Vigor 167

35b Modem

User's Guide

Version: 1.3_UK

Firmware Version: V5.2.5

Date: Dec. 09, 2024

Intellectual Property Rights (IPR) Information

Copyrights

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

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

Importer

UK - CMS Distribution Limited, 15 Worship Street, London, EC2A 2DT

Ireland - CMS Distribution Limited, Bohola Road, Kiltimagh, Co Mayo, Ireland

Table of Contents

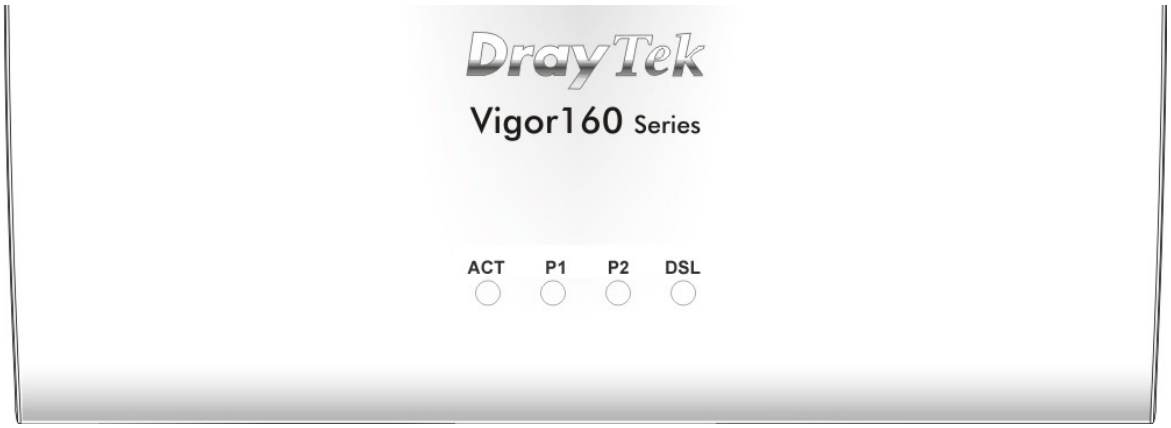
Chapter I Installation

I-1 Introduction

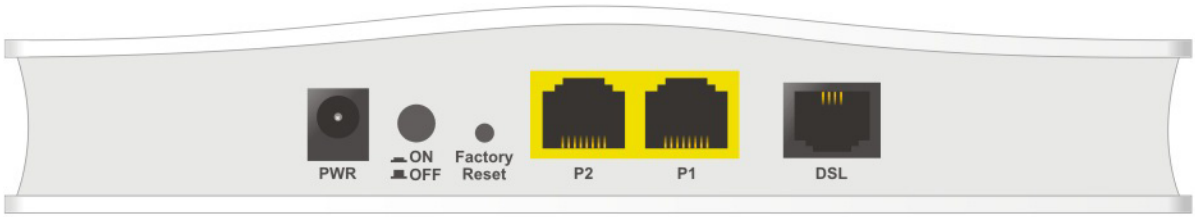
This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

I-1-1 LED Indicators and Connectors

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



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
P1/P2	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
DSL	On	xDSL connection synchronized.
	Blinking	xDSL connection is synchronizing.



Interface	Explanation
PWR	Connecter for a power adapter.
ON/OFF	ON/OFF: Power switch.
Factory Reset	Restore the default settings. Usage: Turn on the modem. Press the button and keep it for more than 10 seconds. Then the modem will restart with the factory default configuration.
P2-P1	Connecter for local networked devices.
DSL	Connecter for accessing the Internet through xDSL.

Note

Remove the protective film from the router before use to ensure ventilation.

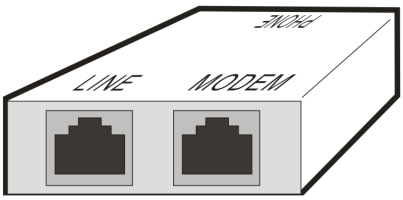
I-2 Hardware Installation

This section will guide you to install the Vigor167 through a hardware connection and configure the device's settings through the web browser.

Before starting to configure Vigor167, you have to connect your devices correctly.

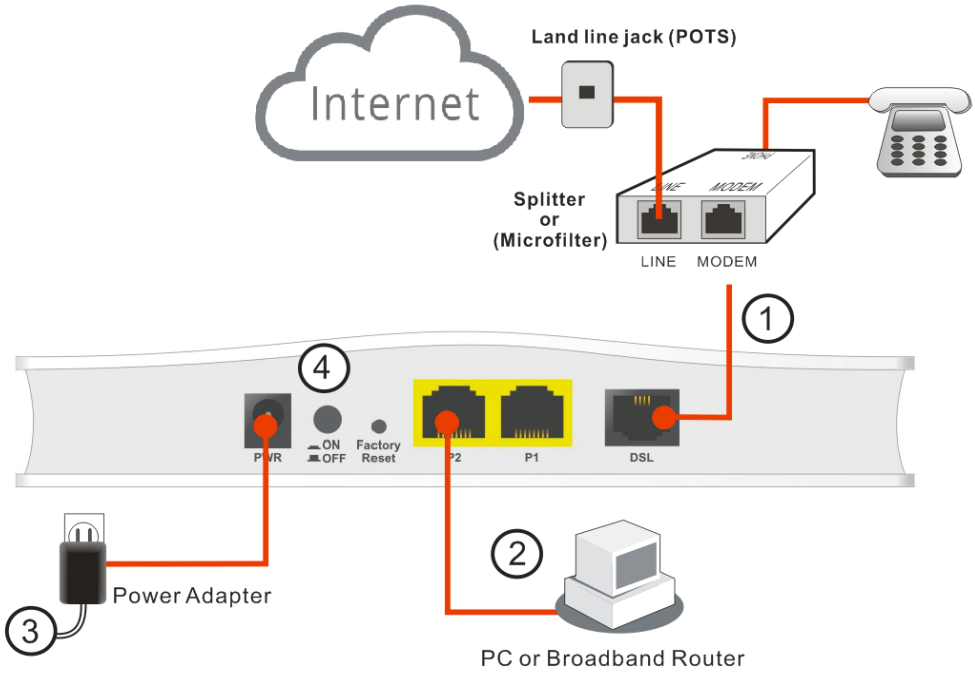
I-2-1 Network Connection

1. Connect the DSL interface to the MODEM port of the external splitter with a DSL line cable.



(splitter)

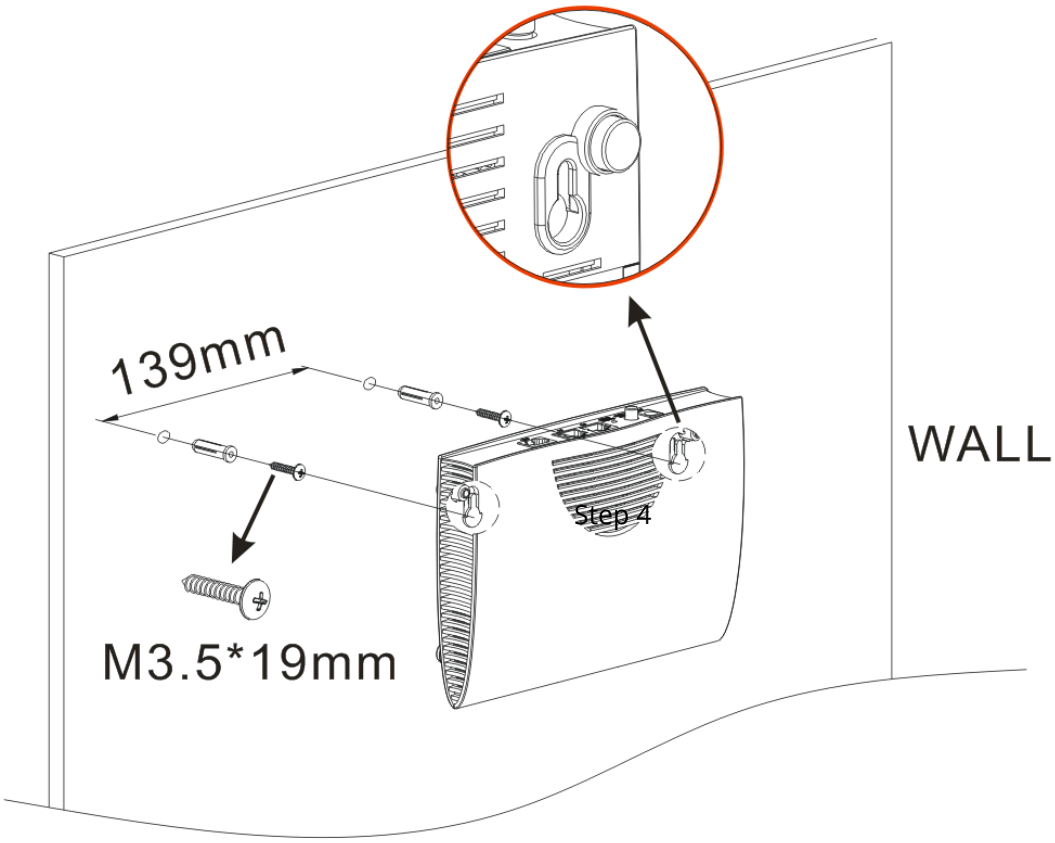
2. Connect the LAN port to your computer with an RJ-45 cable.
3. Connect one end of the power adapter to the Power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the modem.
5. Check the POWER, ACT, LAN, DSL, and INTERNET LEDs to assure network connections.



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

I-2-2 Wall-Mounted Installation

1. Drill the holes on the wall according to the recommended instruction.
2. Fit screws into the wall using the appropriate type of wall plug.



Note

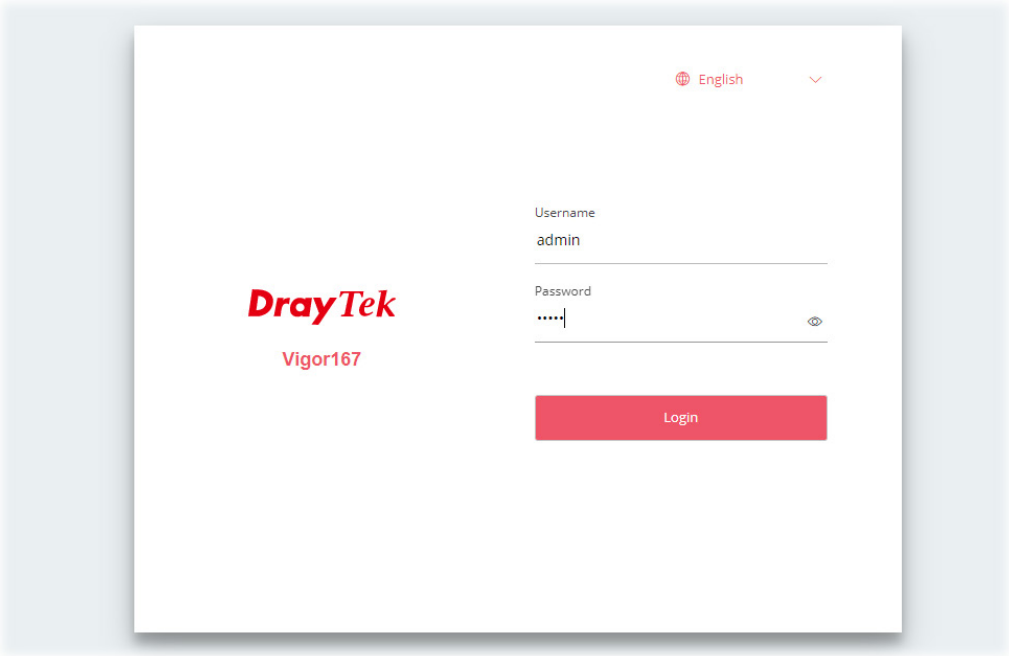
The recommended drill diameter shall be 6.5mm (1/4”).

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

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).

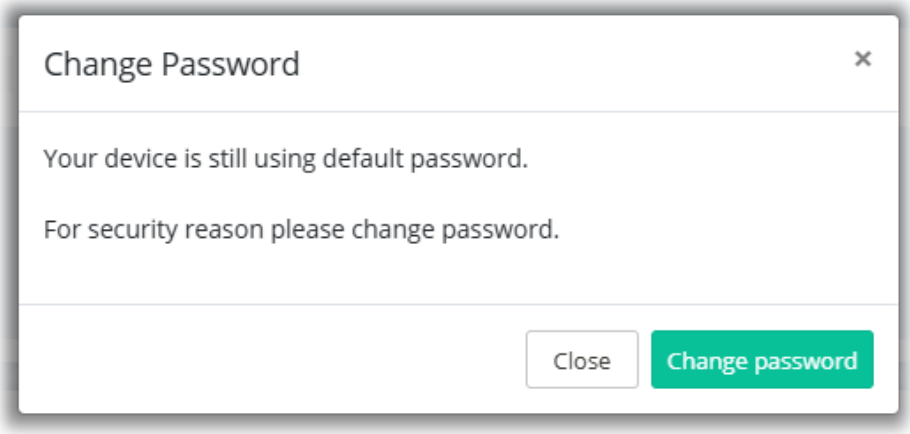
1. Make sure your PC connects to the Vigor router correctly.
2. Open a web browser on your PC and type http://192.168.2.1. A pop-up window will open to ask for a username and password. Pease type “admin/admin” on Username/Password and click Login.



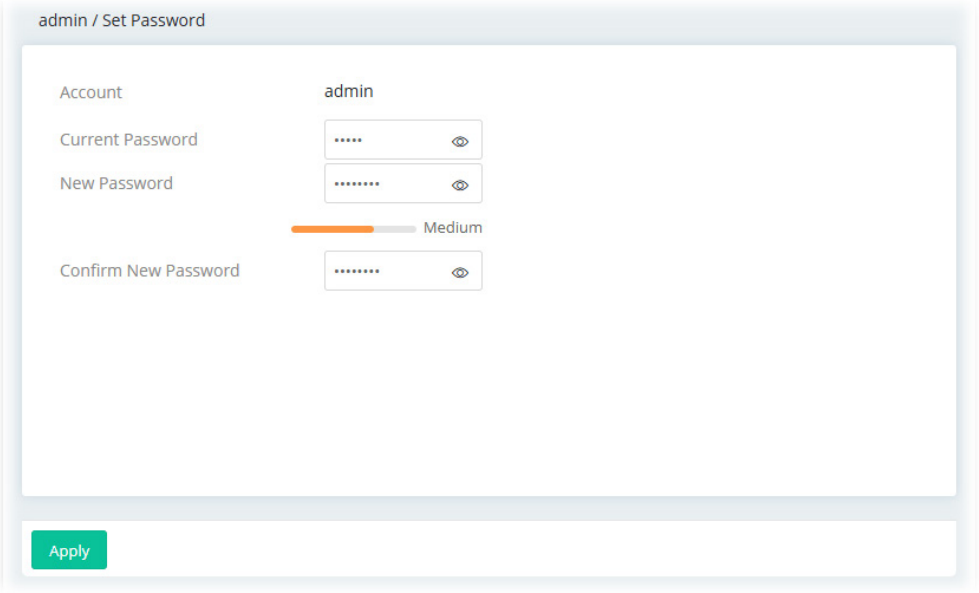
Note:

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

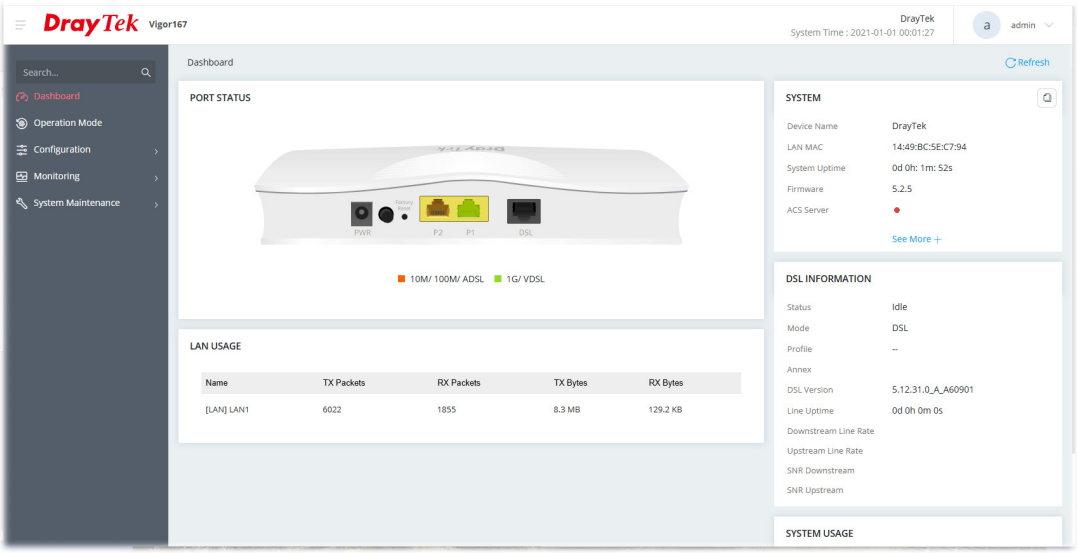
3. Next, the page will appear to guide you change the login password.



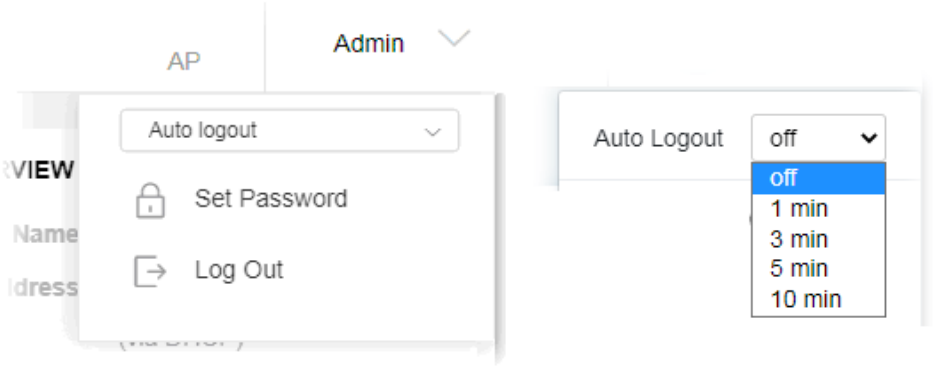
4. You MUST change the login password before accessing the web user interface. Please set a new password for network security.



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



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.



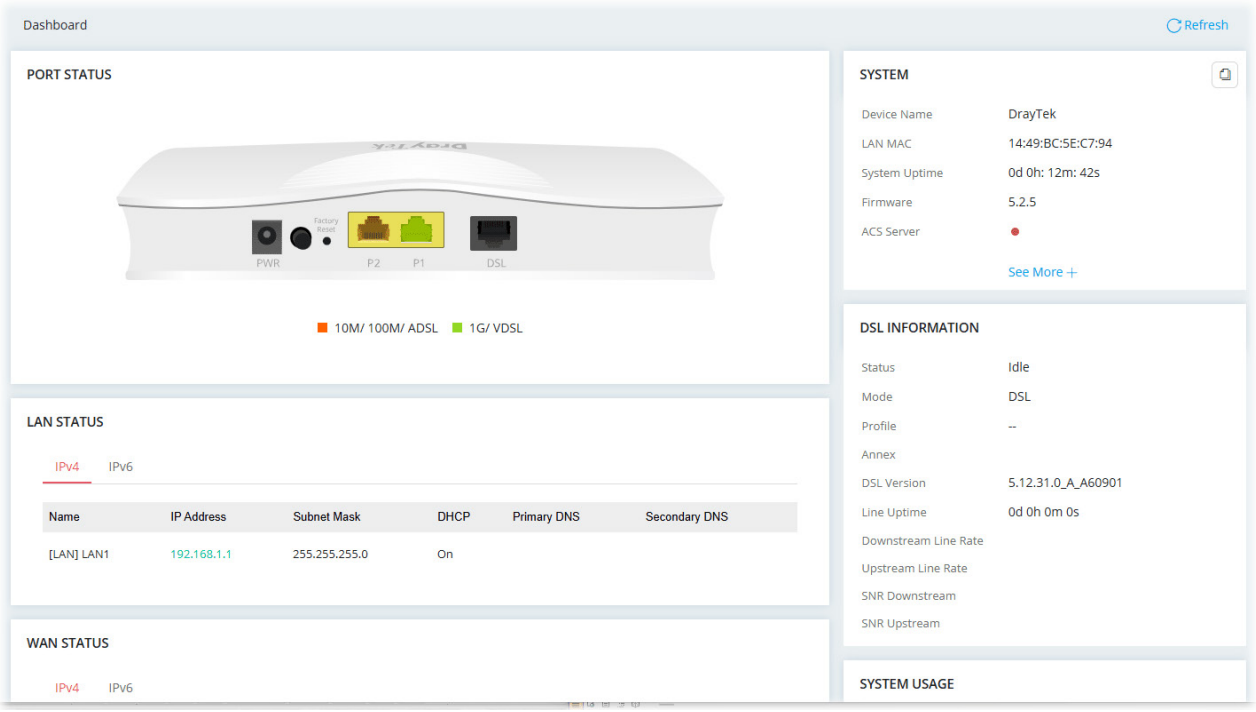
Note:

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

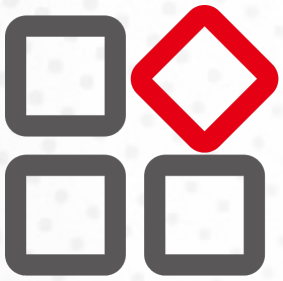
I-4 Dashboard

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.

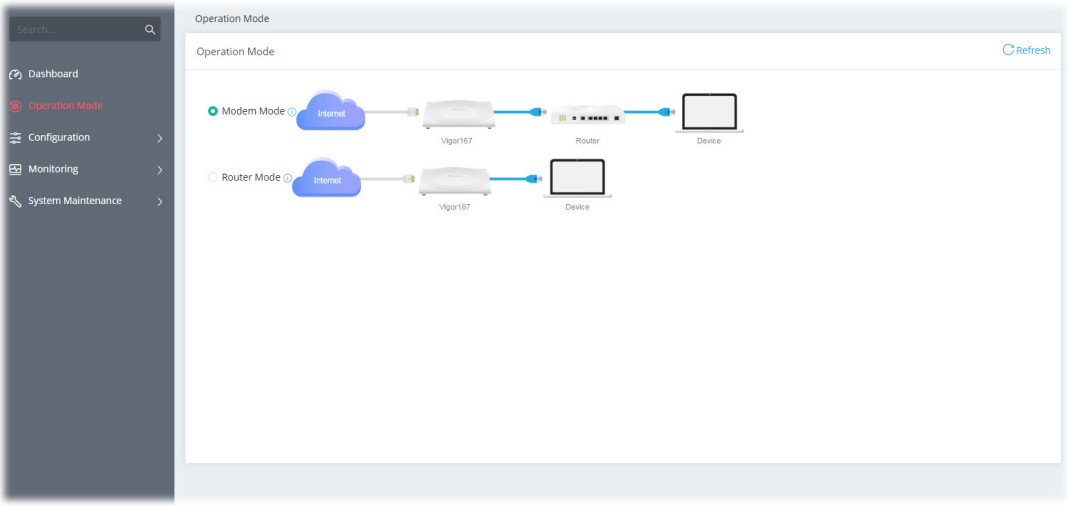


Chapter II Connectivity



II-1 Operation Mode: Modem Mode

This page provides available modes for you to choose for different conditions. Choose the one (e.g., Modem Mode) you want. The system will configure the required settings automatically.

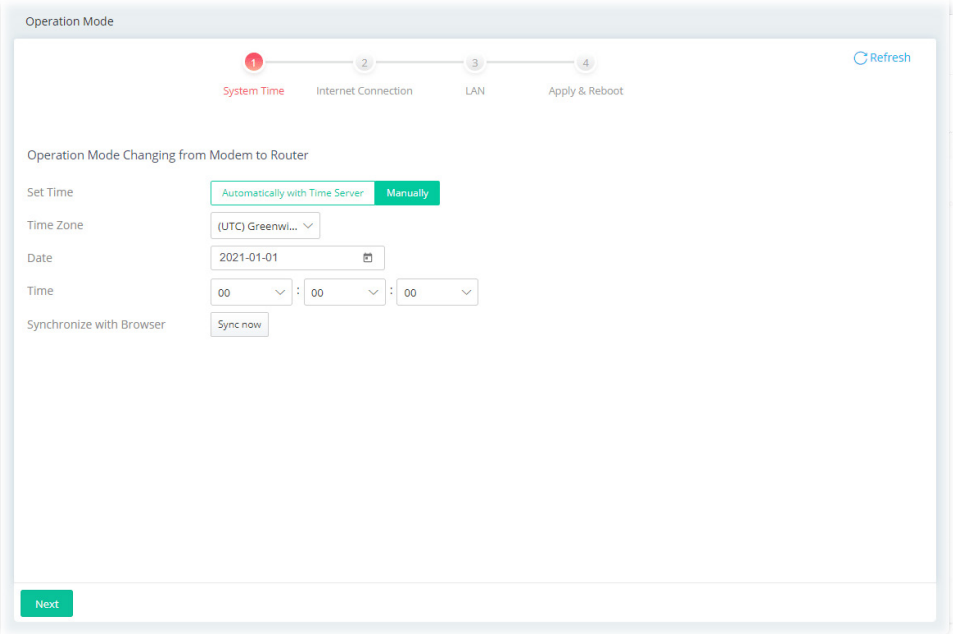


Available settings are explained as follows:

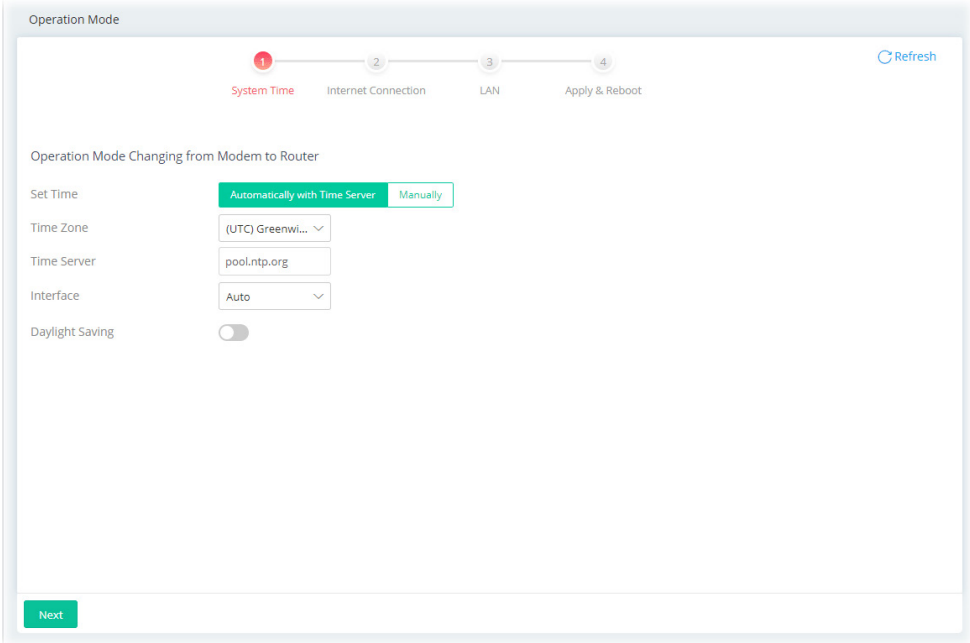
Item	Description
Modem Mode	This mode allows wireless clients to connect to the access point and exchange data with the devices connected to the wired network.
Router Mode	The built-in DHCP server can assign different IPs to the devices connecting to this router.

Click the Modem Mode to configure advanced settings.

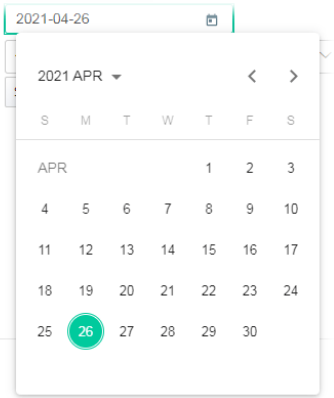
Step 1: Set the System Time.



Or,

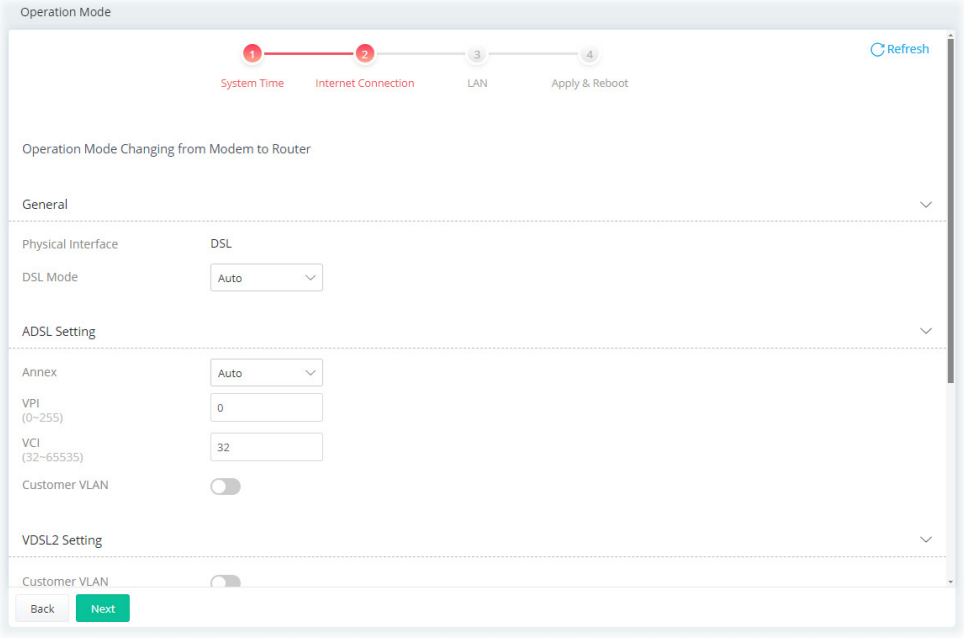


Available settings are explained as follows:

Item	Description
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 is selected, the Vigor system will renew the time through WAN or LAN. Daylight Saving - Enable Daylight Saving Time (DST) if it is applicable to your location.
When Manually is selected as Set Time	Time Zone - Select the time zone where the router is located. Date - Use the drop-down calendar to specify correct date.  Time - Set the time by specifying hours, minutes, and seconds.

	Synchronize with Browser - Click Sync now to sync the time setting with the browser.
Next	Get into the next setting page.

Step 2: Configure the settings for Internet connection.

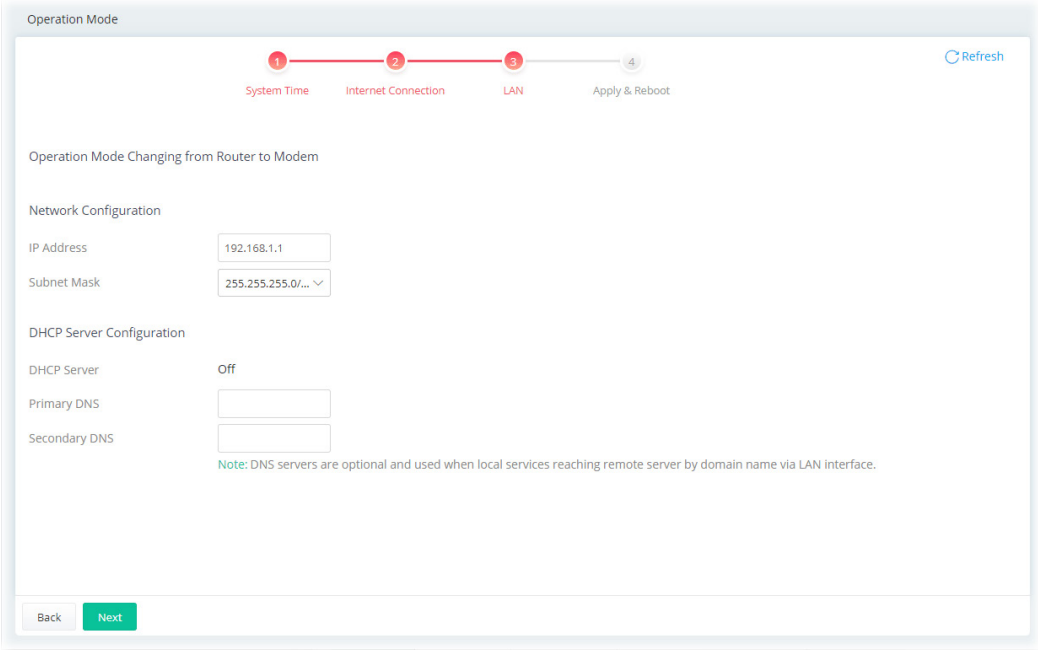


Available settings are explained as follows:

Item	Description
	General
Physical Interface	Displays the physical interface used for the network connection.
DSL Mode	Select the DSL connection mode. Auto - The router will first attempt to connect using VDSL2, and will fall back to ADSL# if VDSL2 is unavailable.
	ADSL Setting
Annex	Specifies the modulation standard used for the ADSL connection.
VPI / VCI	Set values for Virtual Path Identifier(VPI) and Virtual Channel Identifier(VCI).
Customer VLAN	Enabled - Switch the toggle to enable or disable the function. 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.
	VDLS2 Setting
Customer VLAN	Enabled - Switch the toggle to enable or disable the function. 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	Enabled - Switch the toggle to enable or disable the function. 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.
Back	Return to previous setting page.
Cancel	Discard current settings and return to the previous page.
Next	Get into the next setting page.

Step 3: Configure the LAN settings.

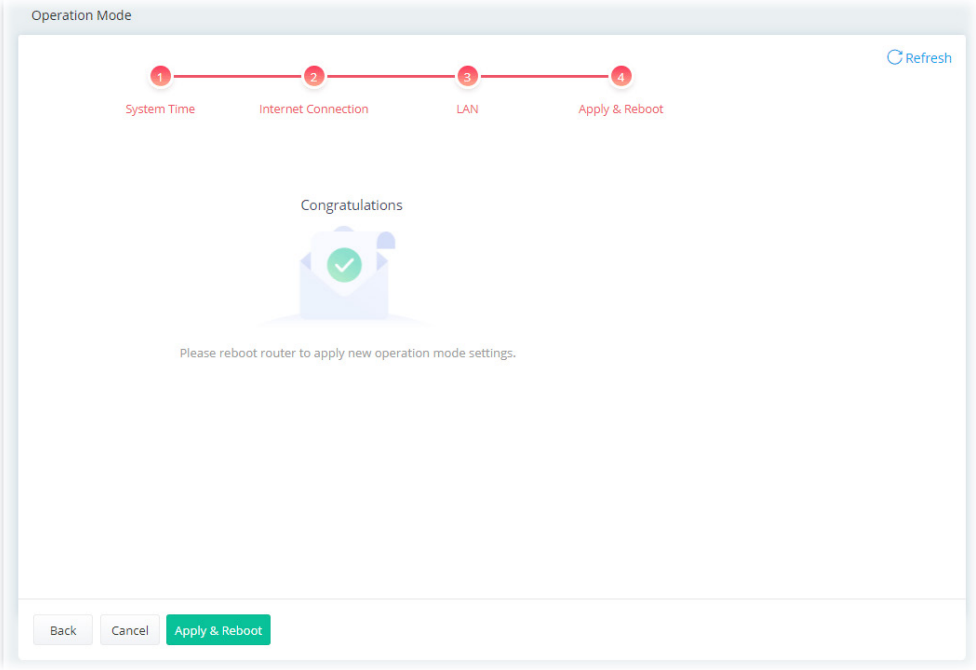


Available settings are explained as follows:

Item	Description
Network Configuration	
IP Address	This is the IP address of the router. (Default: 192.168.2.1).
Subnet Mask	The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).
DHCP Server Configuration	
DHCP Server	The built-in DHCP server on the router is set to Off.
Primary DNS	DNS servers are optional. It can be used when local services reach a remote server by domain name via LAN interface. Specify a DNS server IP address here.
Secondary DNS	Specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.

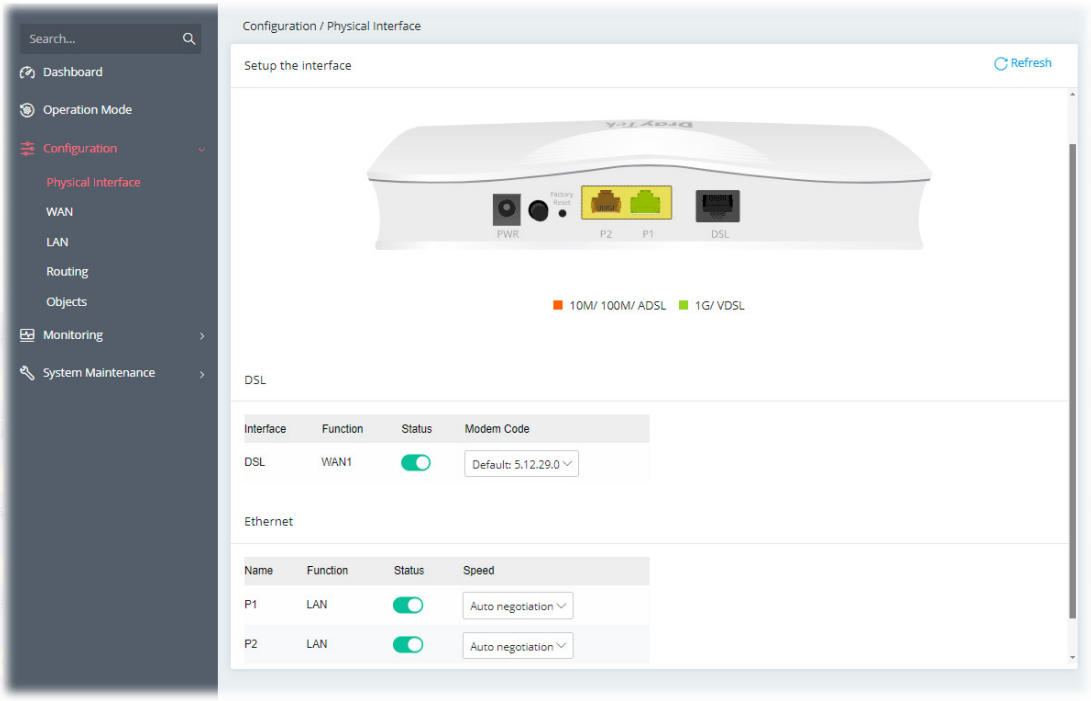
Back	Return to previous setting page.
Next	Get into the next setting page.

Step 4: After finishing the configuration, click Apply & Reboot.



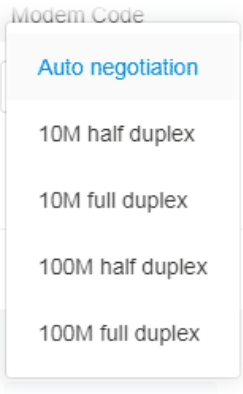
II-1-1 Physical Interface

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



Available settings are explained as follows:

Item	Description
DSL	
Interface	Displays the interface (DSL, ADSL or xDSL and etc.) used for WAN connection.
Function	Displays the WAN# of the WAN connection.
Status	Switch the toggle to enable or disable the function.
Modem Code	Use the default one. Consult your ISP to select the one matching the country in which the router is installed.
Ethernet	
Interface	Displays the interface (P1, P2) used for LAN connection.
Function	Displays the LAN# of the LAN connection.
Status	Switch the toggle to enable or disable the function.
Speed	Set the LAN port speed capabilities:



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.

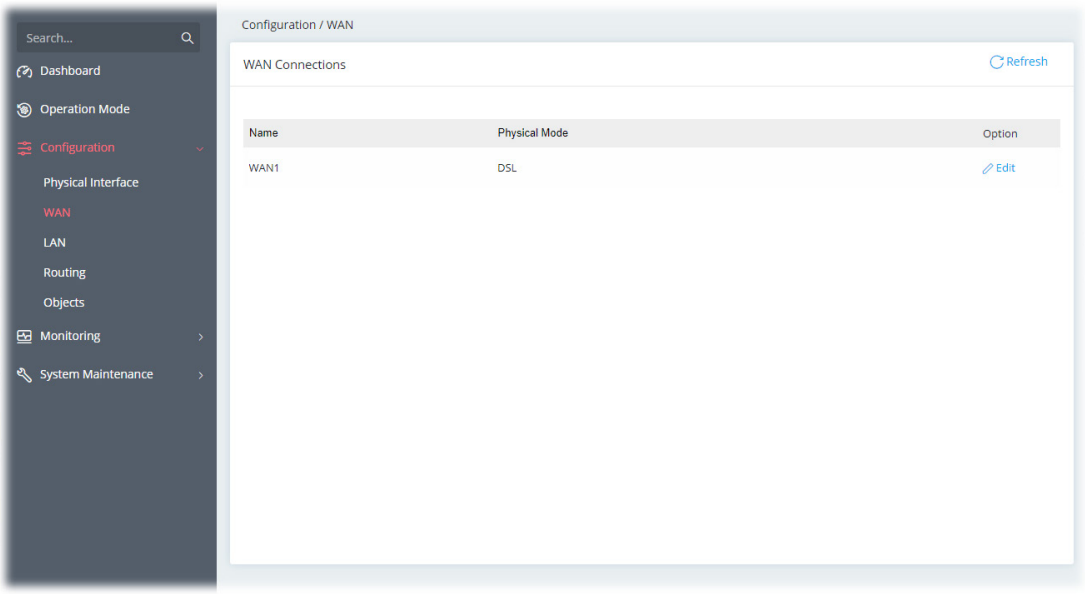
100M full duplex: Force speed with 100M ability.

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.

II-1-2 WAN

When the operation mode is configured as Modem Mode, the Configuration>>WAN page will be shown as the following page.

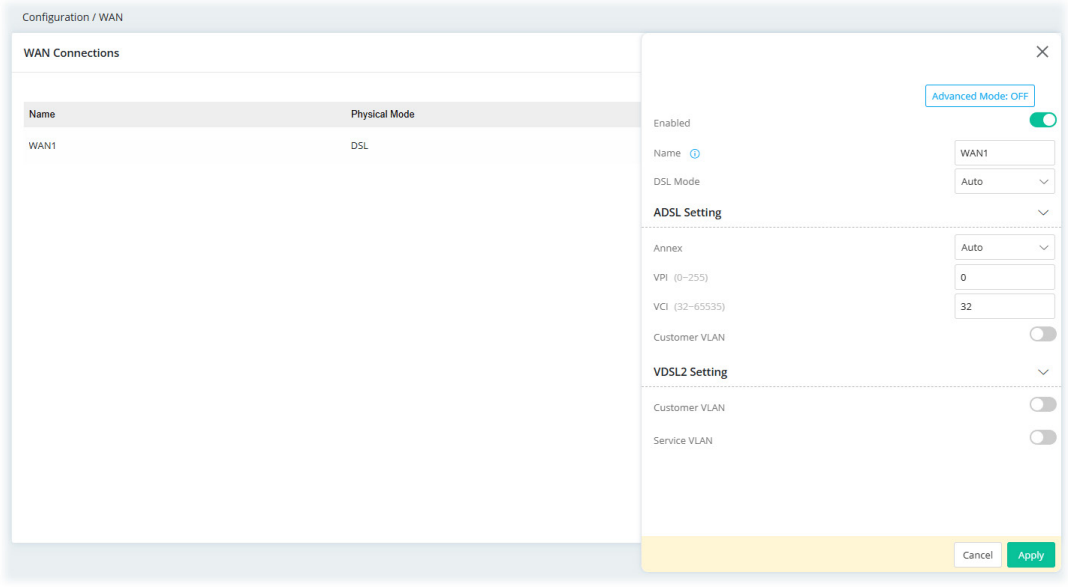
This page is to configure the general settings for WAN connection.



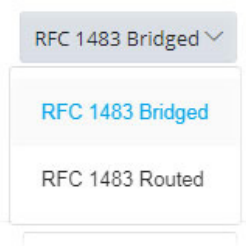
Available settings are explained as follows:

Item	Description
Name	Displays the name of the interface.
Physical Mode	Displays the physical mode (e.g., ADSL, VDSL, and etc.) used by the WAN interface.
Option	Edit - Click to modify the interface name and physical mode.

To configure the detailed settings for the selected WAN interface, click the Edit link to the right side of the WAN interface.



Available settings are explained as follows:

Item	Description
Show / Hide Advanced Mode	Click to show or hide the advanced settings for the WAN interface. The advanced settings include Encapsulation and QoS. Encapsulation -  QoS - Be explained later.
Name	Displays current WAN interface.
Enabled	Switch the toggle to enable or disable the function.
DSL Mode	Specify which DSL mode (e.g., VDSL2, ADSL2, ADSL2 multimode, ADSL2+, T1.413, G.DMT) can be used for such WAN connection. Auto – The system will choose the suitable one automatically.
ADSL Setting	
Annex	Choose the correct modem version of the device, e.g., Annex A, Annex B, Annex A/B/M, Annex A/B/J and etc.
VPI	Enter the value provided by ISP.
VCI	Enter the value provided by ISP.
Customer VLAN	Enabled - 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.
VDSL2 Setting	
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. 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.
QoS	

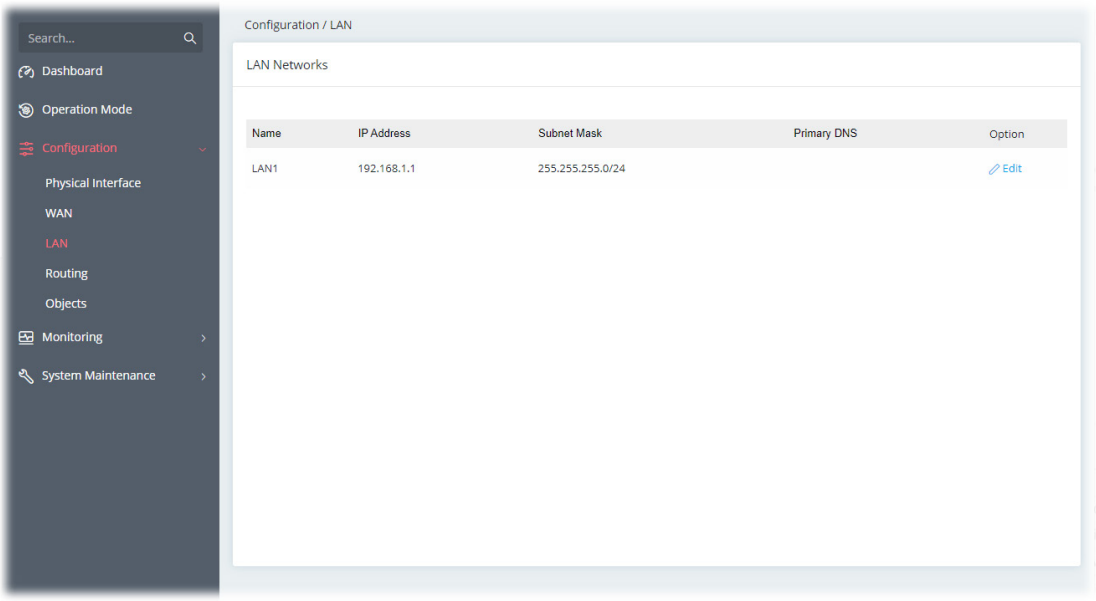
ATM QoS	Configure the Quality of Service (QoS) of the ATM circuit. Select a proper QoS type for the interface.  UBR Without PCR- Unspecified Bit Rate. UBR With PCR- Unspecified Bit Rate. Enter the value for PCR (Peak Cell Rate, 0_5500) if select UBR With PCR. CBR - Constant Bit Rate. nrtVBR - Non-real-time Variable Bit Rate. rtVBR - Real-time Variable Bit Rate.
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-1-3 LAN

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

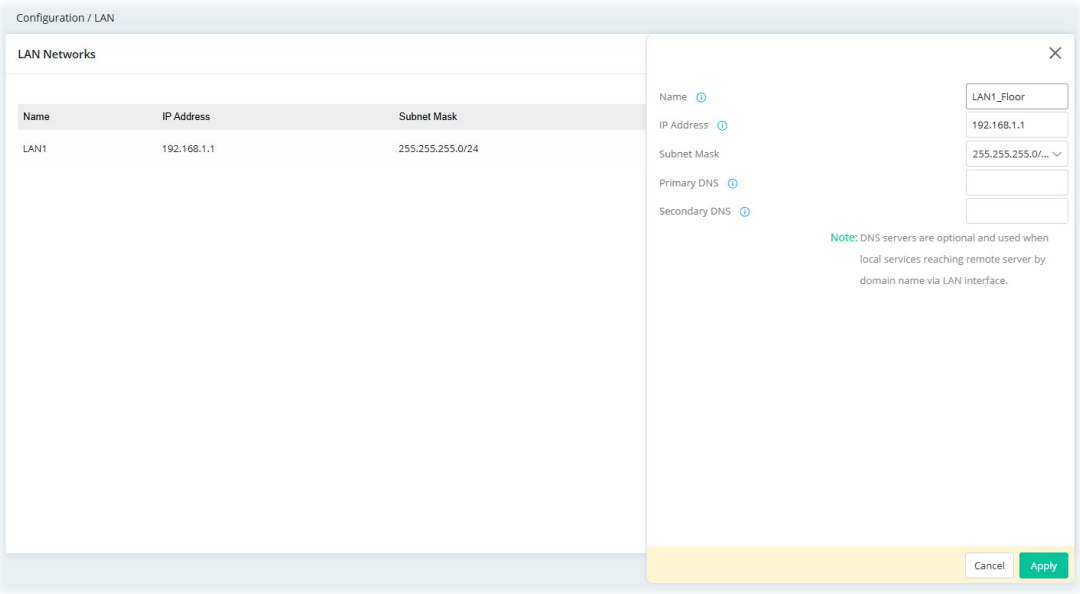
Open Configuration>>LAN to open the following page.



Available settings are explained as follows:

Item	Description
Name	Displays the number of LAN interface.
IP Address	Displays the IP address of the LAN interface.
Subnet Mask	Displays the subnet mask of the LAN interface.
Primary DNS	Displays the DNS server IP address.
Option	Edit - Click to modify the name, IP address, and subnet mask settings.

To configure the detailed settings for the selected WAN interface, click the Edit link to the right side of the LAN interface.



Available settings are explained as follows:

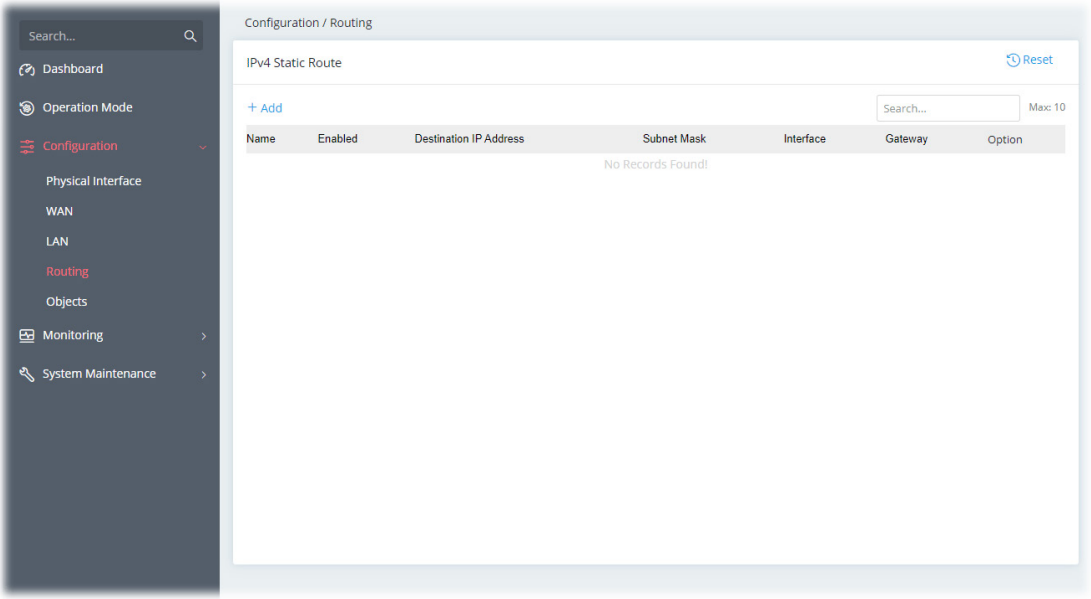
Item	Description
Name	Enter a brief comment for the LAN interface.
IP Address	Enter the IP address of the LAN interface.
Subnet Mask	Select a subnet mask of the LAN interface.
Primary DNS	DNS servers are optional. It can be used when local services reach a remote server by domain name via LAN interface. Specify a DNS server IP address here.
Secondary DNS	Specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.
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.

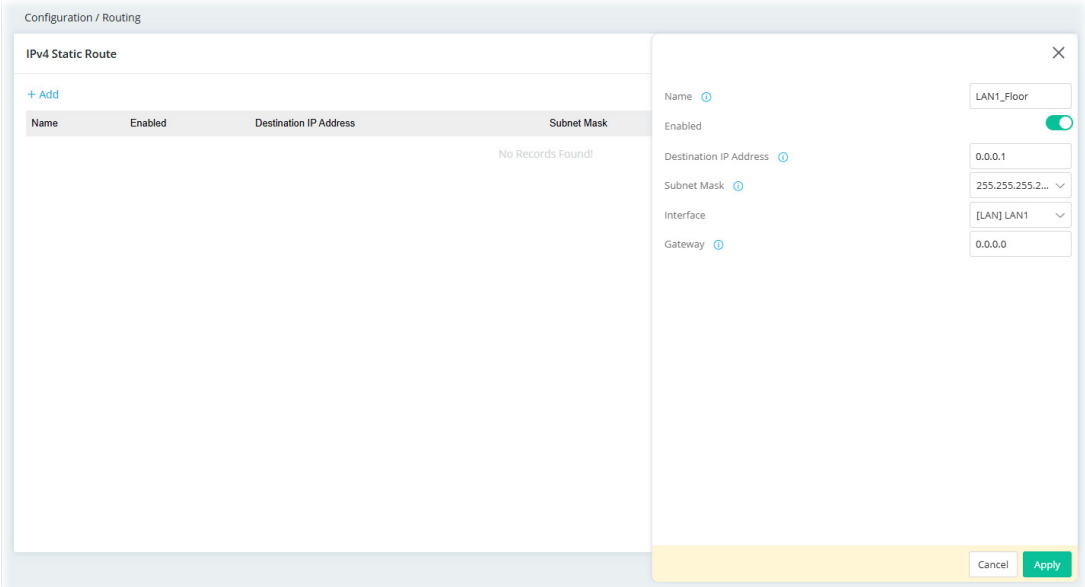
II-1-4 Routing

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.

Open Configuration >> Routing.



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



Available settings are explained as follows:

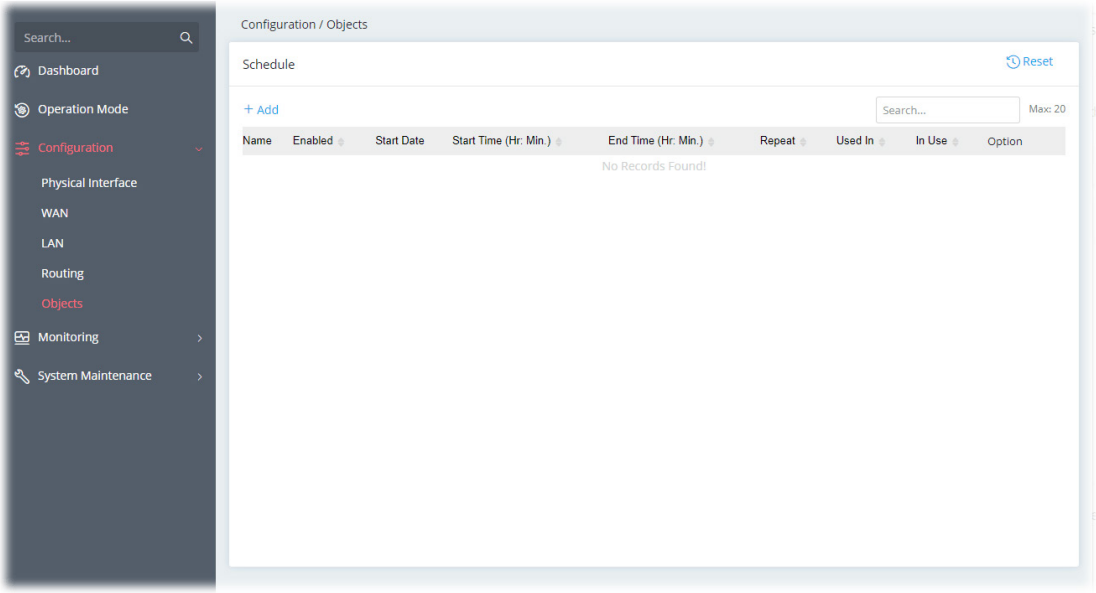
Item	Description
Name	Enter a name as the profile name.
Enabled	Switch the toggle to enable or disable the function.
Destination IP Address	Enter the IP address as the destination IP address.

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.

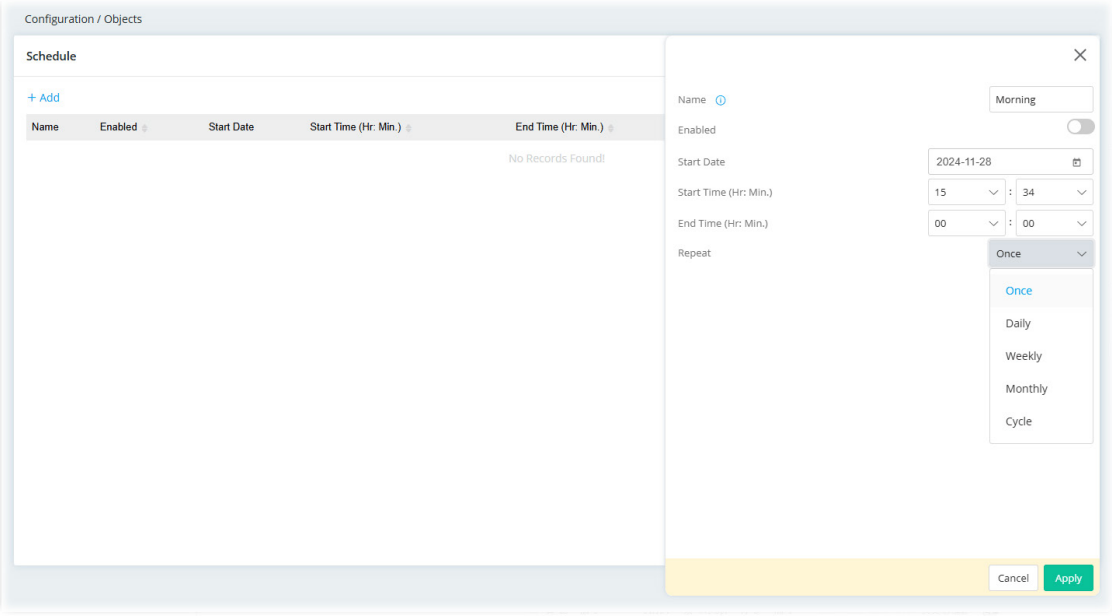
After finishing this web page configuration, please click Apply to save the settings.

II-1-5 Objects

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.



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



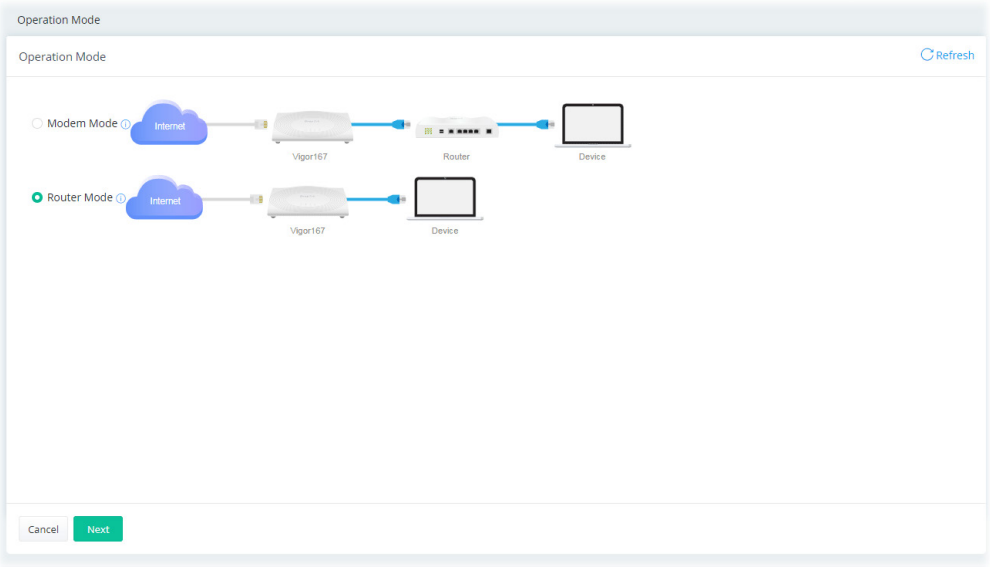
Available settings are explained as follows:

Item	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. Cycle - Any action applied this schedule will be executed per several days. ● Every (days) - Enter a number as cycle duration. Then, any action applied this schedule will be executed per several days. For example, “3” is set as cycle duration. That means, the action applied this schedule will be executed every three days since the date defined on the Start Date. ● 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.

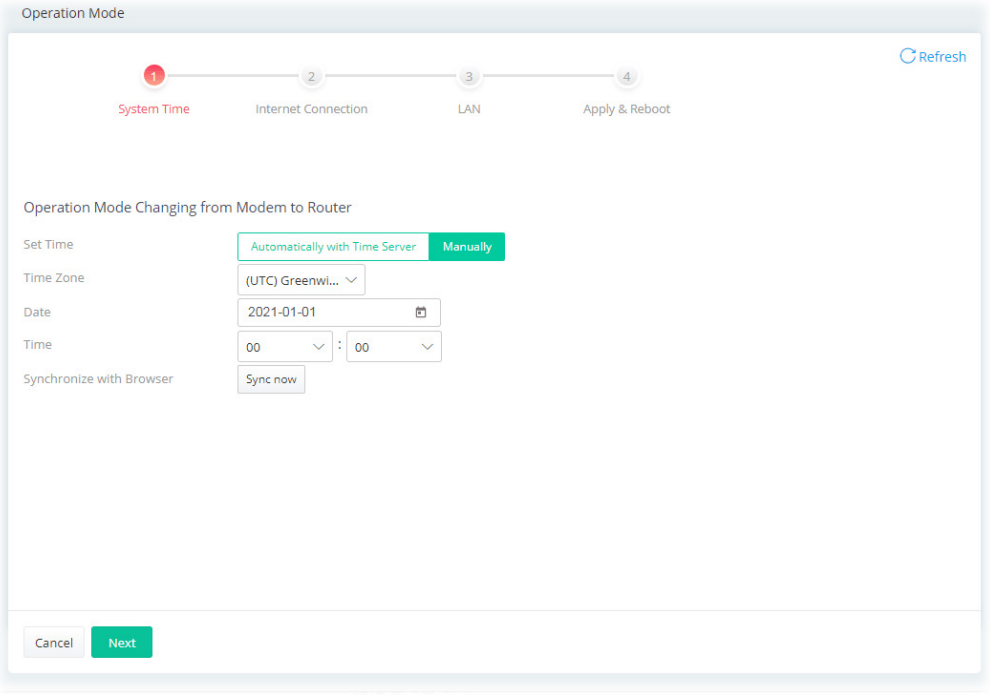
After finishing this web page configuration, please click Apply to save the settings.

II-2 Operation Mode: Router Mode

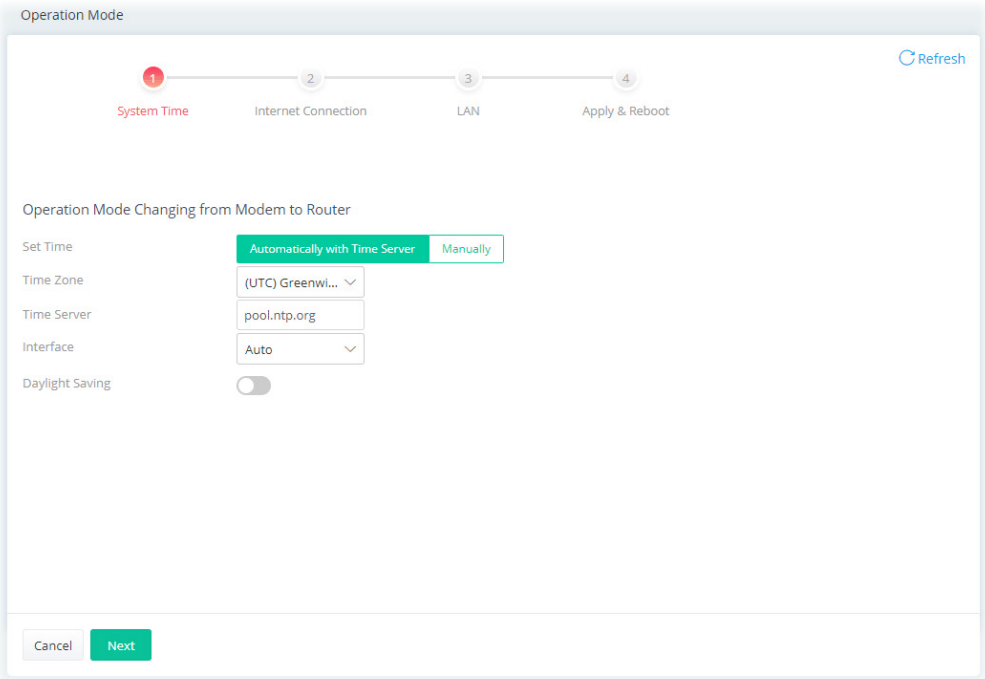
Click the Router Mode and click Next to configure advanced settings.



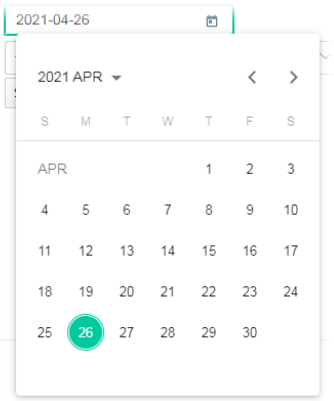
Step 1: Set the System Time.



Or,

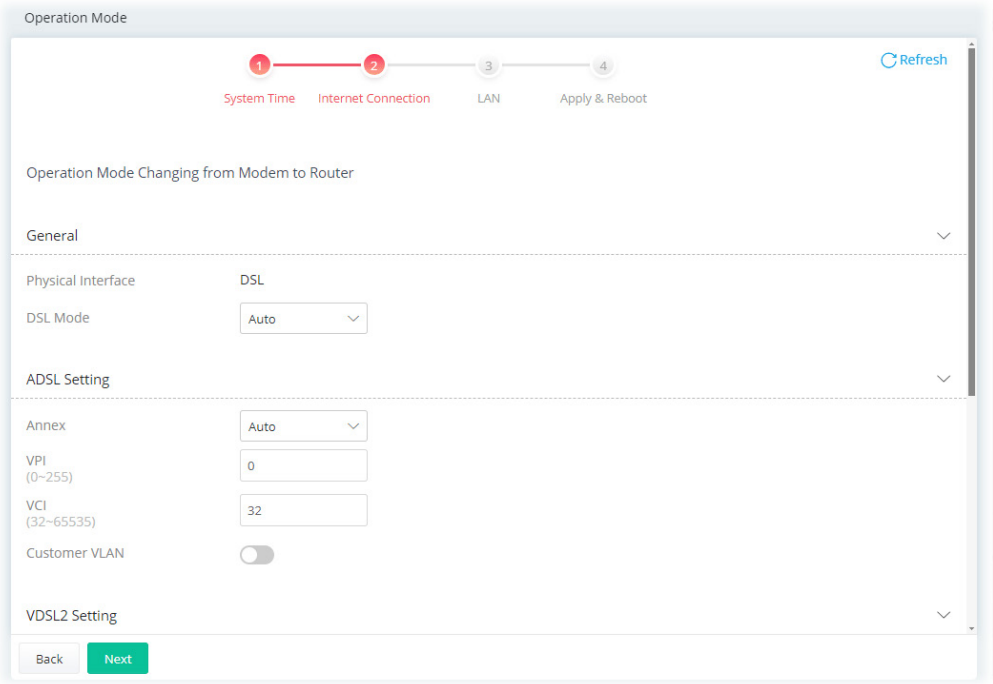


Available settings are explained as follows:

Item	Description
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 is selected, the Vigor system will renew the time through WAN or LAN. Daylight Saving - Enable Daylight Saving Time (DST) if it is applicable to your location.
When Manually is selected as Set Time	Time Zone - Select the time zone where the router is located. Date - Use the drop-down calendar to specify correct date.  Time - Set the time by specifying hours, minutes, and seconds.

	Synchronize with Browser - Click Sync now to sync the time setting with the browser.
Next	Get into the next setting page.

Step 2: Configure the settings for Internet connection.

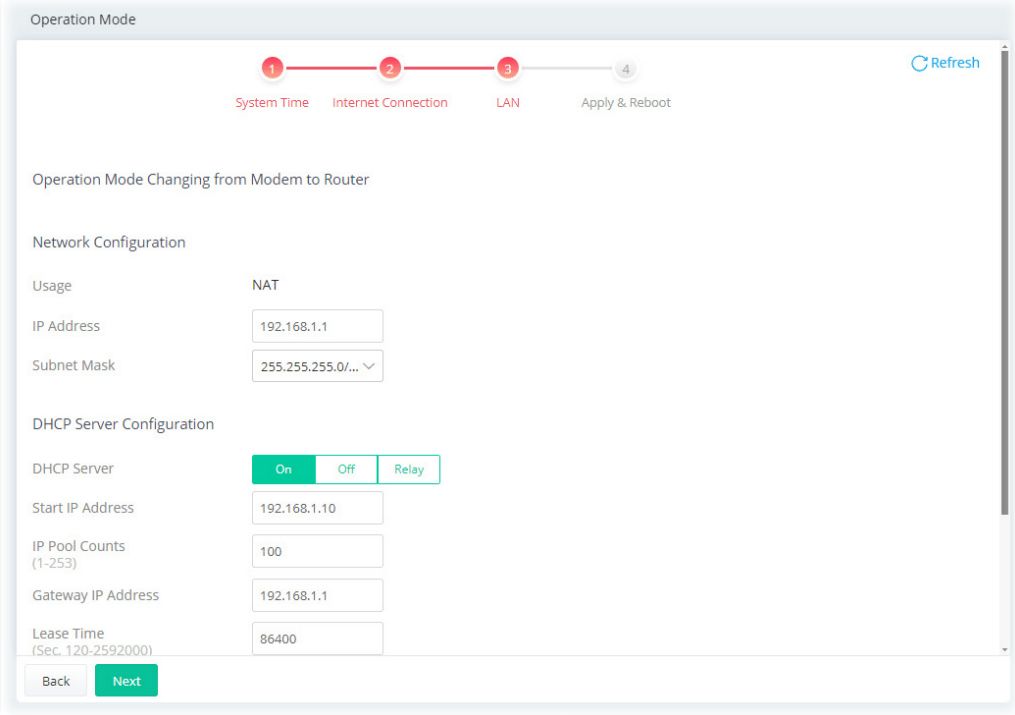


Available settings are explained as follows:

Item	Description
	General
Physical Interface	Displays the physical interface used for the network connection.
DSL Mode	Select the DSL connection mode. Auto - The router will first attempt to connect using VDSL2, and will fall back to ADSL# if VDSL2 is unavailable.
	ADSL Setting
Annex	Specifies the modulation standard used for the ADSL connection.
VPI / VCI	Set values for Virtual Path Identifier(VPI) and Virtual Channel Identifier(VCI).
Customer VLAN	Enabled - Switch the toggle to enable or disable the function. 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.
	VDLS2 Setting
Customer VLAN	Enabled - Switch the toggle to enable or disable the function. 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	Enabled - Switch the toggle to enable or disable the function. 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.
IPv4	
IPv4 Connection Type	Specify the Internet Access Type (PPPoE, PPPoA, Static IP, DHCP).
Username	Enter the username provided by the ISP if PPPoE / PPPoA is selected as IPv4 Connection Type.
Password	Enter the password provided by the ISP if PPPoE / PPPoA is selected as IPv4 Connection Type.
IP Address	Enter the WAN IP address of the router if Static IP is selected as IPv4 Connection Type.
Subnet Mask	Enter the subnet mask of the router if Static IP is selected as IPv4 Connection Type.
Gateway IP	Enter the IP address of the remote gateway if Static IP is selected as IPv4 Connection Type.
Specify DNS	
IPv4 Primary Server	Enter the IP address of the primary DNS server.
IPv4 Secondary Server	Enter the IP address of the secondary DNS server.
Back	Return to previous setting page.
Next	Get into the next setting page.

Step 3: Configure the LAN settings.

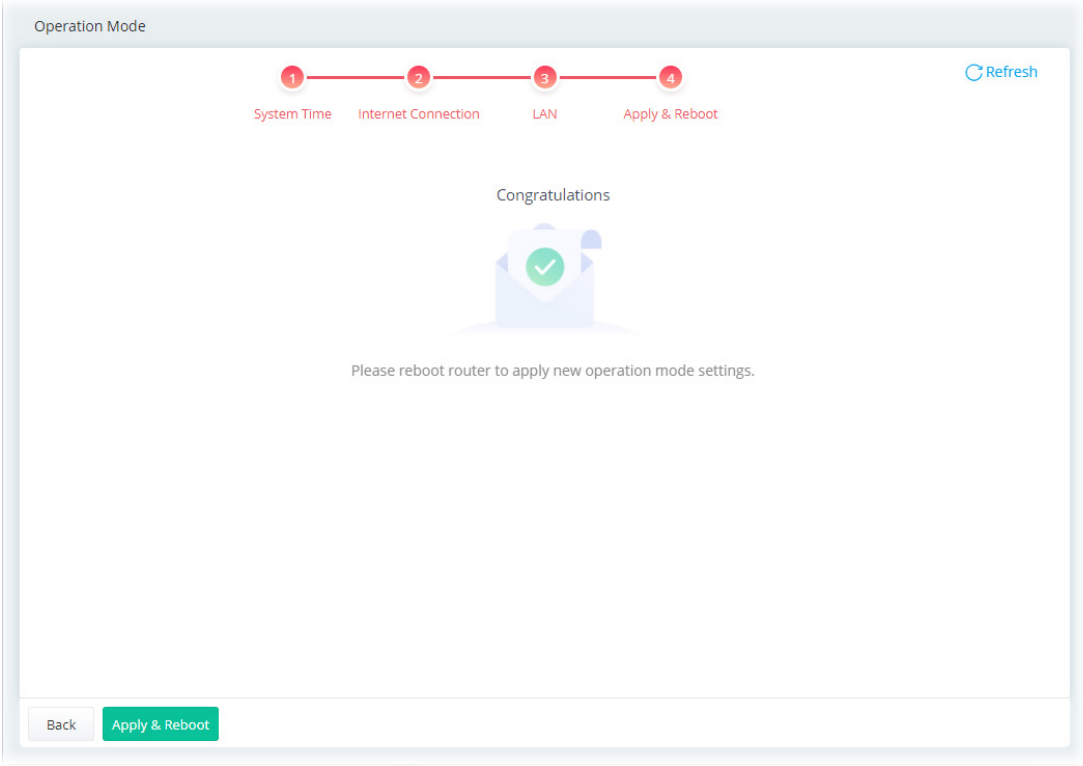


Available settings are explained as follows:

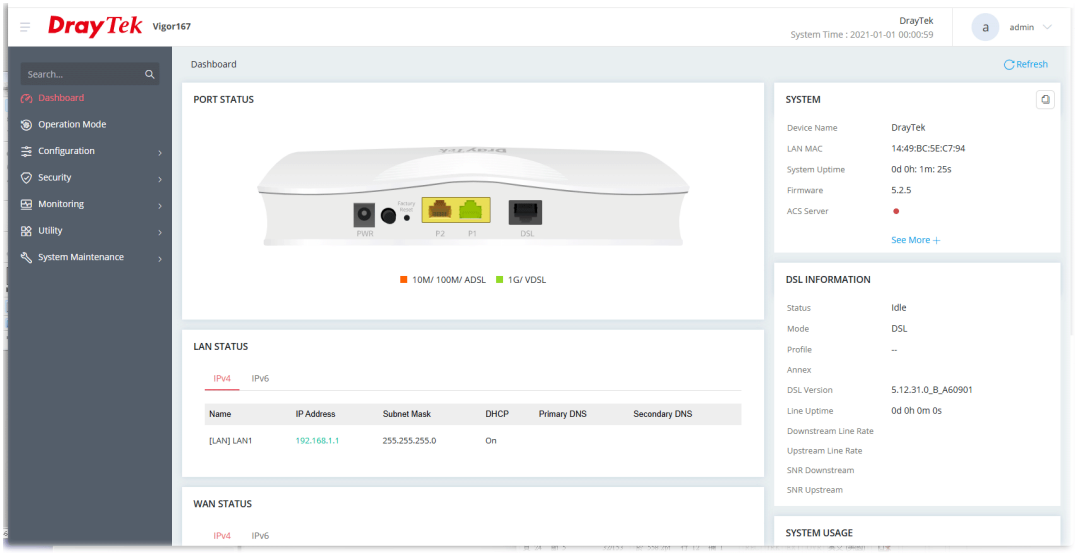
Item	Description
	Network Configuration
Usage	The current is for NAT.
IP Address	This is the IP address of the router. (Default: 192.168.2.1).
Subnet Mask	The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).
	DHCP Server Configuration
DHCP Server	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 server 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.
Start IP Address	It is available when the DHCP server is on. The beginning LAN IP address that is given out to LAN DHCP clients.
IP Pool Counts	It is available when the DHCP server is on. The maximum number of IP addresses to be handed out by DHCP. The default value is 100. Valid range is between 1 and 253. The actual

	number of IP addresses available for assignment is the IP Pool Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller.
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. It is available when the DHCP server is on.
Lease Time	The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. It is available when the DHCP server is on.
Primary DNS	Specify a DNS server IP address. It is available when the DHCP server is on.
Secondary DNS	Specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. It is available when the DHCP server is on.
Interface for 1st DHCP Server	It is available when the DHCP server is set as Relay. Specify a WAN interface for the first DHCP Server.
1st DHCP Server IP Address	It is available when the DHCP server is set as Relay. Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded.
Interface for 2nd DHCP Server	It is available when the DHCP server is set as Relay. The secondary DHCP server is an optional setting. If required, specify a WAN interface for the second DHCP Server as a backup server.
2nd DHCP Server IP Address	It is available when the DHCP server is set as Relay. Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded.
Back	Return to previous setting page.
Next	Get into the next setting page.

Step 4: After finishing the configuration, click Apply & Reboot.

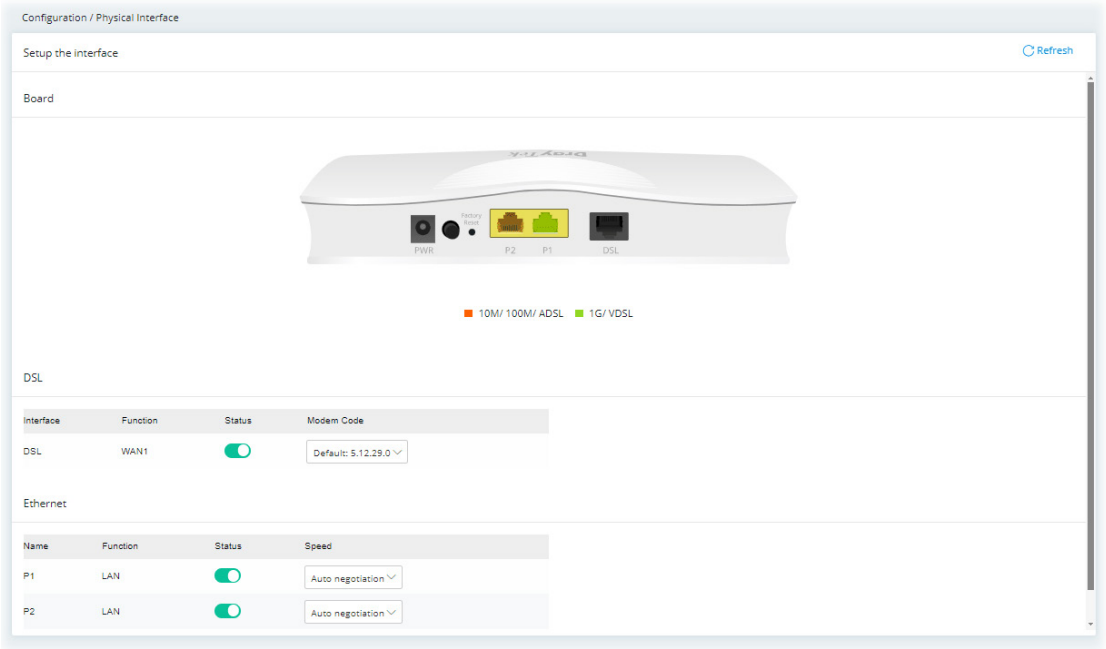


The Main Screen based on Router Mode will be shown as follows.

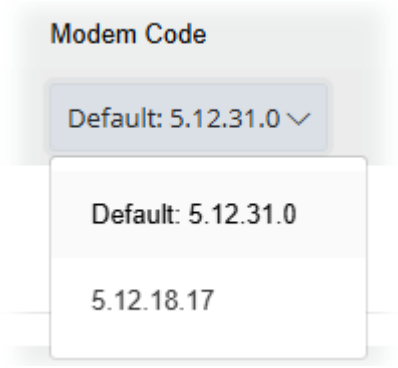


II-2-1 Physical Interface

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



Available settings are explained as follows:

Item	Description
DSL	
Interface	Displays the interface (DSL, ADSL or xDSL and etc.) used for WAN connection.
Function	Displays the WAN# of the WAN connection.
Status	Switch the toggle to enable or disable the function.
Modem Code	Use the default one. Consult your ISP to select the one matching the country in which the router is installed. 
Ethernet	
Interface	Displays the interface (P1, P2) used for LAN connection.
Function	Displays the LAN# of the LAN connection.
Status	Switch the toggle to enable or disable the function.

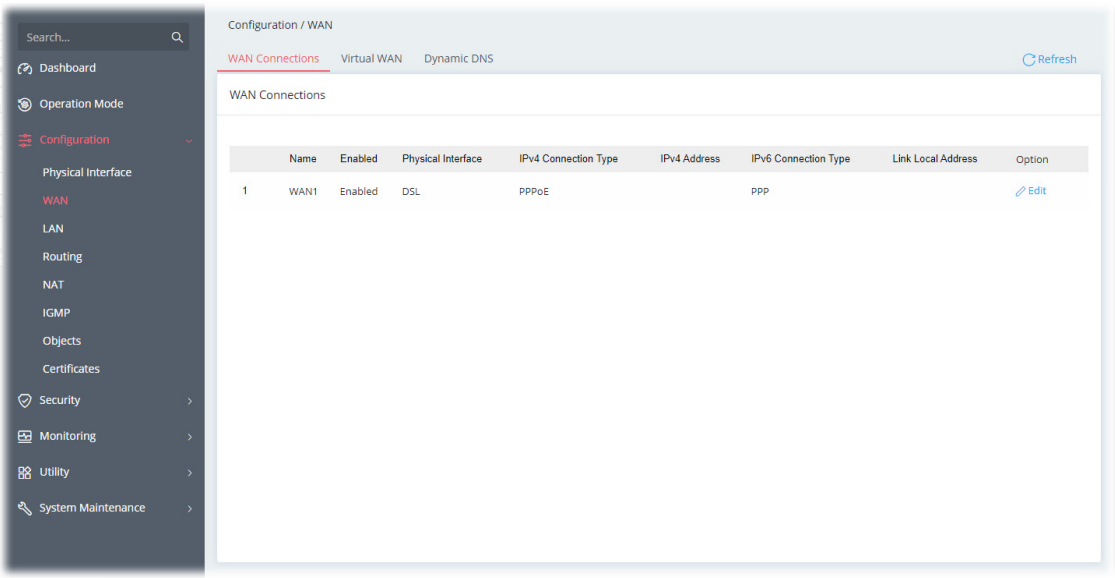
Speed	Set the LAN port speed capabilities:  Port speed capabilities: Auto negotiation: Auto speed with all capabilities. 10M half duplex: Force speed with 10M ability. 10M full duplex: Force speed with 10M ability. 100M half duplex: Force speed with 100M ability. 100M full duplex: Force speed with 100M 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.

II-2-2 WAN

When the operation mode is configured as Router Mode, the Configuration>>WAN page will be shown as the following page.

II-2-2-1 WAN Connections

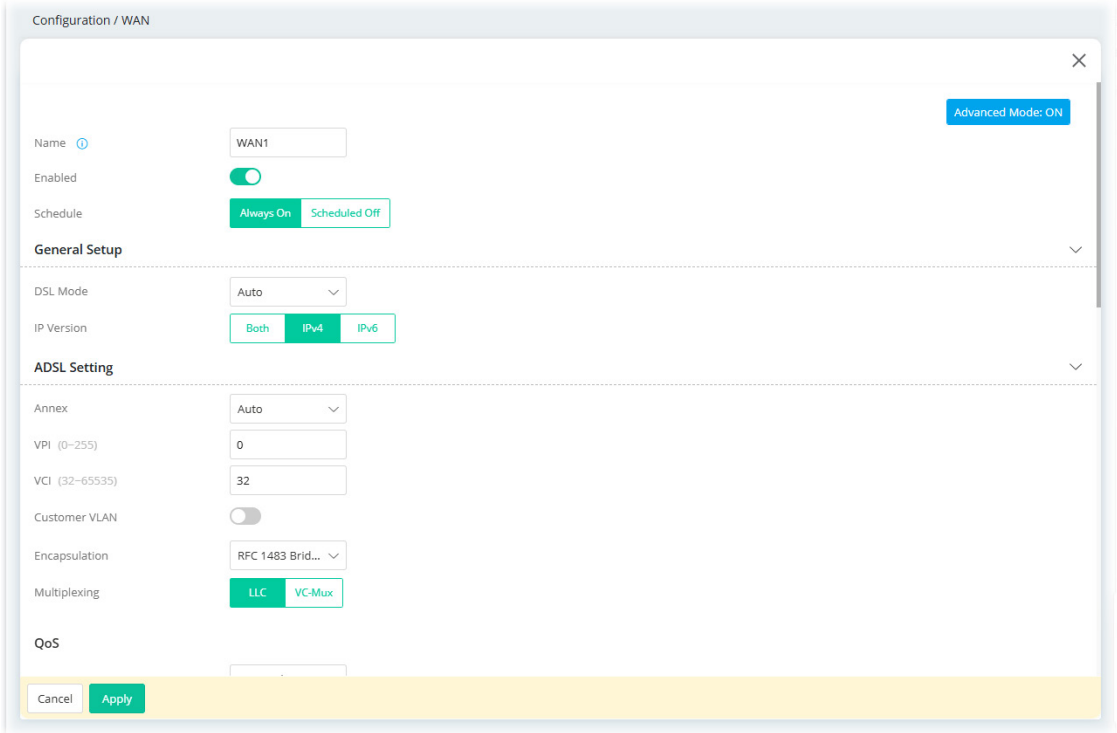
This page is to configure the general settings for WAN connection.



Available settings are explained as follows:

Item	Description
Name	Displays the name of the interface.
Enabled	Displays if the WAN connection is enabled or disabled.
Physical Interface	Displays the physical mode (e.g., ADSL, VDSL, and etc.) used by the WAN interface.
IPv4 Connection Type	Displays the connection type (e.g., PPPoE, DHCP, and etc.).
IPv4 Address	Displays the IP address used by the WAN interface.
IPv6 Connection Type	Displays the connection type (e.g., PPPoE, DHCP, and etc.).
Link Local Address	Displays ink local address.
Option	Edit - Click to modify the interface name and physical mode.

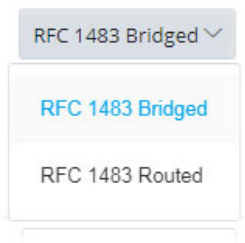
To configure the detailed settings for the selected WAN interface, click the Edit link to the right side of the WAN interface.



Available settings are explained as follows:

Item	Description
Show / Hide Advanced Mode	Click to show or hide the advanced settings for the WAN interface.
Name	Displays current WAN interface.
Enabled	Switch the toggle to enable or disable the function.
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 schedule profile.
General Setup	
DSL Mode	Specify which DSL mode (e.g., VDSL2, ADSL2, ADSL2 multimode, ADSL2+, T1.413, G.DMT) can be used for such WAN connection. Auto – The system will choose the suitable one automatically.
IP Version	Set the protocol (IPv4 or IPv6 or both) that this WAN interface used.
ADSL Setting	
Annex	Choose the correct modem version of the device, e.g., Annex A, Annex B, Annex A/B/M, Annex A/B/J and etc.
VPI	Enter the value provided by ISP.
VCI	Enter the value provided by ISP.
Customer VLAN	Click to enable the function of VLAN with tag. If enabled, 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.
Encapsulation	Encapsulating type of the ADSL connection.
Multiplexing	Encapsulating type of the ADSL connection. Available values are LLC (Logical Link Control) and VC-Mux (Virtual Circuit Multiplexing). Contact your ISP for the correct encapsulating type.
VDSL2 Setting	
Customer VLAN	Click to enable the function of VLAN with tag. If enabled, 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	Click to enable the function of VLAN with tag. If enabled, for what? 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	There are four types: • PPPoE • PPPoA • DHCP • Static IP
Username/Password	It is available when PPPoE/PPPoA is selected as IPv4 Connection Type. Enter the username and password as the primary user account for network connection.
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.
Specify DNS	Switch the toggle to enable/disable the function. IPv4 Primary IP Address - Enter the primary IP address for the router IPv4 Secondary IP Address - If necessary, Enter secondary IP address for necessity in the future.
WAN Connection Detection	
Mode	Configures how the WAN connection is monitored. Choose Always On, ARP Detect or Ping Detect for the system to execute for WAN detection. ARP Detect - The router broadcasts an ARP request every 5 seconds. If 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.
TTL	It is available when Ping Detect is selected as WAN Connection Detection Mode. Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
Ping Interval	It is available when Ping Detect is selected as WAN Connection Detection Mode. Enter the interval for the system to execute the PING operation.
Ping Retry	It is available when Ping Detect is selected as WAN Connection Detection Mode. Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
PPPoE Pass-through	
To Wired LAN	Switch the toggle to enable or disable the function. If enabled, the wired LAN clients can initiate PPPoE dial-up connections to the WAN. 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.
Options under the Advanced Mode	
ADSL Setting	Below shows the additional options for ADSL Setting: Encapsulation - Encapsulating type of the ADSL connection.  Multiplexing - Encapsulating type of the ADSL connection. Available values are LLC (Logical Link Control) and VC-Mux (Virtual Circuit Multiplexing). Contact your ISP for the correct encapsulating type.
QoS	
ATM QoS	Configure the Quality of Service (QoS) of the ATM circuit. Select a proper QoS type for the interface.

	 UBR Without PCR- Unspecified Bit Rate. UBR With PCR- Unspecified Bit Rate. Enter the value for PCR (Peak Cell Rate, 0_5500) if select UBR With PCR. CBR - Constant Bit Rate. nrtVBR - Non-real-time Variable Bit Rate. rtVBR - Real-time Variable Bit Rate.
IPv4 - Below shows the additional options for IPv4 Setting:	
Service Name (Optional)	It is available when PPPoA/PPPoE is selected as IPv4 Connection Type. Sets the PPP service name tag. Required by some ISPs. Leave blank unless instructed otherwise by your ISP.
Fallback Account	It is available when PPPoA/PPPoE is selected as IPv4 Connection Type. Switch the toggle to enable or disable the function. Once the primary user account fails to set a network connection, use the fallback account instead. Username - Enter a string as a username of the fallback account. Password - Enter a string as the password.
Separate Account for ADSL	It is available when PPPoA/PPPoE is selected as IPv4 Connection Type. In default, WAN1 supports VDSL2/ADSL and uses the same PPPoE account and password for connection. If ADSL mode requires a separate user name and password, enable this function and fill out the Username and Password fields below. Switch the toggle to enable or disable the function. Username - Enter a string as the username. Password - Enter a string as the password.
PPP Authentication	It is available when PPPoA/PPPoE is selected as IPv4 Connection Type. 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 PPPoA/PPPoE is selected as IPv4 Connection Type. DHCP - WAN IP address is dynamically allocated. Static IP - ISP has assigned a fixed WAN IP address. ● IP Address - Enter the IP address offered by your ISP.
IP Alias	+Add - Click to enter multiple WAN IPv4 addresses assigned by your ISP.
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

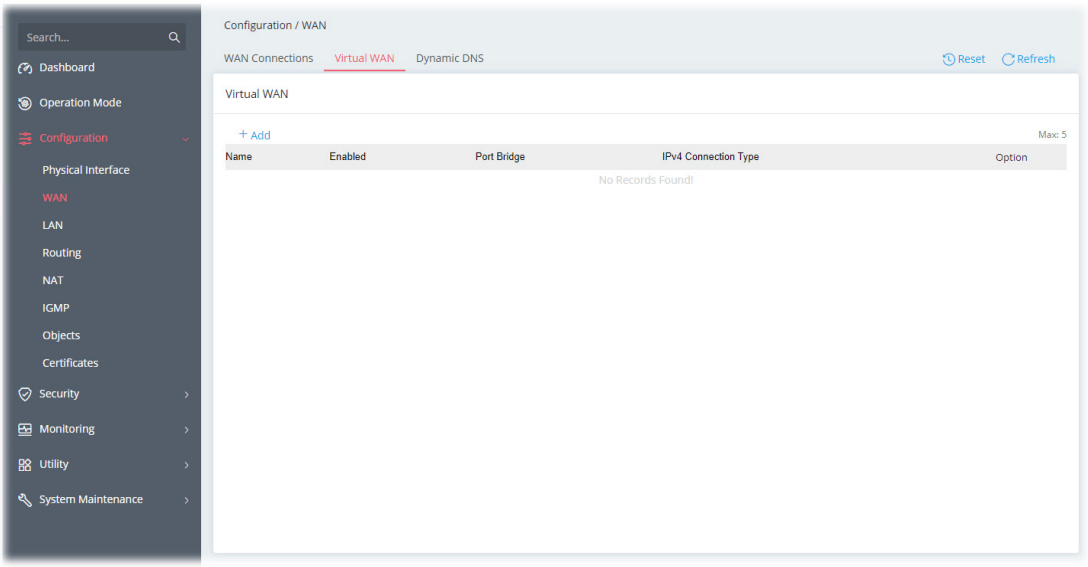
	PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492.
WAN MAC Address	
Mode	Default - Use the default MAC address for the WAN Ethernet port. Customized - Select this option if your ISP authenticates by MAC addresses. • MAC - Specify a MAC address for the WAN Ethernet port.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

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

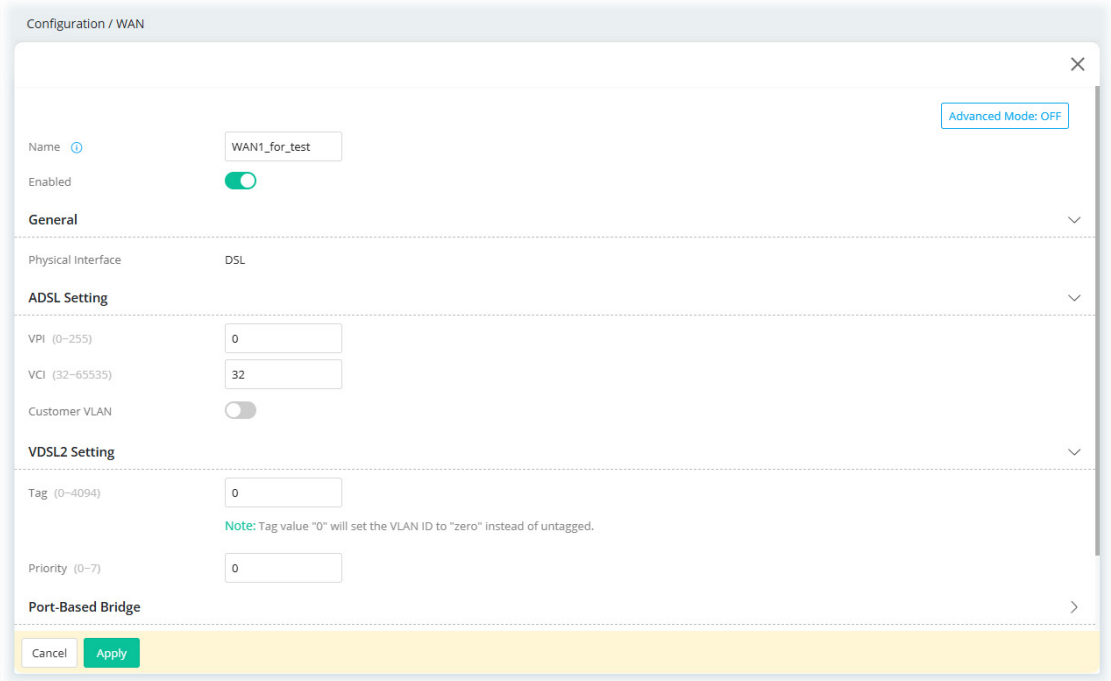
II-2-2-2 Virtual WAN

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

Each profile can be specified with ATM QoS, VLAN, and binding interfaces according to the requirement of the practical network environment.

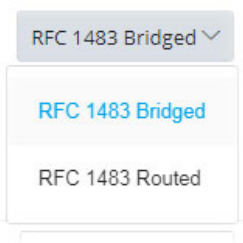


To add a new virtual WAN, click the +Add link to get the following page.



Available settings are explained as follows:

Item	Description
Show / Hide Advanced Mode	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	
Physical Interface	Displays the WAN type (e.g., DSL) of the physical interface.
ADSL Setting	VPI - Enter the value provided by ISP. VCI - Enter the value provided by ISP. Customer VLAN - Click to enable the function of VLAN with tag. If enabled, • 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.
VDSL2 Setting	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.
Port-Based Bridge	
Port Bridge	Switch the toggle to enable or disable the function. Binding Interface - Click +Add to add an interface for binding.
IPv4	
Enabled	Switch the toggle to enable or disable the function.
IPv4 Connection Type	There are four types for network connection: • PPPoE • PPPoA • DHCP • Static IP
Username/Password	It is available when PPPoE/PPPoA is selected as IPv4 Connection Type.
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.
Options under the Advanced Mode	
ADSL Setting	Below shows the additional options for ADSL Setting: Encapsulation - Encapsulating type of the ADSL connection.  Multiplexing - Encapsulating type of the ADSL connection. Available values are LLC (Logical Link Control) and VC-Mux (Virtual Circuit

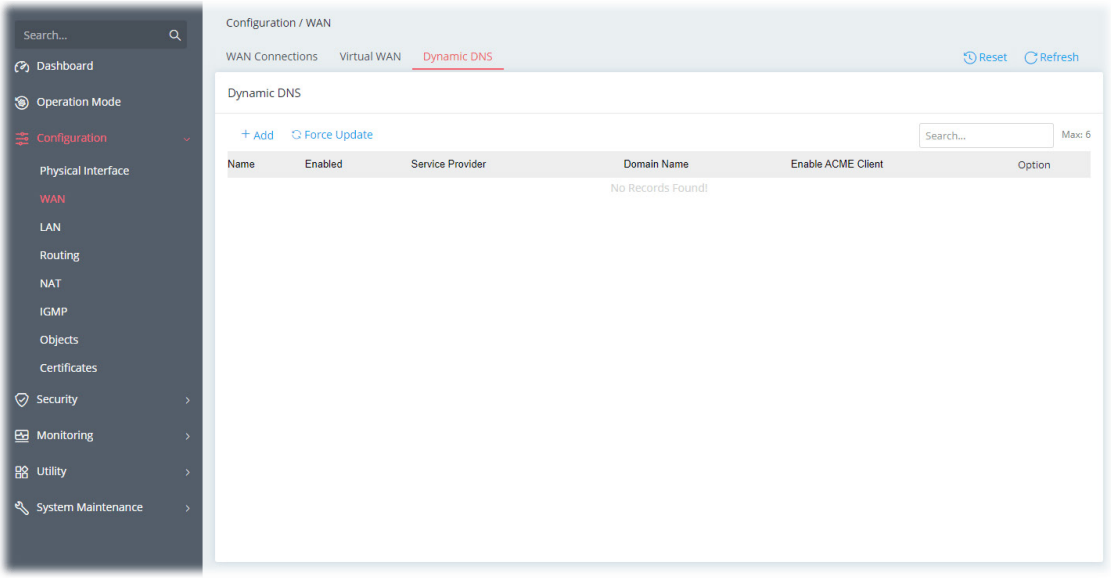
	Multiplexing). Contact your ISP for the correct encapsulating type.
	QoS
ATM QoS	Configure the Quality of Service (QoS) of the ATM circuit. Select a proper QoS type for the interface.  UBR Without PCR- Unspecified Bit Rate. UBR With PCR- Unspecified Bit Rate. Enter the value for PCR (Peak Cell Rate, 0_5500) if select UBR With PCR. CBR - Constant Bit Rate. nrtVBR - Non-real-time Variable Bit Rate. rtVBR - Real-time Variable Bit Rate.
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-2-2-3 Dynamic DNS

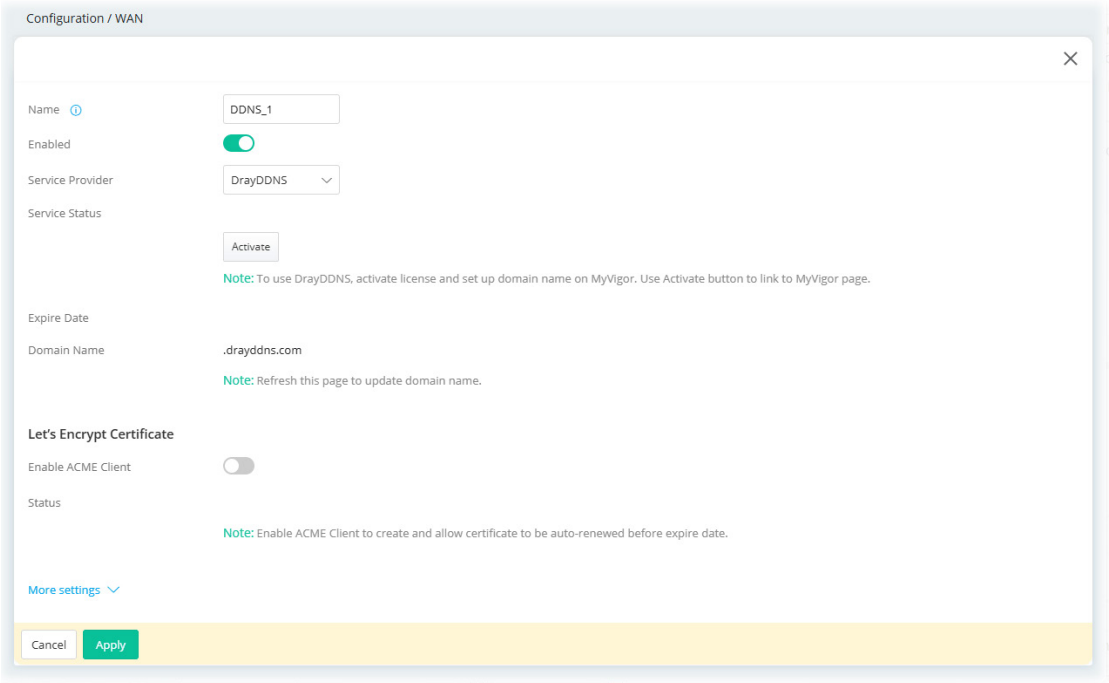
Most ISPs assigns dynamic WAN IP addresses to their customers. Dynamic IP addresses presents challenges to users who would like to accept remote connections to their LANs from the Internet, as service could be disrupted due to the IP address changing without notice. By setting up service with a Dynamic 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.



Item	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.



Available settings are explained as follows:

Item	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 ● 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.
If NO-IP 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.
Let's Encrypt Certificate	Display the information related to Let's Encrypt certificate. Activate - Click it to generate a certificate issued by Let's Encrypt for applying to such DDNS account.
More settings	
Update DDNS with	If a Vigor router is installed behind any NAT router, you can enable such 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: ● WAN IP - The IP address of the router's WAN interface will be used. ● Internet IP – The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address.
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.

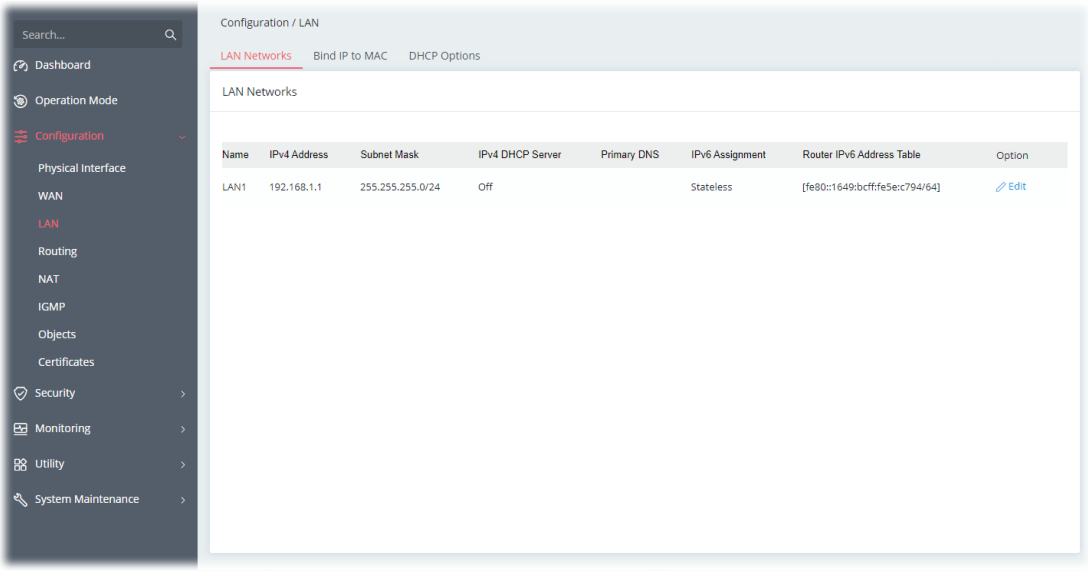
After finishing this web page configuration, please click Apply to save the settings.

II-2-3 LAN

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

II-2-3-1 LAN Networks

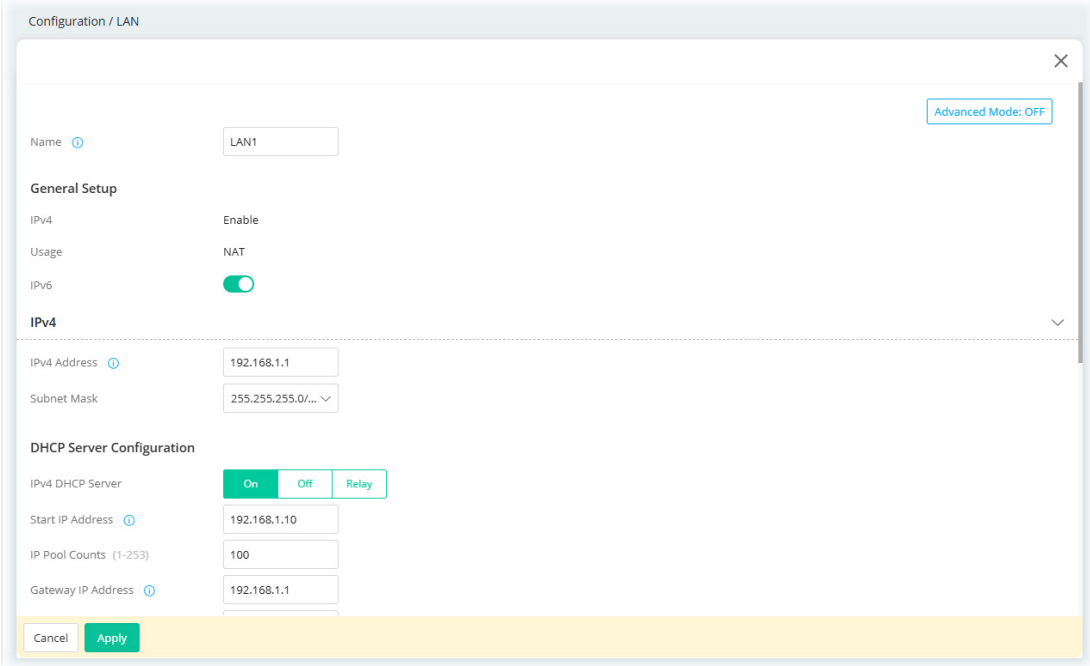
To configure the general settings the LAN network, select Configuration>>LAN to open the following page.



Available settings are explained as follows:

Item	Description
Name	Displays the number of LAN interface.
IP Address	Displays the IP address of the LAN interface.
Subnet Mask	Displays the subnet mask of the LAN interface.
Option	Edit - Click to modify the name, IP address, and subnet mask settings.

To configure the detailed settings for the selected WAN interface, click the Edit link to the right side of the LAN interface.



Available settings are explained as follows:

Item	Description
Advanced Mode: ON/OFF	Click to show or hide the advanced settings for LAN.
Name	Enter a brief comment for the LAN interface.
General Setup	
IPv4	Display the status (enable/disable) of the profile.
Usage	Display current IP forwarding method.
IPv6	Switch the toggle to configure / ignore the IPv6 settings.
IPv4	
IP Address	Enter the IP address of the LAN interface.
Subnet Mask	Select a subnet mask of the LAN interface.
DHCP Server Configuration	
DHCP Server	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 server 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 200. Valid range is between 1 and 1021. The actual number of IP addresses available for assignment is the IP Pool Counts, or 1021 minus the last octet of the Start IP Address, whichever is smaller. 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, and therefore the Gateway IP Address should be identical to the IP Address in the IPv4 section above. 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. 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.
If Off is selected as DHCP Server	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.
If 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. 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. 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.

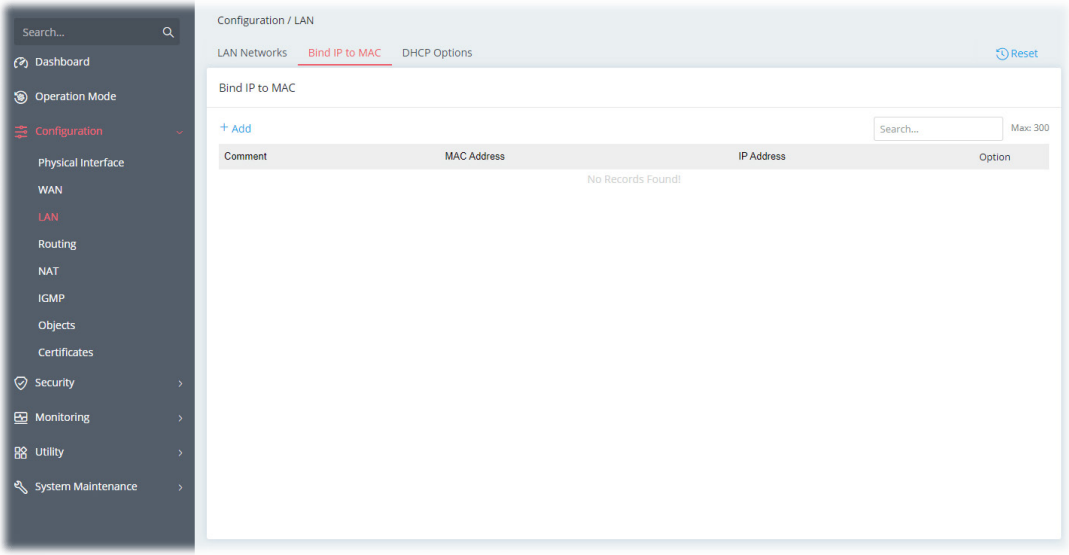
IPv6	
IPv6 Assignment	Configures the Managed Address Configuration flag (M-bit) in Route Advertisements. Stateless – M-bit is unset. DHCPv6(Stateful) – M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor router, or a separate DHCPv6 server. Manual – No configuration information is sent.
Router Advertisement Configuration	It is available when Stateless is selected as the IPv6 Assignment. 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. 
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. Secondary DNS Address - Enter another IPv6 address for DNS server if required.
Options under the Advanced Mode	
Router IPv6 Address Table	Enter IPv6 Address and Prefix length to be added, or click an existing 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.
IPv6 - More settings	
Force DNS Redirection	Switch the toggle to enable or disable the function. It allows all outgoing DNS lookups to be intercepted and redirected to the router's built-in DNS server, improving the domain lookup performance by caching DNS queries and results.
Virtual Interface	Switch the toggle to enable or disable the function. The virtual interface is a routing interface that can be used for routing packets to specified domain. IP Address - Enter an IP address. Subnet Mask - Select a subnet mask. After configuring this option, set a Bind IP to MAC profile (based on the IP address and subnet mask set above) or specify a static IP for the clients.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

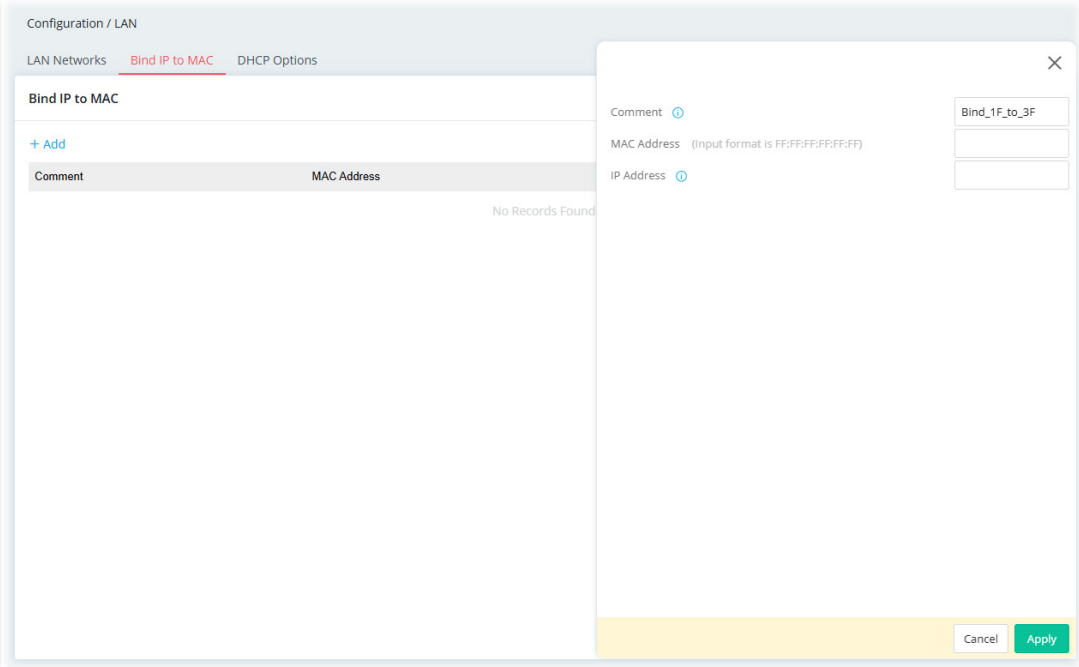
After finishing this web page configuration, please click Apply to save the settings.

II-2-3-2 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.



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



Available settings are explained as follows:

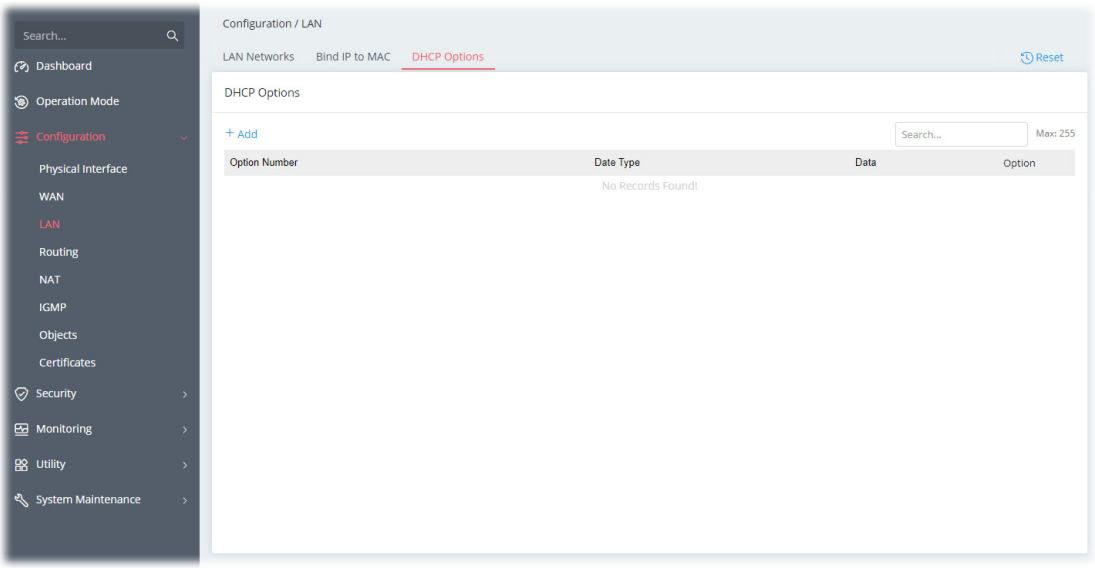
Item	Description
Comment	Enter a brief comment to identify this IP Address – MAC Address pair.
MAC Address	Enter the MAC address of the LAN client's network interface.
IP Address	Enter the IP address to be associated with a MAC address.

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

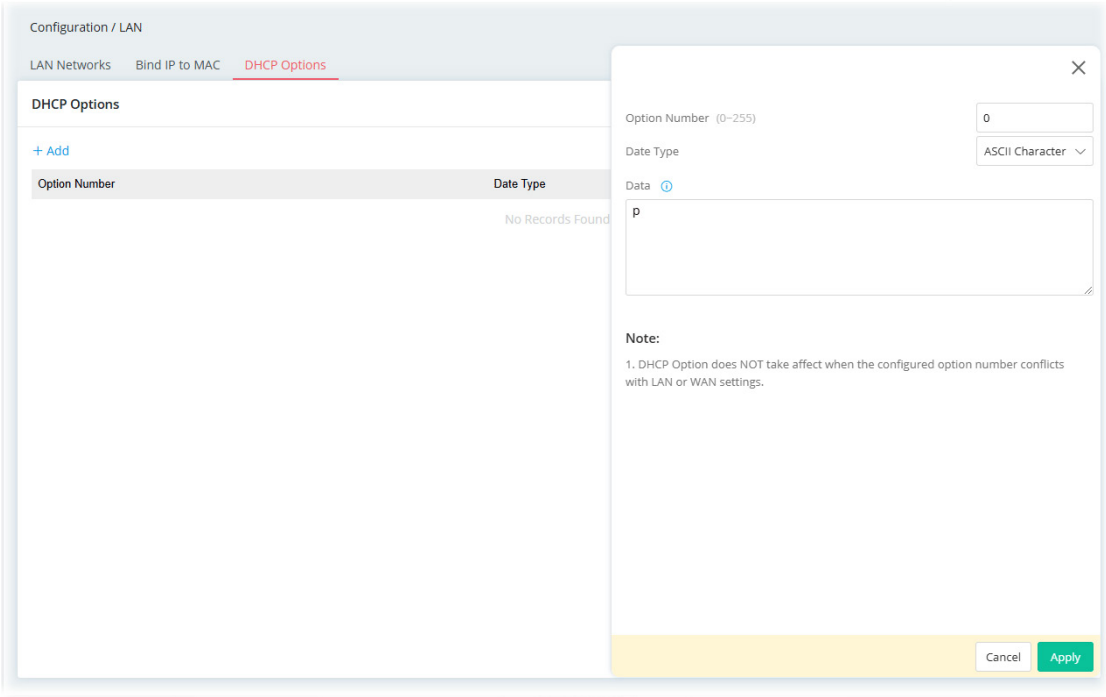
After finishing this web page configuration, please click Apply to save the settings.

II-2-3-3 DHCP Options

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



To add an option, click the +Add link to get the following page.



Available settings are explained as follows:

Item	Description

Option Number	Enter a number for this function.
Data Type	Choose the type (ASCII or Hex or Address List) for the data to be stored.
Data	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.
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-2-4 Routing

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

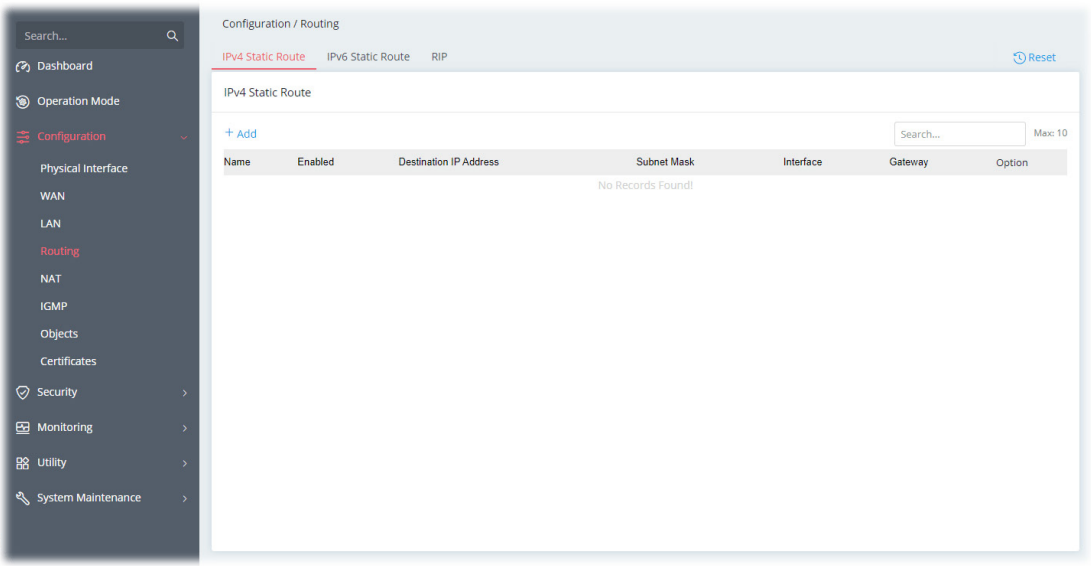
The packets will be directed to the specified interface if they match one of the routing policies.

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

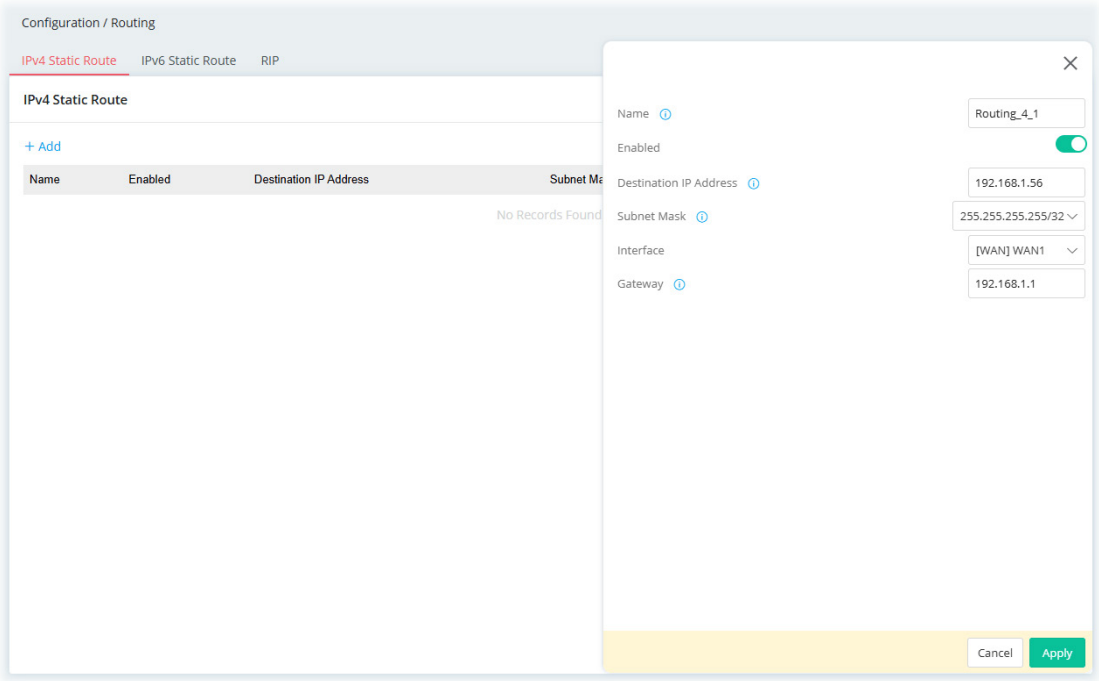
Open Configuration >> Routing.

II-2-4-1 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.



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



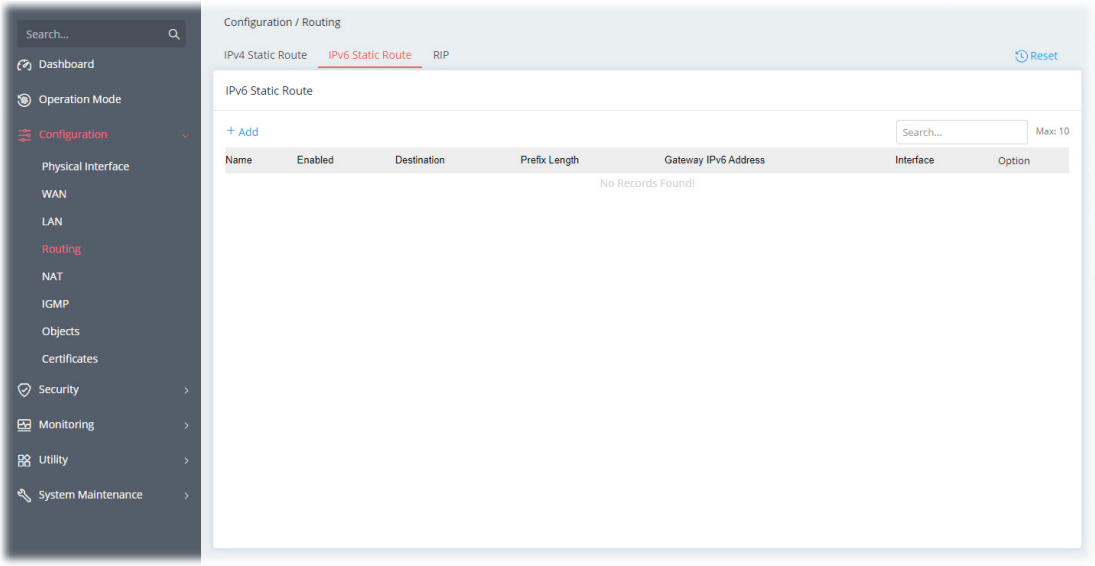
Available settings are explained as follows:

Item	Description
Name	Enter 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.

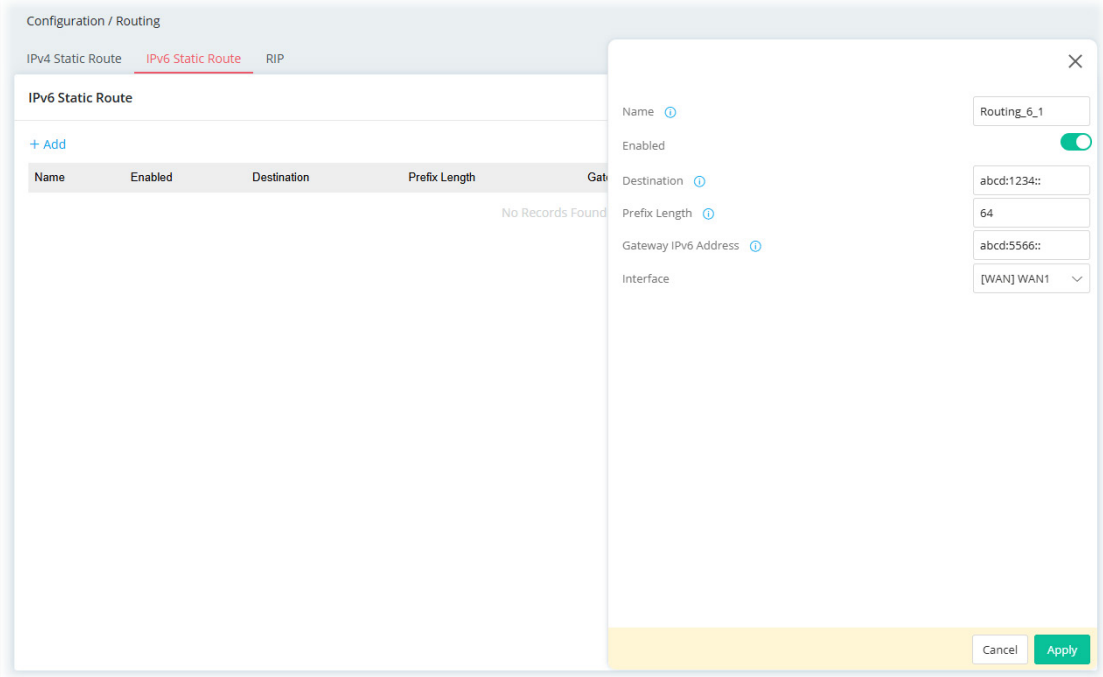
After finishing this web page configuration, please click Apply to save the settings.

II-2-4-2 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.



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



Available settings are explained as follows:

Item	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.

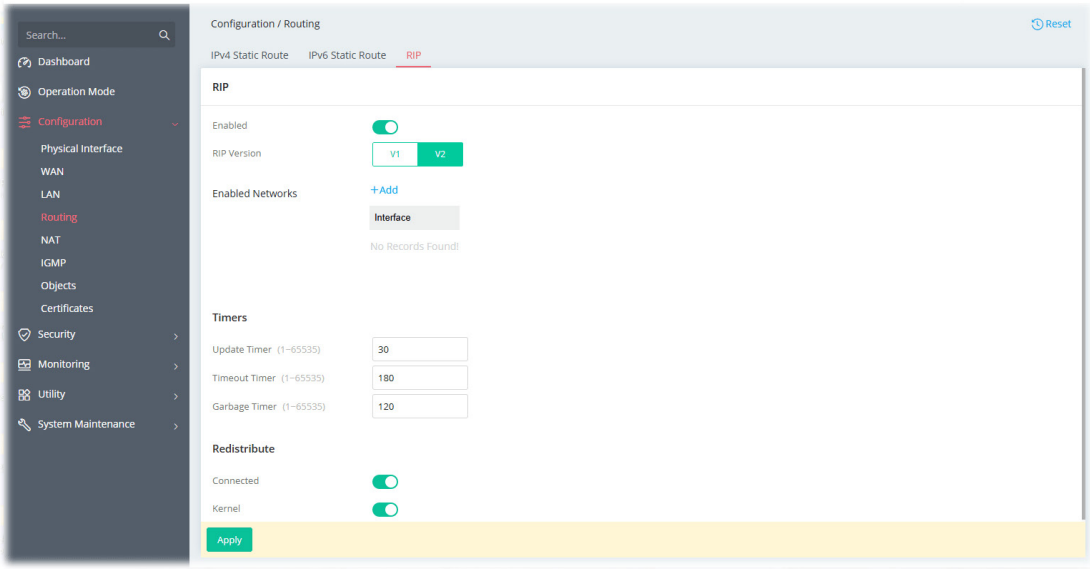
Prefix Length	Enter the fixed value for prefix length.
Gateway IPv6 Address	Enter an IPv6 address as the gateway.
Interface	Use the drop-down list to specify an interface for this static route.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-2-4-3 RIP

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

The Routing Information Protocol (RIP) is the most popular interior routing protocol used by a router.



Available settings are explained as follows:

Item	Description
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.
Enabled Networks	+Add - Specify an interface (LAN/WAN) for applying the RIP.
Timers	
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.
Redistribute	
Connected	Redistribute connected routes into the RIP tables.
Kernel	Redistribute kernel routes into the RIP tables.
Apply	Save the current settings and exit the page.

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

II-2-5 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.

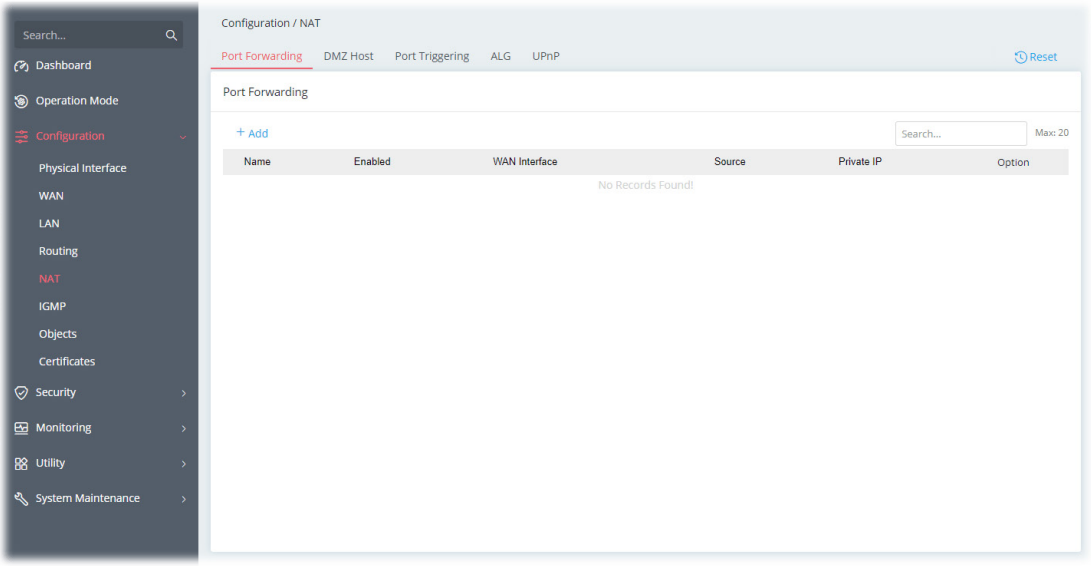
The benefit of the NAT includes:

- 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.

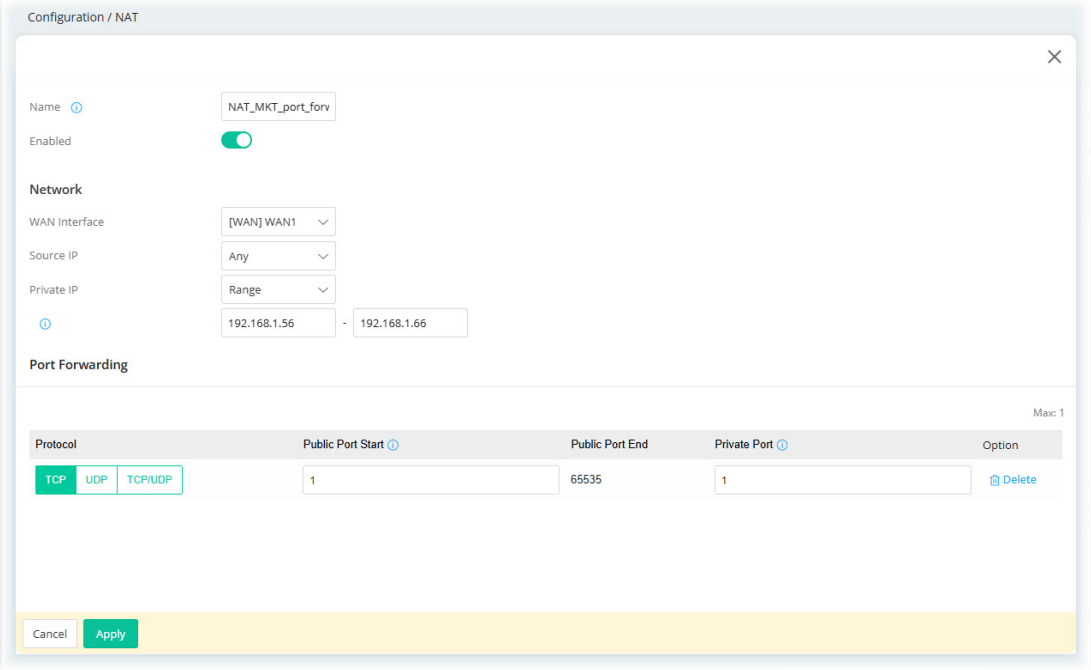
II-2-5-1 Port Forwarding

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

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



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



Available settings are explained as follows:

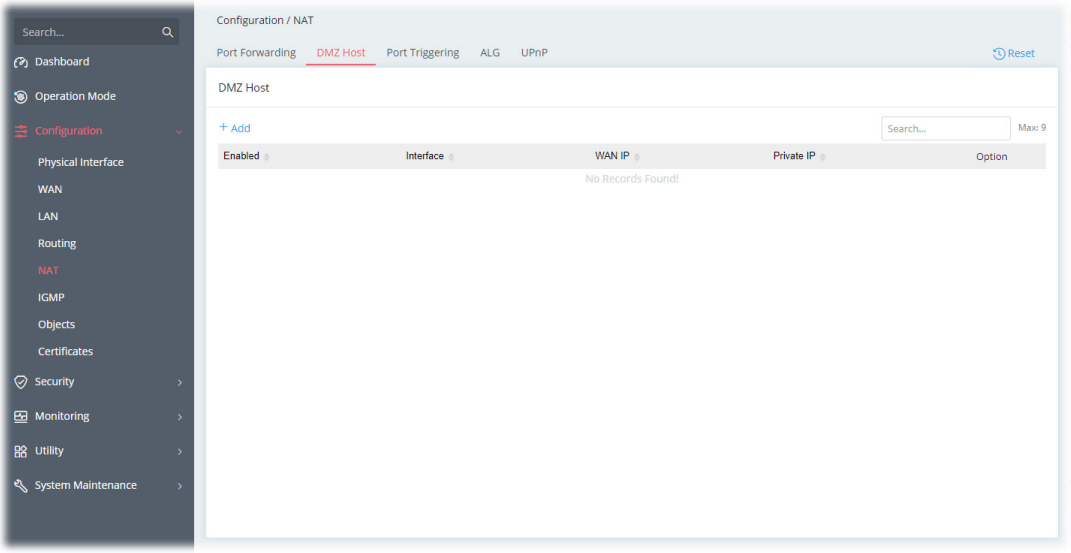
Item	Description
Name	Enter a name that identifies the rule.
Enabled	Switch the toggle to enable or disable the function.
	Network
WAN Interface	The WAN port(s) whose incoming traffic will be forwarded to a LAN client. Select from a specific WAN interface WAN# to apply the rule to the WAN interface.
Source IP	Any - 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 - Use the drop down list to specify an IP object profile. 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 - 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. Options - 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.

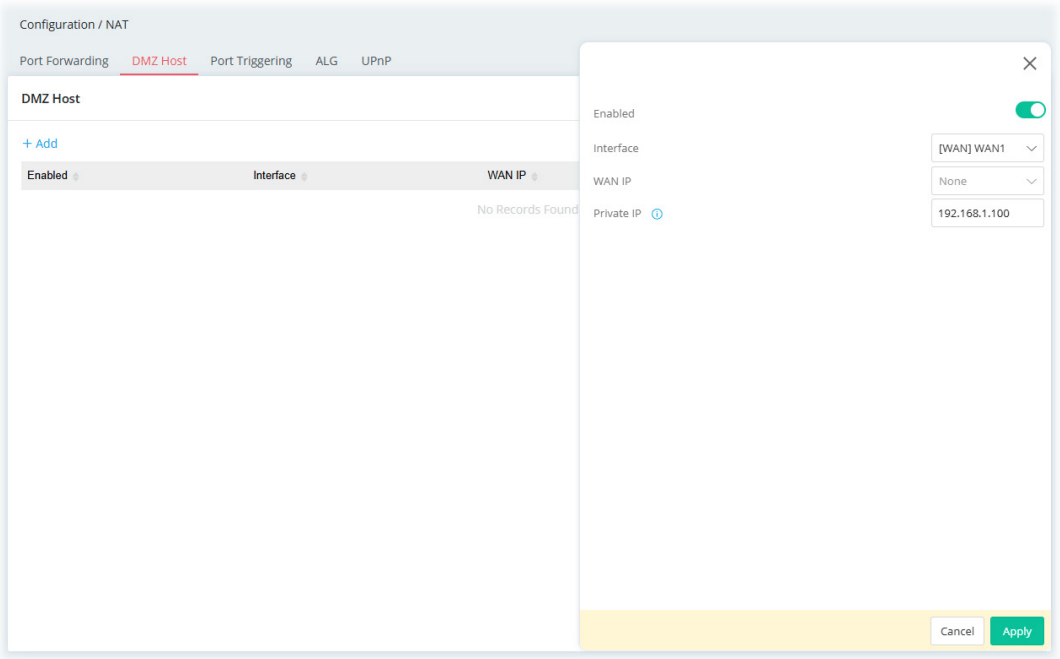
After finishing this web page configuration, please click Apply to save the settings.

II-2-5-2 DMZ

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.



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



Available settings are explained as follows:

Item	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	Select one private IP address in the list to be the DMZ host.
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-2-5-3 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.

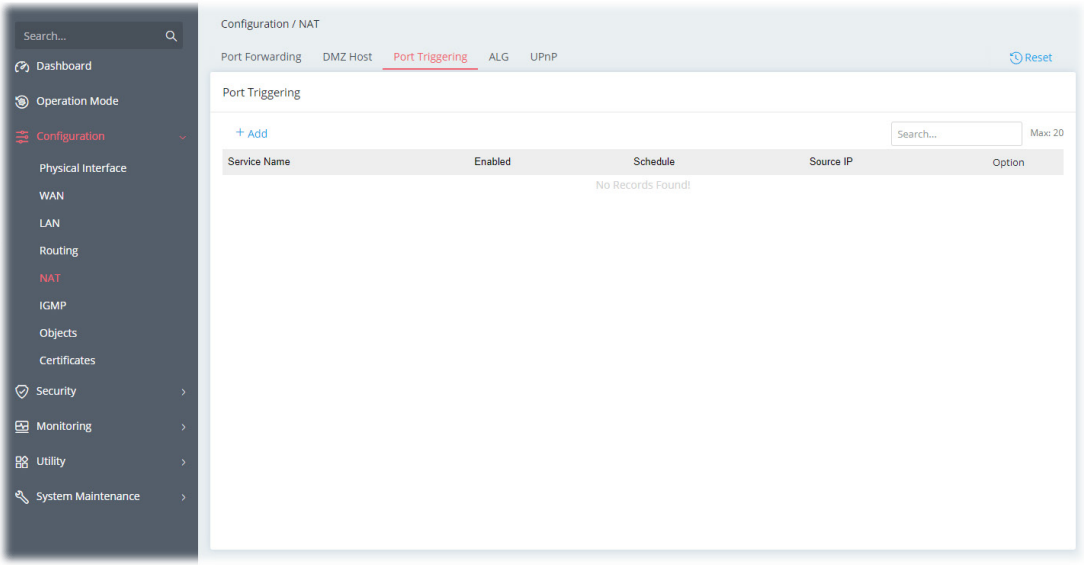
TCP: 86400 sec.

UDP: 180 sec.

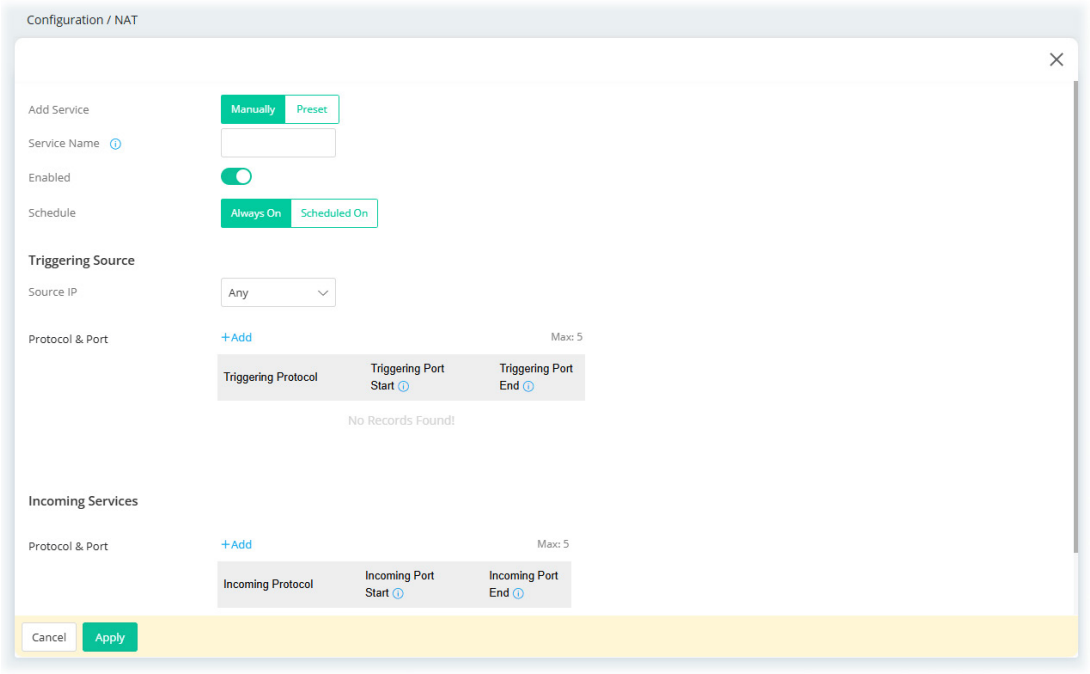
IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.



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



Available settings are explained as follows:

Item	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. Preset - If selected, various services will be offered for you to choose as the service name.
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 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 Object - Use the drop down list to specify an IP object profile. IP Group - Use the drop down list to specify an IP group profile.
Protocol & Port	+Add - Click to set port numbers (start and end) for the specified protocol (TCP, UDP or TCP/UDP) for the outgoing data (that this rule monitors).
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 - 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.

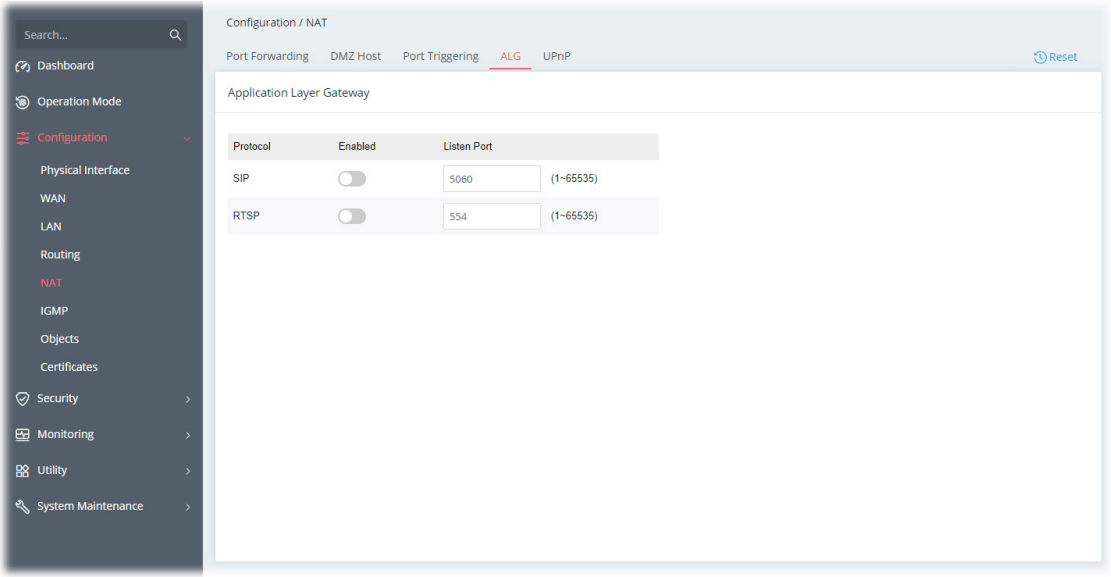
After finishing this web page configuration, please click Apply to save the settings.

II-2-5-4 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 voice and 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.



Available settings are explained as follows:

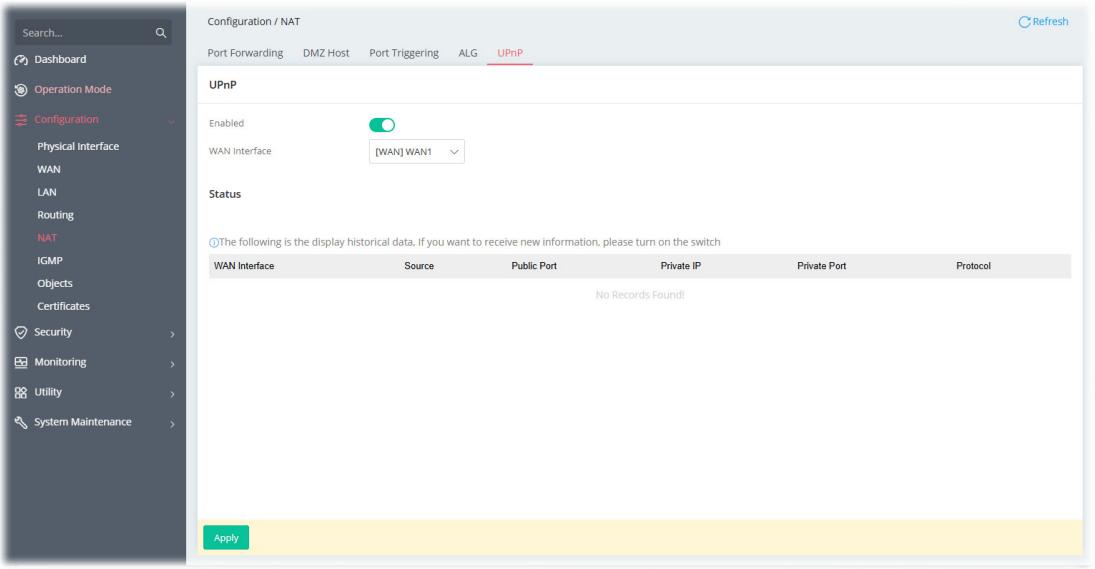
Item	Description
Enabled	Switch the toggle to enable or disable the function.
Listen Port	Enter a port number for SIP or RTSP protocol.
Apply	Save the current settings and exit the page.

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

II-2-5-5 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.



Available settings are explained as follows:

Item	Description
UPnP	
Enabled	Switch the toggle to enable or disable the function. UPnP is required for some applications such as PPS, Skype, eMule...and 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.

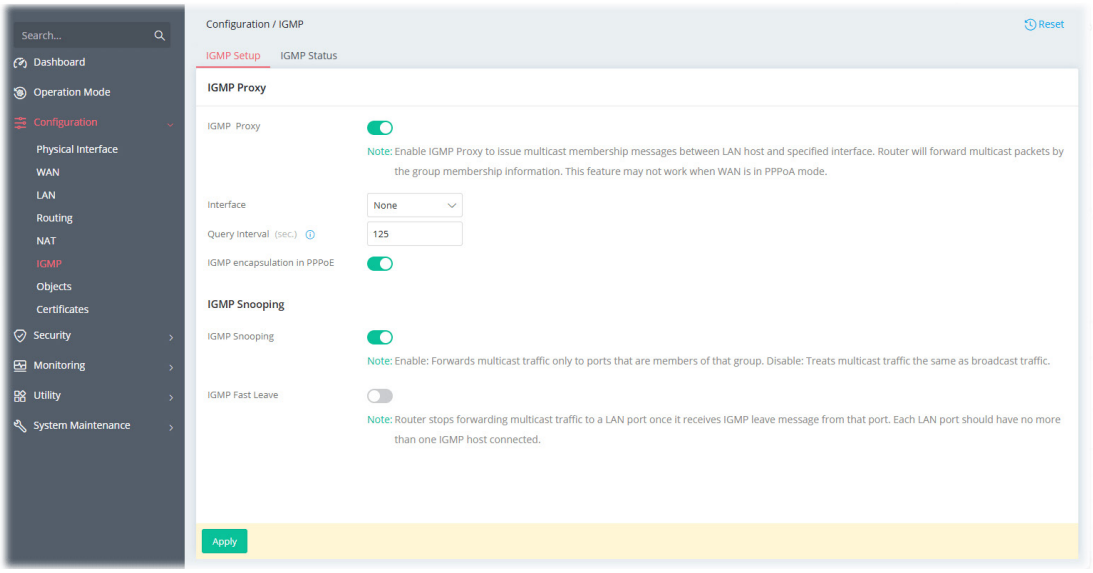
After finishing this web page configuration, please click Apply to save the settings.

II-2-6 IGMP

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

II-2-6-1 IGMP Setup

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



Available settings are explained as follows:

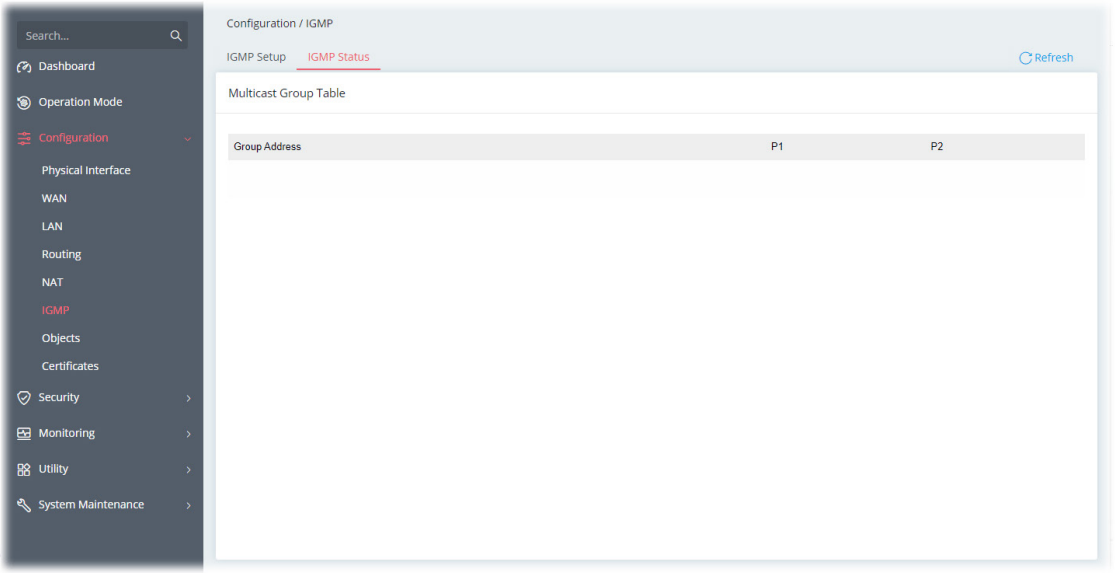
Item	Description
IGMP Proxy	
IGMP Proxy	Switch the toggle to enable or disable the function. The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode.
Interface	Specify an interface for packets passing through.
Query Interval	Vigor 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	Enable this function if the interface type for IGMP is 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 Snooping	Select to enable IGMP Snooping so that multicast traffic are 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.

Apply	Save the current settings and exit the page.

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

II-2-6-2 IGMP Status

Displays a list of active multicast groups.

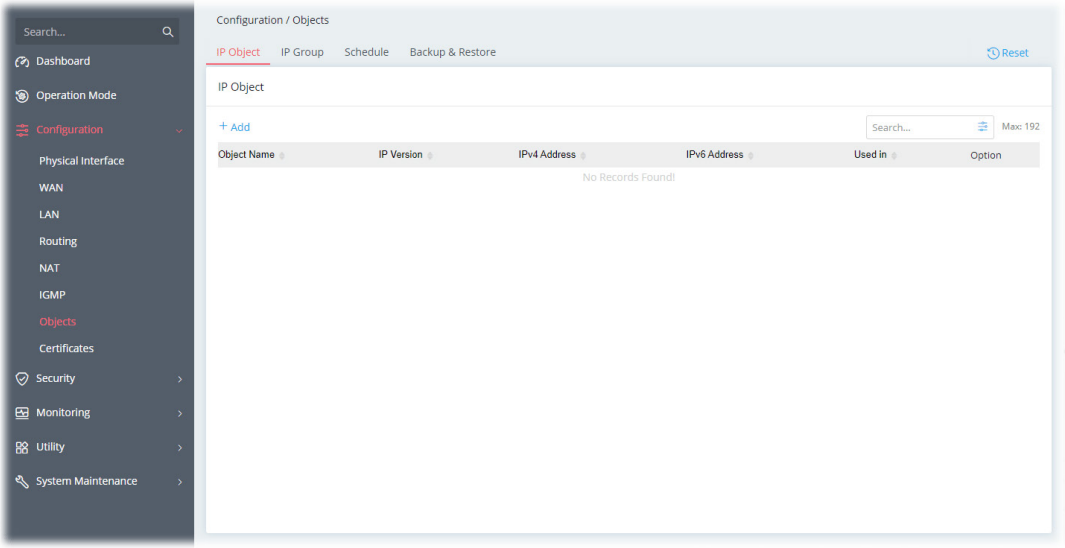


Item	Description
Group ID	ID port of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254.
P1 to P2	LAN ports that have IGMP hosts joined to this multicast group.

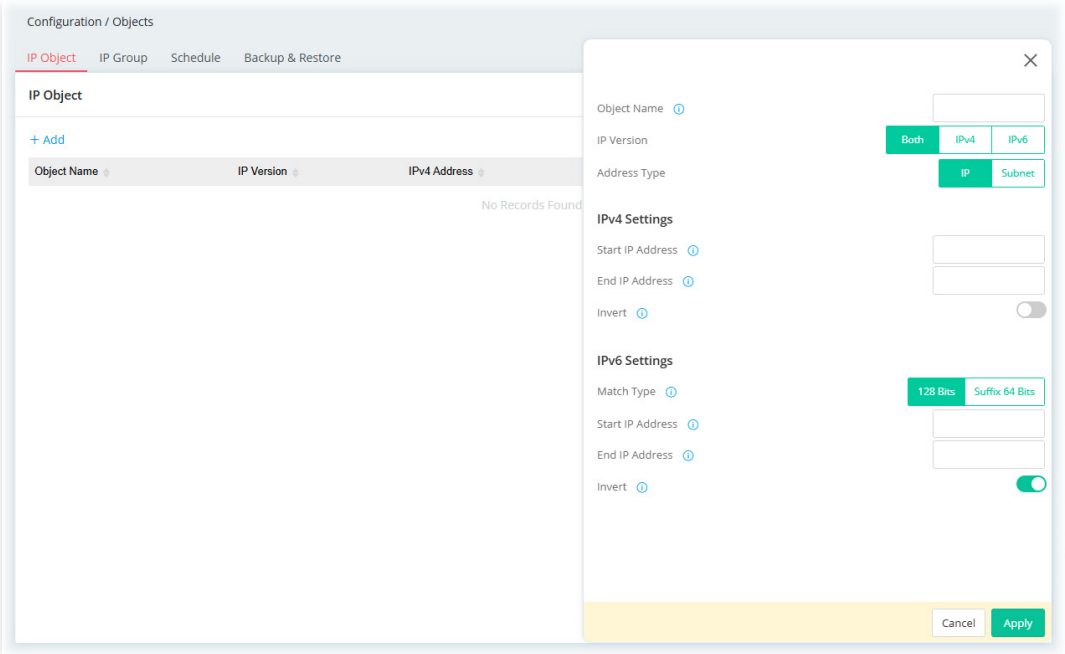
II-2-7 Objects

II-2-7-1 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 them with groups for using conveniently. Later, we can select that object/group for applying it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).



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



Available settings are explained as follows:

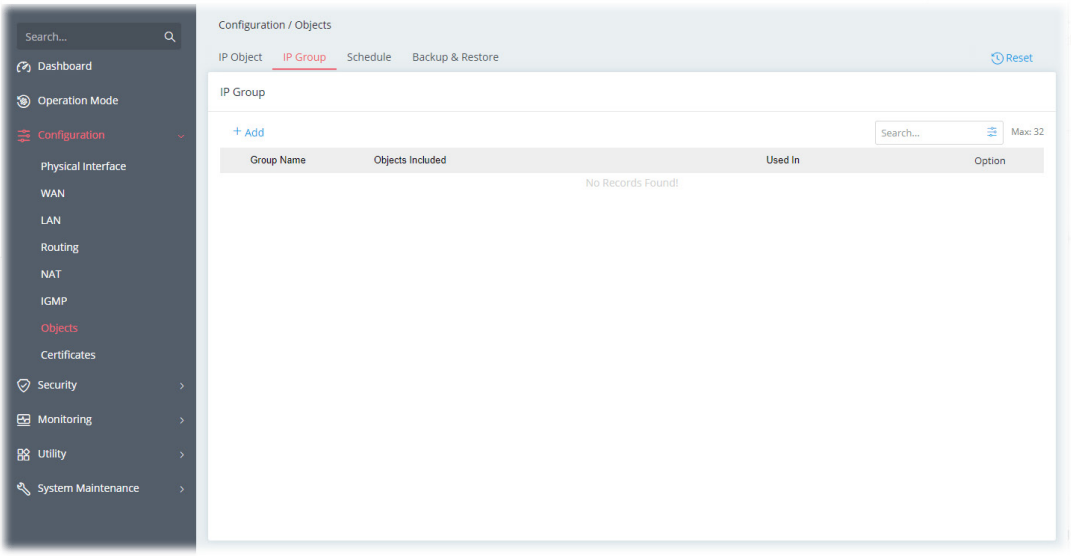
Item	Description
Object Name	Enter the name that identifies this profile.
IP Version	Select the IP version (IPv4, IPv6 or Both) for entering correct IP address.
Address Type	Select the type (IP or Subnet) of address.
IPv4 Settings	
Start IP Address	Enter the beginning IP address, if the Address Type 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 Mask.

Subnet Mask	Enter subnet mask, if Address Type is Subnet Mask.
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.
IP Address	Enter the IPv6 address.
Prefix Length	Enter IPv6 prefix length of the IPv6 block.
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.

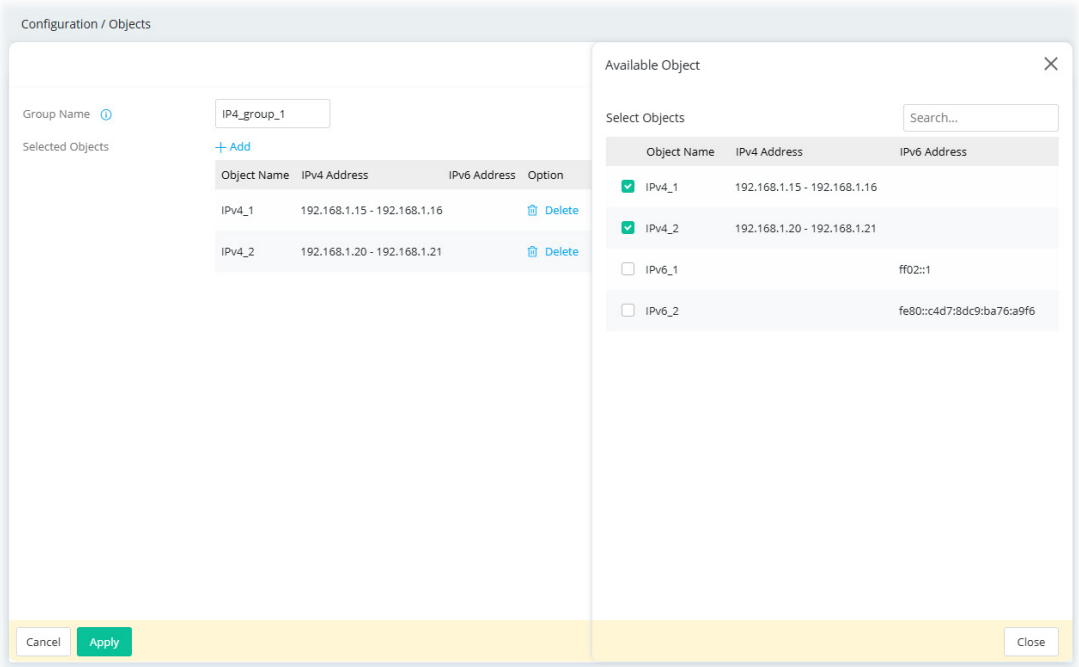
After finishing this web page configuration, please click Apply to save the settings.

II-2-7-2 IP Group

Multiple IP Objects can be placed into an IP Group.



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



Available settings are explained as follows:

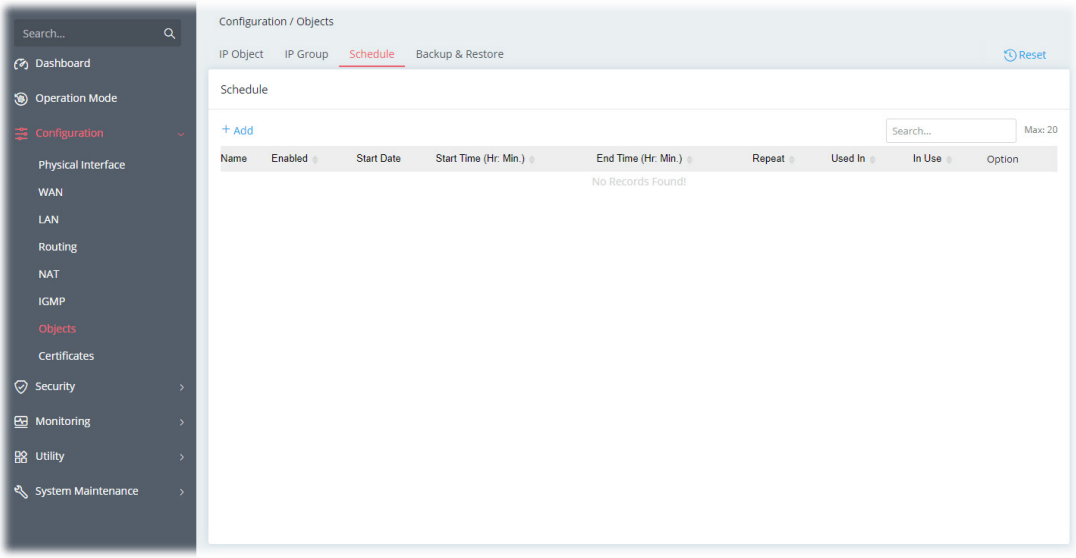
Item	Description
Group Name	Enter a name that identifies this profile.
Selected Objects	+Add - Click to open the page with available objects.
Available Object	
Selected Objects	Search - Enter the IP object name or the IPv4 address to display related information.
Object Name / IPv4	Select the object(s) to be grouped under the current IP group.

Address	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.

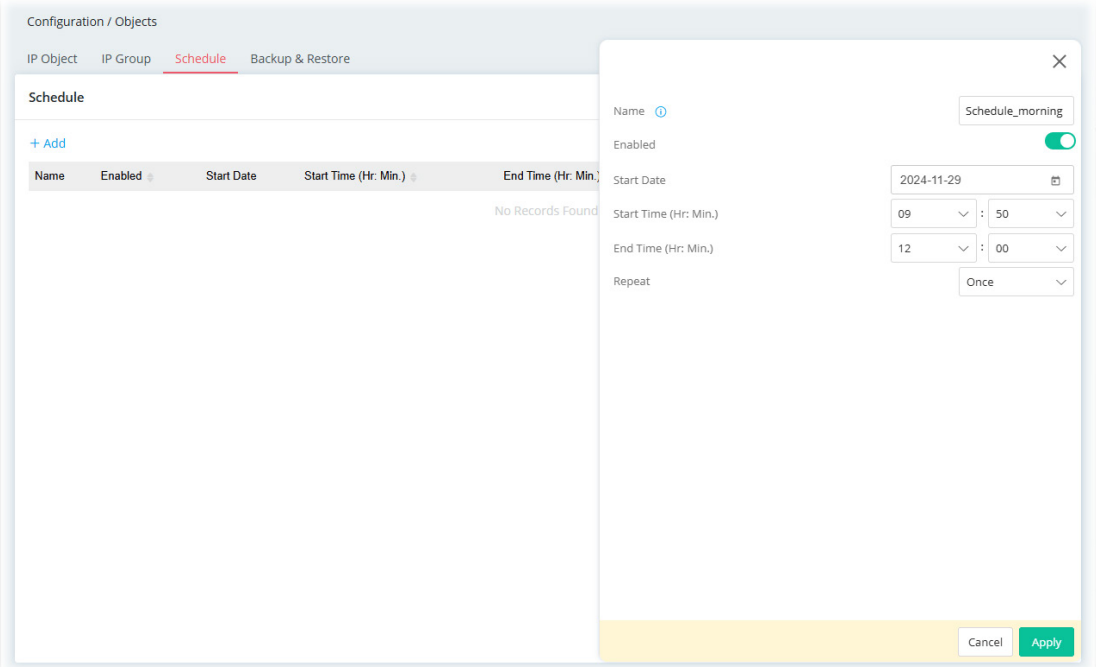
After finishing this web page configuration, please click Apply to save the settings.

II-2-7-3 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.



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

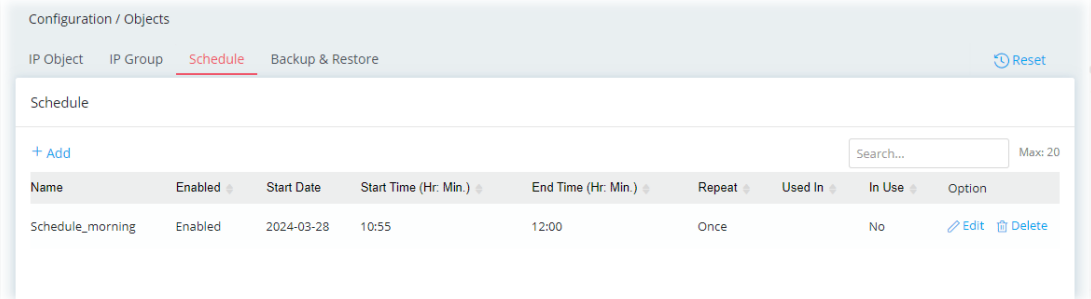


Available settings are explained as follows:

Item	Description
Name	Enter the name of the schedule profile.
Enabled	Switch the toggle to enable or disable this schedule profile.
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.

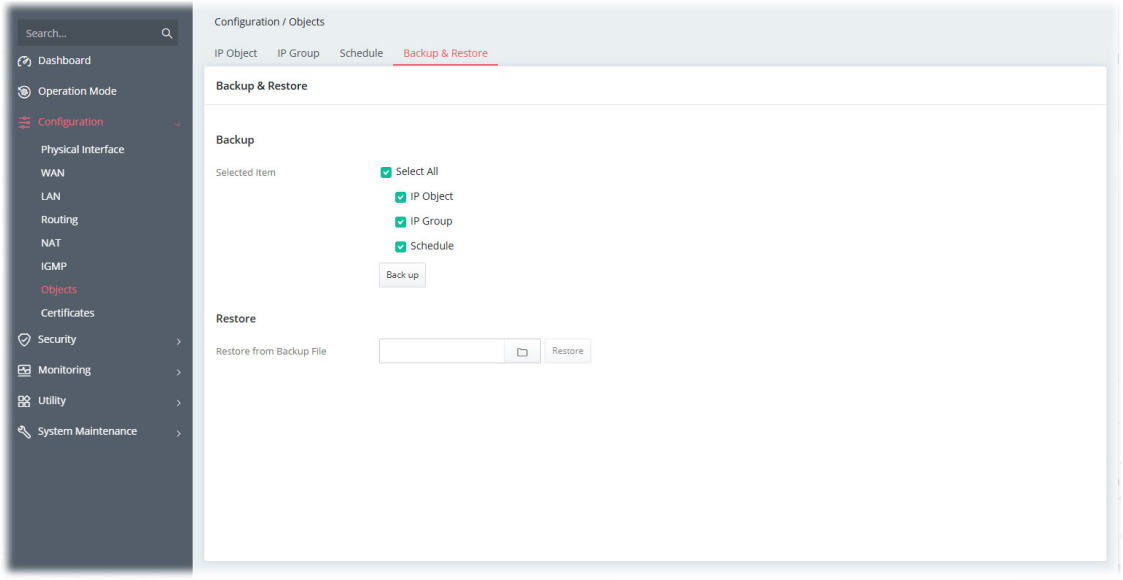
Repeat	Once - The schedule is triggered once based on Date, Start Time and End Time. Daily - The schedule is triggered everyday based on Start Time and End Time. • End Repeat - If enabled, the schedule will be triggered every day till the date defined in the End Repeat Date. • End Repeat Date - The schedule 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. Cycle - Any action applied this schedule will be executed per several days. • Every (days) - Enter a number as cycle duration. Then, any action applied this schedule will be executed per several days. For example, "3" is set as cycle duration. That means, the action applied this schedule will be executed every three days since the date defined on the Start Date. • 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.

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



II-2-7-4 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.



Available settings are explained as follows:

Item	Description
Backup	Usually, a user can create the objects through the web page under Objects. However, for a user who wants to save more time in bulk creating various objects, a method is offered to modify the objects with a single file, a CSV file. All the objects (or the template) can be saved and exported as a file by clicking Download. Then, the user can open the CSV file through Microsoft Excel and modify all the IP objects if required. Back up – Click it to backup current objects as a CSV file. Such file can be restored for future use.
Restore	Restore from Backup File – Click it to specify a predefined CSV file. Restore – Click to execute the restoration.

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

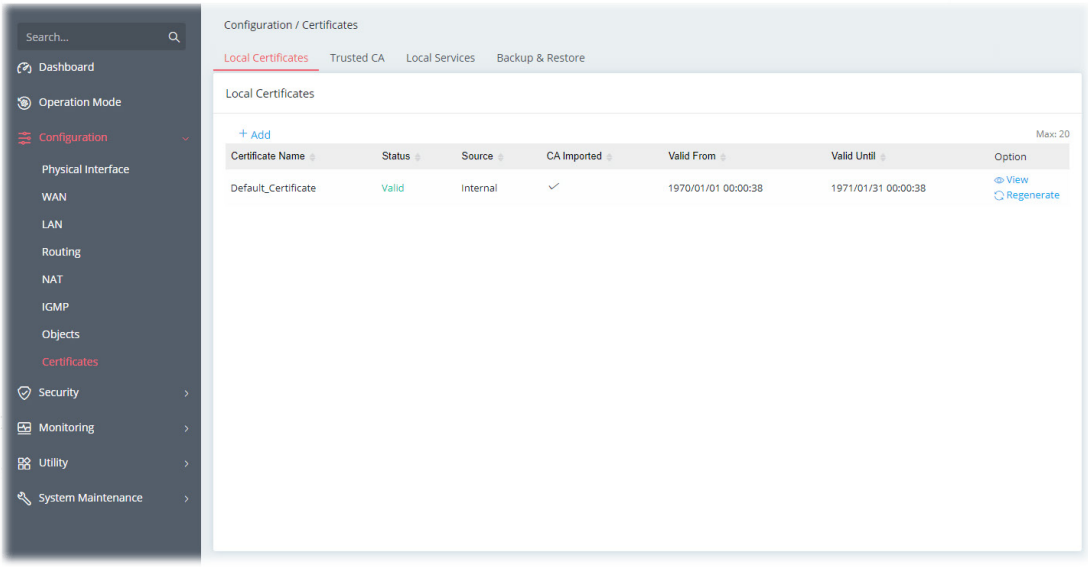
II-2-8 Certificates

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.

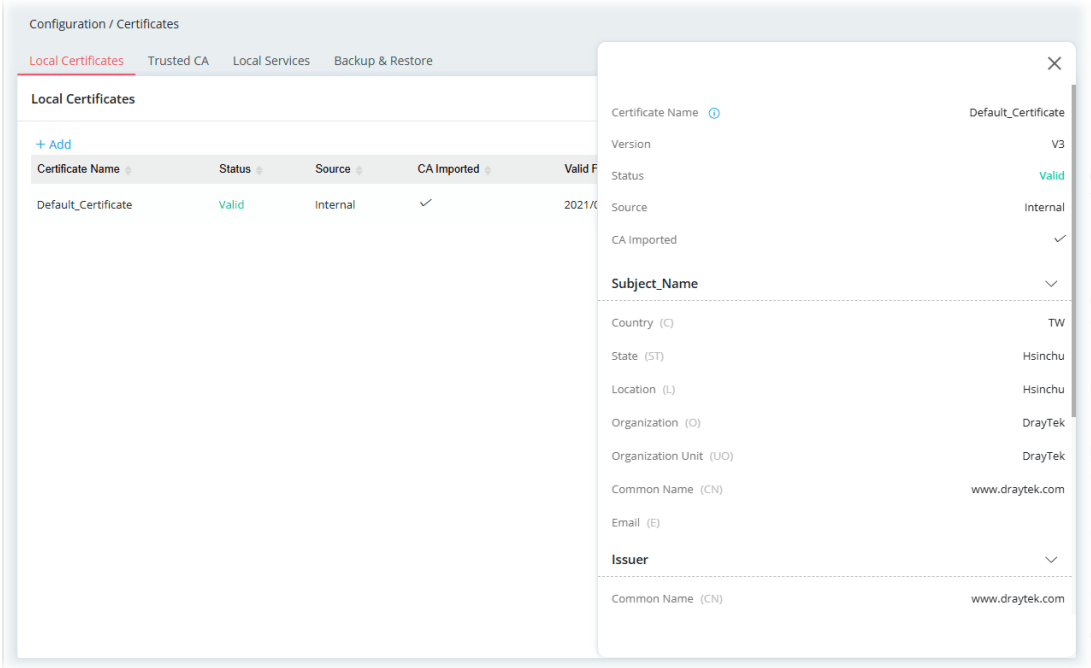
In this section, you can generate and manage local digital certificates, and import trusted CA certificates. Be sure that the system time is correct on the router so that certificates will not be erroneously considered to be invalid because of an incorrect system time falling outside of the certificate's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

II-2-8-1 Local Certificates

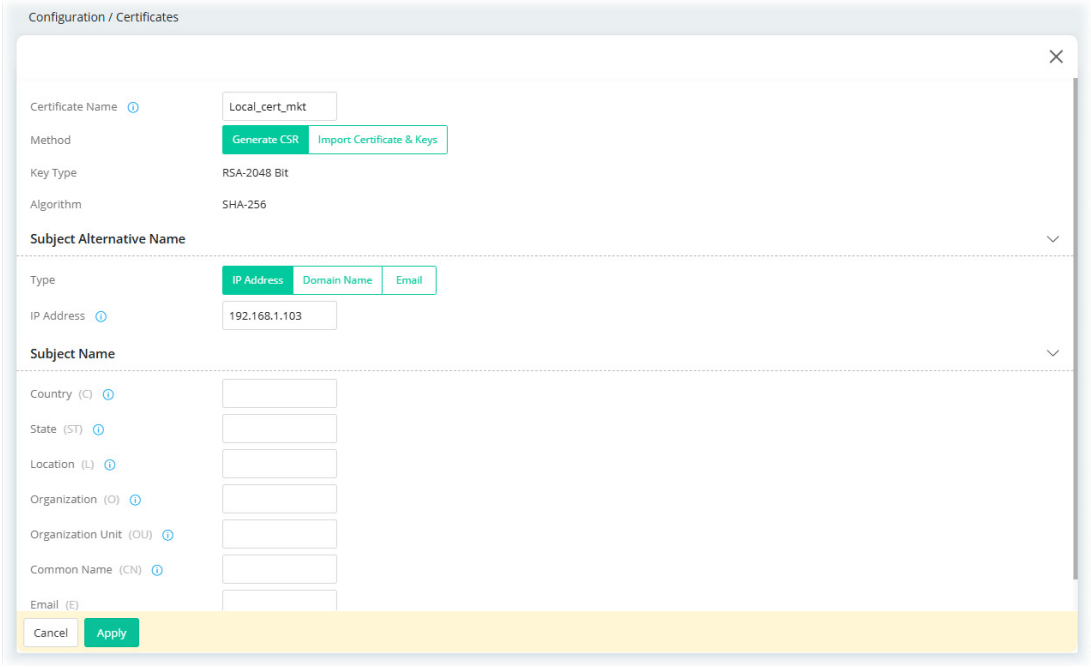
You can generate, import or view local certificates on this page.



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



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



Available settings are explained as follows:

Item	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	

Key Type	Displays the key type used by the certificate.
Algorithm	Displays the algorithm for generating the certificate.
Type	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.

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

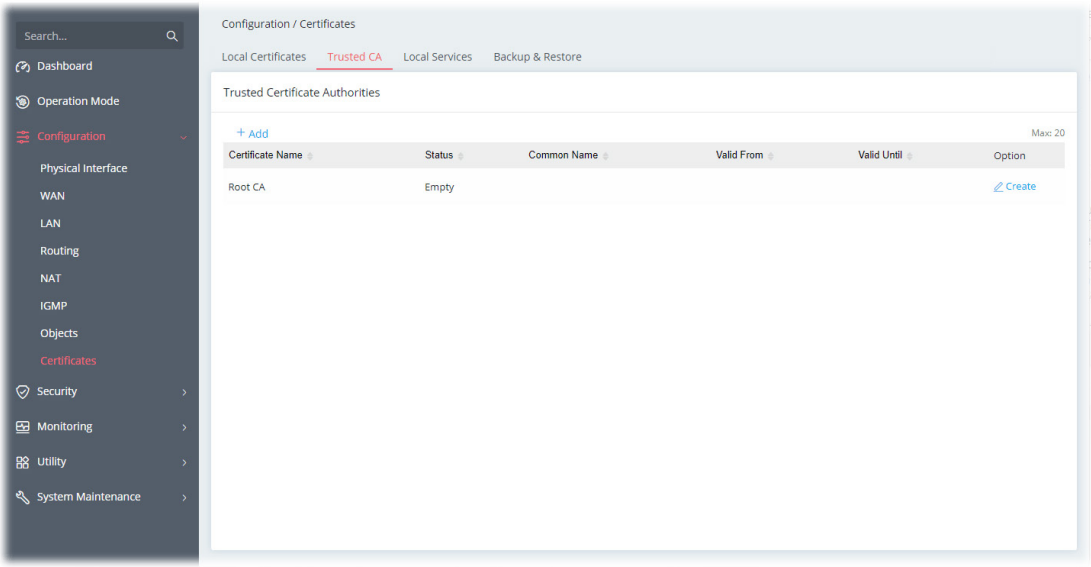
II-2-8-2 Trusted CA

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

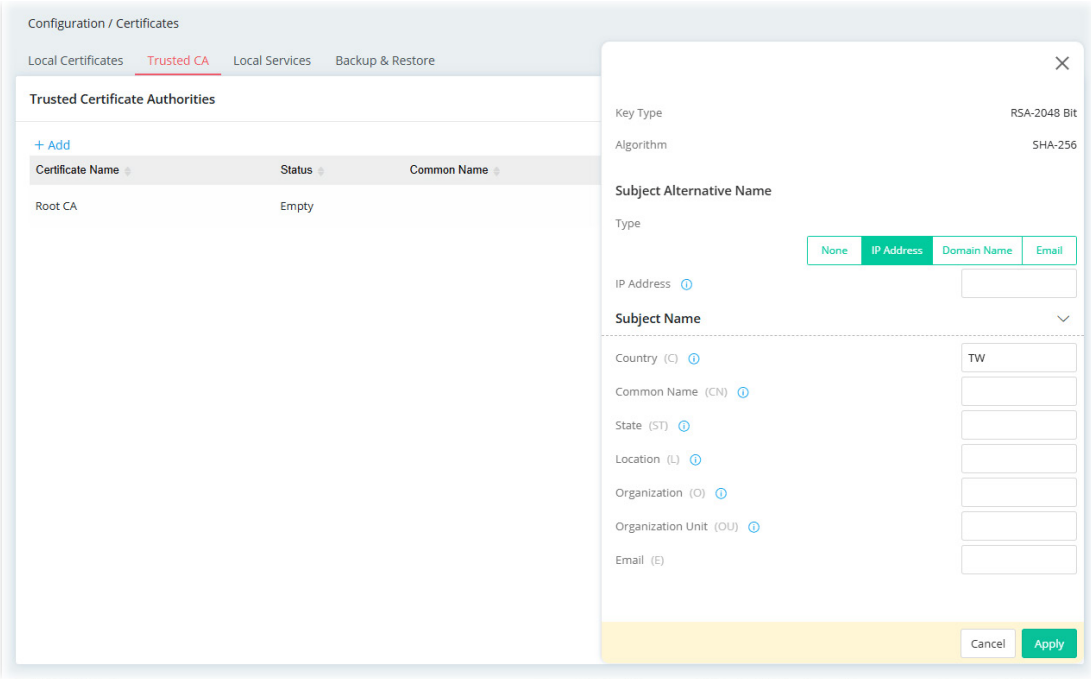
Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

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.



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

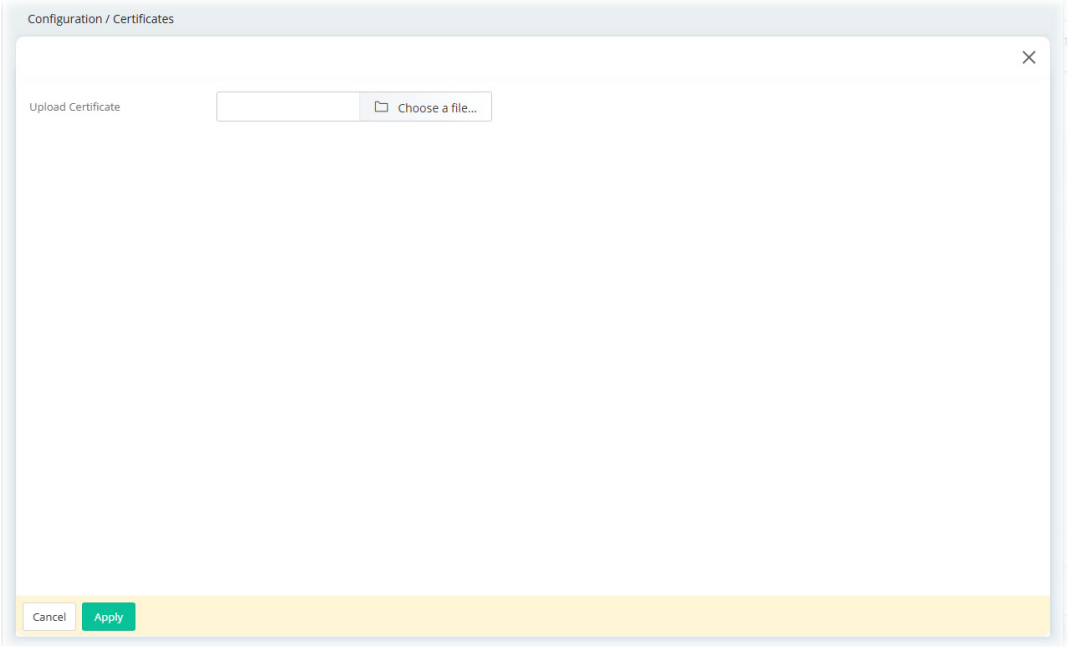


Available settings are explained as follows:

Item	Description
Key Type	Displays the key type (set to RSA).
Algorithm	Displays the algorithm.
Subject Alternative Name	
Type	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.

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

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



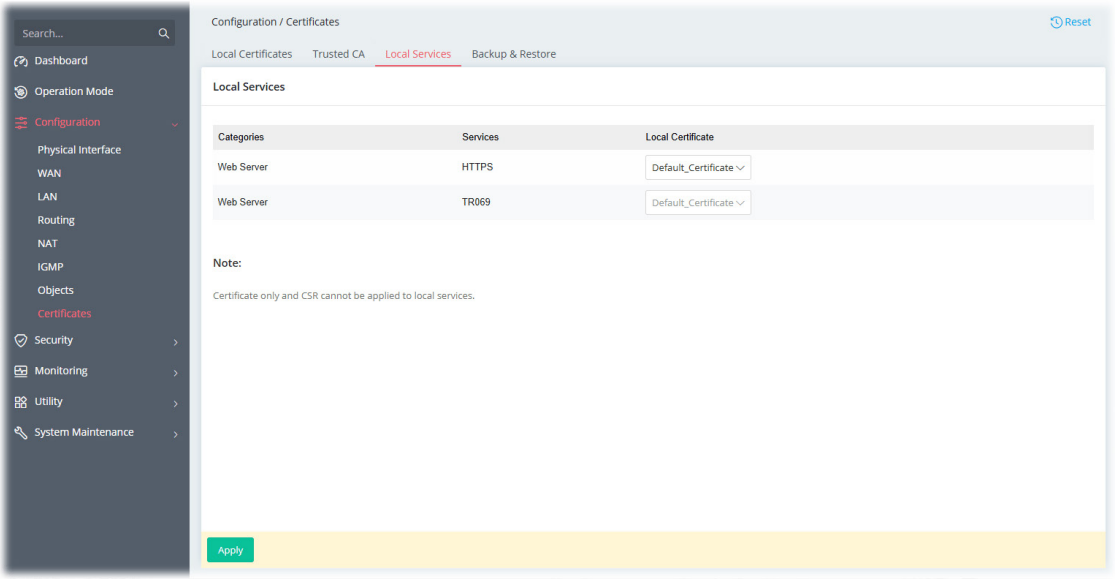
Available settings are explained as follows:

Item	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.

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

II-2-8-3 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.



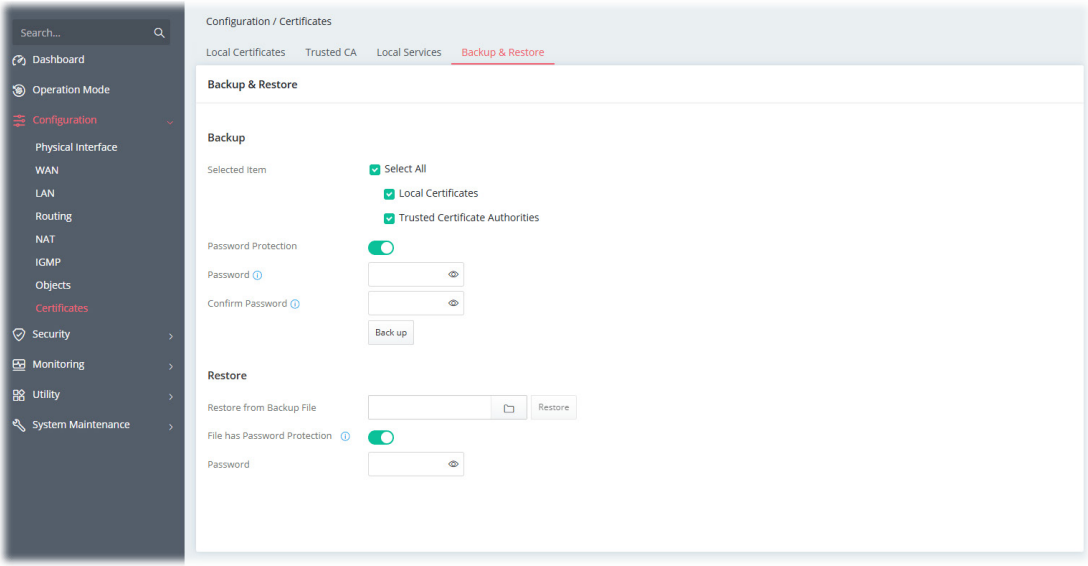
Available settings are explained as follows:

Item	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.
Apply	Save the current settings.

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

II-2-8-4 Backup & Restore

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



Available settings are explained as follows:

Item	Description
Backup	
Selected Item	Select the certification type (local, trusted or all certificate).
Password Protection	Enabled - Switch the toggle to enable or disable the function. ● Password - Enter the password with which you wish to encrypt the certificate. ● Confirm Password - Enter the password again. Backup - Click to download the certificate.
Restore	
Restore from Backup file	Click to select the backup file you wish to restore. Restore - Click to retrieve the certificate.
File has Password Protection	Enabled - Switch the toggle to enable or disable the function. ● Password - Enter the password that was used to encrypt the certificates.

II-3 Security

II-3-1 Firewall Filters

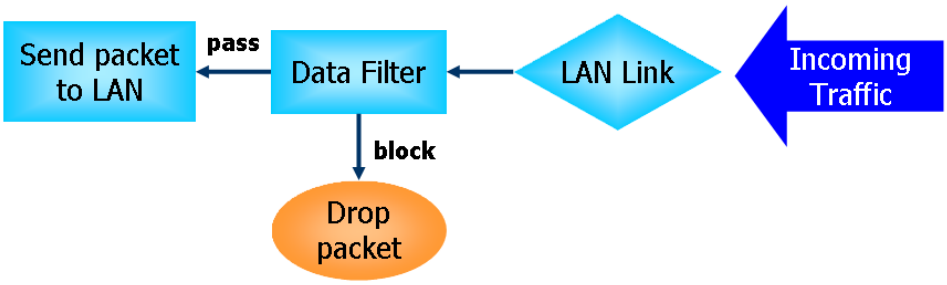
A network firewall monitors traffic travelling between networks, with the ability to selectively allow or block traffic using a predefined set of security rules. This helps to maintain the integrity of networks by stopping unauthorized access and the exchange of sensitive information.

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.

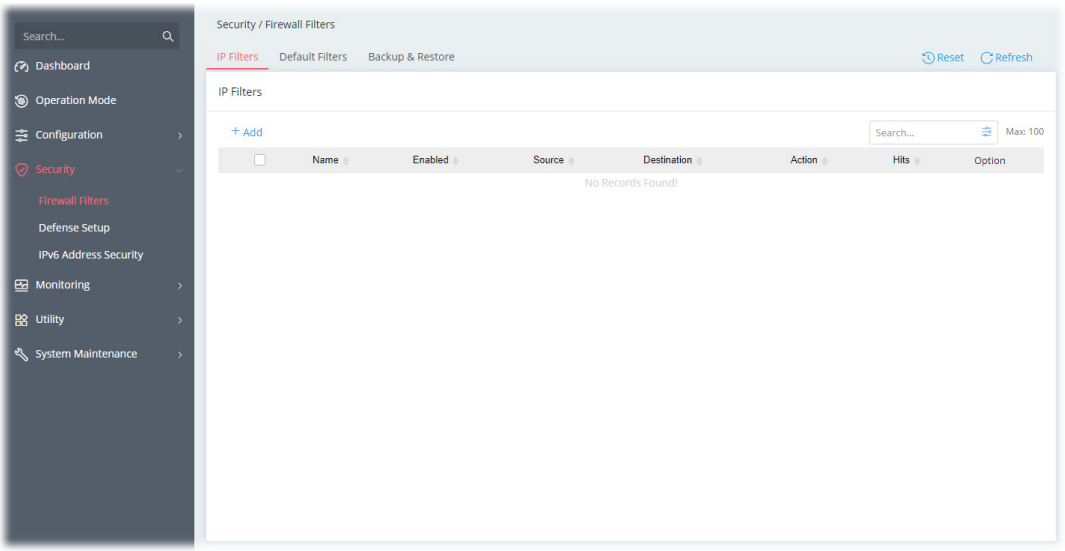
The below shows the attack types that DoS/DDoS defense function can detect:

1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
9. SYN fragment
10. Fraggle attack
11. TCP flag scan

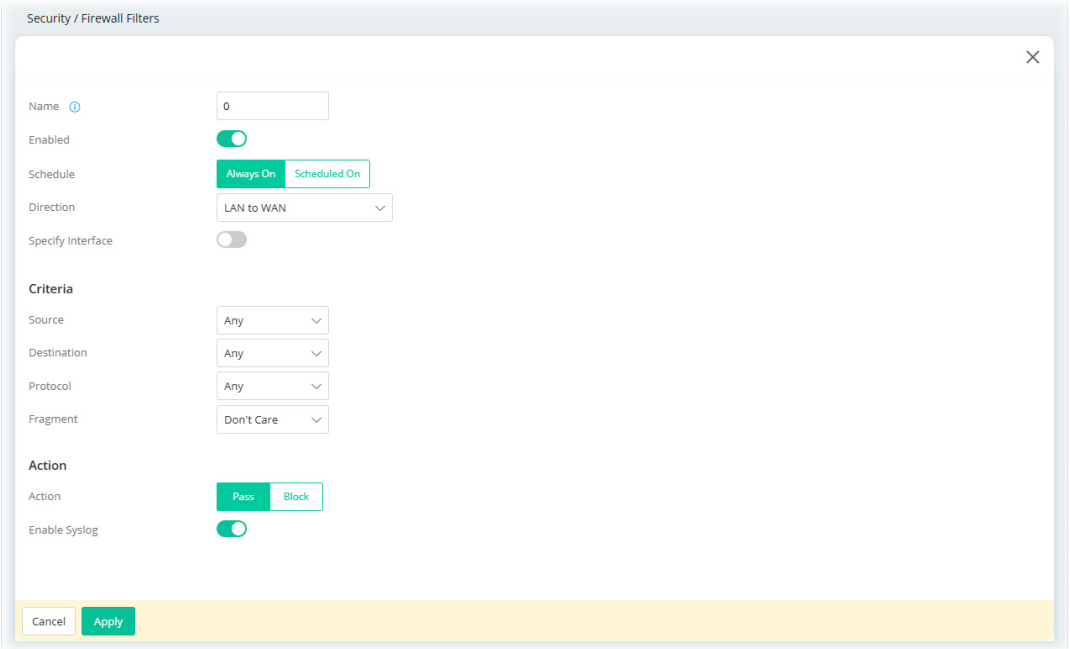
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unassigned Numbers

II-3-1-1 IP Filters

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



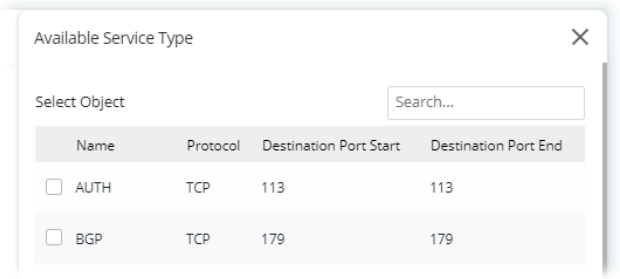
To add a new IP filter profile, click the +Add link to get the following page.



Available settings are explained as follows:

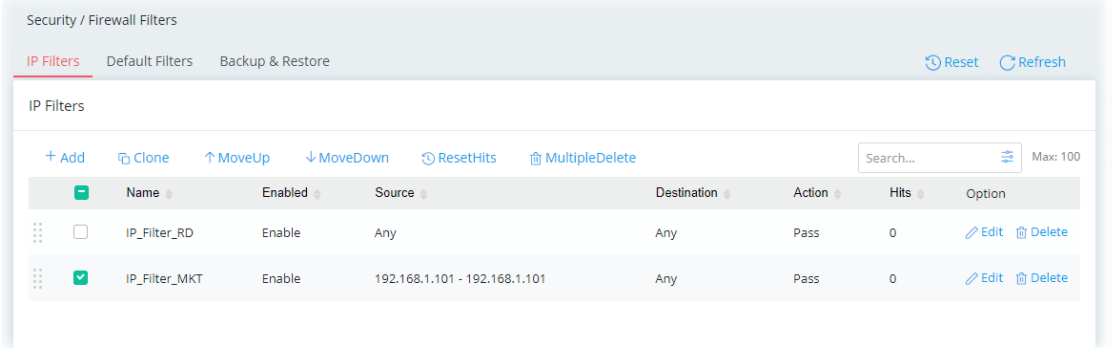
Item	Description
Name	Enter a name to identify the rule.
Enabled	Switch the toggle to enable/disable this profile.

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 to LAN
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 / 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.
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 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.
Protocol	Specify the protocol(s) which this filter rule will apply to. • Any • Service Object • TCP/UDP • TCP • UDP • ICMP • ICMPv6 • IGMP • Others
Service Type Object	It is available when Service Object is set as the Protocol. Click +Add to select the service type objects (up to 12) you want. 
Specify Source Port	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 is set as the Protocol. To define a port range, please provide the starting and ending port values.
Protocol Number	It is available when Others is set as the Protocol. Enter a value as the protocol number.
Fragment	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 contain a complete header.
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 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.

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



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

Available settings are explained as follows:

Item	Description
Clone	Duplicate the selected IP filter profile with a new name.
MoveUp	Move the selected item up.
MoveDown	Move the selected item down.
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.

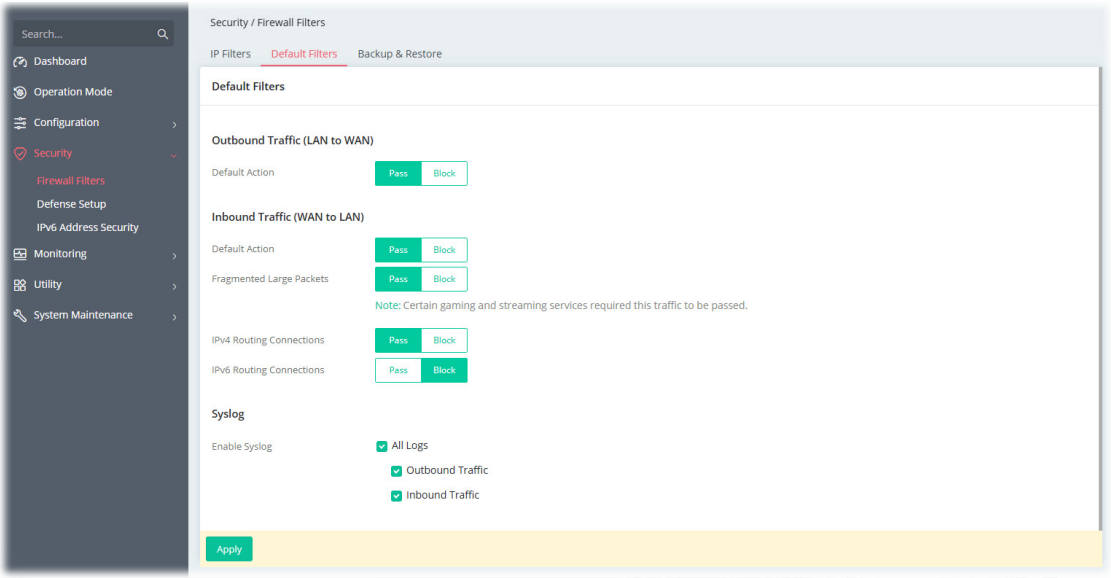
II-3-1-2 Default Filters

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.



Available settings are explained as follows:

Item	Description
	Outbound Traffic (LAN to WAN)
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.
	Inbound Traffic (WAN to LAN)
Default Action	Define the default action for the incoming packets that do not match any IP filter rule. Pass – The incoming packets that do not match any filter rule will be passed. Block – The incoming packets that do not match any filter rule will be blocked.
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, enable 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.

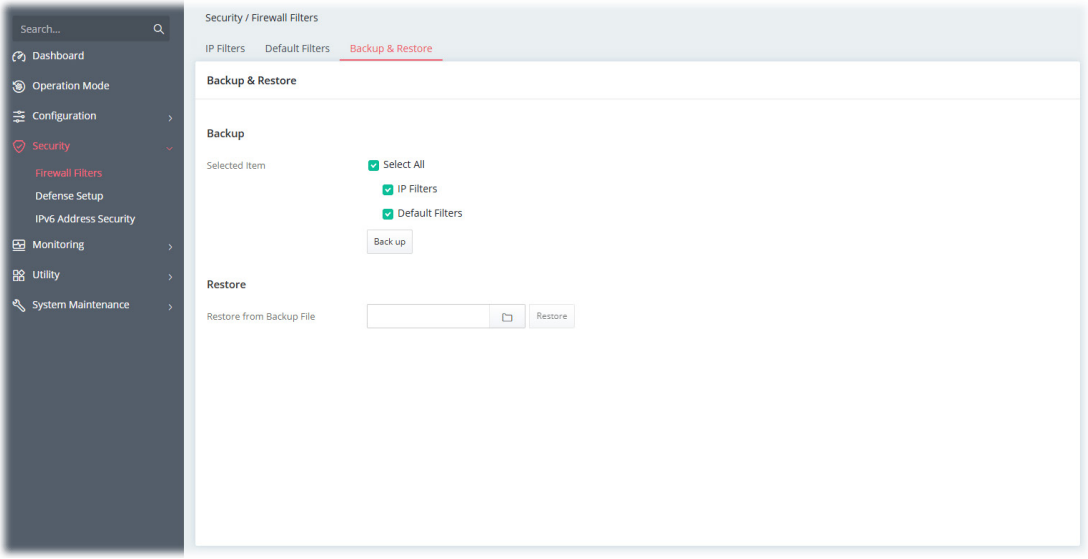
Syslog	Enable Syslog – If enabled, the log related to default filter will be recorded to Syslog.
Apply	Save the current settings.

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

II-3-1-3 Backup & Restore

This page allows the backup and restoration of router settings.

In addition to restoring Vigor router's own configuration backup, it is possible to restore backups from certain DrayTek routers on Vigor167.

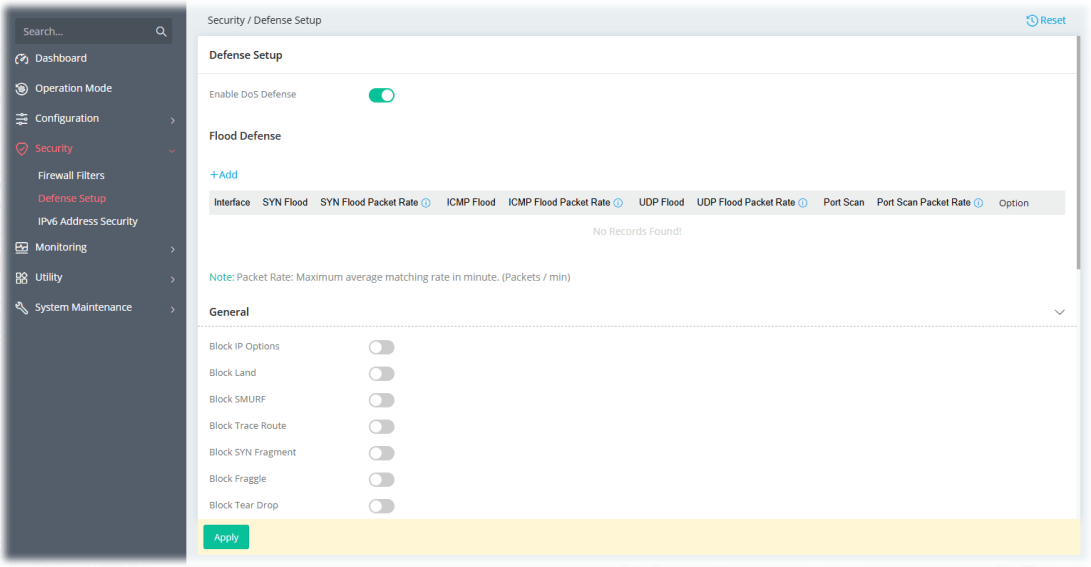


Available settings are explained as follows:

Item	Description
Backup	Selected Items – Select the item(s). Back up - 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.

II-3-2 Defense Setup

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.



Available settings are explained as follows:

Item	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, the 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 Threshold 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, the 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.

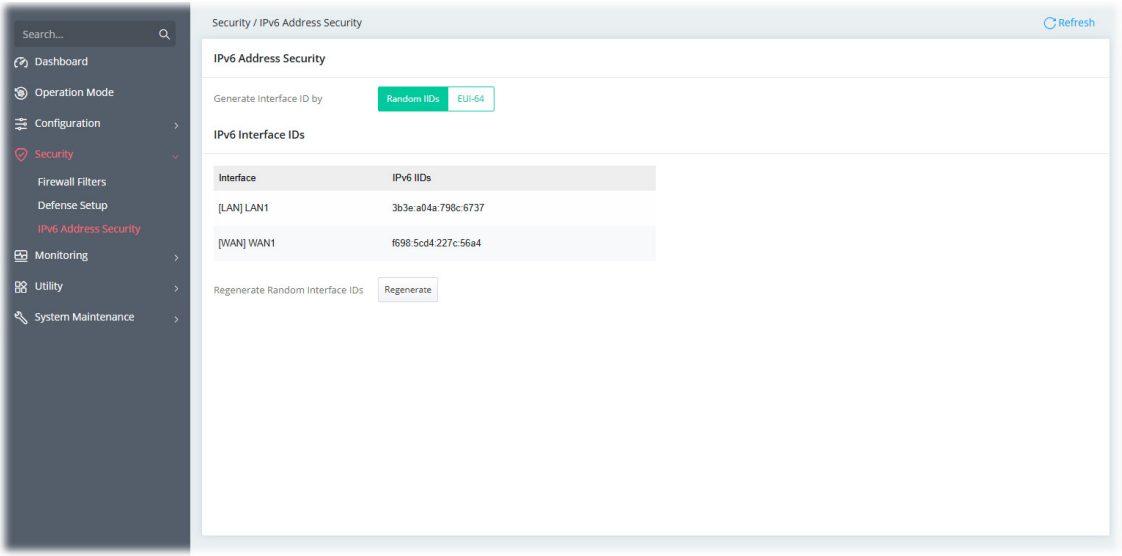
	Port Scan – Switch the toggle to enable/disable the Port Scan detection. Port Scans attack your network by sending packets to a range of ports in an attempt to find services that would respond. When Port Scan detection is enabled, the router sends warning messages when it detects port scanning activities 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.

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

II-3-3 IPv6 Address Security

This page allows you to configure the IPv6 interface ID.

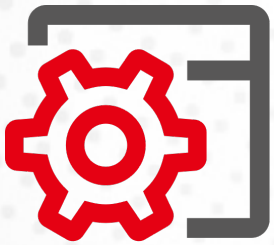


Available settings are explained as follows:

Item	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.
Apply	Save the current settings.

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

Chapter III Management



III-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Device Settings, Management, Firmware, Backup & Restore, Accounts and Reboot System, and Firmware Upgrade.

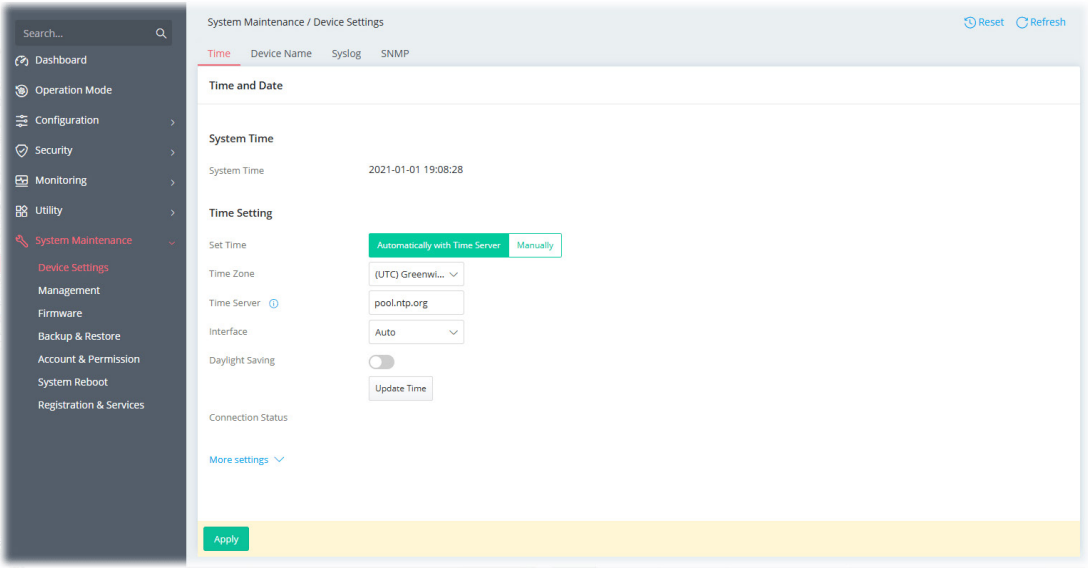
III-1-1 Device Settings

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

III-1-1-1 Time

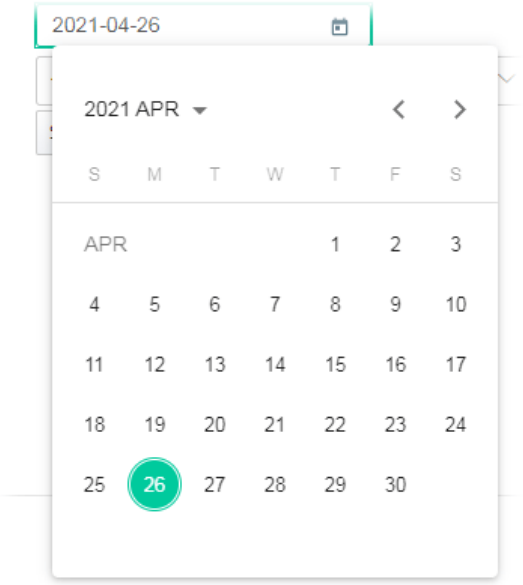
Open System Maintenance>>Device Settings and click the Time tab.

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



Available parameters are explained as follows:

Item	Description
System Time	
Current 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 is selected, the Vigor system will renew the time through WAN or

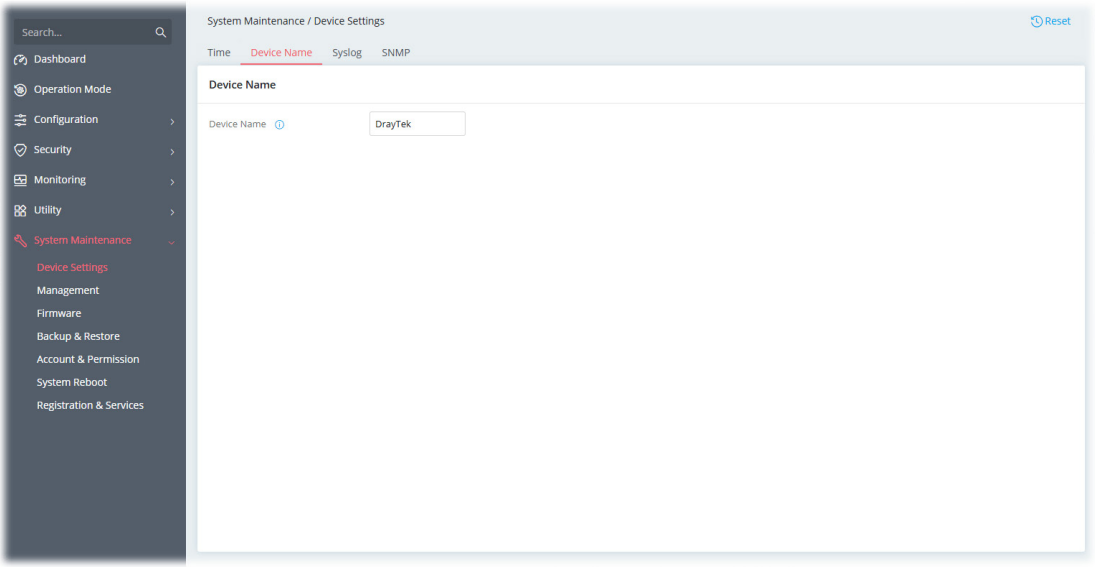
	LAN. Daylight Saving - Enable Daylight Saving Time (DST) if it is applicable to your location. Update Time - Force to renew current time setting. Connection Status - Displays last update time status. More Settings - Click to open advanced settings for the time server. ● Auto Update Interval - Select the time interval (30min or 60min) at which the router updates the system time periodically. ● Secondary Server - For having a backup time server, please enter the URL/IP address in the field of Secondary Server. ● Secondary Interface - Renew the time through the selected WAN/LAN interface. If Auto is selected, the Vigor system will renew the time through WAN or LAN. This is an optional setting and is used as the interface for the backup time server. If the primary time server fails to renew the time setting, the Vigor system will use the secondary time server instead. ● Daylight Saving Period - It is available when Daylight Saving is enabled. Enter a custom schedule to enable the DST - Default, by Week and by Date.
When Manually is selected as Set Time	Time Zone - Select the time zone where the router is located. Date - Use the drop-down calendar to specify correct date.  Time - Set the time by specifying hours, minutes, and seconds. Synchronize with Browse - Click Sync now to sync the time setting with the browser.
Apply	Save the current settings and renew the system time.
Cancel	Discard current settings and return to the previous page.

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

III-1-1-2 Device Name

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

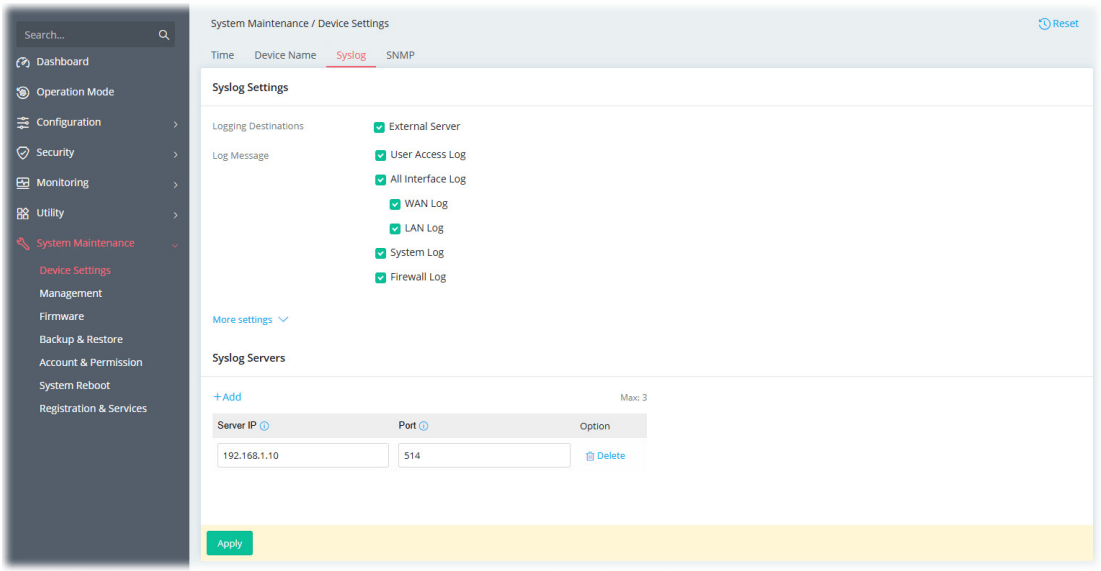
Open System Maintenance>>Device Settings and click the Device Name tab.



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.



Available parameters are explained as follows:

Item	Description
Syslog Settings	
Logging Destinations	Select External Server to display Log Message and Syslog Servers for detailed configuration.
Log Message	Select to send the corresponding message of user access, interface, and system information to Syslog.

Syslog Servers	
+Add	Click to display new entry boxes for creating a new Syslog server profile. The maximum number of Syslog servers to be added is "3".
Server IP	Enter the IP address of the Syslog Server.
Port	Enter the port number of the Syslog Server.
Option	Delete - Click it to remove the selected server profile.
Apply	Save the current settings and exit the page.
Cancel	Discard current settings and return to the previous page.

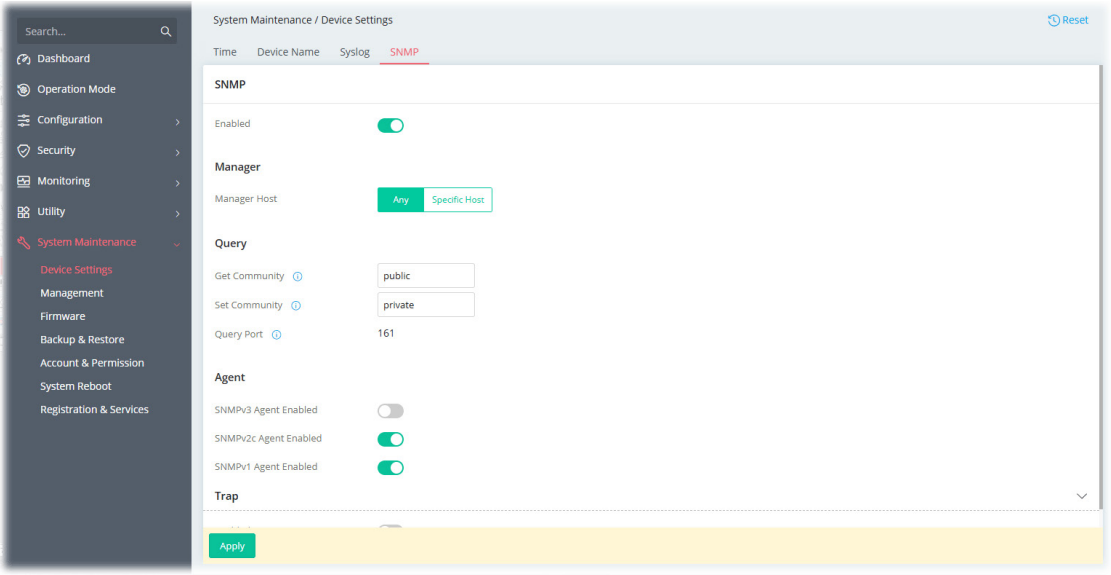
After finishing this web page configuration, please click Apply to save the settings.

III-1-1-4 SNMP

This section allows you to configure settings for SNMP services.

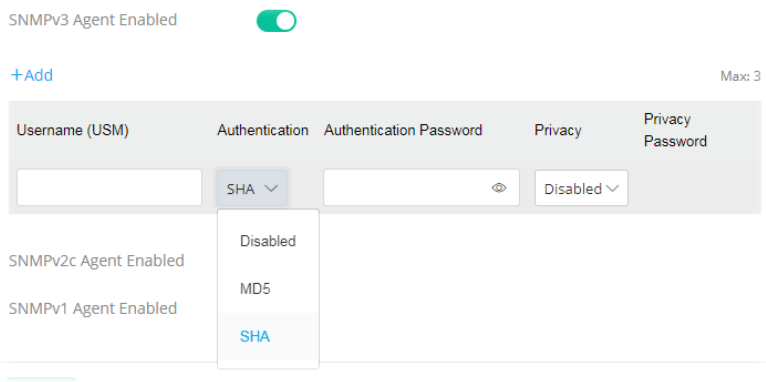
The SNMPv3 is more secure than SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.

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



Available parameters are explained as follows:

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

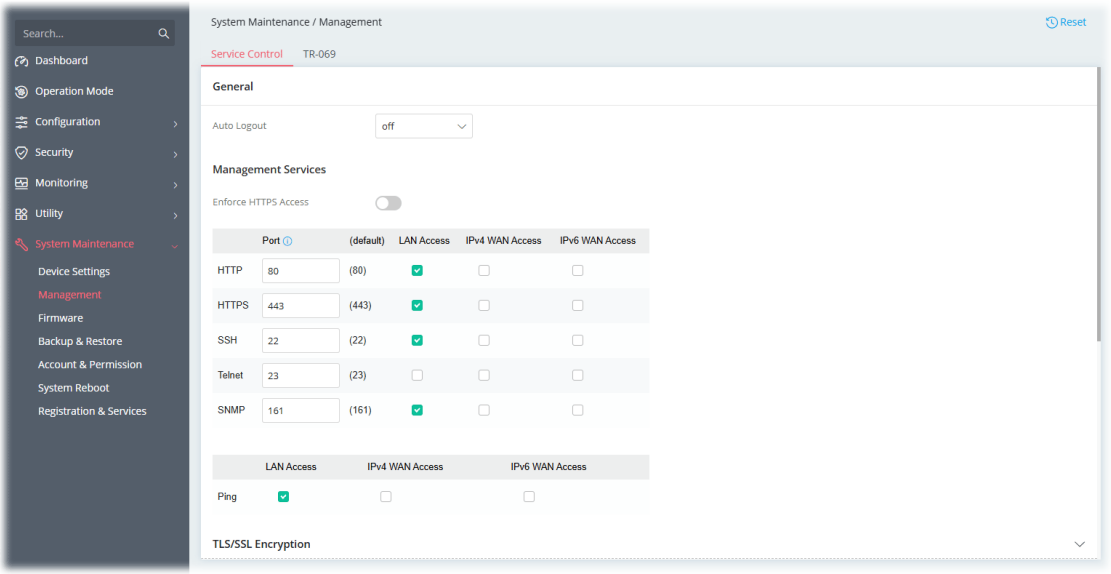
	selected as the IP Type. Click +Add to have a new entry. Enter the IPv4 address with subnet mask / IPv6 address with specified prefix length of hosts that are allowed to issue SNMP commands. If these fields are left blank, any IPv4/IPv6 LAN host is allowed to issue SNMP commands.
Query	
Get Community	Enter the Get Community string. The default setting is public. Devices that send requests to retrieve information using get commands must pass the correct Get 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 Agent Enabled	Switch the toggle to enable/disable the SNMPv3 function. If enabled, specify corresponding settings. Click +Add to have a new entry.  Username(USM) - USM means user-based security mode. Enter the username to be used for authentication. Authentication - Select one of the hashing methods to be used with the authentication algorithm. Authentication Password - Enter a password for authentication. Privacy - Select an encryption method as the privacy algorithm. Privacy Password - Enter a password for privacy.
SNMPv2c Agent Enabled	Switch the toggle to enable/disable the SNMPv2 function.
SNMPv1 Agent Enabled	Switch the toggle to enable/disable the SNMPv1 function.
Trap	
Enabled	Switch the toggle to enable/disable the Trap function.
Trap Version	Select the trap version. • V1 • V2c • V3
Trap Community	Enter the Trap Community string. The default setting is public. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string. The maximum length of the text is 23 characters.

Trap Port	Enter the port number used for the Trap server.
Notification Host IP Type	Select the type of the notification host. ● Both ● IPv4 ● IPv6
Notification Host(IPv4)	+Add - Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
Notification Host(IPv6)	+Add - Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
Trap Events	Select the event(s) to apply the settings configured in this page.
Apply	Save the current settings and exit the page.

III-1-2 Management

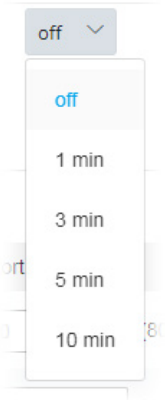
III-1-2-1 Service Control

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



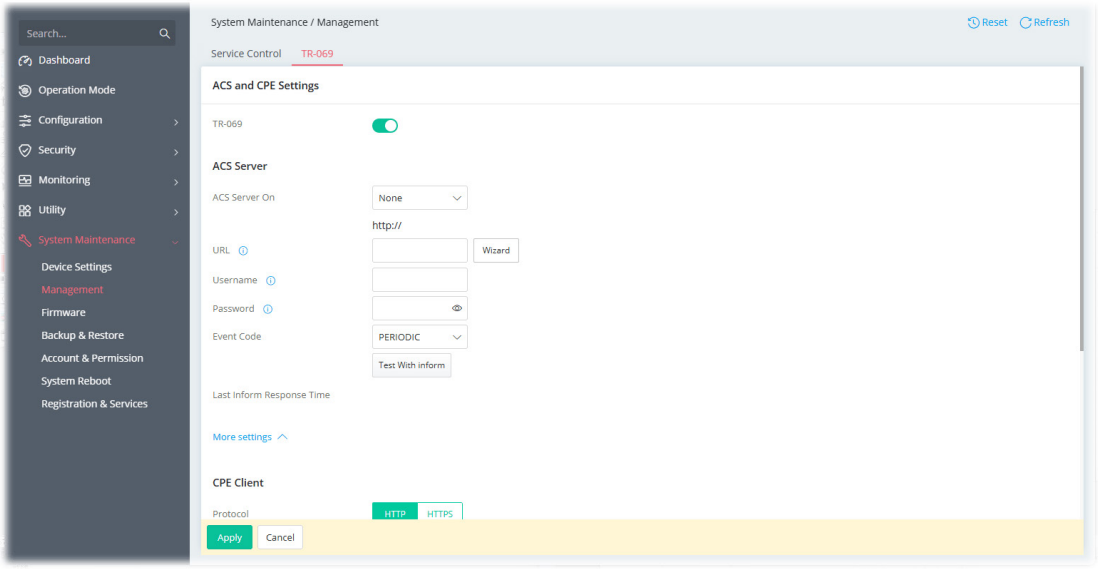
Available settings are explained as follows:

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.

	
Management Services	
Enforce HTTPS Access	Enable the checkbox to allow system administrators to login Vigor router via HTTPS.
Allow PING from LAN	Allow all PING packets from LAN.
Allow PING from Internet	Allow all PING packets from the Internet. For increased security, this setting is disabled by default.
Port	Specify user-defined port numbers for the HTTP, HTTPS,SSH and Telnet servers.
LAN Access	Select the checkbox to allow system administrators to login from LAN interface.
IPv4 WAN Access	Select the checkbox to allow system administrators to login from IPv4 WAN interface.
TLS/SSL Encryption	
TLS 1.3/TLS 1.2/ TLS 1.1/TLS 1.0/SSL 3.0	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.
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.



Available settings are explained as follows:

Item	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.
URL	Enter the URL for connecting to the ACS. Wizard - Click it to enter the IP address of VigorACS server, port number and the handler.
Username/Password	Enter the credentials required to connect to the ACS server.
Event Code	Use the drop down menu to specify an event to perform the test. Test With Inform - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS server.
Last Inform Response Time	Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
More settings	
CPE Client	This section specifies the settings of the CPE Client. Protocol - Select Https if the connection is encrypted; otherwise 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

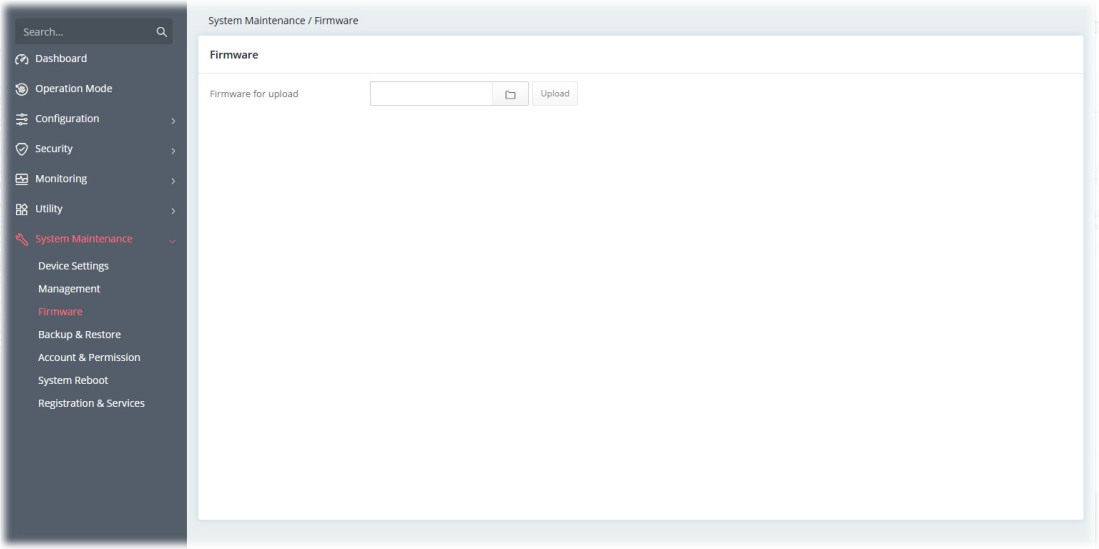
	parameters at intervals specified in the Interval Time field. Time Interval - Set interval time or schedule time for the router to send notification to CPE.
STUN Settings	Enable / Disable - Switch the toggle to enable or disable the function. The default is Disable. If select Enable, please enter the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

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

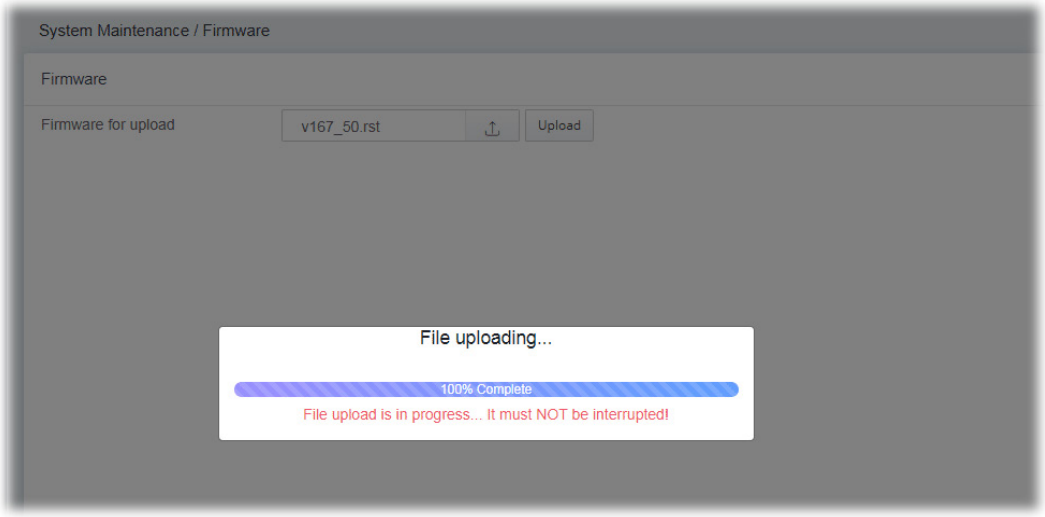
III-1-3 Firmware

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

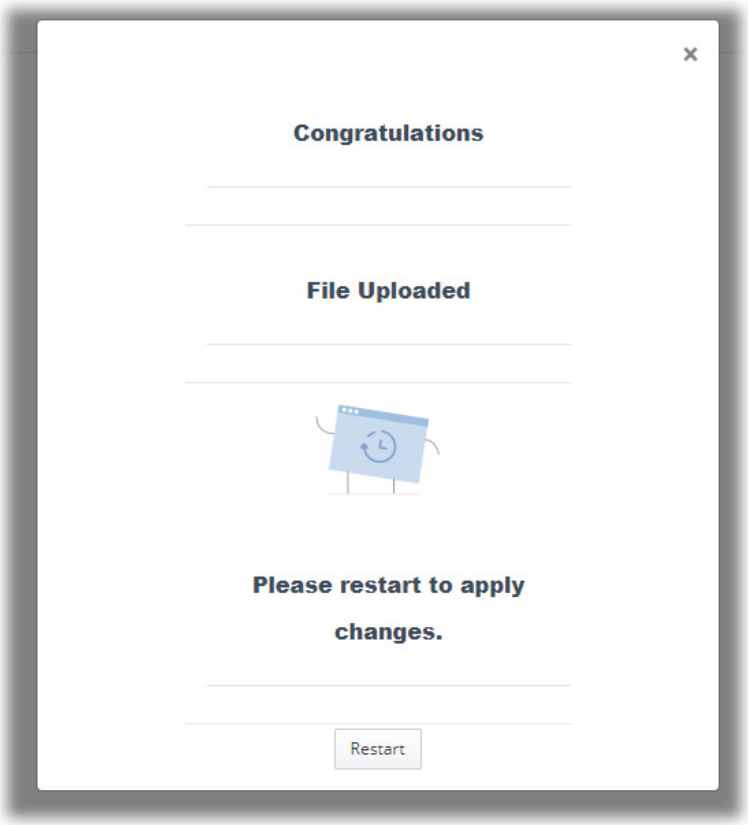
Open System Maintenance>>Firmware. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).



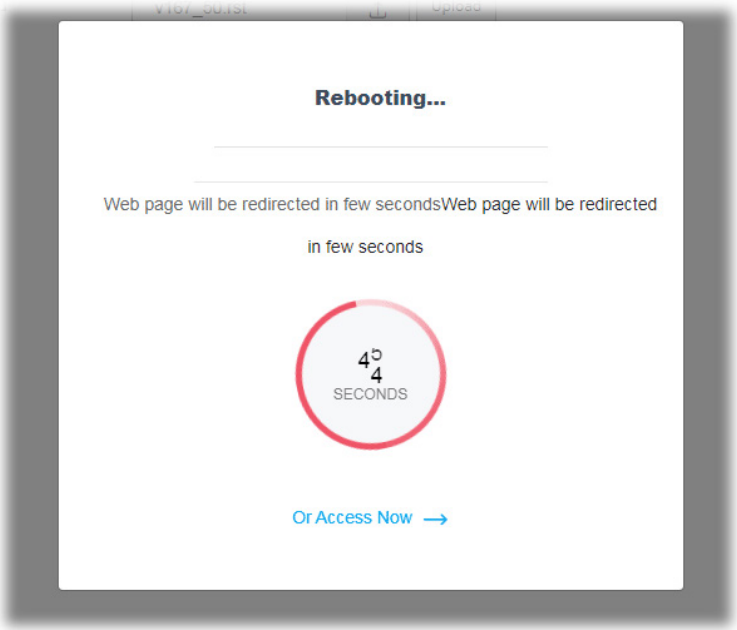
Then click Upload and wait for a few seconds.



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

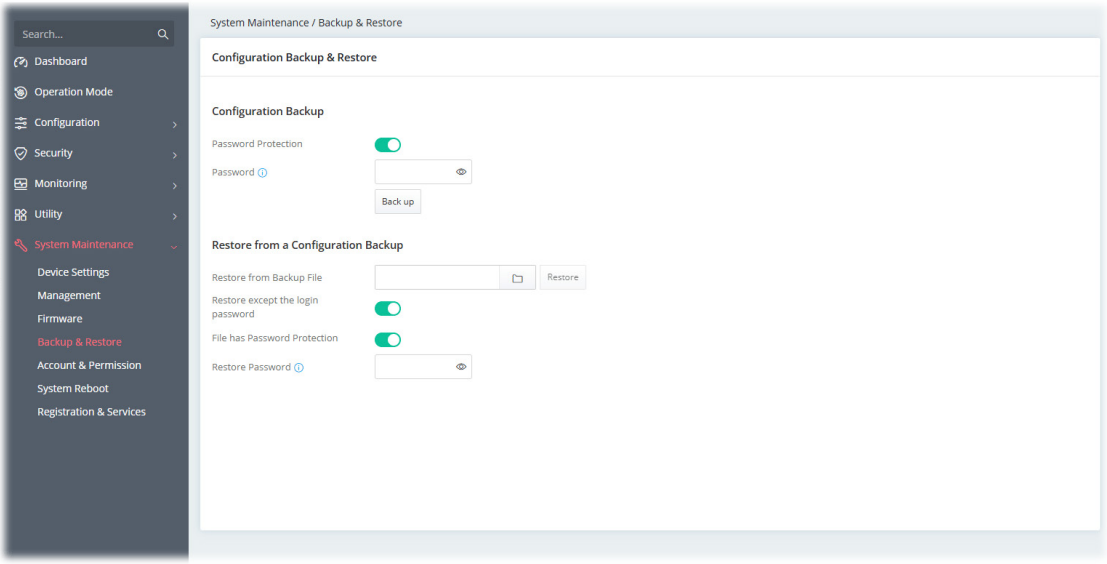


Wait for a while until the system finishes the rebooting.



III-1-4 Backup and Restore

This function can be used to backup/restore the Vigor167 settings.



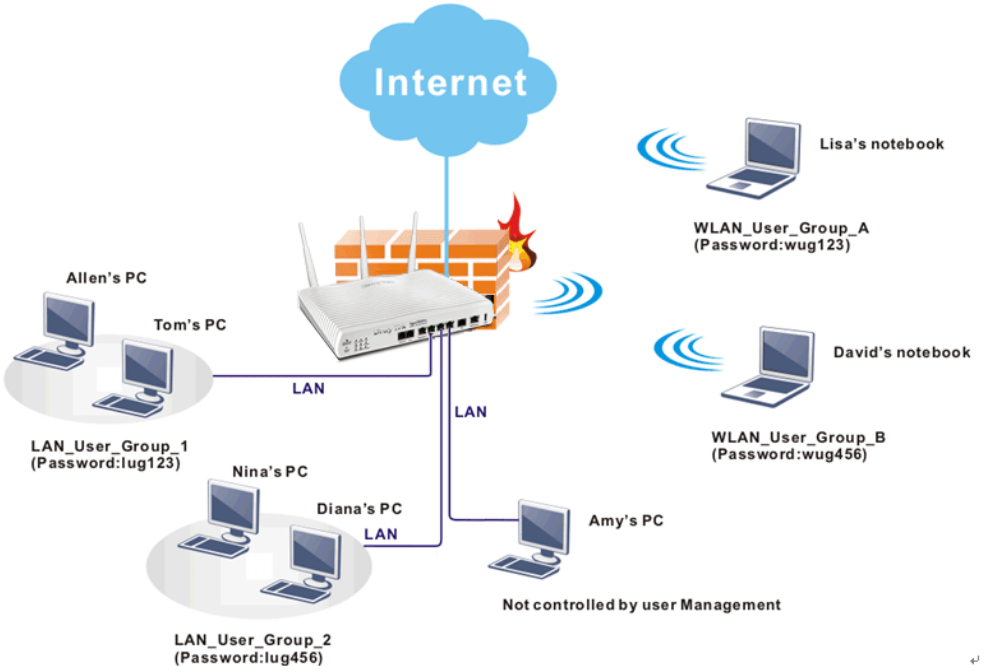
Available settings are explained as follows:

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

III-1-5 Accounts & Permission

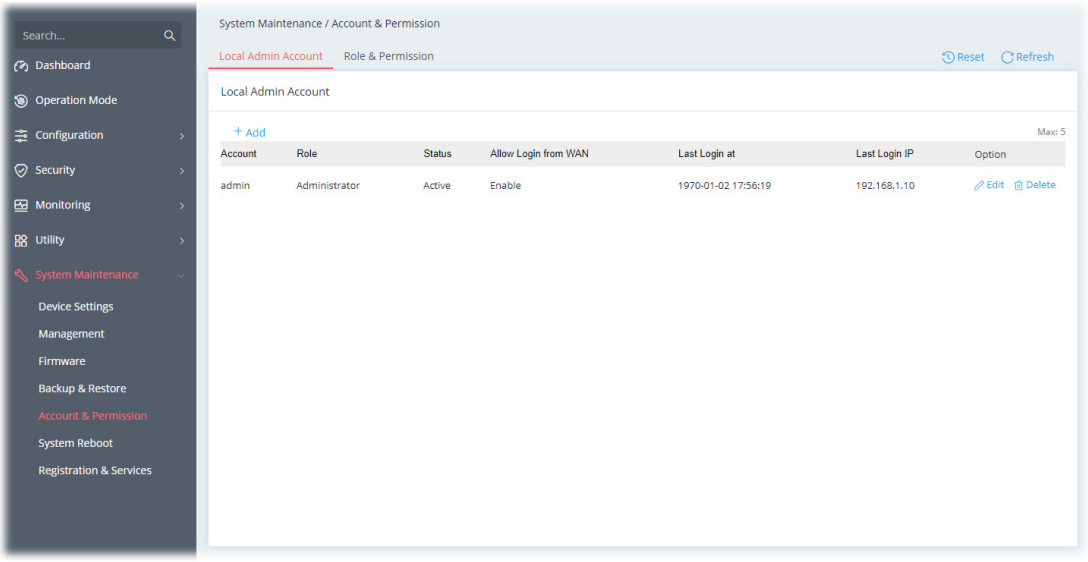
This page allows you to modify current administration account and password.

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.

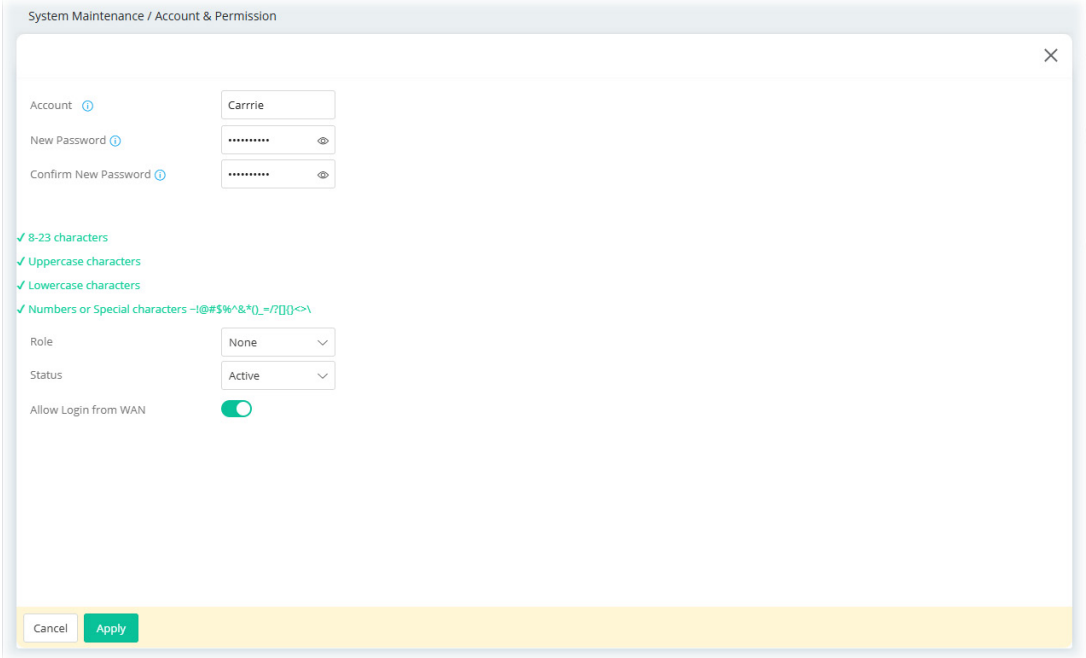


Available settings are explained as follows:

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

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

To add a new profile, click +Add.



Available settings are explained as follows:

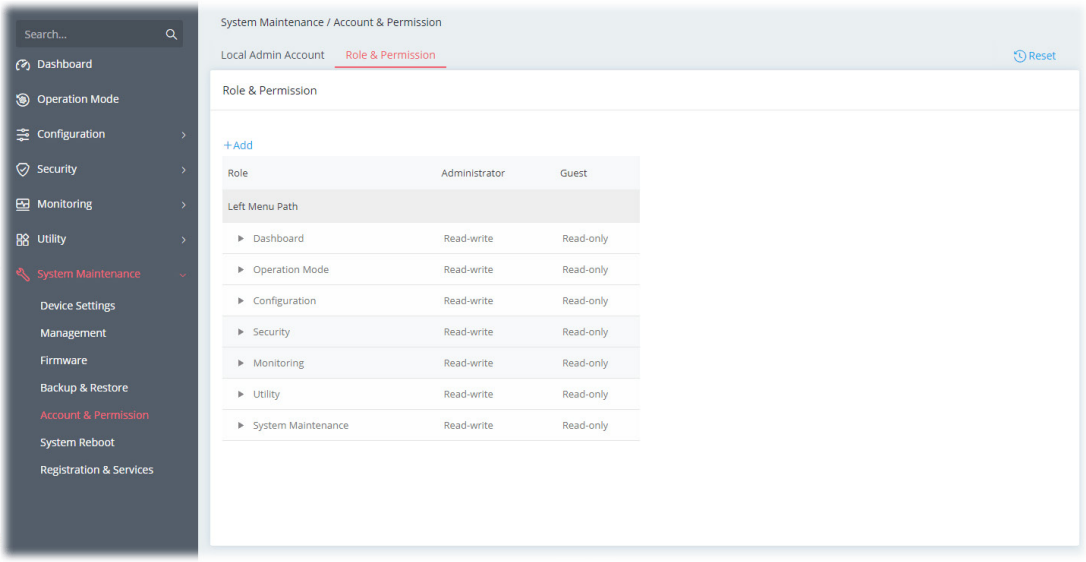
Item	Description
Account	Display the name of the account.
New Password	Enter a new password in this field.
Confirm New Password	Enter the new password again.
Role	Specify the role of the account. • Administrator • Guest
Status	Active - Enable the selected account profile. Inactive - Disable the selected account profile.
Allow Login from WAN	If enabled, the user can login from WAN by using this 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.

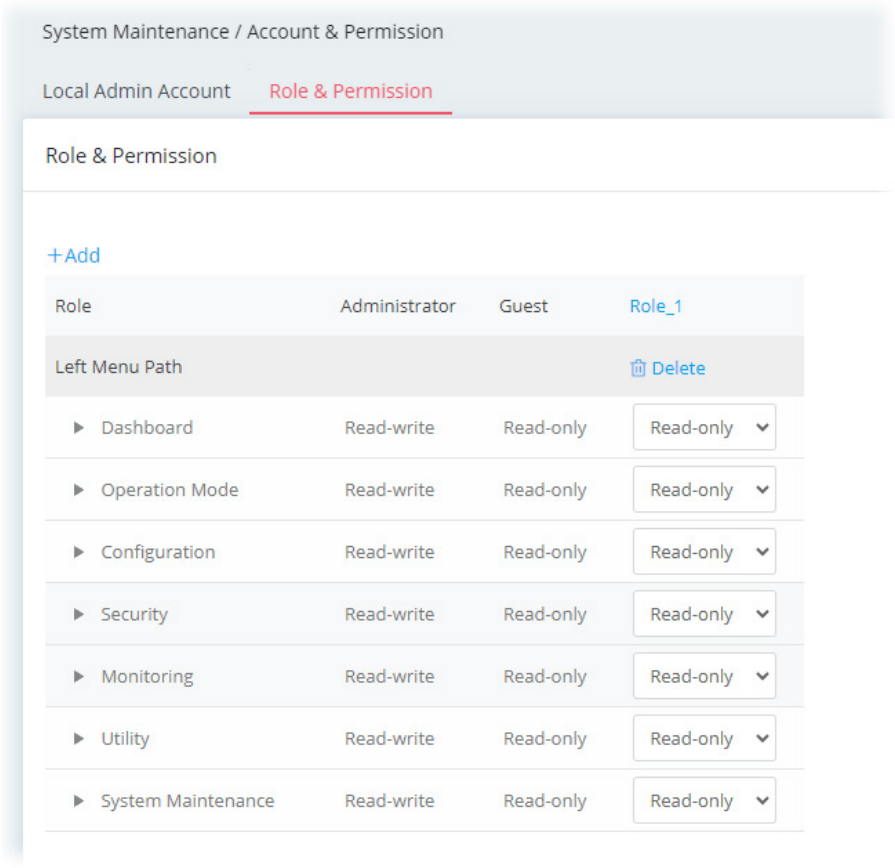
III-1-5-2 Role & Permission

This page allows the creation of up to five roles which can be applied to the local admin account.

The default roles are Administrator and Guest.

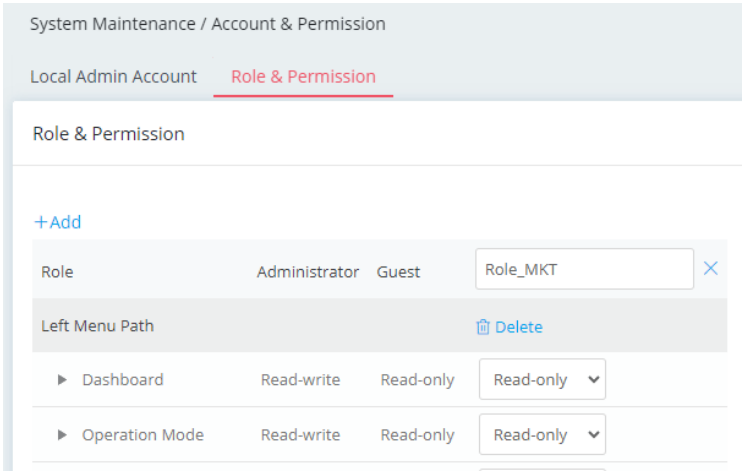
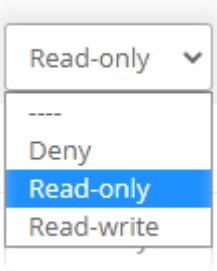


To create a new role profile, click +Add. A new role will be added on to the page.

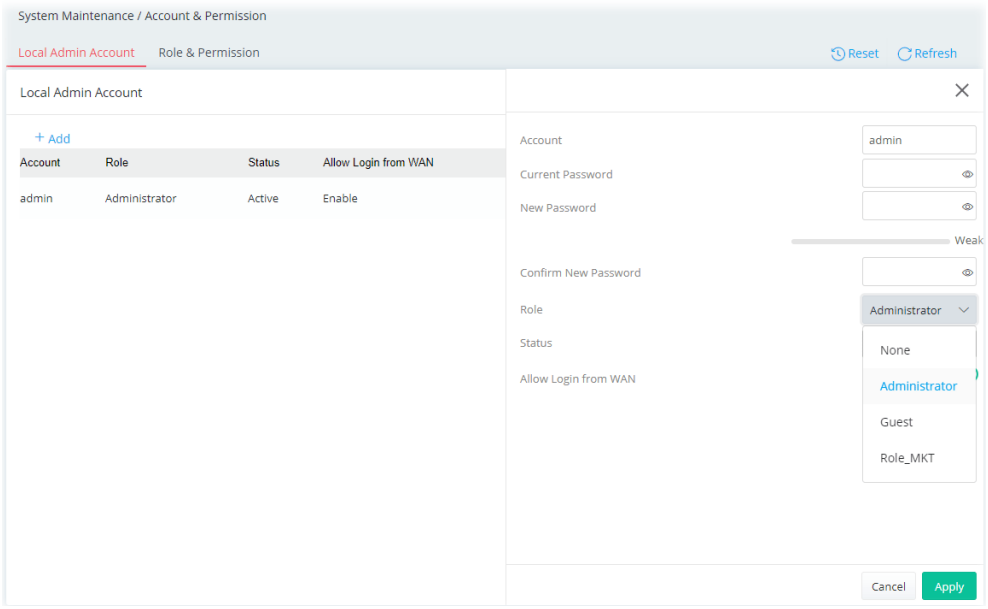


Available settings are explained as follows:

Item	Description
+Add	Create a new role profile.

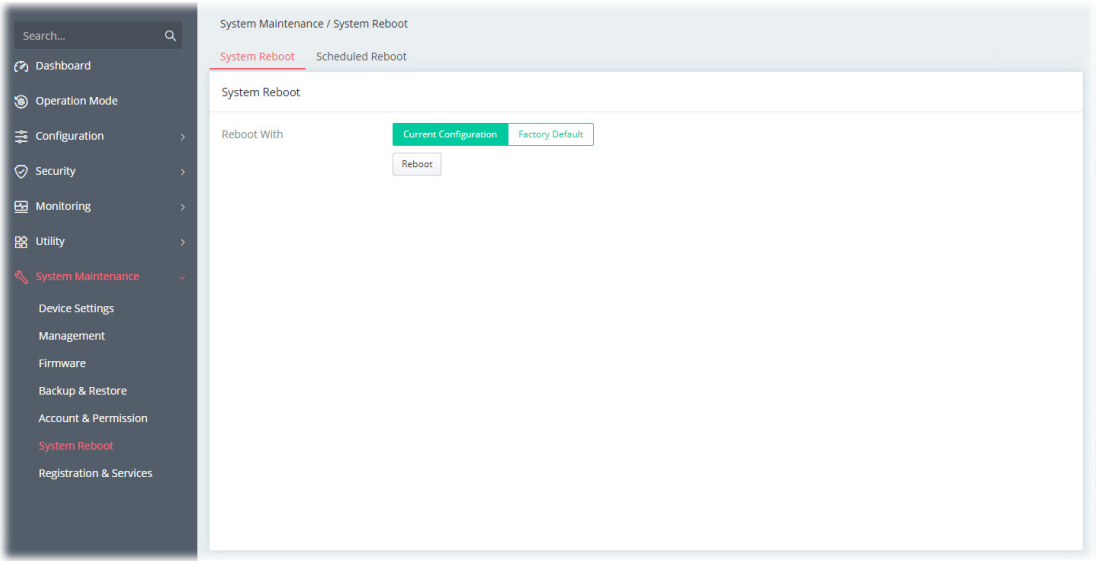
Role_1	The field of profile name. New added profile will be named as Role_#. To modify the name, simply click the name and enter a new string (e.g., Role_MKT). 
Left Menu Path	Lists all of the features that a role can have. The role of Administrator has the highest authority for accessing Vigor router. The role of Guest has the lowest authority for accessing Vigor router. 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	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 allowed for the user-defined role profile to be read-only. Read-write - The permission for the menu item on the left side allowed for the user-defined role profile to be both read-only and written.
Apply	Save the current settings and exit the page.

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


System Maintenance / Account & Permission
Local Admin Account
Role & Permission
Reset
Refresh
Local Admin Account
+ Add
Account
Role
Status
Allow Login from WAN
admin
Administrator
Active
Enable
Account
admin
Current Password
New Password
Weak
Confirm New Password
Role
Administrator
Status
Allow Login from WAN
None
Administrator
Guest
Role_MKT
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.



Available settings are explained as follows:

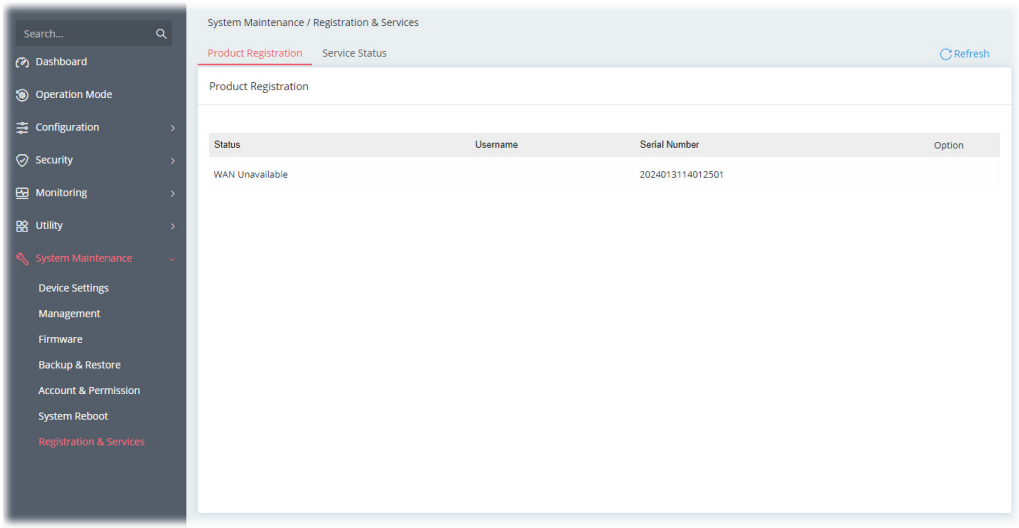
Item	Description
Reboot With	Select one of the following options, and press the Reboot button to reboot the router. Current Configuration – Select this option to reboot the router using the current configuration. Factory Default – Select this option to reset the router's configuration to the factory defaults before rebooting.

III-1-7 Registration & Services

Register your Vigor router to MyVigor website for getting more services.

III-1-7-1 Registration & Services

1. Open System Maintenance >> Registration & Service.



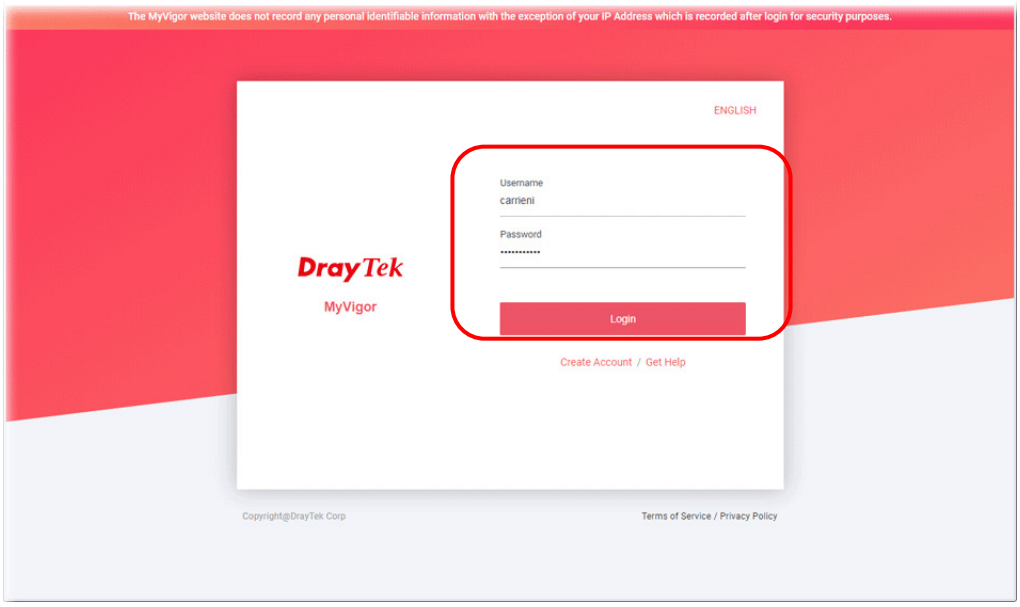
Note:

Before registration, make sure the Vigor router has been set to access the Internet. Then, the link to Register will be shown under Option. If not, the link to Login will appear instead.

---

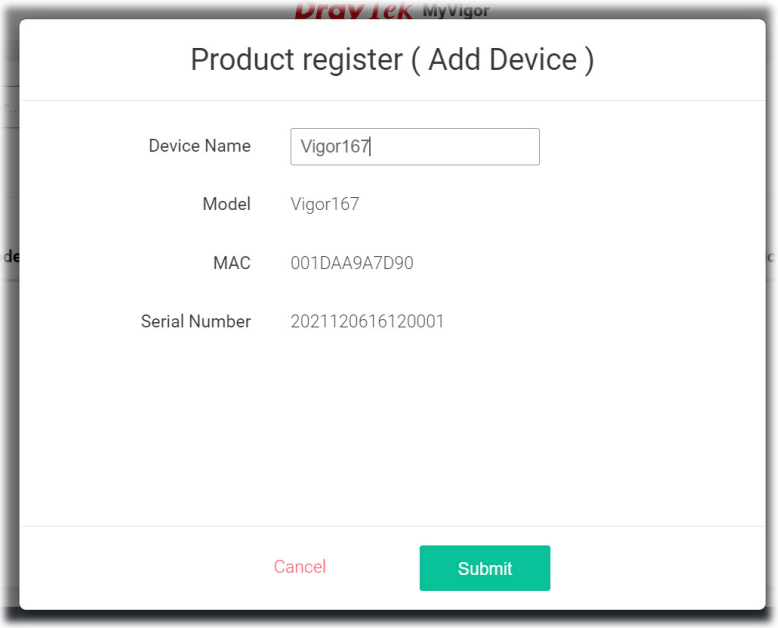
2. Click Register.

3. A Login page will be shown on the screen. Please enter the account and password that you created previously. And click Login.

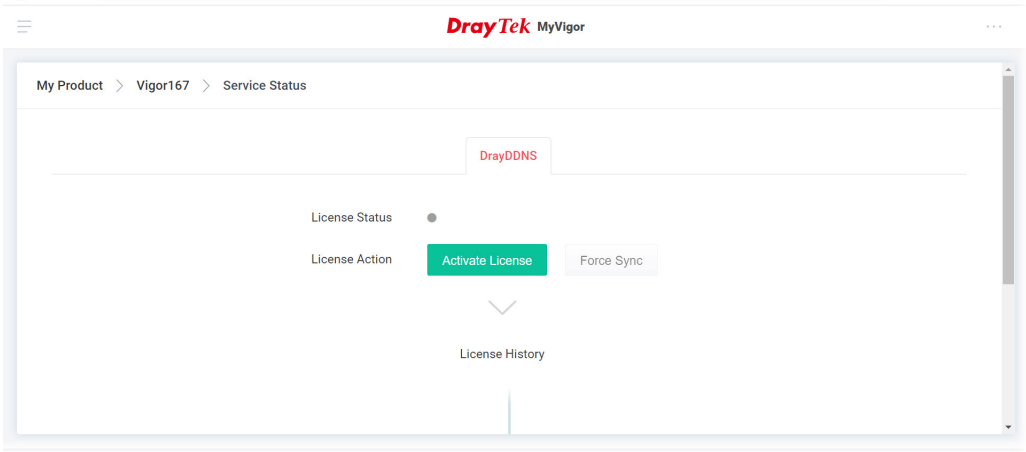


If you haven't an accessing account, please refer to section Create Account for MyVigor to create your own one. Please read the articles on the Agreement regarding user rights carefully while creating a user account.

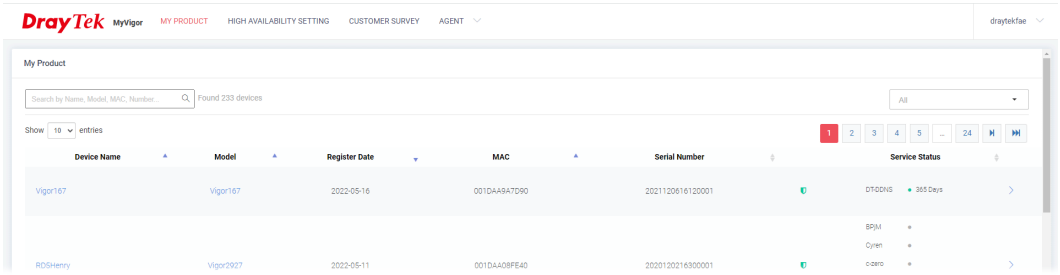
4. The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click Submit.



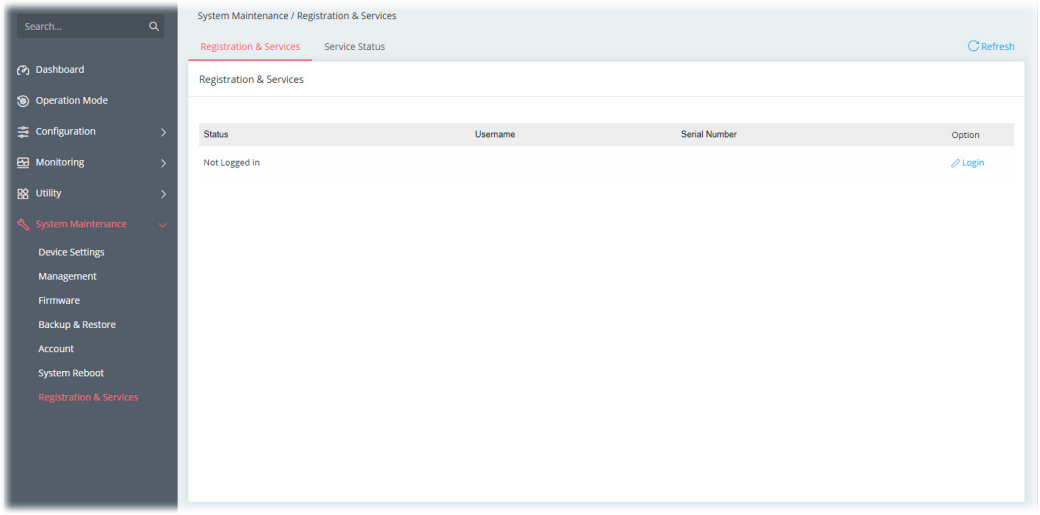
5. When the following page appears, your router has been registered to *myvigor* website successfully. However, the DrayDDNS service has not been activated yet.



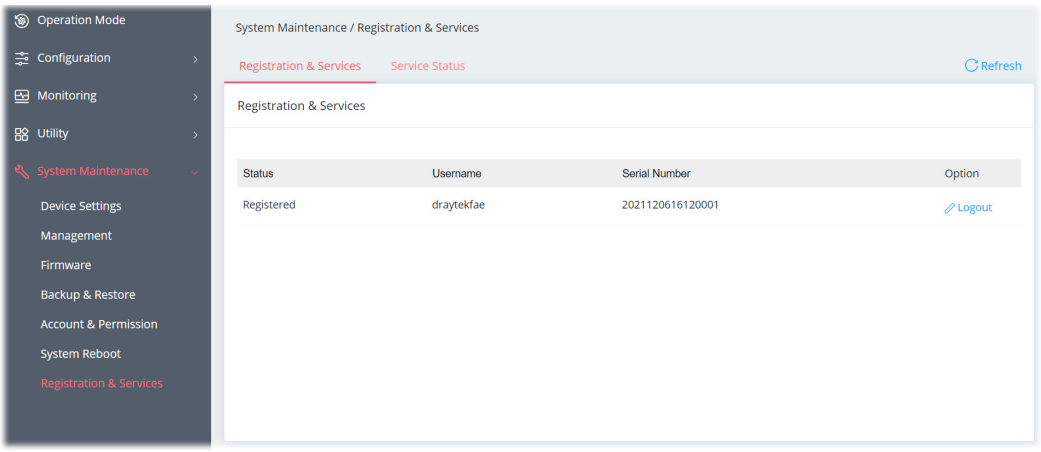
6. Clicking MY PRODUCT for viewing the general information of the registered router on MyVigor website.



7. Return to the System Maintenance >> Registration & Service page. Click the Login link under the Option to load the registration information.



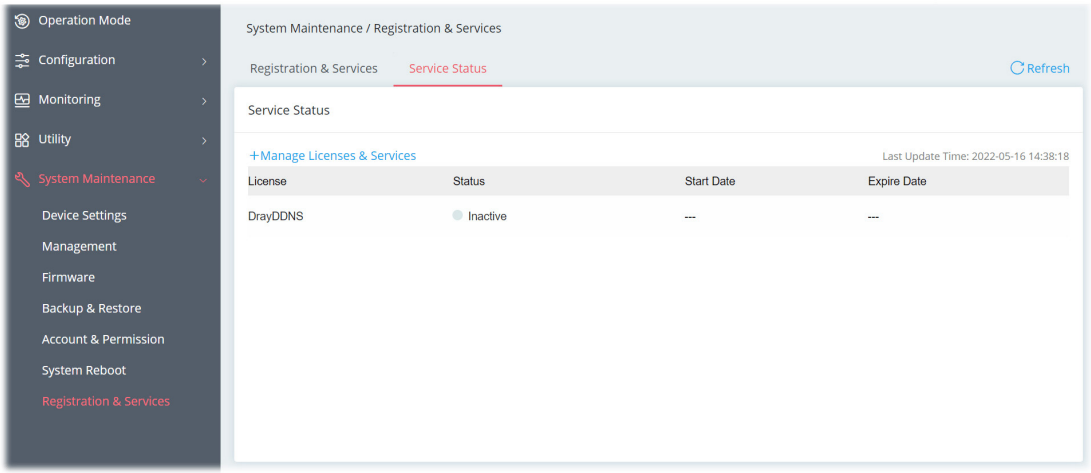
8. Now the registered information of Vigor167 has been shown on this page.



III-1-7-2 Services Status

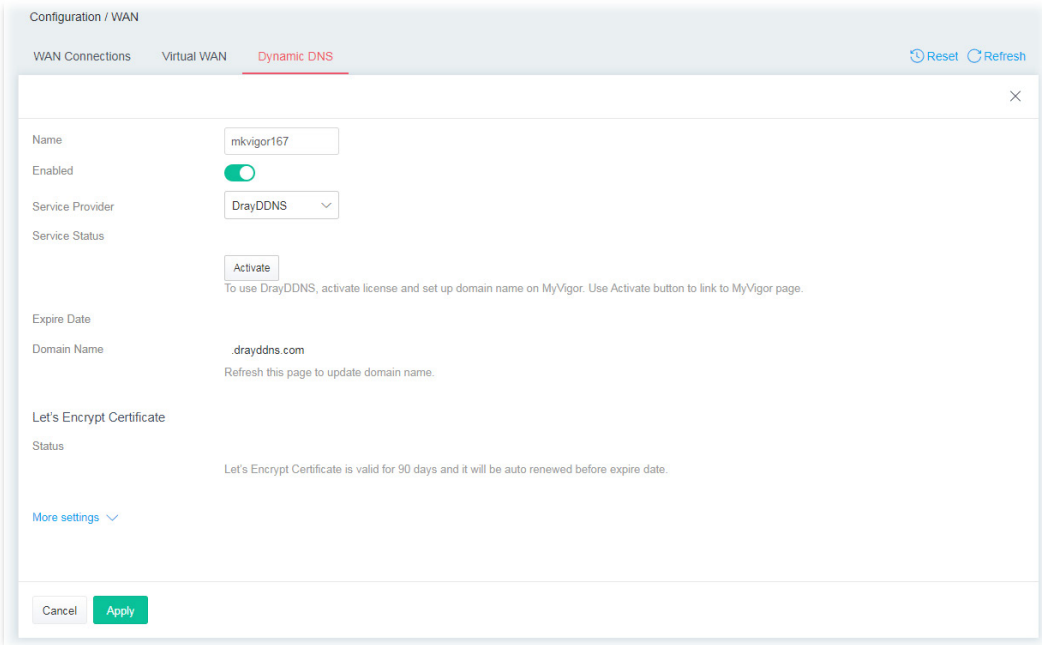
This page displays the current status (including the license name, the start date, and the expiration date) for the license service.

After registering the Vigor router, the type of license (at present, only DrayDDNS) available for this router will be shown on this page.

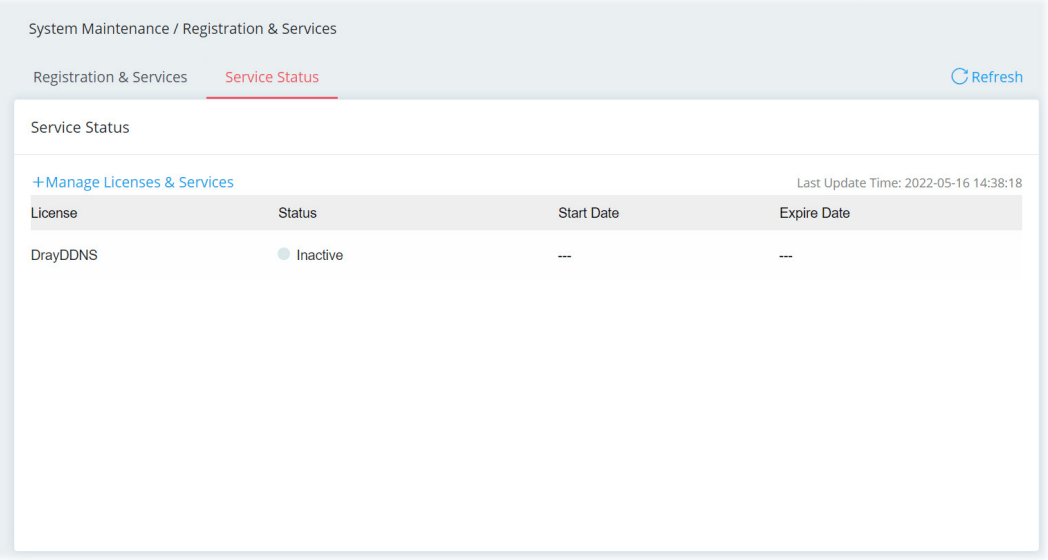


To activate the DrayDDNS service:

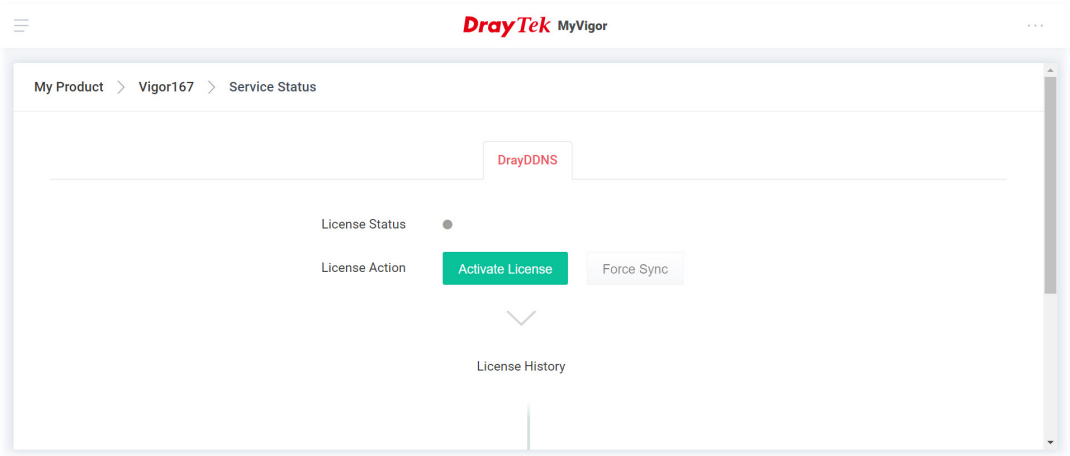
1. Open Configuration>>WAN>>Dynamic DNS to create a DrayDDNS server profile. For example, the name is defined as *mkvigor167* in this case.



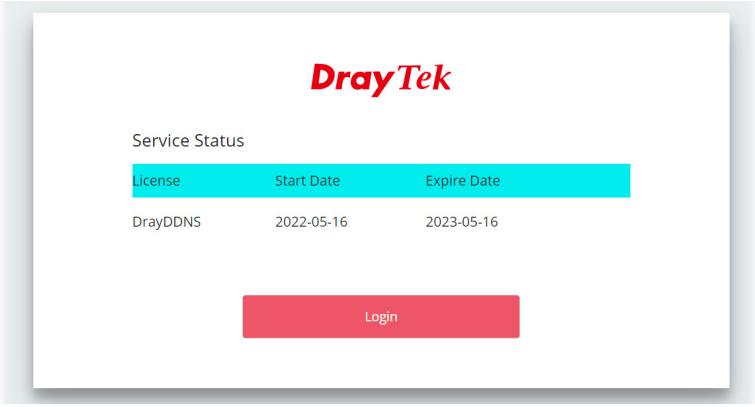
2. Open the page of System Maintenance>>Registration & Services>>Service Status.



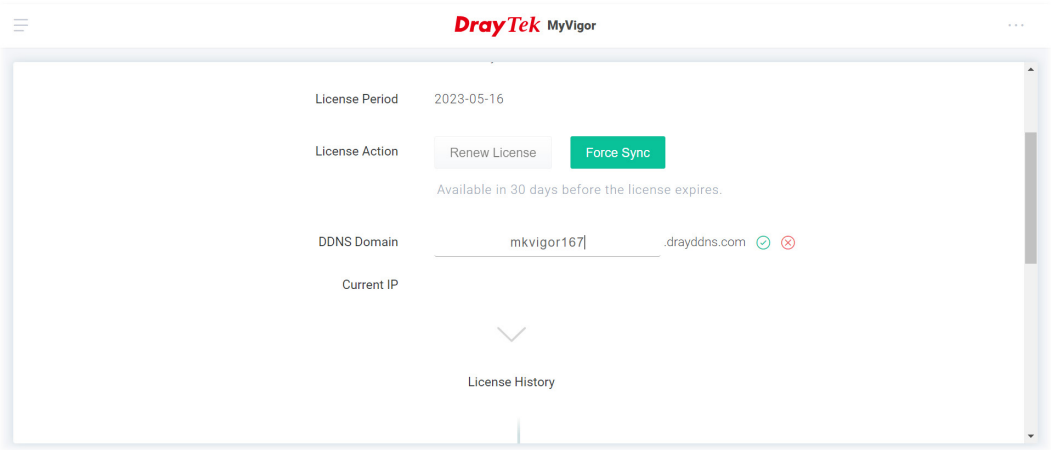
3. Click +Manage Licenses & Services to access MyVigor website.
4. Enter the account and password that you created previously. And click Login.
5. Open the Service Status page and click Activate License.



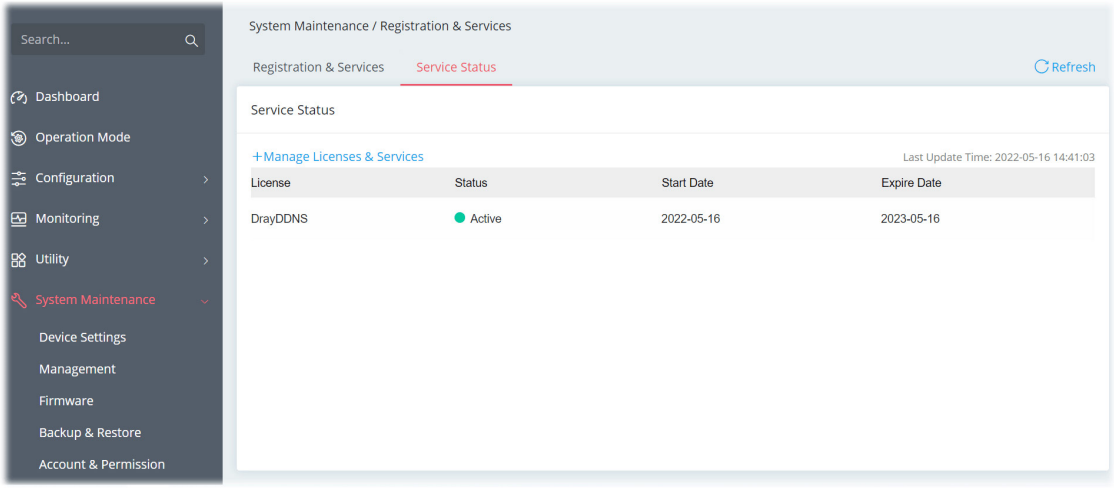
6. After the license has been activated, the following page will be shown on your screen.



7. Click Login. Later, enter the DDNS domain name for DrayDDNS service.



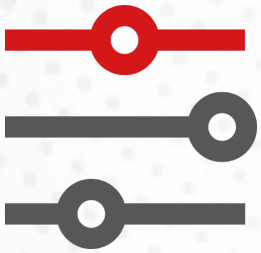
8. Return to the System Maintenance >> Registration & Service>>Service Status page. The activated license with start/expire date information will be shown on the screen.



Note:

If there is no license information, please go to System Maintenance>>Registration & Services>>Registration & Service and click Login (III-1-7-1 , step 7) to load the license information from MyVigor website.

Chapter IV Others

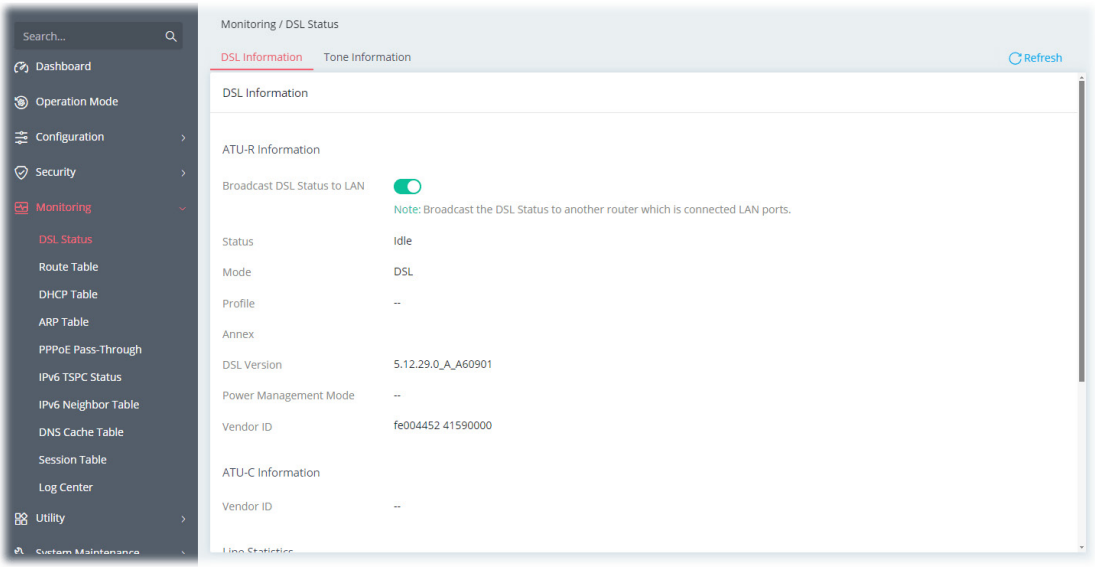


IV-1 Monitoring

IV-1-1 DSL Status

IV-1-1-1 DSL Information

The DSL information (packets) of this router can be broadcasted periodically. The information can be received by the routers under LAN.



Available settings are explained as follows:

Item	Description
Broadcast DSL Status to LAN	Switch the toggle to enable or disable the function.

Note:

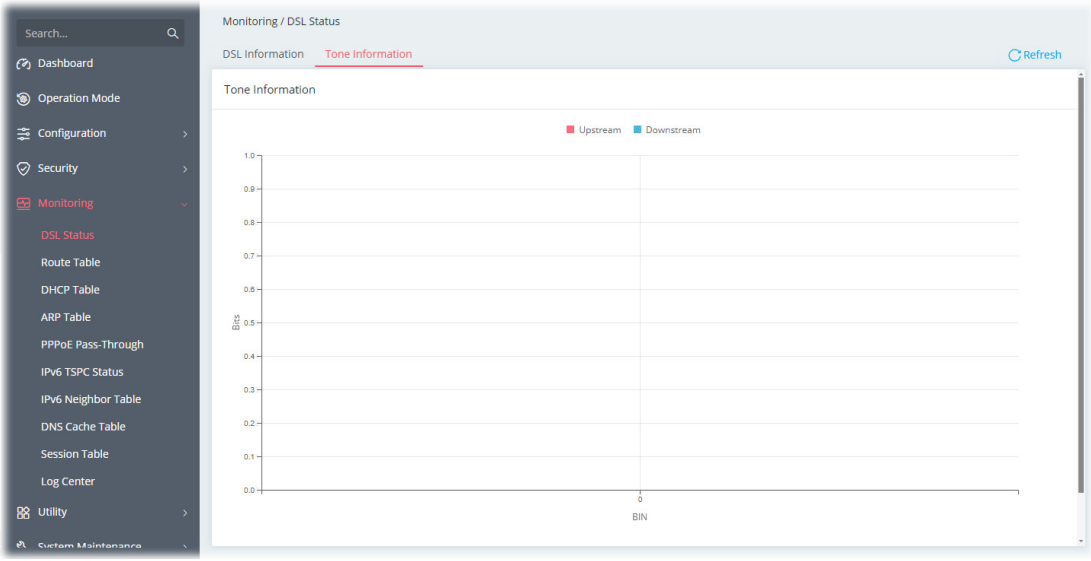
Switch these two icons by click the mouse cursor on them.

- means “Enable”.

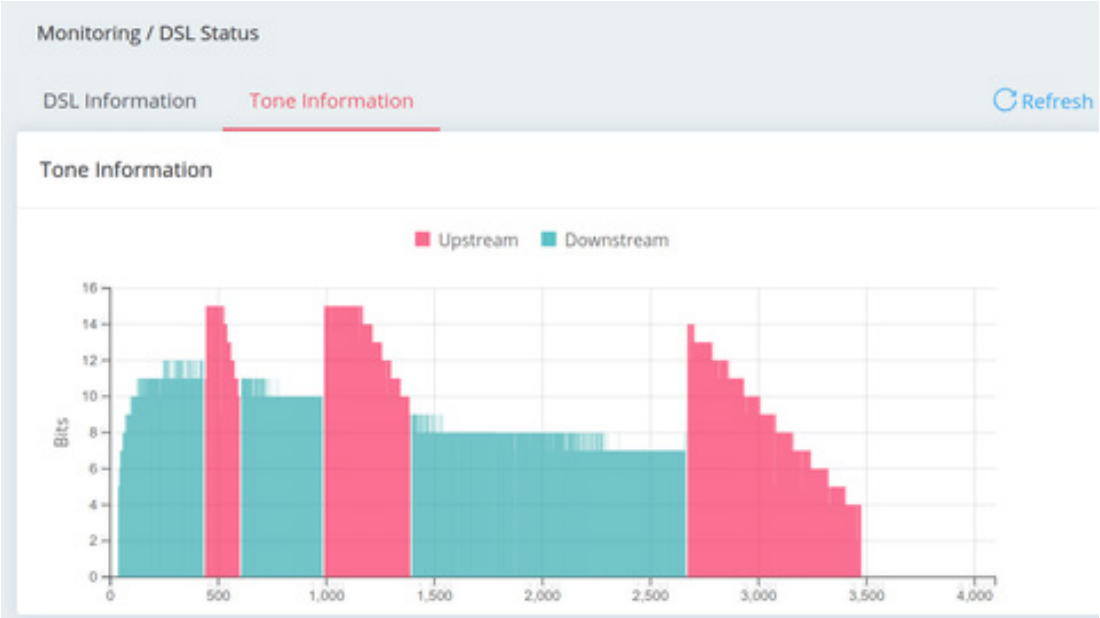
- means “Disable”.

IV-1-1-2 Tone Information

This web page displays the DSL line quality and bin usage.



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

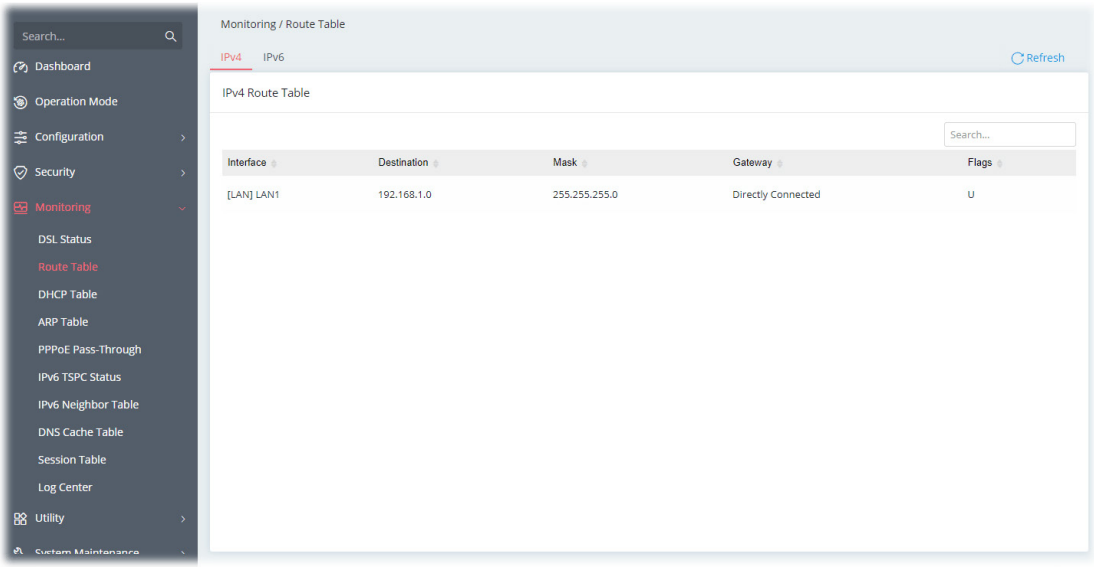


The above figure shows the bandwidth shared between Upstream (Red) and Downstream (Blue).

IV-1-2 Route Table

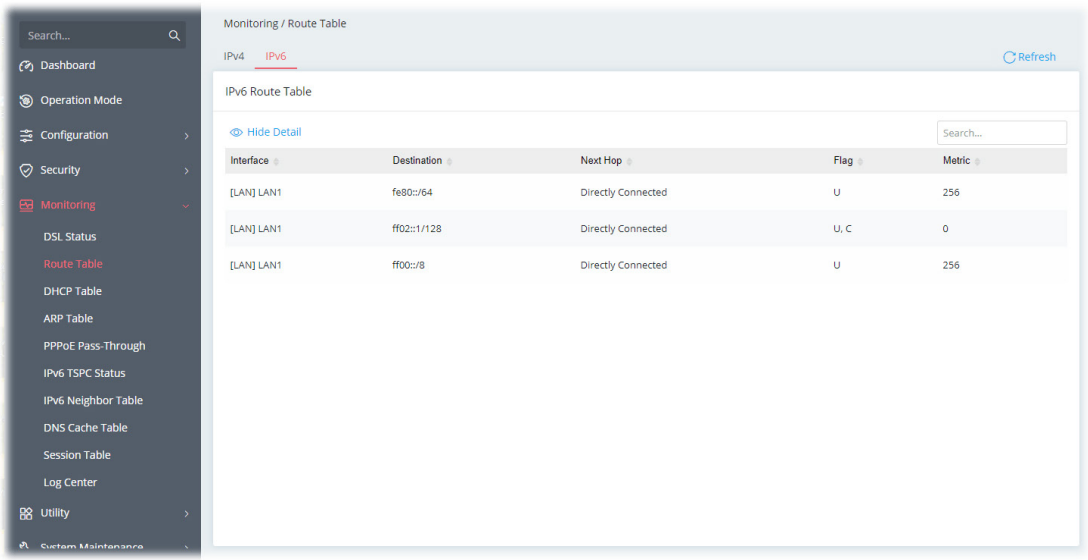
IV-1-2-1 IPv4

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



IV-1-2-2 IPv6

Click Refresh to reload this page with the most up-to-date IPv6 routing information.



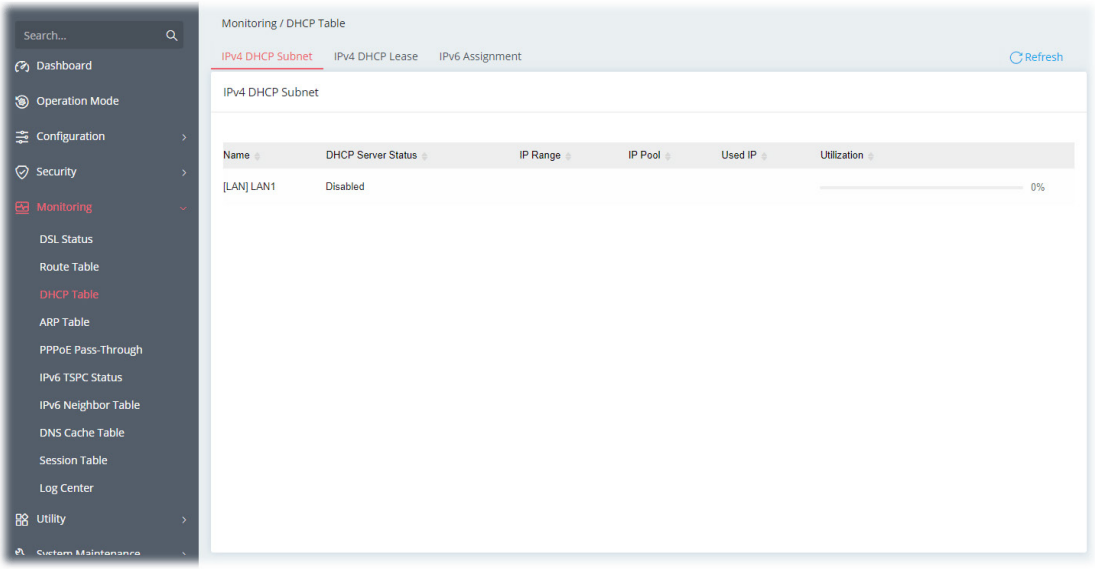
IV-1-3 DHCP Table

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.

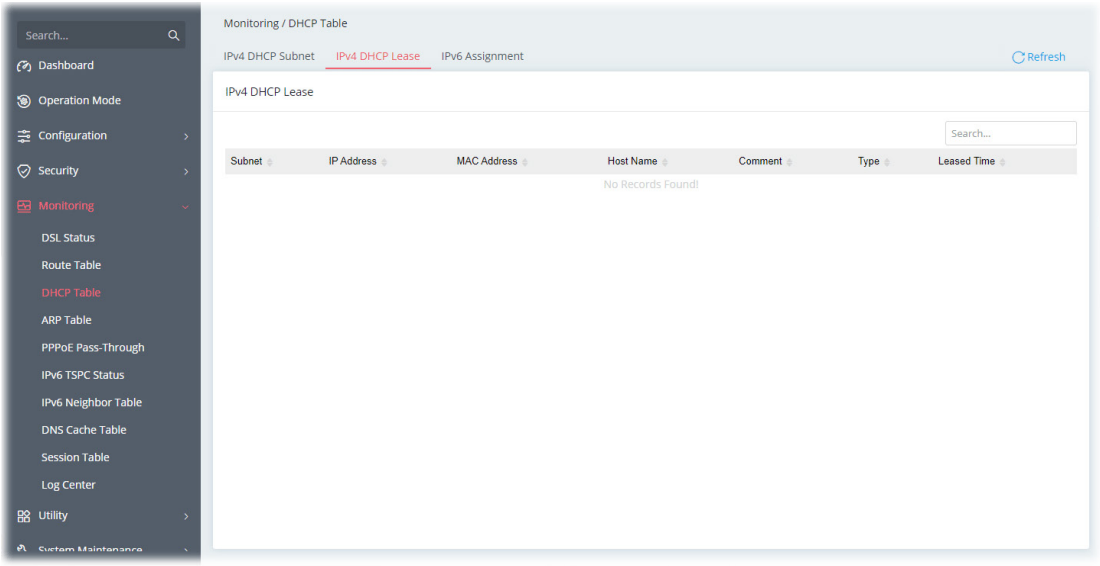
IV-1-3-1 IPv4 DHCP Subnet

This page shows the DHCP server status, IP range, IP pool, Used IP, and percentage of utilization for each LAN interface.



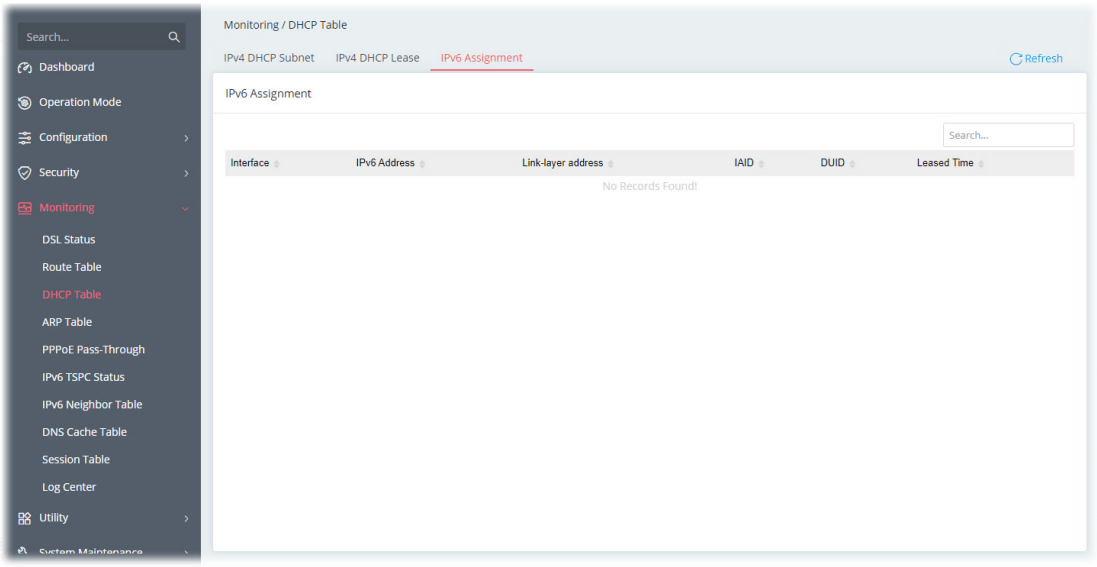
IV-1-3-2 IPv4 DHCP Lease

This page shows the remaining time of the IPv4 DHCP lease of the device.



IV-1-3-3 IPv6 Assignment

This page shows the remaining time of the IPv6 DHCP lease of the device.

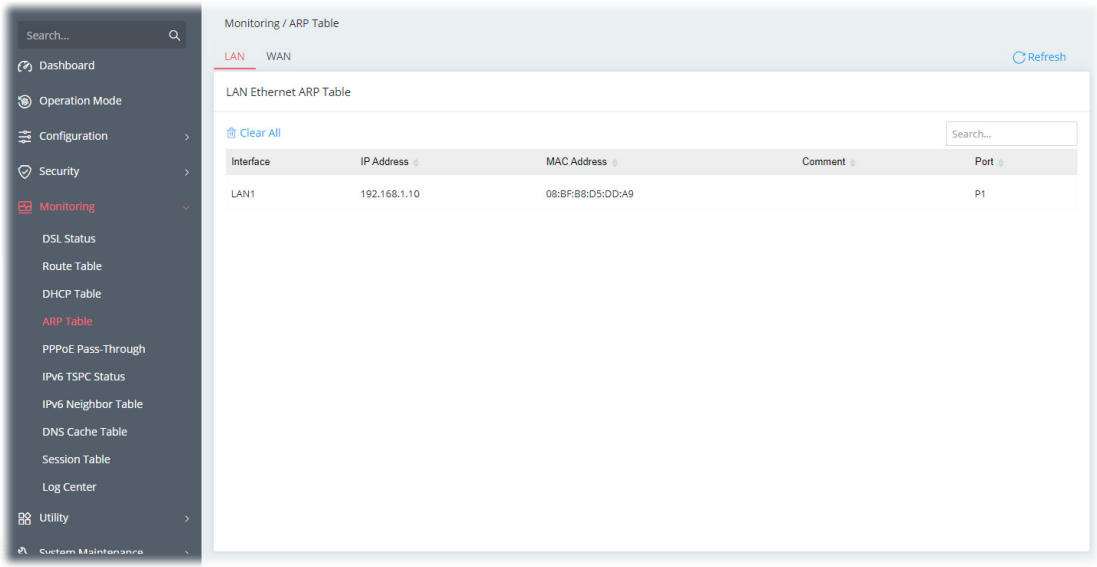


IV-1-4 ARP Table

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.

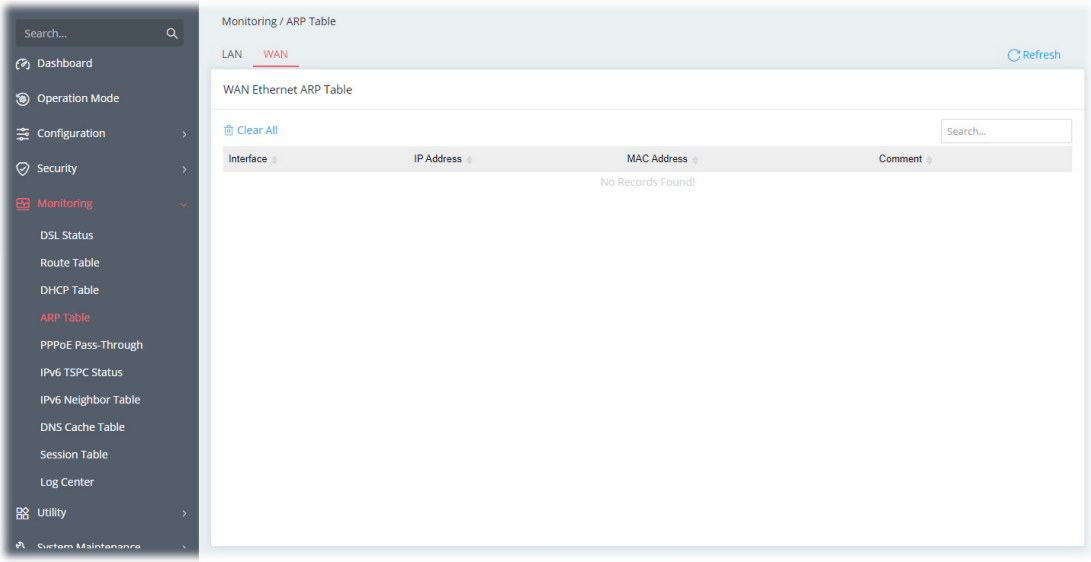
IV-1-4-1 LAN

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



IV-1-4-2 WAN

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

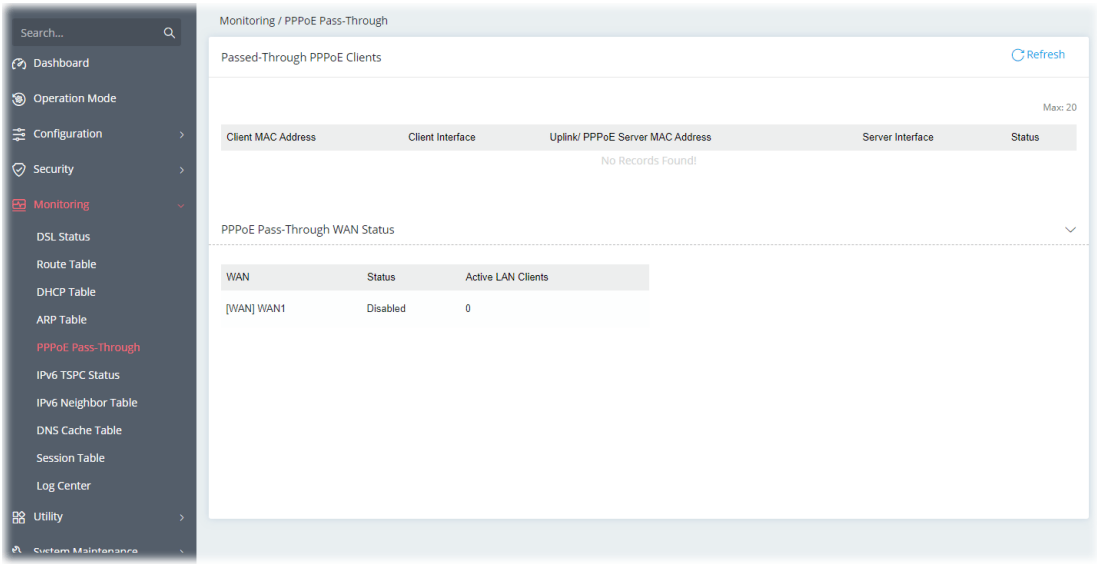


IV-1-5 PPPoE Pass-Through

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.

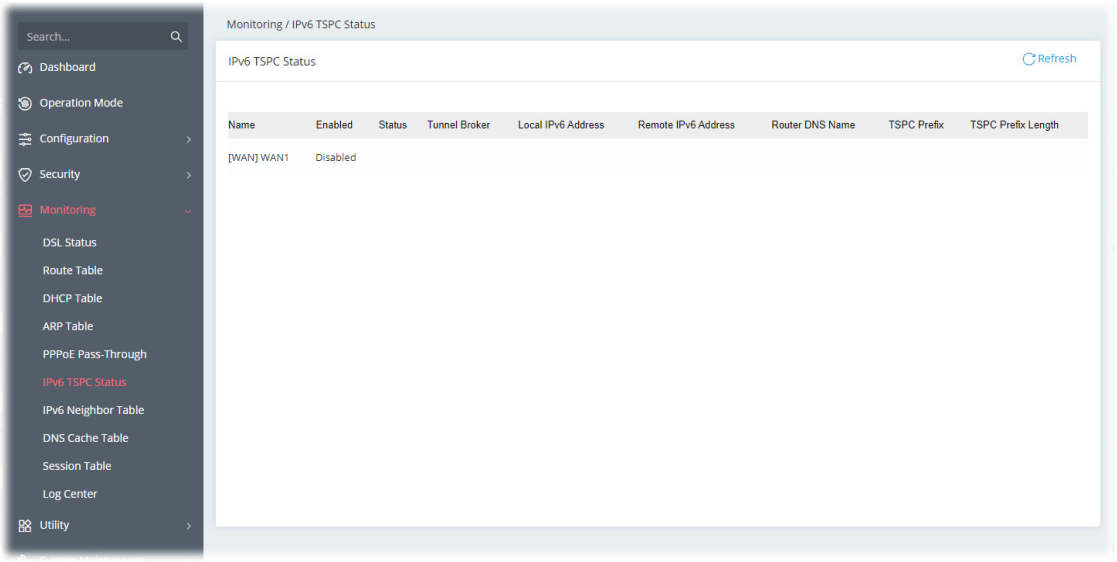
Click Refresh to reload this page with the most up-to-date information.



IV-1-6 IPv6 TSPC Status

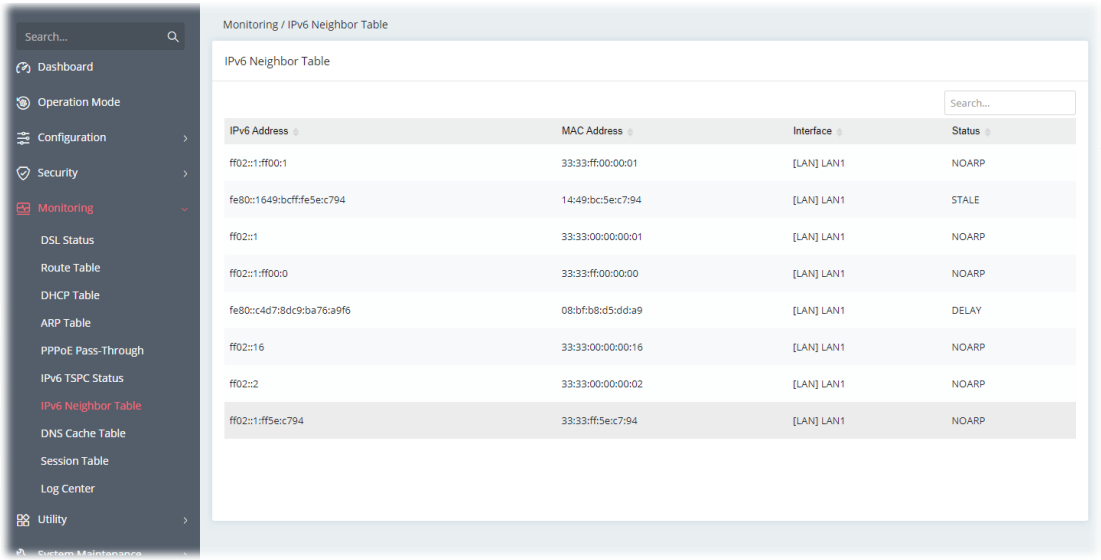
IPv6 TSPC (Tunnel Setup Protocol Client) status page could help you diagnose issues with IPv6 connections that utilize TSP.

If TSPC is configured properly, the router will display the following when the router has connected to the tunnel broker successfully.



IV-1-7 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.

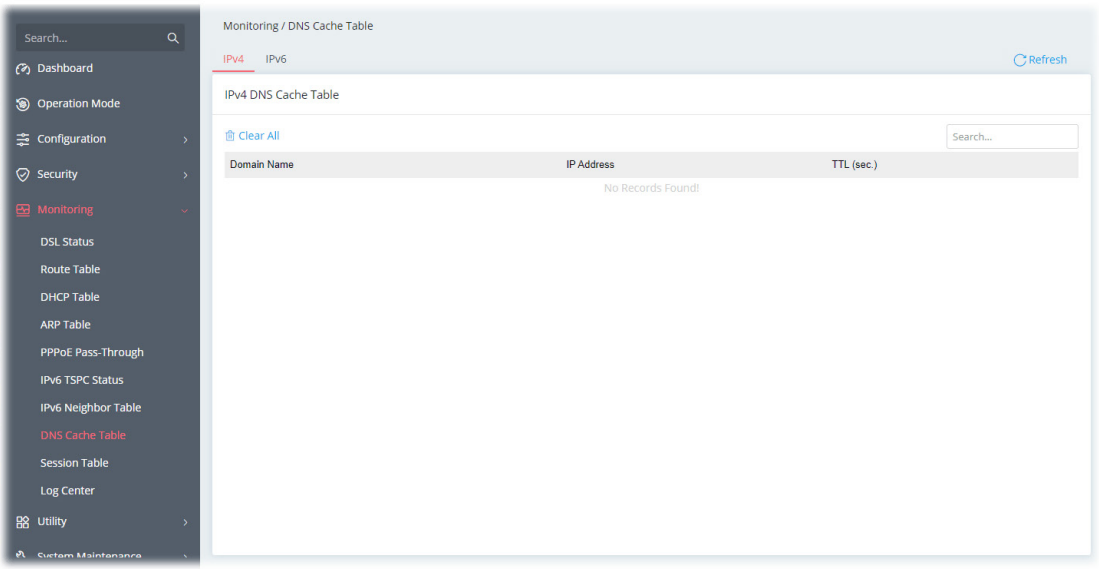


IV-1-8 DNS Cache Table

The router can function as a DNS server which allows LAN clients to look up DNS information by sending DNS requests to the router. Such DNS information is temporarily cached on the router and can be viewed on this page.

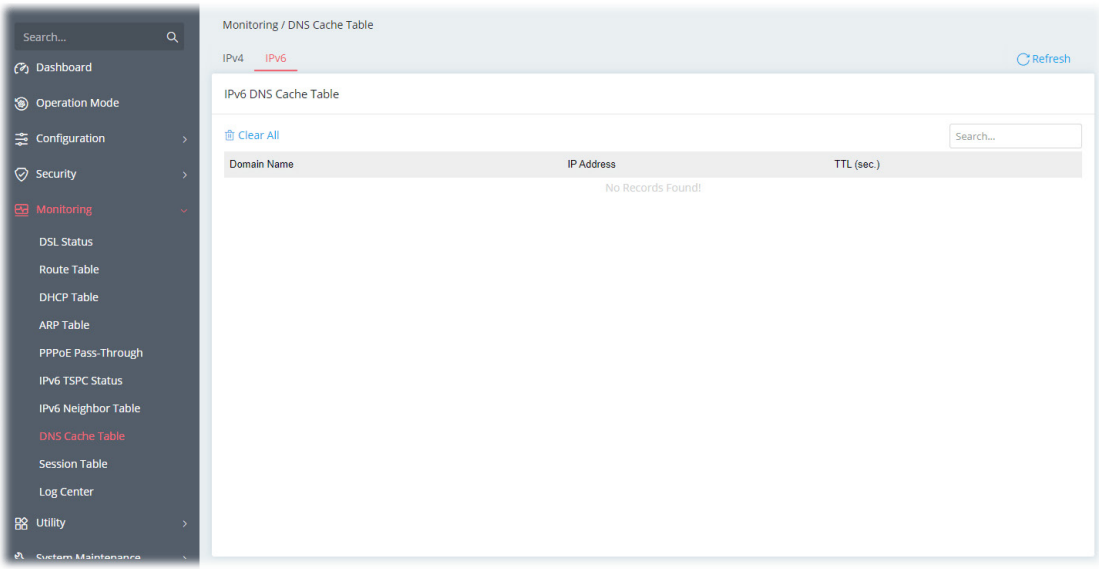
IV-1-8-1 IPv4

Click Refresh to reload the most up-to-date information of the IPv4 DNS cache data.



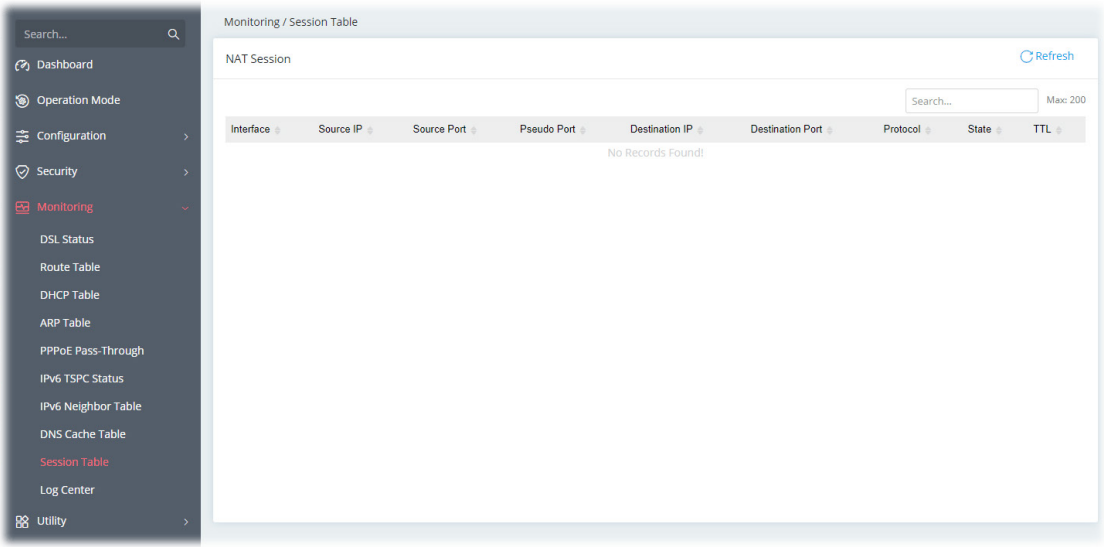
IV-1-8-2 IPv6

Click Refresh to reload the most up-to-date information of the IPv6 DNS cache data.



IV-1-9 Session Table

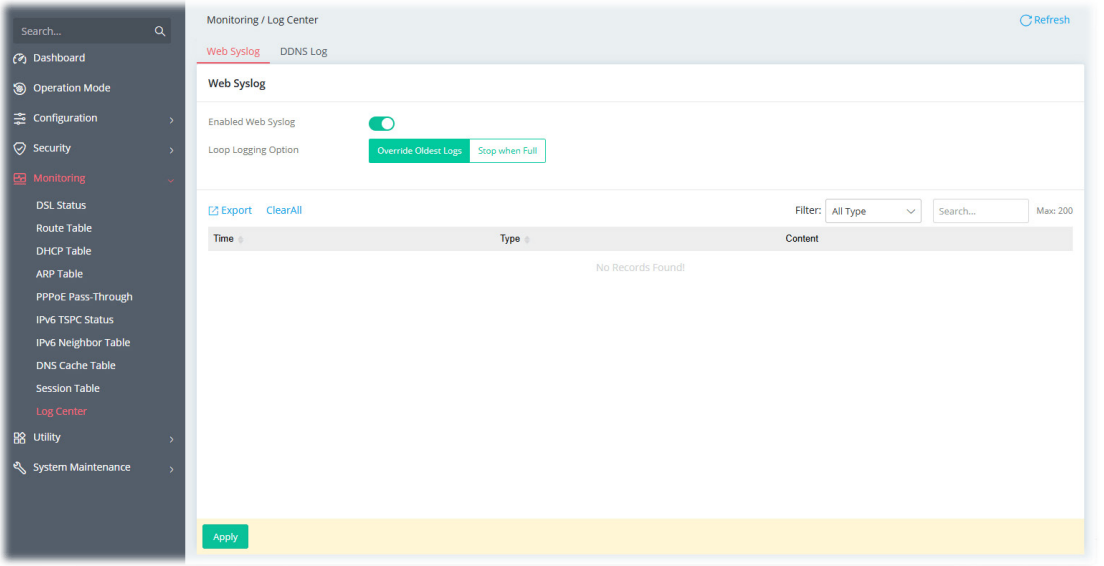
This screen shows the 200 newest entries in the NAT sessions table. Click Refresh to reload this page with the most up-to-date information.



IV-1-10 Log Center

IV-1-10-1 Web Syslog

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



Available settings are explained as follows:

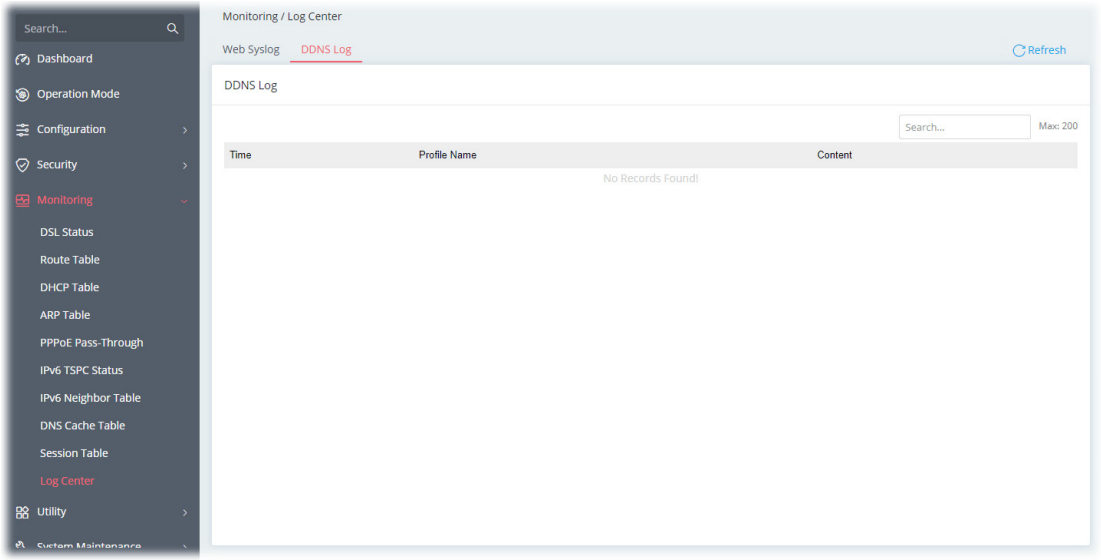
Item	Description
Enabled Web Syslog	Switch the toggle to enable or disable the function.
Loop Logging Option	Override Oldest Logs - Vigor router system will backup all existed information on the USB disk onto the host and clean up the

	information from USB disk. Later, it will start a new record. Stop when Full - Vigor router system will stop to record the user information onto USB disk.
Export	Click it to export the configuration as a file (.json).
Clear All	Click it to clear all settings on this page and return to the factory settings.
Filter	Select the type of log to display on this page.
Apply	Save the current settings and exit the page.

Click Apply to save the settings.

IV-1-10-2 DDNS Log

This page displays the log (time, profile name and content) related to Dynamic DNS actions performed by this device.



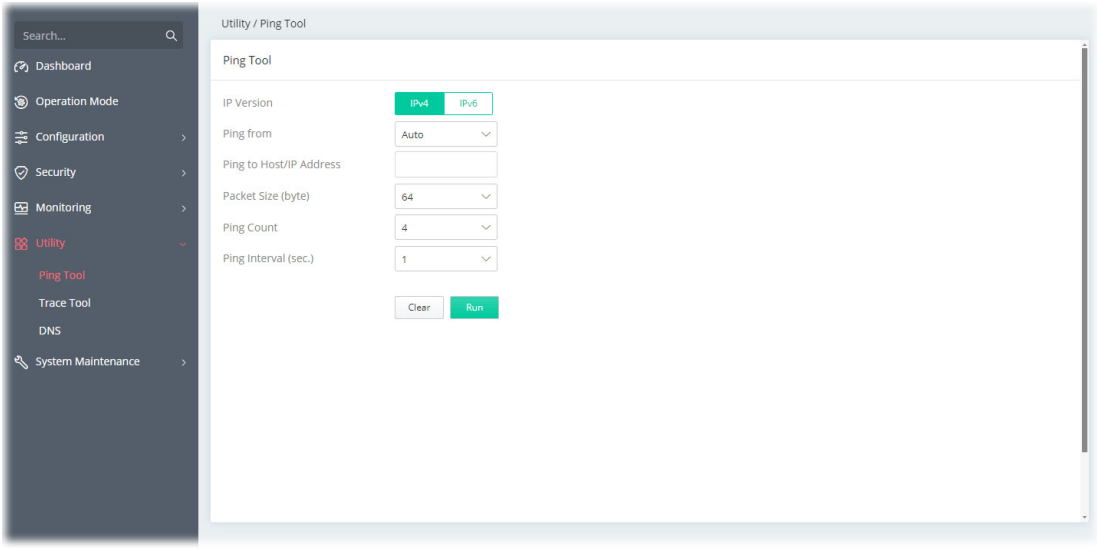
Click Refresh to reload this page with the most up-to-date information.

IV-2 Utility

This section contains utilities (e.g., ping tool, trace tool, DNS and etc.) that can assist you in analyzing issues and failures during the setup and operation of the router.

IV-2-1 Ping Tool

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

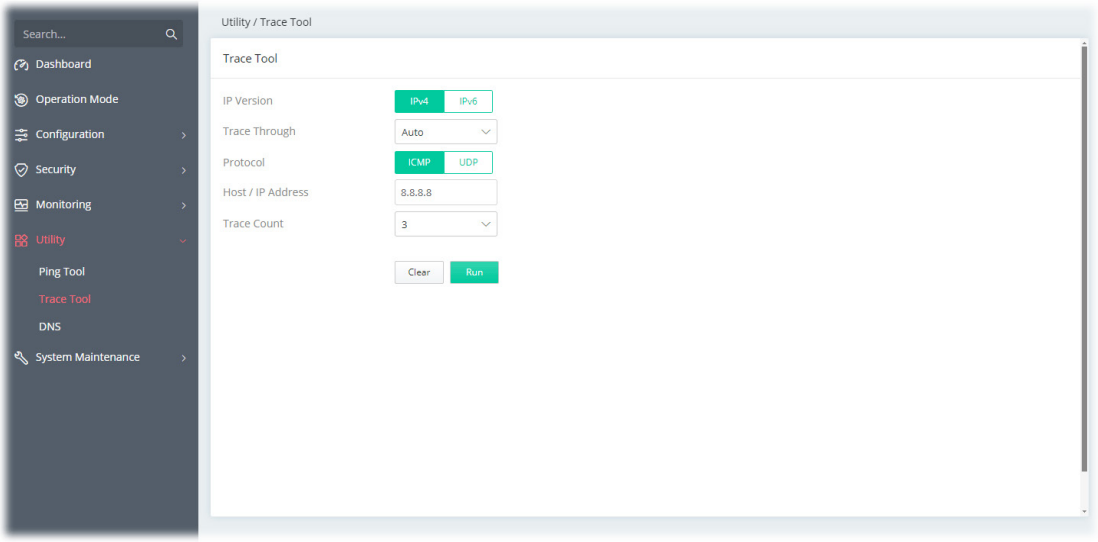


Available settings are explained as follows:

Item	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-2-2 Trace Tool

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

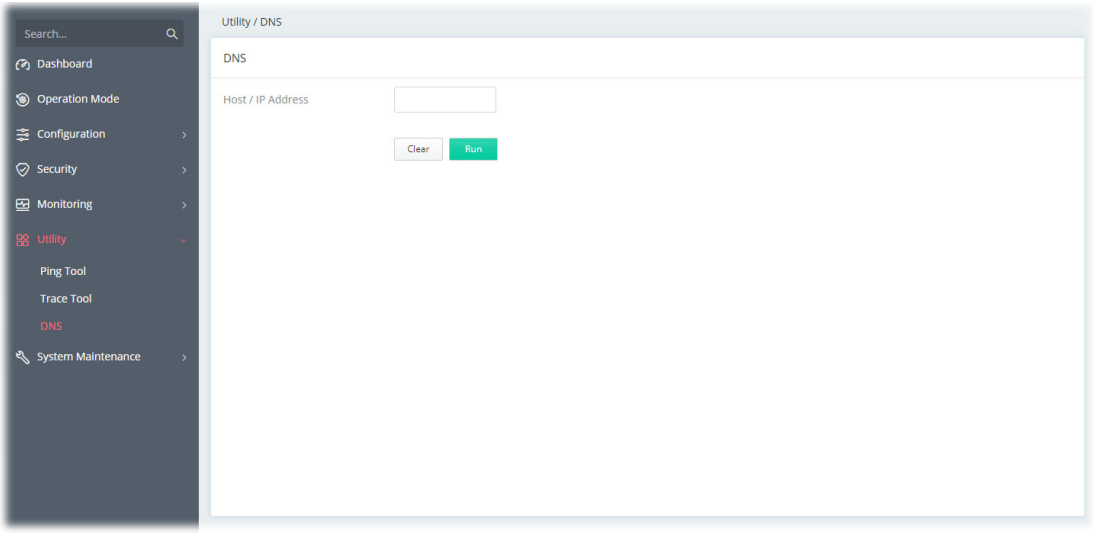


Available settings are explained as follows:

Item	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 trace.
Trace Count	Select the max hops for trace the route, select none for unlimited.
Clear	Remove the settings and return to the factory settings.
Run	Perform the job.

IV-2-3 DNS

The user can diagnose the router by query Domain Name System (DNS) servers to obtain domain name or IP address information.



Available settings are explained as follows:

Item	Description
Host/IP Address	Enter the host / IP address that you want to trace.
Clear	Remove the settings and return to the factory settings.
Run	Perform the job.

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.

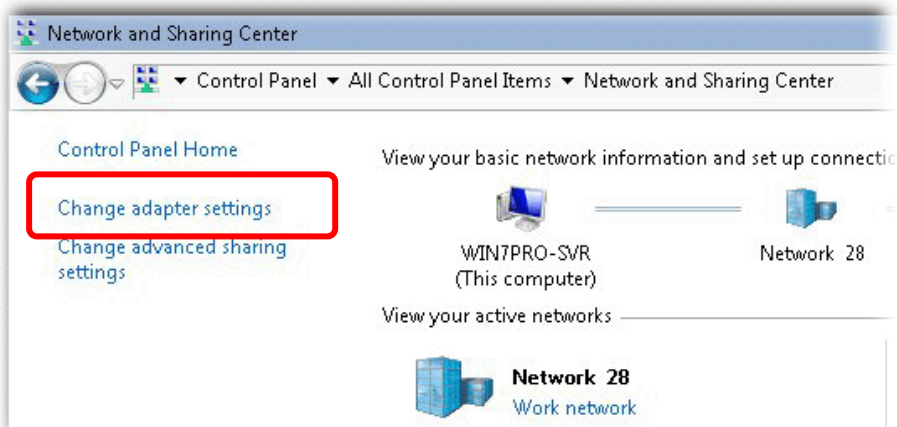
V-2-1 For Windows

Note:

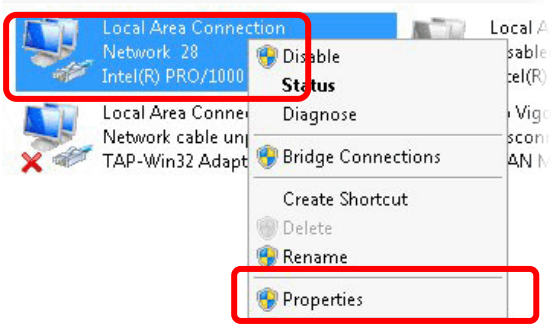
The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

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

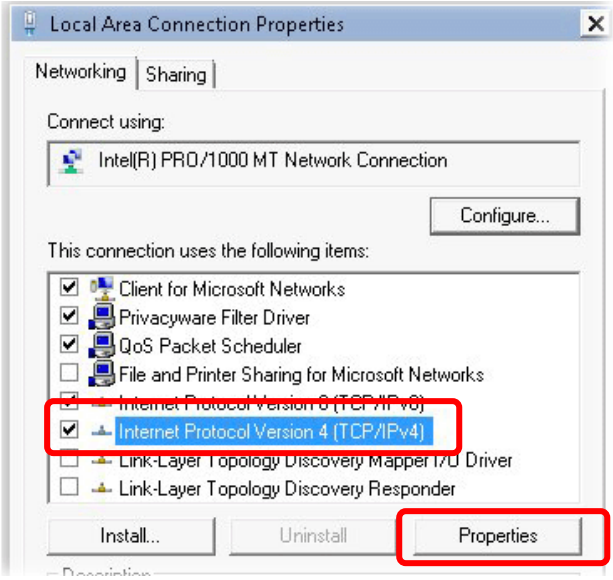
2. In the following window, click Change adapter settings.



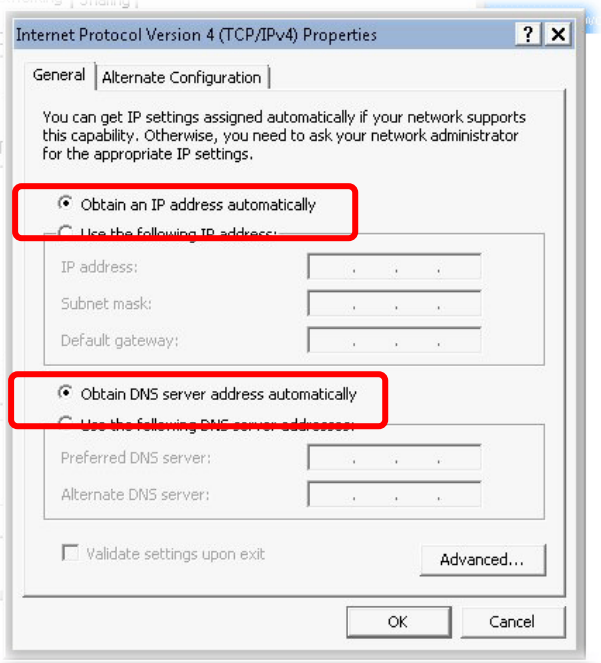
3. Icons of the network connection will be shown on the window. Right-click on Local Area Connection and click on Properties.



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

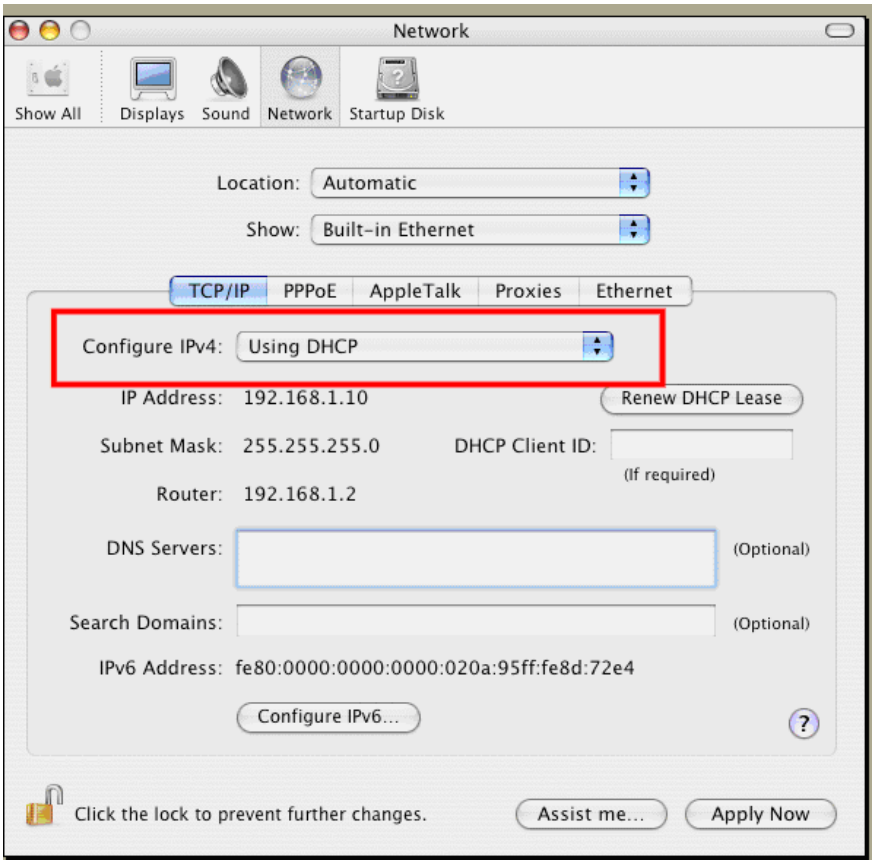


5. Select Obtain an IP address automatically and Obtain DNS server address automatically. Finally, click OK.



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.



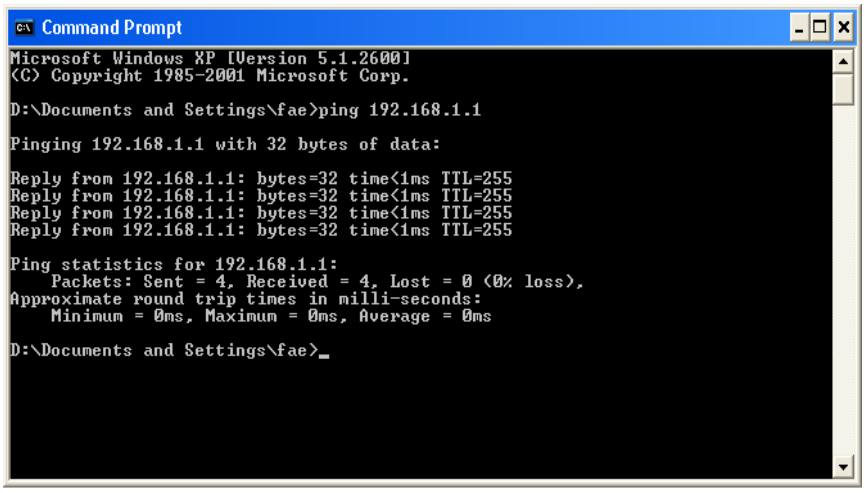
V-3 Pinging the Device

The default gateway IP address of the modem is 192.168.2.1. 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 192.168.2.1. 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

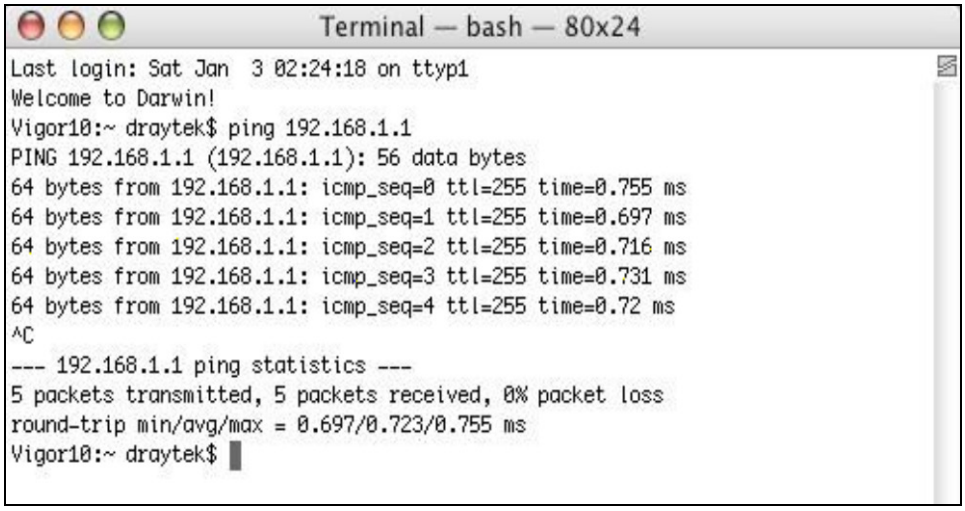
1. Open the Command Prompt window (from Start menu> Run).
2. Type cmd. The DOS command dialog will appear.



3. Type ping 192.168.2.1 and press [Enter]. If the link is OK, the line of “Reply from 192.168.2.1: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 192.168.2.1 and press [Enter]. If the link is OK, the line of “64 bytes from 192.168.2.1: icmp_seq=0 ttl=255 time=xxxx ms” will appear.


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

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.

ⓘ Warning:

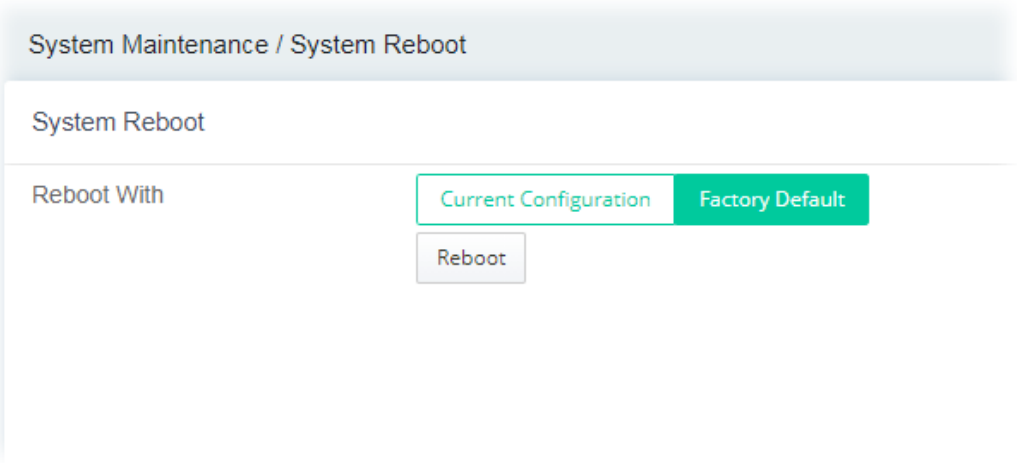
After using the factory default settings, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing.

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.



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.