidth Management										
NAT										
IGMP										
Objects										
Wake on LAN										
Notification Services										
RADIUS/ TACACS+										
Certificates										

To add/edit a profile, click the **+Add/Edit** link to get the following page. Here, we take LAN1 as an example.

		×
Name 🛈	LAN1	Advanced Mode: ON
General Setup		
IPv4	Enable	
Usage	NAT Routing	
IPv6		
IPv4		~
IPv4 Address 🕡	192.168.1.1	
Subnet Mask	255.255.255.0/24 🗸	
DHCP Server Configuration		
IPv4 DHCP Server	On Off Relay	
Start IP Address 🕕	192.168.1.10	
IP Pool Counts (1-253)	100	
Gateway IP Address 🕕	192.168.1.1	
	86400	

ltem	Description
Advanced Mode: ON/OFF	Click to show or hide the advanced settings for LAN.
Name	Display the name for identification. Change the name if required.

	General Setup			
IPv4	Display the status (enable/disable) of the profile.			
Usage	 Specify the IP forwarding method. NAT Routing 			
IPv6	Switch the toggle to configure / ignore the IPv6 settings.			
	IPv4			
IPv4 Address	This is the IP address of the LAN interface (default: 192.168.1.1).			
Subnet Mask	Select a subnet mask of the LAN interface.			
	DHCP Server Configuration			
IPv4 DHCP Server	LAN1 is configured with DHCP in default.			
	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP serve for your network.			
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.			
	On - Enables the built-in DHCP server on the router.			
	Off - Disables the built-in DHCP server on the router.			
	Relay - When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field.			
If On is selected as DHCP Server	Start IP Address - The beginning LAN IP address that is given out to LAN DHCP clients.			
	IP Pool Counts - The maximum number of IP addresses to be handed out by DHCP. The default value is 100. Valid range is between 1 and 253.			
	Gateway IP Address - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN The gateway is normally the router.			
	Lease Time - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.			
	 Primary DNS - DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. 			
	Secondary DNS - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.			
lf Relay is selected as DHCP Server	When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field.			
	Primary DNS - DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a			

	human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.				
	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server.				
	Secondary DNS - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.				
	DHCP Relay over WAN (Primary) – Switch the toggle to enable this function. Then, specify a WAN interface for the first DHCP Server.				
	• Primary DHCP Server Interface – Use the drop-down list to choose a WAN interface for the first DHCP Server.				
	Primary DHCP Server IP Address - Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded.				
	DHCP Relay over WAN (Secondary) - The secondary DHCP server is an optional setting. If required, specify a WAN interface for the second DHCP Server as a backup server.				
	• Secondary DHCP Server Interface – Use the drop-down list to choose a WAN interface for the second DHCP Server.				
	Secondary DHCP Server IP Address - Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded.				
IP Assignment for Teleworkers	The VPN client will receive an IP address from the DHCP pool or IP address range (defined below) for Teleworkers.				
	Assignment Start IP – Enter an IP address that serves as the starting point of a range of IP addresses.				
	Assignment End IP – Enter an IP address that serves as the end point of a range of IP addresses.				
	IPv6				
IPv6 Assignment	Configures the Managed Address Configuration flag (M-bit) in Route Advertisements.				
	Stateless – M-bit is unset.				
	DHCPv6(Stateful) – M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor router, or a separate DHCPv6 server.				
	Manual – No configuration information is sent.				
Router Advertisement	It is available when Stateless is selected as the IPv6 Assignment.				
Configuration	The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.				
	Generate Prefix From – Select the primary WAN interface which is capable to generate the prefix for IPv6 address. Use the drop down list to specify a WAN interface for IPv6.				

	Disabled [WAN] WAN1 (Static_IP_1) [WAN] WAN2 (Static_IP_22) [WAN] WAN3 () [WAN] WAN4 () Disabled
DNS Configuration	 It is available when Stateless is selected as the IPv6 Assignment. DNS Assign Methods RA(RDNSS) – The DNS server used for hosts (e.g., PC) will be configured via the Router Advertisement Configuration. Bit(DHCPv6) – The DNS server used for hosts will be configured via DHCPv6 server. Manual – Vigor router system will not send DNS sever configuration to the hosts. Primary DNS Address - Enter the IPv6 address for Primary DNS server is required.
DHCPv6 Server Configuration	 It is available when DHCPv6 (Stateful) is selected as the IPv6 Assignment. On - Enables the built-in DHCPv6 server on the router. Generate Prefix From – Select the primary WAN interface which is capable to generate the prefix for IPv6 address. Use the drop down list to specify a WAN interface for IPv6. Auto IPv6 Address Range Random IPv6 Address Allocation Off - Disables the built-in DHCPv6 server on the router. Relay - When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field. DHCPv6 Server Interface – Use the drop down list to specify a WAN interface for IPv6. DHCPv6 Server Address - Enter the IPv6 address of the DHCPv6 server.
DNS Configuration	It is available when DHCPv6 (Stateful) is selected as the IPv6 Assignment. Primary DNS Address - Enter the IPv6 address for Primary DNS server Secondary DNS Address - Enter another IPv6 address for DNS server is required.
More Settings - Force DNS Redirection	Enabled – Switch the toggle to enable or disable the function. This function allows all outgoing DNS queries to be intercepted and redirected to the router built-in DNS server, improving the domain lookup performance by caching DNS queries and results.

Router IPv6 Address	Enter IPv6 Address and Prefix length to be added, or click an existing
Table	IPv6 address to be deleted in the Current IPv6 Address Table below

	and the values will be automatically copied over.			
	+Add – Click it to add a new entry. Max is 5.			
	Static IP Address – Enter the static IPv6 address for LAN.			
Unique Local Address Configuration	Unique Local Addresses (ULAs) are private IPv6 addresses assigned to LAN clients.			
	ULA Prefix – LAN clients will be assigned ULAs generated based on the prefix manually entered.			
	• Off – ULA is disabled.			
	 Auto – LAN clients will be assigned ULAs using an automatically-determined prefix. 			
	• Manual – Enter an IPv6 address.			
Router Advertisement Configuration	The Advanced Settings page has additional settings for Router Advertisement and enabling multiple WANs for IPv6 traffic.			
	RA Priority – Select the default preference value (Low, Medium, High) of the router sent in route advertisement messages.			
	Min / Max Interval Time – Minimum/ Maximum time, in seconds, between unsolicited multicast route advertisement messages sent by the RA server.			
	Valid Lifetime – Enter one number (unit is second) to specify the valid lifetime for the DHCPv6 server. The device (connected via the LAN interface) is to be used as the default router.			
	This device (connected via the LAN interface) will be treated as the default router within the valid lifetime.			
	Preferred Lifetime – Enter one number (unit is second) to specify the preferred lifetime for the DHCPv6 server. It must be lower or equal to the valid lifetime. This device (Vigor router) will be treated as the default router within the preferred lifetime. When there are multiple routers, priority is necessary. In general, the router within the preferred lifetime has higher priority than the router within the valid lifetime.			
	Hop Limit - The value is required for the device behind the router when IPv6 is in use. Default value of hop limit field in Route Advertisement messages.			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

II-1-3-2 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.

Search Q	Configuration / LAN			🕲 Rese
and the second	LANS Bind IP to MAC DHC	Options Inter-LAN Routing VLAN List In	tterface VLAN LAN Port 802.1X	
evice Menu				
) Dashboard	Bind IP to MAC			
	+ Add			Search Mex: 3
Physical Interface	Comment	MAC Address	IP Address	Option
WAN				
DNS				
Wireless LAN				
Routing				
RIP				
BGP				
OSPF				
Bandwidth Management				
NAT				
IGMP				
Objects				
Wake on LAN				
Notification Services				
RADIUS/ TACACS+				
Certificates				

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

P to MAC DHCP C	Options Inter-LAN Routing	VLAN List Interf		×
C		_	Comment 🕕	Bind_1F_to_3F
	MAC Address	_	MAC Address (Input format is FF:FF:FF:FF:FF:FF:FF:	08:BF:B8:D5:DD:A9
	MAC Address		IP Address 🕕	192.168.1.100
				Cancel Apply

Available settings are explained as follows:

ltem	Description
Comments	Enter a brief comment to identify this IP Address – MAC Address pair.
MAC Address	Enter the MAC address of the LAN client's network interface.
IP Address	Enter the IP address to be associated with a MAC address.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-3-3 DHCP Options

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

Search Q	Configuration / LAN				() Reset
	LANS Bind IP to MAC DHCP Op	tions Inter-LAN Routing VLAN List	Interface VLAN LAN Port 8	02.1X	
Device Menu					
Dashboard	DHCP Options				
	+ Add			Search	Max: 5
Physical Interface	Option Number	Data Type	Data	Apply to	Option
WAN					
DNS					
Wireless LAN					
Routing					
RIP					
BGP					
OSPF					
Bandwidth Management					
NAT					
IGMP					
Objects					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates					

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

Bind IP to MAC	DHC ² Options	Inter-LAN Routing	VLAN List	Interf			×
Options				8	Option Number (0-255)	47	
Number		Data Type		8	Data Type	ASCII Chara	icter ∨
				sorits.	Data 🕐		
				8	Apply to	All LANS	/
				8	Note:	All LANS	
					 DHCP Option does NOT take effect when the configured option LAN or WAN settings. 	Specified	LAN

ltem	Description
Option Number	Enter a DHCP option number for this function.

Choose the type (ASCII or Hex or Address List) for the data to be stored.				
Enter the data in the Data field based on the data type selected. ASCII Character - A text string. Example: /path. Hexadecimal Digital - 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.				
Select LAN interface(s) to which this entry is applicable.				
Discard current settings and return to the previous page.				
Save the current settings and exit the page.				

II-1-3-4 Inter-LAN Routing

Up to 25 routing profiles provided by the router allow the users to divide groups into different subnets. In addition, different subnets can link for each other by configuring **Inter-LAN Routing**.

Search Q	Configuration / LAN			3 Rese
	LANS BIND IP to MAC DHCP Opt	tions Inter-LAN Routing VLAN List	Interface VLAN LAN Port 802.1X	
Device Menu	Laurian Barrison			
Dashboard	Inter-LAN Routing			
	+ Add			Search Maxi 2
Physical Interface	Group Name	Enabled	Selected LANs	Option
WAN				
DNS				
Wireless LAN				
Routing				
RIP				
BGP				
OSPF				
Bandwidth Management				
NAT				
IGMP				
Objects				
Wake on LAN				
Notification Services				
RADIUS/ TACACS+				
Certificates				

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

s Bind IP to MAC DHCP Opti	ons Inter-LAN Routing VLAN List	interi	×
er-LAN Routing		Group Name 🕕	Inter_100
Add		Enabled	
roup Name	Enabled		
		Selected LANs	select your options
			Select All
			Search
			[LAN] LAN1
			Cancel Apply

ltem	Description
Group Name	Display the name for identification. Change the name if required.
Enabled	Switch the toggle to enable the settings.
Selected LANs	Select the box to link two or more different subnets (LAN and LAN).
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-3-5 VLAN List

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

Search Q	Configuration / LAN			Theset C Hefresh
	LANS BIND IP to MAC DHO	P Options Inter-LAN Routing VLAN List	Interface VLAN LAN Port 802.1X	
evice Menu	VLAN List			
b Dashboard	YEAY LIST			
	y Add			Max
Physical Interface	VLAN ID	Name	LAN	Option
WAN	- +	Default VLAN	(LAN) LAN1	an Edit
DNS				
Wireless LAN				
Routing				
RIP				
OSPF				
Bandwidth Management				
NAT				
IGMP				
Objects				
Wake on LAN				
Notification Services				
RADIUS/ TACACS+				
Certificates				

This page allows you to create up to 8 VLAN profiles.

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

AC DHCP Options Inter-LAN Routing	VLAN LIST Interf	>
	VLÂN ID 🕕	100
Name	Name	VLAN
Default VLAN	LAN	Please select >
		[LAN] LAN1

ltem	Description
item	Description

VLAN ID	Enter a number as the VLAN Identifier. Valid values are form 1 to 4094. VIDs must be unique.			
Name	Enter a name of the VLAN profile.			
LAN	Display the physical LAN subnet on the router. Select the LAN subnet(s) to bind them under the selected VLAN.			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

II-1-3-6 Interface VLAN

Port-based VLAN uses physical ports (P1 ~ P4/P5) to separate the clients into different VLAN group.

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. The multi-subnet can let a small businesses have much better isolation for multi-occupancy applications.

Search	Configura	IUON / LAN						③ Reset C Refres
	LANS	Bind IP to MAC	DHCP Options	Inter-LA	N Routing VLAN Lit	at Interlace VLAN	LAN Fort 802.1X	
levice Menu	Interface	e VLAN Settings						
Dashboard	internace	e vesav secongs						
Physical Interface	Ethernet	t.						
WAN								
	Ethernet		Interface	Port Type	Untagged VLAN	Tagged VLAN		
DNS			Port 1	Trunk 🗸	1 (Default VLAN) ~	All VLANs Select V	LANS	
Wireless LAN			Port 2	Trunk	1 (Default VLAN) ~	ALVLANS SoleCT	LANS	
Routing								
RIP			Port 3	Trunk 🗸	1 (Default VLAN) ~	All VLANS Select VI	LANS	
BGP			Port 4	Trunk 🗸	1 (Default VLAN) ~	AT VLANA Select V	LAN	
OSPF								
Bandwidth Management			Port 5	Trunk 🗸	1 (Default VLAN) 🗸	AT VLANS Select V	LANS	
NAT								
IGMP								
Objects								
LTE Wake on LAN								
Notification Services								
RADIUS/ TACACS+								
Certificates								

ltem	Description
Port Type	Select the VLAN type that the interface (Port 1 to 4) will be applied.
	Trunk – The selected Ethernet port can be used or applied to Multiple VLAN profiles.
	Access – The selected Ethernet port can be used or applied to single VLAN profile.
Untagged VLAN	Select the VLAN profile(s) which will not be tagged.
	Leave one VLAN untagged at least to prevent from not connecting to Vigor router due to unexpected error.
Tagged VLAN	Enable 802.1Q tagging for the selected VLAN.
	The router will add specific VLAN number to all packets on the LAN while sending them out.
	All VLANs – All VLAN profiles will be tagged.
	Selected VLANs – Only the selected VLAN profiles will be tagged.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-3-7 LAN Port 802.1x

Wired 802.1X provides authentication for clients wishing to connect to the LAN by Ethernet. Only one client can be authenticated on each LAN port.

Search C	Configuration / LAN				3 Rest
Searcha.	LANS Bind IP to MAI	DHCP Options Inter-LA	N Routing VLAN List	nterface VLAN LAN Port 802.1X	
evice Menu					
ŋ Dashboard	LAN Port 802.1X				
	Enable LAN Port 802.1X				
Physical Interface					
WAN	802.1X Ports	Port Name	Function	Enabled	
		Port 1	LAN		
DNS				-	
Wireless LAN		Port 2	LAN		
Routing		Port 3	LAN		
RIP		Port 4	LAN		
BGP		Port 4	DAN		
OSPF		Port 5	LAN		
Bandwidth Management					
NAT	Note: 802.1X requires 1	AN function on the port. Manag	e in Dhusical Interface		
IGMP	Hoterooza i regones e	And insured on one pore manual	and the second second		
Objects					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates	Cancel Apply				

ltem	Description
Enabled LAN 802.1X	Switch the toggle to enable or disable LAN 802.1x function.
Port Name	Display the name of the physical LAN port.
Enabled	Switch the toggle to enable or disable the function. If enabled, the 802.1X authentication will be available for the selected LAN ports.
Cancel	Discard current settings.
Apply	Save the current settings.

II-1-4 DNS

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

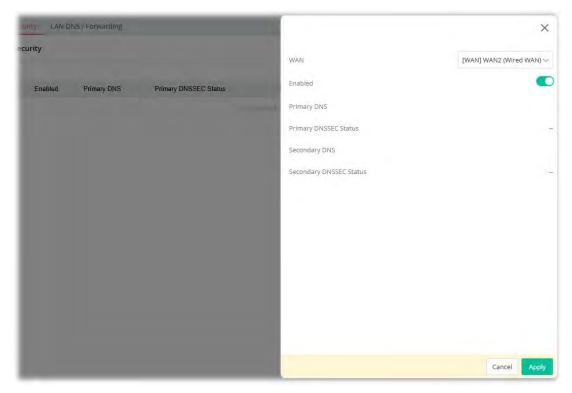
This section offers settings for DNS security and LAN DNS/Forwarding.

II-1-4-1 DNS Security

The DNS servers must support DNS security validation for the feature to function properly.

searchQ	Configuration / DNS	IS / Forwarding				SReset CRefresh
Device Menu (?) Dashboard Confected/on	DNS Security					Masc 6
Contentation Physical Interface WAN LAN THE Writeless LAN Routing RIP BGP OSFF Bandwidth Management NAT IGMP Objects USB Application Wake on LAN Notification Services RADIUS/TACACSH Certificates	WAN Enabled	Primary DNS	Primary DNSSEC Status	Secondary DNS	Secondary DNSSEC Status	Option

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



ltem	Description
WAN	Select the WAN interface for which DNS security is to be configured.
Enabled	Switch the toggle to enable or disable DNS security for this WAN Interface. Bogus DNS Reply will be dropped when DNS security enabled.
Primary DNS	Shows the primary DNS server used by this WAN.
	If "" appears, it means that no WAN is up or no DNS server is configured.
Primary DNSSE Status	Shows the inspection results if the DNS server supports the DNS security. The result might be:
	• [Supported] means the DNS server supporting DNS security.
	 [Unsupported] means the DNS server does not support DNS security,
	• "" means the WAN interface is not up or no DNS server detected
	 [Check Failed - WAN Issue] means failure to inspect due to no Internet connection.
	• [DNSSEC Disabled] means the DNS security is disabled.
	Note : Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.
Secondary DNS	Shows the secondary DNS server used by this WAN.
	If "" appears, it means that this WAN is not up or no DNS server is configured.
	it means that this WAN is not up or no DNS server is configured.
Secondary DNSSE Status	Shows the inspection results if the DNS server supports the DNS security. The result might be:
	 [Supported] means the DNS server supporting DNS security.
	 [Unsupported] means the DNS server does not support DNS security,
	• "" means the WAN interface is not up or no DNS server detected
	 [Check Failed - WAN Issue] means failure to inspect due to no Internet connection.
	• [DNSSEC Disabled] means the DNS security is disabled.
	Note : Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-4-2 LAN DNS/Forwarding

LAN DNS is a simple version of DNS server. LAN DNS allows the network administrator to override standard DNS resolutions for selecting domain addresses. The router will respond to queries on matched domain addresses with custom IP addresses. It is not necessary for the user to build another DNS server in LAN. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.

DNS Forwarding allows the network administrator to forward DNS queries to different DNS servers based on the domain name.

LAN DNS and DNS Forwarding only affect DNS queries that are sent to the WAN through the router. DNS queries that are directed to a DNS server on the LAN will not be intercepted by the router.

Search Q	Configuration / D	NS					() Result
Device Menu	LAN DNS / Forv						
a configuration	- Add					Search	Max: 120
Physical Interface	Name	Enabled	Туре	Domain Name	Mapping	Apply to	Option
WAN							
LAN							
DNB							
Wireless LAN							
Routing							
RIP							
BGP							
OSPF							
Bandwidth Management							
NAT							
IGMP							
Objects							
LTE							
Wake on LAN							
Notification Services							
RADIUS/ TACACS+							
Certificates							

To add/edit a profile (up to 120), click the **+Add/Edit** link to get the following page.

		>
Name 🕡		
Enabled		
уре	IP CNAME Forwarding	
Jomain Name	+ Add	Max: 12
	Domain Name	
	Note: Support wildcard subdomain, e.g. *.example.com	
Napping IP Address Type		
	Note: Support wildcard subdomain, e.g. *.example.com	
Mapping IPv4 Address	Note: Support wildcard subdomain, e.g. *.example.com	
Vapping IPv4 Address Vapping IPv6 Address	Note: Support wildcard subdomain, e.g. *.example.com	
Mapping IP Address Type Mapping IPv4 Address Mapping IPv6 Address Apply to	Note: Support wildcard subdomain, e.g. *.example.com	

ltem	Description					
Name	Enter a string as the profile name.					
Enabled	Switch the toggle to enable/disable this profile.					
Туре	Select IP, CNAME or Forwarding.					
Domain Name	+Add – Enter the domain name for the router to look for in DNS queries to intercept and reply to. Wildcards in the form of asterisks (* can be used to match a domain level. For example, *.draytek.com will match domain names such as www.draytek.com and ftp.draytek.com Up to 12 domain names can be created.					
If IP is selected as Service Provider	The IP address listed here will be used for mapping with the domain name specified above.					
	Mapping IP Address Type – Select Both, IPv4, or IPv6.					
	Mapping IPv4 Address – If Both/IPv4 is selected, enter an IPv4 address in this field.					
	Mapping IPv6 Address – If Both/IPv6 is selected, enter an IPv6 address in this field.					
	Apply to – Select all LANs or specified LAN interfaces for applying this DNS server profile.					
If CNAME is selected as	CNAME – Enter a domain name alias for the domain name.					
Service Provider	Apply to - Select all LANs or specified LAN interfaces for applying this DNS server profile.					
If Forwarding is selected	DNS Server Type – Both, IPv4, IPv6					
as Service Provider	Primary IPv4 DNS Server – Enter the primary IPv4 address of the DNS server you want to use for DNS forwarding.					
	Secondary IPv4 DNS Server – Enter the secondary IPv4 address of the DNS server you want to use for DNS forwarding.					
	Primary IPv6 DNS Server –Enter the primary IPv6 address of the DNS server you want to use for DNS forwarding.					
	Secondary IPv6 DNS Server – Enter the secondary IPv6 address of the DNS server you want to use for DNS forwarding.					
	Apply to - Select all LANs or specified LAN interfaces for applying this DNS server profile.					
Cancel	Discard current settings and return to the previous page.					
Apply	Save the current settings and exit the page.					

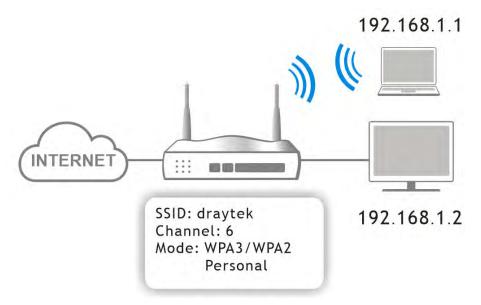
II-1-5 Wireless LAN

Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

In recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches virtually every location on earth. Billions of people exchange information daily with wireless communication products. The Vigor C410/C510 series of wireless routers (with "ax" in the model name), designed with maximum flexibility and efficiency in mind, is ideal for use in a small office or home. In a business environment, any authorized personnel can bring a WLAN-equipped tablet, PDA or notebook into a meeting room and connect to the network without drilling holes through walls or tearing up flooring to lay a clot of LAN cabling. Wireless networking enables high mobility so WLAN users can access all LAN resources in the same manner just as they would on a wired LAN, but without the cables.

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

In an Infrastructure Mode of wireless network, Vigor wireless router 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 Vigor wireless router. The wireless network settings, such as SSID, channels, encryption protocol, can be configured in this section.



Multiple SSIDs

Vigor wireless routers support up to four SSIDs (Service Set Identifiers) per band for wireless connections. A service set is a group of wireless network clients that have the same networking parameters. Each service set can be configured to have a unique name (SSID) and specific VLAN or MAC Filtering List, and can be used by different categories of users.

Real-time Hardware Encryption

Vigor wireless routers are equipped with a hardware AES encryption engine to provide the most effective and efficient protection of wireless traffic, without sacrificing user experience.

Complete Security Standard Selection

To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

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 (PSK) is used to encrypt traffic during data transmission. WPA uses the Temporal Key Integrity Protocol (TKIP) for data encryption whereas WPA2/WPA3 applies AES (Advanced Encryption Standard). A major advantage of WPA-Enterprise is that it supports not only encryption but also authentication.

You should select the appropriate security mechanism according to your needs. Because WEP has proven to be vulnerable to attacks, you should consider using WPA instead for the most secure connection. 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 Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.



The default password (PSK) is listed on a label attached to the bottom of the router. Since anyone who has physical access to the router can discover the default password, you are strongly advised to change it.



Manage Wireless Stations – Monitoring - Clients List

All stations on the wireless network and their connection status will be shown here.

WPS

WPS (Wi-Fi Protected Setup) makes connecting wireless clients to wireless access points and routers a simple process.



II-1-5-1 SSID

On Wi-Fi-equipped models, you can set up SSID for use by internal users, who are allowed to access both the LAN and the WAN (Internet).

This page also allows you to configure a guest SSID (for wireless clients that are restricted to Internet access only, typically used by visitors) with LAN VLAN settings.

	Configuration / Wireless LAN	4								3 Reset
	SSID Radio Settings F	Roaming AP I	Discovery WPS WDS							
Device Menu	SSID									
Dashboard										
Physical Interface	+ Add									Max:
WAN	SSID ()	Enabled	Security	Password ①		VLAN	Scheduled On	2.4GHz	5GHz	Option
LAN	DrayTek-86FAB8		WPA3/WPA2 Personal \backsim		Ð	Please select _ <<	Always On $\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!$	•		Ø Edit
DNS										
Routing										
RIP										
BGP										
OSPF										
Bandwidth Management										
NAT										
IGMP										
Objects										
Wake on LAN										
Notification Services										
RADIUS/ TACACS+										
Certificates										

To add a new SSID profile, click **+Add** to create new entry boxes.

onfiguration / Wireles	s LAN									C Rese
SID Radio Settings	Roaming	AP Discovery WPS	WDS							
SID										
-										
Add										Max
-Add SSID (7	Enabled	Security	Password ()		VLAN	Scheduled On	2.4GHz	5GHz	Option	Max:
	Enabled	Security WPA3/WPA2 Personal ~	Password ()	٢	VLAN Please select V	Scheduled On Always On ~	2.4GHz	5GHz	Option	Max:

To edit a profile, click the **Edit** link on the right side to get the following page.

ISID 🕕	DrayTek-366100	
Enabled		
Security	WPA3/WPA2 Personal 🔗	
Password		
/LAN	Please select	
Scheduled On	Always On \sim	
SSID Band		
2.4GHz		
5GHz		
SSID Settings		
VAC Filtering List	Disabled V	
solate Client from Wireless		
Hide SSID		
WPA Settings		
Cancel Apply		

ltem	Description
SSID	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters. Modify the name if required.
Enabled	Switch the toggle to enable/disable the SSID profile.
Security	There are several modes provided for you to choose from. Below shows the modes with higher security;
WPA3/WPA2 Personal · · · · · · · · · · · · · · · · · · ·	WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal - Accepts only WPA clients and the encryption key should be entered in Password. The WPA encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password."
WPA2 Personal WPA2/WPA Personal WPA3 Enterprise	• WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise - Accepts only WPA clients and the Authentication Server should be set in Configuration >> RADIUS/ TACACS+ >> External RADIUS and be selected in RADIUS Server. The WPA encrypts each frame transmitted from the radio using the key which 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 Password. The WPA encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password.
	 WPA Enterprise - Accepts only WPA clients and the Authentication Server should be set in Configuration >> RADIUS/ TACACS+ >> External RADIUS and be selected in RADIUS Server. The WPA encrypts each frame transmitted

	from the radi via 802.1x au	io using the key which automatically negotiated thentication.		
	• WEP Personal - Accepts only WEP clients and the encryption key should be entered in WEP Settings.			
	• None - The e	ncryption mechanism is turned off.		
Password	available for WPA F	naracters, such as "012345678". This feature is Personal, WPA2/WPA Personal, WPA2 Personal, nal, and WPA3 Personal mode.		
RADIUS Server		lable for WPA3 Enterprise, WPA2 Enterprise, rise, and WPA Enterprise mode.		
	Use the drop-dowr	n list to select a RADIUS server setting.		
		guring the RADIUS server, go to . DIUS/TACACS+ to create external RADIUS ne) first.		
VLAN	Select a VLAN to w	hich this SSID belongs.		
Scheduled On	This SSID profile wi profile used (profile Configuration>>Ob			
	Scheduled On	Always On 🔗		
		Always On		
		Schedule_morning		
		Schedule_noon		
		Schdule_night		
	The default is Alwa	ys On.		
	SSID	Band		
2.4GHz/5GHz	Select the band(s)	for the SSID.		
	SSID Se	ettings		
MAC Filtering List	The default is Disa l	bled.		
	Select one of the N Filtering Profile) for	IAC filter profiles (created via Security>>MAC r this SSID setting.		
	Only the valid MAC to access the wirele	address that has been configured allow or den ess LAN interface.		
	Disabled			
	MAC_Filter_E	ast		
	MAC_Filter_V	Vest		
	MAC_Filter_S	outh		
	Disabled	2		
Isolate Client from Wireless	Switch the toggle to	o enable/disable the function.		
If enabled, it disallows communication between wireless clie (stations) on the same SSID.				

Hide SSID	Switch the toggle to enable(hide) /disable (show) the SSID. Select to keep SSIDs from showing up when scans are performed by wireless clients, which makes it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless client and software used, the user may see only an AP listed without the SSID, or the AP might not even show up.	
	WPA Settings	
WPA Algorithm	This feature is available for WPA3 Enterprise, WPA2 Enterprise, WPA Enterprise, WPA3 Personal, WPA2 Personal, WPA Personal, WPA3/WPA2 Personal, or WPA2/WPA Personal mode.	
	Select TKIP, AES, or TKIP/AES as the algorithm for WPA.	
	Note that not all modes of Vigor router support WPA3 mode. However, if the Vigor router supports WPA3 Personal/Enterprise security mode, the WPA algorithms will be set as AES.	
Key Renewal Interval	It is available when WPA # is selected as Security.	
	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.	
	WEP Settings	
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 charact or 10 hexadecimal values in 64-bit encryption level, or restricted 13 ASCII characters or 26 hexadecimal values in 128-bit encryptic level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.	
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.	
Cancel	Discard current settings and return to the previous page.	
Apply	Save the current settings and exit the page.	

II-1-5-2 Radio Settings

This page lets you configure the most basic settings of your wireless network, including mode, WLAN channels and channel bandwidth.

Search Q	Configuration / Wireless LAN	Dass
Device Menu		aming AP Discovery WPS WDS
(?) Dashboard	Radio Settings	
E Configuration		Advanced Mode: OFF
Physical Interface	2.4GHz Radio	
WAN		
LAN	Enabled	
DNS	Mode	Mixed (11b+11g+11n+11ax) 🐱
Wireless LAN	Transmit Power	100%
Routing	transmit Hower	100%
RIP	Channel	Auto Select 🔰 😒
BGP	Channel Bandwidth	Auto 20/40 MHz V
OSPF		
Bandwidth Management	Current Channel	Channel 13
NAT	Current Extension Channel	Channel 9
IGMP	Update Channel	Scan and Update
Objects	Update Channel	scan and update
LTE		Note: Execute a one-time channel optimization for this AP. This would result in wireless downtime for few minutes.
Wake on LAN	Updated Channel Result	
Notification Services	Opdated Channel Result	
RADIUS/ TACACS+	5GHz Radio	
Certificates	JGHZ RADIO	

Item Description						
Advanced Mode:ON/OFF	Click to show or hide the advanced settings for the Radio setting					
	2.4GHz Radio					
Enabled	Switch the toggle to enable/disable the RADIO settings.					
Mode	 Select the 802.11 mode allowed on the band. On the 2.4GHz band on ax models, the following wireless mode options are available: 11b Only 11g Only 11n Only (2.4 GHz) Mixed (11b+11g) Mixed (11b+11g+11n) Mixed (11b+11g+11n) Mixed (11b+11g+11n+11ax) 					
Transmit Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.					
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting " Auto Select ". The list of available channels varies depending on the locale for which the router is intended.					
Channel Bandwidth 20 MHz –Vigor Router will utilize 20 MHz channels for data transmission and reception between the router and wireles						

	 40 MHz – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations. Auto 20/40 MHz – Vigor Router will utilize either 20 MHz or 40 MHz for data transmission and reception depending on the number of AP nearby the router. 20MHz will be used when there are more than 10 wireless APs; otherwise 40MHz will be used. Selecting this setting ensures the best performance for data transit on networks with both 20 MHz and 40 MHz clients. 			
Current Channel	Displays current used channel number.			
Current Extension Channel	Displays current used extension channel number.			
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.			

5GHz Radio

Enabled	Switch the toggle to enable/disable the RADIO settings.
Mode	Select the 802.11 mode allowed on the band.
	On the 5GHz band on ax models, the following options are available:
	• 11a Only
	• 11n Only (5 GHz)
	• Mixed (11a+11n)
	• Mixed (11a+11n+11ac)
	• Mixed (11a+11n+11ac+11ax)
Transmit Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting " Auto Select ". The list of available channels varies depending on the local for which the router is intended.
Channel Bandwidth	20 MHz –Vigor Router will utilize 20 MHz for data transmission and reception between the router and wireless stations.
	40 MHz – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations.
	80 MHz –Vigor Router will utilize 80 MHz for data transmission and reception between the router and wireless stations.
	160 MHz – Vigor Router will utilize 160 MHz for data transmission and reception between the router and wireless stations.
Current Channel	Displays current used channel number.
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.				
	Band Ste	eering Settings				
5Ghz Client Minimum RSSI	If it is enabled, Vigor router 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 Vigor router, Vigor router will allow the client to connect to the 2.4GHz network.					
Options under the Adva	nced Mode					
Antenna	transmission via w	e attached with two antennas to have good data ireless connection. However, if you have only one please choose 1T1R.				
	4T4R	~				
	1T1R					
	2T2R					
	4T4R					
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2346.					
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.					
	Set the RTS threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2347.					
Country Code	Available for 2.4GF	-				
	Vigor router broadcasts country codes according to the 802.11d standard. However, some wireless stations will detect/scan access points looking for country codes to determine which country it is i and utilize channels appropriate to the country. The wireless clien might get confused if there are multiple access points in the vicini broadcasting different country codes. In such cases, it might be necessary to change the country code of the access point to ensur these clients can successfully establish a wireless connection.					
WMM Capable	 WMM stands for Wi-Fi Multimedia. It provides basic Quality of Service (QoS) by prioritizing traffic based on four access categories defined in the IEEE 802.11e standard. The access categories are AC_VO, AC_VI, AC_BE and AC_BK, which corresponds to traffic types of voice, video, best effort and low priority (background) data, respectively. To apply WMM parameters for wireless data transmission, please 					
		o enable the function.				
APSD Capable	power-saving mecl	ower-Save Delivery) is an enhancement over the nanisms supported by Wi-Fi networks. It allows Iffer 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. The default setting is Disable .
Airtime Fairness	Switch the toggle to enable/disable the function. With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.
	Environments that can benefit by applying airtime fairness:
	(1) Many wireless stations.
	(2) All stations mainly use download traffic.
	(3) The performance bottleneck is wireless connection.
Cancel	Discard current settings.
Apply	Save the current settings.

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

II-1-5-3 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 by enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

This page allows you to enable the roaming feature.

SearchQ	Configuration / Wireless LAN	3 Reset
and a second	SSID Radio Settings Roaming AP Discovery WPS WDS	
Device Menu	Assisted Client Roaming	
🖓 Dashboard	Assisted their Roaming	
🚊 Configuration	Enabled 802.11r	
Physical Interface	Note: 802.11r is not applicable with WPA3 Security Mode and may not compatible with some wireless clie	mis,
WAN		
LAN	802.11r Mode Over the DS Over the Ar	
DNS		
Wireless LAN	Assisted Roaming by Signal Strength (RSSI)	
Routing	Enabled	
RIP	Assisted Roaming Signal Strength Threshold - documing algorial range - documine Condumn, 85 dBm (Default: -85)	
BGP		
OSPF	Assist reaming when adjacent AP signal is better than (adjacent AP signal) (angle: 108 - 2083) 5 dB.(Default: 5)	
Bandwidth Management		
NAT		
IGMP		
Objects		
LTE		
Wake on LAN		
Notification Services		
RADIUS/ TACACS+		
Certificates	Cancel Apply	
19 H		

ltem	Description			
Assisted Client Roaming				
Enabled 802.11r	Switch the toggle to enable/disable the function of fast roaming to make Wireless clients switch between the hotspots fast and securely. There are two methods to run fast roaming.			

802.11r Mode	Over the DS - In response to the needs of 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 - In response to the needs of signal strength change, the client can communicate directly with the other AP using a fast roaming authentication algorithm (without requiring reauthentication at every AP).				
	Assisted Roaming by Signal Strength (RSSI)				
Enabled	Switch the toggle to enable/disable the function. When the link rate of the wireless station is too low or the signal received by the wireless station is too worse, Vigor router 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.				
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 Router/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 Vigor router, Vigor router 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 current settings.				
Apply	Save the current settings.				

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

II-1-5-4 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on 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 Vigor router.

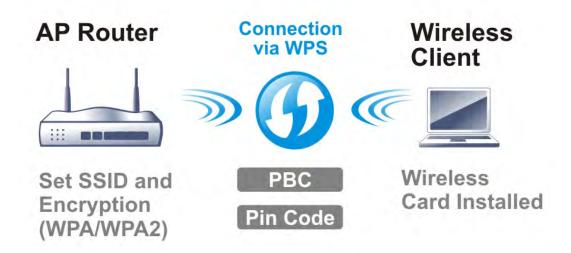
This page is used to scan the existence of the APs around. Please click **Scan** to discover all the nearby APs.

iearchQ	Configuration / Wire	less LAN					CRefres
	SSID Radio Settin	igs Roaming AP Discove	ery WPS WDS				
vice Menu	AP Discovery						
Dashboard	AP Discovery						
Configuration	Start AP Discovery	Scan					
Physical Interface		Moto Cramina	process would result in wireless dow	mitima for fast minut	er		
WAN		mile, acaming)	process would result in wreness due	interne for new minute	c.		
LAN							
DNS	Radio Information						
Witcless LAN							
Routing		2.4GHz	5GHz				
RIP	Mode	Mixed(11b+11g+11n+11ax)	Mixed(11a+11n+11ac+11ax)				
BGP	Current Channel		116				
OSPF	Current Channel	13	110				
Bandwidth Management	Channel Utilization	1%	1%				
NAT	Channel Width	20/40 MHz	160 MHz				
IGMP	Channel Width	20/40 MHz	160 MPIZ				
Objects							
LTE	Neighbor AP List						
Wake on LAN	0						
Notification Services	SSID BSS	SID Signal Strength (F	SSI) Band	Channel	Mode	Security	Encryption
RADIUS/ TACACS+							
Certificates							

ltem	Description
Start AP Discovery	Scan - It is used to discover all the nearby AP. The results will be shown on the box below this button.
Radio Information	Displays current information for 2.4GHz and 5GHz used by Vigor router.
Neighbor AP List	Displays all the nearby APs scanned by Vigor router.

II-1-5-5 WPS

WPS (Wi-Fi Protected Setup) provides an easy way to connect wireless to wireless access points and routers with WPA or WPA2 encryption.



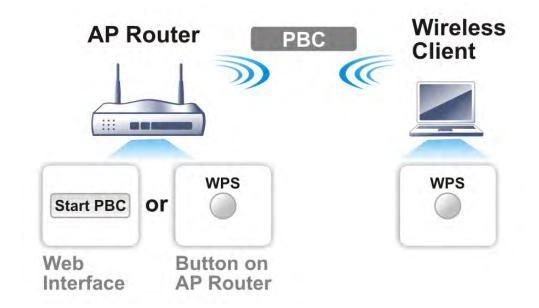
WPS works with wireless stations with WPA or WPA2 support. It does not work with WEP.

It is the simplest way to build connection between wireless network clients and vigor router. 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 router automatically.

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

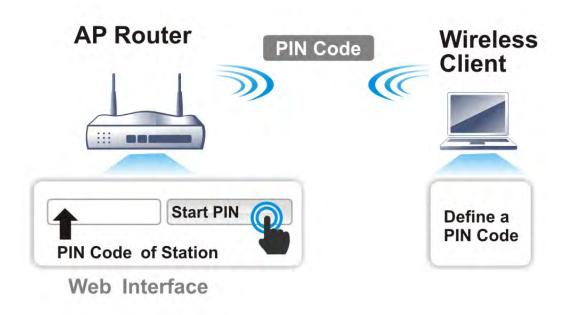
Using the PBC button

On the Vigor router, press and hold the WPS button on the front panel for 2 seconds, or click the **Start PBC** button on the **Configuration>>Wireless LAN>>WPS** page in the Web User Interface. On the wireless station (for example, a laptop computer), press the **WPS/Start PBC** button on the network card.



Using a PIN code

You may establish a wireless connection by entering a PIN code generated by a wireless client that supports WPS.



Below shows **Configuration>>Wireless LAN>>WPS** web page:

Search Q	Configuration / Wireless LAN		Reset C Refresh
	SSID Radio Settings Rd	paming AP Discovery WPS WDS	
Device Menu	WPS		
 Dashboard 			
E Configuration	Enabled		
Physical Interface	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	Note: only WPA2/WPA Personal security mode support WPS.	
WAN			
LAN	Band	2.4GHz 5GHz	
DNS	2.4GHz SSID	DrayTek-86FAB8	
Wireless FAN			
Routing	Method 1 : WPS Button		
RIP	method 1. Wr 5 button		
BGP	Enable WPS	Start PBC	
OSPF			
Bandwidth Management			
NAT	Method 2 : Using PIN Code		
IGMP	method 2 . Osing Pile Code		
Objects	Generate PIN code from	Chere	
LTE	Client PIN Code	73156788	
Wake on LAN	Client PIN Cobe	73126/88	1
Notification Services		Connect	
RADIUS/ TACACS+			
Certificates	Cancel Apply		

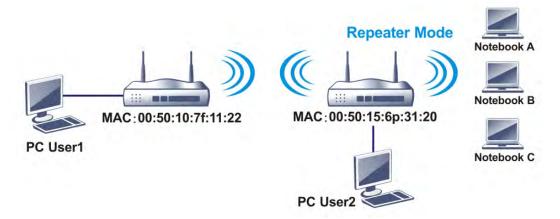
ltem	Description
Reset	Click to reset WPS with the default value.
Refresh	Click to refresh current page.
Enabled	Switch the toggle to enable/disable the function.
Band	Select the band (2.4GHz/5GHz) for this function.
2.4GHz SSID / 5GHz SSID	Displays the SSID used for 2.4GHz/5GHz.
Method 1: WPS Button	Enable WPS – Switch the toggle to enable/disable the function.
	Start PBC –Click it to invoke the Push-Button style WPS setup procedure. The router will wait for about 2 minutes for WPS connection requests from wireless clients. The ACT LED and WLAN LED on the router will blink fast simultaneously when WPS is in progress and will return to normal condition after two minutes.
Method 2: Using PIN	Enter a PIN code, and click the Connect button.
Code	Generate PIN code from – At present, only Client is available.
	Client PIN Code – Enter a PIN code.
	Connect – Click it to make a connection. The ACT LED and WLAN LED on the router will blink fast simultaneously when WPS is in progress, for up to 2 minutes or until a successful WPS connection from a wireless client has been established.
Connection Status	Displays the connection status after clicking Connect or Start PBC .
Cancel	Discard current settings.
Apply	Save the current settings.

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

II-1-5-6 WDS

Wireless Distribution System (WDS) is a protocol for linking access points (AP) wirelessly. Vigor C410/C510ax WDS only supports Repeater mode.

• **Repeater mode**, which extends the coverage range of a WLAN.



Below shows **Configuration>>Wireless LAN>>WDS** web page:

SearchQ	Configuration / Wireless LAN SSID Radio Settings Ro	aming AP Discovery V	VPS WDS			3 Reset C Refresh
Device Menu						
 Dashboard 	WDS					
🚎 Conliguration 🐰	Enabled					
Physical Interface		-				
WAN	Mode	HE (11ax)	Ŷ			
LAN	2.4GHz WDS List					¥
DNS						
Windess LAN-	+ Add					Maur é
Routing	Peer MAC Address ()		Enabled	Security	Password ①	
RIP						
BGP						
OSPF	5GHz WDS List					~
Bandwidth Management	SGHZ WUS LISE					~
NAT						
IGMP	+ Add					Max: 4
Objects	Peer MAC Address ()		Enabled	Security	Password ①	
LTE			N/6 RECORD EF			
Wake on LAN						
Notification Services						
RADIUS/ TACACS+						
Certificates	Cancel Apply					

ltem	Description			
Reset	Click to reset WPS with the default value.			
Refresh	Click to refresh current page.			
Enabled	Switch the toggle to enable/disable the WDS function.			
Mode	 Select the physical mode for this WDS setting. HE(11ax) VHT(11ac) HTMIX(11n) 			
2.4GHz/5GHz WDS List	+Add – Click to create WDS list (up to 4). Peer MAC Address – Enter the MAC address of the WDS peer.			

	Enabled – Switch the toggle to enable/disable this WDS link.
	Security – Select the encryption method of this WDS link.
	• Open - Security is disabled.
	• TKIP – Enter a string.
	• AES - Enter a string.
	Password – Enter the key of the WDS link when Security is TKIP or AES. It should be a string with 8 ~ 63 ASCII characters.
	Delete – Remove current entry.
Cancel	Discard current settings.
Apply	Save the current settings.

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

II-1-6 Routing

Through the IP address and interface configuration, a route policy can be used to configure any routing rules to fit actual requests.

The packets will be directed to the specified interface if they match one of the routing policies.

The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

II-1-6-1 Route Policy

Route Policy (also well known as PBR, policy-based routing) is a feature where you may need to get a strategy for routing. The packets will be directed to the specified interface if they match one of the policies. You can setup route policies in various reasons such as load balance, security, routing decision, and etc.

Through protocol, IP address, port number and interface configuration, Route Policy can be used to configure any routing rules to fit actual request.

	Configuration / Routing						3	Reset CRefresh
evice Menu	Route Policy IPv4 Static R	oute IPv6 Static Ro	ute					
	Route Policy							
ე Dashboard								
	+ Add						Search	Masc
Physical Interface	Policy Name	Enabled	Source	Destination	Protocol	Priority	Primary Path	Option
WAN								
LAN								
ONS								
Wireless LAN								
RIP								
BGP								
OSPF								
Bandwidth Management								
NAT								
IGMP								
Objects								
Wake on LAN								
Notification Services								
RADIUS/ TACACS+								
Certificates								

To add a new IPv4 route policy, click the **+Add** link to get the following page.

Primary Path WAN/Virtual WAN Primary Path WAN/Virtual WAN Primary Path WAN + Add Interface Interface IP Gateway Gateway IP Force NAT/Routing			×
Schedule Nwoys Dn Scheduled On Criteria Source Any Destination Any Protocol Any Interface Selection Primary Path Primary Path WAN/Virtual WAN Any Max: 1 Interface Interface IP Gateway IP Force NAT/Routing	Policy Name ()		
Criteria Source Any Destination Any Protocol Any Protocol Any	Enabled		
Source Any Destination Any Protocol Any Interface Selection Primary Path Primary Path Primary Path WAN/Virtual WAN Any Max: 1 Interface Interface IP Gateway Gateway IP Force NAT/Routing	Schedule	Always On Scheduled On	
Destination Any Protocol Any Protocol Any Primary Path Primary Path Primary Path WAN/Virtual WAN Primary Path WAN Add Max: 1 Interface Interface IP Gateway Gateway IP Force NAT/Routing	Criteria		
Protocol Any Interface Selection Primary Path Primary Path WAN/Virtual WAN Any Max: 1 Interface Interface IP Gateway Gateway IP Force NAT/Routing	Source	Any \checkmark	
Interface Selection Primary Path Primary Path WAN/Virtual WAN Primary Path WAN + Add Max: 1 Interface Interface IP Gateway Gateway IP Force NAT/Routing	Destination	Any 🗸	
Primary Path WAN/Virtual WAN Primary Path WAN/Virtual WAN Primary Path WAN + Add Interface Interface IP Gateway Gateway IP Force NAT/Routing	Protocol	Any 🗸	
Primary Path WAN Primary Path WAN +Add Max: 1 Interface Interface IP Gateway Gateway IP Force NAT/Routing	Interface Selection		~
Primary Path WAN + Add Max: 1 Interface Interface IP Gateway Gateway IP Force NAT/Routing	Primary Path		
Interface Interface IP Gateway Gateway IP Force NAT/Routing	Primary Path	WAN/Virtual WAN \sim	
	Primary Path WAN	+ Add Max: 1	
		Interface Interface IP Gateway Gateway IP Force NAT/Routing	

ltem	Description			
Policy Name	Enter a name as the routing profile name.			
Enabled	Switch the toggle to enable/disable the profile.			
Schedule	Determine the valid time for the routing profile.			
	Always On – The routing profile will be valid all the time if it is enabled			
	Scheduled On – The routing profile will be valid based on the time schedule specified here.			
	Criteria			
Source / Destination	Select the type of IP addresses to which this rule is to be applied.			
	• Any - This policy applies to all source/destination IP addresses.			
	• IPv4 Address - This policy applies to the specified range of source IP addresses.			
	• IPv4 Subnet - This policy applies to source IP addresses defined by the specified network IP address and subnet mask.			
	• IP Object - This policy applies to a preconfigured IP object.			
	• IP Group - This policy applies to a preconfigured IP group.			
Source / Destination	It is available when Source / Destination is set as IPv4 Address .			
IPv4 Address	+Add – Click to have new entries for setting IPv4 Address Start and End.			
	IPv4 Address Start / End – Enter two IPv4 address(s), one for start and one for end.			
	Delete – Click to remove current entries.			
Source / Destination	It is available when Source / Destination is set as IPv4 Subnet .			
IPv4 Subnet Address	+Add – Click to have new entries for setting IPv4 subnet.			
	IPv4 Address – Enter an IP address.			
	Subnet Mask - Use the drop down list to choose a suitable mask for			

 available when Source / Destination is set as IP Object. d – Click it to create a new object (containing different IP resses). Up to 12 objects can be created. ct Object – Check to select an object or objects. available when Source / Destination is set as IP Group. d –Click it to create a new group (containing different IP objects).
–Click it to create a new group (containing different IP objects).
o 12 groups can be specified here. c t Group - Check to select a group or groups.
 bese a proper protocol for the WAN interface. Any kind of protocol will be used for the WAN interface. ice Object – The protocol used will be determined by the service ct. Service Type Object – Click +Add to create a new object (containing different protocols). Up to 12 objects can be created. UDP – Select TCP/UDP for the WAN interface. Specify Source Port – Switch the toggle to enable the setting of Source Port. Source Port / Destination Port – Set the range (1 to 65535). Same as TCP/UDP.

Interface Selection

Primary Path Specify the interface that the traffic described by this rule is to be directed. If the packet traffic is matched with the criteria set above, it will be sent to the designated interface and gateway. **Primary Path** – Packets will be transferred to the interface chosen here. Select an interface from the list (WAN/LAN: A WAN or LAN interface; VPN: A Virtual Private Network). WAN/Virtual WAN WAN/Virtual WAN VPN LAN **Primary Path WAN** – It is available when the WAN/Virtual WAN is selected. +Add – Click +Add to create the primary path. Select WAN interface and the corresponding IP address. Packets match with the criteria will be transferred to the interface chosen here. Select an interface from the list. Specify the gateway (using the default device or customized a gateway IP). Then determine which mechanism (Force NAT/Routing) that the router will use to forward the packet to WAN. Primary Path VPN - It is available when the VPN is selected. +Add - Click +Add to create a new VPN path. Use the drop-down list to select a VPN profile.

	 Primary Path LAN - It is available when the LAN is selected. +Add – Click +Add to create a new VPN path. Use the drop-down list to select a VPN profile. 				
Secondary Path	Disabled – Disable the function settings for the secondary path.				
	Disabled				
	WAN/Virtual WAN				
	VPN				
	LAN				
	Disabled				
	Secondary Path WAN – It is available when the WAN/Virtual WAN is se for Secondary Path.				
	+Add – Click +Add to create the secondary path by specifying WAN settings.				
	Secondary Path VPN - It is available when the VPN is set for Secondar Path.				
	+Add – Click +Add to create a new VPN path.				
	Secondary Path LAN - It is available when the LAN is set for Secondar Path.				
	+Add – Click +Add to create a new LAN path.				
	Path or the Secondary Path could not be used for directing the traffic Disabled –Disable the function settings for the Last Resort Path.				
	• Gateway – Select Default or Customize.				
	 Gateway IP Address – Enter the IP address of the gateway if Customize is selected. 				
	 Force NAT/Routing – Determine which mechanism (Force NAT/Routing) that the router will use to forward the packet to WAN. 				
	WAN/Virtual WAN – Specify a WAN interface or a virtual WAN interface for the last resort path.				
	 Last Resort Path WAN – Click +Add. Then select a WAN interface, the IP address (WAN), the gateway IP address(LAN) and the pack forwarding mechanism. 				

	VPN –Specify a VPN profile for the last resort path.
	• Last Resort Path VPN – Click +Add. Select one of the VPN profiles.
	LAN – Specify a LAN interface for the last resort path.
	 Last Resort Path LAN – Click +Add. Then select a LAN interface with an IP address (gateway) and the packet forwarding mechanism.
More settings	
Priority	Specifies the priority of the rule about other rules.
	Normal – The routing profile does not affect other routes on the routing table.
	High – The routing profile will override the VPN routes only. However, it will not affect LAN/Static route.
	Top – The routing profile will override VPN and LAN/Static route.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

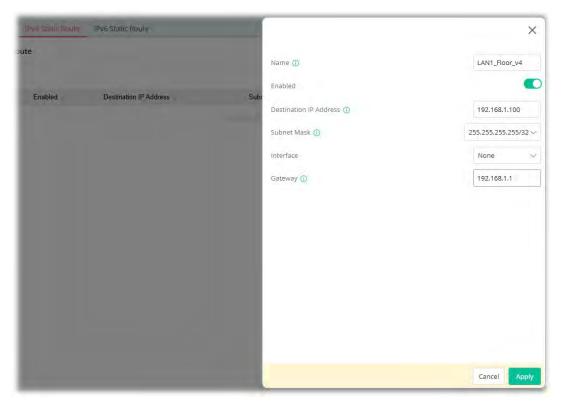
After finishing this web page configuration, please click **Apply** to save the settings.

II-1-6-2 IPv4 Static Route

Static routing is an alternative to dynamic routing. It is a process that the system network administrator can configure network routers with all the required information for packet forwarding.

Search	Configuration	/ Routing					3 Reset
		IPv4 Static Route	IPv6 Static Route				
evice Menu	IPv4 Static R	nute	-				
Dashboard	IF V4 Static R	Jule					
	+ Add					Search	Max:
Physical Interface	Name	Enabled	Destination IP Address	Subnet Mask	Interface	Gateway	Option
WAN							
LAN							
DNS							
Wireless LAN							
RIP							
BGP							
OSPF							
Bandwidth Management							
NAT							
IGMP							
Objects							
Wake on LAN							
Notification Services							
RADIUS/ TACACS+							
Certificates							

To add a new IPv4 static route, click the **+Add** link to get the following page.



ltem	Description		
NameEnter a name as the profile name.			
Enabled	Switch the toggle to enable or disable the function.		
Destination IP Address	Enter the IP address as the destination IP address.		
Subnet Mask	Select a subnet mask of this static route.		
Interface	Use the drop-down list to specify an interface for this static route		
Gateway Enter an IP address as the gateway.			
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.

II-1-6-3 IPv6 Static Route

Static routing is an alternative to dynamic routing. It is a process that the system network administrator can configure network routers with all the required information for packet forwarding.

iearch Q	Configuration	/ Routing					⁽¹⁾ Reset
	Route Policy	IPv4 Static Route	IPv6 Static Route				
wice Menu	ID & DUILL D						
Dashboard	IPv6 Static Ro	oute					
	+ Add					Search	Мах: 4
Physical Interface	Name	Enabled	Destination	Prefix Length	Gateway IPv6 Address	Interface	Option
WAN							
LAN							
DNS							
Wireless LAN							
RIP							
BGP							
OSPF							
Bandwidth Management							
NAT							
IGMP							
Objects							
Wake on LAN							
Notification Services							
RADIUS/ TACACS+							
Certificates							

To add a new IPv6 static route, click the **+Add** link to get the following page.

olicy IPv4 Static Route	IPv6 Static Route			×
atic Route			Name 🕕	LAN1_Floor_v6
Enabled	Destination	Prefix Length	Enabled	C
			Destination ①	abcd:1234::
			Prefix Length ①	64
			Gateway IPv6 Address 🕡	abcd:5566::
			Interface	None 🗸 🗸
				Cancel Apply

ltem	Description		
Name	Enter a name as the profile name.		
Enabled	Switch the toggle to enable or disable the function.		
Destination	Enter the IPv6 address as the destination IP address.		
Prefix Length	Enter the fixed value for prefix length.		
Gateway IPv6 Address	Enter an IPv6 address as the gateway.		
Interface	Use the drop-down list to specify an interface for this static route.		

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.

II-1-7 RIP

The Routing Information Protocol (RIP) and the RIPng (RIP next generation) are the most popular interior routing protocols. The difference is that the RIPng (RIP next generation) is based on the IPv6 address, but offers the same functions and benefits as IPv4 RIP v2.

If enabling the RIP feature, the router will attempt to exchange routing information with neighboring routers using the Routing Information Protocol.

II-1-7-1 General Setup

There are two versions of RIP available. This page offers comprehensive settings for each of these versions.

Search Q	Configuration / RIP		() Res
	General Setup RIP Networ	k RIPng Network	
evice Menu	General Setup		
ව Dashboard	General Setup		
	Enabled		
Physical Interface	RIP Version	V1 V2	
WAN			
LAN	Timers		
DNS	Timers		
Wireless LAN	Update Timer (Secolida) 🕥	30	
Routing	Timeout Timer (Seconds)	180	
	timeout timer (seconda) ()	150	
BGP	Garbage Timer (Seconds)	120	
OSPF			
Bandwidth Management	Redistribute		
NAT	Construction of the		
IGMP	Connected	0	
Objects	Static	0.0	
LTE	BGP		
Wake on LAN	BAL.	0	
Notification Services	OSPE	0	
RADIUS/ TACACS+	RIPng		
Certificates	Cancel Apply		

ltem	Description				
General Setup					
Enabled	When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.				
RIP Version	Specify the version number (V1/V2) for RIP protocol.				
Update Timer	Enter a value as the update timer. When the time is up, the Vigor router will send a message containing the complete routing table to all neighboring routers for exchanging the routing information.				
Timeout Timer	The routing information will be valid (but not removed) till the time expiration set in this field.				

	The information will be kept in the routing table temporarily. At the same time, the neighbors will be notified that the route has been dropped.
Garbage Timer	The route will be removed from the routing table upon the expiration set in Garbage Timer.
Connected	Switch the toggle to enable/disable the function.
	All Networks – Apply the RIP profile to all the LAN interfaces.
	Exclude NAT Networks - Apply the RIP profile to all the LAN interfaces except for NAT network.
Static	Switch the toggle to enable (apply the static route to the RIP profile) o disable the function.
BGP	Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function.
OSPF	Switch the toggle to enable (allow dynamically route traffic based on information learned from the OSPF protocol) or disable the function.
	RIPng
Enabled	Switch the toggle to enable/disable the function of Routing Information Protocol next generation (RIPng).
Update Timer	Enter a value as the update timer.
	When the time is up, the Vigor router will send a message containing the complete routing table to all neighboring routers for exchanging the routing information.
Timeout Timer	The routing information will be valid (but not removed) till the time expiration set in this field.
	The information will be kept in the routing table temporarily. At the same time, the neighbors will be notified that the route has been dropped.
Garbage Timer	The route will be removed from the routing table upon the expiration set in Garbage Timer.
Connected	Switch the toggle to enable (apply the RIPng settings to all the LAN interfaces) or disable the function.
Static	Switch the toggle to enable (apply the static route to the RIP profile) o disable the function.
BGP	Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function.
OSPF	Switch the toggle to enable (allow dynamically route traffic based on information learned from the OSPF protocol) or disable the function.
Cancel	Discard current settings.
Apply	Save the current settings.

II-1-7-2 RIP Network

This page allows you to configure up to eight neighboring routers for exchanging the routing information with the local router (Vigor C410/C510).

Search	q	Configuration / I	NP					1 Reset
Provide Law Street Stre		General Setup	RIP Network	RIPng Network				
Device Menu	1	RIP Network						
(?) Dashboard		RIP Network						
≘ Continuestion-		+ Add						Mars II
Physical Interface		Interface		,	uthentication		Key ID	Option
WAN								
LAN								
DNS								
Wireless LAN								
Routing								
BGP								
OSPF								
Bandwidth Managemer	nt							
NAT								
IGMP								
Objects								
LTE								
Wake on LAN								
Notification Services								
RADIUS/ TACACS+								
Certificates								
1								

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

neral Setup RIP Network	RIPng Network		×
P Network		Interface	[WAN] WAN1 (Wired WAN) ~
Add			Luna .
terface	Authentication	Authentication	MD5 ~
		Password ()	
		Key ID 🕕	16

Available settings are explained as follows:

ltem	Description
Interface	Select a LAN / WAN interface to apply the settings configured for this profile.
Authentication	Select the authentication mechanism for this profile. Disabled – No authentication mechanism will be used.
	Plain-Text – Only password will be used for authentication.
	• Password –Enter characters as the password for MD5

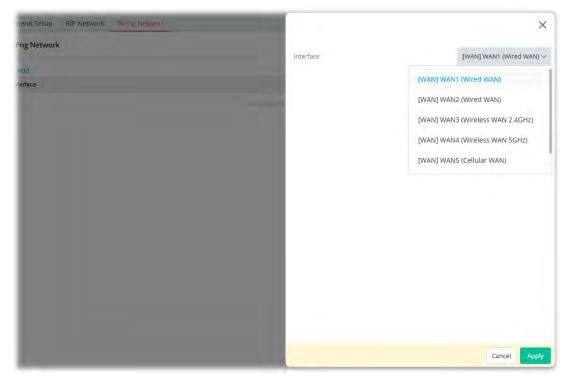
	authentication.
	MD5 – Use MD5 authentication.
	 Password – Enter characters as the password for MD5 authentication.
	 Key ID – Enter a number (0~255). The ID will help Vigor router to be identified in an autonomous system.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-7-3 RIPng Network

This page allows you to configure up to eight interfaces (WAN or LAN) for exchanging the routing information with the local router (Vigor C410/C510) based on IPv6 address(es).

search Q	Configuration / RIP	() Rese
	General Setup RIP Network RIPng Network	
evice Menu	RIPng Network	
Dashboard	In 18 Issuer	
	+ Add	Max
Physical Interface	Interface	Option
WAN	Longerou Langerou La	
LAN		
DNS		
Wireless LAN		
Routing		
nip.		
BGP		
OSPF		
Bandwidth Management		
NAT		
IGMP		
Objects		
LTE		
Wake on LAN		
Notification Services		
RADIUS/ TACACS+		
Certificates		
certificates		

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



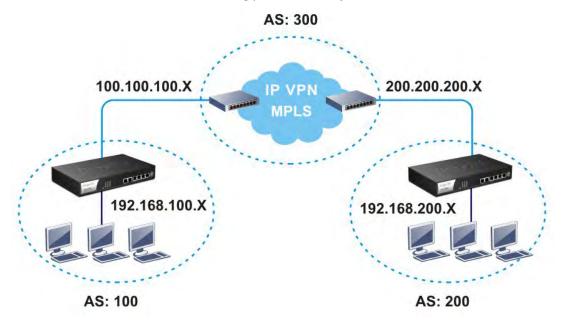
ltem	Description
Interface	Select a LAN / WAN interface to apply the settings configured for this profile.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-8 BGP

Border Gateway Protocol (BGP) is a standardized protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.

The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the "neighbor" of other BGP routers. Define the IPv4/IPv6 address, AS number for the router is essential for TCP connection of BGP routing information exchange.

AS, the abbreviation of Autonomous System, is a group interconnected with multiple IPv4/IPv6 addresses. Each AS shall be assigned with one AS number (ASN). The ASN is a unique identifier for AS to distinguish each network group in the whole interconnected network. It can be operated by one or several ISPs and follows the routing policies made by ISP.



II-1-8-1 General Setup

Set general settings for for local router and neighboring routers.

	Configuration / BGP		1 Res
	General Setup IPv4	Neighbors IPv4 Networks IPv6 Neighbors IPv6 Networks	
evice Menu	General Setup		
Dashboard	General Secop		
	Enabled		
Physical Interface	Local AS ()		
WAN	1000 FD Q		
LAN	Router ID 🕕		
DNS			
Wireless LAN	IPv4 Redistribute		
Routing			
RIP	Connected	0	
	Static	0	
OSPF	RIF		
Bandwidth Management			
NAT	OSPF	0.0	
IGMP			
Objects	IPv6 Redistribute		
	Connected	09	
Wake on LAN	Commised		
Notification Services	Static	0	
RADIUS/ TACACS+	RIP	- (The	
Certificates	Cancel Apply		

ltem	Description
Enabled	Switch the toggle to enable/disable the basic BGP function for local router.
Local AS	Set the AS number for local router.
Router ID	Specify the LAN subnet for the router.
	IPv4 Redistribute
Connected	All Networks – Apply the BGP profile to all the LAN interfaces.
	Exclude NAT Networks - Apply the BGP profile to all the LAN interfaces except for NAT network.
Static	Switch the toggle to enable or disable the function (apply the static route to the BGP profile).
RIP	Switch the toggle to enable or disable the function (apply the RIP function to the BGP profile).
OSPF	Switch the toggle to enable or disable the function (apply the OSPF function to the BGP profile).
	IPv6 Redistribute
Connected	Switch the toggle to enable (apply the BGP profile to all the LAN interfaces) or disable the function.
Static	Switch the toggle to enable or disable the function (apply the static route to the BGP profile).
RIP	Switch the toggle to enable or disable the function (allow dynamically route traffic based on information learned from the RIP protocol).
OSPF	Switch the toggle to enable or disable the function (allow dynamically route traffic based on information learned from the OSPF protocol).
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-8-2 IPv4 Neighbors

Set general settings for the neighboring routers (based on IPv4 address).

	Configuration / BGP				@Reset C Refresh
	General Setup IPV4 Neighbor	IPv4 Networks IPv6 Neighb	ors IPv6 Networks		
Device Menu	IPv4 Neighbors				
Dashboard	IPV4 Neighbors				
	+ Add				Max
Physical Interface	Remote AS Number	IPv4 Address	Authentication	Connection Status	Option
WAN					
LAN					
DNS					
Wireless LAN					
Routing					
RIP					
OSPF					
Bandwidth Management					
NAT					
IGMP					
Objects					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates					

To add a new IPv4 neighbors profile (up to 8), click the **+Add** link to get the following page.

up IFv4 Neighbors	IPv4 Networks IPv6 Neighbors	IPv6 Networ		×
bors			Remote AS Number 🕥	10021002
n Number	IPv4 Address	Authentic	IPv4 Address	192.168.1.55
			Authentication	MD5 \sim
			Password ①	••••••
				Cancel Apply

ltem	Description
Remote AS Number	Specify the AS Number for neighboring router.
IPv4 Address	Enter the IP address specified for the neighboring profile.
Authentication	Select the authentication mechanism for this profile. Disabled – No authentication mechanism will be used.
	MD5 – Use MD5 authentication.
	• Password – Enter characters as the password for MD5 authentication.

Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-8-3 IPv4 Networks

This page allows you to configure up to eight neighboring networks for exchanging the routing information with the local router (Vigor C410/C510). The IP address defined on this page will be used to declare which network will participate in the RIP protocol.

search Q	Configuration / E	BGP					() Reset
	General Setup	IPv4 Neighbors	IPv4 Networks	IPv6 Neighbors	IPv6 Networks		
Device Menu	IPv4 Networks						
 Dashboard 	in terrection is						
🗧 Cardiguration	+ Add						Max: 8
Physical Interface	IPv4 Address				Subnet Mask	Op	tion
WAN					- All- Helmonate Anostration		
LAN							
DNS							
Wireless LAN							
Routing							
RIP							
-NOP1							
OSPF							
Bandwidth Management							
NAT							
IGMP							
Objects							
LTE							
Wake on LAN							
Notification Services							
RADIUS/ TACACS+							
Certificates							

To add a new IPv4 networks profile (up to 8), click the **+Add** link to get the following page.

General Setup	IPv4 Neighbors	IPv4 Networks	IPv6 Neighbors	IPv6 Network		×
IPv4 Networks					IPv4 Address	192.168.1.55
+ Add					Subnet Mask	255.255.255.0/24 ~
IPv4 Address				Subnet M		
				10 /050001		
						Cancel Apply
						concer 1449

Available settings are explained as follows:

ltem	Description
IPv4 Address	Enter the IPv4 address of a neighboring network (following CIDR format).
	Vigor router (e.g., 2136 series) will exchange routing information (RIP info) with the specified network.
Subnet Mask	Select the mask value for the IPv4 address specified above.

Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-8-4 IPv6 Neighbors

Set general settings for local router and neighboring routers (based on IPv6 address).

Search Q	Configuration / BGP				TReset CRefresh
	General Setup IPv4 Neighbor	IPvd Networks IPv6 Neighb	IPv6 Networks		
Device Menu	IPv6 Neighbors				
Dashboard	IPV0 Neighbors				
	+ Add				Max: 8
Physical Interface	Remote AS Number	IPv6 Address	Authentication	Connection Status	Option
WAN					
LAN					
DNS					
Wireless LAN					
Routing					
RIP					
OSPE					
Bandwidth Management					
NAT					
IGMP					
Objects					
LTE					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates					

To add a new IPv6 neighbors profile, click the **+Add** link to get the following page.

Pv6 Neighbors			Remote AS Number 🕡	10021002	
+ Add			IPv6 Address	2001:0db8:85a3:0000	:0000:8a2
Remote AS Number	IPv6 Address	Authentic			
		-	Authentication	MD5	
			Password ()		<

ltem	Description
Remote AS Number	Specify the AS Number for neighboring router.

IPv6 Address	Enter the IPv6 address of a neighboring router.
Authentication	 Select the authentication mechanism for this profile. Disabled – No authentication mechanism will be used. MD5 – Use MD5 authentication. Password – Enter characters as the password for MD5 authentication.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-8-5 IPv6 Networks

This page allows you to configure up to eight neighboring networks for exchanging the routing information with the local router (Vigor C410/C510). The IPv6 address defined on this page will be used to declare which network will participate in the RIPng protocol.

	Q Configuration / BGP	() Rese
	General Setup IPv4 Neighbors IPv4 Networks IPv6 Neighbors IPv6 Networks	
ivice Menu		
Dashboard	IPv6 Networks	
	+ Add	Max
Physical interface	IPv6 Address Prefix Length	Option
WAN	Solid Line stream	
LAN		
DNS		
Wireless LAN		
Routing		
RIP		
OSPF		
Bandwidth Managemer	h.	
NAT		
IGMP		
Objects		
Wake on LAN		
Notification Services		
RADIUS/ TACACS+		
Certificates		

To add a new IPv6 networks profile, click the **+Add** link to get the following page.

eneral Setup	IPv4 Neighbors	IPv4 Networks	IPv6 Neighbors	IPv6 Networ		×
Pv6 Networks					IPv6 Address	2001:0db8:85a3:0000:0000:8a2e
- Add					Prefix Length	125
IPv6 Address				Prefix Len		
				And in case of the		
						Cancel Apply

ltem	Description			
IPv6 Address	Enter the IPv6 address of a neighboring network (following CIDR format).			
	Vigor router will exchange routing information (RIPng info) with the specified network.			
Prefix Length	Enter the IPv6 prefix length for the IPv6 address.			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

II-1-9 OSPF

OSPF(Open Shortest Path First), running within the AS, is a routing protocol based on IP protocol. It uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange. Vigor router supports up to OSPF version 2(for IPv4) and OSPF version 3(for IPv6).

The Autonomous System (AS) used in OSPF can be divided into several **areas**. Usually, Area 0 will be used as OSPF backbone which distributing the routing information among areas.

When you need faster convergence than distance vector, want to support much larger networks or want to have less susceptible to bad routing information, you can enable OSPF feature to fit your request. Note that both routers must support OSPF function at the same time to build the OSPF connection.

II-1-9-1 General Setup

This page allows you to configure general settings for OSPFv2 (IPv4) and/or OSPFv3 (Ipv6) profile.

Search Q	Configuration / OSPF		DRes
	General Setup OSPPv2 I	Networks OSPFv3 Networks	
evice Menu	General Setup		
Dashboard	General Setup		
	Enabled		
Physical Interface	Router ID ()		
WAN	invalue to to		
LAN	OSPF Profile		
DNS	OSFFFFone		
Wireless LAN	2.1.22.22		
Routing	Redistribute		
RIP	Connected		
BGP			
		All Networks, Exclude NAT Networks	
Bandwidth Management	Static	0	
NAT	RIP		
IGMP	KIP	30	
Objects	BGP	0	
LTE	OSPFv3		1.1
Wake on LAN			
Notification Services	Enabled	0	
RADIUS/ TACACS+			
Certificates	Cancel Apply		

ltem	Description				
General Setup					
Enabled	Switch the toggle to enable/disable the OSPFv2 function.				
Router ID	Specify the IPv4 address of the Vigor router for routing and neighbor discovery.				
	Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified, then an IP address of the active interface will be used by system automatically.				
Connected	All Networks – Apply the OSPF profile to all the LAN interfaces. Exclude NAT Networks - Apply the OSPF profile to all the LAN interfaces except for NAT network.				
Static	Switch the toggle to apply the static route to the OSPF profile.				
RIP	Switch the toggle to enable (allow dynamically route traffic based on				

	information learned from the RIP protocol) or disable the function.
BGP	Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function.
	OSPFv3
Enabled	Switch the toggle to enable/disable the OSPFv3 function.
Router ID	Specify the IPv6 address of the Vigor router for routing and neighbor discovery.
	Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified, then an IP address of the active interface will be used by system automatically.
Connected	Switch the toggle to enable (apply the OSPFv3 settings to all the LAN interfaces) or disable the function.
Static	Switch the toggle to enable (apply the static route to the OSPFv3 profile) or disable the function.
RIP	Switch the toggle to enable (allow dynamically route traffic based on information learned from the RIP protocol) or disable the function.
BGP	Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-9-2 OSPFv2 Networks

This page allows you to set neighbors (by Area ID) for OSPFv2 profile.

Search Q	Configuration / OSI	PF				TReset CRefresh
	General Setup	OSPEVZ Networks OS	PFv3 Networks			
Device Menu	ores and a					
Dashboard	OSPFv2 Networks					
	+ Add					Maxi
Physical Interface	Interface	Area ID	Authentication	Key ID	Neighborhoods	Option
WAN						
LAN						
DNS						
Wireless LAN						
Routing						
RIP						
BGP						
Bandwidth Management						
NAT						
IGMP						
Objects						
LTE						
Wake on LAN						
Notification Services						
RADIUS/ TACACS+						
Certificates						

To add a new OSPFv2 networks profile, click the **+Add** link to get the following page.

	OSPEV2 Networks OS	SPEv3 Networks		×
DSPFv2 Network	S		Interface	[WAN] WAN2 (Wired WAN) $$
+ Add Interface	Area ID	Authentication	Area ID 🕦	30
			Authentication	MD5 V
			Password ()	
			Key ID 🕕	16

ltem	Description
Interface	Select a LAN / WAN interface to apply the settings configured for this profile.
Area ID	An AS will be divided into several areas. Each area must be assigned with a dedicated number.
	Please enter a number or IPv4 address as the area ID.
Authentication	Select the authentication mechanism for this profile.
	Disabled – No authentication mechanism will be used.
	Plain-Text – Only password will be used for authentication.
	• Password –Enter characters as the password for MD5 authentication.
	MD5 – Use MD5 authentication.
	• Password – Enter characters as the password for MD5 authentication.
	 Key ID – Enter a number (0~255). The ID will help Vigor router to be identified in an autonomous system.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-9-3 OSPFv3 Networks

	Configuration / OS					③Reset C Refres
	General Setup	OSPFv2 Networks OS	PPv3 Networks			
Device Menu	OSPFv3 Network	s				
Dashboard						
	+ Add					Max
Physical Interface	Interface	Area ID	Authentication	Key ID	Neighborhoods	Option
WAN						
LAN						
DNS						
Wireless LAN						
Routing						
RIP						
BGP						
Bandwidth Management						
NAT						
IGMP						
Objects						
Wake on LAN						
Notification Services						
RADIUS/ TACACS+						
Certificates						

This page allows you to set neighbors for OSPFv3 profile.

To add a new OSPFv3 networks profile, click the **+Add** link to get the following page.

		PFv3 Networks			×
OSPFv3 Networks					
+ Add				Interface	[WAN] WAN1 (Wired WAN) \sim
Interface	Area ID	Authentication	_	Area ID 🕕	40
			anto ant	Authentication	HMAC-SHA-256 V
				Password ()	
				Key ID 🕡	18

Available settings are explained as follows:

ltem	Description
Interface	Select a LAN / WAN interface to apply the settings configured for this profile.
Area ID	An AS will be divided into several areas. Each area must be assigned with a dedicated number.

	Please enter a number or IPv6 address as the area ID.
Authentication	Select the authentication mechanism for this profile.
	Disabled – No authentication mechanism will be used.
	Plain-Text – Only password will be used for authentication.
	• Password –Enter characters as the password for MD5 authentication.
	MD5 – Use MD5 authentication.
	• Password – Enter characters as the password for MD5 authentication.
	 Key ID – Enter a number (0~255). The ID will help Vigor router to be identified in an autonomous system.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-10 Bandwidth Management

When LAN clients share a common public IP address by means of Network Address Translation (NAT), the router must track NAT sessions so that traffic to and from the WAN can reach the intended destinations. There is an finite number of sessions that can be tracked by the router, and by setting session limits will ensure that the router does not run out of resources. This is especially important when P2P applications are used. P2P applications, such as BitTorrent, that attempt to simultaneously establish connections to as many WAN hosts as possible.

II-1-10-1 Traffic Shaping Policy

This page allows you to configure the session limits and QoS settings.

Search	Q	Configuration /	Bandwidth Manag	ement					(1) Reset
	-	Traffic shaping	Policy Bandwid	th Limit QoS Setup	App QoS Del	ault Policy			
Device Menu		Traffic Shapin	a Policy						
🝘 Dashboard		Tranic Shapin	ig Policy						
≘ Configuration		+ Add						Search	Máx: 50
Physical interface			Name	Enabled	Source	Destination	Max Sessions	QoS	Option
WAN									
LAN									
DNS									
Wireless LAN									
Routing									
RIP									
BGP									
OSPF									
	CT-HEAVE								
NAT									
IGMP Objects									
LTE									
Wake on LAN									
Notification Service:									
RADIUS/ TACACS+									
Certificates									

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

Name 🛈	BM_Apart	
Enabled		
Schedule	Always On Scheduled On	
Criteria		
Source	Any 🗸	
Destination	Any ~	
Protocol	Any 🗢	
Traffic Shaping Policy		
Session Limit Mode	Disabled ~	
QoS	Lowest (Others)	

ltem	Description					
Name	Enter a name for identification.					
Enabled	Switch the toggle to enable/disable the traffic shaping policy profile.					
Schedule	 Vigor router can perform the traffic shaping policy profile all the time or on a certain date and time. Always On - The function of traffic shaping policy profile is running all the time. Scheduled On - The function of traffic shaping policy profile is activated based on the schedule profile. 					
	Criteria					
Source / Destination	 Specify the IP type. Vigor router will restrict the sessions for the IPs by the default policy. Any – If Any is selected, the limitation will applied to any IP. IPv4 Address IPv4 Subnet IPv6 Address IPv6 Subnet IP Object IP Group 					
Source / Destination IPv4 Address	It is available when Source / Destination is set as IPv4 Address . +Add – Click to create a new entry. IPv4 Address Start / End - Enter an IPv4 address as the starting point. And, enter another IPv4 address as the ending point.					
Source / Destination IPv4 Subnet Address	 It is available when Source / Destination is set as IPv4 Subnet. +Add – Click to create a new entry. IPv4 Address – Enter an IPv4 address. Subnet Mask – Specify the subnet mask for the IPv4 address. 					
Source / Destination IPv6 Address	It is available when Source / Destination is set as IPv6 Address . +Add – Click to create a new entry. IPv6 Address Start / End - Enter an IPv6 address as the starting point. And, enter another IPv6 address as the ending point.					
Source / Destination IPv6 Subnet Address	It is available when Source / Destination is set as IPv6 Subnet. +Add - Click to create a new entry. IPv6 Address - Enter an IPv6 address. Prefix Length - Set the prefix length for the IPv6 address.					
Source / Destination IP Object	It is available when Source / Destination is set as IP Object . +Add – Up to 12 objects can be specified here. Select Object – Select the object(s) from the available object list on the right side.					
Source / Destination IP Group	It is available when Source / Destination is set as IP Group . +Add – Up to 12 groups can be specified here. Select Group - Select the object(s) from the available group list on the right side.					

Protocol	Only the traffic passing through the selected protocol will be limited.
	Select one of the protocols from the drop-down menu.
	Any – All traffic will be limited.
	Service Type Object – Vigor system offers several service types set with different protocols.
	 Service Type Object – Click +Add to create a new object. Up to 12 objects can be created.
	TCP/UDP – Select Transmission Control Protocol/User Datagram Protocol.
	• Specify Source Port – Switch the toggle to enable the setting of Source Port.
	• Source Port / Destination Port – Set the port range (1 to 65535).
	TCP – Transmission Control Protocol. Setting method is the same as TCP/UDP.
	UDP – User Datagram Protocol. Setting method is the same as TCP/UDP.
	Traffic Shaping Policy

Session Limit Mode	Disabled – Select to deactivate session limit function.			
	Per Source IP Limit – Apply the session limit to the traffic.			
	 Max Sessions - The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List. 			
QoS	Select the class level (Class 1, Class 2, Class 3 and others) of bandwidth which will be applied to this profile.			
	High (Class 1) Medium (Class 2) Low (Class 3)			
	Lowest (Others)			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

II-1-10-2 Bandwidth Limit

Bandwidth Limit ensures LAN clients get their fair share of network bandwidth by placing restrictions on upstream and downstream network speeds.

Search Q	Configuration / Bandy	width Management				3 Reset
	Traffic Shaping Policy	Bandwidth Limi	QoS Setup A	pp QoS Default Policy		
Device Menu	Bandwidth Limit		-			
ව Dashboard	Dandwidth Linit					
	+ Add				Search	Max: 1
Physical Interface	Profile Name	Enabled	Schedule	Source Upload Limit (Mb/s)	Download Limit (Mb/s)	Option
WAN				Air Sector() (Const.)		
LAN						
DNS						
Wireless LAN						
Routing						
RIP						
BGP						
OSPF						
NAT						
IGMP						
Objects						
Wake on LAN						
Notification Services						
RADIUS/ TACACS+						
Certificates						

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

		×
Profile Name 🕕		
Enabled		
Schedule	Always On Scheduled On	
Source	Any 🗸	
Туре	Shared by All Source IP	
Upload Limit (Mb/s) 🕕		
Download Limit (Mb/s) 🕕		
Note:		
LTE/5G-NR WAN upload can no	be limited.	
Cancel Apply		

ltem	Description
Profile Name	Enter a string as the profile name.
Enabled	Switch the toggle to enable/disable this profile of bandwidth limit.
Schedule	Vigor router can perform the bandwidth limit all the time or on a certain date and time.
	Always On - The function of bandwidth limit is running all the time.
	Scheduled On - The function of bandwidth limit is activated based on the schedule profile.

Source	 Identify the object to which the bandwidth limit will be applied. Any - All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX Limit below. 		
	 IPv4 Address 		
	IPv4 Subnet		
	 IP Object 		
	 IP Group 		
Source IPv4 Address	It is available when IPv4 Address is selected as the Source.		
	Click +Add to add a new entry.		
	• IPv4 Address Start - The beginning IP address for this limit entry.		
	• IPv4 Address End - The ending IP address for limit entry.		
Source IPv4 Subnet	It is available when IPv4 Subnet is selected as the Source.		
Address	Click +Add to add a new entry.		
	• IPv4 Address - Specify Start IP Address.		
	• Subnet Mask - Select a Subnet Mask.		
Source IP Object	It is available when IP Object is selected as the Source.		
	All the IPs specified by the selected IP object will be restricted by bandwidth limit defined by TX Limit and RX Limit below.		
	Click on +Add to open the IP object table. Select the IP object(s) and click Close. A new entry will be added immediately.		
Source IP Group	It is available when IP Group is selected as the Source.		
	All the IPs specified by the selected IP group will be restricted by bandwidth limit defined by TX Limit and RX Limit below.		
	Click on +Add to open the IP Group table. Select the IP group(s) and click Close. A new entry will be added immediately.		
Туре	Per Source IP Limit – The upload limit and the download limit will be applied to the source IPv4 address, source IPv4 subnet address, source IP object or source group selected as the Source.		
Upload Limit	Upstream speed limit for each LAN client. Value must be between 1 and 3999 (Mbps).		
Download Limit	Downstream speed limit for each LAN client. Value must be between 1 and 3999 (Mbps).		
Cancel	Discard current settings and return to the previous page.		
Apply	Save the current settings and exit the page.		

II-1-10-3 QoS Setup

QoS (Quality of Service) ensures that all LAN clients receive their fair share of bandwidth that is required for applications to function properly and efficiently.

Without QoS, it is possible that certain applications may consume excessive network resources that they degrade performance of more important applications, especially ones that are less tolerant of jitter (delay variation) or lost or delayed packets. Additionally, at times of network congestion, QoS is able to prioritize different types of traffic according to their predefined priority, thus ensuring traffic of higher importance gets processed first.

A typical QoS deployment consists of two components:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Prioritizing packets by assigning them to different queues and service types according to service levels.

Pervise Menu CoS Setup	[®] Rese				inagement	dwidth Ma	tion / Ban	Configura	a	
QoS Setup Prostal interface Mardware QoS WAN Hardware QoS UNN Interface Enabled Direction Speed (Mtps) High (Class 1) Medium (Class 2) Low (Class 3) Lowest (Others) DNS WAN 2 Upload 1000 25 % 25 % 25 % 25 BIP Port 1 Downloa Downloa 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % <th>QoS Default Policy</th> <th>licy</th> <th>Default Pol</th> <th>etup App QoS E</th> <th>dwidth Limit Qos s</th> <th>y Band</th> <th>iping Poli</th> <th>Traffic Sh</th> <th></th> <th></th>	QoS Default Policy	licy	Default Pol	etup App QoS E	dwidth Limit Qos s	y Band	iping Poli	Traffic Sh		
Dashboard Physical Interface WAN LAN Interface Enabled Direction Speed (Mbps) (Maps)										Menu
Physical interface Hardware QoS WAN LAN Interface Enabled Direction Speed (Mbps) () High (Class 1) Medium (Class 2) Low (Class 3) Lowest (Others) DNS WAN1 I Uplaad 1000 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>P</td> <td>Qos setu</td> <td></td> <td>shboard</td>							P	Qos setu		shboard
Physical interface WAN UNN Interface Endeled Direction Speed (Mbps) High (Class 1) Medium (Class 2) Low (Class 3) Lowest (Others) DNS WAN1 Uplead 1000 25 % 25 % 25 % 25 Wireless LAN WAN2 Uplead 1000 25 % 25 % 25 % 25 Rip Port 1 Downloa 1000 25 % 25 % 25 % 25 GSPF Port 1 Downloa 1000 25 % 25 % 25 % 25 MAT Port 2 Downloa 1000 25 % 25 % 25 % 25 MAT Downloa 1000 25 % 25 % 25 % 25 Item constant Downloa 1000 25 % 25 % 25 % 25 Item constant Downloa 1000 25 % 25 % <td></td>										
LN Interface Enabled Direction Speed (Mtps) High (Class 1) Medium (Class 2) Low (Class 3) Lowect (Opiners) DNS VVAN1 Uplade 1000 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25							e QoS	Hardwar		ysical Interface
DNS WAN1 Uplead 1000 25 % 25 % 25 % 25 Rip Pot1 Downlea 1000 25 % 25 % 25 % 25 % 25 BGP Pot1 Downlea 1000 25 % 25 % 25 % 25 OSPF Pot1 Downlea 1000 25 % 25 % 25 % 25 OSPF Pot2 Downlea 1000 25 % 25 % 25 % 25 OSPF Pot2 Downlea 1000 25 % 25 % 25 % 25 Objects Downlea 1000 25 % 25 % 25 % 25 Vitilication Services Downlea 1000 25 % 25 % 25 % 25 Vitilication Services <									-	NN.
Wireless LAN WANZ Uplead 1000 25 % 25 % 25 % 25 Rip Port 1 Dewnloa d 1000 25 % 25 % 25 % 25 BGP Port 1 Dewnloa d 1000 25 % 25 % 25 % 25 OSPF Downloa d Downloa d 1000 25 % 25 % 25 % 25 NAT Port 3 Downloa d 1000 25 % 25 % 25 % 25 Objects Downloa d 1000 25 % 25 % 25 % 25 Vitikation Services Downloa d 1000 25 % 25 % 25 % 25 Vitikation Services Downloa d 1000 25 % 25 % 25 % 25	is 1) Medium (Class 2) Low (Class 3) Lowest (Others)	Medium (Class 2)		High (Class 1)	Speed (Mbps) ①	Direction	Enabled	Interface	_	
Routing WAA2 U pload 1000 25 % 25 % 25 % 25 Rip Port 1 Downloa d Tool 25 % 25 % 25 % 25 BCP Port 1 Downloa d Tool 25 % 25 % 23 % 25 OSPF Downloa d Tool 25 % 25 % 25 % 25 OSPF Downloa d Tool 25 % 25 % 25 % 25 OSPF Downloa d Tool 25 % 25 % 25 % 25 Objects Downloa d Tool 25 % 25 % 25 % 25 Vide on LAN Downloa d Tool 25 % 25 % 25 % 25	% 25 % 25 % 25 %	25	%	25	1000	Upload		WAN1		
Boding Downloa Downloa 25 % 25 % 25 % 25 BGP OSPF Downloa 1000 25 % 25 % 25 % 25 % 25 NAT Downloa Downloa 000 25 % 25 % 25 % 25 Objects Downloa Downloa 000 25 % 25 % 25 % 25 Value on LAN Port 4 Downloa 1000 25 % 25 % 25 % 25 Notification Services Downloa 1000 25 % 25 % 25 % 25	5 25 5 25 % 25 S	25	5	25	1000	Upload	-	WAN2		
BGP Port 1 1000 25 % 25 % 25 % 25 % 25 CSPF: Domloa Domloa 1500 25 % 25 % 25 % 25 % 25 NAT Icon 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>-</td> <td></td> <td>_</td> <td></td>							-		_	
OSPF Downloa Downloa 1000 25 % 25 % 25 NAT Compo Downloa 000 25 % 25 % 25 % 25 NAT Compo Downloa 000 25 % 25 % 25 % 25 Objects Downloa d 1000 25 % 25 % 25 % 25 Value on LAN Port 4 Downloa 1000 25 % 25 % 25 % 25 Notification Services Downloa 1000 25 % 25 % 25 % 25	% 25 % 25 % 25 %	25	%	25	1000		0	Port 1		
Control Port 2 Downloa d 1000 25 % 25 % 25 % 25 NAT Common Downloa Downloa d 1000 25 % 25 % 25 % 25 NAT Downloa Downloa Downloa 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % 25 % <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>										
NAT Downloa Downloa 000 25 % 25 % 25 % 25 LTE Port 4 Downloa 1000 25 % 25 % 25 % 25 Notification Services Downloa d 1000 25 % 25 % 25 % 25	% 25 % 25 % 25 %	25	%	25	1000			Port 2	ताची.	
ICAIP Port 3 1000 25 % 25 % 25 % 25 Objects Image: Comparison of the state										
Objects Downloa LTE Port 4 Downloa d 1000 25 % 25 % 25 Notification Services Downloa	% 25 % 25 % 25 %	25	%	25	1000		0	Port 3		ир
Wake on LAN Port 4 1000 25 % 25 % 25 % 25 Notification Services Downloa Down						d				jects
Wake on LAN d Notification Services Downloa	% 25 % 25 % 25 %	25	%	25	1000	Downloa	-	Port 4		
Downioa		-		11.00		d	-			ike on LAN
						Downloa	-			
	% 25 % 25 % 25 %	25	15	25	1000	d	Port 5	Port 5		DIUS/ TACACS+

Available settings are explained as follows:

Item	Description
Enabled	Switch the toggle to enable/disable the WAN interface settings.
Direction	At present, only Upload (for outgoing traffic) is available.
Speed(Mbps)	Set the outbound bandwidth (default is 1000) of the WAN/LAN.
High(Class 1)	Set the percentage of bandwidth (upload speed) reserved for class 1.
Medium(Class 2)	Set the percentage of bandwidth (upload speed) reserved for class 2.
Low(Class 3)	Set the percentage of bandwidth (upload speed) reserved for class 3.
Lowest(Others)	Set the percentage of bandwidth (upload speed) reserved for others.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-10-4 APP QoS

APP QoS allows QoS to be applied to select protocols and applications.

Search	q	Configuration / Bandwidth Management	() Reset
		Traffic Shaping Policy Bandwidth Limit QoS Setup App QuS Default Policy	
Device Menu		to be	
(?) Dashboard		App QoS	
Physical Interface		+ Add	Max 20
WAN		Apps QoS DSCP Retag	
LAN		The Second County	
DNS			
Wireless LAN			
Routing		VoIP Prioritize	
RIP		Enable First Priority for VolP	
BGP			
OSPF		SIP UDP Port 5060	
NAT			
IGMP			
Objects			
Wake on LAN			
Notification Servi	ices		
RADIUS/ TACACS			
Certificates		Cancel Apply	

Available settings are explained as follows:

tem Description			
+Add	Apps – The drop-down menu displays various APPEs. Select the one you want.		
	QoS – Select the class level (Class 1, Class 2, Class 3 and others) of bandwidth reserved for the Apps.		
	DSCP Retag – Select the level of the data for processing with QoS control.		
	Delete – Click to remove the selected entry.		
	VolP Prioritize		
Enable First Priority for VoIP	Switch the toggle to enable/disable the function. If enabled, it allows VoIP traffic to receive the highest priority.		

VoIP	If enabled, it allows VoIP traffic to receive the highest priority.
SIP UDP Port	Enter a port number to be monitored for SIP traffic.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-10-5 Default Policy

Default policy defines the bandwidth limit and the session limit for all traffic in default.

Search Q		③Reset
Device Menu	Traffic Shaping Policy Bandwidth Limit QoS Setup App QoS Default Policy	
 Dashboard 	Default Policy	
	Session Limit Mode Per Source IP Limit	
	Per available Promit	
Physical Interface	Max Sessions () 1000	
WAN		
LAN		
DNS		
Wireless LAN		
Routing		
RIP		
BGP		
OSPF		
NAT		
IGMP		
Objects		
LTE		
Wake on LAN		
Notification Services		
RADIUS/ TACACS+		
Certificates	Cancel Apply	

Available settings are explained as follows:

ltem	Description
Session Limit Mode	Disabled – Select to deactivate session limit function.
	Per Source IP Limit – Apply the session limit to the traffic.
	• Max Sessions - The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-11 NAT

Most ISPs allocate one WAN IP address to each subscriber. In order to simultaneously connect multiple devices to the Internet, a technique called Network Address Translation is employed.

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network by obscuring the IP address. There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

II-1-11-1 Port Forwarding

This function allows inbound traffic from specific ports on WAN interfaces to be forwarded to LAN clients.

search Q	Configuration / f	NAT					3 Reset
	Port Forwarding	DMZ Host Port T	riggering ALG UPnP				
Device Menu	Des Francisco da						
Dashboard	Port Forwardin	8					
	+ Add					Search	Max: 40
Physical Interface	Name	Enabled	WAN Interface	WAN IP	Source	Private IP	Option
WAN							
LAN							
DNS							
Wireless LAN							
Routing							
RIP							
BGP							
OSPF							
Bandwidth Management							
IGMP							
Objects							
LTE							
Wake on LAN							
Notification Services							
RADIUS/ TACACS+							
Certificates							

It allows you to open a range of ports for the traffic of special applications.

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

				×
Enabled				
Schedule	Always On Scheduled On			
Network				
WAN Interface	Please Select " 😒			
WAN IP	Please Select 🗸			
Source IP	IP Address \sim			
IP ①	192.168.1.77 - 192.168.1.88			
Private IP	Range 🗸 🗸			
Private IP	Range ~ 192.168.1.155 - 192.168.1.201			
9 ()				Mase
0 g		Public Port End	Private Port 🕕	Maxe

ltem	Description
Name	Enter a name that identifies the rule.
Enabled	Switch the toggle to enable or disable the function.
Schedule	Vigor router can perform the port forwarding all the time or on a certain date and time.
	Always On - The function of port triggering is running all the time.
	Scheduled On - The function of port triggering is activated based on the schedule profile.

Network

WAN Interface	The WAN port(s) whose incoming traffic will be forwarded to a LAN client. Select from a specific WAN interface WAN# to apply the rule to the WAN interface.
Source IP	Any IP Address IP Object IP Group Any – Any data traffic coming from the source IP will be forwarded to a LAN. IP Address – Set a range of IP addresses. Any data traffic coming from the IP addresses within the range will be forwarded to a LAN. IP Object – IP Object – IP Object – Use the drop down list to specify an IP object profile. IP Group –

	• IP Group - Use the drop down list to specify an IP group profile.
Private IP	 Specify a LAN IP address or a range of LAN IP addresses to which the traffic will be forwarded. Single Single Range Single - Specify a destination LAN IP address that will receive the forwarded traffic. Range - Specify a range of destination LAN IP addresses that will receive the forwarded traffic.
	Port Forwarding
+Add	Click to set port numbers for the specified protocol (TCP, UDP, or TCP/UDP) for a port forwarding profile.
Protocol	The protocol to which this rule applies, TCP, UDP or TCP/UDP.
Public Port Start	Specify which port can be redirected to the specified Private IP and Port of the internal host. Enter the required number as the starting port.
Public Port End	Enter the required number as the ending port.
Private Port Start	The port on each LAN client to which the traffic will be directed to. Enter the required number as the starting port.
Private Port End	Enter the required number as the ending port.
Option	Click Delete to remove the selected entry.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

ort	Forwarding	g						
+ Ad	bid					Search		Max: 4
	Name	Enabled	WAN Interface	WAN IP	Source	Private IP	Option	
0	905	Enabled	[WAN] WAN1	[WAN IP](WAN1)172.16.3.132	Any	192.168.1.10	/ Edit	🗊 Delete
0	2136	Enabled	[WAN] WAN1	[WAN IP](WAN1)172.16.3.132	Any	192.168.1.1	0 Edit	🗊 Delete
0	3912	Enabled	[WAN] WAN1	[WAN IP](WAN1)172.16.3.132	Any	192.168.100.252	0 Edit	ሰ Delete
0	for_Carrie	Disabled	None	None	192.168.1.77 - 192.168.1.88	192.168.1.155 - 192.168.1.201	C Edit	🗇 Delete
	Proto	col	Public	Port Start	Public Port End	Private F	ort	

II-1-11-2 DMZ Host

Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.

	Configuration / NAT				3 Reset
Device Menu		Z Host Port Triggering ALG U	PnP		
Dashboard	DMZ Host				
	+ Add				Search Max:
Physical Interface	Enabled	Interface	WAN IP	Private IP	Option
WAN					
LAN					
DNS					
Wireless LAN					
Routing					
RIP					
BGP					
OSPF					
Bandwidth Management					
IGMP					
Objects					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates					

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

IZ Host		Enabled	
Add			
nabled	Interface	Unterface- WAN IP	[WAN] WAN1 (Wired WAN) ~
		WAN IP	[WAN IP](WAN1) ~
		Privațe IP 🕕	192.168.1.100

ltem	Description
Enabled	Switch the toggle to enable or disable the function.

Interface	Allows WAN traffic to be sent to a specific LAN IP address.
WAN IP	Enable the function of applying WAN alias IP. Then, select a WAN alias IP from the available IPv4 alias settings set on Configuration >> WAN >> WAN Connections.
Private IP	Enter an IP address to be the DMZ host.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-11-3 Port Triggering

If you run programs that function as server applications where they expect to receive unsolicited traffic from the WAN, you can set up rules in Port Triggering to detect LAN-to-WAN traffic initiated by those programs, and automatically open up WAN ports to accept incoming traffic and forward it to the LAN client running the server applications.

The duration that these ports are opened depends on the type of protocol used. The "default" values are shown below and these duration values can be modified via telnet commands.

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

Search	Configuration / NAT				3 Reset
Concession of the local division of the loca	Port Forwarding DMZ	Host Port Triggering ALG	UPnP		
Device Menu	Port Triggering				
 Dashboard 	Fort magering				
= Contiguation	+ Add				Search Max 20
Physical Interface	Service Name	Enabled	Schedule	Source IP	Option
WAN					
LAN					
DNS					
Wireless LAN					
Routing					
RIP					
BGP					
OSPF					
Bandwidth Management					
NAT					
IGMP					
Objects					
LTE					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates					
11.14					

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

			×
Add Service	Manually Preset		
Service Name ①			
Enabled			
Schedule	Always On Scheduled On		
Triggering Source			
Source IP	IP Address 🛛 🗸		
IP Address (j)	÷		
Protocol & Port	+ Add	Max: 5	
	Triggering Protocol Triggering Port Start ①	Triggering Port End 🕔	
	TCP: UDP TCP/UDP 1	65535	
Incoming Services			
Drotocol 9 Dort	- And	Mays 5	
Cancel Apply			

ltem	Description				
Add Service	Select from list of predefined service, or manually configure triggering and incoming protocols and ports.				
	Manually - If selected, self-define the service name.				
	• Service Name – Enter the name of the service.				
	Preset - If selected, various services will be offered for you to choose as the service name.				
	• Service Name – Use the drop-down list to specify one service.				
Enabled	Switch the toggle to enable or disable the function of port triggering.				
Schedule	Vigor router can perform the port triggering all the time or on a certain date and time.				
	Always On - The function of port triggering is running all the time.				
	Scheduled On - The function of port triggering is activated based on the selected schedule profile.				
	Triggering Source				
Source IP	Any - Any source IP will be forwarded to a LAN.				
	IP Address - Set a range of IP addresses forwarded to a LAN.				
	• IP Address – Enter the IP address and the subnet mask.				
	IP Object – Click +Add to specify the IP object profile (up to 12 profiles).				
	IP Group - Click +Add to specify the IP group profile (up to 12 profiles)				
Protocol & Port	+Add - Click to set the port numbers (start and end) for the specified protocol (TCP, UDP or TCP/UDP) for the outgoing data (that this rule monitors).				
	Triggering Protocol - The protocol(s) of the outgoing traffic.				
	• TCP - open port(s) to TCP traffic.				
	• UDP - open port(s) to UDP traffic.				

	• TCP/UDP - open port(s) to both TCP and UDP traffic.			
	Select the protocol (TCP, UDP or TCP/UDP) for the outgoing data of such triggering profile.			
	Triggering Port Start / Triggering Port End - Outgoing traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule.			
	Enter the port or port range for the outgoing packets.			
	Incoming Services			
Protocol & Port	+Add - Click to set port numbers (start and end) for the specified protocol (TCP, UDP or TCP/UDP) for the incoming data.			
	Incoming Protocol - The protocol(s) of the incoming traffic.			
	• TCP - open port(s) to TCP traffic.			
	• UDP - open port(s) to UDP traffic.			
	• TCP/UDP - open port(s) to both TCP and UDP traffic.			
	Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.			
	Incoming Port Start / Incoming Port End - Incoming traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule.			
	Enter the port or port range for the incoming packets.			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

II-1-11-4 ALG

ALG means **Application Layer Gateway**. There are two methods provided by Vigor router, RTSP (Real Time Streaming Protocol) ALG and SIP (Session Initiation Protocol) ALG, for processing the packets of the voice and the video.

RTSP ALG makes RTSP message, RTCP message, and RTP packets of voice and video be transmitted and received correctly via NAT by Vigor router.

However, SIP ALG makes SIP message and RTP packets of voice be transmitted and received correctly via NAT by Vigor router.

Search Q	Configuration /	NAT			3 Res
	Port Forwardin	g DMZ Host I	Port Triggering AL	G UPnP	
levice Menu	Application La	nuer Cateman			
වා Dashboard	Application	ayer Gateway			
Physical Interface	Protocol	Enabled	Listen Port ()		
WAN	SIP		5060	(1-65535)	
LAN	RTSP		554	(1~65535)	
DNS				it must	
Wireless LAN					
Routing					
BGP					
OSPF					
Bandwidth Management					
IGMP					
Objects					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates	Cancel Ap	ply			

ltem	Description
Enabled	Switch the toggle to enable or disable the function.
Listen Port	Enter a port number for SIP or RTSP protocol.
Apply	Save the current settings and exit the page.

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

II-1-11-5 UPnP

The Vigor supports UPnP (Universal Plug and Play), which is a suite of network protocols that simplifies network configuration. Applications and network devices on the LAN, that support UPnP, may request the router to modify its settings to allow NAT Traversal, so that WAN hosts can connect to them directly.

Examples of applications and devices that support UPnP include file-sharing applications such as uTorrent, Vuze and eMule, gaming consoles such as the Sony PlayStations 3 and 4 Xbox 360 and Xbox One, media streaming applications such as Plex and XBMC, and messaging and calling applications such as Skype. To find out if a certain application or network device supports or requires UPnP, please consult its user manual or check with its vendor.

SearchQ	Configuration / NAT					C Refresh
	Port Forwarding DMZ Ho	st Port Triggering	ALG UPhP			
Device Menu	UPnP					
(?) Dashboard						
a configuration	Enabled					
Physical Interface	WAN Interface	None				
WAN	The second se	Nume 0				
LAN	Status					
DNS	status					
Wireless LAN						
Routing	OThe following is the displation of the displ	y historical data. If you wa	nt to receive new info	rmation, please turn on the swi	tch	
RIP	WAN Interface	Source	Public Port	Private IP	Private Port	Protocol
BGP						
OSPF						
Bandwidth Management						
NATI						
IGMP						
Objects						
LTE						
Wake on LAN						
Notification Services						
RADIUS/ TACACS+						
Certificates	Cancel Apply					

ltem	Description					
UPnP						
Enabled	Switch the toggle to enable or disable the function. UPnP is required for some applications such as PPS, Skype, eMuleand etc. If you are not familiar with UPnP, it is suggested to turn off this function for security.					
WAN Interface	Select the WAN port on which ports will be opened in response to UPnP commands.					
Status	Displays the historical data.					
Cancel	Discard current settings and return to the previous page.					
Apply	Save the current settings and exit the page.					

II-1-12 IGMP

Internet Group Management Protocol (IGMP) is an IPv4 communication protocol for establishing multicast group memberships.

II-1-12-1 General Setup

This page offers the general setting for configuring the IGMP function.

Search Q	Configuration / IGMP General Setup IGMP Status	() Reset
Device Menu (?) Dashboard	General Setup	
Economicon Physical Interface	IGMP Version	Auto v2 v2
WAN LAN	IGMP Proxy	
DNS	IGMP Praxy	3
Wireless LAN Routing		Note: Enable IGMP Proxy to issue multicast membership messages between LAN host and specified interface. Router will forward multicast packets by the group membership information.
RIP BGP	Interface	None v
OSPF Bandwidth Management	Query Interval Seconds (125
NAT IGMP	IGMP Snooping	
Objects LTE	IGMP Snooping	3
Wake on LAN Notification Services RADIUS/ TACACS+		Note: Enable: Forwards multicast traffic only to ports that are members of that group. Disable: Treats multicast traffic the same as broadcast traffic
Certificates	Cancel Apply	

ltem	Description			
IGMP Version	Select v2 or v3 or Auto. At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe.			
	IGMP Proxy			
IGMP Proxy	Switch the toggle to enable or disable the function.			
	The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode.			
Interface	Specify an interface for packets passing through.			
Query Interval	Vigor router will periodically check which IP obtaining IPTV service by sending query. It might cause inconvenience for client. Therefore, set a suitable time (unit: second) as the query interval to limit the frequency of query sent by Vigor router.			
IGMP encapsulation in PPPoE	It depends on the specifications regulated by each ISP. If you have no idea to enable or disable, simply contact your ISP providers.			
	IGMP Snooping			
IGMP SnoopingSelect to enable IGMP Snooping so that multicast traffic will be forwarded to IGMP clients that have joined a multicast group				
IGMP Fast Leave	This option is shown only when IGMP Snooping is enabled. Select to enable IGMP Fast Leave.			

	Normally when the router receives a "leave" message from an IGMP host, it will send a last member query message to see if there are still members within the multicast group. When Fast Leave is enabled, multicast for a group is immediately terminated when the last host in that group sends a "leave" message.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-12-2 IGMP Status

This page displays a list of active multicast groups.

Séarch Q	Configuration / IGMP					C Refresh
Device Menu (🕗 Dashboard	General Setup IGMPStatus Multicast Group Table					
Configuration Physical Interface	Group Address	Pt	P2	P3	P4	P5
WAN						
DNS Wireless LAN						
Routing RiP						
BGP OSPF Bandwidth Management						
NAT						
Objects LTE						
Wake on LAN Notification Services						
RADIUS/ TACACS+ Certificates						

Available settings are explained as follows:

ltem	Description
Group Address	Address of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254.
P1 to P5 (C410 series) P1 to P4 (C510 series)	LAN ports that have IGMP hosts joined to this multicast group.

II-1-13 Objects

Vigor router system provides the object functions.

Users can define various types of objects and groups, and then apply them at various scenarios, like Configuration>>NAT>> Port Forwarding, Security>>Firewall Filters.

The advantage is that the user doesn't have to set data repetitively and it significantly enhances efficiency.

Currently, the objects that can be preset include IP, MAC, Schedule, Service Type, Keyword, and groups that include IP, MAC, etc.

II-1-13-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind the objects with *groups* for using conveniently. Later, we can select that object/group for applying it.

For example, a range of IP address in the same department can be defined with an IP object.

Search Q	Configuration	/ Objects								() Reset
	IP Object	IP Group	MAC Object	MAC Group	Schedule	Service Type Object	Country Object	Keyword Object	Backup & Restore	
Device Menu	IP Object									
 Dashboard 	ir object									
	+ Add								Search	Max: 19
Physical Interface	Object Name		IP V	ersion	IPv4	Address	IPv6 Address		Used in	Option
WAN						1				
LAN										
DNS										
Wireless LAN										
Routing										
RIP										
BGP										
OSPF										
Bandwidth Management										
NAT										
IGMP										
Wake on LAN										
Notification Services										

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

bject IP Group	MAC Object MAC Group	Schedule Service Type Obj		×
Dbject			Object Name 🛞	IP_Object_10
dd			IP Version	Both IPv4 IPv6
ject Name	IP Version	IPv4 Address	Address Type	IP Subnet
			IPv4 Settings	
			Start IP Address 🕕	192.168.1.100
			End IP Address 🕦	192.168.1.100
			Invert 🕕	
			IPv6 Settings	
			Match Type 🕕	128 Bits Suffix 64 Bits
			Start IP Address 🕧	ff02::1
		_	End IP Address 🕕	ff02::1
			lövert 🛈	
				Cancel Apply

ltem	Description							
Object Name	Enter the name that identifies this profile.							
IP Version	Select the IP version (IPv4, IPv6 or Both) for entering correct IP address.							
Address Type	Select the type (IP or Subnet) of address.							
	IPv4 Settings							
Start IP Address	Enter the beginning IP address, if the Address Type is IP.							
	To set a range of IP addresses, enter the different IP addresses as start IP address and end IP address.							
End IP Address	Enter the ending IP address, if Address Type is IP.							
IP Address	Enter an IP address if Address Type is Subnet.							
Subnet Mask	Enter subnet mask, if Address Type is Subnet.							
Invert	If enabled, all addresses except the ones entered above will be used.							
	IPv6 Settings							
Match Type	Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address							
Start IP Address	Enter the beginning IPv6 address, if the Address Type is IP. To set a range of IP addresses, enter the different IP addresses as start IP address and end IPv6 address.							
End IP Address	Enter the ending IPv6 address, if Address Type is IP.							
IP Address	Enter an IPv6 address if Address Type is Subnet.							
Prefix Length	Enter IPv6 prefix length, if Address type is Subnet.							
Invert	If enabled, all addresses except the ones entered above will be used.							
Cancel	Discard current settings and return to the previous page.							

Apply	Save the current settings and exit the page.
-------	----------------------------------------------

II-1-13-2 IP Group

Multiple IPv4 Objects /IPv6 Objects can be placed into an IPv4 Group / IPv6 Group.

SearchQ	Configuratio	on / Objects								1 Reset
	IP Object	IP Group	MAC Object	MAC Group	Schedule	Service Type Object	Country Object	Keyword Object	Backup & Restore	
Device Menu	IP Group									
Dashboard	IF Group									
	+ Add								Seartha	a Mater 3
Physical Interface	Group Na	ime	Objects Incl	uded				Used In		Option
WAN										
LAN										
DNS										
Wireless LAN										
Routing										
RIP										
BGP										
OSPF										
Bandwidth Management										
NAT										
IGMP										
Wake on LAN										
Notification Services										
RADIUS/ TACACS+										
Certificates										

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

			Availabl	le Object			>
Group Name 🕧	IP4_group_1		Select O	bjects		Search	
Selected Objects	+ Add	Max		Object Name	IPv4 Address	IPv6 Address	
	Object Name IPv4 Address IPv6 Addr	ess Option		IP_Object_10	192.168.1.100		
	IP_Object_10 192.168.1.100	Delete					
Cancel Apply							Close

Available settings are explained as follows:

ltem	Description					
Group Name	Enter a name that identifies this profile.					
Selected Objects	+Add - Click to open the page with available objects.					
Available Object						

Search	Enter the IP object name or the IPv4/IPv6 Address to search related IP object(s).
Select Objects	Objects available for grouping will be displayed here. Select one or more objects to group under the current IP group.
Object Name	Display current existed IPv4/IPv6 object(s). To add an IP object to the current IP group, simply select the object(s) you want. The selected items will then appear under the Selected Objects section on the left side.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

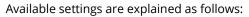
II-1-13-3 MAC Object

The MAC address of local or remote clients can be specified in the MAC Object page.

Search	Q Cor	nfiguration /	Objects							() F	eset CRefresh
	the second s	Object IP	Group	MAC Object	MAC Group	Schedule	Service Type Object	Country Object	Keyword Object	Backup & Restore	
Device Menu		of object									
 Dashboard 	M/	AC Object									
	1.00	Add								Search_	Max: 192
Physical Interface	0	bject Name				MAC Addr	ess		Used in		Option
WAN											
LAN											
DNS											
Wireless LAN											
Routing											
RIP											
BGP											
OSPF											
Bandwidth Management											
NAT											
IGMP											
Wake on LAN											
Notification Services											
RADIUS/ TACACS+											
Certificates											

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

Group MAC Object MAC Group Sched	ule Service Type Obj	×
	Object Name ①	MAC_Obejct_1
	MAC Address ①	08:BF:B8:D5:DD:A9
MAC	Address	
		Cancel Apply



ltem	Description				
Object Name Enter a name that identifies this object.					
MAC Address	Enter the MAC address of the client.				
Cancel	Discard current settings and return to the previous page.				
Apply	Save the current settings and exit the page.				

II-1-13-4 MAC Group

	Configuratio	n / Objects							() R	eset C Refresh
	IP Object	IP Group	MAC Object	MAC Group	Schedule	Service Type Obje	ct Country Obje	t Keyword Object	Backup & Restore	
Device Menu	MAC Group	· ·								
Dashboard										
	+ Add								Search	Max: 31
Physical Interface	Group Na	me		Objects Included		Use	ed in	Selected Objects		Option
WAN										
LAN										
DNS										
Wireless LAN										
Routing										
RIP										
BGP										
OSPF										
Bandwidth Management										
NAT										
IGMP										
Wake on LAN										
Notification Services										
RADIUS/ TACACS+										
Certificates										

Multiple MAC Objects can be placed into a MAC Group.

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

			Available	e MAC Object		
Group Name 🛈	MAC_Group_Anna		Select M	AC Objects	Search	
Selected Objects	+ Add	Max: 12		Object Name	MAC Address	
	Object Name MAC Address	Option		MAC_Obejct_1	08:BF:B8:D5:DD:A9	
	MAC_Obejct_1 08:BF:B8:D5:DD:4					
Cancel Apply						Close

Available settings are explained as follows:

ltem	Description				
Group Name	Enter a name that identifies this profile.				
Selected Objects +Add - Click to open the page with available objects.					
	Available MAC Object				
Select MAC Objects	Search - Enter the MAC object name to display existed MAC objects.				
Object Name	Select the object(s) to be grouped under the current MAC group.				

	The selected one will be shown under the Selected Objects on the left side.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-13-5 Schedule

Time schedules can be created and used with router features that support them, so that those features can be turned on and off automatically at preconfigured times.

Search	Configurat	ion / Objects							3 Reset
	IP Object	IP Group	MAC Object	AAC Group Schedule	Service Type Object	Country Object	Keyword Object	Backup & Restore	
Device Menu	Schedule								
(?) Dashboard	Schedule								
😄 Configuration .	+ Add							Search	Max: 20
Physical Interface	Name	Enabled	Start Date	Start Time (HH: mm)	End T	lime (HH: mm)	Repeat	In Use	Option
WAN									
LAN									
DNS									
Wireless LAN									
Routing									
RIP									
BGP									
OSPF									
Bandwidth Management.									
NAT									
IGMP									
Wake on LAN									
Notification Services									
RADIUS/ TACACS+									
Certificates									

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

IP Object	IP Group	MAC Object MA	C Group	Service Type Obj				×
Schedule					Name 🗊		Schedule_	noon
+ Add					Enabled			0
Name	Enabled	Start Date	Start Time (HH: mm)	E				
					Start Date	2025-02-3	27	۵
					Start Time (HH: mm)	11	~ : 28	~
					End Time (HH: mm) 🕧	04	~ : 00	~
					Repeat		Once	~
							Cancel	Apply

ltem	Description
Name	Enter the name of the schedule profile.
Enabled	Switch the toggle to enable or disable this schedule profile.
Start Date	Select the date when the entry comes into effect.
Start Time	Set the time when the schedule is triggered.
End Time	Set the time for the schedule to be ended.
Repeat	Once - The schedule is triggered once based on Date, Start Time and End Time.
	Daily - The schedule is triggered everyday based on Start Time and End Time .
	 End Repeat - If enabled, the schedule will be triggered every day till the date defined in the End Repeat Date.
	• End Repeat Date - The schedule will be ended on the specified date.
	Weekly - The schedule will be triggered, starting at the Start Time and ending at the End Time, on the selected days of the week.
	• Every - Select the day for triggering the schedule.
	 End Repeat - If enabled, the schedule will be triggered every week till the date defined in the End Repeat Date
	• End Repeat Date - The schedule will be ended on the specified date.
	Monthly - The schedule will be triggered monthly based on the Date setting. For example, choose 2022-04-27 as the date set. Later, this schedule will be triggered on the 27th of every month.
	 End Repeat - If enabled, the schedule will be triggered every month till the date defined in the End Repeat Date.
	• End Repeat Date - The schedule will be ended on the specified date.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-13-6 Service Type Object

Up to 255 Service Type Objects can be created.

earch Q	Configuration /	Objects								() Reset
	IP Object IP	Group M	AC Object MAC	Group Sched	lute Service 1	ype Object Country	Object Keyword Obj	ect Backup & Res	tore	
vice Menu	Service Type O	biect								
Dashboard										
	+ Add							Search		Max: 25
Physical Interface	Name	Protocol	Source Port Start	Source Port End	Source Invert	Destination Port Start	Destination Port End	Destination Invert	Option	
WAN	AUTH	TCP	1	65535	false	113	113	false	@ Edit	1 Delete
LAN					225		100			
DNS	BGP	TCP	1	65535	false	179	179	false	Ø Edit	Delete
Wireless LAN	BOOTPCLIENT	UDP	1	65535	false	68	68	false	Ø Edit	😭 Delete
Routing	BOOTPSERVER	UDP	+	65535	false	67	67	false	/ Edit	Delete
RIP	BUUTPSERVER	UUP		03333	raize	67	67	19:06	Pr sais	El merese
BGP	CU_SEEME_HI	TCP/UDP	1	65535	false	24032	24032	false	Ø Edit	Delete
OSPF	CU_SEEME_LO	TCP/UDP	1	65535	false	7648	7648	false	@ Edit	1 Delete
Bandwidth Management										-
NAT	DNS	TCP/UDP	1	65535	false	53	53	false	@ Edit	1 Delete
IGMP	FINGER	TCP	1	65535	false	79	79	false	Ø Edit	Delete
Objects	and a second sec				-			177		
Wake on LAN	FTP	TCP	1	65535	false	20	21	false	@ Edit	1 Delete
Notification Services	H323	TCP	1	65535	false	1720	1720	false	Ø Edit	1 Delete
RADIUS/ TACACS+	Showing 1 to 10 of	f 34 entries						a Sh	ow 10	v entrie
Certificates								34	10	~ entrie

To add/edit a service type profile, click the **+Add / Edit** link to get the following page.

P Object P	Group N	IAC Object MAG	Group Sched	ule Service T	ype Obj		×
Service Type C	bject						
						Name	AUTH
+ Add						Protocol	TCP 🗸 🗸
Name	Protocol	Source Port Start	Source Port End	Source Invert	Destin		
AUTH	тср	i	65535	false	113	Specify Source Port	
BGP	700	1	65535	false	179	Source Port Start	1
BGb	TCP	1	03535	Taise	1/9	Source Port End	65535
BOOTPCLIENT	UDP	Ĩ	65535	false	68		
BOOTPSERVER	HDP	1	65535	false	67	Source Invert	
						Destination Port Start	113
CU_SEEME_HI	TCP/UDP	1	65535	false	24032	Destination Port End	113
CU_SEEME_LO	TCP/UDP	1	65535	false	7648	Destination Invert	
DNS.	TCP/UDP	ī	65535	false	53	Destination invert	
FINGER	TCP	1	65535	false	79		
FTP	тср	1	65535	false	20		
H323	тср	1	65535	false	1720		
Showing 1 to 10 o	f 34 entries						
							Cancel Apply

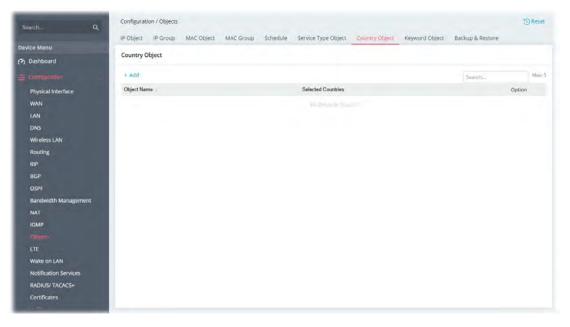
ltem	Description		
Name	Name that identifies this profile. Maximum length is 15 characters.		
ProtocolProtocol(s) to which this profile applies.Any – All protocols.			
	ICMP / ICMPv6 – Internet Control Message Protocol		
	IGMP – Internet Group Management Protocol		

	TCP – Transmission Control Protocol
	UDP – User Datagram Protocol
	TCP/UDP – Transmission Control Protocol and User Datagram Protocol
	Other – Other protocols not listed above. Enter protocol number in the textbox.
Specify Source Port	When protocol selected includes TCP or UDP, the source and destination ports can be specified.
	Switch the toggle to enable/disable the source port settings.
	Source Port Start / Source Port End – Enter two values to define the port range of source port.
	Source Invert - If enabled, all port values except the ones entered above (Source Port Start/End) will be used.
Destination Port Start / Destination Port End	When protocol selected includes TCP or UDP, the source and destination ports can be specified.
Destination Invert	If enabled, all port values except the ones entered above (Destination Port Start/End) will be used.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-13-7 Country Object

The country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.

Up to 5 country object profiles can be created for use as blacklists or white lists.



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

		Available Cou	untry	
		- *		
By clicking Apply, ye	ou agree to the terms and policy of Maxmind License.	🗆 им	"U.S. Outlying Islands"	Oceania
		C AS	"American Samoa"	Oceania
bject Name 🕕	For_TW	CA CA	Canada	"North America"
lected Countries	+ Add Max: 12 Country Continent Option	US US	"United States"	"North America"
	"United States" "North America" 🍵 Delete	PS	Palestine	Asia
	N ote: To upgrade database, please check: <u>System Mai</u>		Serbia	Europe
	Note: To upgrade database, please check: <u>System Mar</u>		Antarctica	Antarctica
		🗆 sx	"Sint Maarten"	"North America"
		□ cw	Curaçao	"North America"
		D BQ	"Bonaire	"North America"
		□ ss	"South Sudan"	Africa
		Showing 1 to 25 entries	50 of 250	Show All 🗸
ancel Apply				Close

Available settings are explained as follows:

ltem	Description
Object Name	Name that identifies this profile. Maximum length is 63 characters.
Selected Countries	+Add – Click to create an entry. A list of country codes will appear on the right side. Select up to 12 required codes for the new object.
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.

II-1-13-8 Keyword Object

50 Keyword Object Profiles can be created for use as blacklists or white lists.

Search_	Q	Configurati	ion / Objects								3 Reset
	-	IP Object	IP Group	MAC Object	MAC Group	Schedule	Service Type Object	Country Object	Keyword Object	Backup & Restore	
Device Menu		Keyword (Ohlast								
 Dashboard 		Keyword	Object								
E Configuration		+ Add								Search	Max: 50
Physical Interface		Object Nan	ne					Keywords			Option
WAN											
LAN											
DNS											
Wireless LAN											
Routing											
BGP											
OSPF											
Bandwidth Manageme	int										
NAT											
IGMP											
Wake on LAN											
Notification Services											
RADIUS/ TACACS+											
Certificates											

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

		×
Object Name 🕕	Forbidden	
+ Add		Max: B
Keywords		Option
Gamble, gambling		(i) Delete

Available settings are explained as follows:

Item	Description					
Object Name	Name that identifies this profile. Maximum length is 16 characters.					
Keywords	Keywords to be matched. Enter the content for this profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.					
	In addition, up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered. For key phrases that contain spaces, replace spaces with the sequence %20. For example, the phrase "keep out" is to be entered as "keep%20out".					
Delete	Click to remove the selected entry.					
Cancel	Discard current settings and return to the previous page.					
Apply	Save the current settings and exit the page.					

II-1-13-9 Backup & Restore

The object settings can be backed up as a file. The backup file can be imported to the device to restore the configuration in the future if required.

SearchQ	Configuration / Objects IP Object IP Group MAC Object MAC Group Schedule Service Type Object Country Object Keyword Object Backup & Restore-
Device Menu 🕢 Dashboard	Backup & Restore
E Continuantion	Backup
WAN LAN DNS Wireless LAN Routing RIP BGP OSPF Bandwidth Management	Salietied Item Salietied Item Pobject PGroup MAC Object MAC Group Schedule Scruice Type Object Country Object Keyword Object
NAT IGMP Chipters: LTE Wake on LAN Notification Services RADIUS/TACACS+ Certificates	Restore Restore from Backup Alls

Available settings are explained as follows:

ltem	Description
Backup	Usually, a user can create the objects through the web page under Objects.
	All the objects (or the template) can be saved and exported as a file by clicking Download.
	Back up – Click it to backup current objects to a file. Such file can be restored for future use.
Restore	Restore from Backup File – Click it to specify a file backed up previously.
	Restore – Click to execute the restoration.

II-1-14 LTE

II-1-14-1 SIM Inbox

This page will list the received SMS messages in the LTE SIM card. The SMS Inbox table shows the received date, the phone number or sender ID where this message was from, and the beginning of the message content.

Search, Q	Configuration / LTE				③Reset CRefresh
1000 C 1000	SMS Inbox Send	SMS SMS Outbox			
Device Menu	LTE SMS inbox				
 Dashboard 	LTE SWIS INDOX				
					Max: 255
Physical Interface		From	Date	Message	Option
WAN					
LAN					
DNS					
Wireless LAN					
Routing					
RIP					
BGP					
OSPF					
Bandwidth Management					
NAT					
IGMP					
Objects					
L TE					
Wake on LAN					
Notification Services					
RADIUS/ TACACS+					
Certificates					

II-1-14-2 Send SMS

This page is used to send SMS messages by the LTE SIM card. It also displays the number of SMS required to send the message.

E Cooliguration	Configuration / LTE	1 Rese
Physical Interface	SMS inbox Send SMS SMS Outbox	
WAN		
LAN	Send SMS Message	
DNS		
Wireless LAN	Redpient Number () +886123456789	
Routing	Message Please send a message to the third party to test this feature.	
RIP		
BGP		
OSPF	627160 characters (1 SMS)	
Bandwidth Management	And the state of t	
NAT		
IGMP		
Objects		
Wake on LAN		
Notification Services		
RADIUS/ TACACS+		
Certificates		
Security >		
, IAM >		
y VPN >	Cancel Apply	

ltem	Description
Recipient Number	Enter the phone number of the recipient.

	The format can be an international phone number (+8869123455678) or a general phone number (0912345678).
Message	Enter the message content to send. The total number of characters that you can Enter this field is 160.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-14-3 SMS Outbox

This page lists the SMS messages that have been sent. The LTE Outbox table displays the date the SMS was sent, the recipient's phone number, and the beginning of the message content.

Search Q	 ration / LTE ox Send SMS S	M5 Outbox		(3) Reset	C Refresh
Device Menu	tbox Cache	MS OULDOX			
🚍 Configuration	То	Date	Message	Option	Max: 255
Physical Interface WAN	 +886123456789	2021/10/24 11:40:35	Please send a message to the third party to test this feature.	© View	Delete
LAN DNS					
Wireless LAN					
Routing RIP					
BGP OSPF					
Bandwidth Management					
NAT IGMP					
Objects					
Wake on LAN					
Notification Services RADIUS/ TACACS+					
Certificates					

ltem	Description
View	Show detailed information for the selected SMS.
Delete	Delete the chosen SMS entry.

II-1-15 Wake on LAN

Using the Wake on LAN (WoL) feature, LAN clients that support WoL can be powered on or resume from sleep over the network, without the need for physical access to the device.

In order for LAN clients to be able to wake from sleep or off states, the network interface card must be configured to monitor Wake-on-LAN messages. Consult the documentation of the LAN client for details on setting up its network interface for Wake on LAN.

If you wish to be able to select the IP address of the Wake-on-LAN client, its MAC address must first be bound to a static IP address using the Bind IP to MAC function.

SearchQ	Configuration / Wake on LAN				BReset CRefresh
	Wake on LAN from Router				
Device Menu					
 Dashboard 	Wake by	MAC Address Blied IR to MAC List			
😑 Configuration 🚽	MAC Address ()				
Physical Interface			and the second se	and the second	
WAN		Note: Houter Will send magic packets to	wake device up. Make sure b	ie device supports wake on LAN feature.	
LAN		Wake UP			
DNS					
Wireless LAN					
Routing	Wake on LAN/ WAN Device Li	et.			
RIP	Wake on Daw Walk Device L	56			
BGP	+ Add			Max: 10	
OSPF	Name () Device ()	Auto Wake Up by Schedule	Wake on WAN	Public Port	
Bandwidth Management					
NAT					
IGMP					
Objects	Wake on WAN Access Control Mode	Allow List 🗸 🗸			
LTE					
Welke on LAN	IP Group	yun uun 🔍			
Notification Services		Note: Wake on WAN opens router port a	utomatically.		
RADIUS/ TACACS+					
Certificates	Cancel Apply				

ltem	Description			
	Wake on LAN from Router			
Wake by	 The type of address of the LAN client to be woken up. MAC Address Bind IP to MAC List 			
MAC Address	The MAC address provided here will be the device that the Vigor router will wake up.			
	If MAC Address is selected in Wake by, the content listed on ARP Table will be shown for you to choose.			
	Configuration / Wake on LAN			
	Wake on LAN from Router			
	Wake by MAC Address Bind IP to MAC List			
	MAC Address 🕡			
	SUGGESTIONS C			
	50:3E:AA:0D:2E:B1 (192.168.1.20)			
	If Bind IP to MAC List is selected in Wake by the profile content listed			

	on Configuration>>l choose one.	AN>>Bind IP to MAC will be shown	for you to			
	Configuration / Wake on L	AN				
	Wake on LAN from Rou	ter				
	Wake by	MAC Address Bind IP to MAC List				
	MAC Address 🕧					
		SUGGESTIONS 77:77:77:77:77 (192.168.1.77)	C			
	Configuration / LAN					
	LANS Bind IP to MAC DHCP Options	Inter-LAN Routing VLAN List Interface VLAN LAN Port 802.1X				
	Bind IP to MAC					
	+ Add					
	Comment	MAC Address	IP Address			
	LAN_PC_1	TELEVELEN	192,108,1,77			
Wake Up	Click to send Wake-o	on-LAN message to the specified LA	N client.			
	Wake on LAN	/WAN Device List				
+Add	Click to specify a new device which will be awakened.					
	Name – Enter the na	ame of the device.				
	Device – Enter the MAC address of the device.					
	Auto Wake Up by Schedule – The device can be awakened based on the schedule automatically.					
	Wake on WAN – Switch the toggle to enable / disable this function. The device can be awakened by the IPs selected on the Allow List.					
	Public Port – Enter a port number.					
	Option (Delete) – Remove the selected device.					
Wake on WAN Access Control Mode	Set the path for the boot packet (sent by a mobile phone) to deliver to the remote device.					
		e IP group. The boot packets will be a any WAN IP or the IP listed on the				
Cancel	Discard current sett	Discard current settings.				
Apply	Save the current set					

II-1-16 Notification Services

Generally, the notification service refers to notifying users via email or SMS.

II-1-16-1 Services & Providers

Before notifying the clients, the router's system administrator needs to configure the server and provider used to send letters or SMS messages.

SearchQ	Configuration / No	otification Services			() Rese
	Services & Provide	s SMTP Server SMS Provider	Webhook Notification Backup & Restore		
rvice Menu	Services & Provi				
) Dashboard	Services & Provi	ders			
Physical Interface	Categories	Notification Type	SMTP Server	SMS Provider	
WAN	System	System Notifications	Default_Email_Profile ∨	Default_SMS_Profile \lor	
LAN	MFA	Email & SMS PIN Code	Default_Email_Profile ~	Default_SMS_Profile ~	
DNS	1.00				
Wireless LAN					
Routing					
RIP					
BGP					
OSPF					
Bandwidth Management					
NAT					
NAT IGMP					
IGMP					
IGMP Objects					
IGMP Objects LTE					
IGMP Objects LTE Wake on LAN					

Available settings are explained as follows:

ltem	Description
SMTP Server	Use the drop-down menu to select the SMTP server for sending the e-mail.
SMS Provider	Use the drop-down menu to select the SMS Provider for sending the SMS.
Cancel	Discard current settings.
Apply	Save the current settings.

II-1-16-2 SMTP Server

Up to 2 SMTP server profiles can be set up for chosen by Services & Providers.

SearchQ.	Configuration / Notifica	ation Services							③ Reset
Landar and	Services & Providers	SMTP Server	SMS Provider	Webhook	Notification	Backup & Rest	ore		
Device Menu									
 Dashboard 	SMTP Server								
😑 Configuration									Max: 2
Physical Interface	Name			Enabled	SMTE	P Server	Last Sent at	Option	
WAN	Default_Email_Profile			Enabled				/ Edit	
LAN									
DNS	Senders_MKT			Enabled	8.8.8.	8		@ Edut	Delete
Wireless LAN									
Routing									
RIP									
BGP									
OSPF									
Bandwidth Management									
NAT									
IGMP									
Objects									
LTE									
Wake on LAN									
Notification Services									
RADIUS/ TACACS+									
Certificates									

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

Name ())	Senders_MKT	
Enabled		
connecting Sender Through	Default WAN 🛛 🗸	
MTP Server 🛞	8.8.8.8	
Specify Port		
Sender Address	carrie@draytek.com	
Connection Security	SSL 🗠	
uthentication Required		
Jsername	test123	
Password	····· @	
iending Intervals (Seconds)	15	
Send Test Email to	NnN20200331@gmail.com	
	Send Test Message	

ltem	Description	
Name	nter the name of the profile.	
Enabled	Switch the toggle to enable/disable this profile.	
Connecting Sender Through	Specify the WAN interface for connecting the sender.	
SMTP Server	Enter the IP address of the SMTP server.	

Specify Port	Switch the toggle to enable the port setting.
	Specify SMTP Port – Enter the port number of the SMTP server.
Sender Address	Enter the E-mail address of the sender.
Connection Security	There are three methods to enhance the connection security of SMTP server.
	None - No SSL. Packets will be transferred without encryption.
	SSL - Packets will be transferred with encrypted connection. Select to use SMTPS (SMTP over SSL) to communicate with the SMTP server. Note that the port number used for SMTPS server is 465.
	StartTLS - It is a protocol used in communication to initiate a transition from an insecure one to a secure channel.
Authentication Required	Select to send username and password to SMTP server for authentication.
	Username – Username for authentication. Maximum length is 31 characters.
	Password – Password for authentication. Maximum length is 31 characters.
Sending Intervals	Minimum amount of time, in seconds, to wait between sending e-mail messages.
Send Test Email to	Specify an email address.
	Send Test Message - Click it to send a test e-mail according to above configuration.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-16-3 SMS Provider

Up to 2 SMS profiles can be set up as the SMS Providers.

	Configuration / Notifica	ation Services				() Reset
	Services & Providers	SMTP Server SMS Provider	Webhook Notification Backup & Rest	pre		
Device Menu	SMS Provider					
🝘 Dashboard	SMS Provider					
						Mass
Physical Interface	Name	Enabled	Service Provider	Last Sent at	Option	
WAN	Default_SMS_Profile	Enabled	None		@ Edit	
LAN					2410	-
DNS	MKT_1000	Enabled	Vigor Router SMS Gateway		Ø Edit	會 Delete
Wireless LAN						
Routing						
RIP						
BGP						
OSPF						
Bandwidth Management						
NAT						
IGMP						
Objects						
Wake on LAN						
RADIUS/ TACACS+						
Certificates						

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

ltem	Description
Name	Enter the name of the profile.
Enabled	Switch the toggle to enable/disable this profile.
Connecting Sender Through	Specify the WAN interface for connecting the sender.
Service Provider	Vigor Router SMS Gateway – Not all Vigor routers support the SMS

	function. This option allows you to set the IP address of the router which can be treated as a SMS gateway.
	Customized – Set the IP address or URL provided by the SMS provider
When Vigor Router SMS Gateway is selected as	SMS Gateway URL – Enter an identifier (domain name or IP address) for the service provider.
the Service Provider	Connection Protocol – Specify HTTP or HTTPS.
	Username - Used for being authenticated by the Service Provider. Maximum length is 31 characters.
	Password - Used for being authenticated by the Service Provider. Maximum length is 31 characters.
When Customized is selected as the Service Provider	SMS Provider API URL – Enter the URL for the SMS service. Maximum length is 255 characters. Contact the service provider for the appropriate URL to use.
	SMS API Parameter - For each API (Application Programming Interface with an independent Text Message and Recipient Number (Send to), please enter the strings represented by each API.
	HTTP Method – Two request methods offered here.
	• GET - Used to request data from a specified resource.
	• POST - Used to send data to a server to create/update a resource
SMS Quota	Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0.
Sending Intervals	Minimum amount of time, in seconds, to wait between sending SMS messages.
Send Test SMS to	Specify an email address.
	Send Test Message - Click it to send a test e-mail according to above configuration.
	Discard current settings and return to the previous page.
Cancel	Discard current settings and return to the previous page.

II-1-16-4 Webhook

Vigor router will send a report (webhook message) including WAN up, down, CPU usage, memory usage and etc. to a monitoring server periodically.

Up to 10 webhook profiles can be set up.

	Configuration / Notification	Services			3 Reset
	Services & Providers SM	ATP Server SMS Provide	webhool Notification Back	up & Restore	
evice Menu					
Dashboard	Webhook				
	+ Add				Max: 10
Physical Interface	Webhook Name	Enabled	Server Protocol Type	Monitoring Server URL	Option
WAN	Slack	Disabled	HTTPS		🖉 Edit
LAN	Telegram	Disabled	HTTPS		/ Edit
DNS	reiegram	000000	nuns -		S. man
Wireless LAN					
Routing					
RIP					
BGP					
OSPF					
Bandwidth Management					
NAT					
IGMP					
Objects					
Wake on LAN					
RADIUS/ TACACS+					

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

	MTP Server SMS Provider	Webhook Notification			3
Webhook			Webhook Name 🕠		Hook_1
+ Add			Enabled		
Webhook Name	Enabled	Server Protocol Type	enabled		
Slack	Disabled	HTTPS	Server Protocol Type		HTTPS HTTP
Telegram	Disabled	HTTPS	Monitoring Server URL 🕦	www.draytek.com	

Available settings are explained as follows:

ltem	Description
Webhook Name	Enter the name of the profile.
Enabled	Switch the toggle to enable/disable this profile.
Server Protocol Type	Select the protocol (HTTPS or HTTP) used for the server.

Monitoring Server URL	Enter the URL of a server.	
Cancel	Discard current settings and return to the previous page.	
Apply	Save the current settings and exit the page.	

II-1-16-5 Notification

Up to 20 notification profiles can be created and applied with the provider notification services.

	Configuration / Notification S	ervices				(3) Rese
	Services & Providers SMT	P Server SMS Provider Wet	nook Notification Backs	ip & Restore		
evice Menu	Notification					
ን Dashboard	wouncation					
	+ Add					Max:
Physical Interface	Profile Name	Events Type	# of Event	Schedule	Option	
WAN	Notify_MKT	Alarm	1	Schedule_noon	Ø Edit	Delete
LAN						
DNS						
Wireless LAN						
Routing						
RIP						
BGP						
OSPF						
Bandwidth Management						
NAT						
IGMP						
Objects						
Wake on LAN						
RADIUS/ TACACS+						
Certificates						

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

		×
Profile Name	Notify_MKT	
Trigger Events		
Events Type	Alarm Report	
Trigger Events	WAN / Disconnected WAN / Reached Limit. × Budget ×	
WAN Disconnected	_ [WAN] WAN1 _ [WAN] WAN2 _ [WAN] WAN3 _ [WAN] WAN4 _ [WAN] WAN5	
WAN Reached Limit Budget	📄 [WAN] WAN1 📄 [WAN] WAN2 📄 [WAN] WAN3 📄 [WAN] WAN4 📄 [WAN] WAN5	
Notification		
Email Alert		
Send Alert Email to	select your rook on s	
SMS Alert	3	
Webhook		
Schedule	select your options 💉	
Cancel Apply		

ltem	Description

Profile Name	Enter the name of the service profile.
Events Type	Alarm – The Vigor system will send alert messages to recipients if an alert event occurs.
	Report – The Vigor system will periodically send reports to recipients when an alert event occurs.
	 Report Period – Set the period (60-360 minutes) for Vigor system to send out the report by email, SMS and etc.
Trigger Events	Select the events that allow the Vigor system to send reports or alerts via email, SMS, and more using the drop-down list.
Email Alert	Switch the toggle to enable / disable the email alert function.
	Send Alert Email to - Select the email profile(s) for sending out the notification by email.
SMS Alert	Switch the toggle to enable / disable the SMS alert function.
	Send Alert SMS to - Select the SMS profile(s) for sending out the notification by SMS.
Webhook	Switch the toggle to enable / disable the webhook notification.
	Webhook Profile - Select the webhook profile(s) for sending out the notification.
Schedule	Select the schedule profile(s) to send the notification (SMS, Email).
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-1-16-6 Backup & Restore

Backup and restore the configuration settings for notification services.

StearchQ	Services & Providers SMTP S	server SMS Provider Webhook Notification Backup & Restore
	Backup & Restore	
Device Menu	Contrast, Contrast,	
(?) Dashboard	1000	
🚍 Configuration	Backup	
Physical Interface	Selected Item	🖸 Select All
WAN		Services & Providers
LAN		SMTP Server
DNS		SMS Provider
Wireless LAN		Vebhook
Routing		Votification
RIP	Password Protection	0
BGP	Posantona Protection	
OSPF		Back up
Bandwidth Management		
NAT	Restore	
IGMP	Restore from Backup File	C Restore
Objects	receiver in an and the	La contract
LTE	File has Password Protection	
Wake on LAN	Password	۵
Notification Services		
RADIUS/ TACACS+		
Certificates		

ltem	Description
Selected Item	Select the items for which settings will be backed up or restored.

Password Protection	Switch the toggle to enable or disable the function.				
	If enabled, set a password.				
	New Password – Enter a string as the password. Confirm New Password – Enter the string again.				
	Back up – Click to perform the backup job.				
Restore from Backup File	Select the backup file you wish to restore.				
File has Password	Switch the toggle to enable or disable the function.				
Protection	If enabled, set a password.				
	Password – Please enter a string to use as the password for restoring the configuration.				
Cancel	Discard current settings and return to the previous page.				
Apply	Save the current settings and exit the page.				

II-1-17 RADIUS/TACACS+

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.

The router supports external TACACS+ and internal and external RADIUS servers for user authentication. Services that require user authentication include WLAN and VPN.

II-1-17-1 External RADIUS

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

Vigor router can be operated as a RADIUS client. This web page is used to configure settings for external RADIUS server. Then LAN users of Vigor router will be authenticated and accounted by such server for network application.

Select External RADIUS to configure the router to use an external RADIUS server for user authentication.

Search		on / RADIUS/ TACACS+					() Reset
Device Menu	External RA		ernal TACACS+				
∋ Contiguration	+ Add Name	Primary Authentication Server	Secondary Authentication Server	Primary Accounting Server	Secondary Accounting Server	Option	Max: 4
Physical Interface WAN LAN DNS Wireless LAN Routing REP BGP OSPF Bandwidth Management NAT ICAMP Objects LTE Wake on LAN Notification Services PMIDUS/TACACS+	RADIUS_1	rmmay Autoencasoo Server 172.16.3.62	university Automotion Only P	remer Accounting Server	Secondary Accounting Server	Ciption © East	(1) Delete
Certificates							

To add a new profile, click the **+Add** link (up to 4) to get the following page.

							>
Name 🕥	RADIUS	5_1					
Authentication							
RADIUS Authentication							
Authentication Server	+ Add					Max: 3	
	Priority	Server IP	Secret		Authentication Port	Option	
	0	172.16.3.62		۵	1812	窗 Delete	
Authorization							
RADIUS Authorization							
Accounting							
RADIUS Accounting							
RADIUS Server Failover Policy							
Cancel Apply							

ltem	Description				
Name	Enter the name of the profile.				
	Authentication				
RADIUS Authentication	Switch the toggle to enable/disable this profile.				
Authentication Server	+Add – Click to add a server (up to 3).				
	Server IP –Enter the IP address of RADIUS server.				
	Secret – The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.				
	Authentication Port – The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.				
	Option (Delete) - Remove the selected server.				
	Authorization				
RADIUS Authorization	Switch the toggle to enable/disable this profile.				
	Disconnect Message Port - Set a UDP port number (3799 in default) for receiving the disconnected-request packets from the AAA server. Note that these packets have been accepted by the RADIUS server before being disconnected by the AAA server.				
	Accounting				
RADIUS Accounting	RADIUS Accounting is a network customer billing mechanism for RADIUS server.				
	If enabled, Vigor router will deliver accounting request (e.g., IP address, traffic from the client) to the specified RADIUS server periodically.				
	Switch the toggle to enable/disable this profile.				
Accounting Server	+Add - Click to add a server (up to 3).				

	Server IP - Enter the IP address of RADIUS server.
	 Secret - The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters. Authentication Port - Set the UDP port number (1813 in default) as the accounting port.
	Option (Delete) - Remove the selected server.
Interim Update Interval	Set an interval time from 10 minutes to 1440 minutes (1 day) for the router to deliver the accounting request to the RADIUS server.
	RADIUS Server Failover Policy
Retry	Set the number of attempts to perform reconnection with RADIUS server. If the connection (with the Primary Server) still fails, stop the connection attempt and begin to make connection with the secondary server.
Timeout	Set a timeout value for the router waiting for a response from the RADIUS server. If no response, Vigor router will send the authentication request again.
	Connection Test
Connection Test	Test with Status Server – Click to make a test of authentication server and accounting server.
Server Status	Display the test result of the connection test.
Cancel	Discard current settings and return to the previous page.
	Save the current settings and exit the page.

II-1-17-2 Internal RADIUS

Except for being a built-in RADIUS client, Vigor router also can be operated as a RADIUS server which performs security authentication by itself. This page is used to configure settings for internal RADIUS server. Then LAN user of Vigor router will be authenticated by Vigor router directly.

Select Internal RADIUS to configure the router's built-in RADIUS server.

search Q	Configuration / RADIUS/ TACAC	+	() Res
	External RADIUS Internal R	DIUS External TACACS+	
Device Menu	Internal RADIUS		
 Dashboard 	Internal RADIOS		
🚊 Configuration	Enabled		
Physical Interface		1812	
WAN	Authentication Port	1812	
LAN	hanning etc		
DNS	RADIUS Client Access List		
Wireless LAN			
Routing	IPv4 Client List	+ Add Max 10	
RIP		Enabled Shared Secret IPv4 Address IPv4 Mask	
BGP		No Records Former	
OSPF			
Bandwidth Management			
NAT	IPv6 Client List	+ Add Max: 10	
IGMP		Enabled Shared IPv6 Address IPv6	
Objects		Secret Length Q	
LTE			
Wake on LAN			
Notification Services			
RADIUS/ TACACS+	Authentication		
Certificates	Cancel Apply		

ltem	Description			
Enabled	Switch the toggle to enable/disable settings for this RADIUS server.			
Authentication Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.			
	RADIUS Client Access List			
IPv4 Client List	Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server.			
	+Add – Click to add a client (up to 10).			
	Enabled –Switch the toggle to enable/disable this entry.			
	Shared Secret – A text string that is known to both the router's RADIU server and the RADIUS client that is used to authenticate messages sent between them. Maximum length is 36 characters.			
	IPv4 Address – Enter the IPv4 address of the client.			
	IPv4 Mask – Select the IP mask to configure the size of the IP block.			
	Option (Delete) - Remove the selected client.			
IPv6 Client List	Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server.			
	+Add – Click to add a client (up to 10).			
	Enabled –Switch the toggle to enable/disable this entry.			
	Shared Secret – A text string that is known to both the router's RADIU server and the RADIUS client that is used to authenticate messages sent between them. Maximum length is 36 characters.			
	IPv6 Address –Enter the IPv6 address of the client.			
	IPv6 Length – Enter the prefix length of the IPv6 block.			
	Option (Delete) - Remove the selected client.			
	Authentication			
Method	Specify the way to authenticate the wireless client.			
	PAP Only – Only the Password Authentication Protocol will be used to validate users.			

	PAP/CHAP/MS-CHAP/MS-CHAP2 - PAP, CHAP (Challenge-Handshake Authentication Protocol), and Microsoft versions of CHAP can be used to validate users.		
802.1X Method	Support 802.1X Method – The built in RADIUS server offered by Vigor router can act as the AAA server. Select to enable 802.1X support.		
Certificate	Select the certificate (created by Configuration>>Certificates>>Local Certificates) for applying to Internal RADIUS.		
	User Profile		
User	During the process of security authentication, user account and user password will be required for identity authentication. Before configuring such page, create at least one user profile in IAM>>Users & Groups first.		
	All Users – Click to make all user profiles for security authentication.		
	Select Users – Click to select the user profile(s) for security authentication.		
User Groups	All Groups – Click to make all user groups for security authentication. Select Groups – Click to select the user groups for security authentication.		
Cancel	Discard current settings and return to the previous page.		
Apply	Save the current settings and exit the page.		

II-1-17-3 External TACACS+

It means Terminal Access Controller Access-Control System Plus. It works like RADIUS does. Click the **External TACACS+** to open the following page:

Configuration / RADIUS/ TACACS+	DRes
External RADIUS Internal RADIUS External TACACS+	
External TACACS+	
Enabled	
Primary Server	
1	
Server IP Address	
Destination Port 49	
Shared Secret ()	
a substances and a substances of the substances	
Secondary Server	
Server IP Address	
Destination Port 49	
Shared Secret ()	
Cancel Apply	
	External RADIUS Internal RADIUS External TACACS+ Enabled Primary Server Server IP Address Destination Port Server IP Address

ltem	Description
Enabled	Switch the toggle to enable/disable this profile.

Authentication Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.		
	Primary Server/Secondary Server		
Server IP Address	Enter the IP address of the TACACS+ server.		
	Two external TACACS+ servers are allowed to set in this page.		
	The secondary TACACS+ server will be used as a backup server when the primary TACACS+ server is down.		
Destination Port	Enter the port used by the TACACS+ server. Port 49 is most common.		
Shared Secret	A text string that is known to both the TACACS+ server and client (the router) that is used to authenticate messages sent between them. Maximum length is 36 characters.		
Cancel	Discard current settings and return to the previous page.		
Apply	Save the current settings and exit the page.		

II-1-18 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 router 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 router 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-1-18-1 Local Certificates

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

SearchQ	Configuration / Certificate						
Device Menu		sted CA Local	Services Back	up & Restore			
(?) Dashboard	Local Certificates						
	+ Add					Search	Maxe 2
Physical Interface	Certificate Name	Status	Source	CA Imported	Valid From	Valid Until	Option
WAN	Default_Certificate	Valid	Internal	~	2021/10/24 09:02:04	2022/11/23 09:02:04	© View © Regenerate
LAN							C Regenerate
DNS							
Wireless LAN							
Routing							
RIP							
BGP							
OSPF							
Bandwidth Management							
NAT							
IGMP							
Objects							
Wake on LAN							
Notification Services							
RADIUS/ TACACS+							

To check detailed information of the selected certificate, click View.

Local Certificates True	sted CA Local S	ervices Backi	ip & Restore		×
Local Certificates					Copy PEM Content to clipboard
+ жба				Certificate Name 🕕	Default_Certificate
Certificate Name	Status	Source	CA Imported	Version	V3
Default_Certificate	Valid	Internal	4	Status	Valid
				Source	internal
				CA Imported	~
				Subject_Name	~
				Country (C)	тw
				State (ST)	Hsinchu
				Location (L)	Hsinchu
				Organization (O)	DrayTek
				Organization Unit (OU)	DrayTek
				Common Name (CN)	www.draytek.com
				Email (E)	
-					

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

ertificate Name 🕡		
Aethod	Generate CSR Import Certificate & Keys	
еу Туре	RSA-2048 Bit	
lgorithm	SHA-256	
Subject Alternative Name		
ype	IP Address Domain Name Email	
P Address		
Subject Name		
ountry(C) 🕕		
tate (ST) 🕕		
ocation (L) 🕕		
Organization (O) ①		
Organization Unit(OU) ()		

ltem	Description					
Certificate Name	Enter the name that identifies the certificate.					
Method	Generate CSR - Generate a new local certificate. Import Certificate & Keys - Vigor router 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 router 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 certificate whose extensions are usually .pfx or .p12. And these 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 certificate 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 File - 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	Discard current settings and return to the previous page.				
Apply	Save the current settings and exit the page.				

II-1-18-2 Trusted CA

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

Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

When the local client and remote client are required to make certificate authentication (e.g., IPsec X.509) for data passing through SSL tunnel and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

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

Search	Q	Configuration / Certificates									
and the second se		Local Certificates	Trusted CA	Local Services	Backup & Restore						
Device Menu		Trusted Certificat	Authorition								
 Dashboard 		rusted certificat	e Authonties								
😤 Configuration		+ Add						Search		Max: 20	
Physical Interface		Certificate Name		Status	Common Name	Valid I	rom	Valid Until	Option	1	
WAN		Root CA		Empty					ℓ Cre	ate	
LAN											
DNS											
Wireless LAN											
Routing											
RIP											
BGP											
OSPF											
Bandwidth Managerr	ent										
NAT											
IGMP											
Objects											
LTE											
Wake on LAN											
Notification Services											
RADIUS/ TACACS+											
Contilication											

To import a RootCA to the Vigor router, click **+Add** to upload one certificate.

				×
Upload Certificate	Local_cert_N.txt	Choose a file		
Cancel Apply				

Available settings are explained as follows:

ltem	Description
Upload Certificate	Choose a file - Select a local certificate file.
Cancel	Discard current settings and return to the previous page.
Apply	Click to import selected certificate file to the router.

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

d Certificates Trusted C	A Local Services E	lackup & Restore		×
sted Certificate Authoriti	es		Кеу Туре	RSA-2048 Bit
⊲rtificate Name	Status	Common Name	Algorithm	SHA-256
JCA	Empty		Subject Alternative Name Type IP Address () Subject Name Country (C) () Common Name (CN) () State (ST) () Location (L) () Organization (On () Crganization Unit (OL) () Email (E)	IP Address Domain Name Email

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	Vigor router accepts the type and value of the specified subject alternative name as valid authentication. Supported subject alternative types are IP Address , Domain Name and E-Mail .						
	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.

II-1-18-3 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.

Search	Configuration / Certificates			3 Rese
		Local Services Backup & Restor	e	
evice Menu	La serie de la			
) Dashboard	Local Services			
	and the second sec			
Physical Interface	Categories	Services	Local Certificate	
WAN	Web Server	HTTPS	Default_Certificate ~	
LAN	Web Server	TR069	Default_Certificate ~	
DNS			Projanja na Kinder	
Wireless LAN	the second second second			
	Notes Certificate only and CSR C	annot be applied to local services.		
Routing				
RIP				
RIP BGP	ent			
RIP BGP OSPF	ent			
RIP BGP OSPF Bandwidth Manageme	ent			
RIP BGP OSPF Bandwidth Manageme NAT	ent			
RIP BGP OSPF Bandwidth Manageme NAT IGMP	ent			
RIP BGP OSPF Bandwidth Manageme NAT IGMP Objects	ent			
RIP BGP OSPF Bandwidth Manageme NAT IGMP Objects LTE	ent			
RIP BGP OSPF Bandwidth Manageme NAT IGMP Objects LTE Wake on LAN	ent			

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	Discard current settings and return to the previous page.					
Apply	Save the current settings.					

II-1-18-4 Backup & Restore

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

Search Q	Configuration / Certificates	
	Local Certificates Trusted C/	A Local Services Backup & Restore
Device Menu	Backup & Restore	
🕫 Dashboard		
	Backup	
Physical Interface	Selected item	Select All
WAN		Local Certificates
LAN		Trusted Certificate Authorities
DNS	Password Protection	
Wireless LAN	Password Protection	
Routing	New Password ()	•
RIP	Confirm New Password ()	Φ
BGP		At least 8 characters
OSPF		Uppercase characters
Bandwidth Management		Lowercase characters
NAT		 Numbers or Special characters」のこと・#新()17*
IGMP		
Objects		
		Back up
Wake on LAN	and the second sec	
Notification Services	Restore	
RADIUS/ TACACS+	Restore from Backup File	C) Rescore
	File has Password Protection	

Available settings are explained as follows:

ltem	Description
	Backup
Selected Item	Select the certification type (local, trusted or all certificates).
Password Protection	Enabled - Switch the toggle to enable or disable the function.
	 New Password - Enter the password with which you wish to encrypt the certificate.
	• Confirm New Password - Enter the password again.
	Back up - Click to download the certificate.
	Restore
Restore from Backup	Click to select the backup file you wish to restore.
file	Click to locate the file for restoring.
	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.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

II-2 Security

II-2-1 Firewall Filters

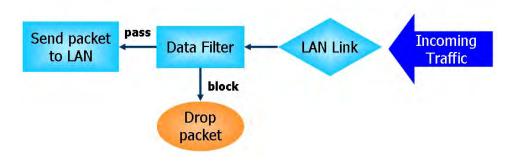
A network firewall monitors traffic travelling between networks, with the ability to selectively allow or block traffic using a predefined set of security rules. This helps to maintain the integrity of networks by stopping unauthorized access and the exchange of sensitive information.

LAN users are provided with secured protection by the following firewall facilities:

- User-configurable IP filter (Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

Data Filter

All traffic, both incoming and outgoing, that does not trigger a PPP connection attempt (either because a PPP connection is not necessary, or the required PPP connection has already been established) is checked against the Data Filter, and will be allowed or blocked according to the rules configured within.



Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not only examines the header information also monitors the state of the connection.

Denial of Service (DoS) Defense

DoS attacks are categorized into two types: flooding-type attacks and vulnerability attacks. Flooding-type attacks attempts to exhaust system resources while vulnerability attacks attempts to paralyze the system by exploiting vulnerabilities of protocols or operation systems.

Vigor's DoS Defense functionality detects DoS attacks and mitigates their damage by inspecting every incoming packet, and malicious packets will be blocked. If Syslog is enabled, alert messages will also be sent. Abnormal traffic flow such as flood and port scan attacks that exceed allowable thresholds are also blocked.

The below shows the attack types that DoS/DDoS defense function can detect:

- SYN flood attack
 UDP flood attack
 ICMP flood attack
 Port Scan attack
 IP options
 Land attack
 Smurf attack
- 8. Trace route

9. SYN fragment
 10. Fraggle attack
 11. TCP flag scan
 12. Tear drop attack
 13. Ping of Death attack
 14. ICMP fragment
 15. Unassigned Numbers

II-2-1-1 IP Reputation Filters

An IP Reputation Filter is a security tool that evaluates the trustworthiness of an IP address based on its historical behavior and various factors. This filter helps detect and prevent malicious activities, such as spam, hacking attempts, and other forms of cyberattacks.

The IP Reputation Filter used by the Vigor router is designed to filter and block dangerous IP addresses. To effectively implement this filtering, three directions need to be considered as filtering conditions:

1. Inbound (from the Internet to the router's WAN)

2. Inbound (from the Internet to the router's LAN)

3. Outbound (from the LAN to the Internet)

This approach ensures comprehensive protection against harmful IP addresses.

	Security / Firewall Filters				C Refres
evice Menu	IP Reputation Filters IP Filters	Content Filters D	efault Filters Backup &	Restore	
ት Dashboard	10 December Files				
Configuration	IP Reputation Filters				
	Enable IP Reputation Filters	D			
	No	ote: To use IP Reputa	lion, activate and manage	the license on Registration & Services	
Defense Setup					
MAC Filtering Profile		High Risk Suspice	ous Moderate Low	Risk Trustworthy	
IPv6 Address Security	0	20	40 60	80 100	
Security Defense Status					
URL/IP Lookup					
iam >	the second second				
2 VPN >	Block Report				
A Monitoring	Enable IP Reputation Log	D			
g Utility 5	Inbound/Outbound	E	llock when under (()	Log when under	
System Maintenance	Inbound (Internet to Router WAN)		Disabled \checkmark	Disabled 🗸	
irtual Controller	inbound (internet to Router LAN)		Disabled 🗸	Disabled ~	
+ Wireless	Outbound (LAN to internet)		Disabled ~	Disabled ~	
Switch 3					
	Cancel Apply				

ltem	Description
	IP Reputation Filters
Enable IP Reputation Filters	Switch the toggle to enable/disable this feature.
Block Report	Click to show the IP Reputation blocked report.
Enable IP Reputation	Switch the toggle to enable or disable the logging function.

Log							
Block when under	Select the risk level. Once the risk for the packets (incoming/outgoing) reaches the threshold (20/40/60/80) defined here, Vigor system will block the IP immediately. The default setting is "Disabled," which means that no filtering will be performed.						
Log when under	Select the risk level. Once the risk for the packets (incoming/outgoing) reaches the percentage defined here, Vigor system will record corresponding information to the SysLog server. The default is Disabled.						
	Port List						
Inbound (Internet to Router WAN) / Inbound (Internet to LAN) / Outbound (LAN to	 For packet transmission in various directions, select the appropriate service protocol and corresponding port number to be used. The direction of packet transmission includes: Inbound to Router WAN - Packets coming from the WAN to the localhost and entering the Vigor router will be filtered and 						
Internet)	 checked. Inbound to Router LAN - Packets entering the Vigor router from outside via LAN will be filtered and checked. 						
	• Outbound (LAN to Internet) - Packets sent out through the LAN interface of the Vigor router will be filtered and examined.						
	+Add – Click to select a service from the list of available service options.						
	Allow List						
Inbound (Internet to Router WAN) /	IP address(es) of the clients within the allow list will not be filtered via IP Reputation Filter.						
Inbound (Internet to	The direction of packet transmission includes:						
LAN) /	 Inbound (Internet to Router WAN) 						
Outbound (LAN to Internet)	Inbound (Internet to LAN)						
	Outbound (LAN to Internet)						
	Click on each tab to create the allow list separately.						
	+Add – Click to add a new IP address as the member within the allow list.						
	• IP Address – Enter the IP address.						
	+Add – Click to add a new object / group as the member within the allow list.						
	• Object & Group – Use the drop-down list to specify the object & group profile.						
Cancel	Discard current settings and return to the previous page.						

II-2-1-2 IP Filters

Search Q	Security / Fir									-	eset C Refresh
evice Menu	IP Reputatio	n Filters	IP Filters	Content Filters	Default Filters	Backup & Restor	e				
and the second	IP Filters										
ት Dashboard											
Configuration	+ Add								Sear	:H	🚊 Maxi 4
7 Security		Name	Enabled	Direction	Source	Destination	Protocol	Service Type Object	Action	Hits	Option
Firewall Filters											
Defense Setup											
MAC Filtering Profile											
IPv6 Address Security											
Security Defense Status											
URL/IP Lookup											
IAM X											
VPN >											
Monitoring											
tutility >											
System Maintenance											
rtual Controller											
Wireless											
Switch S.											

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

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

		×
Name 🕕		
Enabled		
Schedule	Always On Scheduled On	
Direction	LAN to WAN \sim	
Specify Interface	C00	
Criteria		
Source	Any 💛	
Destination	Any ~	
Protocol	Any	
Fragment	Don't Care 🗸	
Action		
Action	Pass. Block	
Bypass Content Filter	C30	
	Note: Disable: Apply content filtering rules.	
	Enable: Bypass content filtering and execute actions directly.	

ltem	Description
Name	Enter a name to identify the rule.
Enabled	Switch the toggle to enable/disable this profile.
Schedule	Always On – This rule is enabled and active for always. Scheduled On - Select Schedule indexes to allow the rule to be enabled at specific times. You may choose up to 4 out of the 15 schedules in Configurations>>Objects>>Schedule. The rule is always enabled when no indexes have been selected.

	 Clear Session when Schedule is On - Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset. 					
Direction	Specify the direction of traffic flow to which this filter rule applies.					
	LAN to WAN					
	WAN to LAN					
	LAN/VPN to LAN/VPN					
Specify Interface	Switch the toggle to enable/disable the function.					
	If enabled, specify the interfaces for the traffic flow.					
	Source Interface – Select the LAN/VPN interface(s).					
	Destination Interface – Select the WAN interface(s).					
	Criteria					
Source	Configure the source IP addresses.					
	To set the IP address manually, please choose Any / IPv4 Address / IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group / MAC Object / MAC Group as the source and enter required information.					
	Any – All IP addresses					
	IPv4 Address–Enter the IP address.					
	• Source IPv4 Address – Click +Add to enter the IP address.					
	IPv4 Subnet–Enter the IP Address and the Subnet Mask.					
	 Source IPv4 Subnet Address - Click +Add to enter the IPv4 address with a subnet mask. 					
	IPv6 Address–Enter the IPv6 address.					
	• Source IPv6 Address – Click +Add to enter the IPv6 address.					
	IPv6 Subnet-Enter the IPv6 Address and the prefix length.					
	 Source IPv6 Subnet Address - Click +Add to enter the IPv6 address with a subnet mask. 					
	IP Object -Allows selection of predefined IP Objects.					
	 Source IP Object – Click +Add to select an IP object. 					
	IP Group –Allows selection of predefined IP Groups.					
	 Source IP Group - Click +Add to select an IP group. 					
	MAC Object–Allows selection of predefined MAC Objects.					
	 Source MAC Object – Click +Add to select an MAC object. 					
	MAC Group –Allows selection of predefined MAC Groups.					
	Source MAC Group - Click +Add to select an MAC group.					
Destination	Configure the destination IP addresses.					
	To set the IP address manually, please choose Any / IPv4 Address / IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group / Country Object as the destination and enter required information.					
	Any – All IP addresses					
	IPv4 Address–Enter one IPv4 address.					
	• Destination IPv4 Address – Click +Add to enter the IP address.					
	IPv4 Subnet–Enter the IPv4 Address and the Subnet Mask.					
	 Destination IPv4 Subnet Address - Click +Add to enter the IPv4 address with a subnet mask. 					
	IPv6 Address–Enter the IPv6 address.					
	 Destination IPv6 Address – Click +Add to enter the IPv6 address. 					

	IPv6 Subnet –Enter the IPv6 Address and the prefix length.								
	 Destination IPv6 Subnet Address - Click +Add to enter the IPv6 address with a subnet mask. IP Object–Allows selection of predefined IP Objects. 								
	 Destination IP Object – Click +Add to select an IP object. 								
	IP Group – Allows selection of predefined IP Groups.								
	 Destination IP Group - Click +Add to select an IP group. Country Object –Allows selection of predefined Country Objects. 								
	 Destination Country Object – Select the object. 								
Protocol	Specify the protocol(s) which this filter rule will apply to.								
	Any								
	Service Object								
	• TCP/UDP								
	• TCP								
	• UDP								
	• ICMP								
	 ICMPv6 IGMP 								
	• Others								
	Available Service Type								
	Select Object Search								
	Name Protocol Destination Port Start Destination Port End								
	□ AUTH TCP 113 113.								
	BGP TCP 179 179								
Spacify Source Bort	It is available when TCD or LIDD or TCD/LIDD is get as the Protocol								
Specify Source Port	It is available when TCP or UDP or TCP/UDP is set as the Protocol. Switch the toggle to enable / disable the port settings. Source Port – If enabled, please provide the starting and ending port								
	values.								
Destination Port	It is available when TCP or UDP or TCP/UDP is set as the Protocol.								
	To define a port range, please provide the starting and ending port values.								
	It is available when Others is set as the Protocol.								
Protocol Number	It is available when Others is set as the Protocol.								
Protocol Number	It is available when Others is set as the Protocol. Enter a value as the protocol number.								
	Enter a value as the protocol number.								
	Enter a value as the protocol number. Action to be taken for fragmented packets.								
Protocol Number Fragment	 Enter a value as the protocol number. Action to be taken for fragmented packets. Don't care –No action will be taken towards fragmented packets 								
	 Enter a value as the protocol number. Action to be taken for fragmented packets. Don't care –No action will be taken towards fragmented packets 								
	 Enter a value as the protocol number. Action to be taken for fragmented packets. Don't care –No action will be taken towards fragmented packets. Unfragmented –Apply the rule to unfragmented packets. 								
	 Enter a value as the protocol number. Action to be taken for fragmented packets. Don't care –No action will be taken towards fragmented packets Unfragmented –Apply the rule to unfragmented packets. Fragmented – Apply the rule to fragmented packets. Too Short – Apply the rule only to packets that are too short to 								

	Pass - Packets matching the rule will be passed immediately. Block - Packets matching the rule will be dropped immediately.
Bypass Content Filter	Switch the toggle to enable the function. If enabled, Vigor router will perform the data transmission bypassing the content filter rules.
Enable Syslog	Switch the toggle to enable the recording the filter log onto SysLog.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

Reput	itatio	n Filters	IP Filters	Content Filters	Default Filters	Backup & Re	store						
P Filte	ers												
+ Add	q	Clone	ResetHits	ሰ MultipleDelete	2					Search		414	Max: 4
		Name	Enabled	Direction	Source	Destination	Protocol	Service Type Object	Action	Hits	Option		
		Firewall_1	Enable	LAN to WAN	Any	Country:	Any		Pass	0	/ Edit	<u>ا</u> ش ۵	elete

Select one of the existed IP filter profile, more options will appear.

ltem	Description
Clone	Duplicate the selected IP filter profile with a new name.
ResetHits	Reset the number of times that each IP rule has been matched when comparing packets to the default value.
MultipleDelete	When more than one item is selected, click it to remove the items at one time.
Edit	Modify the selected IP filter profile.
Delete	Remove the selected IP filter profile.

II-2-1-3 Content Filters

Content Filter includes APPE, URL Filter, and WCF services. APPE is filtered by defined pattern. URL and WCF filters filter the servers to connect to by examining the server name in DNS request packets or TLS client hello packets.

This page allows you to configure up to 40 content filters profiles (including APPE, URL, and WCF) previously.

Vigor router will perform the payload (content) analysis for the packets in each session (LAN to WAN) based on the filter profiles defined in this page till to find out which content filter meeting the traffic.

Device Menu		Security									() Re	set CR	fresh
 Dashboard 		IP Reput	ation F	Iters IP Filter	rs Content Fill	ers Default Fi	ters Backup	o & Restore					
출 Configuration	>	Content	Filten	5									
Security		+ Add								Se	arch		Aax: 40
Fitewall Fiters				Profile Name	Enabled	Direction	Source	Destination	Action	Keyword Exceptions	Hits	Option	
Defense Setup													
MAC Filtering Profile IPv6 Address Security													
Security Defense Status													
URL/IP Lookup													
A IAM	У.												
VPN	×												
🔂 Monitoring	2												
88 Utility	3												
🖏 System Maintenance	*												
Virtual Controller													
}⊶ Wireless	>												
믕 Switch	*												

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

		×
Profile Name 🛈	NOgambling	
Enabled		
Schedule	Always On Scheduled On	
Direction	LAN to WAN	
Specify Interface		
Source	Any 🗸	
Destination	Please select 😒	
	Note: To use WCF, activate and manage the license on Registration & Services	
Action		
Action	Pass Block	
Enable Keyword Exception		
Enable Syslog		
Cancel Apply		

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

Profile Name	Enter a name to identify the filter profile.					
Enabled	Switch the toggle to enable/disable this profile.					
Schedule	Always On – This rule is enabled and active for always.					
	 Scheduled On - Select Schedule indexes to allow the rule to be enabled at specific times. You may choose up to 4 out of the 20 schedules in Configurations>>Objects>>Schedule. Clear Session when Schedule is On - Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset. 					
Direction	Display the direction of traffic flow to which this filter rule applies.					
Specify Interface	Switch the toggle to enable/disable the function.					
	If enabled, specify the interfaces for the traffic flow.					
	Specified LAN – Select the LAN interface(s).					
Source	Configure the source IP addresses.					
	To set the IP address manually, please choose Any / IPv4 Address / IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group / MAC Object / MAC Group as the source and enter required information.					
	Any – All IP addresses					
	IPv4 Address -Enter the IP address.					
	 Source IPv4 Address – Click +Add to enter the IP address. IP 4.6 heat 5 to atle IP 4 block and the Schwart Made 					
	 IPv4 Subnet–Enter the IP Address and the Subnet Mask. Source IPv4 Subnet Address - Click +Add to enter the IPv4 address 					
	with a subnet mask.					
	IPv6 Address–Enter the IPv6 address.					
	 Source IPv6 Address – Click +Add to enter the IPv6 address. IPv6 Subset Enter the IPv6 Address and the prefix length 					
	IPv6 Subnet –Enter the IPv6 Address and the prefix length.					
	 Source IPv6 Subnet Address - Click +Add to enter the IPv6 address with a prefix length. 					
	IP Object –Allows selection of predefined IP Objects.					
	• Source IP Object – Click +Add to select an IP object.					
	IP Group –Allows selection of predefined IP Groups.					
	 Source IP Group - Click +Add to select an IP group. 					
	MAC Object–Allows selection of predefined MAC Objects.					
	 Source MAC Object – Click +Add to select an MAC object. 					
	MAC Group –Allows selection of predefined MAC Groups.					
	• Source MAC Group - Click +Add to select an MAC group.					
Destination	Select specific WCF and/or APPE and/or UCF (keyword object) profile to be included in the filter.					
	Action					
Action	Action to be taken when packets match the rule.					
	Pass - Packets matching the rule will be passed immediately.					
	Block - Packets matching the rule will be dropped immediately.					
Enable Keyword	Switch the toggle to enable/disable the function.					
Exception	Keyword Exceptions - Displays selected keyword objects.					
	The system will check the sessions additionally with the selected					
	keyword profile(s). If the session meets the keyword filter profile, the					

	system will perform the action reversely.
Enable Syslog	Switch the toggle to enable the recording the filter log onto SysLog.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

II-2-1-4 Default Filters

Traffic is filtered by firewall functions in the following order:

- 1. Data Filter Sets and Rules
- 2. Block connections initiated from WAN
- 3. Default Rule

This page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor router.

The default rule applies to all traffic that is not constrained by other filters or rules.

Concession in which the Party New York, New Yo	Security / Firewall Filters	CRefresh
Device Menu	IP Reputation Filters IP Filters Content Filters Default Filters Backup & Restore	
(?) Dashboard		1
	Default Filters	
@ Security	The second second second	
Firewell Gilbert	Outbound Traffic (LAN to WAN)	
Defense Setup	IP Filters Default Action Pass Block	
MAC Filtering Profile IPv6 Address Security	Enable Content Filter Default Rule	
Security Defense Status	Content Filter Default Rule Pass Block	
URL/IP Lookup	Content Destination Please select	
A IAM →	Note: To use WCF, activate and manage the license on Registration & Services	
O VPN >		
🔂 Monitoring	Inbound Traffic (WAN to LAN)	
👷 Utility 💦 🖇		
System Maintenance	Fragmented Large Packets Pass Block	
	Note: Certain gaming and streaming services required this traffic to be passed.	
Virtual Controller	IPv4 Routing Connections Pess Block	
S→ Wireless →	Isale Montrill Fourier Cronics NST2 Block	
📰 Switch	IPv6 Routing Connections Pass Block	
	Cancel Apply	

Item	Description		
Outbound Traffic (LAN to WAN)			
IP Filters Default Action	Define the default action for the outgoing packets that do not match any IP filter rule.		
	Pass –The packets that do not match any IP filter rule will be passed and next wait for the content filter.		
	Block – The packets that do not match any IP filter rule will be blocked by Vigor system.		
Enable Content Filters Default Rule	Switch the toggle to enable or disable the function.		
Content Filters Default Rule	Define the default action for the outgoing traffic that match the following Content Destination rule.		
	If the outgoing traffic doesn't match any IP/content filter rule and the		

	IP Filters Default Action is PASS, it will be checked with this rule additionally.
	If the outgoing traffic meets the above conditions but still doesn't meet the following Content Destination rules, the system will perform the action reversely.
	Pass –The outgoing traffic that matches the following Content Destination rule will be passed. Otherwise, it will be blocked.
	Block – The outgoing traffic that matches the following Content Destination rule will be blocked. Otherwise, it will be allowed to pass through.
Content Destination	Select specific WCF and/or APPE and/or UCF (keyword object) profile to be included in the filter.
	Inbound Traffic (WAN to LAN)
Fragmented Large Packets	Certain games and video streaming service use fragmented UDP packets to transfer data.
	Pass - The router always passes fragmented packets without reassembling them, regardless of the size of the packet.
	Block - The router will attempt to reassemble fragmented packets up to a certain value (e.g., 15xx~2102) kilobytes long. Packets larger than the certain value will be discarded.
IPv4 Routing Connections	Pass – For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, select this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on private LAN subnets.
	Block - Block the LAN hosts from connecting to WAN hosts using IPv4.
IPv6 Routing Connections	Pass – IPv6 does not make use of Network Address Translation (NAT), so all LAN hosts receive public IPv6 IP addresses that are exposed to the WAN.
	Block - Block the WAN hosts from connecting to LAN hosts using IPv6.
Syslog	Enable Syslog – If enabled, the log related to default filter will be recorded to Syslog.
Cancel	Discard current settings and return to the previous page.
Apply Save the current settings.	

II-2-1-5 Backup & Restore

This page allows the backup and restoration of router settings.

In addition to restoring Vigor C410/C510's own configuration backup, it is possible to restore backups from certain DrayTek routers on Vigor C410/C510.

Statement of the local division of the local	Security / Firewall Filters		
Device Menu	IP Reputation Filters IP Filters Content Filters Default Filters Backup & Restore		
 Dashboard 			
Configuration	Backup & Restore		
Security	Backup		
Defense Setup	Selected Item 🗧 Select All		
MAC Filtering Profile	IP Filters		
IPv6 Address Security	Content Filters		
Security Defense Status	Default Filters		
URL/IP Lookup	Back up		
Ja IAM ⇒	and an		
	Restore		
🖸 Monitoring >			
BS Utility >	Restore from Backup File 🖻 Restore		
🖏 System Maintenance 🔗			
Virtual Controller			
}⊷ Wireless ⇒			
🚍 Switch 🤉			
Long-			

Available settings are explained as follows:

ltem	Description
Backup	Selected Items – Select the item(s).
	Backup - Perform the configuration backup of this router based on the item (Selected All, IP Filters, Content Filters and Default Filters) selected above.
Restore	Restore from Backup File – Click the button to specify a file to be restored
	Restore - Click to initiate restoration of configuration. If the backup file is encrypted, you will be asked to enter the password.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

II-2-2 Defense Setup

II-2-2-1 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are several types of detect / defense function in the **DoS Defense** setup. In default, the DoS Defense is disabled.

	-	Security / Defense Setup		() Reset
Device Menu	-	Defense Setup		
 Dashboard 				
Configuration	.>	DoS Defense BFP Settings	Allow/Block List Defense Syslog	
		Enable DoS Defense	C39	
Firewall Filters Defense Secup		ARP Spoofing Defense		
MAC Filtering Profile		Block ARP replies with	Inconsistent Source MAC addresses.	
IPv6 Address Security			Inconsistent Destination MAC addresses.	
Security Defense Status		Virtual MAC Address in ARP Table (VRRP)	Accept Decline	
URL/IP Lookup		1		
1 IAM	2	IP Spoofing Defense		
D VPN	5	Block IP Packets with	Inconsistent Source IP addresses from WAN.	
Monitoring	>		Inconsistent Source IP addresses from LAN.	
g Utility	- 2-			
System Maintenance	>			
irtual Controller				
- Wireless	>			
🔓 Switch	.,			
		Cancel Apply		

ltem	Description	
Defense Setup		
Enable DoS Defense	Switch the toggle to enable/disable the DoS Defense.	
Flood Defense	+Add – Click it set profiles for flood defense. Up to 6 profiles can be created.	
	Interface – Select a WAN interface.	
	SYN Flood – Switch the toggle to enable/disable SYN flood defense. When the arrival rate of SYN packets exceeds the Threshold value, th router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. This is to prevent TCP SYN packets from exhausting router resources.	
	 SYN Flood Packet Rate – The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively. 	
	ICMP Flood – Switch the toggle to enable/disable the ICMP flood defense. When the arrival rate of ICMP packets exceeds the Threshol value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout.	
	 ICMP Flood Packet Rate – The default values of threshold and timeout are 250 packets per second and 10 seconds, respectively. 	
	UDP Flood – Switch the toggle to enable/disable UDP flood defense. When the arrival rate of UDP packets exceeds the Threshold value, th router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout.	

	 UDP Flood Packet Rate – The default values of threshold and timeout are 5000 packets per second and 10 seconds, respectively.
	 Port Scan – Switch the toggle to enable/disable the Port Scan detection. Port Scans attack your network by sending packets to a range of ports in an attempt to find services that would respond. When Port Scan detection is enabled, the router sends warning messages when it detects port scanning activities that exceed the Threshold rate. Port Scan Packet Rate – The default threshold is 2000 packets
	per second. Option (Edit/Delete) – Click Edit to open the setting page to modify in detail (packet rate and burst rate). Click Delete to remove the selected entry.
General	Switch the toggle to enable/disable the function listed below.
	Block IP Options – If enabled, the Vigor router will ignore IP packets with IP option field set in the datagram header. IP options are rarely used and could be abused by attackers as they carry information about the private network otherwise not available to the external network, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages, etc, which external eavesdroppers can use to discover details about the private network.
	Block Land – Enable to block LAND attacks. LAND attacks happen when an attacker sends spoofed SYN packets with both source and destination addresses set to that of the target system, which causes the target to reply to itself continuously.
	Block SMURF – Enable to block Smurf attacks. The router will ignore any broadcasting ICMP echo request.
	Block Trace Route – Enable to block traceroutes. The router will not forward traceroute packets.
	Block SYN Fragment – Enable to block SYN packet fragments. The router will drop any packets having both the SYN and more-fragments bits set.
	Block Fraggle – Enable to block Fraggle Attacks. Broadcast UDP packets received from the Internet are blocked.
	Activating this feature might block some legitimate packets. Since all broadcast UDP packets coming from the Internet are blocked, RIP packets from the Internet could also be dropped.
	Block Tear Drop – Enable to block Tear Drop attacks. Some clients may crash when they receive ICMP datagrams (packets) that exceed the maximum length. The router discards any fragmented ICMP packets having lengths greater than 1024 octets.
	Block Ping of Death – Enable to block Ping of Death, where fragmented ping packets are sent to target hosts so that those hosts could crash as they reassemble the malformed ping packets.
	Block ICMP Fragment – Enable to block ICMP Fragments. ICMP packets with the more-fragments bit set are dropped.
	Block Unknown Protocol – Enable to block Unassigned Protocol Numbers, and the router will block packets having unassigned protocol numbers. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and
	undefined at this time. Therefore, the router should have ability to

	detect and reject this kind of packets.
	ARP Spoofing Defense
Block ARP replies with	This feature can protect a network from ARP (Address Resolution Protocol) spoofing attacks.
	Inconsistent Source MAC addresses – If the sender's MAC address in the ARP packets does not match the source MAC address from ARP packet's ethernet header, the Vigor system will block the packets immediately.
	Inconsistent Destination MAC addresses - If the target MAC address in the ARP packets does not match the destination MAC address from ARP packet's ethernet header, the Vigor system will block the packets immediately.
Virtual MAC Address in ARP Table (VRRP)	Accept – The virtual MAC address can be recorded in the ARP table. Decline –The virtual MAC address cannot be recorded in the ARP table.
	IP Spoofing Defense
Block IP Packets with	IP spoofing defense can prevent unauthorized access and then protect the data integrity to make sure the security of network.
	Inconsistent Source IP addresses from WAN – Blocks the fake IP from WAN. For example, if the source IP address from the WAN interface is LAN subnet IP packets, the Vigor system will block the packets immediately.
	Inconsistent Source IP addresses from LAN – Blocks the fake IP from LAN. For example, if the source IP address from the LAN interface is WAN subnet IP packets, the Vigor system will block the packets immediately.
	Syslog
Enable Syslog	All Defense Logs – Check the box to record all defense logs onto the Syslog.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

II-2-2-2 BFP Settings

BFP is the abbreviation of Brute Force Protection.

Any client trying to access into Internet via Vigor router will be asked for passing through user authentication. Such feature can prevent Vigor router from attacks when a hacker tries every possible combination of letters, numbers and symbols until find out the correct combination of password.

	Security / Defense Setup		() Reset
Device Menu	Defense Setup		
Configuration	 Do5 Defense BFP Setting 	B Allow/Block List Defense Syslog	
Security	Enable Brute Force Protection		
Firewall Filters Defense Scrup	Login Protection for Service		
MAC Filtering Profile	Service Server	All Server	
IPv6 Address Security		V HTTPS/HTTP	
Security Defense Status		SSH	
URL/IP Lookup		Telnet	
A IMM	×	C FTP	
VPN	>	SNMP	
	×	TR069	
SS utility	2.1	O IAM	
🖏 System Maintenance	*		
	Protection Rules		
Virtual Controller			
}→ Wireless	> IAM Users	Enable Maximum Login Attempts Penalty Period () Enable User Account Lockout Login Attempts Unlock User Account After Email	Notification
🗃 Switch	×		
	Cancel Apply		

ltem	Description	
Enable Brute Force Protection	Switch the toggle to enable or disable the detection of brute force login attempts.	
	Login Protection for Service	
Service Server	BFP can protect the Vigor router's login feature from hacker attacks attempting to crack accounts and passwords through protocols such as HTTPS/HTTP, SSH, Telnet, FTP, SNMP, TR-069, VPN, IAM, and more.	
	The default setting is All Server .	
	Protection Rules	
IAM Users	Define the protection rules for IAM users (e.g., using FTP and IAM service.	
	Enable –Switch the toggle to enable or disable the defense setup settings for the IAM users.	
	Maximum Login Attempts – Specify the maximum number of failed login attempts before further login is blocked.	
	The users who fail to log in multiple times by reaching the maximum login attempts will be penalized a period not to login Vigor system (e.g., using FTP and IAM Service).	
	Penalty Period – Set the period for penalty delay.	
	During this period, the user cannot log in. This setting aims to preven outside automated attacks that attempt to guess passwords, authentication codes, or other credentials through repeated trials.	
	Enable User Account Lockout – Switch the toggle to enable or disable the IAM users account lockout function.	
	Login Attempts – Set a maximum number of failed login attempts for all user accounts. After reaching this limit, the IAM user account will be locked if login fails (e.g., through FTP or IAM Service).	
	Unlock User Account After – Set a time period to unlock specific IAM user accounts.	
	Email Notification – Send a notification to the account via an e-mail when lockout event happened to the user.	

VPN	Define the protection rules for VPN connection.
	Enable –Switch the toggle to enable or disable the defense setup settings for the VPN connection.
	Maximum Login Attempts – Specify the maximum number of failed login attempts before further login is blocked. The users who fail to log in multiple times by reaching the maximum login attempts will be penalized a period not to login Vigor system.
	Penalty Period – Set the period for penalty delay.
	During this period, the user is unable to log in or access Vigor's system. This setting aims to prevent outside automated attacks that attempt to guess passwords, authentication codes, or other credentials through repeated trials.
	Email Notification - Send a notification to the account via an e-mail when lockout event happened to the user.
System Account	Define the protection rules for the system account (User and Administrator).
	Enable – Switch the toggle to enable or disable the defense setup settings for the system account.
	Maximum Login Attempts – The System Accounts who fail to log in multiple times by reaching the maximum login attempts will be penalized a period not to login Vigor system (e.g., using HTTPS/HTTP, SSH, Telnet, SNMP, and TR069 Service).
	Penalty Period – Set the period for penalty delay.
	During this period, the user is unable to log in or access Vigor's system. This setting aims to prevent outside automated attacks that attempt to guess passwords, authentication codes, or other credentials through repeated trials.
	Enable User Account Lockout –Switch the toggle to enable or disable the System Account lockout function.
	Login Attempts – Specify the maximum number of failed login attempts for all System Accounts. After that, the System Accounts will be locked if login failed (e.g., logging into HTTPS/HTTP, SSH, Telnet, SNMP, and TR-069 Service).
	Unlock User Account After – Specify a time period to unlock specific system account.
	Email Notification - Send a notification to the account via an e-mail when lockout event happened to the user.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

II-2-2-3 Allow/Block List

Define the white list and the black list for the clients.

Participation in the second seco	Security / Defense Setup	(1) Reset
Device Menu	Defense Setup	
 Dashboard 		
Configuration >	DoS Defense BFP Settings Allow/Block List Defense Syslog	
Second .	DoS Defense	
Firewall Filters	Priority for Conflicts Allow List first-Pass 🗸	
Onforme-Setup MAC Filtering Profile	Allow List	
IPv6 Address Security Security Defense Status	+ Add M	Ax: 50
URL/IP Lookup	IP Address	
Да IAM ⇒		
🔁 Monitoring 5		Are: 50
88 Utility >	Object & Group	
🐁 System Maintenance >		
Virtual Controller	Block List	
S→ Wireless S		
📰 Switch >	+ Add Mi	ax: 50
	Cancel Apply	

Available settings are explained as follows:

ltem	Description
DoS Defense	Switch the toggle to enable or disable the DoS Defense function.
Priority for Conflicts	 Define the processing order/priority for the conflicts. Allow List first-Pass – Let the IP address listed on the Allow List pass through first. Block List first-Block – Block the IP address listed on the Block List pass through first.
Allow List	Define the IP address(es) of the clients that the packets can be received / delivered via Vigor router.
	+Add – Click to add a new IP address as the member within the allow list.
	• IP Address – Enter the IP address.
	+Add – Click to add a new object / group as the member within the allow list.
	• Object & Group – Use the drop-down list to specify the object & group profile.
Block List	Define the IP address(es) of the clients that will be blocked by Vigor router.
	+Add – Click to add a new IP address as the member within the allow list.
	• IP Address – Enter the IP address.
	+Add – Click to add a new object / group as the member within the allow list.
	• Object & Group – Use the drop-down list to specify the object & group profile.
Apply	Save the current settings.

II-2-2-4 Defense Syslog

Display the type of Syslog provided by Vigor router. Corresponding information related to operation, status, and defense to Vigor router will be recorded to the Syslog server.

a construction of the local division of the	Security / Defense Setup	(i) Reset
Device Menu	Defense Setup	
 Dashboard 	Defense setup	
🛱 Configuration	Do5 Defense BFP Settings Allow/Block List Defense Syrlog	
	1.1.1	
Firewall Filters	Syslog	
	Enable Systog 🛃 All Defense Logs	
MAC Filtering Profile	Flood Defense	
IPv6 Address Security	General Defense	
Security Defense Status	V IP Reputation Defense	
URL/IP Lookup	ARP Spoofing Defense	
A IAM →	IP Spoofing Defense	
	Ali Allow & Block List Logs	
Monitoring	Allow List	
BS Utility >	Sock List	
System Maintenance		
Virtual Controller		
> Wireless >		
。 雷 Switch 。		
and south a		
	Cancel Apply	

Available settings are explained as follows:

Item	Description
Enable Syslog	Select the feature(s). Operation procedure, result or any information related to the feature will be recorded to the Syslog server.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

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

II-2-3 MAC Filtering Profile

Vigor router may restrict wireless access to specified wireless clients only by referencing a MAC address black/white list.

The router's administrator may block wireless clients by inserting their MAC addresses into a black list, or only allow some wireless clients to connect by inserting their MAC addresses into a white list.

II-2-3-1 MAC Filtering Profile

This page allows to set the MAC Filtering Profiles (up to 10) that will be applied to SSID (configured on Configuration>>Wireless LAN>>SSID) to meet different needs.

Concession in the local division in the loca	Security / MAC Filterin	g Profile		③Reset C Refresh
Device Menu	MAC Filtering Profile	Backup & Restore		
(2) Dashboard				
🚔 Configuration	MAC Filtering Profile			
Security	+ Add			Mass 10
Firewall Filters	Name	Policy	Included Devices	Option
Defense Setup				
IPv6 Address Security				
Security Defense Status				
URL/IP Lookup				
A IAM	*			
VPN	*			
	*			
88 Utility	5			
🖏 System Maintenance				
Virtual Controller				
}⊷ Wireless	5			
Switch	Sec. 1			
and the second se				

To add a new profile, click +Add.

licy Disabled Allow List Block List	ype Device List +/	Manual MAC Object MAC Grou		Search	Option	
licy Disabled Allow List Block List De Marcual MAC Object MAC Group vice List + Add + Search Max: 128 Name MAC Address ③ Option	olicy ype Ievice List +/	Manual MAC Object MAC Grou		Search	Option	
vice List + Add Search Max: 128 Name MAC Address () Option	evice List +/	Add		Search	Option	
Name MAC Address ① Option			MAC Address 🕕	Search	Option	
	N	ame	MAC Address 🕡			
(i) Delete					Delete	
	ancel Apply					

ltem	Description	
Name	Enter a string as the profile name.	
Policy	Disabled – Disable this policy.	
	Allow List – Only allow wireless clients whose MAC addresses are listed in the Device list.	
	Block List - Only allow wireless clients whose MAC addresses are not listed in the Device list.	
Туре	Determine which wireless clients can be applied to SSID.	
	Manual – Enter the MAC address of certain device one by one.	
	MAC Object – Select the MAC object(s). All the MAC address under the	

	MAC object will be allowed or blocked.
	MAC Group – Select the MAC group(s). All the MAC objects under the MAC group will be allowed or blocked.
Device List	+Add – Click to add a new device by entering the device name and the MAC address.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-2-3-2 Backup & Restore

This page allows the backup and restoration of MAC filtering profile settings.

Device Menu	Security / MAC Filtering Profile			
 Dashboard 		p & Restore		
🛱 Configuration 5	Backup & Restore			
Ø Security	Download Backup File	Download		
Firewall Filters	Restore from Backup File	6	Restore	
Defense Setup				
MAC Faltering Profile				
IPv6 Address Security				
Security Defense Status				
URL/IP Lookup				
& IAM				
O VPN →				
🔂 Monitoring 🤉				
28 Utility >				
System Maintenance 3				
Virtual Controller				
איץ Wireless א				
물 Switch >				

Available settings are explained as follows:

ltem	Description
Download Backup File	Click to save current configurations for MAC Filtering Profile.
Restore from Backup File	- Click to locate the file for restoring.
	Restore – Click to execute the restoration.

II-2-4 IPv6 Address Security

	Security / IPv6 Address	Security	CRefr
Device Menu	IPv6 Address Securit		
Dashboard	in formula cas becan		
	Generate Interface ID by	Random IDsB4	
Firewall Filters	IPv6 Interface IDs		
Defense Setup	Interface +	IPv6 IIDs	
MAC Filtering Profile	[LAN] LAN1	1d6b:279c:1899:e026	
Security Defense Status URL/IP Lookup	[WAN] WAN1	e9b:b8d3:d510:1b1f	
	[WAN] WAN2	a467:eadc:9a73:6803	
	[WAN] WAN3	<001:ad15:7843:909b	
O VPN		2bc4:ab5c:6c5e:156f	
Monitoring >	[WAN] WAN4	20c4:a05c:0c5e:1507	
88 Utility ;	[WAN] WAN5	2cb5:8d42:1c2c:990a	
🖏 System Maintenance 💡			
	Regenerate Random Int	erface IDs Regenerate	
Virtual Controller			
> Wireless			
🖀 Switch >			
	Cancel Apply		

This page allows you to configure the IPv6 interface ID.

Available settings are explained as follows:

ltem	Description	
Generate Interface ID by	 Select to use Random IIDs or EUI-64 IIDs as the interface ID. Random IIDs EUI-64 	
IPv6 Interface ID	Display the interface and corresponding IPv6 IIDs.	
Regenerate Random Interface IDs	Regenerate - Re-generate the random IIDs for all interfaces.	
Cancel	Discard current settings.	
Apply	Save the current settings.	

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

II-2-5 Security Defense Status

The router's current security protection mechanisms include Brute Force Protection and IP Reputation. This page provides details on the status of these protection mechanisms.

II-2-5-1 BFP Status

Device Menu

Image: Device

This page shows the status of Brute Force Protection.

ltem	Description
IP Address	Displays the IP addresses that have been blocked due to triggering the Penalty or User Account Lockout function when using a System Account (e.g., logging into HTTPS/HTTP, SSH, Telnet, SNMP, and TR-069 Service
Account Name	Displays the account names that have been blocked due to triggering the Penalty or User Account Lockout function when using a System Account (e.g., logging into HTTPS/HTTP, SSH, Telnet, SNMP, and TR-069 Service.
Role	Displays the role of the account.
Service Type	Displays the service type set for the user account.
Blocked Start Time / Blocked End Time	Displays both the start and end times for blocking the IP address.
Hit Count	Displays the number of times a System Account has triggered the Penalty or User Account Lockout.
Option	Unblock – Click to remove the blocked IPs. Add to Block List - Add IPs to the Defense Setup's Allow/Block List.

II-2-5-2 IP Reputation

This page displays the IP Reputation status for the Vigor router regarding both inbound and outbound traffic.

Contraction of the local division of the loc	Security / Secur	ity Defense Status				CRefre
Device Menu	BFP Status	P Reputation				
 Dashboard 						
🚔 Configuration >	IP Reputation	Blocked Report				
	Inbolind (Inte	rnet to Router WAN) Inbound (I	internet to Router LAN) Outb	bound		
Firewall Filters Defense Setup						Maxe
MAC Filtering Profile	Seen at	Source IP (Threat)	Destination IP	Reputation	Attempts	Threat Type
IPv6 Address Security						
URL/IP Lookup						
🔏 IAM 💡						
G Monitoring						
88 Utility >						
🖏 System Maintenance 🥠						
Virtual Controller						
> Wireless						
Switch 5						

ltem	Description
Seen at	Displays the time when the packet matches the specified rule.
Source IP	Displays the IP address of the source of the threat.
Destination IP	Displays the IP address of the destination to which the threat is directed.
Reputation	Displays the score of the IP address.
Attempts	Displays the times of attempts made by the threat towards the target destination.
Threat Type	Displays the type of the threat.

II-2-6 URL/IP Lookup

This page allows you to view various score of specified IP or URL, click the **Look Up** button to see the relevant information. After analysis, the Vigor system will provide relevant information about the IP/URL, including risk level, reputation score, category, and more.

Search Q	Security / URUP Lookup	C Refresh
Device Manu	URL/IP Lookup Metricd URL/IP Context URL/IP URL/IP Note: Enter a URL or IP address to view threat, content and reputation analysis. Look Up	

ltem	Description
Method	 Enter URL/IP – Select this method to look up using URL or IP address. URL/IP - Enter the URL or the IP address of the subject you want to look up. Router WAN IP – Select this method to look up through WAN interface
Look Up	Click to display information related to the IP/URL you look up.In which, the relevant information associated, see below, with the IP address will be shown on the page.• Threat Type• Threat Count• Reputation Score• Average Reputation Score• Organization• Location• Latitude• LongitudeOr, enter the name of the URL. The relevant information associated with the URL will be shown on the page.• Reputation Score• Category• Category Confidence• Popularity• Name Servers• Registrar Name• Created Date• Expired Date

•	Organization
•	Location

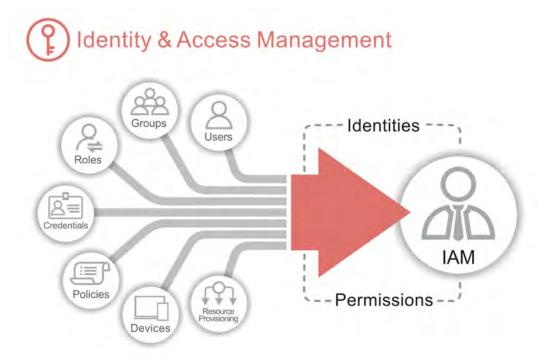
Below shows an example of look up IP/URL:

URL/IP Lookup History						
URL/IP Lookup						
Method	Enter	URL/IP Rou	ter WAN IP			
URL/IP	202.4	3.195.52				
	Note: I	Enter a URL o	or IP address to vie	ew threat, c	ontent and re	putation analys
	Look	dr				
Threat Type						
Threat Count 🕕	2					
	High	n Risk Sus	picious Modera	ate Low	Risk Trust	worthy
	0	20	40	60	80	100
Reputation Score	89					
Average Reputation Score						
	Chang	e at	Reputation Score			
	2022-0	4-08 09:00:56	84			
	2022-0	4-01 09:00:51	80			
	2021.0	7 02 00:00:54	07			

II-3 IAM

Identity and Access Management (IAM) allows the network administrator to manage Internet access at the user level. After a user has been authenticated using a username and password, the user will be granted Internet access and additionally, optional firewall rules and LAN access policies can be applied.

In addition to being used for identification (via user account/VLAN), IAM can also set access policies to control users accessing network, and can be used as a firewall through group policy (group policy) to perform network management.



II-3-1 Users & Groups

Before accessing the Internet through the device, any user must be authenticated by the Vigor system to ensure system security.

This section helps the system administrator create different users and groups profiles as the verification basis.

II-3-1-1 Users

Up to 100 user profiles can be configured in this section.

	Q	IAM / Use	ers & Groups								OR	eset C Refresh
	.	Users	User Groups	Authenti	cation Se	rver						
Jevice Menu		Users										
Dashboard		Gaera										
Seconfiguration	>	+ Add	S OpenVPN	Config Gene	erator						Search	Max: 10
🦻 Security	5	Source	Usemame	Usage	Role	Status	Group Policy	Allow Login from WAN	Created Time	Last Login at	Last Login IP	Option
IAM Policies												
Resources												
Hotspot Web Portal												
Account Status												
Backup & Restore												
D VPN	>											
Monitoring	3											
8 Utility	5											
🔓 System Maintenance	2											
irtual Controller												
⊷ Wireless	5											
🗄 Switch	<u>,</u>											

To add a new user account profile, click **+Add**.

lsername (j)	
Isage	IAM User Router Management
	Note: IAM User: Permits user authentication for VPN, RADIUS, 802.1X, USB, and IAM, but not for router management. Router Management: Enables router management access while disabling VPN, RADIUS, 802.1X, USB, and IAM authentication.
assword ()	@
General Teleworke	r VPN
tatus	Active 🗠
	Active v
oup Policy	
roup Policy xpiration Time	None 🗸
roup Policy xpiration Time ser Information	None 🗸
roup Policy xpiration Time I ser Information nable Email	None ~ Never ~
tatus iroup Policy xpiration Time Iser Information nable Email nable SMS	None v Never v

ltem	Description
Username	Enter the Login name (e.g., <i>LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B</i> , etc.) for this user profile.
Usage	Define the type of this user profile. IAM User – This profile can be used for VPN, RADIUS, 802.1X, USB and IAM (Identity and Access Management) authentication.
	Router Management – This profile is only for router management access and cannot be used for VPN, RADIUS, 802.1X, USB, and IAM authentication.
Password	Password (e.g., <i>lug123, wug123,wug456,</i> etc.) for this user profile.

New Password/ Confirm New Password	When a user tries to access the Internet, he or she must supply a valid user name and password combination for authentication. The profile with matching user name and password will be applied to the session
	General
Status	Active – Enable the general settings in this page. Inactive – Disable the general settings in this page.
Group Policy	It is available if "IAM User" is selected as the usage. Select a group policy profile to be applied by this user profile.
Expiration Time	It is available if "IAM User" is selected as the usage. Set the network connection to work at certain time interval only. All user accounts will apply the time configuration automatically by default. Never – The network connection is always on.
	 Expire in –The network connection will expire and terminate the connection after specified minutes, hours, days, or weeks once built. Expire at – The network connection will expire and terminate the connection on the date and time specified below once built. Date Time Expiration Time
Role	 It is available if "Router Management" is selected as the usage. Administrator Guest Users
Allow Login from WAN	It is available if "Router Management" is selected as the usage. If enabled, the user can login from WAN by using this user account.
User Information	 Enable Email – Switch the toggle to enable or disable the email setting Email – Enter the email address for receiving the MFA PIN code. Send Email Notification to the newly created User – Send a notification email to this user account. Enable SMS – Switch the toggle to enable or disable the SMS setting. SMS - Enter the destination SMS number for receiving the MFA PIN code.
MFA	 Multi-factor authentication (MFA) can offer a more secure network connection. Enable MFA – Switch the toggle to enable/disable the MFA function. Allowed MFA Method - Select to require mOTP, TOTP or 2-step authentication when logging in from the WAN. TOTP – For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone.

	9107					
	Secret: JELUMZERMICUE4JEM/BENYTONE2DERMINIKOARBYNDAWA4DPR65CDQUDEKZAX557P QR Code:					
	iline and					
	In the filed of Validation Code, enter the one-time password and click Verify.					
	Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication SMS/Email – The password will be transferred via the SMS and/or Mail profiles selected from User Information above. mOTP - Mobile one-Time Password (mOTP) allows the use of mOTP passwords. Enter the PIN Code and Secret settings for getting one-time passwords.					
Account Info	Displays general information (created time, last login at and last login IP) for the user account.					
	Teleworker VPN					
	(available if IAM User is selected as the Usage)					
General	Enable Teleworker VPN – Switch the toggle to enable/disable Teleworker VPN configuration.					
	Idle Timeout – If the user is idle over the limitation of the timer, the network connection will be stopped for this user. By default, the Idle Timeout is set to 300 seconds.					
	VPN Schedule – Select Always On (Telework VPN is running all the time). Or choose Scheduled On to make the VPN connection based on the schedule.					
	Before configuring VPN Schedule, add the required time intervals in Configuration>>Objects >>Schedule.					
	Download SmartVPN Client - Click to download the utility of DrayTeck SmartVPN client for building VPN connection.					
Allowed VPN Protocols	Select IPsec, WireGuard or OpenVPN as the protocol for the teleworker VPN connection.					
	IPsec – Switch the toggle to enable the IPsec protocol.					
	If enabled, select IKEv1/v2, EAP and/or XAuth as the IPsec protocol.					
	OpenVPN - Switch the toggle to enable OpenVPN protocol.					
	WireGuard –Switch the toggle to enable WireGuard protocol. If enabled, configure the following settings:					
	• Public Key – Enter the string offered by the remote WireGuard					
	VPN client.					

	 Persistent Keepalive – Default is 60 seconds. If the peer is behind a NAT or a firewall, use the default setting.
Security	Specify VPN Peer – Switch the toggle to enable/disable the security mechanism for the remote client.
	Remote Client IP – Enter the IP address of the remote peer if Specify VPN Peer is enabled.
	Pre-Shared Key – It is available when the IPsec is selected as the Allowed VPN Protocols. "Specify VPN Peer" can restrict the IPsec to be initiated only by the specified peer IP address or domain name, and specify the private key to be used.
	X.509 Digital Signature - It is available when the IPsec is selected as the Allowed VPN Protocols. Accept the certificates authentication. To use an X.509 digital signature, select one of the authentication methods and enter the required information for each method.
	 Disabled – Select to disable the certificate application for VPN connection.
	 Accept Subject Alternative Name –The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.
	 Select from Existing Certificates –Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.
	 Accept Subject Name – Enter the complete certificate subject name.
	 Accept Any – Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid.
	IPsec Advanced Settings – Click to get the following options. Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional).
	 Peer ID – Specify a local ID to be used when establishing a VPN connection using IPsec VPN type. Enter the ID name for the remote client.
	 Local ID (optional) - If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Local IP Assignment	Assign IP By – Select LAN DHCP or Static IP.
	Assign IP from – Select a LAN interface for IP assignment.
	 Static IP – Specify an IPv4 address.
	Assign DNS By – Choose LAN DHCP (the DNS IP will be assigned by Vigor router automatically) or Static DNS . If Static DNS is selected, configure Primary DNS and Secondary DNS.
	 Primary DNS – Enter the IPv4 address for Primary DNS server. Secondary DNS – Enter another IPv4 address for DNS server if required.
	If Static IP is selected,
	Il Static IP is selected,
	 Static IP - Specify an IPv4 address.
Cancel	

To add a new OpenVPN profile, click **OpenVPN Config Generator**.

On this page, you can create configuration required for a remote OpenVPN client to connect to the router and then download it directly or send it to the user via email.

penVPN Config Generato	Dr	3
Specify Server URL by	WAN IP DDNS Profile Custom URL	
WAN IP	Please select ". 🤝	
	Please select 🤟	
Set VPN as Default Gateway	0	
Transport Protocol	UDP ~	
Auto Dial Out		
Cache password for auto reconnect		
UDP Ping		
UDP Ping Exit		
Export Configuration by	Email to Users Download zip file	
Included Users	select your pations	

ltem	Description
Specify Server URL by	The OpenVPN client will use the IP address or domain name to connect to the router.
	WAN IP – The OpenVPN configuration file will use the numeric IP address as the server address.
	• WAN IP – Select the WAN interface.
	DDNS Profile – The OpenVPN configuration file will use the domain name from the DDNS Profile.
	 DDNS Profile – Select a DDNS profile.
	Custom URL – The OpenVPN configuration file will use the user-defined server IP or domain name.
	 Custom URL – Specify a user-defined URL.
Set VPN as Default Gateway	Switch the toggle to enable/disable the function.
	Enable - The Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel.
	Disable - Disable the function.
Transport Protocol	TCP/UDP - Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router.
Auto Dial Out	Switch the toggle to enable/disable the function.

	Enable - The remote client can auto-dial to this Vigor router to build an OpenVPN tunnel.
	Disable - Disable the function.
Cache password for	Switch the toggle to enable/disable the function.
auto reconnect	 Enable - OpenVPN will reconnect per hour. While reconnecting, the password is required. If the function is enabled, the password for OpenVPN connection will be kept and used by the Vigor system for reconnection every time. Disable - Disable the function.
UDP Ping	Ping remote device over the UDP control channel, if no packets have been sent for the number of seconds configured here.
UDP Ping Exit	Let OpenVPN exit after the seconds set here if no reception of a ping or other packet from the remote device.
Export Configuration by	Email to Users – If selected, the Included Users field below will be displayed. The OpenVPN configuration file will be sent to users listed on Included Users.
	 Included Users – Select teleworker users that will receive the configuration from Vigor router.
	 Send Email – Click to email the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections to teleworker users.
	Download zip file – The configuration file for OpenVPN will be stored on the database. If selected, the Download Configuration button below will be displayed.
	 Download Configuration - Click this button to download the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections.
Close	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-3-1-2 User Groups

This page allows you to place multiple user profiles into groups.

Search	Q, IAM / Users & Groups		DReset C
Device Menu	Users User Groups. Authentication Server		
Dashboard	User Groups		
2 Configuration	s + Add		Search_
Security	Group Name	# of Users	Option
	Default	0	// Edit
IAM Policies			
Resources			
Hotspot Web Portal			
Account Status Backup & Restore			
D VPN	*		
Monitoring			
18 Utility			
System Maintenance	2		
Virtual Controller			
≻ Wireless	- 2		
a Switch			

			Available U	lsers		×
Group Name (j)	Group_MKT1		Select User	S	Search	
Selected Users	+ Add	Max: 12		Source	Username	
	Source Username Op	otion		Internal	Sales_Abby	
	Internal Sales_Abby 💼	Delete		Internal	Sales_Bill	
				Internal	Sales_Calvin	
Cancel Apply						Close

To add a new user group profile, click **+Add**.

Available settings are explained as follows:

ltem	Description
Group Name	Enter a name for identification.
Selected Users	+Add – Click to select user profiles to be grouped under the current group profile.
Available Users	It appears after clicking +Add . Selected Users – Select the member from available user profiles.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

M / Users & Groups		🕲 Reset 🔿 Refresh
Sers User Groups Authentication Server		
ser Groups		
+ Add		Search Max: 3
Group Name	# of Users	Option
		/ Edit
Default	1	0 2010

II-3-1-3 Authentication Server

Vigor router can authenticate users using either a built-in (None) or external service (Radius or TACACS+) server.

	IAM / Use	ers & Groups				OReset ORefr
	Users	User Groups Authentica	tion Server			
Pevice Menu	Authenti	ication Server				
Dashboard	0.000					
Configuration	+ Add					M
Security		Server Name	Authentication Type	Server Profile	Hit Count	Option
IAM Policies						
Resources						
Hotspot Web Portal						
Account Status						
Backup & Restore						
O VPN						
Monitoring						
38 Utility						
🖏 System Maintenance						
Virtual Controller						
≻ Wireless						
🖹 Switch						

To create a new authentication server profile, click **+Add**.

sers User Groups Authenticatio	in Server		×
Authentication Server		Server Name	Auth_Server_1
+ Add Server Name	Authentication Type	Authentication Type	RADIUS 🗸
		Server Profile	None 🗸

ltem	Description
Server Name	Enter a name for identification.
Authentication Type	Select the authentication type (RADIUS or TACACS+).
Server Profile	If RADIUS is selected as Authentication Type, the available RADIUS server profiles (created on Configuration>>RADIUS/TACACS+) will be

shown in this area. Select the one you need.			
Cancel	Discard current settings and return to the previous page.		
Apply	Save the current settings and exit the page.		

uthentio	cation Server					
- Add						Max:
	Server Name	Authentication Type	Server Profile	Hit Count	Option	
	Auth_Server_1	TACACS+	None	0	🖉 Edit	🗊 Delete

II-3-2 IAM Policies

IAM Policy contains access policy, group policy and conditional access policy.

II-3-2-1 Apply Policies to LAN

This page is used for selecting access policy and group policy which will be applied to the LAN profile.

Search	Q IAM / IAN	1 Policies						C Refresh
	Apply Pol	Incles to LAN	Access Policies G	roup Policies C	onditional Acces	s Policy		
Device Menu	Apply Po	licies to LAN						
 Dashboard 								
S Configuration	> LAN Ne	hunde		ccess Policy			Group Policy	
Security								
	[LAN] LA	N1		Default_Access_Poli	d~		Disabled ∨	
Users & Groups				Disabled				
				Default_Access_P	olicy			
Resources								
Hotspot Web Portal								
Account Status								
Backup & Restore								
(VPN	*							
🔂 Monitoring	× .							
28 Utility	5							
Nystem Maintenance								
Virtual Controller								
>- Wireless	*							
🖀 Switch	> Cancel	Apply						

ltem	Description
LAN Network	Display the interface that the IAM policy will apply to.
Access Policy	Select an access policy for this interface. Or select Disabled to ignore the setting.
Group Policy	Select a group policy for this interface. Or select Disabled to ignore the setting.

Cancel	Discard current settings.
Apply	Save the current settings.

II-3-2-2 Access Policies

Access Policies can be applied to LAN interface to determine how the users/clients access the Internet via identification authentication.

This page is used for define different access policies for IAM application.

	Q	IAM / IAM Policies			TReset	C Refresh
		Apply Policies to LAN	Access Policies Group Policies Conditional Access Policy			
ievice Menu	_	Access Policies				
Dashboard		Piccess Folicies				
Configuration	5	+ Add		Search		Max: 2
Security	5	Name	Access Control Mode		Option	
		Default_Access_Policy	Disabled, clients can access the network (MFA may still be requested when accessing resources).		@ Edit	Delete
Users & Groups						
Resources						
Hotspot Web Portal						
Account Status						
Backup & Restore						
VPN	5					
Monitoring						
3 Utility	5					
System Maintenance	>					
rtual Controller	-					
Wireless	>					
Switch						

To add a new access policy profile, click **+Add**.

		×
Name 🛈		
Identity Access Control		\sim
	O Disabled, clients can access the network (MFA may still be requested when accessing resources).	
Access Control Mode	MAC Allow/Block List Only	
Access Control Mode	Login with built-in User function	
	Guest Hotspot	
Cancel Apply		

Available settings are explained as follows:

Item Description					
NameEnter a name for identification.					
	Identity Access Control				
Access Control Mode Disabled – All clients/user accounts can access the network.					
	MAC Allow/Block List Only – Allow or deny the clients/user accounts				

	access to the network by the MAC address filter profile.
	Login with built-in User function – The clients will be authenticated before accessing the network.
	Guest Hotspot - Allow or deny the clients/user accounts access to the network based on the hotspot profile selected.
If MAC Allow/Block List C	Dnly is selected as the Access Control Mode.
	MAC Address Filter
Set up MAC Address Filter by	Selecting from Profile – Use pre-defined MAC Filtering profiles as the filtering basis.
	 MAC Filtering Profile - Select one of the MAC filtering profiles (Security>>MAC Filtering Profile) as the filtering basis.
	Manually – Define the MAC addresses and separate them as Allow List or Block List.
	 MAC Address Filter Mode – Select Allow List (allow the clients to access) or Block List (deny the clients access). Then, enter the MAC address of the clients separately on the MAC Address Filter Table.
	• MAC Address Filter Table – Click +Add to enter the MAC address of the client.
If Login with built-in Use	r function is selected as the Access Control Mode
Authentication Mode	Single-Factor - Only identification authentication is required.
	Multi-Factor - Multi-Factor authentication adds an extra layer of security, ensuring that only those users or devices within the Users of VLAN that apply specified Group Policy can access the specified resource.
	MAC Address Filter
Set up MAC Address Filter by	Selecting from Profile – Use pre-defined MAC Filtering profiles as the filtering basis.
-	 MAC Filtering Profile - Select one of the MAC filtering profiles (Security>>MAC Filtering Profile) as the filtering basis.
	Manually – Define the MAC addresses and separate them as Allow List or Block List.
	 MAC Address Filter Mode – Select Allow List (allow the clients to access) or Block List (deny the clients access). Then, enter the MAC address of the clients separately on the MAC Address Filter Table.
	• MAC Address Filter Table – Click +Add to enter the MAC address of the client.
If Guest Hotspot is selec	ted as the Access Control Mode
Hotspot Profile	Select one of the hotspot profiles.
	Login Session Lifetime
Login Session Lifetime	Control the session time for users/clients. After the session's lifetime, the users/clients must log in to access the network, again.
Cancel	Specify the number of days, hours, and minutes.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

Apply Policies to LAN Access P			
Apply I blicles to EAR Access F	olicies Group Policies Conditional Access Policy		
Access Policies			
+ Add	Searc	h	Max: 20
Name Acc	ess Control Mode	Option	
Default_Access_Policy Disa	bled, clients can access the network (MFA may still be requested when accessing resources).	/ Edit	🗊 Delete
Acc_Policy_1 Gue	st Hotspot	/ Edit	🗊 Delete

II-3-2-3 Group Policies

The traditional firewall generally provides a blocking mechanism with IP-based rules to permit or block traffic on designated ports. To more securely manage access privilege, Group Policies provide a better way to help administrators decide permission for specific users, which define limitations and configuration based on role behavior to authorize corresponding restrictions, such as Time and Date Limit, Resources, Firewall Policies, and Traffic Shaping Policies.

This page is used for configuring group policies for IAM application.

	۹							
Device Menu		Apply Policies t	o LAN Access Policies Gr	roup Policies Conditional	Access Policy			
Dashboard		Group Policie	5					
Configuration	5	+ Add					Search	Max: 20
 Ə Security		Name	Allowed Resources.	IPv4 Filters	Content Filters	Traffic Shaping Policies		Option
Users & Groups								
WM Policies								
Resources								
Hotspot Web Portal								
Account Status								
Backup & Restore								
D Abn	2							
Monitoring	>							
8 Utility	5							
👌 System Maintenance	5-							
rirtual Controller								
- Wireless								
冒 Switch	>							

(i) Note:

Once Group Policies are applied to user account/VLAN profile, even if the firewall filter setting has been setup, Group Policies will override rules set at the firewall filter.

To add a new group policy profile, click **+Add**.

		×
Name ()		
Schedule	Always On Scheduled On	
	Note: When group policy is off, network firewall/traffic shaping policies will be enforced.	
Allowed Resources		V
Allowed Resources	+ Add Max: 50	
	Resource Conditional Access Policy Log	
	No Records Foundt	
Firewall Policies		~
Firewall	Use Network Default 🛛 🗸	
Cancel Apply		

ltem	Description
Name	Enter a name for identification.
Schedule	Always On - The function of group policy is running all the time.
	Scheduled On - The function of group policy is activated based on the schedule profile.
	Allowed Resources
Allowed Resources	Select resources profile(s) and apply to this policy profile.
	+Add – Click to add a new resource profile.
	Resource – Use the drop-down menu to select IP or MAC resource profile.
	Conditional Access Policy – Use the drop-down menu to select access condition profile.
	Log – Select Pass or Block or Both. Corresponding records (related to passing or blocking packets) will be stored as a log.
	Option (Delete) – Click to remove the entry.
	Firewall Policies
Firewall	Use Network Default – Select this item to use the default group firewall filter settings.
	Customize Group firewall filters – Select this item to customize the group firewall filter settings. The firewall policy will be applied to allowed resources defined above.
If Customize Group fire	wall filters is selected as the Firewall
Outbound IPv4 Filters	+Add – Click to add new IPv4 filter profiles (up to 10) for outgoing traffic.
	Name – Set a name that identifies the IP filter profile. The maximum length of the Profile Name is 15 characters.
	Destination IP Start – Enter an IP address as the starting IP address.

	Destination IP End – Enter an IP address as the ending IP address. If only one static IP address will be filtered by this profile, enter the same IP address as the value in Destination IP Start.
	Protocol – Specify the protocol(s) which this filter rule will apply to.
	Dest Port Start – Specify the target port range (starting point) if the protocol is TCP or UDP.
	Dest Port End – Specify the target port range (ending point) if the protocol is TCP or UDP.
	Action –Select Pass to allow access to the IP address; select Block to disallow access to the IP address.
	Option(Delete) - Click to remove the selected entry.
Content Filters	The system will check the outgoing sessions additionally with the selected content filters profile(s).
	+Add – Click to add a new content filter profile (up to 10).
	Profile Name – Set a name that identifies the content filter profile. The maximum length of the Profile Name is 15 characters.
	Scheduled On - The filter profile will be valid based on the time schedule specified here.
	Destination – Select specific WCF and/or APPE and/or UCF (keyword object) profile to be included in the filter.
	Action – Select Pass to allow access to the Destination; select Block to disallow access to the Destination.
	Enable Keyword Exception – Switch the toggle to enable/disable the function.
	Keyword Exceptions - Display selected keyword objects.
	The system will check the sessions additionally with the selected keyword profile(s). If the session meets the keyword filter profile, the system will perform the action reversely.
	Option(Delete) - Click to remove the selected entry.
IP Filters Default Action	Any packet that does not comply with the rules set in Outbound IPv4 Filters and Content Filters will be processed according to the default action.
	 Pass - Allow access to the IP address.
	• Block - Disallow access to the IP address.
Enable Content Filter	If enabled,
Default Rule	Content Filters Default Action - Any session that does not comply with the above firewall filters rules but matches the content destination rule will be processed according to the default action.
	 Pass - Allow the session pass which is matched Content Destination rule. The outgoing traffic that matches the following Content Destination rule will be passed. Otherwise, it will be blocked.
	 Block - Disallow the session pass which is matched Content Destination rule. The outgoing traffic that matches the following Content Destination rule will be blocked. Otherwise, it will be allowed to pass through.
	Content Destination – Select the WCF and/or APPE and/or UCF (keyword object) profile to be included in the filter. It is treated as an additional content filter rule to determine whether the packets/sessions will be passed or blocked.

Enable Syslog	The filtering result can be recorded according to the setting selected for Syslog.Discard current settings and return to the previous page.	
Cancel		
Apply	Save the current settings and exit the page.	

II-3-2-4 Conditional Access Policy

Different from the Access Policies designed for setting Access Control Mode, this page provides a policy combination of time schedule, source IP, and multi-factor authentication (MFA). It can be used together with the resources.

	Q	IAM / IAM Policies				🕥 Rese
		Apply Policies to LAN	Access Policies Group Policies	Conditional Access Policy		
evice Menu	-	Conditional Access	Policy			
b Dashboard	-					
Configuration	8	+ Add			St	Styre H Maxe :
Security	x	Name	MFA Condition	Source IP Condition	Time Condition	Option
	8					
Users & Groups						
Resources						
Hotspot Web Portal						
Account Status						
Backup & Restore						
VPN	э.					
Monitoring	*					
Utility	×					
System Maintenance	*					
tuai Controller						
Wireless	*					
Switch						

To add a new conditional policy profile, click **+Add**.

		×
Name	Con_Access_100	
Multi-Factor Authentication		
MFA Condition		
Required Reauthentication	When Login Session Lifetime expires within $ \sim 4 \sim 4 \sim $ Hours $ 0 \sim $ Minutes	
Source IP		
Source IP Condition		
Source IP	Permit \checkmark access if source IP is \checkmark from any of following VLAN/IP	
LAN	(LAN) LANT 🛪 🗠	
IP Group	anner son adding.	
Time Schedule		
Time Condition		
Source IP	Permit \sim access if time is \sim Within any of following range	
Cancel Apply		

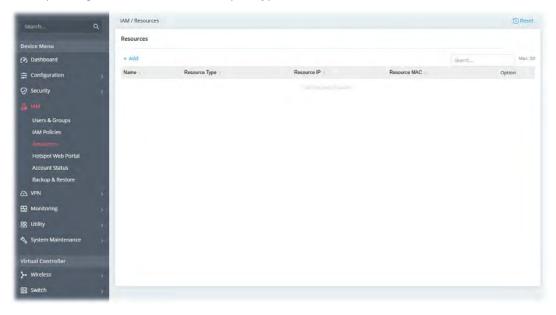
Available settings are explained as follows:

ltem	Description
Name	Enter a name for identification.
	Multi-Factor Authentication
MFA Condition	Switch the toggle to enable/disable the function.

Required Reauthentication	Set the time period for re-authenticating the user when the user wants to access the other IP address (defined in IAM>>Resources).
	Select Everytime or When Login Session Lifetime expires within.
	Vigor system will perform the reauthentication job for users (clients)
	Source IP
Source IP Condition	To Permit or Deny Access if the source IP is from the designated VLAN/IP.
Source IP	Specify the action (Permit or Deny) for the source IP.
LAN	Select an interface.
IP Group	Select an appropriate IP group or multiple IP groups that you would like to include in this policy.
	Time Schedule
Time Condition	Switch the toggle to enable/disable the time schedule.
Source IP	Determine whether you would like to Permit or Deny the source IP.
Schedule Object	Select an appropriate schedule profile or multiple profiles that you would like to apply to this policy.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-3-3 Resources

This page assists to lock down source objects under IAM control by specifying their **IP**, corresponding **MAC** addresses and the port type.



To add a new resources profile (up to 50), click **+Add**.

		×
Name 🕢	ResourcesMAC1	
Resource Type	IP MAC	
Resource IP	192.168.1.47	
Resource Port	All TCP / UDP ports \sim	
Allow ICMP		

ltem	Description
Name	Enter a name for identification.
Resource Type	Select IP or MAC as the resource type.
Resource IP / MAC	Enter the IP address or MAC address according to the resource type selected for this profile.
Resource Port	Select the resource port type. • All TCP/UDP ports - Transmission Control Protocol and User Datagram Protocol • All TCP ports - Transmission Control Protocol • All UDP ports - User Datagram Protocol • All UDP ports - Select this port type and set the port number for TCP/UDP, TCP, or UDP respectively. • Add • Protocol • Port • Option • TCP/UDP • Service Type Object - Up to 12 service-type object profiles can be set in this field. Service Type Object • Add Max: 12 • Add Max: 12 • Option • Click +Add to display the available service type list to the right side. Select the one(s) you want.
Allow ICMP	It's for diagnostic and control purposes, to send error messages abou IP operations, messages about requested services, or messages abou the reachability of a host or router.

Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-3-4 Hotspot Web Portal

The Hotspot Web Portal, or the so-called captive portal allows you to control and manage access from LAN users.

II-3-4-1 Profile Setup

It is also a manner of IAM to identify, authenticate, and authorize any Access from the LAN or redirect to your appointed landing page.

	Q	IAM / Hotspot Web Portal			1 Reset
		Profile Setup Quota Policy Profile Users Information			
levice Menu	-	Profile Setup			
Dashboard		Trone setup			
Configuration		+ Add			Mex: 2
Security	\$	Profile Name	Portal Method	Option	
2 000	-	Default_Hotspot_Profile	Click through	d Edit	@ Preview
Users & Groups					
IAM Policies					
Resources					
Account Status					
Backup & Restore					
) VPN	κ.				
Monitoring					
3 Utility					
System Maintenance					
irtual Controller					
Wireless	*				
3 Switch					

To add a new hotspot profile (up to 2), click **+Add**.

Click Login Method, Login Page Setup, Whitelist Setting, and/or More Options for detailed configuration.

1 Login Method

At present, there are three login methods to choose from for authenticating network clients: **Click Through**, **Skip Login**, **landing page only**, **External Portal Server** and **Various Login**. Each login mode will present a different web page to users when they connect to the network.

		×
1 Login Method 2 Lo	gin Page Setup 3 Whitelist Setting 4 More Options	
rofile Name 🕕	Floor_4_MKT	
	Click through	
ortal Method	Skip Login, landing page only External Portal Server	
	Various Login	
aptive Portal URL	https:// \sim portal.draytek.com	

ltem	Description	
Profile Name	Enter a name for identification.	
Portal Method	Click through – The user will be redirected to the landing page (defined in Captive Portal URL) and be granted access to the Internet.	
	Skip Login, landing page only – This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.	
	External Portal Server - External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.	
	Various Login - An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook account, Google account PIN code, password for RADIUS sever, they will be redirected to the landing page and be granted access to the Internet.	
Captive Portal URL	Enter the captive portal URL.	
Redirection URL	It is available when the External Portal Server is selected as the Porta Method.	
	Enter the URL to which the client will be redirected.	
RADIUS	It is available when the External Portal Server is selected as the Porta Method.	
	If enabled, configure the following settings:	
	External RADIUS Server Profile - To configure the RADIUS server, click the <u>External RADIUS</u> link and you will be presented with the configuration page.	

	Configuration / RADIUS/ TACACS+
	External RADIUS Internal RADIUS External TACACS+
	External RADIUS
	+ Add
	Name Primary Authentication Server Secondary Authen
	RADIUS MAC Authentication – Switch the toggle to enable/disable the function. If the RADIUS server supports authentication by MAC address, enable RADIUS MAC Authentication and select the MAC address format that is used by the RADIUS server.
	MAC Address Format - Select the MAC address format.
	RADIUS NAS-Identifier - Enter an ID.
Login Method	This setting is available when Various Login is selected as the portal method.
	Choose Login Method - Select one or more desired login methods.
	Facebook
	Google
	PIN via SMS
	PIN via Mail
	RADIUS
	Leave Info
	Facebook - This setting is available when Facebook is selected as the
	login method.
	Facebook APP ID - Enter a valid Facebook developer app ID.
	 Facebook APP Secret - Enter the secret configured for the APP ID entered above.
	Google - This setting is available when Login with Google is selected as
	the login method.
	• Google App ID - Enter a valid Google app ID.
	 Google App Secret - Enter the secret configured for the APP ID entered above.
	PIN via SMS - This setting is available when Receive PIN via SMS is selected as the login method.
	• SMS Provider - Select the SMS Provider to send PIN notifications.
	• SMS Content – Enter a message.
	PIN via Mail - This setting is available when Receive PIN via Mail is selected as the login method.
	• Mail Server - Select the mail server to send PIN notifications.
	• Mail Content – Enter a message.
	Table (for Leave Info) – This setting is available when Leave Info is selected as the login method.
	• +Add – Click to add a new entry (up to 10) of leave info.
	 Info Type – Select the information (e.g., General Info, Phone, Email or Checkbox) that the client needs to offer for connection.
	 Required – If enabled, items on the login page will ask for entering required information for further connection.
	• Title – Enter the heading of the Leave Info.
	 Content – Enter the placeholder for the Leave Info.
	• Option (Delete) – Click to remove the selected entry.

Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

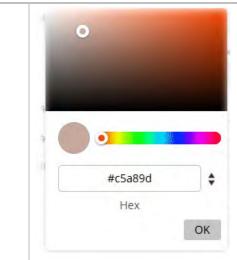
2 Login Page Setup

If you have selected a Login Mode that requires authentication, click **Login Page Setup** to select a background for the login page.

1 Login Method 2 Lo	ogin Page Setup 3 White	ist Setting 4 More	Options	
ogin Page background				
	Property			
lackground Image	None Upload Im	age		
Custom Logo	None Upload Im-	age HTML		
	None Upload Im Draytek Hotspot Serv			
Browser Tab Title				
Browser Tab Title			Box Color	
Custom Logo Browser Tab Title Color Scheme	Draytek Hotspot Serv	lice	Box Color Button Text Color	
Browser Tab Title	Draytek Hotspot Serv Background Color	Text Color		

Available settings are explained as follows:

ltem	Description
	Login Page background
Background Image	Set the login page background scheme.
	None – No image will be used.
	Upload Image – Click to select an image file (.JPG or .PNG format) as the background image. The file size must be less than 5MB.
	• Current Background Image – Click Upload to upload the selected file to Vigor router system.
Custom Logo	Set a logo displayed on the portal.
	None – DrayTek default logo will be used.
	Upload Image – Click to use another image as the logo. The file size must be less than 1MB.
	• Current Logo Image – Click Upload to store the selected file to Vigor router system.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.
Color Scheme	Set the color used for the background, text, box, link, button and button text. A color box will appear for you to drag your mouse cursc on it to choose the color you want.



Set the opacity (0 – 100%) of the background image.					
Set the transparency (0 – 100%) of login column.					
Enter the text to be displayed as the welcome message.					
Select Internal Content or External Content.					
Internal Content - Enter the text to be displayed in the Terms and Conditions pop-up window.					
External Content - Enter a URL. After clicking the link of Terms and Conditions on the hotspot login page, the client will be redirected to access the web page of the URL specified here.					
Enter the text to inform the user.					
Discard current settings and return to the previous page.					
Save the current settings and exit the page.					

3 Whitelist Setting

In this page you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

1 Login Method 2 Login Page Setup 3 Whitelist Setting	4 More Options
Destination Domain/IP	
+ Add Max: 30	
Enabled Destination Domain/IP Whitelist ①	
Destination Port	
+ Add Max: 30	
Enabled Destination Port Whitelist Port 🕧	
Destination Groups	
Destination Objects/ Groups select group options	
Source IP	
Cancel Apply	

Available settings are explained as follows:

ltem	Description
	Destination Domain/IP
+Add	Enabled – Switch the toggle to enable/disable the setting.
	Destination Domain/IP Whitelist – Please enter IP address or domain name without the 'http://' or 'https://' prefix.
	Option (Delete) – Remove current entry.
	Destination Port
+Add	Enabled – Switch the toggle to enable/disable the setting.
	Destination Port Whitelist – Select TCP, UDP, or TCP/UDP. The, enter the port number.
	Option (Delete) – Remove current entry.
	Destination Groups
Destination Objects/ Groups	Select one IP object/group or multiple IP objects/groups as the destination.
	The selected groups are allowed to be accessed.
	Source IP
+Add	The selected IPs are allowed through the router.
	Enabled – Switch the toggle to enable/disable the setting.
	Source IP Whitelist – Enter the IP address.
	Option (Delete) – Remove current entry.
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.

4 More Options

1 Login Method	2 Login Page Setup	3 Whitelist	t Setting	4 More Options				
Quota Management.		2 1111213	, Section (S					
Login Methods	Quota Policy Profile	Valid Time	Idle Timeout	Allowed device #	Reconnection Time Restriction	Block Users	Bandwidth Limit (Mbps)	Session Limit
Click Through	Disable 😒							
Skip Login	Disable 🗸							
External Portal Server	Disable ∽							
Facebook Login	Disable 🗠							
Google Login	Disable ∽							
SMS Login	Disable 🗠							
Email Login	Disable 🗠							
RADIUS Login	Disable 🗠							
LeaveInfo	Disable 😒							

In this step you can configure **advanced** options for the Hotspot Web Portal.

Available settings are explained as follows:

ltem	Description					
Quota Management						
Login Methods	Show different login methods. Set individual quota policy profiles for each method.					
Quota Policy Profile	Specify a quota policy profile for each login method. The default is Disable .					
	Go to IAM>>Hotspot Web Portal>>Quota Policy Profile to configure several profiles, if required.					
Landing Page After Authentication						
Landing Page After Auth	Fixed URL – Specifies the webpage that will be displayed after the user has successfully authenticated.					
	The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.					
	User Requested URL - The user will be redirected to the URL they initially requested.					
Cancel	Discard current settings and return to the previous page.					
Apply	Save the current settings and exit the page.					

II-3-4-2 Quota Policy Profile

The system administrator can set restrictions on valid time, idle time, reconnection time, bandwidth, and session quotas that apply only to the web portal clients.

Search	a	IAM / Hotspot V	Veb Portal						3 Re	set CRE	fresh
Landau and		Profile Setup	Duota Polic	y Profile Us	ers information						
Device Menu	-	Quota Policy F	Profile								
(P) Dashboard		quotar oney i	(unit								
n Configuration		I Add									Maje 4
Security		Profile Name	Valid Time	Idle Timeout	Allowed Device #	Reconnection Time Restriction	Block users	Bandwidth Limit (Mbps)	Session Limit	Option	
J. 1044											
Users & Groups											
IAM Policies											
Resources.											
Account Status											
Backup & Restore											
VPN	à.										
🖽 Monitoring	×										
BS Utility	×										
🖏 System Maintenance	5										
Virtual Controller											
>- Wireless	*										
🔠 Switch	×										

To add a new quota policy profile, click **+Add**.

					0
 Only apply on Web Porta 	l Clients, the polic	ies take precedence o	ver Bandwidth Managen	nent.	
Profile Name	Quota_Policy				
Account Validity					
Valid Time	10	1	10		
Enable Idle Timeout					
Device Control					
Limited Device / Account.					
Limited Device / Account Reconnection Time Restriction	No by	Time by Period			
	No by	Time by Period	Block users		

Available settings are explained as follows:

ItemDescriptionProfile NameEnter a name as the profile name.					
Valid TimeConfigure the validity duration for login by setting days (0-180), (0-23), and minutes (0-59).Once the login period expires, the Vigor router will disconnect to the login period expires.					

	client from accessing the network or the Internet. If the client wishes to log in again, they will need to be verified or authenticated by the Vigor router.
Enable Idle Timeout	When this option is enabled, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed.
	Idle Timeout – Enter a number (1-480, minutes).
	Device Control
Limited Device / Account	Set the maximum number of devices that can be connected for each account, and the time restriction for the client accessing Internet via the web portal.
	Switch the toggle to enable or disable the function.
	If enabled, set the number of Allowed device.
	Allowed device # – Set the maximum number of devices that can be connected for each account, and the time restriction for the client accessing Internet via the web portal. The maximum is 100.
Reconnection Time Restriction	Blocks the account from being used to connect devices to the network in one of three ways:
	No – No block.
	by Time – After the login expires, the account cannot be used to connect devices to the network until the set time of day.
	 Block users before – Choose the deadline (hour and minute) from the drop-down menu. When the time expires, the user's access will be disconnected and blocked.
	by Period – After the login expires, the account cannot be used to connect devices to the network for a set period of time.
	 Block users for – Enter the number of hours and minutes to specify the user block period.
	Bandwidth & Session Limit
Bandwidth Limit	Set the maximum upload and download speeds. Switch the toggle to enable or disable the function. If enabled, configure the following settings:
	Upload Limit / Download Limit –Enter a number (1 to 9999).
Session Limit	Configure a maximum session limit for web portal clients.
	Switch the toggle to enable or disable the function.
	If enabled, configure the following setting:
	Sessions – Enter a number (1 to 50000).
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-3-4-3 User Information

This page provides details about users (web portal clients) connected to this router.

	IAM / Hotspot	Web Portal						CR	etrest
	Profile Setup	Quota Policy Prof	Ne Users Informat	ion					
evice Menu	Users Inform	nation							
Dashboard	and the second second								
Configuration	Online Users		0						
Security	All Users		0						
Users & Groups	🕑 Export as T	XT Z Export as JSC	ON Export as CSV				Filter: All Profile	✓ Search	
IAM Policies	Status	Profile	User Login Method	is IP	MAC Expire	ed Time Email	Phone Number	Custom Info	
Resources									
Account Status									
Backup & Restore									
2 VPN									
2 Monitoring									
8 Utility									
System Maintenance									
irtual Controller									
• Wireless									

ltem	Description
Online Users	Display the number of online users connected to the Internet via the Vigor router.
All Users	Display the total number of users (both online and offline) connecting to the Internet through the Vigor router.
Export as TXT	Click to export the user information as a TXT file.
Export as JSON	Click to export the user information as a JSON file.
Export as CSV	Click to export the user information as a CSV file.
Filter	Display the hotspot web portal profiles.

II-3-5 Account Status

This page displays the status of Brute Force Protection for the IAM user account (e.g., using FTP and IAM Service).

	Q	IAM / Account St	atuş					C Refresh
Device Menu		Brute Force Pro	otection Status					
 Dashboard 							Search	Max: 20
Configuration		IP Address	Username/Profile Name	Service Type	Blocked Start Time	Blocked End Time	Hit Count	Option
- o ∋ Security								
Users & Groups								
IAM Policies								
Resources								
Hotspot Web Portal								
Backup & Restore								
VPN	2							
Monitoring	\$							
Utility								
System Maintenance	ż.							
	-							
rtual Controller	-							
Wireless	5							
🖁 Switch	*							

ltem	Description
Hit Count	Displays the number of times a IAM user has triggered the Penalty or User Account Lockout.
Option	Unblock – Click to remove the blocked IPs. Add to Block List - Add IPs to the Defense Setup's Allow/Block List.

II-3-6 Backup & Restore

This page can be used to backup/restore the IAM configuration.

	q	IAM / Backup & Restore	
Device Menu		Backup & Restore	
	-		
Dashboard		Backup	
Configuration	2	Selected nem	Select All
Security			Users & Groups
			Access Policies
Users & Groups			Group Policies
IAM Policies			Conditional Access Policy
Resources			🖉 Resources
Hotspot Web Portal		Password Protection	0
			Back up
D VPN	5		
Monitoring	5	Restore	
28 Utility	2	Restore from Backup File	ET Resorre
🖇 System Maintenance	2	File has Password Protection	
	-	Password	٥
- Wireless			
🖁 Switch	2		

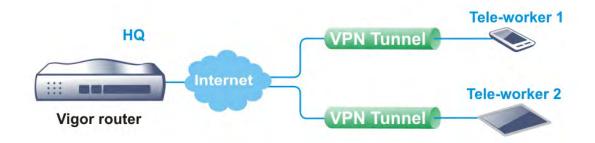
Item	Description			
Backup				
Selected Item Select the policy or policies for the configuration backup.				
Password Protection	For the sake of security, the configuration file for the access point can be encrypted.			
	Switch the toggle to enable/disable the function.			
	New Password – Enter a string as the new password.			
	Confirm New Password – Enter the string again for confirmation.			
	Back up – Click to save the settings.			
	Restore			
Restore from Backup	Click to locate the file for restoring.			
File	Restore - Click to execute the restoration.			
File has Password Protection	Switch the toggle to enable/disable the function. If enabled, a password will be required for restoring the configuration.			
	Password – Enter a string used for configuration restoration.			

II-4 VPN

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Here are some uses of VPNs:

- Communication between home office and customer.
- Secure connection between Teleworker, staff on business trip and main office.
- Exchange data between remote office and main office.
- POS between chain store and headquarters.
- Circumvention of Internet censorship that filters websites or contents.
- Circumvention of geolocation techniques employed by service providers or vendors to block or restrict services to users.
- Secure communications over public access points



II-4-1 General Setup

This section offers general settings for the VPN server with different types (e.g., IPsec, WireGuard and OpenVPN).

II-4-1-1 Access Control

Administrators can establish a secure VPN connection by configuring the interfaces allowed for VPN dial-in and pairing them with a whitelist or blacklist of VPN source IP addresses.

search Q	VPN / General Setup	(1) Rese
	General Setup	
evice Menu		
ን Dashboard	Access Control EasyVPN IPsec WireGuard OpenVPN VPN MS5	
Configuration	the second se	
Security >	Accept VPN Connections on All Interface Specified Interface	
IAM S	VPN Access Control Mode Allow All Connections ~	
y .994		
commol Smup		
Site-to-Site VPN		
Teleworker VPN		
VPN Connection Status		
Backup & Restore		
Monitoring >		
) Utility		
System Maintenance		
rtual Controller		
• Wireless		
switch ,		

Available settings are explained as follows:

ltem	Description
Accept VPN Connections on	It can filter trusted VPN connections by setting up IP object/group allow lists or block lists.
	Select the WAN interfaces to accept VPN connections.
	All Interfaces – Accept the VPN connections on all WAN interfaces.
	Specified Interface – Customize the WAN interface, IP address, and VPN protocols which allow the VPN connections.
	+Add – Click to add up to 8 settings.
	• WAN – Select the WAN interface.
	 IPv4 – Select the WAN IP address (Default WAN IP) or disable this option.
	 Allowed VPN Protocols – There are four protocols (IPsec, WireGuard, OpenVPN and EasyVPN). Select the one(s) allowed for VPN connection.
	• Option – Click Delete to remove the selected interface.
VPN Access Control Mode	It can filter trusted VPN connections by setting up IP object/group allow lists or block lists.
	Allow All Connections – Accept the VPN connections from all clients.
	Allow List – Accept VPN connections from users within the IP object/group settings selected below.
	• +Add - Click to have a new entry setting.
	Block List – Deny VPN connections from users within the IP object/group settings selected below.
	• +Add - Click to have a new entry setting.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-4-1-2 EasyVPN

The Vigor router supports multiple VPN protocols, including IPsec, WireGuard, and OpenVPN. However, general users may find it challenging to choose the right protocol or may face difficulties during the VPN setup. Additionally, environmental factors can sometimes prevent a successful VPN connection. To address these issues, the Vigor router introduces a new protocol called EasyVPN, designed to simplify the process.

With EasyVPN, users no longer need to generate keys for WireGuard, import configuration files for OpenVPN, or upload certificates. To establish a successful VPN connection, users simply need to enter their username and password or obtain an OTP code via email.

Moreover, if a VPN connection cannot be established for any reason, the Vigor system will automatically switch the EasyVPN connection to the next available protocol and attempt to reconnect.

SearchQ	VPN / General Setup	
evice Menu	General Setup	
evice Menu b Dashboard	Access Control EasyVPN IPsec WireGuard OpenVPN VPN MSS	
Configuration s		
	Enabled	
	Listen Port Mode Fortow HTTPS WAN Access Port Customite	
, IAM 5	Listen Port ()	
	Note: If MTTPS IPv4 WAN access is disabled or restricted by an Access Control List, you misst customize the port.	
Site-to-Site VPN Teleworker VPN	VPN Type Preference Preference VPN Protocols	
VPN Connection Status	1 IPsec	
Backup & Restore	2 WireGuard	
Monitoring	3 OpenVPN	
utility		
System Maintenance		
rtual Controller		
Wireless >		
Switch 5		
	Cancel Apply	

Available settings are explained as follows:

ltem	Description	
Enabled	Switch the toggle to enable/disable this service.	
Listen Port Mode	Configure the ports that the EasyVPN service listens to.	
	Follow HTTPS WAN Access Port – For the EasyVPN service, use the same port as the HTTPS management port. Ensure that HTTPS management from the WAN is enabled to allow communication between the EasyVPN client and the EasyVPN server.	
	Customize – Select to define the listening port number manually.	
	• Listen Port – Enter a port value (1-65535).	
VPN Type Preference	This feature enables users to customize the priority of their Dial-In VPN connections. By default, the order is based on VPN performance, arranged as follows: IPsec VPN > WireGuard VPN > OpenVPN.	
	To change the order, simply drag and rearrange the items in the provided interface.	
	Preference – Display the order of the VPN protocols.	
	VPN Protocols – Display the name of the VPN protocols.	
Cancel	Discard current settings and return to the previous page.	
Apply	Save the current settings and exit the page.	

II-4-1-3 IPsec

IPsec (Internet Protocol Security) encrypts and authenticates network traffic, ensuring secure data transmission over VPNs. It protects against unauthorized access, data tampering, and eavesdropping, making it ideal for remote work, site-to-site and teleworker connections, while safeguarding sensitive information across untrusted networks.

Search Q	VPN / General Setup	3 Reset
Device Menu	General Setup	
 Dashboard 	Access Control EasyVPN IPsec WireGuard OpenVPN VPN MSS	
🚊 Configuration		
Security	Enabled C	
Д им >	Authentication Settings for Dynamic Peer	
25 VPN	Certificate 🖂	
General Series	Preferred Local ID Alternative Subject Name 🔗 😔	
Site-to-Site VPN Teleworker VPN	General Site-to-Site PSK	
VPN Connection Status	Pre-Shared Key ()	
Backup & Restore	Preshared key ()	
🖼 Monitoring 💦 🗧	XAuth User PSK	
😫 Utility 🔗	Pre-Shared Key (j)	
🖏 System Maintenance 💦		
Virtual Controller		
> Wireless		
Switch >		
100	Cancel Apply	

Available settings are explained as follows:

ltem	Description
Enabled	Switch the toggle to enable/disable the settings.
	Authentication Settings for Dynamic Peer
Certificate	Select a router VPN server certificate. It will be used for X.509 authentication in the IPsec connection.
	To set up certificates on the router, go to the Configuration>>Certificates section.
Preferred Local ID	Select Alternative Subject Name or Subject Name. Specify the preferred local ID information (Alternative Subject Name or Subject Name) for IPsec authentication.
General Site-to-Site PSK	Pre-Shared key - Define the PSK key for general authentication.
XAuth User PSK	Pre-Shared Key - Define the PSK key for IPsec XAuth authentication.
Cancel	Discard current settings and return to the previous page.
Apply Save the current settings and exit the page.	

II-4-1-4 WireGuard

WireGuard is a secure, fast, and modern open-source VPN Protocol. This VPN connection can build a VPN by exchanging private and public keys between VPN servers (e.g., Vigor router) and VPN clients (e.g., WireGuard VPN Client).

Search	à	VPN / General Setup	(3) Reset
Device Menu		General Setup	
(?) Dashboard		Access Control EasyVPN IPsec WireGuard OpenVPN VPN MSS	
	>	Enabled	
Security			
Se IAM	5	Listen Port ① 51920	
		Default Key Pairs	
General Selup Site-to-Site VPN Teleworker VPN VPN Connection Status Backup & Restore		Generate Private Key Generate Private Key Public Key	
Honitoring	2		
BB Utility	×		
🖏 System Maintenance	>		
Virtual Controller			
>- Wireless	2		
📰 Switch	2		
		Cancel Apply	

Available settings are explained as follows:

Item	Description	
Enabled Switch the toggle to enable/disable the settings.		
Listen Port	Enter a port number for WireGuard VPN server. The default number is 51820.	
	Default Key Pairs	
Generate Private Key	Generate – Click to generate keys (private and public) for the VPN server.	
Private Key	Displays the private key generated.	
Public Key	It is required to be configured in the WireGuard VPN client router. After clicking Generate , the public key will be shown on this page.	
Cancel	Discard current settings and return to the previous page.	
Apply	Save the current settings and exit the page.	

II-4-1-5 OpenVPN

The OpenVPN protocol utilizes public keys, certificates, and usernames and passwords to authenticate the client. Traffic is carried over secure channels built upon industry-standard SSL/TLS encryption protocols.

With integrating of OpenVPN, Vigor router can help users to achieve more robust, reliable and secure private connections for business needs.

OpenVPN offers a convenient way for users to build a VPN between the local end and the remote end. There are two advantages of OpenVPN:

- It can be operated on different systems such as Windows, Linux, and MacOS.
- Based on the standard protocol of SSL encryption, OpenVPN can provide you with a scalable client/server mode, permitting multi-client to connect to a single OpenVPN Server process over a single TCP or UDP port.

In terms of credentials, the administrator can choose to let the router generate the certificates, or import certificates issued by third-party certificate authorities (CAs). When the router generates the certificates, it acts as the root CA to issue the trusted CA certificates. If, however, a certificate issued by a third-party CA is used, both the CA's certificate and the issued certificate need to be imported to the router in the Trusted CA Certificate and Local Certificate sections, respectively.

OpenVPN requires the use of certificates. Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.

Search_	a	VPN / General Setup		() Reset
Device Menu		General Setup		
 Dashboard 		Access Control EasyVPN	IPsec WireGuard OpenVPN VPN MSS	
	2			
Security		Enabled		
A IAM	*	OpenVPN Server Setup		
(D) VIII		UDP Enabled		
		UDP Part	1194	
Site-to-Site VPN		TCP Enabled		
Teleworker VPN VPN Connection Statu	<.	TCP Port	1194	
Backup & Restore	-	Cipher Algorithm	AE5-256-CBC 🗸	
Monitoring	5	HMAC Algorithm	SHA256 🗸	
88 Utility	,	Certificate Authentication		
🖏 System Maintenance		Certificate Source	Select from Existing Certificates Router Generate Certificates	
		Server CA	Please Select	
Virtual Controller		Server Certificate	Please Select	
}- Wireless	*			
😁 Switch	*			
		Cancel Apply		

ltem	Description	
Enabled	Switch the toggle to enable/disable the settings.	
	OpenVPN Server Setup	
UPD Enabled	Switch the toggle to enable/disable the UDP protocol for OpenVPN connections. UDP Port - Enter the UDP port number.	
TCP Enabled	Switch the toggle to enable/disable the TCP protocol for OpenVPN connections. TCP Port - Enter the TCP port number.	

Cipher Algorithm	Select the desired cipher algorithm. Two encryption algorithms are supported: AES128, AES192 and AES256. AES256 is more secure than AES128 but may result in lower performance because it incurs higher computational overhead.	
HMAC Algorithm	HMAC stands for Hash-based Message Authentication Code. It is used to validate the data integrity and authenticity of the VPN data. Select the desired HMAC hash algorithm. Two hash algorithms, SHA1 and SHA256, are supported. SHA256 is preferred as it is more robust and reliable than SHA1.	
CertificateSwitch the toggle to enable if you would like to validateAuthenticationcertificate was issued by a trusted CA.		
Certificate Source Select a source for the certificate to be used for OpenVPN. Select from Existing Certificates – Third-party certificates will be for OpenVPN. Router Generate Certificates – Router-generated certificates that be used for OpenVPN.		
Server CAUse the dropdown list to select the trust CA certificate that already been uploaded to the router.To upload more Trusted CA certificates to the router, go to Configuration>>Certificates page and click the Trusted CA obtaining more certificates.		
Server Certificate	Use the dropdown list to select a server certificate that has already been uploaded to the router. To upload more local certificates to the router, go to Certificate Configuration>>Certificates page and click Local Certificate tab for obtaining more certificates.	
	Discard current settings and return to the previous page.	
Cancel	Distaid current settings and return to the previous page.	

II-4-1-6 VPN MSS

MSS is the abbreviation of Maximum TCP segment size.

This page is used to automatically adjust the TCP MSS value within a VPN tunnel. It optimizes packet size to prevent fragmentation and ensure the efficient data transmission over the network.

Search	Q VPN / General Setup		1 Reset
Device Menu	General Setup		
(?) Dashboard	Access Control Ea	SyVPN IPsec WireGuard OpenVPN VPN MSS	
	> Maximum TCP segmen	st cize	
Security	> Mode	Auto Adjustment by WAN MTU Menually	
A IAM) IPSec (512-1301)	1360	
ON YON	WireGuard (\$12-1412)	1360	
General Settin Site-to-Site VPN Teleworker VPN VPN Connection Status Backup & Restore G Monitoring	Oper/VPN(512)452	1360 Note: VPN MSS is the maximum data size that can be sent in a single TCP packet, it should be fragmentation.	e set to a value lower than the networks MTU to prevent
System Maintenance			
Virtual Controller			
⊁ Wireless	>		
🖀 Switch	2		
	Cancel Apply		

Available settings are explained as follows:

ltem	Description	
Mode	Auto Adjustment by WAN MTU – Obtain the MSS value by automatically adjusting it according to the WAN MTU.	
	Manually - Please specify the MSS values for each type to avoid packets cut by MTU during the data transmission period via the VPN connection.	
	IPsec	
	WireGuard	
	OpenVPN	
Cancel	Discard current settings and return to the previous page.	
Apply	Save the current settings and exit the page.	

II-4-2 Site-to-Site VPN

The VPN means a connection between two router's LAN networks, which

• Allows employees in branch offices and head office to share the same network resources.



• Configures the VPN server for inbound connections from other routers.

This page allows to configure the VPN server for inbound connections from other routers.

	VPN / Site-to-Site	VPN			TReset C Refrest
evice Menu	Site-to-Site VPN	4			
b Dashboard	+ Add				Mase 3
Configuration	Profile Name	Enabled	Remote Network	Status	Option
) Security					
IAM.					
General Setup					
Teleworker VPN					
VPN Connection Status					
Backup & Restore					
Monitoring					
Utility					
System Maintenance					
rtual Controller					
Wireless					
Switch					

II-4-2-1 VPN Type - IPsec

IPsec (Internet Protocol Security) encrypts and authenticates network traffic, ensuring secure data transmission over VPNs. It protects against unauthorized access, data tampering, and eavesdropping, making it ideal for remote work, site-to-site and teleworker connections, while safeguarding sensitive information across untrusted networks.

To add a new resources profile (IPsec VPN type), open VPN>>Site-to-Site VPN and click **+Add**.

		×
		Advanced Mode: ON
Profile Name 🕡		
Enabled		
General		~
Direction	Both ~	
Dial-Out Interface Mode	Selected Interface First \sim	
Dial-Out Interface	Auto Select 🛛 🗸	
	Default WAN IP $$	
PN Type	IPsec 🗸 🗸	
Psec Dial-Out Protocol	IKEV1 🗸	
Psec Dial-In Protocol	🕑 IKEv1/v2 🗌 XAuth	
Remote IP/Domain 🕕		
Dial-Out Mode	On Demand Always On Scheduled	
	Note: On Demand VPN will be triggered up when detecting traffic going to remote network.	
Cancel Apply		
concer poppy		

ltem	Description	
Advanced Mode:ON/OFF	Click to show or hide the advanced settings for the site-to-site VPN.	
Profile Name	Enter the name of the profile.	
Enabled	Switch the toggle to enable/disable the settings.	
	General	
Direction	Specify the allowed call direction of this VPN profile.	
	Both – Profile is to be used to initiate (dial out) or accept (dial in) connections.	
	Dial-Out – Profile is to be used to initiate outgoing connections.	
	Dial-In – Profile is to be used to accept incoming connections.	
VPN Type	Select a VPN type for building the VPN connection.	
	Direction on Dial-out – Available VPN type includes:	
	• IPsec	
	OpenVPN	
	WireGuard	
	Direction on Dial-In – Available VPN type includes:	
	• IPsec	
	OpenVPN	
	WireGuard	
	Direction on Both – Available VPN type includes:	
	IPsec	
	OpenVPN	
	Options related to the IPsec VPN type will be changed according to the Direction used.	
	IPsec (with the direction on Both, Dial-In) -	
	 IPsec Dial-In Protocol 	

	Dial-in Allowed Schedule
	IPsec (with the direction on Both, Dial-Out)-
	IPsec Dial-Out Protocol
	Remote IP/ Domain
	Dial-Out Mode
IPsec Dial-In Protocol	Select a protocol to trigger an IPsec VPN connection through the Internet.
	 IKEv1/v2
	• XAuth.
Dial In Allowed	
Dial-In Allowed Schedule	Connect and disconnect according to schedule profiles. Always Allow – Select this option to maintain an always on dial-in
	connection.
	Scheduled –Select this option to make the VPN connection based on
	the schedule.
	• Drop the Active Tunnel when Schedule is Enforced – Switch the toggle to enable/disable the function.
	• VPN Schedule – Use the drop-down menu to specify one VPN
	profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule.
IPsec Dial-Out Protocol	Select a protocol to trigger an IPsec VPN connection through the
	Internet.
	 IKEv1
	• IKEv2
	IKEv2 EAP
	XAuth
Remote IP/ Domain	Enter IPv4 or hostname for the remote VPN server.
Dial-Out Mode	On Demand – The VPN connection will be triggered when detecting traffic going to the remote network.
	Always On – Select this option to maintain an always on dial-out connection.
	Scheduled –Select this option to make the VPN connection based on the schedule.
	• Drop the Active Tunnel when Schedule is Enforced – Switch the toggle to enable/disable the function.
	• VPN Schedule – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required
	time intervals in Configuration>> Objects>> Schedule.
	Username and Password
Username	It is available when XAuth is selected as IPsec Dial-In/Dial-Out Protocol.
	Used by the remote LAN to establish a VPN connection.
Password	It is available when XAuth is selected as IPsec Dial-In/Dial-Out Protocol.
	Used by the remote LAN to establish a VPN connection.
	IKE Authentication for Dial-Out/Both
Dial-Out Settings	It is available when Dial-Out is selected as the Direction and IPsec is

Negotiation	It is available when IKEv1 is selected as IPsec Dial-Out Protocol.
	Select Main mode or Aggressive mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. The default value in Vigor router is Main mode.
	Main Mode – Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPsec session. However, the Aggressive mode is faster.
	Aggressive Mode – Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPsec session. However, the Aggressive mode is faster.
	• Pre-Shared Key – Input the characters as pre-shared key.
Authentication	It is available when using IKEv1 (under Main Mode) or IKEv2 is selected.
	Pre-Shared Key – Select as the authentication method.
	• Pre-Shared Key – Input the characters as pre-shared key.
	Certificate –Select as the authentication method.
	 Local Certificate – Select one of the profiles set in Configuration>>Certificates Local Certificates.
	• Local ID – Select Subject Name or Subject Alternative Name.
	 Peer ID – Select Accept Subject Alternative Name, Peer Certificate Accept Subject Name, Accept Any.
	Select Accept Subject Alternative Name - The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.
	Peer Certificate - Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.
	Accept Subject Name – Enter the complete certificate subject name.
	Accept Any - Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid.
IKE Identifier	Set the local ID and Peer ID for identification.
	Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional).
Local ID	Specify a local ID to be used when establishing a VPN connection using IPsec VPN type.
Peer ID	Enter the ID name for the remote client.
	If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
	IKE Authentication for Dial-In/Both
Dial-In Settings	It is available when Dial-In is selected as the Direction and IPsec is selected as VPN Type.
Negotiation	Select Main mode or Aggressive mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. The default value in Vigor router is Main mode.
	Main Mode – Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPsec session. However, the Aggressive mode is faster.

	Aggressive Mode – Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPsec session. However, the Aggressive mode is faster.
Specify VPN Peer	It is available when IKEv1/v2 is selected as IPsec Dial-In Protocol.
	This feature can restrict this IPsec to be initiated only by the specified peer IP address or domain name, and specify the private key to be used.
	If enabled,
	Remote IP – Enter the IP address of the remote peer.
	Pre-Shared Key – Input characters as pre-shared key for authentication.
X.509 Digital Signature	It is available when IKEv1/v2 is selected as IPsec Dial-In Protocol.
	To use an X.509 digital signature, select one of the authentication methods and enter the required information for each method.
	Select Accept Subject Alternative Name - The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.
	Peer Certificate - Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.
	Accept Subject Name – Enter the complete certificate subject name.
	Accept Any - Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid.
IKE Identifier	Set the local ID and Peer ID for identification.
	Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional).
Local ID	Specify a local ID to be used when establishing a VPN connection using IPsec VPN type.
Peer ID	Enter the ID name for the remote client.
	If the values are specified, only connections coming from the specifie IP address and/or having the specified Peer ID will be accepted.
More settings for IKE Aut	hentication
IKE Phase 1	Encryption – Use Auto/AES/3DES/DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
	Group – Specify a key exchange proposal.
	Authentication – Select SHA256 or SHA1 for packet authentication.
	Lifetime - For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.
IKE Phase 2	Specify the security protocol, proposal encryption and proposal authentication.
	Security Protocol – AH (Medium) means data will be authenticated, but not be encrypted. By default, this option is active. ESP (High) means payload (data) will be encrypted and authenticated.
	Encryption – Use AES/3DES/DES encryption algorithm.
	Authentication – Select All, SHA256 or SHA1 for packet authentication
	Lifetime – For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in betwee 600 and 86400 seconds.

	Perfect Forward Secret – Switch the toggle to enable/disable this function. PFS forces key exchange during Phase-2 periodic Rekey.
Dead Peer Detection	Dead Peer Detection (DPD) is the method to detect an IPsec connection.
	DPD Delay – It is a keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.
	DPD Timeout - It is the timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.
	Network
Network	Specify that traffic from the local subnet and remote subnet can pass through the VPN connection.
	Local Network – The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	Subnet Mask – Display the local network IP and mask for TCP / IP configuration. Select the one to meet the local network value.
	Remote Network – The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	Subnet Mask - Select the one to meet the local network value. It is used to add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.
Routing/NAT Mode	Routing Mode – It enables a standard site-to-site VPN, where the traffic is directly routed between two networks without altering the source IP address.
	NAT Mode – It modifies VPN traffic to the remote site by translating the source IP into a virtual IP address before sending it to the destination.
More Remote Subnets	It is used to add more static routes for subnets destined for the remote network.
	Disabled – Disable this function.
	Multiple SAs – Multiple SAs will establish different Phase 2 SAs based on the local network and remote network to provide additional security for data transmission. Select for adding new route.
	 +Add – Click to add new static route. Enter required information for local network, subnet mask, remote network and subnet mask.
More Options under the	Advanced Mode
Dial-Out Interface Mode	

Select the WAN connection for connections made using this profile.

	This setting is useful for dial-out only.
	Selected Interface First – While connecting, the router will use the selected WAN interface first for VPN connection. If selected WAN fails, the router will try to use other WAN(s).
	Selected Interface Only – While connecting, the router will use selected WAN as the only interface for VPN connection.
	Manual – Customize VPN settings. Specify which WANs can be used as outgoing interfaces.
Dial-Out Interface	It is available when the call direction of this VPN profile is set to Dial-Out the Advanced Mode is ON.
	Auto Select – Decide which interface to dial out based on the default route.
	Default WAN IP / IP Address – Use the drop-down list to specify one WAN IP address for this VPN profile.
Idle Timeout	The tunnel will be disconnected when no traffic is detected within Idle Timeout. Disable this feature by setting the value to 0.
GRE Over IPsec	 Switch the toggle to enable/disable the function. It will verify data and transmit data in encryption with GRE over IPsec packet after configuring IPsec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication. GRE Local IP – Enter the virtual IP for router itself for verified by peer. GRE Remote IP - Enter the virtual IP of peer host for verified by router
Routing/NAT Mode	Routing Mode – It enables a standard site-to-site VPN, where the traffic is directly routed between two networks without altering the source IP address.
	NAT Mode – It modifies VPN traffic to the remote site by translating the source IP into a virtual IP address before sending it to the destination.
Cancel	Discard current settings and return to the previous page.
Apply	

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

II-4-2-2 VPN Type - WireGuard

WireGuard is a secure, fast, and modern open-source VPN Protocol. This VPN connection can build a VPN by exchanging private and public keys between VPN servers (e.g., Vigor router) and VPN clients (e.g., WireGuard VPN Client).

To add a new resources profile (WireGuard VPN type), open VPN>>Site-to-Site VPN and click **+Add**.

		>
		dvanced Mode: ON
Profile Name 🕕		
nabled		
Seneral		×
irection	Dial-in ~	
PN Type	WireGuard 🗸	
ial-In Allowed Schedule	Always Allow Scheduled	
rop the Active Tunnel when chedule is Enforced		
PN Schedule	select your runnows 🗸 🗸	
lle Timeout (Seconds) 🛈	0	
	Note: The tunnel will be disconnected when no traffic is detected within idle Timeout. Disable this feature by setting the value to 0,	
VireGuard		- 3

Available settings are explained as follows:

ltem	Description	
Advanced Mode:ON/OFF	Click to show or hide the advanced settings for the site-to-site VPN.	
Profile Name	Enter the name of the profile.	
Enabled	Switch the toggle to enable/disable the settings.	
	General	
Direction	Specify the allowed call direction of this WireGuard VPN profile.	
	Dial-Out – Profile is to be used to initiate outgoing connections. Dial-In – Profile is to be used to accept incoming connections.	
VPN Type	Select a VPN type for building the VPN connection. Options related to WireGuard VPN type will be changed according to the Direction used.	
	WireGuard (with the direction on Dial-In) - The WireGuard VPN type is available when Dial-In or Dial-Out is selected as the Direction.	
	Dial-in Allowed Schedule	
	WireGuard (with the direction on Dial-Out) –	
	Remote IP/Domain	
	Server Port	
	Dial-Out Mode	
Dial-In Allowed	Connect and disconnect according to schedule profiles.	
Schedule	Always Allow – Select this option to maintain an always on dial-in	

	connection. Scheduled –Select this option to make the VPN connection based on the schedule.
	 Drop the Active Tunnel when Schedule is Enforced – Switch the toggle to enable/disable the function.
	 VPN Schedule – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule.
Remote IP/Domain	Enter IPv4 or hostname for the remote VPN server.
Server Port	Set a port number for the VPN server.
Dial-Out Mode	On Demand – The VPN connection will be triggered when detecting traffic going to the remote network.
	Always On – Select this option to maintain an always on dial-out connection.
	Scheduled – Connect and disconnect according to schedule profiles. The default setting of this field is blank and the function will always work.
	 Drop the Active Tunnel when Schedule is Enforced – Switch the toggle to enable/disable the function.
	 VPN Schedule – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule.
	WireGuard
Interface	It is available when Dial-Out is selected as the Direction and Wireguard is selected as VPN Type.
	Private Key – Displays the private key generated by clicking Generate .
	Generate Private Key – Click the Generate button to generate a key pair (including private key and public key).
	Public Key - Displays the public key generated by clicking Generate .
Peer	It is available when Dial-Out/Dial-In is selected as the Direction and Wireguard is selected as VPN Type.
	Configure the settings for the client (peer).
	Public Key - Enter the Public key of the Peer VPN server.
	Pre-Shared Key - Displays the private key generated by clicking Generate PSK .
	Generate PSK - Click Generate to generate the pre-shared key.
	For NAT Client Address (Optional) – It is for Dial-In only. Enter the IP address of the remote peer.
	Keepalive - Default is 60 seconds.
	Network
Network	It is crucial for defining the traffic routing. Traffic from both the local and remote subnets can pass through the WireGuard VPN connection.
	Local Network – Defines the range of IP addresses that belong to you local network, which will be used when routing traffic through the VPN.
	Subnet Mask – The subnet mask helps define the size of your local network and tells the VPN how to interpret the network portion of the IP address. A subnet mask of 255.255.255.0 (or /24 in CIDR notation)

	means that the first 24 bits of the IP address are for the network, and the remaining 8 bits are for hosts (devices) within the local network.
	Remote Network – Defines the IP address range of the remote network that you are connecting to. For instance, if the remote network is 10.0.0.0/24, you are telling the VPN that the remote network's IP range is 10.0.0.1 through 10.0.0.254.
	Subnet Mask - Similar to the local network, the subnet mask for the remote network determines how the remote network's IP range is divided. If the remote network has a subnet mask of 255.255.255.0 (o /24), it means that the remote network has 254 possible addresses fo devices.
Routing/NAT Mode	 If the remote network only allows one IP address for the local network, select NAT; otherwise, select Routing. Routing NAT
More Subnets	It is used to add more static routes for subnets destined for the remote network. Disabled – Disable this function.
	 +Add – Click to add new static route. Enter required information for the remote network and subnet mask.
Options under the Advan	ced Mode
Dial-Out Interface Mode	Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.
	Selected Interface First – While connecting, the router will use the selected WAN interface first for VPN connection. If selected WAN fails, the router will try to use other WAN(s).
	Selected Interface Only – While connecting, the router will use selected WAN as the only interface for VPN connection.
	Manual – Customize VPN settings. Specify which WANs can be used as outgoing interfaces.
Dial-Out Interface	It is available when the call direction of this VPN profile is set to Dial-Out.
	Auto Select – Decide which interface to dial out based on the default route.
	Default WAN IP / IP Address – Use the drop-down list to specify one WAN IP address for this VPN profile.
Cancel	Discard current settings and return to the previous page.

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

II-4-2-3 VPN Type - OpenVPN

The OpenVPN protocol utilizes public keys, certificates, and usernames and passwords to authenticate the client. Traffic is carried over secure channels built upon industry-standard SSL/TLS encryption protocols.

OpenVPN requires the use of certificates. Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.

To add a new resources profile (OpenVPN VPN type), open VPN>>Site-to-Site VPN and click **+Add**.

		×
		Advanced Mode: ON
Profile Name 🕕		
Enabled		
General		\sim
Direction	Dial-Out 🗸	
Dial-Out Interface Mode	Selected Interface First \sim	
Dial-Out Interface	Auto Select 🗸 🗸	
	Default WAN IP 😒	
VPN Type	OpenVPN V	
Remote IP/Domain ①	OpenVPN	
Server Port	1194	
Dial-Out Mode	On Demand Always On Scheduled	
	Note: On Demand VPN will be triggered up when detecting traffic going to remote network.	
Idle Timeout (Seconds) 🛈	0	
Cancel Apply		

Dial-In Allowed	Connect and disconnect according to schedule profiles.
Schedule	Always Allow – Select this option to maintain an always on dial-in connection.
	Scheduled –Select this option to make the VPN connection based on the schedule.
	• Drop the Active Tunnel when Schedule is Enforced – Switch the toggle to enable/disable the function.
	 VPN Schedule – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule.
Remote IP/Domain	Enter IPv4 or hostname for the remote VPN server.
Server Port	Set a port number for the VPN server.
Dial-Out Mode	On Demand – The VPN connection will be triggered when detecting traffic going to the remote network.
	Always On – Select this option to maintain an always on dial-out connection.
	Scheduled – Connect and disconnect according to schedule profiles. The default setting of this field is blank and the function will always work.
	• Drop the Active Tunnel when Schedule is Enforced – Switch the toggle to enable/disable the function.
	• VPN Schedule – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule.
	Username and Password
Username and Password	It is available when Dial-Out/Dial-In is selected as the Direction and OpenVPN is selected as VPN Type.
	Username - Used by the remote LAN to establish a VPN connection.
	Password - Used by the remote LAN to establish a VPN connection.
	Network
Network	It is crucial for defining the traffic routing. Traffic from both the local and remote subnets can pass through the VPN connection.
	Local Network – Defines the range of IP addresses that belong to you local network, which can be accessed through the VPN tunnel.
	Subnet Mask – The subnet mask helps define the size of your local network and tells the VPN how to interpret the network portion of th IP address. A subnet mask of 255.255.255.0 (or /24 in CIDR notation) means that the first 24 bits of the IP address are for the network, and the remaining 8 bits are for hosts (devices) within the local network.
	Remote Network –Defines the IP address range of the remote network that you are connecting to. For instance, if the remote network is 10.0.0.0/24, you are telling the VPN that the remote network's IP range is 10.0.0.1 through 10.0.0.254.
	Subnet Mask - Similar to the local network, the subnet mask for the remote network determines how the remote network's IP range is divided. If the remote network has a subnet mask of 255.255.255.0 (or /24), it means that the remote network has 254 possible addresses for devices.
Routing/NAT Mode	If the remote network only allows one IP address for the local network, NAT will be shown in this field. Otherwise, Routing will be

	shown in this field.
More Subnets	It is used to add more static routes for subnets destined for the remote network.
	Switch the toggle to enable/disable this function.
	 +Add – If the function is enabled, click Add to add new static route. Enter required information for remote network and subnet mask.

Options under the Advanced Mode

Dial-Out Interface Mode	Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.
	Selected Interface First – While connecting, the router will use the selected WAN interface first for VPN connection. If selected WAN fails the router will try to use other WAN(s).
	Selected Interface Only – While connecting, the router will use selected WAN as the only interface for VPN connection.
	Manual – Customize VPN settings. Specify which WANs can be used a outgoing interfaces.
Dial-Out Interface	Auto Select – Decide which interface to dial out based on the default route.
	Default WAN IP / IP Address – Use the drop-down list to specify one WAN IP address for this VPN profile.
OpenVPN Settings	It is available when Dial-Out is selected as the Direction and OpenVPI is selected as VPN Type.
	Dial-Out Protocol – Select TCP or UDP as VPN server protocol.
	Import OpenVPN Config - An OpenVPN config file from other Vigor router can be imported and apply to this router.
	Select to import an OpenVPN configuration file from a specified OpenVPN server (e.g., Vigor router, PC, other VPN provider, etc.) onto to Vigor router. Later, as a VPN client, this router can access into VPN server via the username and password. If the configuration file contains certificates, they will be automatically imported.
Dial Out Advanced Settings	Cipher Algorithm – Select the desired cipher algorithm. Two encryption algorithms are supported: AES128, AES192 and AES256. AES256 is more secure than AES128 but may result in lower performance because it incurs higher computational overhead.
	HMAC Algorithm – HMAC stands for Hash-based Message Authentication Code. It is used to validate the data integrity and authenticity of the VPN data.
	Select the desired HMAC hash algorithm. Two hash algorithms, SHA1 and SHA256, are supported. SHA256 is preferred as it is more robust and reliable than SHA1.
	Client Certificate – Use the dropdown list to select a client certificate that has already been uploaded to the router. Default (Use CERT from OPenVPN Config) will be selected automatically after import OpenVPI Config file.
	Trusted CA – Use the dropdown list to select a trust CA certificate that has already been uploaded to the router. Default (Use CA from OpenVPN Config) will be selected automatically after import OpenVPI Config file.
	Compress – Select a method to compress the packets to reduce the

	bandwidth usage while transferring the compressed packets.
	TLS Auth – Switch the toggle to use/close the TLS authentication method. If the OpenVPN configuration file contains TLS Key, they will be automatically imported.
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.

II-4-3 Teleworker VPN

The VPN means a connection between the remote host and router's LAN network. The host will use an IP address in the local subnet. It allows employees to access the company's internal resources when they are traveling.



Open VPN>>Teleworker VPN to get the following page.

	a	VPN / Tele	eworker VPN								3	leset C Refresh
		Telework	ter VPN									
		t-Add	S OpenVPN C	antia Canada								Max: 100
Dashboard											Search	
Configuration	2	Source	Username	Usage	Role	Status	Group Policy	Allow Login from WAN	Created Time	Last Login at	Last Login IP	Option
Security	->											
S IAM	8											
General Setup												
Site to Site VPN												
VPN Connection Status												
Backup & Restore												
표 Monitoring	*											
88 Utility												
🖇 System Maintenance	>											
+ Wireless	>											
Switch												

To add a new VPN profile, click +Add.

Note that the settings modification related to the user profile (no matter add or edit) here will rewrite the settings on IAM>>Users & Groups>>Users synchronically, and vice versa.

ername 🕕		
sage	IAM User Router Management	
	Note: IAM User: Permits user authentication for VPN, RADIUS, 802.1X, USB, and IAM, but not for router management. Router Management: Enables router management access while disabling VPN, RADIUS, 802.1X, USB, and IAM a	
assword 🕡	\$	
General Telewor	ter VPN	
tatus	Active V	
roup Policy	None 🗸	
xpiration Time	Never	
ser Information		
nable Email	0	
nable SMS		
MFA		
nable MFA		

Available settings are explained as follows:

ltem	Description
Username	Enter the Login name (e.g., <i>LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B</i> , etc.) for this user profile.
Usage	Define the type of this user profile.
	IAM User – This profile can be used for VPN, RADIUS, 802.1X, USB and IAM (AWS Identity and Access Management) authentication.
	Router Management – This profile is only for router management access and cannot be used for VPN, RADIUS, 802.1X, USB, and IAM authentication.
Password/	Password (e.g., <i>lug123, wug123, wug456,</i> etc.) for this user profile.
New Password/	When a user tries to access the Internet, he or she must supply a valid
Confirm New Password	user name and password combination for authentication. The profile with matching user name and password will be applied to the session
	General
Status	Active – Enable the general settings in this page.
	Inactive – Disable the general settings in this page.
Group Policy	It is available if "IAM User" is selected as the usage.
	Select a group policy profile to be applied by this user profile.
Expiration Time	It is available if "IAM User" is selected as the usage.
	It means that the user account will be automatically disconnected after the time is up.
	Set the network connection to work at certain time interval only. All user accounts will apply the time configuration automatically by default.
	Never – The network connection is always on.
	-

Expire in – The network connection will expire and terminate the connection after specified minutes, hours, days, or weeks once built.
 Expire at – The network connection will expire and terminate the

	connection on the date and time specified below once built.
	Date
	Time
Role	 It is available if "Router Management" is selected as the usage. Administrator Guest Users
Allow Login from WAN	It is available if "Router Management" is selected as the usage. If enabled, the user can login from WAN by using this user account.
User Information	 Enable Email – Switch the toggle to enable or disable the email setting. Email – Enter the email address for receiving the MFA PIN code. Send Email Notification to the newly created User – Send a notification email to this user account. Enable SMS – Switch the toggle to enable or disable the SMS setting. SMS - Enter the destination SMS number for receiving the MFA
	PIN code.
MFA	Multi-factor authentication (MFA) can offer a more secure network

connection.

Enable MFA – Switch the toggle to enable/disable the MFA function.

• Allowed MFA Method - Select to require TOTP, Email, SMS and/or mOTP authentication when logging in from the WAN.

TOTP – For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone.

Secret: JBLUN	NZRXMJCUE4JPWRJEKYTONB2DER	IKINIKDARBYKAAWAADP656DQUD	FRZAX527P	
Ę	影響物里			
QR Code:				
Ō	動音樂政制			
Validation Cod	le:			
			1104	1000

SMS/Email – The password will be transferred via the SMS and/or Mail profiles selected from User Information above.

mOTP - Mobile one-Time Password (mOTP) allows the use of mOTP passwords. Enter the PIN Code and Secret settings for getting one-time passwords.

Account Info	Displays general information (created time, last login at and last login IP) for the VPN user account.
--------------	--------------------------------------------------------------------------------------------------------

Teleworker VPN

(available if IAM User is selected as the Usage)		
General	Enable Teleworker VPN – Switch the toggle to enable/disable Teleworker VPN configuration.	
	Idle Timeout – If the user is idle over the limitation of the timer, the network connection will be stopped for such user. By default, the Idle Timeout is set to 300 seconds.	
	VPN Schedule – Select Always On . Or choose Scheduled On to make the VPN connection based on the schedule.	
	Before configuring VPN Schedule, add the required time intervals in Configuration>>Objects >>Schedule.	
	Download SmartVPN Client – Click to download the utility of DrayTeck SmartVPN client for building VPN connection.	
Allowed VPN Protocols	Select IPsec, WireGuard or OpenVPN as the protocol for the teleworker VPN connection.	
	IPsec – Switch the toggle to enable the IPsec protocol. If enabled, select IKEv1/v2, EAP and/or XAuth as the IPsec authentication.	
	OpenVPN - Switch the toggle to enable OpenVPN protocol.	

	WireGuard – Switch the toggle to enable WireGuard protocol.
	 General Key Mode – Select Auto or Customized. Select Auto and click Generate Key Pair to generate the key pair of the private key and the public key of the peer. Select Customized to enter the public key of the peer side.
	 Public Key – Enter the string offered by the remote WireGuard VPN client.
	 Pre-Shared Key – Displays the private key generated by clicking Generate PSK.
	 Generate PSK – Click the Generate PSK button to generate a pre-shared key.
	 Persistent Keepalive – Default is 60 seconds. If the peer is behind a NAT or a firewall, use the default setting.
Security	Specify VPN Peer – Switch the toggle to enable/disable the security mechanism for the remote client.
	Remote Client IP – Enter the IP address of the remote peer.
	Pre-Shared Key – "Specify VPN Peer" can restrict this IPsec to be initiated only by the specified peer IP address or domain name, and specify the private key to be used.
	X.509 Digital Signature – It is available only for IPsec protocol. Accept the certificates authentication. To use an X.509 digital signature, select one of the authentication methods and enter the required information for each method.
	• Disabled – Select to disable the certificate application for VPN connection.
	 Accept Subject Alternative Name – The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.
	 Select from Existing Certificates – Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.
	 Accept Subject Name – Enter the complete certificate subject name.
	 Accept Any – Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid.
	Click IPsec Advanced Settings to get the following options. Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional).
	 Peer ID – Specify a local ID to be used when establishing a VPN connection using IPsec VPN type. Enter the ID name for the remote client.
	 Local ID (optional) - If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Local IP Assignment	Assign IP from - Select a LAN interface for IP assignment.
	Static IP - Specify an IPv4 address as the static IP.
	Assign DNS By – Select LAN DHCP or Static DNS.
	If LAN DHCP is selected,
	 Assign DNS By – It is available when LAN DHCP is selected. Choose LAN DHCP (the DNS IP will be assigned by Vigor router

	automatically) or Manually.	
	If Static DNS is selected,	
	• Primary DNS – Enter the IPv4 address for Primary DNS server.	
	 Secondary DNS – Enter another IPv4 address for DNS server 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.

OpenVPN Config Generator.

On this page, you can create configuration required for a remote OpenVPN client to connect to the router and then download it directly or send it to the user via email.

ise select 🖂			
se select 🖂			
~			
)			
r			
)			
il to Users Downlo	ad zip file		
et your options	\sim		
d Email			
	ase select 😒	ase select 😒	ase select 😒

ltem	Description
Specify Server URL by	The OpenVPN client will use the IP address or domain name to connect to the router.
	WAN IP – The OpenVPN configuration file will use the numeric IP address as the server address.
	• WAN IP – Select the WAN interface.
	DDNS Profile – The OpenVPN configuration file will use the domain name from the DDNS Profile.
	• DDNS Profile – Select a DDNS profile.
	Custom URL – The OpenVPN configuration file will use the user-defined server IP or domain name.
	• Custom URL – Specify a user-defined URL.
Set VPN as Default	Switch the toggle to enable/disable the function.

Gateway	Enable - The Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel.Disable -Disable the function.			
Transport Protocol	TCP/UDP - Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router.			
Auto Dial Out	Switch the toggle to enable/disable the function. Enable - The remote client can auto-dial to this Vigor router to build ar OpenVPN tunnel. Disable - Disable the function.			
Cache password for auto reconnect	Switch the toggle to enable/disable the function. Enable - OpenVPN will reconnect per hour. While reconnecting, the password is required. If the function is enabled, the password for OpenVPN connection will be kept and used by the Vigor system for reconnection every time. Disable - Disable the function.			
UDP Ping	Ping remote device over the UDP control channel, if no packets have been sent for the number of seconds configured here.			
UDP Ping Exit	Let OpenVPN exit after the seconds set here if no reception of a ping or other packet from the remote device.			
Export Configuration by	 Email to Users – If selected, the Included Users field below will be displayed. The OpenVPN configuration file will be sent to users listed on Included Users. Included Users – Select teleworker users that will receive the configuration from Vigor router. Send Email – Click to email the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections to teleworker users. Download zip file – The configuration file for OpenVPN will be stored on the database. If selected, the Download Configuration button below will be displayed. Download Configuration - Click this button to download the 			
	settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections.			
Close	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

II-4-4 VPN Connection Status

This section displays various VPN connection status, including

- Site-to-Site VPN
- Teleworker VPN
- Connection History
- Failed VPN Connection Attempts
- Blocked by Brute Force Protection

Search	۹	VPN / VPN Connection Sta	tus					0	Refresh
Device Menu (?) Dashboard	8	Site-to-Site VPN Telew		on History Failed VPN (Connection Attempts Brute	Force Protection			
	2	Time Period	Less 2 Hours	Lest 24 Hours					
Security	*	Protocol	Failed	Attempts					
25 VIII		IPsec	0						
General Setup		WireGuard	0						
Site-to-Site VPN Teleworker VPN		OpenVPN	0						
VIN Connection Station Backup & Restore		Failed Attempt History							Ŷ
🖼 Monitoring	5								Max: 100
BS Utility	×	External IP	Location	VPN Type	VPN Profile	Interface	Time	Details	
🖏 System Maintenance	*								
Virtual Controller									
>- Wireless									
🗃 Switch	×								

II-4-5 Backup & Restore

This page can be used to backup/restore the VPN configuration.

	VPN / Backup & Restore	
	Backup & Restore	
Device Menu		
(?) Dashboard	Backup	
🚆 Configuration >	buchup	
Security	Selected Item	Select All
A IAM		General Setup
		Site-to-Site VPN
		Teleworker VPN
General Setup	Password Protection	
Site-to-Site VPN Teleworker VPN	New Password ()	
VPN Connection Status		•
Backud & Restore	Confirm New Password ()	•
Monitoring >		 At least 8 characters
		 Uppercase characters Lowercase characters
BS Utility >		 Numbers or Special characters _ ②:./+ 単()17*
🖏 System Maintenance 💦 🦻		
Virtual Controller	-	
>- Wireless	Restore	
🗃 Switch 3	Restore from Backup File	Em Restore
	File has Password Protection	0

ltem	Description			
Backup				
Selected Item	Select the VPN type for the 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.			
New Password/ Confirm New Password	nter several characters as the password for encrypting the onfiguration file.			
Back up	Click it to backup the configuration file.			
	Restore			
Restore from Backup File	- Click to locate the file for restoring. Restore - Click to execute the restoration.			
File has Password Protection	Switch the toggle to enable or disable the function. If enabled, a password will be required for restoring the configuration.			
Password	Enter a password for configuration restoration.			

II-5 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.

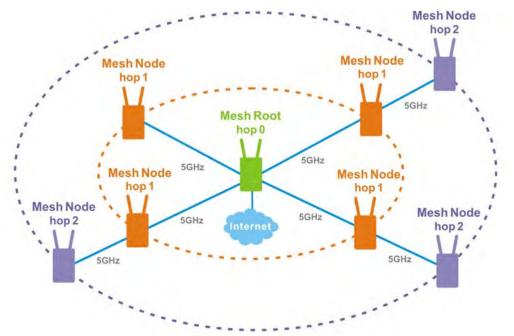
For Mesh networks, Root is also the outlet to the Internet. All devices of a network are in the same Group. The root can add a new Node to its Group or delete members from its Group. Users can choose VigorMesh or EasyMesh to establish the Mesh network. If Mesh is disabled, a network with wired links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

Vigor router plays a role of Mesh root in a VigorMesh network.

Please note that, within VigorMesh network,

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

Refer to the following figure:



For the mesh group set within VigorMesh network,

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

Mesh Root

Mesh Root indicates that Vigor router would be other AP's uplink connection. As a Mesh Root, Vigor router must connect to internet through WANs to have an internet connection.

The following figure shows how Vigor router runs as MESH ROOT:



II-5-1 Role Setup

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

	Wireless / Role Setup		③Reset ©Refres
	Role Setup		
Device Menu			Advanced Mode: OFF
Dashboard	Device Role	Root ~	Advanced mode. OFF
Configuration	Group Admin Account ()	ədmin	
Security	Group Admin Password ()		
A IAM	a and a manual season of a		
D VPN	Password Status	Use random password	
Monitoring	Mesh Setup		
😵 Utility			
🖏 System Maintenance	Mesh Version	Vigor Mesh (R2)	
	Enable Mesh		
/irtual Controller	Mesh Protocol	Vigor Medi	
	and the second sec	a second and a second se	
	Group Name	DrayTekMesh	
Device	AP Management Setup		
🗄 Switch			
	Enable AP Management		
	Cancel Apply		

Available settings are explained as follows:

Item	Description
Advanced Mode:ON/OFF	Click to show or hide the advanced settings (Wireless Download Band, Auto Wireless Uplinks Optimization and Log Level).
Device Role	Root – The device is a Root. It controls the network and syncs configurations to the Nodes of its Group.
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.
Password Status	User random password – The default display state. By default, the

	mesh group password will be generated randomly by the Vigor system.
	Ready – If the password is set or changed manually, after finishing the configuration, the word "Ready" will be shown instead.
	Mesh Setup
Enable Mesh	Switch the toggle to enable or disable the mesh function.
Mesh Protocol	Select the mesh protocol to manage the mesh network.
	Vigor Mesh – A protocol developed by DrayTek.
Group Name	Displays the name of the current mesh group. Change the name if required.
Wireless Download	It is available only when Advanced Mode is set to On.
Band	Select a wireless band (Auto, 2.4GHz or 5GHz) for connecting with a downlink mesh root or a downlink mesh node.
	Auto 2.4GHz 5GHz
Auto Wireless Uplinks Optimization	It is available only when Advanced Mode is set to On . It is enabled in default. To perform the auto reselect, make sure the process for CFG Sync and CFG Check for mesh nodes (members) are successful. If enabled, after changing the environment of mesh network (e.g., offline, disconnection), the root device will perform auto reselect to reconstruct the mesh network.
Log Level	It is available only when Advanced Mode is set to On. Choose Basic or Detailed . Related information will be shown on Syslog.
	AP Management Setup
Enable AP Management	Switch the toggle to enable/disable the AP Management.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-5-2 Device

II-5-2-1 Device List

This page displays general information about the devices grouped under Vigor C410/C510 series.

wice Menu	Device List Mesh S	tatus AP Adoption								
Dashboard	Device List									
Configuration 5										Maoc
Security >	Name	MAC	IP Address	SSID	Status	Role	WLAN Clients (2.4G/5G)	Firmware Version	System Uptime	Option
IAM >	DrayTek-86FA88	14498C86FAB8	192.168.1.1	DrayTek-86FAB8	Online	Root	0/0	5.3.1_RC3	1d 6h 55m 19s	@ Edit
VPN 5										
Monitoring 5										
Utility >										
System Maintenance										
tual Controller										
windless										
Role Setup										
Device										
Switch >										

Click **Edit** 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.

×						us AP Adoption	e List Mesh Stati
DrayTek-86FAB	SSID						ce List
Onlin	Status						
VigorC410Va	Model	Role	Status	SSID	IP Address	MAC	Name
Roo	Role	Root	Online	DrayTek-86FAB8	192.168.1.1	1449BC86FAB8	DrayTek-86FAB8
0/	WLAN Clients (2,4G/5G)						
5.3.1_RC	Firmware Version						
1d 6h 55m 19	System Uptime						
Reboot now	Device Reboot All Nodes						
Factory Reset now	Device Factory Reset All Nodes						
	Device Configuration						
	Config Sync Status All Nodes						
	Last Sync Time All Nodes						
Full Config Select Scope	Config Sync to All Nodes						
	Sync Config						

ltem	Description
Device Reboot All Nodes	Reboot Now – Click to reboot all nodes immediately.
Device Factory Reset All Nodes	Factory Reset Now - Click to reset all nodes with factory settings immediately.

Config Sync to All Nodes	Full Config – Sync the full configuration to all nodes. Select Scope - Sync the selected configuration to all nodes.
Sync Config	Sync now –Click to execute the sync configuration.
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.

II-5-2-2 Mesh Status

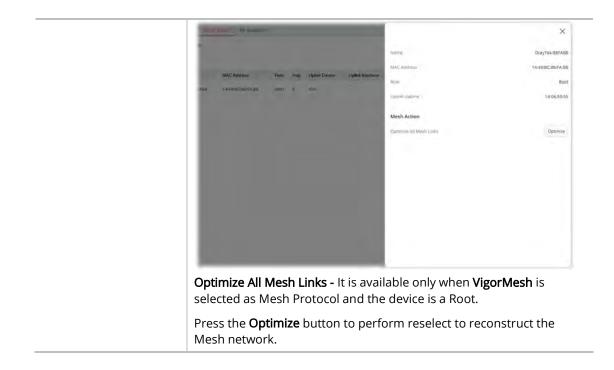
Display general information of the Mesh network.

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

Search Q	Wireless / Device									C Refresh
levice Menu	Device List Mesi	Status AP Adoption								
Dashboard	and the second									
E Configuration	×								Search	Maor: 253
Security	Name	MAC Address	Role	Нор	Uplink Device	Uplink Interface	Signal Strength	Uplink Rate (TX/RX)	Uplink Uptime	Option
IAM	DrayTek-86FAB8	14:49:BC:86:FA:88	Root	0	N/A	-	÷	-	1d 06:55:55	do View
VPN	×									
Monitoring	».									
Utility	×.									
System Maintenance	× .									
tual Controller										
Role Setup										
8 Switch	a									

Available settings are explained as follows:

Item	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.



II-5-2-3 AP Adoption

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

This page is available when current device role is Root.

Device Manu So bashboard Configuration Status Status Status Ready Device Number Status Status Status Ready Status Status Status Ready Status Status Status Ready Status Status <th>SearchQ</th> <th>Wireless / Device</th> <th></th> <th></th>	SearchQ	Wireless / Device		
Pashboard AP Adoption Configuration Status Security Device Number Image: Status Ready Status Status Status Status Status Status Monitoring Status Monitoring AP Discovery Result Monitoring Applicacy System Maintenance Status Wirtual Controller Wirtual Controller Swep		Device List Mesh Status	AP Adoption	
Configuration Startus Rendy Security Device Number Image: Number of Startus Start AP Discovery Start AP Discovery Start AP Discovery Result Adopt AP MAC Montoring Montoring Montoring Montoring System Muintemance Virtual Controller Wireless Role Setup Discovery		AP Adoption		
Security Security Land Security Start AP Discovery Start AP Discovery Result Adopt AP MAC Model Signal Strength Device Name Monitoring VPN Monitoring VPN Monitoring VPN System Maintenance System Maintenance VPClabs Role Setup Device	Dashboard			
Security Device Number AnA Start AP Discovery VPN Monitoring AP Discovery Result Adopt AP MAC Model Signal Strength Device Name	Configuration	Status		
VPN VPN Monitoring AP Discovery Result Adopt AP MAC Model System Maintenance System Maintenance Virtual Contraller	Security	Device Number		
VPN Monitoring AP Discovery Result Adopt AP MAC Model System Maintenance Virtual Controller Wireless Role Setup Dwke	Д, илм	Start AP Discovery	Scan	
Kolicong Virtual Controller Virtual Controller Kole Setup Divke	D VPN			
AS Unity > > System Maintenance ; Virtual Controller - Wircless Role Setup Dwike	Monitoring	AP Discovery Result	Adopt AP MAC Model Signal Strength Device Name	
Virtual Controller) Wireless Role Setup Dowko	88 Utility			
Dowle	System Maintenance			
Role Setup (Sevier	Virtual Controller			
Bookers				
	Role Setup			
🗄 Switch				
	Switch			

ltem	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
	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.

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 a Mesh Group through Wireless or Wired connection.
 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.

Role Setup		🕲 Reset 🔿 Refresh
Device Role	Auto 🗸	Advanced Mode: OF
Current Device Role	Node	
Group Admin Account	admin	
Group Admin Password	• •	
Password Status	Use random password	
Mesh Setup		
Enable Mesh		
Mesh Protocol	Vigor Mesh EasyMesh	
Current Uplink	Wired	
Group Name	DrayTekMesh	
AP Management Setup		

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

Wireless / Device							
Device List Mesh Status	AP Adoption						
AP Adoption							
Status	Ready						
Start AP Discovery	Scan						
AP Discovery Result	Adopt AP MAC	Model	Signal Strength	Device Name			
		No Re	cords 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.

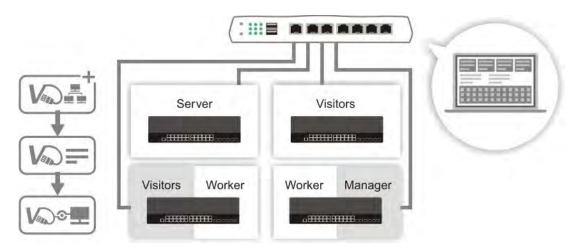
	AP Discovery Result Adopt AP MAC Model Signal Strength Device Name
14:49:BC:51:B7:9F VigorAP1062C -92dBm(weak) 00:1D:AA:66:44:66 VigorAP1062C -94dBm(weak)	
00:1D:AA:66:44:66 VigorAP1062C -94dBm(weak)	14:49:BC:51:B7:9F VigorAP1062C -92dBm(weak)
00:1D:AA:64:10:15 VigorAP1062C -61dBm(good) N1	00:1D:AA:66:44:66 VigorAP1062C -94dBm(weak)
	00:1D:AA:64:10:15 VigorAP1062C -61dBm(good) N1

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

Wireless / Devic	ce									
Device List	Mesh Status	AP Adoption						e.	D Reset	Refresh
Device List										
										Max: 50
Name	MAC	IP Address	SSID	Status	Role	WLAN Clients (2.4G/5G)	Firmware Version	System Uptime	Option	
VigorAP1062C	001DAA102722	192.168.1.10	DrayTek- 102722	Online	Root	0/0	1.5.1_RC8	0d 4h 58n	n 24s 🛷 Edit	
VigorAP1062C	001DAA641015	192.168.1.11	DrayTek- 102722	Online	Node	0/0	1147.8df8de432f_	Beta 0d 1h 00n	n 45s 🧷 Edit	🖞 Delete
Wireless / Devi	ce									
Device List	Mesh Status	AP Adoption							C	Refresh
Mesh Status										
Name	MAC Address	Role He	op Uplink E	evice	Upli	n <mark>k Int</mark> erface	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/869	6 1755M/1755N	/ 0d 02:11:22	@ View

II-6 Virtual Controller - Switch

Vigor router can manage lots of VigorSwitch devices connected to it. Through profile and group settings, the administrator can execute firmware/configuration backup, restore for VigorSwitch device, reboot the device or return to factory default settings of VigorSwitch at one time.



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

II-6-1 General Setup

In this page, switch the toggle to enable / disable the switch management function.

Search	a	Switch / General Setup
		General Setup
Device Menu	-	
(?) Dashboard		Enable Switch Management
	×	
Security	×.	
₿ IAM	2	
D VPN	2	
B Monitoring	à.	
BS Utility	5	
🖏 System Maintenance	.>	
Virtual Controller		
>- Wireless	4	
Device		
Port Profile		
Maintenance		
		Cancel Apply

II-6-2 Device

This page displays information, including Switch name, MAC address, IP address, Firmware Version, Model, Online Status, System Uptime, Port in Use, Clients, Last Process Status and Option of a VigorSwitch connected to the Vigor router.

	۹	Switch / Device										
Device Menu		Device List										
Dashboard	-	G Add New St	witch Refresh									Mane
E Configuration	2	Switch Name	MAC Address	IP Address	Firmware Version	Model	Online Status	Port in Use	Clients	Last Process Status	Option	
Security	2											
Д кам												
D VPN												
표 Monitoring												
😵 utility												
🖇 System Maintenance												
virtual Controller	-											
}⊷ Wireless	*											
General Setup												
Device Port Profile												
Maintenance												

To add a new switch, click the **Add New Switch** link to open the following page.

Add New S	Switch			×
Scanning F	rom Network	Scan		
Switches				
Adopt	Device Name		MAC Address	Model Name
				Close Apply

Add New	Switch			×
Scanning F	From Network	Scan		
Switches				
Adopt	Device Name		MAC Address	Model Name
- 🗇	Q2200x		14-49 BC 44 A0 B9	Q2200x
				Close
_				

Click Scan and wait for a while Vigor router will scan and list the switch connecting to Vigor router.

Check the box below Adopt to select the device and click Apply.

evice List											
add New S	witch Refresh										Max: 5
witch Name	MAC Address	IP Address	Firmware Version	Model	Online Status	System Uptime	Port in Use	Clients	Last Process Status	Option	
2200x	14:49:8C:44:A0:89	192.168.1.24	2.8.1	VigorSwitch Q2200x	Online	7d 22h 50m 6s	1/20	2	Process Successfully	2 Edit	10 Delete

The selected switch, now, has been managed by the Vigor router.

To edit the device information, set port profile or view the port status of the switch, click Edit.

General

This page shows a summary related to the VigorSwitch. Also, it offers Reboot Now and Factory Reset Now buttons to assist users in updating the switch.

		×
General Port Profile	Port Status	
Switch Name	Q2200x	
MAC Address	14:49:BC:44:A0:B9	
IP Address	192.168.1.24	
Firmware Version	2.8.1	
Model	VigorSwitch Q2200x	
Online Status	Online	
System Uptime	0d 0h 11m 18s	
Port in Use	1/20	
Clients	3	
Last Process Status	Process Successfully	
	Reboot Now	
	Factory Reset Now	

Available settings are explained as follows:

ltem	Description
Switch Name	Display the name of the switch. Change the name if required.
Reboot Now	Click to reboot the switch immediately with current configuration.
Factory Reset Now	Click to reset the switch with factory default setting.
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.

Port Profile

This page configures the speed, duplex mode, and port profile for each GE port of the VigorSwitch.

					Search
Port	Description	Port Enabled	Port Speed	Duplex	Port Profile
2.5GE1			Auto 😒	Auto \sim	None \sim
2.5GE2			Auto 🗸	Auto 🗠	None 😒
2.5GE3			Auto 😒	Auto 👓	None 🛩
2.5GE4			Auto 😒	Auto \sim	None 🛩
2.5GE5			Auto 🗸	Auto 😒	None 🛩
2.5GE6					
2.5GE7			Auto 😒	Auto ∨	None 😒
2.5GE8			Auto 😒	Auto \sim	None 🛩
2.5GE9			Auto \sim	Auto 😒	None 🛩
2.5GE10			Auto ~	Auto 🗸	None 🗸

ltem	Description				
Port	Display the number of the GE port.				
Description	If required, enter a brief description to explain the device connected to VigorSwitch via the LAN port.				
Port Enabled	The port (e.g., GE2 in this case) which is used to connect VigorSwitch and Vigor router will not be shutdown by Vigor router. Other LAN ports of VigorSwitch allow to connect to any LAN device. When it is checked, after clicking Apply , the network connection between that device and VigorSwitch will be terminated.				
Port Speed	Ethernet speed is set automatically by router system or manually set to 10M/100M/1000M bit/s.				

	• Auto(1000M): Auto speed with 1000M ability only.		
	• Auto(10/100M): Auto speed with 10/100M ability.		
	• 10M: Force speed with 10M ability.		
	• 100M: Force speed with 100M ability.		
	• 1000M: Force speed with 1000M ability.		
	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. For SFP fiber module, you might need to manually configure the speed to match fiber module speed.		
Duplex	Select the duplex mode for the LAN port.		
	Auto – Auto duplex with all capabilities.		
	Full – Auto speed with 10/100/1000M ability only. Allows data transmission in both directions.		
	Half - Auto speed with 10/100M ability only. Allows data transmission in both directions. However, only one device (router or peer's device) is allowed to transmit data at the same time.		
	Duplex		
	Auto 💛		
	Auto		
	Full		
	Fui		
	Half		
Port Profile	Select a port profile to which the LAN port of VigorSwitch will apply.		
Cancel	Discard current settings and return to the previous page.		
Apply	Save the current settings and exit the page.		

Port Status

This page will display the current status of each GE port of the Vigor switch such as the transmission rate (TX/RX), port type, VLAN ID, applied port profile, etc.

General P	ort Profile Port Status						
							Search
Port	Applied Port Profile	Description	Тх	Rx	Port Type	VLAN	Clients
2.5GE1			0%	0%	Trunk	1	0
2.5GE2			0%	0%	Trunk	i	0
2.5GE3			0%	0%	Trunk	1	0
2.5GE4			0%	0%	Trunk	1	0
2.5GE5			0%	0%	Trunk	1	0
2.5GE6			0%	0%	Trunk	1	3
2.5GE7			0%	0%	Trunk	1	0
2.5GE8			0%	0%	Trunk	1	0
2.5GE9			0%	0%	Trunk	1	0
2.5GE10			0%	0%	Trunk	1	0

II-6-3 Port Profile

This page allows you to configure profiles with general settings such as name, group, IP address, MAC address, model, and password required by VigorSwitch when it connects to this Vigor router.

Search	Q.	Switch /	Port Profile						() Reset
Device Menu		Port Pro	ofile						
 Dashboard 		+ Add						Search_	Max: 30
			Profile Name	Enable Port by Schedule	Port Type	PVID	Untagged VLAN	Tagged VLAN	Option
Security	*								
Д ІАМ									
D VPN									
3 Monitoring									
8 Utility									
System Maintenance									
Virtual Controller									
≻ Wireless									
General Setup									
Device									
Maintenance									

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

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

Below is the settings page after clicking **+Add**.

General

Available settings displayed here will vary according to the VigorSwitch managed by Vigor router.

		Advanced Mode: ON
Profile Name 🕕		
General VLAN GVRP	Multicast STP QoS	
PoE Port Enable		
PoE Priority	Critical High Low	
Enable Port by Schedule	Always On Scheduled On	
	herect your options	
Port Isolation		
LACP Priority (1-65535)	1	
LACP Timeout	Short Long	
EEE		

ltem	Description
Profile Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
Advanced Mode:ON/OFF	Click to show or hide the advanced settings.
PoE Port Enable	Switch the toggle to enable/disable the port profile.
Enable Port by Schedule	Set the valid time for the "port profile" when it is applied to specific GE port.
	Always On – The port profile will be valid all the time if it is enabled.
	Scheduled On – The port profile will be valid based on the time schedule specified here.
Options under the Advan	ced Mode
Port Isolation	It allows the network administrator to configure protected port setting to prevent the selected ports from communication with each other. Port isolation is only allowed to communicate with unprotected port. For example, GE1 and GE3 are selected in Port List and Enable is clicked as port isolation, then users behind GE1 and GE3 are separated and can not communicate with each other. Switch the toggle to enable / disable this function.
LACP Priority	Enter a port priority number (1 to 65535) for the port.
LACP Timeout	The timeout option decides how local switch of LAG connection determines connection to be lost. Switch would also notify the remote

LACE FILDING	Enter a port phonty number (1 to 05555) for the port.
LACP Timeout	The timeout option decides how local switch of LAG connection determines connection to be lost. Switch would also notify the remote switch about this setting value, so that remote switch can send LACP PDU in correct timing. Short - LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout. Long - LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout.
EEE	Switch the toggle to enable or disable port EEE (Energy Efficient Ethernet) function for the selected port.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

VLAN

This page allows a user to configure interface (GE) settings related to VLAN.

ofile Name ① General VLAN GVRP Multicast ort VLAN Settings ort Type Hybrid	Advanced Mode: ON
General VLAN GVRP Multicast	
ort VLAN Settings	
ort Type Hybrid	
/ID 🕕 1	
igged VLAN All VLANS	
orbidden VLAN selectyce	

Available settings are explained as follows:

ltem	Description
Profile Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
Port Type	Select the VLAN mode of the interface.
	Hybrid – Support all functions as defined in IEEE 802.1Qspecification.
	Trunk - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
	Access – Accepts only untagged frames and join an untagged VLAN.
	Tunnel - Accepts only untagged frames and join an untagged VLAN.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
	For port under Access/Tunnel Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.
Accepted Type	It is available when Hybrid is selected as the port type.
	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
	All - Accept frames regardless it's tagged with 802.1q or not.
	Tag Only - Accept frames only with 802.1q tagged.
	Untag Only - Accept frames untagged.
Untagged VLAN	It is available when Hybrid is selected as the port type.
	Specify the VLAN profile to be untagged in the VLAN.

Tagged VLAN	Select all VLAN profiles or independent VLAN profiles to be tagged in the VLAN.

Options under the Advanced Mode

Forbidden VLAN	The GE port set in a VLAN profile allows default VLAN packet to pass through. Select the VLAN profile as forbidden VLAN.
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.

GVRP

This page allows the network administrator to configure registration mode (e.g., Normal, Fixed or Forbidden) of GVRP (GARP VLAN Registration Protocol) for each GE port.

Such function can eliminate unnecessary network traffic and prevent any attempt to transmit information to unregistered users.

		×
Profile Name 🕦		Advanced Mode: ON
General VLAN GVRP	Multicast STP QoS	
Enabled	C10	
Dynamic VLAN Creation		
Registration	Normal Fixed Forbidden	
Cancel Apply		

ltem	Description
Profile Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
Enabled	Switch the toggle to enable / disable the GVRP port setting.
Dynamic VLAN Creation	Switch the toggle to enable / disable the VLAN creation.
Registration	There are three modes to be specified. Normal – Default setting. All packets can pass through the selected GE port.

	 Fixed – The selected GE port only sends static VLAN information to neighboring device and allows static VLAN packet to pass through. Forbidden – The selected GE port only allows default VLAN packet to pass through.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

Multicast

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

MLD snooping does the same thing as IGMP snooping. The difference is that IGMP snooping acts on IPv4 packets; MLD snooping acts on IPv6 packets. MLD snooping is the process of listening to Multicast Listener Discovery network traffic. It can examine IPv6 packets and forward these packets to designate location via VLAN port members.

		×
		Advanced Mode: ON
Profile Name 🕕		
General VLAN GVRP	Multicast STP QoS	
IGMP Snooping		
Throttling Max. Group (0-256) 🕕	256	
Throttling Exceed Action	Deny Replace	
MLD Snooping		
Throttling Max. Group (0-256) ()	256	
Throttling Exceed Action	Deny Replace	
Cancel Apply		

ltem	Description
Profile Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
	IGMP Snooping
Throttling Max. Group	Define the maximum number of IGMP group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the IGMP group profiles (defined in Filtering Profile).

Throttling Exceed Action	VigorSwitch will perform the action defined below when the number of IGMP join reports for the specified interface exceeds the value defined in Max Group.
	Deny – It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded.
	Replace – When it is selected, a new group with IGMP report received will replace the existing group.
	MLD Snooping
Throttling Max. Group	Define the maximum number of MLD group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the MLD group profiles (defined in Filtering Profile).
Throttling Exceed Action	VigorSwitch will perform the action defined below when the number of MLD join reports for the specified interface exceeds the value defined in Max Group.
	Deny – It is default setting. The MLD join report (for multicast service) received by such interface will be discarded.
	Replace – When it is selected, a new group with MLD report received will replace the existing group.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning Tree Protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00, or 01:00:0C:CC:CC:CD for Per VLAN Spanning Tree).

Profile Name 🕥		Advanced Mode: ON
General VLAN GVRP	Multicast STP QoS	
BPDU Filter		
3PDU Guard		
riority	128 ~	
dge Port		
2P Option	Auto Yes No	
Cancel Apply		

ltem	Description
Profile Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
BPDU Filter	Switch the togglee to enable / disable the function of dropping all BPDU packets and no BPDU will be sent.
BPDU Guard	BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port. Check it to enable such function.
	Switch the toggle to enable/disable the BPDU Guard function.
Options under the A	dvanced Mode
Priority	Specify a priority value for the switch. The smaller the priority value, the higher the priority and greater chance of becoming the root.
Edge Port	In the Edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change. Switch the toggle to enable / disable the function.
P2P Option	Auto – VigorSwitch determines the STP of link type for this port automatically.
	Yes – It means the STP of link type on this port is full-duplex and directly connect to another switch or host.
	No - It means the STP of link type on this port is "not" full-duplex and "does not" directly connect to another switch or host.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

QoS

This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

			Advanced Mode: ON
Profile Name 🕕			
General VLAN GVRP	Multicast STP	QoS	
ngress Default CoS	0 ~		
Egress Remark CoS			
Egress Remark DSCP/IP Precedence	Disabled DSCP	IP Precedence	
Enable Ingress Rate Limit			
Enable Egress Rate Limit	0		
Cancel Apply			

Available settings are explained as follows:

ltem	Description
Profile Name	Enter a name for the Switch. The purpose of name is used for identification.
	It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router.
Ingress Default CoS	Specify the default CoS priority value for those ingress frames without given trust QoS tag (802.1q/DSCP/IP Precedence, depending on configuration).
Egress Remark CoS	Switch the toggle to enable/disable the function.
Egress Remark DSCP/IP	Disabled - Select to disable this function.
Precedence	DSCP - Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table.
	IP Precedence - Egress traffic will be marked with IP Precedence value according to the Queue to IP Precedence mapping table.
Enable Ingress Rate Limit	This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.
	Switch the toggle to enable/disable the function.
	Ingress Rate Limit - Enter the rate value (16-1000000), unit:16 Kbps.
Enable Egress Rate Limit	This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.
	Switch the toggle to enable/disable the function.
	Egress Rate Limit - Enter the rate value (16-1000000), unit:16 Kbps.

Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

II-6-4 Maintenance

Vigor router can backup, restore, reboot, or reset the managed Vigor switch devices.

Search Q	Switch / Maintenance	
Device Menu	Maintenance	
 Dashboard 	alera a	
	Select Action	
⊘ security	Action Type	Config Backup 👒
Д им	Select Device	
O VPN	> Existing Device	+ Add Max: 1
🔂 Monitoring	x	Switch Name MAC Address IP Address Option
88 Unliky	2	(maintenance) (maintenance)
🖏 System Maintenance	s.	Back up
Virtual Controller		
}+ Wireless	¥.	
Switch		
General Setup Device		
Port Profile		
Miletterance		

ltem	Description
	Selection Action
Action Type	There are four types of action that can be performed on Vigor switch by Vigor router.
	Config Backup – Backup current configuration of Vigor switch.
	Config Restore – Restore the configuration of Vigor switch with backup file.
	Remote Reboot – Reboot the Vigor switch remotely by Vigor router.
	Factory Reset – Reset the Vigor switch remotely by Vigor router.
	Select Device
Existing Device	+Add – Click to add a new device that will be applied with the settings configured above.
	At present, only one device can be added in this field.
	For the Action Type set as Config Backup :
	 Backup – Click to make a backup copy for the current configurations of the selected device(s) (listed on Existing Device list).
	For the Action Type set as Config Restore :
	• Restore - Click to locate the backup file for restoring.
	 Restore - Click to restore the configuration of the selected device(s) (listed on Existing Device list) with the backup file.
	For the Action Type set as Remote Reboot :

 Reboot – Click to reboot the remote switch (managed by Vigor router) with current configuration.
For the Action Type set as Factory Rest :
 Reset – Click to reset the selected device(s) (listed on Existing Device list) with the factory default switch settings.

Chapter III Management



III-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Device Settings, Management, Firmware, Backup & Restore, Accounts and Reboot System, and Firmware Upgrade.

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.

	Q	System Maintenance / Device Settin	ings (OR	efresh
		Time Device Name Syslog	SNMP	
Device Menu		Time and Date		
(?) Dashboard		Time and Date		
n Configuration	2			
Security	2	System Time		
A IAM	÷	System Time	2021-10-25 16:39:27	
VPN	÷	Time Setting		
	×			
88 Utility	5	Sel Time	Automatically with Time Server Manually	
🗞 System Maintenione	8	Time Zone	Nută Marusalij	
			(UTC) Greenwich Mean Time : Dublin 🛛 🗸	
Management		Time Server ①	time.google.com	
System Upgrade				
Backup & Restore		Interface	Auto 🗸	
Account & Permissi	ion	Test Time Server	Test Time Server Connection	
System Reboot Registration & Servi	ine.	Server Status		
registration & serv				
Virtual Controller		More settings ~		
}⊷ Wireless	5-			
		Cancel Apply		

Available parameters are explained as follows:

ltem	Description			
System Time				
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 selected as Set Time	Time Zone - Select the time zone where the router is located.Time Server - Enter the web site of the primary time server.Interface - Renew the time through the selected WAN/LAN interface. If			

	Auto LAN.	is sele	cted, t	ne Vi	gor s	ystem	n will r	enew the	e time through WAN o
	Test Time Server Connection – Test if the time server works well.								
	Serve	r Statu	is - Di	splay	s last	upda	te tim	e status.	
	More	Settin	gs - Cl	lick to	o opei	n adva	anced	settings	for the time server.
	 Auto Update Interval - Select the time interval (30min or 60min) at which the router updates the system time periodically. 								
	•		-				-	•	me server, please condary Server.
	•	WAN/ renew and is prima syster Daylig featur Daylig	LAN ir v the ti used ry tim n will t ht Sav e. tht Sav	nterfa ime t as th e ser use t /ing F ecify	ace. If hroug e inte ver fa he se Swite Perioc the s	Auto gh WA erface hils to conda ch the tarting	is sele N or I for th renev ary tin togg s avail g time	ected, the _AN. This ne backup v the tim ne server le to ena able whe	bugh the selected e Vigor system will is an optional setting p time server. If the e setting, the Vigor instead. ble/disable the en Daylight Saving is e ending time if "by
When Manually is	Time	Zone -	Selec	t the	time	zone	where	e the rou	ter is located.
selected as Set Time	Date	- Use t	he dro	op-do	own c	alend	ar to s	specify co	orrect date.
	1	2021-04	4-26			10	1		
		202	1 APR	-			<	>	
				1					
		APR	÷			Ť	ź	3	
		4	5	6	7	8	9	10	
			1	2	1		1		
					14	15	16	17	
		11	12	13	14				
		11 18	12 19	13	21	22	23	24	
				20	21				
		18				22 29	23 30		
		18		20	21				
	Synch	18 25 - Set th	19 23 ne tim	20 27 e by Brow	21 28 speci	29 fying	30 hours	24 , minute:	s, and seconds. /nc the time setting
Apply	Synch with t	18 25 - Set th nronize the bro	19 23 ne tim e with owser.	20 27 e by Brow	21 28 speci /ser -	29 fying Click :	30 hours Sync i	24 , minute:	vnc the time setting

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

III-1-1-2 Device Name

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

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

	System Maintenance / Device Settings	3 Reset
	Time Device Name Syslog SNMP	
Device Menu	Device Name	
 Dashboard 		
🖆 Configuration 💦 👌	Device Name 🕥 DrayTek-86FAB8	
🤉 Security 💦 💡		
⊊им ⇒		
D VPN 5		
I Monitoring 5		
8 Utility >		
Management		
System Upgrade		
Backup & Restore		
Account & Permission		
System Reboot		
Registration & Services		
'irtual Controller		
🛏 Wireless 💡		

III-1-1-3 Syslog

SysLog function is provided for users to monitor the router.

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

	System Maintenance / De	ice Settings	() Rese
		Syslog SNMP	
Device Menu	Durlas Cattlens		
 Dashboard 	Syslog Settings		
Configuration	> Logging Destinations	External Server	
Security	> Log Message	User Access Log	
£, IAM	5	All Interface Log	
D VPN	*	C WAN Log	
Honitoring	2	Z LAN LOg	
B2 Utility		Firewall Log	
	>	IAM Log	
		VPN Log	
		System Log	
Management		WiFi Basic Log	
System Upgrade		Mesh Log	
Backup & Restore		APM Log	
Account & Permission	and the second sec		
System Reboot	Syslog Servers		
Registration & Services	+ Add	Mass 3	
Virtual Controller	Server IP ()	Port 0	
}→ Wireless	>		
	Cancel Apply		

Available parameters are explained as follows:

ltem	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.
Cancel	Discard current settings and return to the previous page.

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.

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

- 1

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	Any - Any IP can be set as the manager host.			
Host	Specific Host - Specify a host (IPv4 or IPv6) or hosts (both IPv4 and IPv6).			
	• IP Type – Select Both, IPv4 or IPv6.			

	• Specific Manager Host (IPv4/IPv6) is available when IPv4/IPv6 is selected		
	as the IP Type. Click +Add to have a new entry.		
	Enter the IPv4 address with subnet mask / IPv6 address with specified prefix length of hosts that are allowed to issue SNMP commands. If these fields are left blank, any IPv4/IPv6 LAN host is allowed to issue SNMP commands.		
	Query		
Get Community	Enter the Get Community string. The default setting is public . Devices that send requests to retrieve information using get commands must pass the correct Ge Community string.		
Set Community	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.		
Query Port	Displays the port number used by the query server.		
	Agent		
SNMPv3	Switch the toggle to enable/disable the SNMPv3 function.		
Agent Enabled	If enabled, specify corresponding settings. Click +Add to have a new entry.		
SNMPv2c Agent Enabled	Switch the toggle to enable/disable the SNMPv2 function.		
SNMPv1 Agent Enabled	Switch the toggle to enable/disable the SNMPv1 function.		
	Тгар		
Enabled	Switch the toggle to enable/disable the Trap function.		
Trap Version	Select the trap version. V1 V2c		

Trap	Enter the Trap Community string. The default setting is public. Devices that
ap	Enter the hap commany string. The derivate setting is public, bettees that

• V3

Community	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.	

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. After a user has been authenticated by means of a username and password, he or she can be granted Internet access, and optional firewall rules and WAN access policies can be applied.

	۹	System M	laintenance / M	anagement				
Device Menu		Service Co	ontrol TR-00	9 XMPP				
Dashboard		General						
E Configuration	5	Auto Logo	i.i.	C.	off	~		
Security	5							
		Login Valid	dation Code	3.	9			
g, i∧m	2	Manager	ment Services					
D VPN	2	1.1.1						
Monitoring	2.	Enforce H	TTPS Access		30			
8 Utility	5	LLDP			D			
			Port ()	(default)	LAN Access	IPv4 WAN Access	IPv6 WAN Access	
Device Settings		HTTP	80	(80)				
System Upgrade		nure	80					
System Opgrade Backup & Restore		HTTPS	443	(443)	•			
Account & Permission		SSH	22	(22)	•			
System Reboot		Telnet	23	(23)			0	
Registration & Service	s	SNMP	161	(161)				
irtual Controller		Avanue.	IVI	(191)	-			
- Wireless	5	Note: Por	ts 8001 / 8123	8143 are re	served for Ho	tspot Web Portal.		

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		\sim
off		
1 m	n	
3 m	n	
∋fault) 5 m	n	
²⁾ 10 r	nin	
3)		1

	Management Services		
Enforce HTTPS Access	Switch the toggle to enable/disable the feature of allowing system administrators to login Vigor router via HTTPS.		
LLDP	Switch the toggle to enable/disable the LLDP service.		
Port	Specify user-defined port numbers for the HTTP, HTTPS, SSH, Telnet and SNMP servers.		
LAN Access	Select the checkbox to allow the system administrators to login from LAN interface. Later, configure the LAN Access Control below to determine who (the client) is able to access the LAN management services (HTTP, HTTPS, SSH, Telnet and SNMP).		
IPv4/IPv6 WAN Access	Select the checkbox to allow the system administrators to login from IPv4/IPv6 WAN interface. Later, configure the WAN Access Control below to determine who (the client) is able to access the IPv4 WAN management services (HTTP, HTTPS, SSH, Telnet and SNMP).		
	TLS Encryption		
TLS 1.3/TLS 1.2	Switch the toggle to enable or disable the function.		
	Access Control List		
WAN Access Control	In general, all the clients via WAN interface can access the IPv4 WAN management services (based on the HTTP, HTTPS, SSH, Telnet and SNMP checkboxes selected).		
	WAN Access Control Mode – Select Disabled or Allow List.		
	• Disabled - The default is Disabled .		
	 Allow List – Click +Add to have a new entry. The maximum number you can add is up to 6. 		
	Only the chosen IP objects within the selected IP group object can access the services listed on this page via the WAN interface.		
LAN Access Control	In general, all the clients via LAN interface can access the LAN management services (based on the HTTP, HTTPS, SSH, Telnet and SNMP checkboxes selected).		
	LAN Access Control Mode - Select Disabled or Allow List.		
	• Disabled - The default is Disabled .		
	 Allow List - Click +Add to have a new entry. The maximum number you can add is up to 6. 		
	Only the chosen IP objects within the selected IP group object can access the services listed on this page via the LAN interface.		
Cancel	Discard current settings and return to the previous page.		
Apply Save the current settings and exit the page.			

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.

	System Maintenance / Ma	nagement	③ Reset C Refresh
	Service Control TR-069	XMPP	
Device Menu	ACS and CPE Settings		
(?) Dashboard			
🚔 Configuration 🤅	TR-069		
Security 5	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.		
Se IAM	ACS Server		
O VPN	ACS Server On	[WAN] WAN1 (Wired WAN) ~	
Monitoring	5	[WAN IP](WANT) ~	
88 Utility ,		https://	
	iP/Domain 💿	Witard	
Device Settings	Username 🕢		
		Note: Username support characters: a.z.A.Z.0.9_@,%	
System Upgrade			
Backup & Restore	Password ()	@	
Account & Permission System Reboot		Note: Password support characters: a-z,A-Z,0-9,%65/()=?*@#	
Registration & Services			
Registration & sciences	Test Connection		
Virtual Controller			
> wireless			
	Cancel Apply		

ltem	Description			
TR-069	Switch the toggle to enable or disable the function.			
	ACS Server			
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server.			
IP/Domain	Enter the IP/domain 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.			
	Test Connection			
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.			
	More settings			
CPE Client	This section specifies the settings of the CPE Client.			
	Protocol - Select HTTPS if the connection is encrypted; otherwise select 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 router to send notification to CPE. (1-65535)
STUN Settings	Mode - The default is Auto . 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 (1-65535) 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.

III-1-3 System Upgrade

III-1-3-1 Firmware

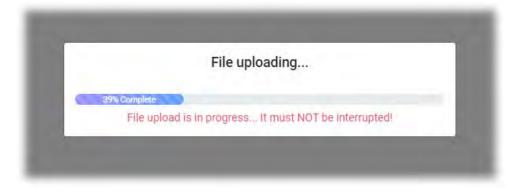
Before firmware upgrade, please **download** the newest firmware from the DrayTeks website or FTP site **first**. The DrayTek website is www.draytek.com (or local DrayTeks website) and the FTP site is ftp.draytek.com.

Open **System Maintenance>> System Upgrade**. 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	۹		System Maintenance / System Upgrade Firmware Country Object Database					
Device Menu		Firmware						
(?) Dashboard		raniware						
		Current Firmware Version	5.3.1_RC3					
Security	>	Firmware for upload	12 Upland					
Д им	>		Note: .sfw: .sfw is selected when you want to update the firmware of Vigor device to a newer version while relaining the existing configuration.					
VPN	*		.rst: .rst is used to reset configuration, but retaining service status. (product registration, license keys, and certificates)					
88 Utility	2							
System Manureaver								
Device Settings								
Management.								
System Opgrade Backup & Restore								
Account & Permission								
System Reboot								
Registration & Services								
Virtual Controller								
S→ Wireless	>							

Click 🗀 to locate the firmware from your host.

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



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



Wait for a while until the system finishes the rebooting.

- 1

III-1-3-2 Country Object Database

GeoIP database provides information for Classless Inter-Domain Routing (CIDR) and location. Vigor router adopts the geographical distribution based on the GeoIP database offered by MaxMind.

If required, update the GeoIP database.

Search	۹	System Maintenance / Syst			C Refresh
	-	Firmware Country Obje	ect Database		
Device Menu	-	Country Object Databas	e		
(7) Dashboard					
		D By clicking Upgrad	e Now or enabling Automatic Upgrad	les, you agree to the terms and policy of Maxmind License.	
Security	>	C 27 51 51 51 50 510		and the other state of the state based on the state of th	
A IAM	*	Last Checked Time	2021-10-25 17:15		
D VPN	>	Current Version	20241119		
E Monitoring		Latest Version			
82 Utility		Last Upgrade Time			
System Managemen					
Device Settings			Upgrade Now		
Management		Upgrade Schedule	O Off	Upgrade later	Repeat
System Upgrode			Note: To ensure data integrity	and prevent potential conflicts, all relevant functions are suspended during database update	k:
Backup & Restore					
Account & Permission					
System Reboot					
Registration & Services					
Virtual Controller					
>• Wireless					

Available settings are explained as follows:

ltem	Description			
Upgrade Now	Click to upgrade the GeoIP database.			
Off/Upgrade later/Repeat	Off – There is no need to upgrade the database, even when a new version is available. Upgrade Later – Allow to specify a time to upgrade the database.			
	 Start Date – Use the drop-down calendar to specify correct da 			
	2021 APR - < >			
	a a t a t a a			
	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 27 28 29 30			
	 Start Time - Use the drop-down list to select the time. 			
	Repeat – The system will check for any new version updates on the first day of every month.			
	• 1 st of each month at - Use the drop-down list to select the tim			

III-1-4 Backup & Restore

This function can be used to backup/restore the Vigor router settings.

Search	q	System Maintenance / Backup & F	lestore	
Device Menu		Configuration Backup & Restor	e	
(?) Dashboard		Configuration Backup		
	>			
Security	,	Password Protection		
S IAM	5	New Password 🕖	0	
O VPN		Confirm New Password ()	0	
🖸 Monitoring			At least 8 characters	
			Uppercase characters	
BS Utility	2		Lowercase characters	
			Numbers or Special characters _ (D:./·#₩()1?*
Device Settings				
Management			Back up	
System Upgrade				
		Restore from a Configuration B	ackup	
Account & Permission				
System Reboot		Restore from Backup File		Restore
Registration & Services		Restore except the login password		
Virtual Controller		File has Password Protection		
>- Wireless	2	Restore Password ①	6	

Item	Description
	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.
New Password/ Confirm New Password	Enter several characters as the password for encrypting the configuration file.
Back up	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 your current administration account and password. It allows the network administrator to manage Internet access at the user level.



III-1-5-1 Local Admin Account

This page allows you to create up to five local admin account profiles.

	۹		ntenance / Account &						TReset C Refrest
Device Menu		Local Admir	Account Role & I	Permission					
(2) Dashboard		Local Adm	in Account						
Configuration		+ Add							Mac
Security		Account	Role	Status	Allow Login from WAN	Last Login at	Last Login IP	Created Time	Option
	·	admin	Administrator	Active	Disable	2021-10-25 15:43:45	192.168.1.100	2021-10-24 09:07:52	@ Edit
🧯 іам	2								
D VPN	5								
편 Monitoring	*								
8 Utility	÷								
Device Settings									
Management									
System Upgrade									
Backup & Restore									
System Reboot									
Registration & Services									
Virtual Controller									
┝• Wireless									

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

DeleteRemove 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**.

Account ()	Carrie	
lew Password 🕕	······· •	
Confirm New Password 🕕		
	✓ At least 8 characters	
	V Uppercase characters V Lowercase characters	
	 Covertage transmission Numbers or Special characters ~!@#\$\$%*&*()_=/?[]{+>\ 	
Role	Users 🗸	
itatus	Active 🗸	
llow Login from WAN		
nable Email		
mail	carrie_ni@draytek.com	
nable SMS		
MFA		
Enable MFA		
Cancel Apply		

ltem	Description
	Local Admin Account
Account	Display the name of the account.
New Password	Enter a new password in this field.
Confirm New Password	Enter the new password again.
Role	 Specify the role of the account. Administrator Guest Users (created on the Role & Permission page)
Status	Active - Enable the selected account profile. Inactive - Disable the selected account profile.
Allow Login from WAN	It is available if "Router Management" is selected as the usage. If enabled, the user can login from WAN by using this user account.
Enable Email	Switch the toggle to enable or disable the email setting. Email – Enter the email address for receiving the MFA PIN code.
Enable SMS	Switch the toggle to enable or disable the SMS setting. SMS - Enter the destination SMS number for receiving the MFA PIN code.
	MFA
Enable MFA	Switch the toggle to enable/disable the function of Multi-Factor Authentication (MFA).

Allowed MFA Method - Select to require TOTP, Email, SMS or mOTP authentication when logging in to Vigor router.

Enable MFA	
Allowed MFA Method	salast your polices 🛛 ∧
Account Info	Select All
Created Time	Search
	TOTP.
	Email
	SMS
	mOTP

TOTP – For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone.

TOTE		8
Secret: JBLU	UMZRXMJCUE4JPNRIEKYTDNE2DERKWJKDARBYKA4W44DP656D	QUDFRZ4X527P
QR Code: Validation C		
		tion and make

In the filed of Validation Code, enter the one-time password and click Verify.

Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.

SMS/Email – The password will be transferred via the SMS and/or Mail profiles selected from User Information above.

mOTP - Mobile one-Time Password (mOTP) allows the use of mOTP passwords. Enter the **PIN Code** and **Secret** settings for getting one-time passwords.

	Account Info
Created Time	Display the created time of the user account.
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 the creation of up to five roles which can be applied to the local admin account. The default roles are Administrator, Guest and Users.

search Q	System Maintenance / A	Account & Permission				
	Local Admin Account	Role & Permission				
evice Menu	Role & Permission					
) Dashboard						
Configuration >	+ Add				Max: 5	
Security						
, IAM >	Role	Administrator	Guest	Users		
VPN >	Left Menu Path					
Monitoring >	 Device Menu 	Deny	Deny	Deny	~	
	 Dashboard 	Read-write	Read-only	Read-only	*	
ttility >	 Configuration 	Read-write	Read-only	Read-only		
System Maintenance	P Coniguration	Nead-write	Read-Only	Read-only	-	
Device Settings	► Security	Read-write	Read-only	Read-only	~	
Management	▶ IAM	Read-write	Read-only	Read-only	*	
System Upgrade Backup & Restore	VPN.	Read-write	Read-only	Read-only	U.	
Account & Permission	► Monitoring	Read-write	Read-only	Read-only		
System Reboot				_		
Registration & Services	 Utility 	Read-write	Read-only	Read-only	v	
and for the line	 System Maintenan 	ce Read-write	Read-only	Read-only	•	
rtual Controller	 Virtual Controller 	Deny	Deny	Deny	•	
Wireless >	▶ Wireless	Read-write	Read-only	Read-only		

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

ocal Admin Account	Role & Permissio	n User 8	MFA Security		
			, mini ocounty		
Role & Permission					
+Add					Max: 5
Role	Administrator	Guest	Users		Role_1
Left Menu Path					道 Delete
Device Menu	Deny	Deny	Deny	*	Deny 🗸

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 User & MFA Security
	Role & Permission
	+Add Max: 5
	Role Administrator Guest Users Role_MKT ×
	Left Menu Path 🔟 Delete
	► Device Menu Deny Deny ► Deny ►
	► Dashboard Read-write Read-only Read-only • Read-only •
	► Configuration Read-write Read-only Read-only V Read-only V
	► Security Read-write Read-only Read-only ▼ Read-only ▼
	 The role of Administrator has the highest authority for accessing V router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or
	router. The role of Guest/Users has the lowest authority for accessing Vigo
Delete	 router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard,
Delete	 router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard, configuration, device menu, etc.) individually
Delete Read-only V	 router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard, configuration, device menu, etc.) individually Remove the selected user-defined role profile.
	 router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard, configuration, device menu, etc.) individually Remove the selected user-defined role profile. Specify the permission for each menu item for the user-defined role allowed for the user-defined role profile. Read-only - The permission for the menu item on the left side is not allowed for the user-defined role profile.
	 router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard, configuration, device menu, etc.) individually Remove the selected user-defined role profile. Specify the permission for each menu item for the user-defined role allowed for the user-defined role profile. Read-only - The permission for the menu item on the left side is not allowed for the user-defined role profile.
Read-only 🗸	 router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard, configuration, device menu, etc.) individually Remove the selected user-defined role profile. Specify the permission for each menu item for the user-defined role allowed for the user-defined role profile. Read-only - The permission for the menu item on the left side is not allowed for the user-defined role profile.
Read-only 🗸	 router. The role of Guest/Users has the lowest authority for accessing Vigorouter. The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard, configuration, device menu, etc.) individually Remove the selected user-defined role profile. 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. Read-only - The permission for the menu item on the left side allow for the user-defined role profile to be read-only. Read-write - The permission for the menu item on the left side

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

		×
Account ()	Carrus	
New Paraword ()	(a)	
Confirm New Pasaweril 🕥		
	+ At loss 6 characters	
	Upperclase characters	
	/ Lowerclase characters	
	- Mumbers of Special covariants $\omega = (10756, 670), -(751)(169)$	
0000	None	
Blakers -	None	
ilaw Logra Porro WAN	Administrator	
natių Email	Guest	
nably SMS	Upers-	
MFA	Fole MAT	
obble MFA	0	
Account Info		
Cancel Apply		

III-1-6 System Reboot

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

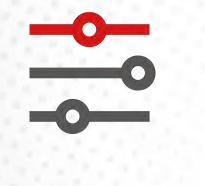
Search	۹	System Maintenance / System Re	boot
Device Menu	8	System Reboot	
(?) Dashboard		Reboot With	Curren Canligunation Reset Canligunation Reset to Focusy Default
	×.		Reboot
⊘ security	×.		Note: Reset Configuration: Reset configurations, retaining service status (product registration, license keys, and certificates), is recommended for
A∎ IAM	3		nori sale/return of ylgor devices.
D VPN	\$		Reset to Factory Default: Revert all settings to factory default, including service status (product registration, license keys, and certificates). Is recommended when selling/returning Vigor devices.
🔂 Monitoring	5		
😫 Utility	5	Auto Reboot Time Schedule	
🗞 System Malaterator		Enable Auto Reboot Schedule	
Device Settings Management		Schedule Profile	Jaiect your obtions
System Upgrade			Note: 1. End Time in the schedule reboot will be ignored.
Backup & Restore			2. Time setting recommend to use Automatically with Time Server.
Account & Permission			
System Repoot			
Registration & Services			
Virtual Controller			
≻ Wireless	>		
The Products		Cancel Apply	

Available settings are explained as follows:

ltem	Description			
Reboot With	Select one of the following options, and press the Reboot button to reboot the router.			
	Current Configuration – Select this option to reboot the router using the current configuration.			
	Reset Configuration – Select this option to reset the router while retaining service status (product registration, license keys, and certificates).			
	Reset to Factory Default – Select this option to reset the router's configuration to the factory defaults before rebooting.			
Auto Reboot Time Schedule	Enable Auto Reboot Schedule – Switch the toggle to enable or disable the function. If enabled, Vigor router will reboot automatically based on the schedule profile.			
	Schedule Profile – Use the drop-down list to select the profile(s).			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

This page is left blank.

Chapter IV Others



IV-1 Monitoring

IV-1-1 Clients List

Clients List displays the configuration status of the wireless clients that connect to the Vigor router via Wi-Fi connection.

Besides, this page offers a quick method to add the wireless client to any existing MAC Filtering Profile.

Security >	Monitoring / Clients List	C Refresh
.} IMM →	Clients List	
🛆 VPN 🕠	Cients List	
· Montoring	S Add MAC Filtering from Clients	Search 🚊 🐵
Climits) and Log Center	Name MAC Up Link RSSI SSID Unage Unage Time Speed RSSI Up Down	IP CH Band BW PSM Physical Auth Encrypt Mode Mode Type
Wireless Information WAN		
ARP Table		
Route Table		
DHCP Table		
IPv6 TSPC Status		
IPv6 Neighbor Table		
LLDP Neighbors information		
DNS Cache Table		
LTE Status		
Remote DSL Status		
PPPoE Pass-Through		
Session Table		
28 Utility ,		
🍕 System Maintenance 💦 🥎		
Virtual Controller		

To add the wireless client(s) onto an existing MAC Filtering Profile, click **Add MAC Filtering from Clients** to open the following page.

dd MAC Filtering from Cli	ents		
Add to MAC Filtering Profile	Please Select	\sim	
Update Client List	Update		
Clients			
Add to MAC Filtering		Name	MAC
			Close Apply

ltem	Description
Add to MAC Filtering Profile	Select one of the MAC filtering profiles (Security>>MAC Filtering Profile) as the filtering basis.

Update Client List	Update – Click connection.	to renew the cl	ient list based	d on the acti	ual wireless	
	Update Client List	Update				
	Clients					
	Add to MAC Filterin	g Na	ne	MAC		
	ē			72:3C:59:06:2B:78		
				B6:8F:21:92:DD:8A		
					Close Apply	
Clients	Displays the SSID name, MAC address, and IP address of the wireless clients.					
	Filtering Profile	tering – Select t e set above. a name for iden		vireless clier	nt join the MAC	
Close	Discard current settings and return to the previous page.					
Apply	To check if the	nt settings and new added wir Security>>MAC	eless clients o	on the MAC	Filtering profile	
	Security / MAC Filtering Profile					
	Name Policy Device List	test2 Disavied <u>Aview Ltst</u> Envisi Lis]	- Search	Macri 201	
	DEVICE LIN	Name	MAC Address ③		Option	
		Andy	72:3C:59:06:28:7	8	@ Delete	
		Carrie	B6:8F:21:92:DD:	łA	Deret+	

Click **Apply** to save the settings.

IV-1-2 Log Center

IV-1-2-1 Log Center

Log related to setting configuration and/or actions performed by this device can be stored on web Syslog. Click **Refresh** to reload this page with the most up-to-date information.

⊘ security >	Monitoring / Log Center							CRefresh
🔏 IAM 🤅	Log Center DDNS Log							
🛆 VPN >								
😔 Monkoung	Log Center							
Clients List	Enabled Web Syslog							
Log Center Wireless Information	Loop Logging Option	Diverride Oldest Logs Stop when Full						
WAN	Export as TXT Z Expo	rt as JSON 🔮 Clear All		Filter:	All Type	~	Search_	Max: 1000
ARP Table Route Table	Time	Туре	Content					
DHCP Table								
IPv6 TSPC Status								
IPv6 Neighbor Table								
LLDP Neighbors information								
DNS Cache Table								
LTE Status								
Remote DSL Status								
PPPoE Pass-Through								
Session Table								
😫 utility 🔅 👌								
🖏 System Maintenance >								
Virtual Controller	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 as TXT, JSON	Click it to export the log records as a file (.txt, .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-1-2-2 DDNS Log

This page displays the log (time, profile name and content) related to Dynamic DNS actions performed by this device.

Security	Monitoring / Log Center				CRefre
NM :	Log Center DDNS Log				
D VPN					
	DDNS Log				
Clients List				Search	Max: 2
	Time	Profile Name	Content		
Wireless Information					
WAN					
ARP Table					
Route Table					
DHCP Table					
IPv6 TSPC Status					
IPv6 Neighbor Table					
LLDP Neighbors information					
DNS Cache Table					
LTE Status					
Remote DSL Status					
PPPoE Pass-Through					
Session Table					
Utility					
System Maintenance					

IV-1-3 Wireless Information

For viewing the SSIDs used by 2.4GHz/5GHz or real time throughput for 2.4GHz/5GHz, open Monitoring>>Wireless Information for detailed.

IV-1-3-1 Wireless Information

This page shows general information (e.g., 2.4GHz/5GHz enabled or not, MAC address, SSID name and etc.) for wireless connection.

Device Menu	Monitoring / Wireles	is Information	C Refresh
(2) Dashboard	Wireless Information	Recent Activities Real Time Throughput 2.4G Real Time Throughput 5G	
n Configuration	Wireless Informati	ion	
Security			
A IAM	2.4GHz		
O VPN	Radio	Enable	
10 Monstoring	MAC	14:49:BC:86:FA:88	
Clients List	Have .		
Log Center	SSID(1)	DrayTek-86FAB8	
WatelessinTermition	1.1.1		
WAN	5GHz		
ARP Table	Radio	Enable	
Route Table			
DHCP Table	MAC	16:49:8C:56:FA:88	
IPv6 TSPC Status	\$51D(1)	DrayTek-86FAB8	
IPv6 Neighbor Table			
LLDP Neighbors information		See More 4	
DNS Cache Table			
LTE Status			
Remote DSL Status			
PPPoE Pass-Through			

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

Click See More+ to view more information.

IV-1-3-2 Recent Activities

The activities regarding to wireless network can be shown with line graphs.

(*) Dashboard	Monitoring / Wireless In	formation				CRefresh
🗯 Configuration 💦 >	Wireless information		Real Time Throughput 2.4G	Real Time Throughput 5G		
⊘ Security >	-		time time to and particle	treat three threeds that and		1
A∎ IAM >	Recent Activities					
O VPN	Last 24 hours 😽					
B Monlaung	2.4 Ghz					6.000
Log Center	1.0					Clienta 1.0
Workliss Information	() () () () () () () () () () () () () (0.5 D
ARP Table	1					
Route Table	10 444		-4'Pm'	70 P.M	1.2.51	
DHCP Table	5 Ghz					and a set
IPv6 TSPC Status	1.0					Throughput Caerca
IPv6 Neighbor Table	2.2					
DNS Cache Table	(treudiput (tree)					0.5 fl
PPPoE Pass-Through Session Table						
88 Utility >	10 AM		4.9078	TO PW	-1 AM -	n.
System Maintenance	Usage per SSID					×
Virtual Controller	2.4 GHz					

IV-1-3-3 Real Time Throughput 2.4G

The real-time throughput (2.4G) can be shown with line graphs.

Device Ménu	Monitoring / Wireless information	CRefresh
(?) Dashboard	Wireless Information Recent Activities. Real Time Throughput 7.4G Real Time Throughput 5G	
	Real Time Throughput 2.4G	
Security >		
A IAM S	10	
() VPN	0.9	
ES MAINABLE	05	
Clients List	07	
Log Center	06	
Wreest information		
WAN	P 0 0 0	
ARP Table	E 04	
Route Table	03	
DHCP Table		
IPv6 TSPC Status	0.2	
IPv6 Neighbor Table	0.1	
LLDP Neighbors information	0	
DNS Cache Table	de < 1 Kbps < 1 Kbps	
LTE Status		
Remote DSL Status		
PPPoE Pass-Through		

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

IV-1-3-4 Real Time Throughput 5G

The real-time throughput (5G) can be shown with line graphs.

Device Menu	Monitoring / Wireless information	CRefresh
 Dashboard 	Wireless Information Recent Activities Real Time Throughput 2.4G Real Time Throughput 5G	
Configuration >	Real Time Throughput 5G	
Security >		
д им ,	10	
O VPN	0.9	
E Mantana	80	
Clients List	07	
Log Center	0.6	
annungs Information	the second s	
WAN ARP Table	04	
Route Table	P 0.4	
DHCP Table	0.3	
IPv6 TSPC Status	62 ·····	
IPv6 Neighbor Table	0.1	
LLDP Neighbors information	9	
DNS Cache Table	.≟.<1 Kbps	
LTE Status		
Remote DSL Status		
PPPoE Pass-Through		

IV-1-4 WAN

This page can display the WAN connection status, including the connection interface, MAC address, connection type, connection IP address, connection gateway, primary DNS and secondary DNS server addresses, online Time, and so on.

IV-1-4-1 WAN Utilization

This page displays the utilization, including upload, download, and percentage of data transmission for each WAN interface.

Device Menu	Monitoring / WAN				C Refresh
(2) Dashboard	WAN Utilization WAN St	atus			
🛎 Configuration	> WAN Utilization				
Security	2				
S. IAM	Name	Upload	Download	Utilization	
D VPN	WAN] WAN1	0.0 B	0.0 B		0%
	[WAN] WAN2	0.0 8	0.0 B		0%
Clients List	[WAN] WAN3	0.0 B	0.0 B		0%
Log Center					
Wireless information	[WAN] WAN4	0.0 B	0.0 8		0%
	[WAN] WANS	0.08	0.0 B		0%
ARP Table	and the second se				
Route Table					
DHCP Table					
IPv6 TSPC Status					
IPv6 Neighbor Table					
LLDP Neighbors information					
DNS Cache Table					
LTE Status					
Remote DSL Status					
PPPoE Pass Through					

IV-1-4-2 WAN Status

IPv4

Select the IPv4 tab to display the IPv4 WAN connection status.

Device Menu	Monitoring / WAN							CRefrest
 Dashboard 	WAN Utilization	WAN Status						
🚖 Configuration	WAN Status							
Security	PV4 IPV6							
S. IAM								
D VPN	Name	MAC Address	Connection Type	IP Address	Gateway	Primary DNS	Secondary DNS	Uptime
	[WAN] WAN1	14:49:8C:86:FA:89	DHCP			8.8.8.8	8.8.4.4	00:00:00
Clients List	(WAN) WAN5	00:50:7P:00:00:55	DHCP			8.8.8.8	8.8.4.4	00:00:00
Log Center	10000							
Wireless Information								
ARP Table								
Route Table								
DHCP Table								
IPv6 TSPC Status								
IPv6 Neighbor Table								
LLDP Neighbors information								
DNS Cache Table								
LTE Status								
Remote DSL Status								
PPPoE Pass-Through								

IPv6

Select the IPv6 tab to get the WAN connection information (e.g., name, IPv6 address, connection type, gateway and the uptime).

Device Menu		Monitoring / WAI	N			CRetresh
(?) Dashboard		WAN Utilization	WAN Status			
	× 12	WAN Status				
Security	,	10.10				
A IAM		IPv4 IPv6	_			
O VPN		Name	IPv6 Address	Connection Type	Gateway	Uptime
Clients List						
Log Center						
Wireless Information						
ARP Table						
Route Table						
DHCP Table						
IPv6 TSPC Status						
IPv6 Neighbor Table						
LLDP Neighbors information						
DNS Cache Table						
LTE Status						
Remote DSL Status						
PPPoE Pass Through						

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

IV-1-5 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.

IV-1-5-1 LAN

Click **Refresh** to reload this page with the most up-to-date information of LAN Ethernet ARP table.

Device Menu	Monitoring / AR	P Table				CRefresh
 Dashboard 	LAN WAN					
Configuration	> LAN Ethernet	ARP Table				
Security	× the Clear All					rch
Д а илм	2 Interface	IP Address	MAC Address	Host Name	Port	Option
O VPN	2 LANI	192.168.1.100	08:8F:B8:D5:DD:A9		Port 2	Delete
Clients List						
Log Center						
Wireless information						
WAN						
Route Table						
DHCP Table						
IPv6 TSPC Status						
IPv6 Neighbor Table						
LLDP Neighbors information						
DNS Cache Table						
LTE Status						
Remote DSL Status						
PPPoE Pass-Through						
- + -++						

IV-1-5-2 WAN

Click **Refresh** to reload this page with the most up-to-date information of WAN Ethernet ARP table.

evice Menu	Monitoring / ARP Table				C Refrest
Dashboard	LAN WAN				
Configuration	WAN Ethernet ARP Ta	ble			
Security ;	the Clear All				Šearch
iam 5	Interface	IP Address	MAC Address	Comment	Option
D VPN					
Clients List					
Log Center					
Wireless Information					
WAN					
Route Table					
DHCP Table					
IPv6 TSPC Status					
IPv6 Neighbor Table					
LLDP Neighbors Information					
DNS Cache Table					
LTE Status					
Remote DSL Status					
PPPoE Pass-Through					

IV-1-6 Route Table

IV-1-6-1 IPv4

Device Menu	Monitoring / Route Ta	ble			Chefr
Dashboard	IPvd IPv6				
E Configuration	> IPv4 Route Table				
🤉 Security	F				standi.
3 MM	E Interface	Destination	Mask	Gateway	Flags
5 VPN	LAN LANT	192.168.1.0	255,255,255,0	Directly Connected	Connected
Clients List					
Log Center					
Wireless Information					
WAN					
ARP Table					
DHCP Table					
IPv6 TSPC Status					
IPv6 Neighbor Table					
LLDP Neighbors Information					
DNS Cache Table					
LTE Status					
Remote DSL Status					
PPPoE Pass-Through					

IV-1-6-2 IPv6

evice Menu	Monitoring / Route T	able			CRefres
Dashboard	IPv4 IPv6				
Configuration	IPv6 Route Table				
Security	D Hide Detail				Search
am iam		Destination	Next Hop	Flag	Metric
D VPN	[LAN] LAN1	fe80::/64	Directly Connected	u	256
	[LAN] LAN1	fe80::/64	Directly Connected	U	256
Clients List			and and a		
Log Center	[LAN] LAN1	fe80::/128	Directly Connected	U. n	0
Wireless Information	[LAN] LAN1	fe80::1649:bcff:fe86:fab8/128	Directly Connected	U. n	0
WAN	A CONTRACTOR OF A CONTRACTOR O				
ARP Table	(LAN) LAN1	ff00::/8	Directly Connected	U	256
DHCP Table					
IPv6 TSPC Status					
IPv6 Neighbor Table					
LLDP Neighbors information					
DNS Cache Table					
LTE Status					
Remote DSL Status					
PPPoE Pass-Through					

IV-1-7 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-1-7-1 IPv4 DHCP Subnet

This page shows the DHCP server status, IP range, IP pool, Used IP, and percentage of utilization for each LAN interface.

Device Menu		Monitoring / DH	ICP Table					CRefresh
 Dashboard 		IPv4 DHCP Subr	IPv4 DHCP Lease IPv	6 Assignment				
a Configuration		IPv4 DHCP Sul	bnet					
Security	×							
A IAM	5	Name	DHCP Server Status	IP Range	IP Pool	Used IP	Utilization	
O VPN	ż	[LAN] LAN1	Enabled	192.168.1.10 - 192.168.1.109	100	0		0%
Clients List								
Log Center								
Wireless Information								
WAN								
ARP Table								
Route Table								
IPv6 TSPC Status								
IPv6 Neighbor Table								
LLDP Neighbors information								
DNS Cache Table								
LTE Status								
Remote DSL Status								
PPPoE Pass-Through								

IV-1-7-2 IPv4 DHCP Lease

This page shows the remaining time of the IPv4 DHCP lease of the device.

Device Menu	Monitoring / DHG	CP Table					C Refresh
 Dashboard 	IPv4 DHCP Subne	et IPV4 DHCP Lease IPV	6 Assignment				
Seconfiguration	> IPv4 DHCP Leas	ie					
Security	2						
S. IAM	3 Subnet	IP Address	MAC Address	Host Name	Type	Search	
O VPN							
Clients List							
Log Center							
Wireless Information							
WAN							
ARP Table							
Route Table							
IPv6 TSPC Status							
IPv6 Neighbor Table							
LLDP Neighbors information							
DNS Cache Table							
LTE Status							
Remote DSL Status							
PPPoE Pass-Through							

IV-1-7-3 IPv6 Assignment

This page shows the remaining time of the IPv6 DHCP lease of the device.

a devide and							Refresh
Dashboard	IPv4 DHCP Subnet	IPv4 DHCP Lease IPv6 Ass	gnment				
Configuration	IPv6 Assignment						
Security 5						Search	
Д им ,	Interface	IPv6 Address	Link-layer address	IAID	DUID	Leased Time	
D VPN							
Clients List							
Log Center							
Wireless Information							
WAN							
ARP Table							
Route Table							
IPv6 TSPC Status							
IPv6 Neighbor Table							
LLDP Neighbors information							
DNS Cache Table							
LTE Status							
Remote DSL Status							
PPPoE Pass Through							

IV-1-8 IPv6 TSPC Status

IPv6 TSPC (Tunnel Setup Protocol Client) status page could help you diagnose issues with IPv6 connections that utilize TSP.

If TSPC is configured properly, the router will display the following when the router has connected to the tunnel broker successfully.

Device Menu		Monitori	ng / IPv6 TSI	PC Status					CRefresh
Dashboard		IPv6 TSP	C Status						
E Configuration	×								
Security	3	Name	Status	Tunnel Broker	Local IPv6 Address	Remote IPv6 Address	Router DNS Name	TSPC Prefix	TSPC Prefix Length
A IAM	2								
D VPN									
Clients List									
Log Center									
Wireless Information									
WAN									
ARP Table									
Route Table									
DHCP Table									
IPv6 Neighbor Table									
LLDP Neighbors information									
DNS Cache Table									
LTE Status									
Remote DSL Status									
PPPoE Pass-Through									

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

IV-1-9 IPv6 Neighbor Table

This page displays the mapping between Ethernet hardware addresses (MAC addresses) and the IPv6 addresses. This information is helpful in diagnosing network problems, such as IP address conflicts.

Clients List	Monitoring / IPv6 Neighbor Table			
Log Center	IPv6 Neighbor Table			
Wireless Information				
WAN	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.			Search
ARP Table	IPv6 Address	MAC Address	Interface	Status
Route Table	fe80::1649:bcff:fe86:fab8	14:49:bc:86:fa:b8	[LAN] LAN1	STALE
DHCP Table	reau; roastocititiego; raba	14049100300114006	[LAN] LANT	STALE
IPv6 TSPC Status	ff02::1:ff57:d30a	33:33:ff:57:d3:0a	[LAN] LAN1	NOARP
	Hozen	33:33:00:00:00:01	(LAN) LANT	NOARP
LLDP Neighbors	100da (32.33.00,000.01	(read room	MUMP.
Information	ff02::to	33:33:00:00:00:fb	[LAN] LAN1	NOARP
DNS Cache Table	fe80::ea9b:6aab:9157:d30a	08:bf/b8:d5:dd:a9	[LAN] LAN1	STALE
LTE Status	reacterationalaboario77630a	00:01:01:02:00:89	[LAN] LANT	21765
Remote DSL Status				
PPPoE Pass-Through				
Session Table				
Utility				
System Maintenance				
rtual Controller				
Wireless				
Switch				

IV-1-10 LLDP Neighbors Information

Clients List	Monitori	ing / LLDP Neighb	ors informa	tion							
Log Center	LLDPN	eighbors inform	ation								
Wireless information	LEDFIN	eignoors morn	auon								
WAN										Search.	
ARP Table	Local	Chassis ID	System	System	Management	Management	System	Port ID	Port	-	Time to
Route Table	Port	Chassis ID	Name	Description	Address(IPv4)	Address(IPv6)	Capabilities	Port ID	Description	Time	Live(sec)
DHCP Table	P2	local MK- CARRIE-A1000						08:bf:b8:d5:dd:a9		0 day. 04:41:04	3601
IPv6 TSPC Status	1.0	CARRIE-A1000								04041304	
IPv6 Neighbor Table											
DNS Cache Table											
LTE Status											
Remote DSL Status											
PPPoE Pass-Through											
Session Table											
Utility >											
System Maintenance 3											
tual Controller											
Wireless >											
Switch a											
	1										

IV-1-11 DNS Cache Table

The router can function as a DNS server which allows LAN clients to look up DNS information by sending DNS requests to the router. The DNS information is temporarily cached on the router and can be viewed on this page.

IV-1-11-1 IPv4

Click **Refresh** to reload the most up-to-date information of the IPv4 DNS cache data.

Clients List	Monitoring / DNS Cache Table			CRefrest
Log Center	(Py4)Py6			
Wireless information				
WAN	IPv4 DNS Cache Table			
ARP Table	1 Clear All			Search_
Route Table	Domain Name	IP Address	TTL (Seconds)	Junitite-
DHCP Table	Louisen rearie			
IPv6 TSPC Status				
IPv6 Neighbor Table				
LLDP Neighbors information				
LTE Status				
Remote DSL Status				
PPPoE Pass-Through				
Session Table				
8 Utility	4			
System Maintenance	a.			
irtual Controller				
+ Wireless	×			
3 Switch	*			

IV-1-11-2 IPv6

Click **Refresh** to reload the most up-to-date information of the IPv6 DNS cache data.

Clients List	Monitoring / DNS Cache Table			CRefresh
Log Center	IPv4 IPv6			
Wireless Information				
WAN	IPv6 DNS Cache Table			
ARP Table	1 Clear All			Search_
Route Table	Domain Name	IP Address	TTL (Seconds)	Desiron
DHCP Table	Dunan Mane			
IPv6 TSPC Status				
IPv6 Neighbor Table				
LLDP Neighbors information				
LTE Status				
Remote DSL Status				
PPPoE Pass-Through				
Session Table				
BS Utility	×			
🆏 System Maintenance				
Virtual Controller				
⊱ Wireless	×			
n Switch				

IV-1-12 LTE Status

Clients List		onitoring / LTE Status	CRefrest
Log Center Wireless Information		TE Status	
WAN			
ARP Table		TE Modem	
Route Table DHCP Table		latus No SIM Card	
IPv6 TSPC Status		AE1	
IPv6 Neighbor Table			
LLDP Neighbors information		451	
DNS Cache Table		MHCCID	
		M2ICCID	
Remote DSL Status PPPoE Pass-Through		ccess Tech	
Session Table		and	
} Utility	»;	perator -	
System Maintenance	5	lobile Country Code	
rtual Controller		toblie Network Code	
- Wireless	5	ocation Area Code	
Switch	5	di ID	

IV-1-13 Remote DSL Status

Clients List Monitoring / Re	emote DSL Status	C Refresh
Log Center Remote DSL	tatus	
Wireless Information		
	dem Status from	
ARP Table WAN Port		
Route Table	Note: Enable this function to receive the DSL status from the DSL me	odem on the WAN port and display the DSI, status on the Dashboard.
DHCP Table		
IPv6 TSPC Status		
IPv6 Neighbor Table		
LLDP Neighbors Information		
DNS Cache Table		
LTE Status		
Remote DSC Status		
PPPoE Pass-Through		
Session Table		
g Utility ,		
🖕 System Maintenance 💡		
irtual Controller		
+ Wireless		
号 Switch)		
Caricel Ap	phy .	

IV-1-14 PPPoE Pass-Through

The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.

This page displays the results of performing PPPoE Pass-Through.

Clients List		Monitoring / PPPoE Pass-Thro	ugh			CRefresh
Log Center		PPPoE Pass-Through Clients	5			
Wireless Information						
WAN						
ARP Table						Max: 20
Route Table		Client MAC Address	Client Interface	Uplink/ PPPoE Server MAC Address	Server Interface	Status
DHCP Table						
IPv6 TSPC Status						
IPv6 Neighbor Table						
LLDP Neighbors information						
DNS Cache Table						
LTE Status						
Remote DSL Status						
IPPOE Pass Through						
Session Table						
88 Utility	- 51					
🖏 System Maintenance	2					
Virtual Controller						
}→ Wireless	>					
E Switch	a'					
X The second second						

IV-1-15 Session Table

This screen shows the 200 newest entries in the NAT sessions table. Click **Refresh** to reload this page with the most up-to-date information.

Clients List	Monitoring / Sess	ion Table							C Refresh
Log Center	NAT Session								
Wireless Information									
WAN							Search	n	Max: 200
ARP Table	Interface	Source IP	Source Port	Pseudo Port	Destination IP	Destination Port	Protocol	State	TTL.
Route Table									
DHCP Table									
IPv6 TSPC Status IPv6 Neighbor Table									
LLDP Neighbors									
information									
DNS Cache Table									
LTE Status									
Remote DSL Status									
PPPoE Pass-Through									
Session Table									
SS Utility 5									
🐁 System Maintenance 💦									
Virtual Controller									
אין איז אין γ									
📰 Switch >									
No. of Concession, name of									

IV-2 Utility

This section contains utilities (e.g., ping tool, traceroute, DNS and etc.) that can assist you in analyzing issues and failures during the setup and operation of the router.

IV-2-1 Network Tools

IV-2-1-1 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.

earch Q	Utility / Network Tools			
	Ping Traceroute DNS			
vice Menu	Ping			
Dashboard				
Configuration >	IP Version	IPvil IPvil		
Security	Ping from	Auto 💛		
IAM >	Ping to Host/IP Address ()			
VPN >		G		
Monitoring >	Packet Size (Bytes)	64 🗸		
	Ping Count	4 🔍		
	Ping Interval (Seconds)	1 ~		
Web CLI		Clear Nun		
System Maintenance				
tual Controller				
Wireless)				
Switch				

Available settings are explained as follows:

ltem	Description
IP Version	Select the IP version for entering correct IP address.
Ping from	Select an interface (LAN or WAN) from drop down list to through which you want to perform the ping operation, or choose Auto to be let the router select the WAN interface.
Ping to Host/IP Address	Enter the IP address of the Host/IP that you want to ping.
Packet Size (byte)	Determine the packet size for the ping job.
Ping Count	Determine the quantity of the packet being pinged.
Ping Interval (sec.)	Set 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-2-1-2 Traceroute

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.

Search Q Unity intervence Device Menu Pring Traceroute Image: Configuration IP Version IP Version Image: Security Trace Through Into Image: Security Protocol Image: Manual Distance Image: Security Protocol Image: Manual Distance Image: Monitoring Protocol Image: Manual Distance Image: Monitoring Trace Count 3 Image: Monitoring Image: Manual Distance Image: Manual Distance Virtual Controllier Manual Distance Image: Manual Distance Virtual Controllier Image: Manual Distance Image: Manual Distance Image: Section Maintenance Image: Manual Distance Image: Manual Distance	Traceroute IP Version Pod Trace Through Auto ~ Protocol CMP UDP	vice Menu Dashboard Configuration s Security s
Dashboard Traceroute Configuration IP Version Security Trace Through Monitoring Protocol Monitoring Ifost / IP Address () Monitoring Trace Count Monitoring Main Hop Monitoring Name Hop	IP Version IDve Trace Through Auto ~ Protocol IDMP (JDP	Dashboard Configuration s Security s
Dochboard Configuration Security Security Max Protocol KM VPN Montoring Trace Count Montoring Trace Count Trace Count Max Hop Job Veb CLi System Maintenance Wireless S	IP Version IDve Trace Through Auto ~ Protocol IDMP (JDP	Configuration s Security s
Security > AMA Protocol VPN Manitoring Manitoring Trace Count Auto Manitoring Manitoring Manitoring Manitoring Manitoring Manitoring Manitoring System Maintenance Veb CU System Maintenance	Trace Through Auto ~ Protocol KNAP UDP	Security 5
VMM > VPN > Host / iP Address Monitoring > Monitoring > Monitoring > Max Hop 20 Web CLI System Maintenance > Virtual Contreller + Wireless	Protocol ICMP UDP	
VPN 32 Monitoring 33 Monitoring 34 Max Hop 30 Veb CLI 35 System Maintenance Virtual Contreller	Protocol UDP	IAM ;
Host //PAddress Host		
Monitoring Immy Australiance Virtual Contrailer Yirtual Contrailer		VPN >
Bit Unitivy Marx Hop 30 Web CLI Clear Num Ay System Maintenance > Virtual Controllar >		Monitoring >
Max Hop 20 Web CU Clear System Maintenance > Virtual Controller > + Wireless 3	Trace Count 3 ~	
Web CLI Clear: Nun & System Maintenance > >virtual Controller >• Wirdess		
& System Mulintenance > > Virtual Controller +* Wireless >		Web CLI
}+ Wireless s		System Maintenance
}+ Wireless s		
Suitch .		
		Switch 5

Available settings are explained as follows:

ltem	Description
IP Version	Select the IP version for entering correct IP address.
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 job.

IV-2-1-3 DNS

The user can diagnose the router by query Domain Name System (DNS) servers to obtain domain name or IP address information.

Ping Traceroute DMS Device Mena DNS Configuration Method Security Method Security IP Version IP Version IP Into	Search	q I	Utility / Network Tools	
Dashboard DNS Configuration Method Security IP Version IAM IP Version IVN IP Version I	Device Manu	F	Ping Traceroute DNS	
Configuration Security Powersion Powersion <	Concession of the local division of the loca	-	DNS	
LAM VPN A System Maintenance Yrrtaal Controller		5	Method	NSLOCIKUP DNS SECTION
LM VPN Mont / IP Address Mont / IP Address Cer Mun Manyers/ Tools web CLI System Maintenance Yrtual Controller		5	IP Version	D.4 D.6
WN > Monitoring > Witting > Web CLI > System Maintenance > Virtual Controller: >	S IAM			
Monitoring Mun Mum M			Host / IP Address ()	
Nettrofic Posts Web CLI System Maintenance		*		Clear Nun
Nettrofic Posts Web CLI System Maintenance	58 villay			
🖏 System Maintenance > Virtual Controller				
Virtual Controller	Web CLI			
	🖏 System Maintenance	*		
and the second se	Virtual Controller			
5- Wireless	>- Wireless	2		
🖀 Switch	🚟 Switch	×		

Available settings are explained as follows:

Item	Description
Method	Select a tool to query Domain Name System (DNS) servers to obtain domain name or IP address information.
	• NSLOOKUP – It is an abbreviation of "Name Server Lookup.
	 DNS SECURITY – To guarantee the DNS reliability, integrity and the confidentiality, use this method to query the domain name system server.
IP Version	Select the IP version for entering correct IP address.
Host/IP Address	Enter the host / IP address that you want to traceroute.
Clear	Remove the settings and return to the factory settings.
Run	Perform the job.

IV-2-2 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**.

	à	Ubility / Web CLI	
Device Menu		Web CLI	
	2 2 2 2 2	Username: admin Password: vigor> help Show available commands quit Disconnect history Show a list of previously run commands enable Turn on privileged commands exit Exit from current mode config Configure exec execute	
•Web CL)	×	vigor>	
- Wireless			
삍 Switch	2		÷

This page is left blank.

Chapter V Troubleshooting



V-1 Checking the Hardware Status

Follow the steps below to verify the hardware status.

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

V-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.

V-2-1 For Windows

(i) Note:

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

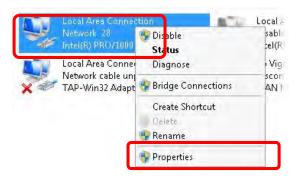
1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



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



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



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

Connect using:	000 MT Network Conn	ection
This connection uses	the following items:	Configure
Client for Mic Privacyware	Filter Driver	Networks
File and Print	acd Version C (TCP/IP acd Version 4 (TCP/IP	

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

neral Alternate Configuration					
u can get IP settings assigned a is capability. Otherwise, you ne r the appropriate IP settings.					
Obtain an IP address autom C Use the following IP address					
IP address:	Ē	(111	-	-
Subnet mask:	Ē	-1	- 00	4	-
Default gateway		ų.	X	i.	
Obtain DNS server address	automatio	ally	٦		
C Use the following DNC come	edd ee		J	_	_
Preferred DNS server:		- 1 2	- ii	Ŧ	
Alternaté DNS serveri			191	ų.	
✓ Validate setting>upon writ.				Adva	anced

V-2-2 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.

00	Network	C
14 📃 🔇		
how All Displays Sou	nd Network Startup Disk	
L	ocation: Automatic	
	Show: Built-in Ethernet	
TCP/	IP PPPoE AppleTalk Proxies Ethernet	
Configure IPv4:	Using DHCP	
IP Address:	192.168.1.10 Renew DHC	P Lease
Subnet Mask:	255.255.255.0 DHCP Client ID:	
Router:	(If required) (If required)	
DNS Servers:		(Optional)
Search Domains:		(Optional)
IPv6 Address:	fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
	Configure IPv6	?
10		
Click the lock to p	revent further changes. Assist me)	pply Now

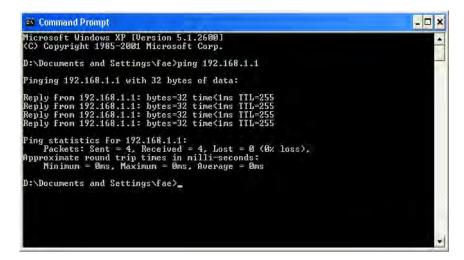
V-3 Pinging the Device

The default gateway IP address of the modem is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section V-2)

Please follow the steps below to ping the modem correctly.

V-3-1 For Windows

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **cmd**. The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

V-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 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.

000	Terminal — bash — 80x24	
Welcome to Darwin! Vigor10:~ draytek\$	n 3 02:24:18 on ttyp1 ping 192.168.1.1 (92.168.1.1): 56 data bytes	2
64 bytes from 192.1 64 bytes from 192.1 64 bytes from 192.1	168.1.1: icmp_seq=0 tt1=255 time=0.755 ms 168.1.1: icmp_seq=1 tt1=255 time=0.697 ms 168.1.1: icmp_seq=2 tt1=255 time=0.716 ms 168.1.1: icmp_seq=3 tt1=255 time=0.731 ms 168.1.1: icmp_seq=4 tt1=255 time=0.72 ms	
192.168.1.1 pir 5 packets transmith	ed, 5 packets received, 0% packet loss /max = 0.697/0.723/0.755 ms	

V-4 Backing to Factory Default Setting

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

(i) Warning:

After using the factory default settings, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing.

V-4-1 Software Reset

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

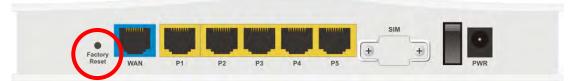
Go to **System Maintenance** and choose **System Reboot** on the web page. The following screen will appear. Choose **Factory Default** and click **Reboot**.

After few seconds, the modem will return all the settings to the factory settings.

System Maintenance / Sys	stem Reboot
System Reboot	
Reboot With	Current Configuration Reset Configuration Reset to Factory Default
	Reboot
	Note Reset Configuration: Reset configurations, retaining service status (product registration, license keys, and certif
	Reset to Factory Default: Revert all settings to factory default, including service status (product registration, lice

V-4-2 Hardware Reset

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



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

V-5 Contacting DrayTek

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