Vigor180 Series

XGS-PON Router

User's Guide

Version: 1.0

Firmware Version: V5.3.3

Date: 31 March 2026

Intellectual Property Rights (IPR) Information

Copyrights

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows 10, 11 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 router.
- The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of 0 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Do not power off the device when saving configurations or firmware upgrades. It may damage the data in a flash. Please disconnect the Internet connection on the router before powering it off when a TR-069/ ACS server manages the router.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor router via https://myvigor.draytek.com.

Firmware & Tools Updates

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

Table of Contents

Chapter I Installation VII

I-1 Introduction 1

I-1-1 LED Indicators and Connectors for Vigor180 1

I-2 Hardware Installation 3

I-2-1 Network Connection 3

I-2-2 Wall-Mounted Installation 4

I-3 Accessing to Web User Interface 5

I-4 Dashboard 8

Chapter II Connectivity 9

II-1 Configuration 10

II-1-1 Physical Interface 10

II-1-2 WAN 12

II-1-2-1 WAN Connections 12

II-1-2-2 Virtual WAN 19

II-1-2-3 Dynamic DNS 22

II-1-2-4 PPPoE Pass Through 26

II-1-3 LAN 27

II-1-3-1 LANs 28

II-1-4 Routing 32

II-1-4-1 IPv4 Static Route 32

II-1-4-2 IPv6 Static Route 35

II-1-5 NAT 36

II-1-5-1 Port Forwarding 37

II-1-5-2 DMZ Host 40

II-1-5-3 Port Triggering 41

II-1-5-4 ALG 44

II-1-5-5 UPnP 44

II-1-6 IGMP 45

II-1-6-1 General Setup 45

II-1-6-2 IGMP Status 47

II-1-7 Objects 48

II-1-7-1 IP Object 48

II-1-7-2 IP Group 50

II-1-7-3 Schedule 52

II-1-7-4 Backup & Restore 54

II-1-8 Certificates 55

II-1-8-1 Local Certificates 55

II-1-8-2 Trusted CA 57

II-1-8-3 Local Services 60

II-1-8-4 Backup & Restore 61

II-2 Security 62

II-2-1 Firewall Filters 62

II-2-1-1 IP Filters 63

II-2-1-2 Default Filters 67
II-2-1-3 Backup & Restore 69
II-2-2 Defense Setup 70
II-2-3 IPv6 Address Security 73

Chapter III Management 75

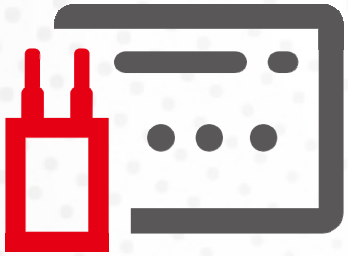
III-1 System Maintenance 76
III-1-1 Device Settings 76
III-1-1-1 Time 76
III-1-1-2 Device Name 78
III-1-1-3 Syslog 78
III-1-1-4 SNMP 79
III-1-2 Management 81
III-1-2-1 Service Control 81
III-1-2-2 TR-069 84
III-1-2-3 XMPP 85
III-1-3 System Upgrade 86
III-1-3-1 Firmware 86
III-1-4 Backup & Restore 89
III-1-5 Accounts & Permission 90
III-1-5-1 Local Admin Account 90
III-1-5-2 Role & Permission 93
III-1-6 System Reboot 95

Chapter IV Others 97

IV-1 Monitoring 98
IV-1-1 Log Center 98
IV-1-1-1 Log Center 98
IV-1-1-2 DDNS Log 99
IV-1-1-3 Notification 99
IV-1-2 WAN 101
IV-1-2-1 WAN Status 101
IV-1-3 ARP Table 102
IV-1-3-1 LAN 102
IV-1-3-2 WAN 103
IV-1-4 Route Table 103
IV-1-4-1 IPv4 103
IV-1-4-2 IPv6 104
IV-1-5 DHCP Table 105
IV-1-5-1 IPv4 DHCP Subnet 105
IV-1-5-2 IPv4 DHCP Lease 105
IV-1-5-3 IPv6 Assignment 107
IV-1-6 IPv6 TSPC Status 107
IV-1-7 IPv6 Neighbor Table 108
IV-1-8 LLDP Neighbors Information 108
IV-1-9 DNS Cache Table 109
IV-1-9-1 IPv4 109
IV-1-9-2 IPv6 110
IV-1-10 XGSPON Status 111
IV-1-11 PPPoE Pass-Through 111

IV-1-12 Session Table 113
IV-1-13 Running Services 113
IV-2 Utility 114
IV-2-1 Network Tools 114
IV-2-1-1 Ping Tool 114
IV-2-1-2 Traceroute 115
IV-2-1-3 DNS 116
IV-2-2 Web CLI 117
Chapter V Troubleshooting 119
V-1 Checking the Hardware Status 120
V-2 Checking the Network Connection Settings 121
V-2-1 For Windows 121
V-2-2 For Mac Os 123
V-3 Pinging the Device 124
V-3-1 For Windows 124
V-3-2 For Mac Os (Terminal) 124
V-4 Backing to Factory Default Setting 126
V-4-1 Software Reset 126
V-4-2 Hardware Reset 127
V-5 Contacting DrayTek 128

Chapter I Installation



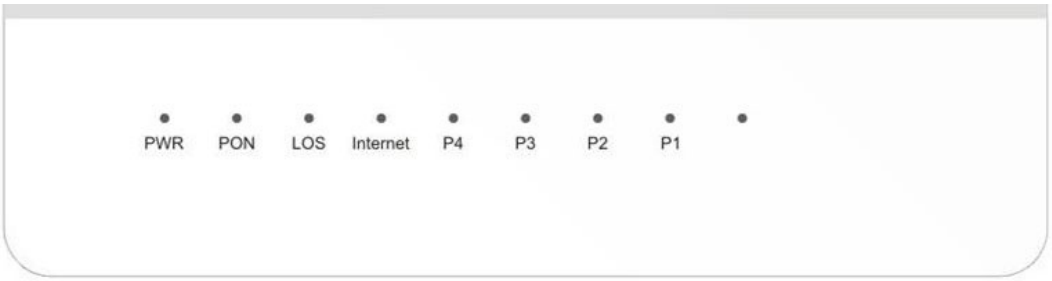
I-1 Introduction

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

I-1-1 LED Indicators and Connectors for Vigor180

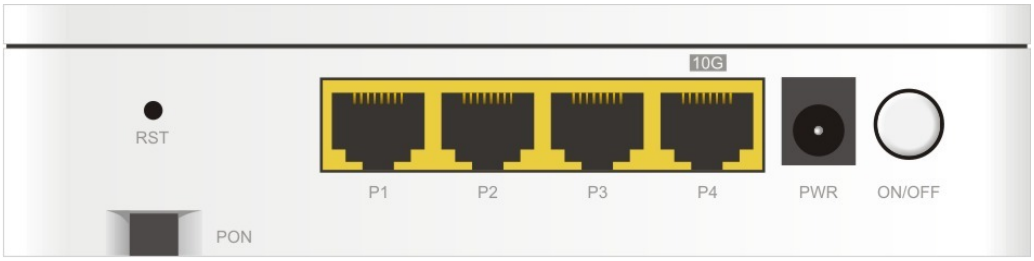
Before you use the Vigor modem, please get acquainted with the LED indicators and connectors first.

LED



LED	Status	Explanation
PWR	Blinking	The device is powered on and running normally.
	Off	The device is powered off.
PON	On	PON (Passive optical network) is registered and ready.
	Blinking	PON (Passive optical network) is detected and registering to the router.
	Off	PON (Passive optical network) is disabled or not registered.
LOS	ON (Red)	Loss-of-Signal detected (fiber disconnected, optical power too low, or transceiver fault); no downstream optical signal can be received.
	Blinking (Red)	The received optical power is lower than the sensitivity of the optical receiver.
	Off	No loss-of-signal detected. The received optical power is normal.
Internet	On	Internet connection is ready.
	Off	Internet connection is not ready.
P4 ~ P1	On	The LAN port is connected.
	Blinking	The data is transmitting.
	Off	The LAN port is disconnected.

Connectors



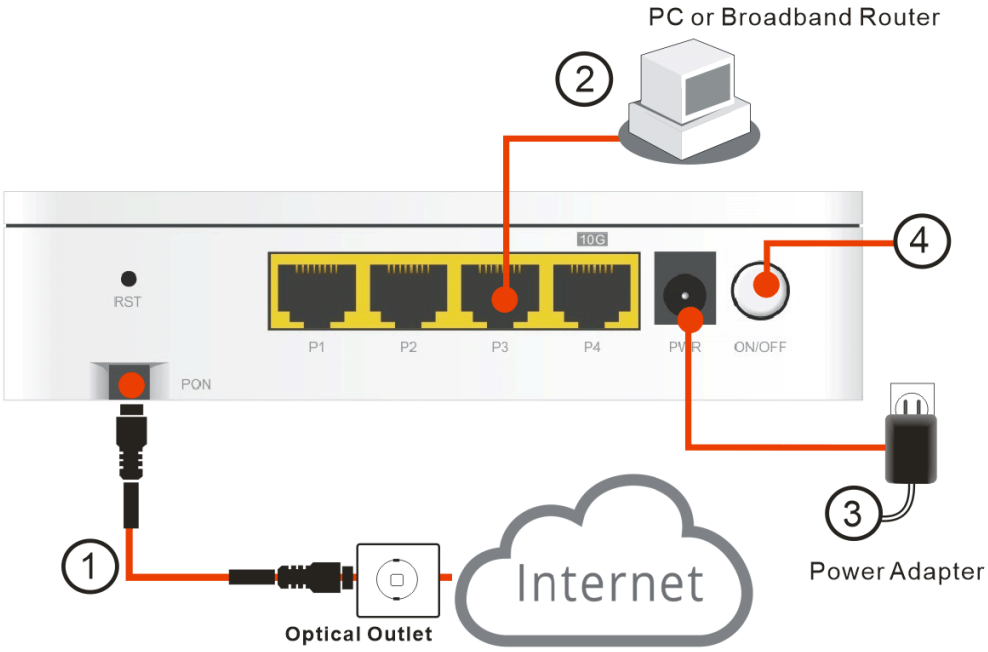
Interface	Description
RST	Restore the default settings. Usage: Press the hole and keep for more than 5 seconds. Then release the button. The device will restart with the factory default configuration.
Phone	Connecter for analog phone.
P1~P4	Connectors for local networked devices. In which, the transmission rate for P4(only) can reach up to 10G.
PWR	Connector for a power adapter.
ON/OFF	Power switch.

I-2 Hardware Installation

This section will guide you to install the Vigor180 through a hardware connection and configure the device's settings through the web browser.

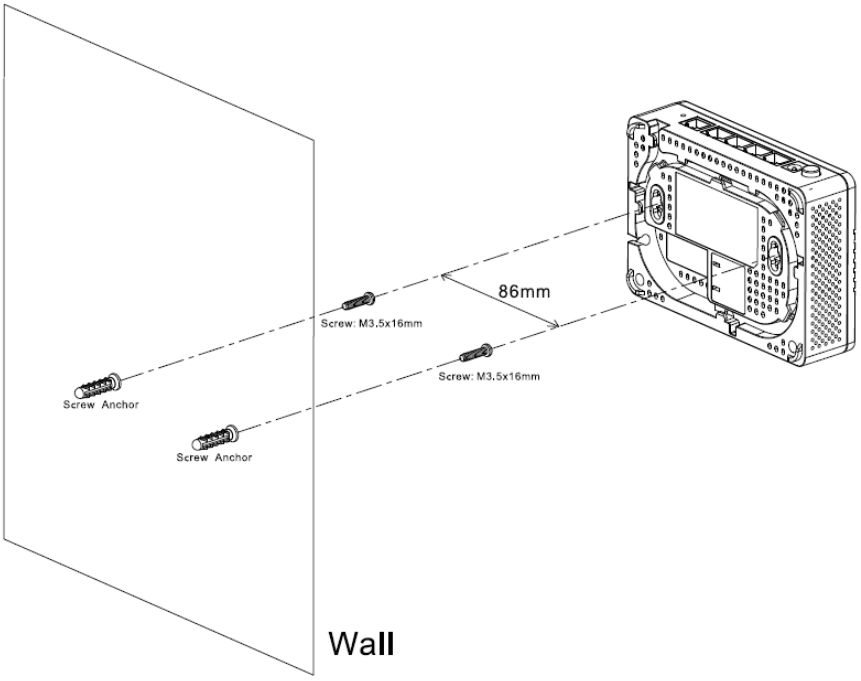
I-2-1 Network Connection

1. Connect the router with a fiber optic cable to get Internet access.
2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the device and the other end of the cable (RJ-45) into the Ethernet port on your computer.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the device. Check the **PON** and **Internet**, **LAN** LEDs to assure network connection.

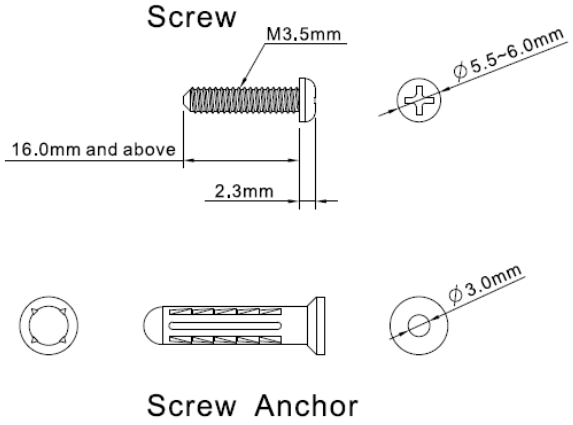


I-2-2 Wall-Mounted Installation

Wall-mounted installation might be required in some cases. Refer to the following figure:



1. Two screw slots are visible on the bottom side of the device, which are used for wall-mounting the router. The distance between the two slots is 86mm.
2. Please search for two suitable screws and fix them to the wall through screw anchors. Note that the wall-mounted slots of the router must be aligned with these two screws.



3. With the screws installed, the device can be slotted into place.

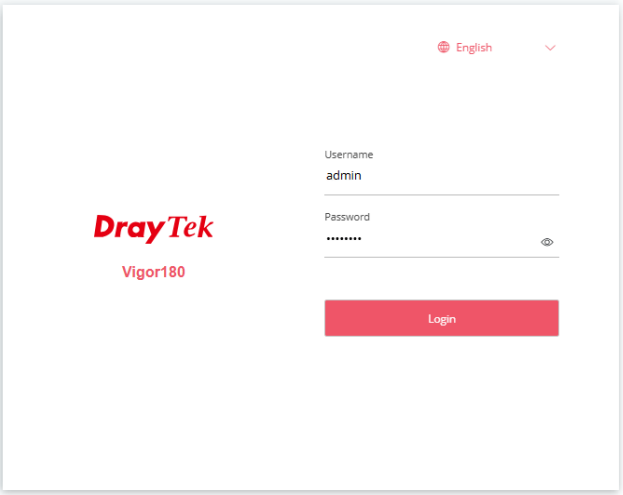
Note

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

I-3 Accessing to Web User Interface

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

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

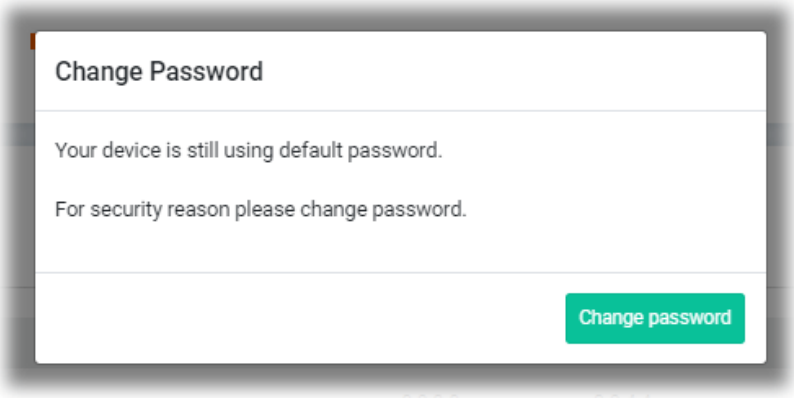


Note:

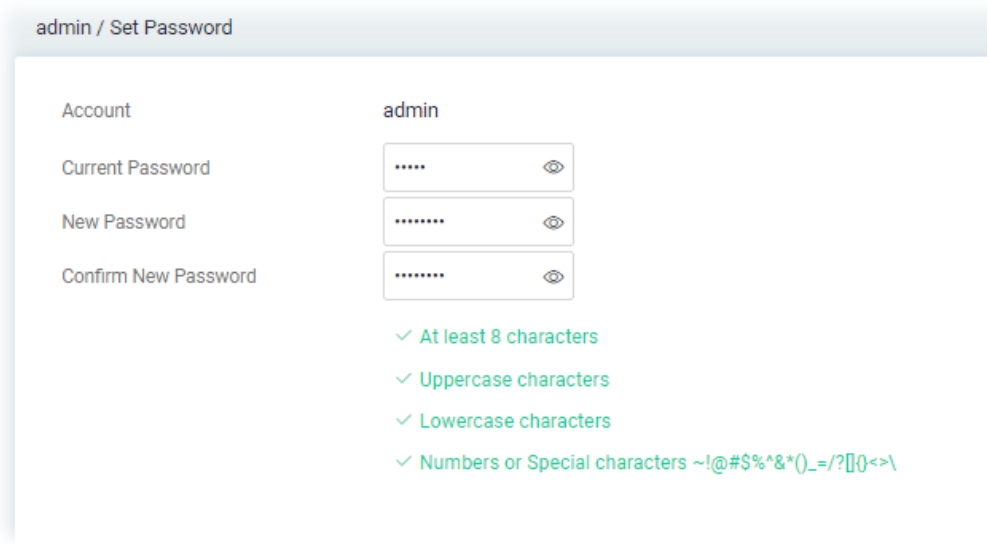
You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**.

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

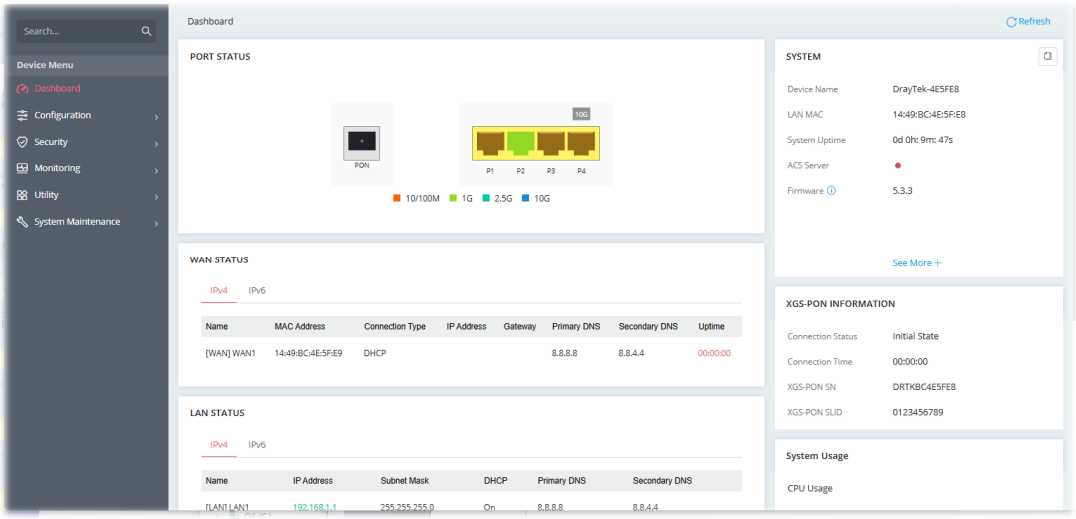
3. Next, the page will appear to guide you change the login password.



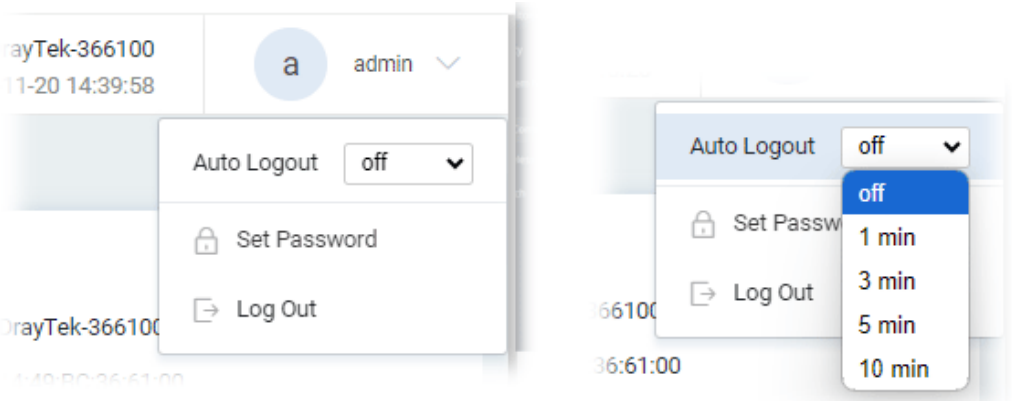
4. You **MUST** change the login password before accessing the web user interface. Please set a new password for network security.



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.



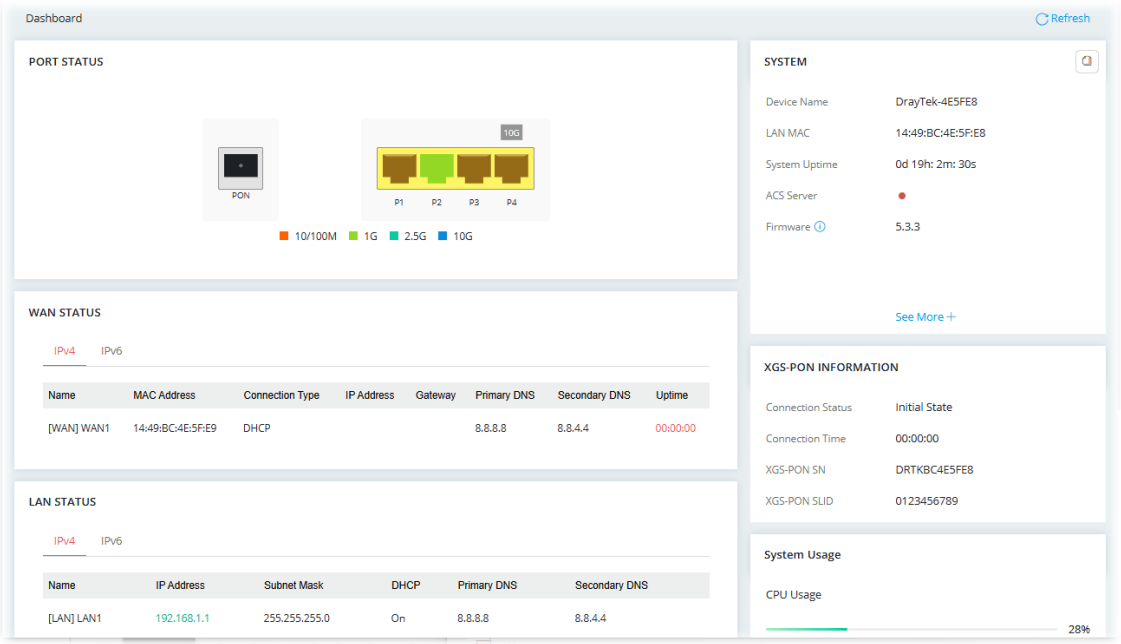
Note:

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.



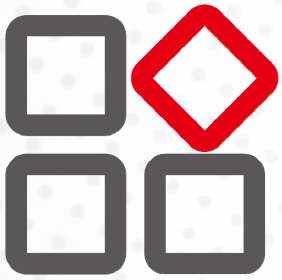
Note:

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

 - means “Enable”.

 - means “Disable”.

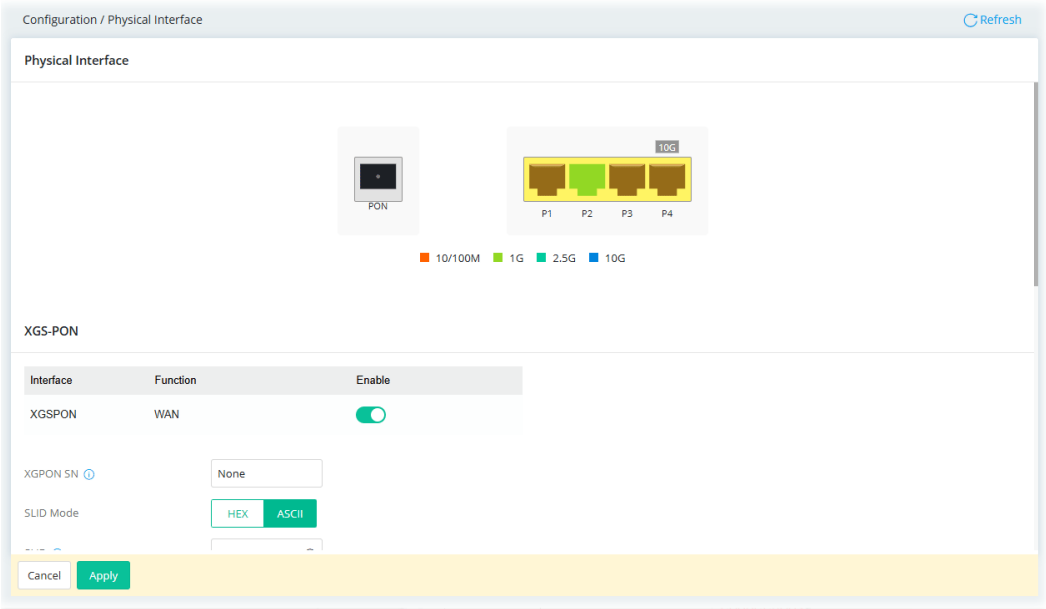
Chapter II Connectivity



II-1 Configuration

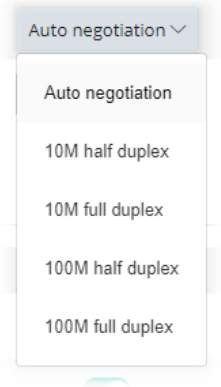
II-1-1 Physical Interface

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



Available settings are explained as follows:

Item	Description
	XGS-PON
Interface	Displays the available interfaces of this device.
Function	Displays the type (WAN) of the interface.
Enable	Switch the toggle to enable or disable the interface.
XGSPON SN	Enter the serial number, obtained from ISP, used by the ONT/ONU (Optical Network Terminal/ Optical Network Unit) to authenticate with the OLT (Optical Line Terminal) in the GPON/XGS-PON network.
SLID	Enter the subscriber line identifier (SLID) assigned by the service provider for ONT/ONU authentication.
Enable OMCI Auto Config	Switch the toggle to enable or disable automatic configuration via OMCI (ONT Management and Control Interface). When enabled, the OLT automatically provisions and manages the ONT/ONU configuration.
Broadcast XGS-PON Status to LAN	Switch the toggle to enable or disable this feature. When enabled, the XGS-PON status is broadcast to devices connected to the LAN ports.
	Ethernet
Interface	Displays the available interfaces of this device.

Function	Displays the type (LAN) of the interface.
Enable	Switch the toggle to enable or disable the interface.
Speed	Set the port speed capabilities for each interface.  Port speed capabilities: **Auto negotiation -** Auto speed with all capabilities. **10M half duplex -** Force speed with 10M ability. **10M full duplex -** Force speed with 10M ability. **100M half duplex -** Force speed with 100M ability. **100M full duplex -** Force speed with 100M ability. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Button	
Interface	Displays the available buttons (Configuration Reset Button) of this device.
Enable	Switch the toggle to enable or disable the function of the buttons.

Note:

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

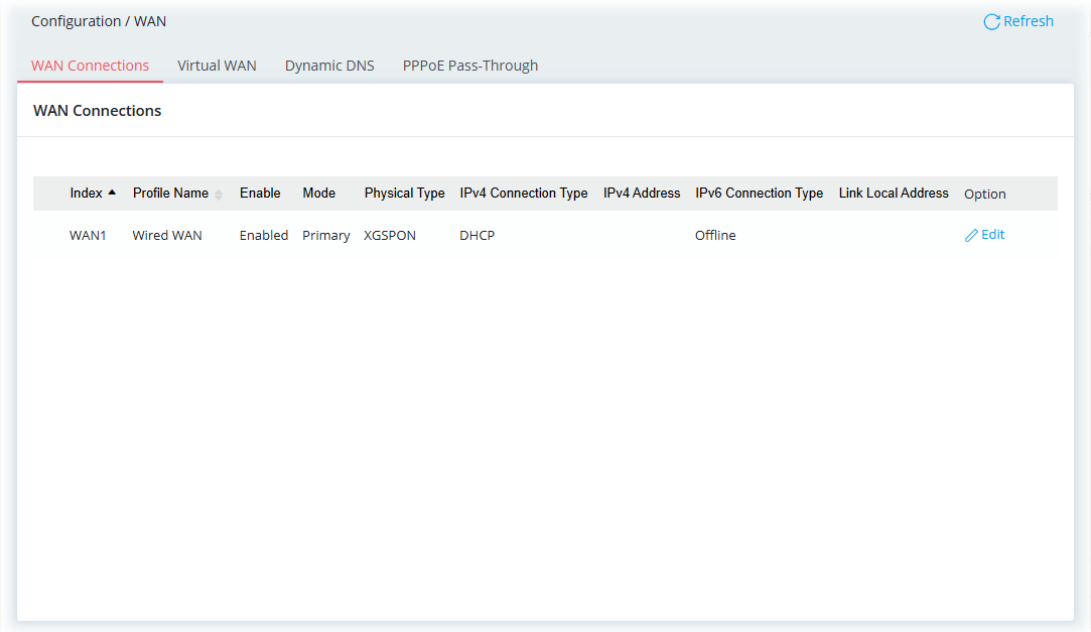
 - means "Enable".

 - means "Disable".

II-1-2 WAN

II-1-2-1 WAN Connections

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

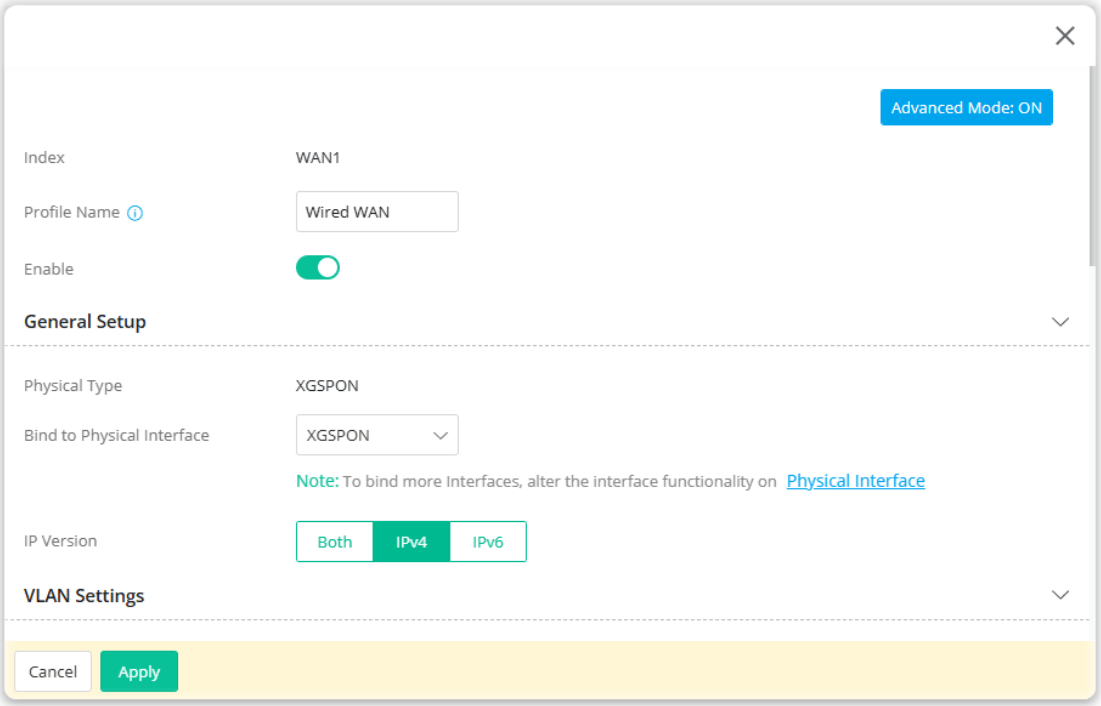


Available settings are explained as follows:

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

For static IP access mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

Click the **Edit** link for WAN1 to open the following page.



Available settings are explained as follows:

Item	Description
Advanced Mode:ON/OFF	Click to show or hide the advanced settings (IP Alias and WAN MAC Address) for the WAN interface.
Index	Displays current WAN interface.
Profile Name	Displays the name of the profile.
Enable	Switch the toggle to enable or disable the function.
General Setup	
Physical Type	Displays the physical type used by this interface.
Bind to Physical Interface	Displays the port number.
IP Version	Set the protocol (IPv4 or IPv6 or both) that this WAN interface used.
VLAN Settings	
Customer VLAN	Determines whether 802.1ad VLAN tags will be added to outbound WAN traffic in ADSL 2 mode. Check with your ISP to determine if this is required, and if so, the proper tag and priority values to be used. Switch the toggle to enable or disable 802.1Q VLAN tagging for the WAN connection. When enabled, the WAN traffic will be tagged with the specified VLAN ID, which is often required by the ISP for internet connectivity.

	Tag - Enter the VLAN ID number required by your ISP. The range is from 1 to 4094. **Priority** - Enter the 802.1p packet priority number. The range is from 0 to 7.
Service VLAN	Switch the toggle to enable or disable Service VLAN (QinQ) tagging. When enabled, the device adds an outer VLAN tag (S-TAG) on top of the Customer VLAN tag, encapsulating traffic for ISP or upstream carrier network transport. **Tag** - Enter the Service VLAN ID number. The range is from 1 to 4094 **Priority** - Enter the packet priority number for the Service VLAN. The range is from 0 to 7.
IPv4	
IPv4 Connection Type	It is available when Both or IPv4 is selected as IP Version. **PPPoE** – Set the access mode as PPPoE. • **Username** – Username provided by the ISP for PPPoE authentication. • **Password** – Password provided by the ISP for PPPoE authentication. • **Service Name –** PPP service name tag. Required by some ISPs. Leave blank unless instructed otherwise by your ISP. This feature is available only when Advanced Mode is activated. • **PPP Authentication –** The protocol used for PPP authentication. **PAP or CHAP**- Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. This feature is available only when Advanced Mode is activated. • **IP Assignment –**This feature is available only when Advanced Mode is activated. It is available when PPPoE is selected as IPv4 Connection Type. **DHCP** - WAN IP address is dynamically allocated. **Static IP** - ISP has assigned a fixed WAN IP address. Enter an IP address. • **WAN DNS** – Select **Auto** or **Manual**. If Manual is selected, specify the primary and secondary DNS servers. **IPv4 Primary DNS** –IP address of primary DNS server. **IPv4 Secondary DNS** - IP address of secondary DNS server. **DHCP** – The router receives IP configuration information from a DHCP server. • **WAN DNS** – Select **Auto** or **Manual**. If Manual is selected, specify the primary and secondary DNS servers. **IPv4 Primary DNS** –IP address of primary DNS server. **IPv4 Secondary DNS** - IP address of secondary DNS server. **Static IP** – Set the access mode as Static IP. • **IP Address** – WAN IP address assigned by the ISP. • **Subnet Mask** – WAN subnet mask. • **Gateway IP** – IP address of the WAN Gateway. • **IPv4 Primary DNS** –IP address of primary DNS server.

	• **IPv4 Secondary DNS** - IP address of secondary DNS server. **Outbound DNS Query IP -** This feature is available only when Advanced Mode is activated. Specify the source IP address which will be used by the router to send out the DNS query. • **Default IP –** The query IP is set by Vigor router automatically. • **Alias IP –** Enter a user-defined IP for DNS query.
WAN Connection Detection	
Mode	Configures how the WAN connection is monitored. **Always On -** The router assumes the WAN connection is always active. **ARP Detect** - The router broadcasts an ARP request every 5 seconds. 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 based on the ping interval setting to the host, whose address is specified in the Ping Gateway IP field, to verify the WAN connection. If the remote host does not respond within certain seconds (defined in the ping interval), the WAN connection is deemed to have failed. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. • **Ping Gateway IP** - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. • **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255. • **Ping Interval (Sec, 10-3600)** – Enter the interval for the system to execute the PING operation. • **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
IP Alias	**IPv4 Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. **+Add** – Click to add an IPv4 address as the IPv4 alias.
IPv6	
IPv6 Connection Type	It is available when Both or IPv6 is selected as IP Version. **Offline** – When Offline is selected, the IPv6 connection will be disabled. • **WAN DNS** – Select **Auto** or **Manual**. If Manual is selected, specify the primary and secondary DNS servers. **IPv6 Primary DNS** –IP address of primary DNS server. **IPv6 Secondary DNS** - IP address of secondary DNS server. **PPP** – IPv6 WAN address is assigned along with the IPv4 WAN address during PPPoE negotiation. This IPv6 access mode requires that the IPv4 uses PPPoE. • **WAN DNS** – Select **Auto** or **Manual**. If Manual is selected, specify the primary and secondary DNS

servers.

IPv6 Primary DNS – IP address of primary DNS server.

IPv6 Secondary DNS - IP address of secondary DNS server.

Static – Configure an ISP-assigned static IPv6 setup.

- **+Add** – Click it to add the values in the IPv6 Address and Prefix Length fields to the **Global Address Table**.
- **IPv6 Global Address** – WAN IPv6 address assigned by the ISP.
- **Prefix Length –** Length of the IPv6 prefix.
- **Gateway Address -** IPv6 address of the ISP gateway.
- **IPv6 Primary / Secondary DNS –** IPv6 address of primary / secondary DNS server.

DHCPv6 – Use DHCPv6 protocol to obtain IPv6 address from server.

- **DUID** – Displays the DHCP unique ID used by this WAN interface.
- **IAID** – Unique integer that identifies this WAN interface.
- **Authentication Protocol** - This protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, **Reconfigure Key**, **Delayed** and **None**.
  - **None** - In general, the default setting is None.
  - **Reconfigure Key** – During the connection process, DHCPv6 server will authenticate the client automatically.
  - **Delayed** - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields.
    Key ID – Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.
    Realm – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.
    Secret – Type a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.
- **WAN DNS** – Select **Auto** or **Manual**.

  If Manual is selected, specify the primary and secondary DNS servers.

  IPv6 Primary DNS – IP address of primary DNS server.

  IPv6 Secondary DNS - IP address of secondary DNS server.

TSPC - Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (http://gogonet.gogo6.com/page/freenet6-account) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.

- **Tunnel Broker Address** – Enter the address for the tunnel broker IP, FQDN or an optional port number.
- **Username** – It is suggested for you to apply another

	username and password for http://gogonet.gogo6.com/page/freenet6-account. • **Password** - Enter the password assigned with the user name. • **WAN DNS** – Select **Auto** or **Manual**. If Manual is selected, specify the primary and secondary DNS servers. **IPv6 Primary DNS** – IP address of primary DNS server. **IPv6 Secondary DNS** - IP address of secondary DNS server. **6in4** – Setup 6in4 Static Tunnel for WAN interface. However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than any cast endpoint. The mode has more reliability. • **Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel** – To use this 6in4 connection type, IPv4 WAN access must be allowed, and the firewall must allow the Tunnel Broker IP address to pass through. • **Remote Endpoint IPv4 Address** – WAN IPv6 address assigned by the tunnel provider. • **6in4 IPv6 Address** – WAN IPv6 address assigned by the tunnel provider. • **6in4 IPv6 Prefix Length –** WAN IPv6 prefix length assigned by the tunnel provider. • **LAN Routed Prefix –** LAN IPv6 address prefix. • **LAN Routed Prefix Length –** LAN IPv6 address prefix length. • **Tunnel TTL –** Time to live value, which is the maximum number of hops allowed to the endpoint. • **WAN DNS** – Select **Auto** or **Manual**. If Manual is selected, specify the primary and secondary DNS servers. **IPv6 Primary DNS** – IP address of primary DNS server. **IPv6 Secondary DNS** - IP address of secondary DNS server. **6rd** - Setup 6rd for WAN interface. • **Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel** – To use this 6rd connection type, IPv4 WAN access must be allowed, and the firewall must allow the Tunnel Broker IP address to pass through. • **Mode** – Two options, Auto and Static. **Auto** - Used in conjunction with DHCPv4, the router automatically provisions IPv6 using option 212. **Static** - IPv6 configuration information is manually entered. • **IPv4 Border Relay** – Enter the IPv4 addresses of the 6rd Border Relay for a given 6rd domain. • **6rd Prefix** – Enter the 6rd IPv6 address. • **6rd Prefix Length** - Enter the IPv6 prefix length for the 6rd IPv6 prefix in number of bits. • **WAN DNS** – Select **Auto** or **Manual**. If Manual is selected, specify the primary and secondary DNS servers. **IPv6 Primary DNS** – IP address of primary DNS server. **IPv6 Secondary DNS** - IP address of secondary DNS server.
IPv6 WAN Connection Detection	

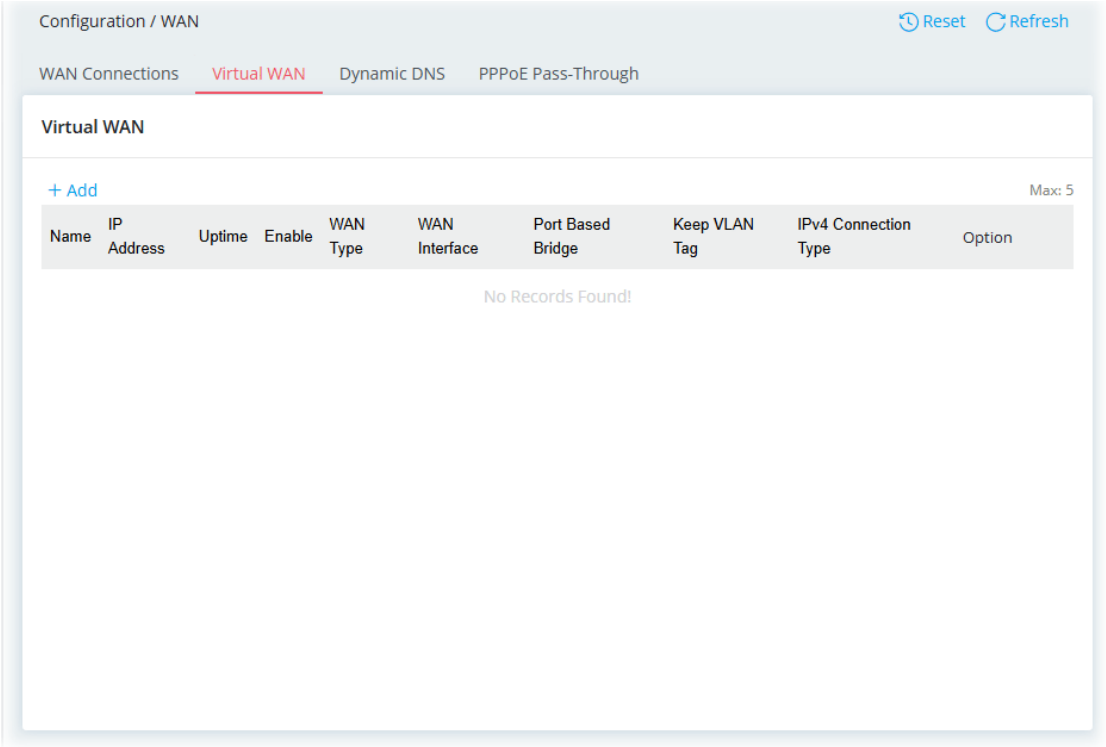
Mode	Configures how the WAN connection is monitored. **Always On -** The router assumes the WAN connection is always active. **NS Detect** - The router verifies connectivity by issuing Neighbor Solicitation packets. **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request based on the ping interval setting 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 certain seconds (defined in the ping interval), the WAN connection is deemed to have failed. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. • **Primary Ping IP** – Enter an IP address in this field for pinging. • **Secondary Ping IP** - Enter an IP address in this field for pinging. • **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255. • **Ping Interval (Sec, 10-3600)** – Enter the interval for the system to execute the PING operation. • **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	
MTU	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492.
WAN MAC Address	
Mode	This feature is available only when Advanced Mode is activated. **Default** – Use the default MAC address for the WAN port. **Customized** - Select this option if your ISP authenticates by MAC addresses. • **MAC** - Specify a MAC address for the WAN Ethernet port.
MAC	Displays the MAC address of this device.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

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

II-1-2-2 Virtual WAN

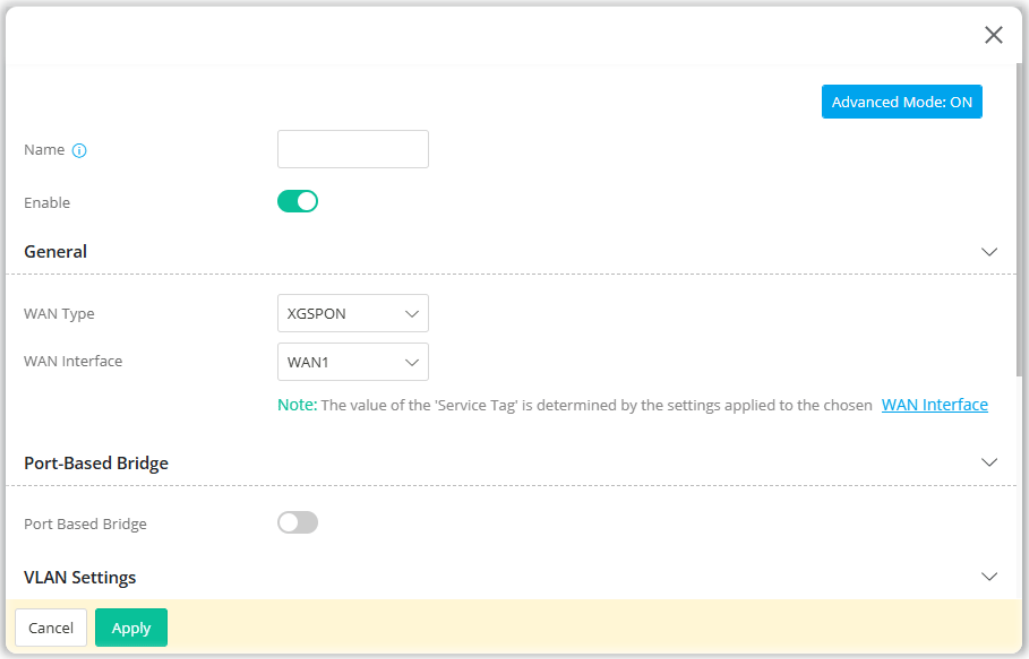
Up to five virtual WAN profiles can be set for applying to different applications.

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



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

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



Available settings are explained as follows:

Item	Description
Advanced Mode: ON/OFF	Click to show or hide the advanced settings for virtual WAN.
Name	Enter a name as the profile name.
Enable	Switch the toggle to enable or disable the function.
	General
WAN Type	Displays the type (e.g., XGSPON) of the physical interface.
WAN Interface	Select one of the available WAN interfaces (enabled on WAN>>WAN Connections).
	Port-Based Bridge
Port Based Bridge	Switch the toggle to enable or disable the function.
Binding Interface	Select an interface for binding
Keep VLAN Tag	Enable this function to keep the VLAN tag while in port-based bridge mode. Some IPTV environments may require it. It depends on the user environment to decide whether to enable it. Default is disabled.
Multicast Stream VLAN Trans	Switch the toggle to enable or disable the function. In some areas, the multicast VLAN tag value might be different from the IGMP VLAN tag. That might cause data transfer issues for IPTV packets flooding to other VLAN ports while watching the IPTV program. Configure the IGMP VLAN tag and the multicast VLAN tag with the same value if required. **Downstream Multicast VLAN Tag** – Enter the value for tagging the multicast packet. The range is from 0 to 4094. **Upstream IGMP VLAN Tag** – Enter the value for tagging the IGMP

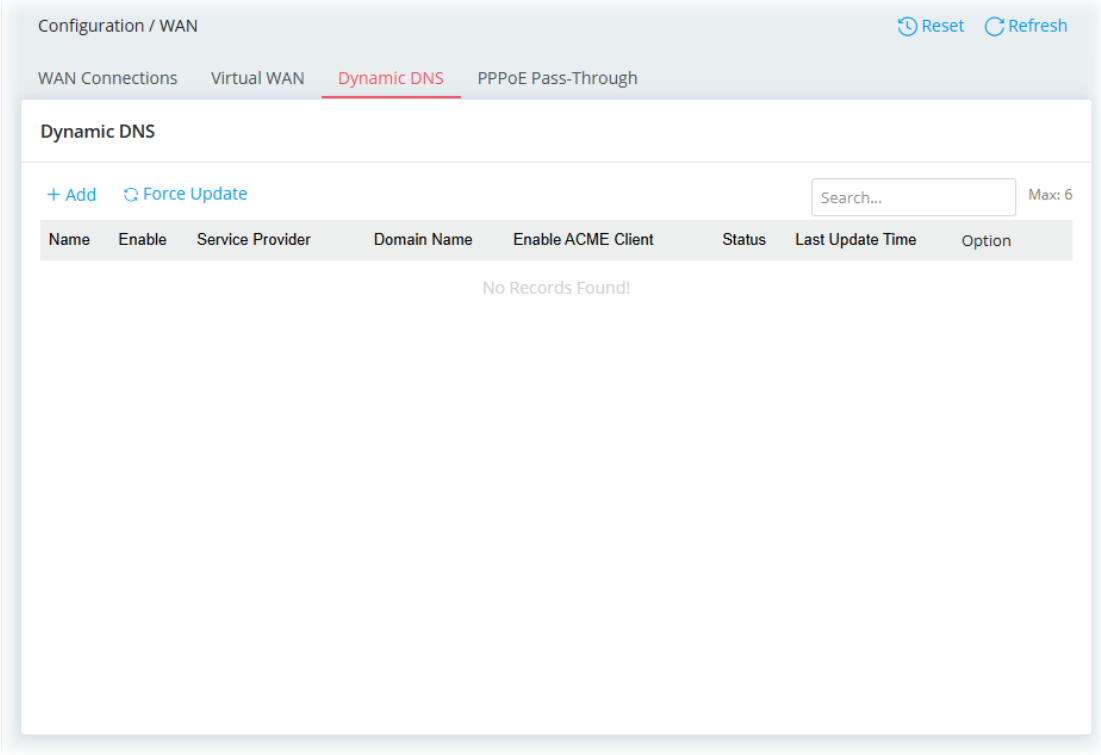
	packet. The range is from 0 to 4094.
VLAN Settings	
Customer VLAN	Determines whether 802.1ad VLAN tags will be added to outbound WAN traffic in ADSL 2 mode. Check with your ISP to determine if this is required, and if so, the proper tag and priority values to be used. Switch the toggle to enable or disable 802.1Q VLAN tagging for the WAN connection. When enabled, the WAN traffic will be tagged with the specified VLAN ID, which is often required by the ISP for internet connectivity. **Tag** - Enter the VLAN ID number required by your ISP. The range is from 1 to 4094. **Priority** - Enter the 802.1p packet priority number. The range is from 0 to 7.
IPv4	
IPv4 Connection Type	It is available if Port-Based Bridge is disabled. **PPPoE** – Set the access mode as PPPoE. • **Username** – Username provided by the ISP for PPPoE authentication. • **Password** – Password provided by the ISP for PPPoE authentication. • **PPP Authentication** – The protocol used for PPP authentication. **PAP or CHAP** - Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. • **IP Assignment** – It is available when PPPoE is selected as IPv4 Connection Type. **DHCP** - WAN IP address is dynamically allocated. **Static IP** - ISP has assigned a fixed WAN IP address. Enter an IP address. **DHCP** – The router receives IP configuration information from a DHCP server. • **Router Name (Optional)** – Used by some ISPs. Contact your ISP for the appropriate values. • **Domain Name (Optional)** - Used by some ISPs. Contact your ISP for the appropriate values. **Static IP** – Set the access mode as Static IP. • **IP Address** – WAN IP address assigned by the ISP. • **Subnet Mask** – WAN subnet mask. • **Gateway IP** – IP address of the WAN Gateway.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

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

II-1-2-3 Dynamic DNS

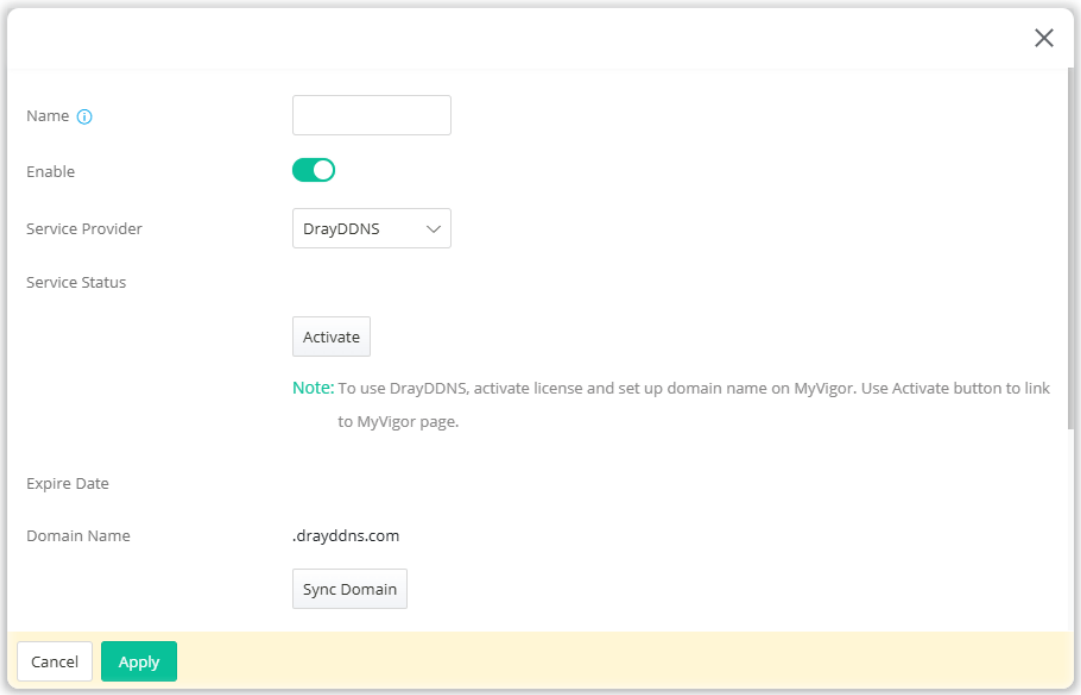
Most ISPs assigns dynamic WAN IP addresses to their customers. Dynamic IP addresses presents challenges to users who would like to accept remote connections to their LANs from the Internet, as service could be disrupted due to the IP address changing without notice. By setting up service with a Dynamic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



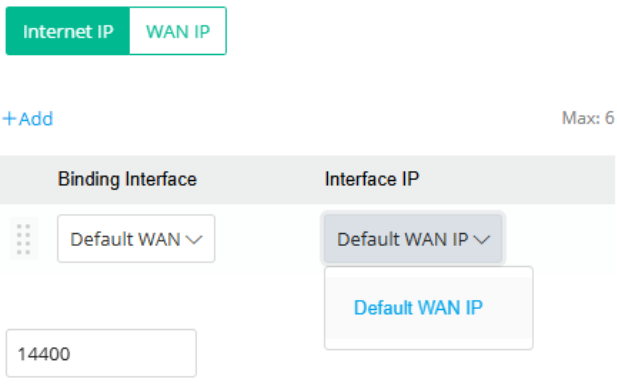
Item	Description
Reset	Click to clear all profiles to factory settings.
+Add	Click to bring up the configuration page of the DDNS profile (max. 6).
Force Update	Click to connect immediately to DDNS servers to update IP address information.

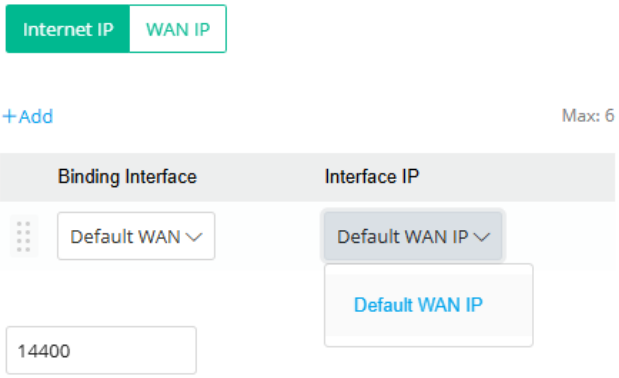
To add a new DDNS profile, click the **+Add** link to get the following page.



Available settings are explained as follows:

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

	Password - Enter the password of the DDNS account. **Auth Type** –Two types can be used for authentication. ● **Basic** – Username and password defined later can be shown from the packets captured. ● **URL** - Username and password defined later can be shown in URL.
Enable ACME Client	Switch the toggle to generate a certificate issued by Let's Encrypt for applying to such DDNS account.
	More settings
Update DDNS with	If a Vigor router is installed behind any NAT router, you can enable this function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: **Internet IP** –The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address. **WAN IP** – The IP address of the router's WAN interface will be used. **+Add** – Click to add IP address (up to six). ● **Binding Interface** – Select an interface (WAN1 to WAN6) for traffic passing through. Up to six interfaces can be defined. ● **Interface IP** – If there is any IP alias configured before, available item(s) will be shown in this field. The first IP listed in the Binding Interface is the default IP. Select one of the items to match the binding interface. 
Update WAN IP Mode	It is available when **DrayDDNS** is set as the Service Provider. **Update All Selected WAN IPs** – The Vigor router system will update all selected WAN IPs. **Update Single WAN IP by Sequence** – The Vigor router system will update the WAN IP in sequence. **+Add** – Click to add IP address (up to six). ● **Binding Interface** – Select an interface (WAN1 to WAN6) for traffic passing through. Up to six interfaces can be defined. ● **Interface IP** – If there is any IP alias configured before, available item(s) will be shown in this field. The first IP listed in the Binding Interface is the default IP. Select one of the items to match the binding interface.

	
Protocol	Select the IP type (IPv4 or IPv6, or Any) of the IP address that would be used for answering to the DDNS service provider.
Auto Update Interval	The frequency, in minutes, at which the router connects to DDNS servers to update IP address information. The default is 14400.
Cancel	Discard current settings and return to previous page.
Apply	Save the current settings and exit the page.

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

DrayDDNS Settings

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

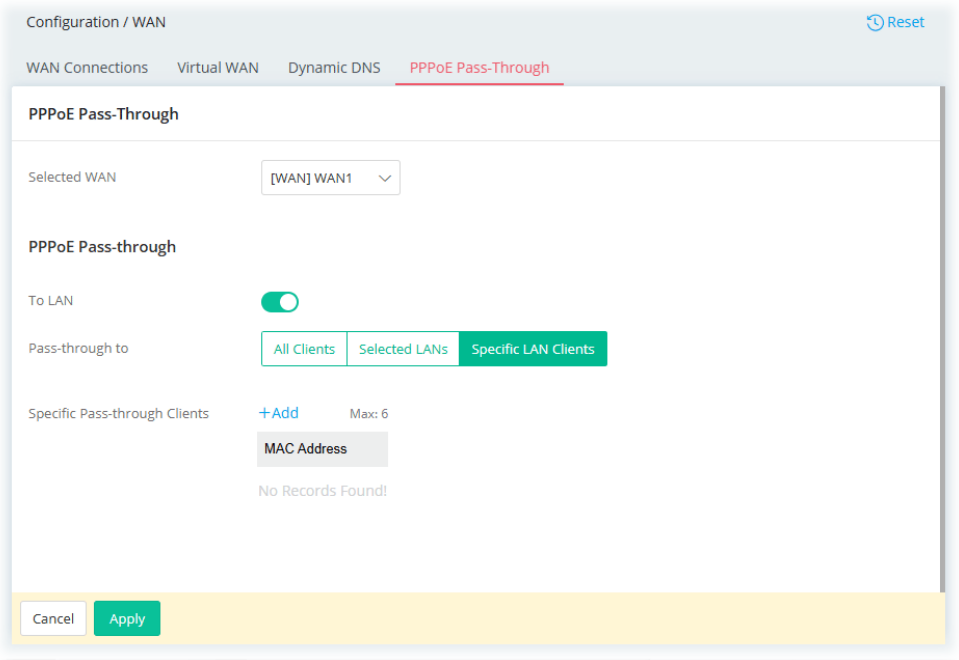
DDNS updates take place when:

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

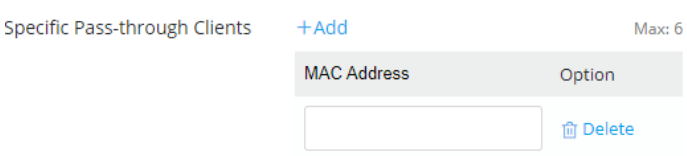
II-1-2-4 PPPoE Pass Through

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

Thus, the PC can access Internet through such direction.



Available settings are explained as follows:

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

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

II-1-3 LAN

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

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

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

IP Address

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

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

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

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

Name	IP Address Range	Number of Available Addresses	Largest Subnet Mask
24-bit Block	10.0.0.0 to 10.255.255.255	16,777,216	255.0.0.0
20-bit Block	172.16.0.0 to 172.31.255.255	1,048,576	255.240.0.0
16-bit Block	192.168.0.0 to 192.168.255.255	65,536	255.255.0.0

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

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

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

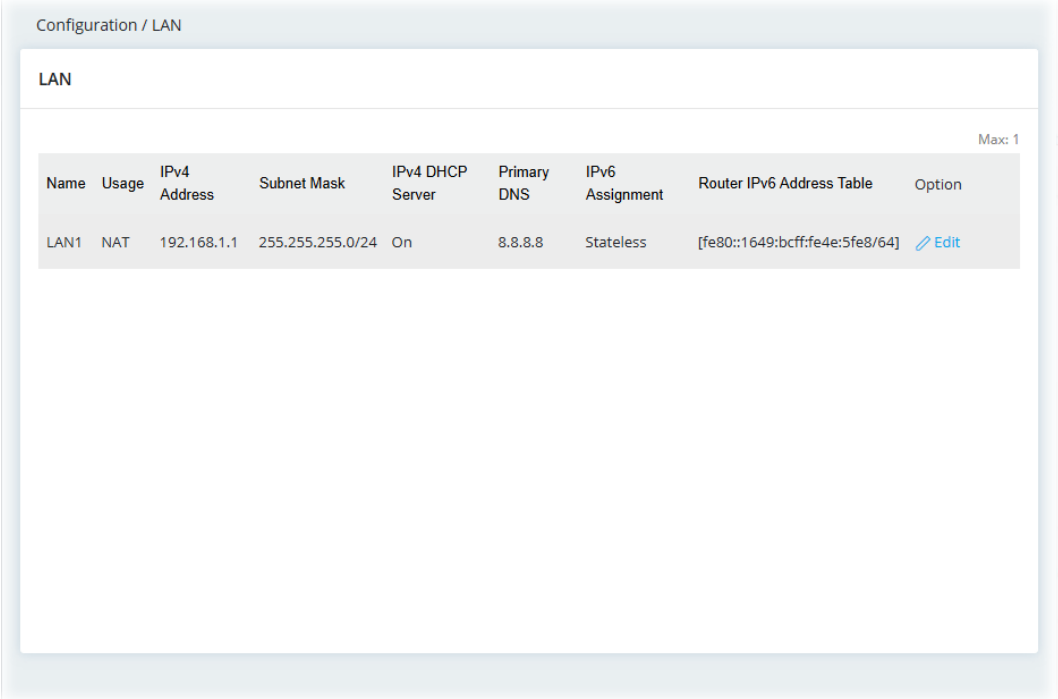
Alternatively, static IP addresses can be manually configured on LAN clients as part of their network settings. No matter how IP addresses are configured, it is important that no two devices get the same IP address. If both DHCP and static assignment are used on a network, it is important to exclude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

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

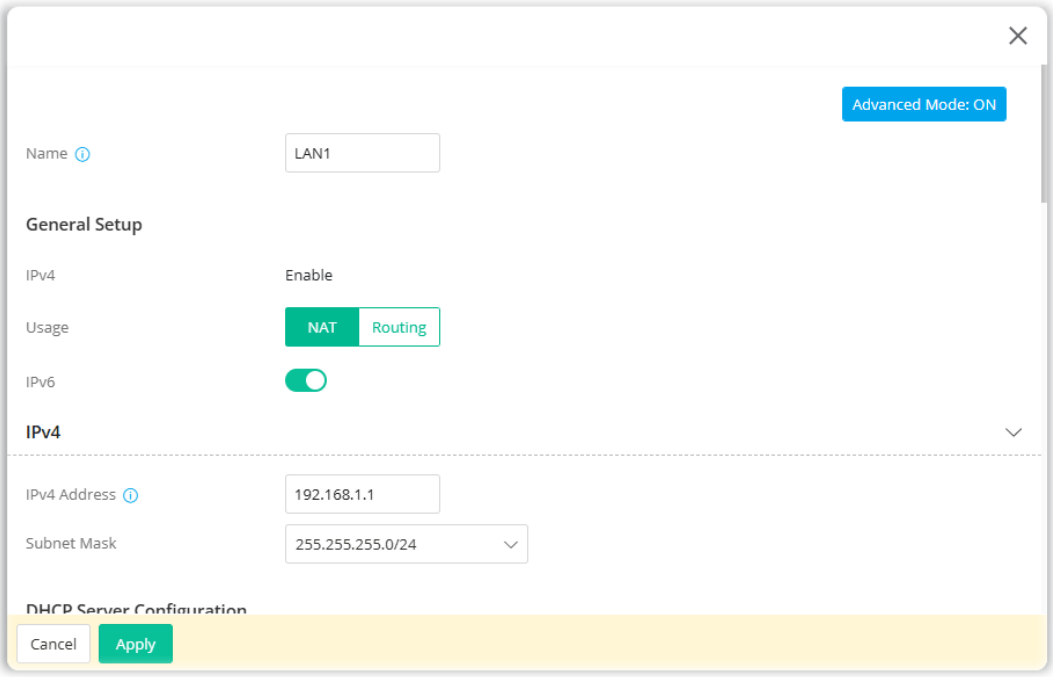
II-1-3-1 LANs

This page provides you the general settings for LAN.

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



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



Available settings are explained as follows:

Item	Description

Advanced Mode: ON/OFF	Click to show or hide the advanced settings for LAN.
Name	Display the name for identification. Change the name if required.
	General Setup
IPv4	Display the status (enable/disable) of the profile.
Usage	Select the IP forwarding method. • **NAT** • **Routing**
IPv6	Switch the toggle to configure / ignore the IPv6 settings.
	IPv4
IPv4 Address	This is the IP address of the LAN interface (default: 192.168.1.1).
Subnet Mask	Select a subnet mask of the LAN interface.
	DHCP Server Configuration
IPv4 DHCP Server	LAN1 is configured with DHCP in default. DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP 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 100. Valid range is between 1 and 253. **Gateway IP Address** - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router. **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. **Primary DNS** - DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. **Secondary DNS** - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.
If Relay is selected as	When selected, all DHCP requests are forwarded to a DHCP server

DHCP Server	outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field. **Primary DNS** - DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. **Secondary DNS** - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. **DHCP Relay over WAN (Primary)** – Switch the toggle to enable this function. Then, specify a WAN interface for the first DHCP Server. • **Primary DHCP Server Interface** – Use the drop-down list to choose a WAN interface for the first DHCP Server. **Primary DHCP Server IP Address** - Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded. **DHCP Relay over WAN (Secondary)** - The secondary DHCP server is an optional setting. If required, specify a WAN interface for the second DHCP Server as a backup server. • **Secondary DHCP Server Interface** – Use the drop-down list to choose a WAN interface for the second DHCP Server. **Secondary DHCP Server IP Address** - Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded.
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.
DHCPv6 Server Configuration	It is available when DHCPv6 (Stateful) is selected as the IPv6 Assignment. **On** - Enables the built-in DHCPv6 server on the router. • **Generate Prefix From** – Select the primary WAN interface which is capable to generate the prefix for IPv6 address. Use the drop down list to specify a WAN interface for IPv6. • **Auto IPv6 Address Range** • **Random IPv6 Address Allocation** **Off** - Disables the built-in DHCPv6 server on the router. **Relay** - When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field. • **DHCPv6 Server Interface** – Use the drop down list to specify a WAN interface for IPv6. • **DHCPv6 Server Address** - Enter the IPv6 address of the DHCPv6 server.
DNS Configuration	It is available when DHCPv6 (Stateful) is selected as the IPv6 Assignment. **Primary DNS Address** - Enter the IPv6 address for Primary DNS server. **Secondary DNS Address** - Enter another IPv6 address for DNS server if required.
More Settings	
Force DNS Redirection	Switch the toggle to enable or disable the function. This function allows all outgoing DNS queries to be intercepted and redirected to the router built-in DNS server, improving the domain lookup performance by caching DNS queries and results.
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. **Prefix Length** - Enter the IPv6 prefix length for the IPv6 address.
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, and

	High) of the router sent in route advertisement messages. **Min / Max Interval Time** – Minimum/ Maximum time, in seconds, between unsolicited multicast route advertisement messages sent by the RA server. **Valid Lifetime** – Enter one number (unit is second) to specify the valid lifetime for the DHCPv6 server. The device (connected via the LAN interface) is to be used as the default router. This device (connected via the LAN interface) will be treated as the default router within the valid lifetime. **Preferred Lifetime** – Enter one number (unit is second) to specify the preferred lifetime for the DHCPv6 server. It must be lower or equal to the valid lifetime. This device (Vigor router) will be treated as the default router within the preferred lifetime. When there are multiple routers, priority is necessary. In general, the router within the preferred lifetime has higher priority than the router within the valid lifetime. **Hop Limit** - The value is required for the device behind the router when IPv6 is in use. Default value of hop limit field in Route Advertisement messages.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-1-4 Routing

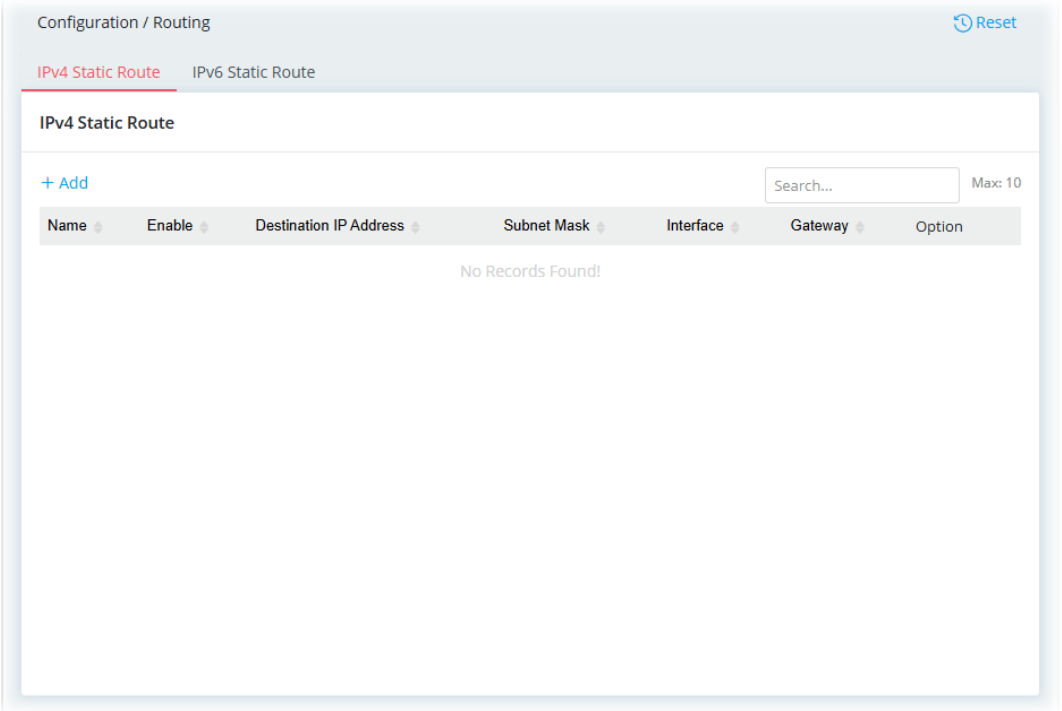
Through the IP address and interface configuration, a route policy can be used to configure any routing rules to fit actual requests.

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

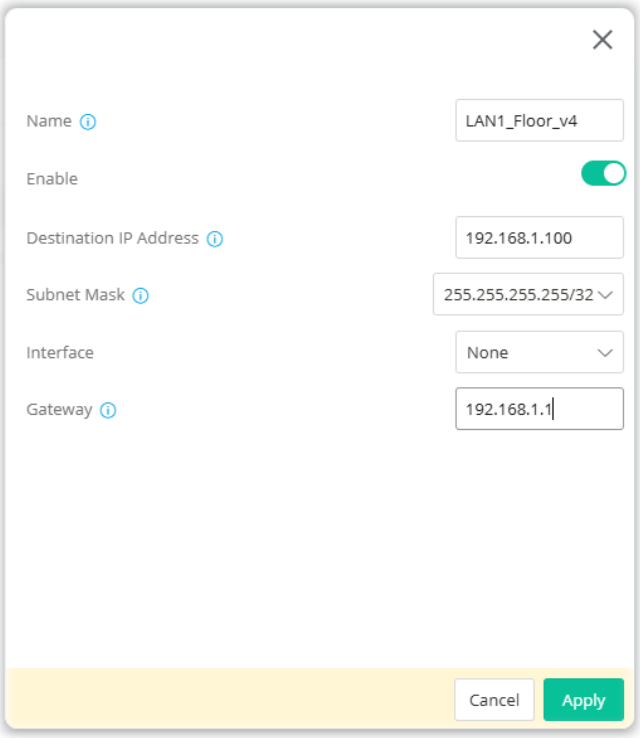
The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

II-1-4-1 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:

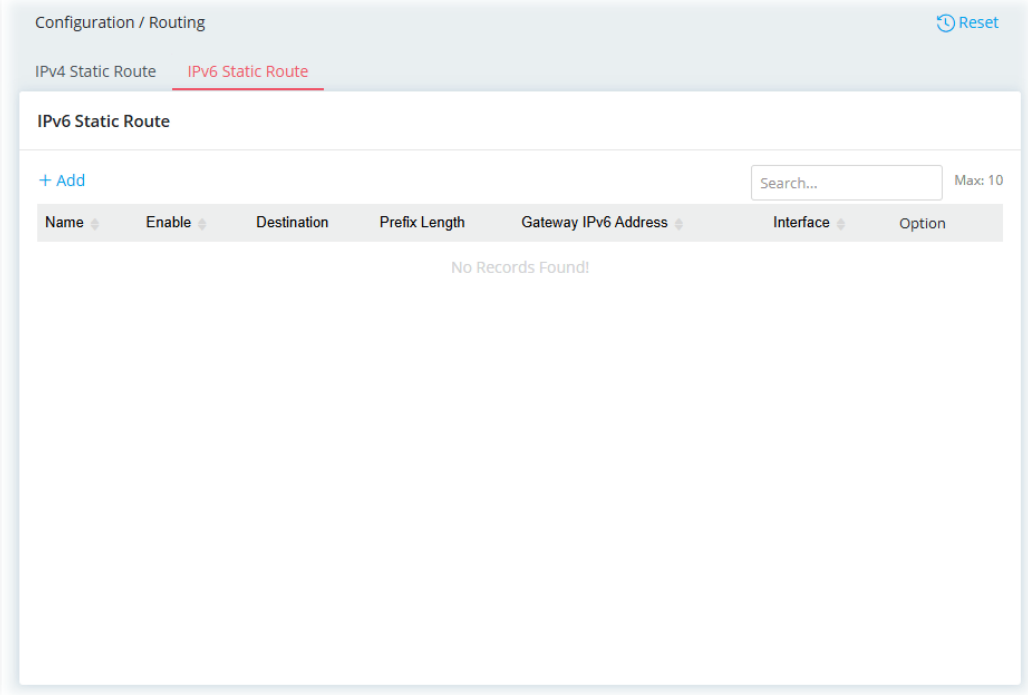
Item	Description
Name	Enter a name as the profile name.
Enable	Switch the toggle to enable or disable the function.
Destination IP Address	Enter the IP address as the destination IP address.

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.

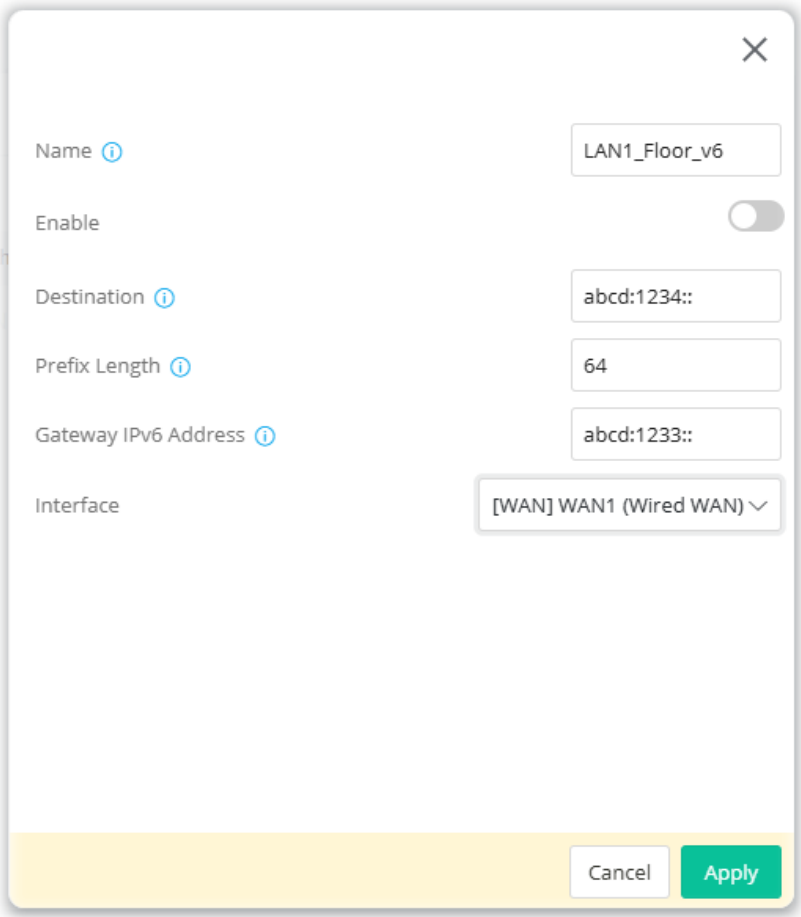
After finishing this web page configuration, please click **Apply** to save the settings.

II-1-4-2 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.
Enable	Switch the toggle to enable or disable the function.
Destination	Enter the IPv6 address as the destination IP address.
Prefix Length	Enter the fixed value for prefix length.
Gateway IPv6 Address	Enter an IPv6 address as the gateway.
Interface	Use the drop-down list to specify an interface for this static route.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-1-5 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.

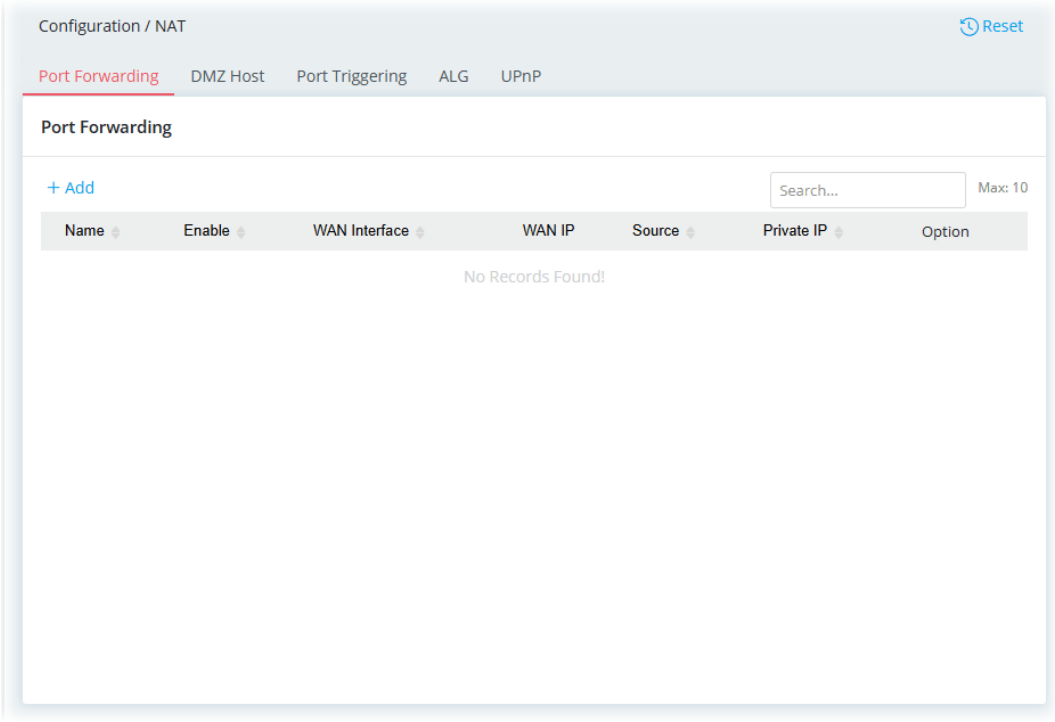
The benefit of the NAT includes:

- **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.

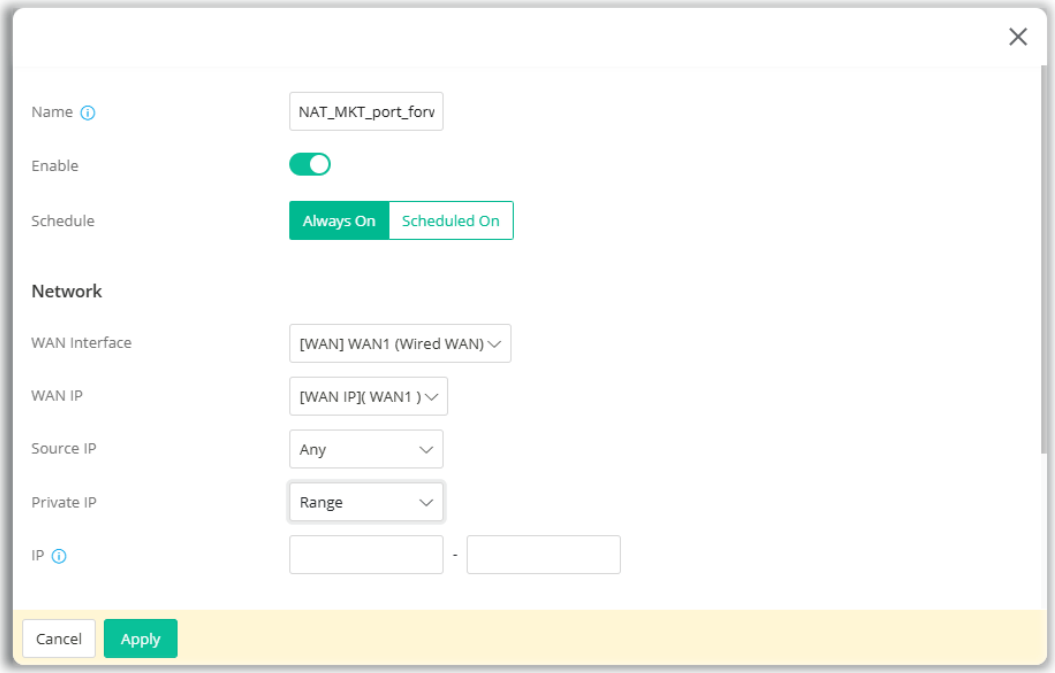
II-1-5-1 Port Forwarding

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 forwarding policy, click the **+Add** link to get the following page.

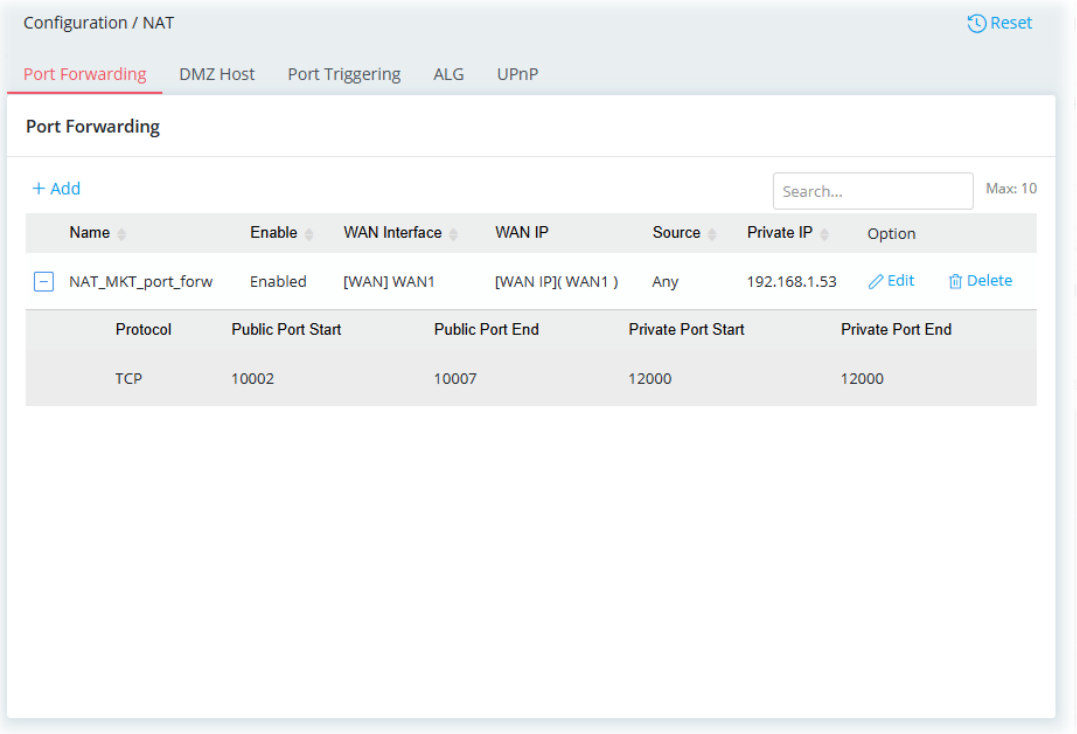


Available settings are explained as follows:

Item	Description
Name	Enter a name that identifies the rule.
Enable	Switch the toggle to enable or disable the function.
Schedule	Vigor router can perform the port forwarding all the time or on a certain date and time. **Always On -** The function of port triggering is running all the time. **Scheduled On -** The function of port triggering is activated based on the schedule profile.
	Network
WAN Interface	The WAN port(s) whose incoming traffic will be forwarded to a LAN client. Select from a specific WAN interface WAN# to apply the rule to the WAN interface.
WAN IP	Select a WAN IP to match 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** – The data traffic coming from IPs within the IP objects will be forwarded to a LAN client. • **IP Object** – Use the drop down list to specify an IP object profile. **IP Group** – The data traffic coming from IP objects within the IP groups will be forwarded to a LAN client. • **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

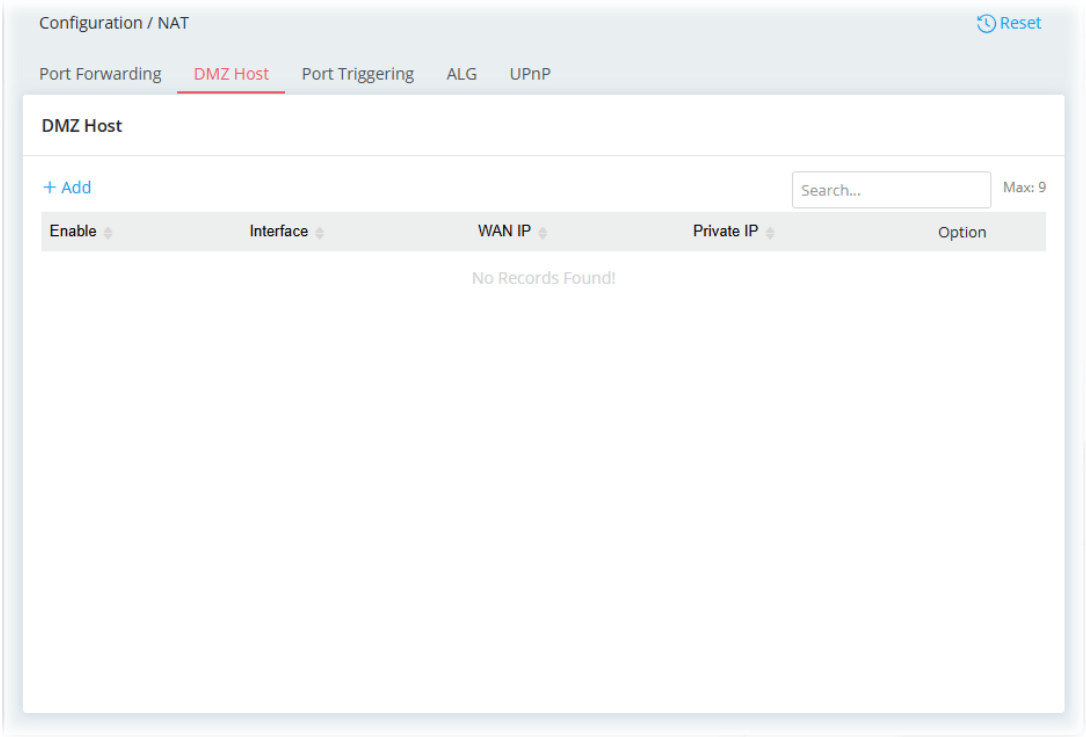
	forwarded traffic. **Range** – Specify a range of destination LAN IP addresses that will receive the forwarded traffic.
	Port Forwarding
+Add	Click to set port numbers for the specified protocol (TCP, UDP, or TCP/UDP) for a port forwarding profile.
Protocol	The protocol to which this rule applies, TCP, 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.
Option	Click **Delete** to remove the selected entry.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

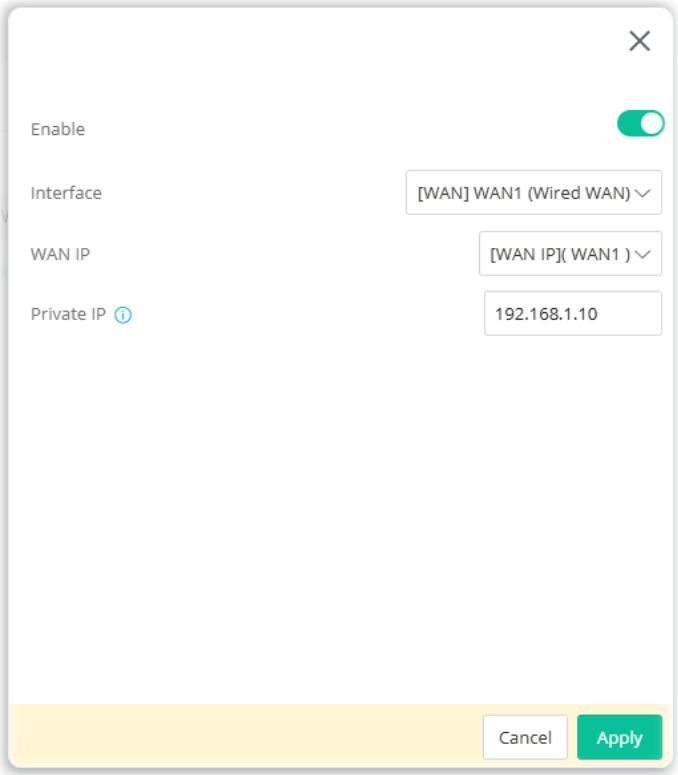


II-1-5-2 DMZ Host

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



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



Available settings are explained as follows:

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

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

II-1-5-3 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.

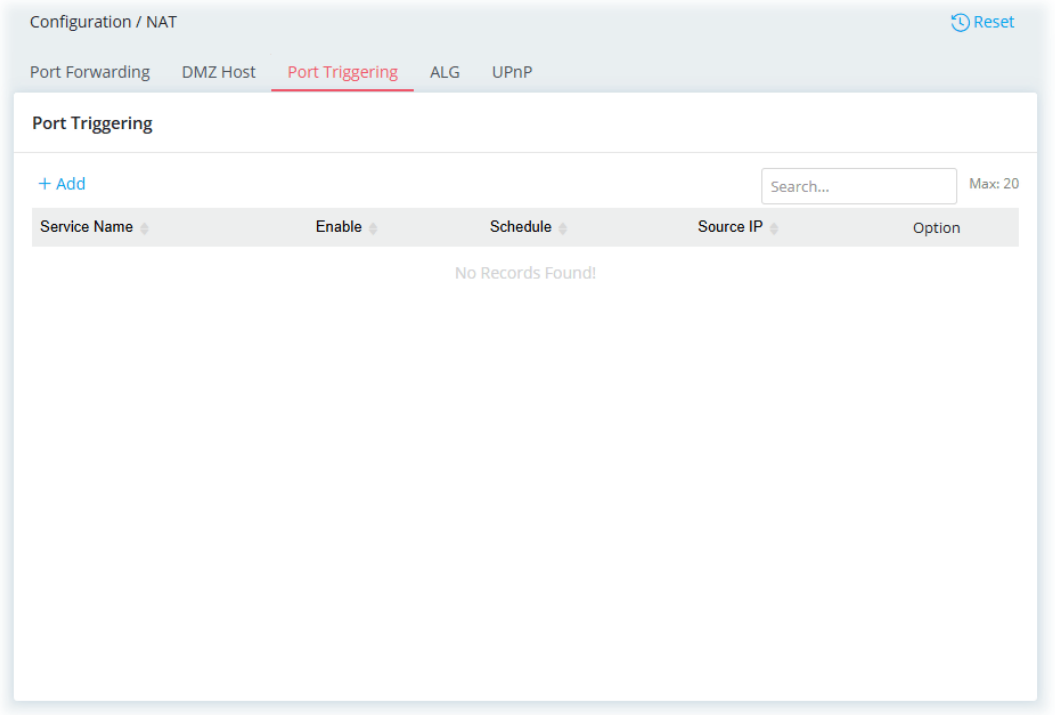
TCP: 86400 sec.

UDP: 180 sec.

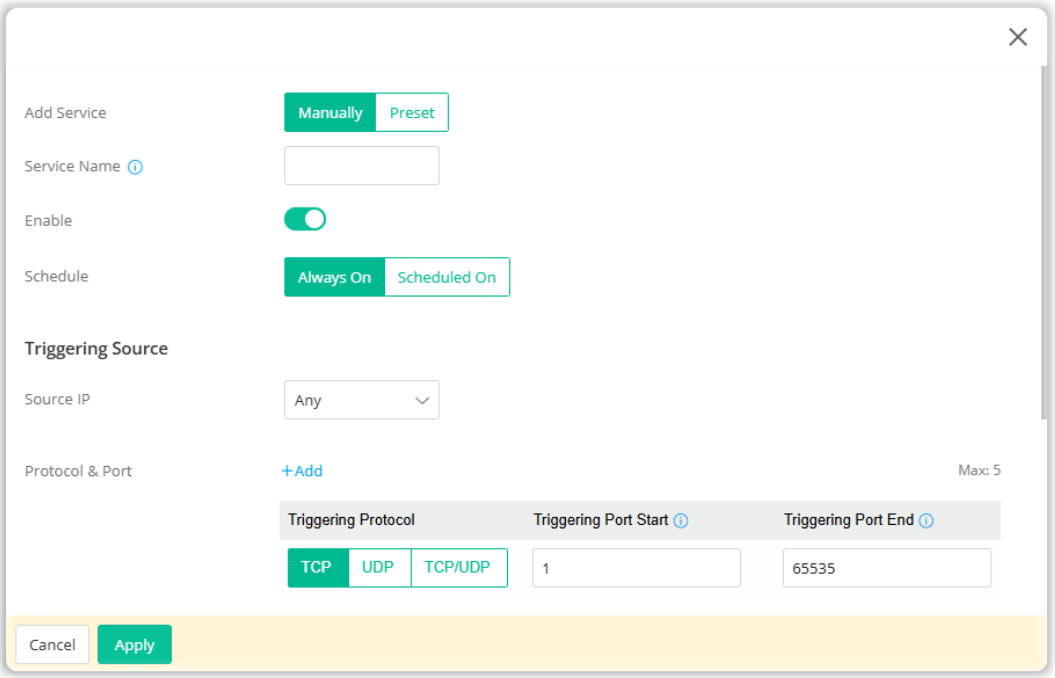
IGMP: 10 sec.

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. • **Service Name** – Enter the name of the service. **Preset -** If selected, various services will be offered for you to choose as the service name.

	• **Service Name** – Use the drop-down list to specify one service.
Enable	Switch the toggle to enable or disable the function of port triggering.
Schedule	Vigor router can perform the port triggering all the time or on a certain date and time. **Always On -** The function of port triggering is running all the time. **Scheduled On -** The function of port triggering is activated based on the selected schedule profile.
	Triggering Source
Source IP	**Any -** Any source IP will be forwarded to a LAN. **IP Address** - Set a range of IP addresses forwarded to a LAN. • **IP Address** – Enter the IP address and the subnet mask. **IP Object** – Click **+Add** to specify the IP object profile (up to 12 profiles). **IP Group** - Click **+Add** to specify the IP group profile (up to 12 profiles).
Protocol & Port	**+Add** - Click to set the port numbers (start and end) for the specified protocol (TCP, UDP or TCP/UDP) for the outgoing data (that this rule monitors). **Triggering Protocol -** The protocol(s) of the outgoing traffic. • **TCP** - open port(s) to TCP traffic. • **UDP** - open port(s) to UDP traffic. • **TCP/UDP** - open port(s) to both TCP and UDP traffic. Select the protocol (TCP, UDP or TCP/UDP) for the outgoing data of such triggering profile. **Triggering Port Start / Triggering Port End** - Outgoing traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule. Enter the port or port range for the outgoing packets.
	Incoming Services
Protocol & Port	**+Add -** Click to set port numbers (start and end) for the specified protocol (TCP, UDP or TCP/UDP) for the incoming data. **Incoming Protocol -** The protocol(s) of the incoming traffic. • **TCP** - open port(s) to TCP traffic. • **UDP** - open port(s) to UDP traffic. • **TCP/UDP** - open port(s) to both TCP and UDP traffic. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile. **Incoming Port Start / Incoming Port End** - Incoming traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule. Enter the port or port range for the incoming packets.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

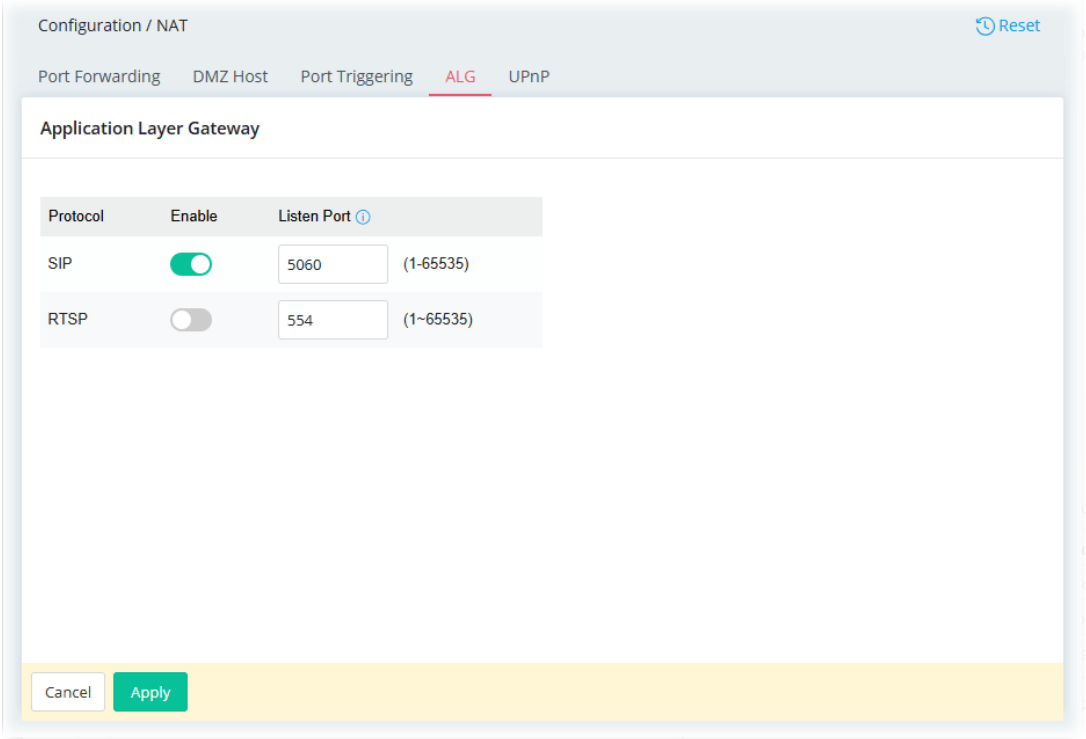
After finishing this web page configuration, please click **Apply** to save the settings.

II-1-5-4 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 the voice and the video.

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

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



Available settings are explained as follows:

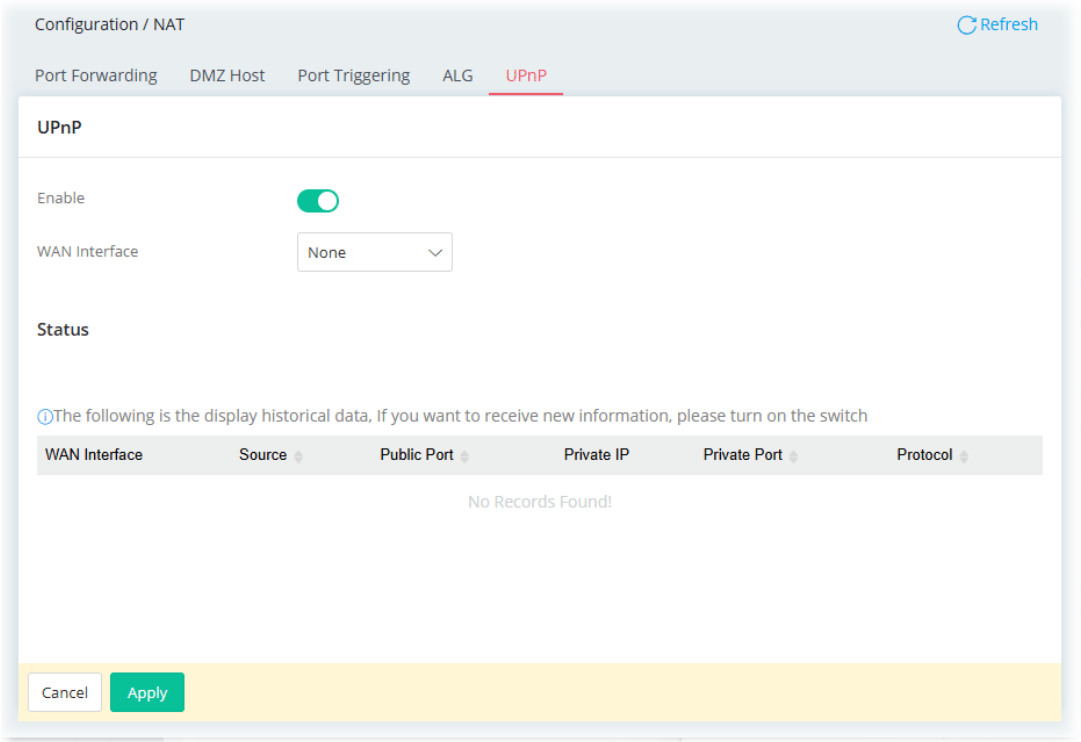
Item	Description
Enable	Switch the toggle to enable or disable the function.
Listen Port	Enter a port number for SIP or RTSP protocol.
Apply	Save the current settings and exit the page.

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

II-1-5-5 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
Enable	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.

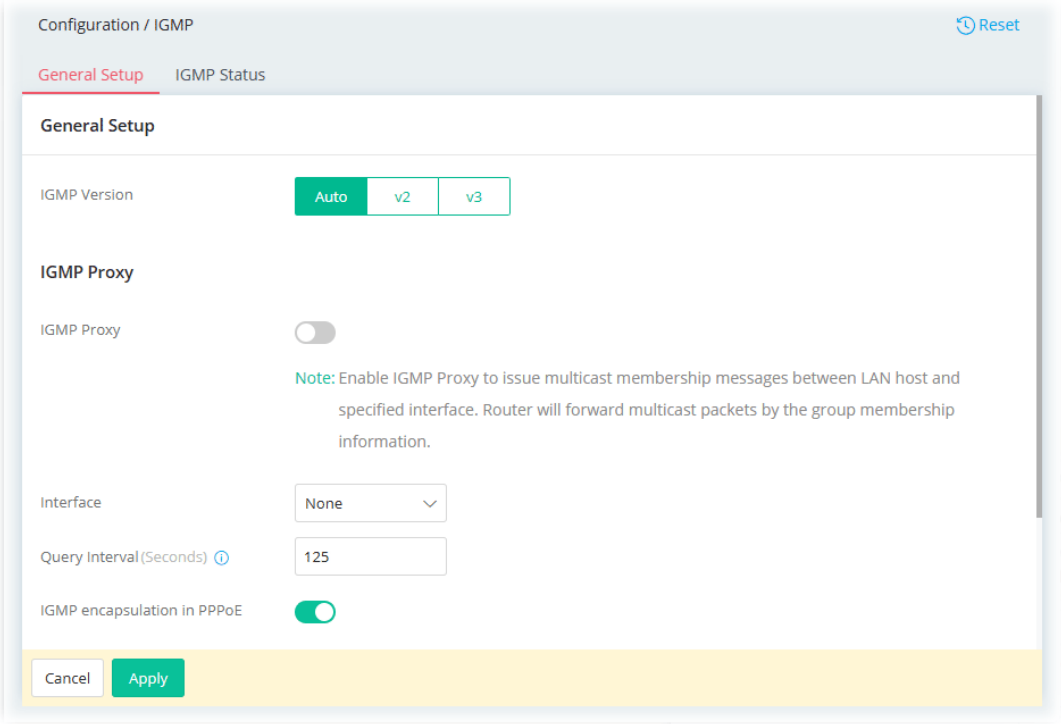
After finishing this web page configuration, please click **Apply** to save the settings.

II-1-6 IGMP

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

II-1-6-1 General Setup

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



Available settings are explained as follows:

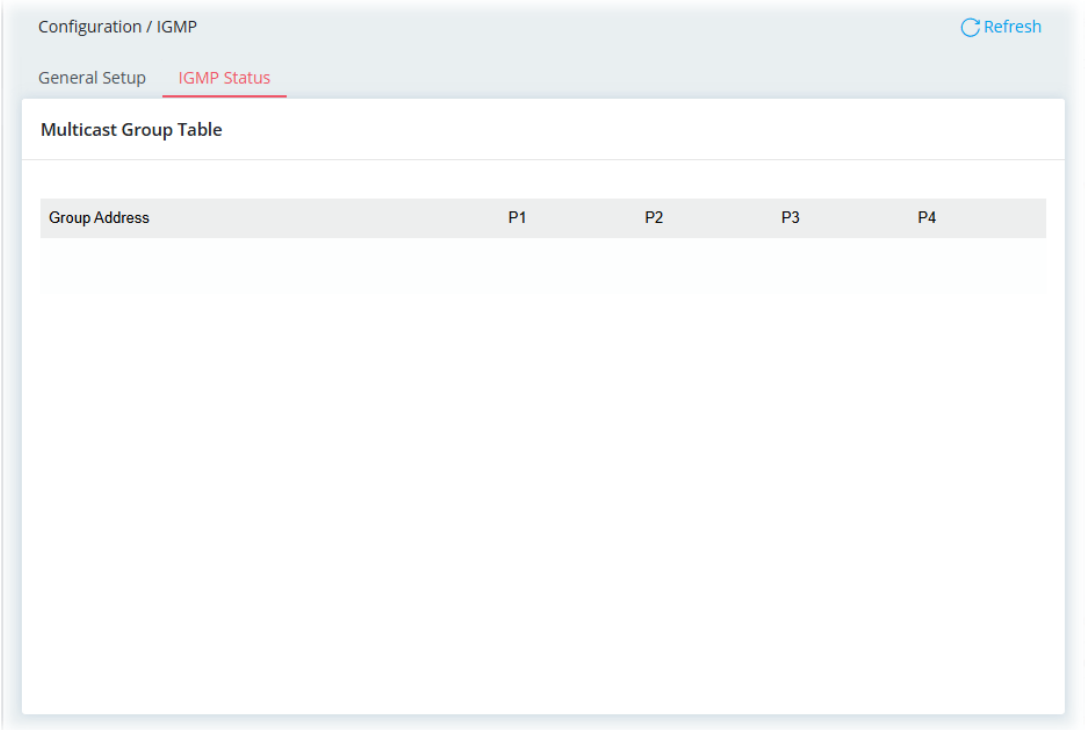
Item	Description
IGMP Version	Select v2 or v3 or Auto. At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe.
IGMP Proxy	
IGMP Proxy	Switch the toggle to enable or disable the function. The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode.
Interface	Specify an interface for packets passing through.
Query Interval	Vigor router will periodically check which IP obtaining IPTV service by sending query. It might cause inconvenience for client. Therefore, set a suitable time (unit: second) as the query interval to limit the frequency of query sent by Vigor router.
IGMP encapsulation in PPPoE	It depends on the specifications regulated by each ISP. If you have no idea to enable or disable, simply contact your ISP providers.
IGMP Snooping	
IGMP Snooping	Select to enable IGMP Snooping so that multicast traffic will be forwarded to IGMP clients that have joined a multicast group.
IGMP Fast Leave	This option is shown only when IGMP Snooping is enabled. Select to enable IGMP Fast Leave. Normally when the router receives a "leave" message from an IGMP host, it will send a last member query message to see if there are still members within the multicast group. When Fast Leave is enabled, multicast for a group is immediately terminated when the last host in that group sends a "leave" message.
IGMP Accept List	Only the device with the IP address specified here is able to process the multicast traffic through the IGMP proxy.

	Any – All IP addresses are allowed for using the IGMP proxy. **IP Object** – Select the IP object(s). The data traffic through those IPs within the object will be processed through the IGMP proxy. **IP Group** - Select the IP group(s). The data traffic through those objects within the group will be processed through the IGMP proxy.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-1-6-2 IGMP Status

This page displays a list of active multicast groups.



Available settings are explained as follows:

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

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

II-1-7 Objects

Vigor router system provides the object functions.

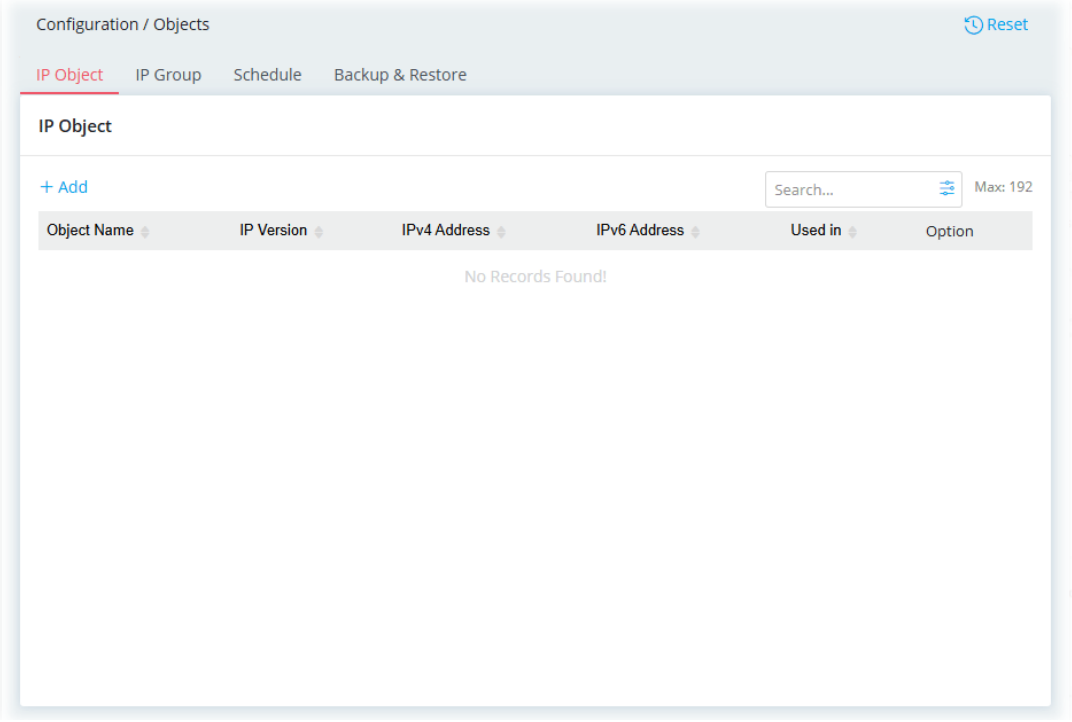
Users can define various types of objects and groups, and then apply them at various scenarios, like Configuration>>NAT>> Port Forwarding, Security>>Firewall Filters.

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

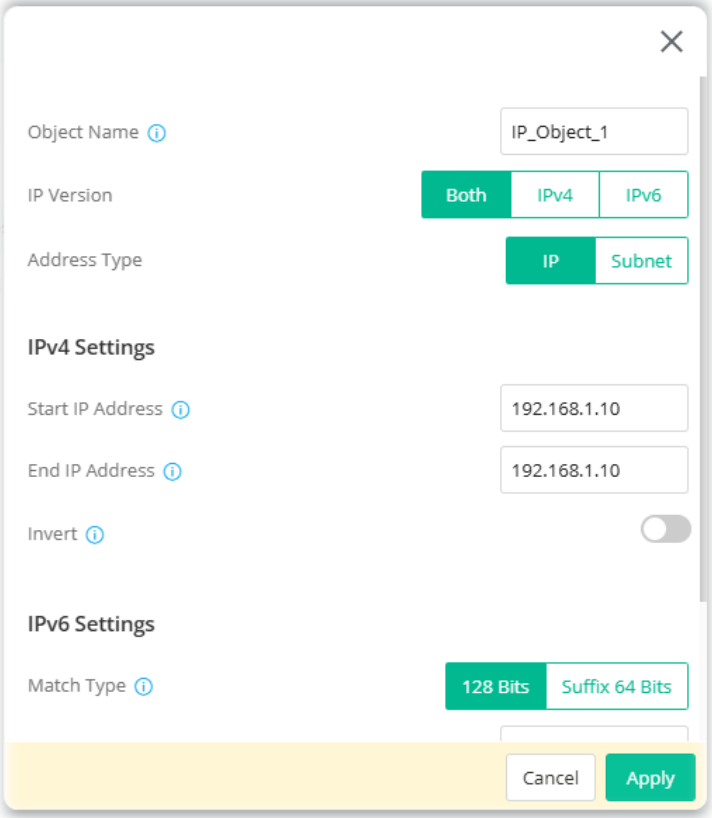
II-1-7-1 IP Object

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 the objects with ***groups*** for using conveniently. Later, we can select that object/group for applying it.

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



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



Available settings are explained as follows:

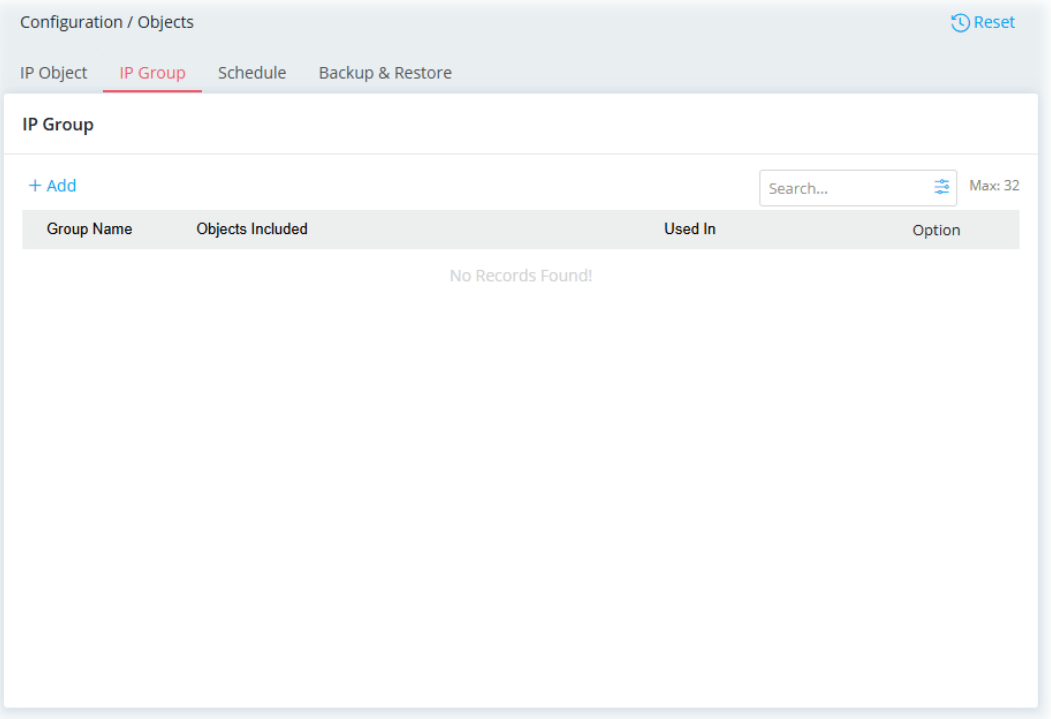
Item	Description
Object Name	Enter the name that identifies this profile.
IP Version	Select the IP version (IPv4, IPv6 or Both) for entering correct IP address.
Address Type	Select the type (IP or Subnet) of address.
	IPv4 Settings
Start IP Address	Enter the beginning IP address, if the Address Type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

Prefix Length	Enter IPv6 prefix length, if Address type is Subnet.
Invert	If enabled, all addresses except the ones entered above will be used.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

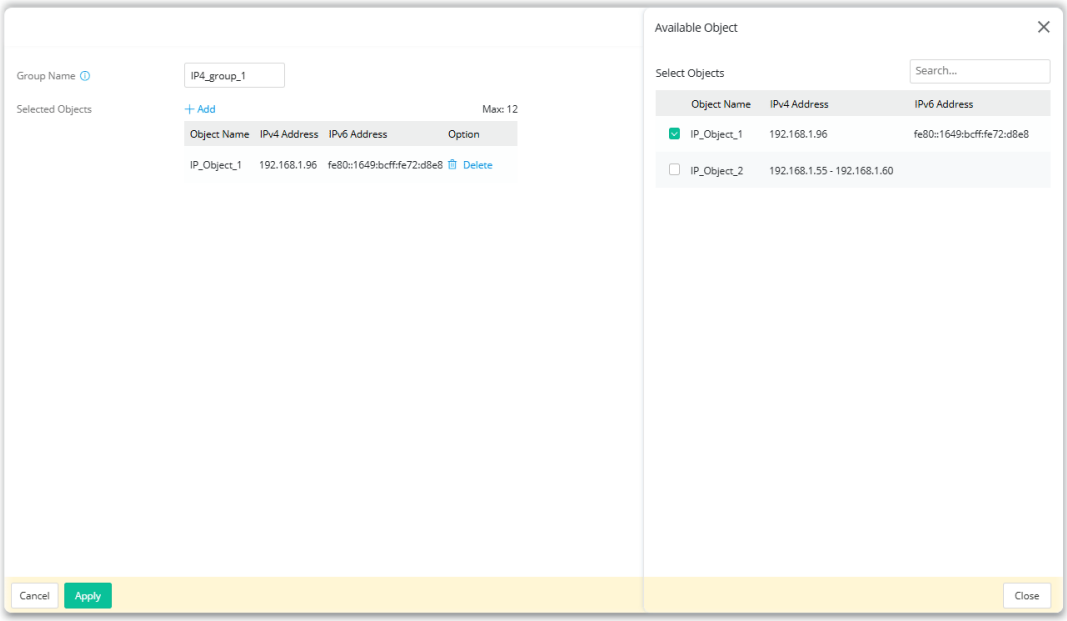
After finishing this web page configuration, please click **Apply** to save the settings.

II-1-7-2 IP Group

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



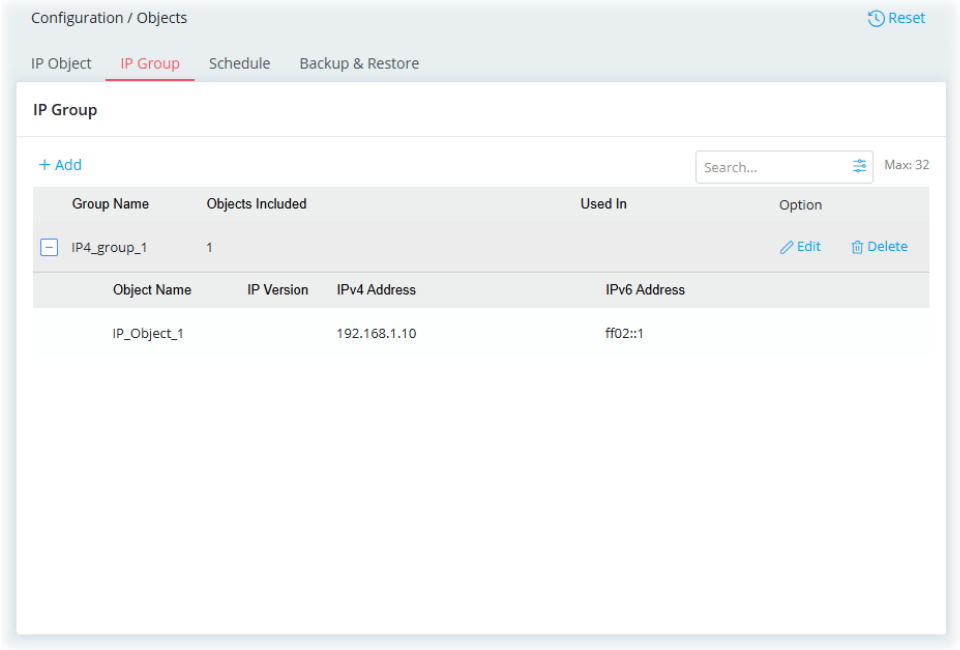
To add a new IP group profile, click the **+Add** link to get the following page.



Available settings are explained as follows:

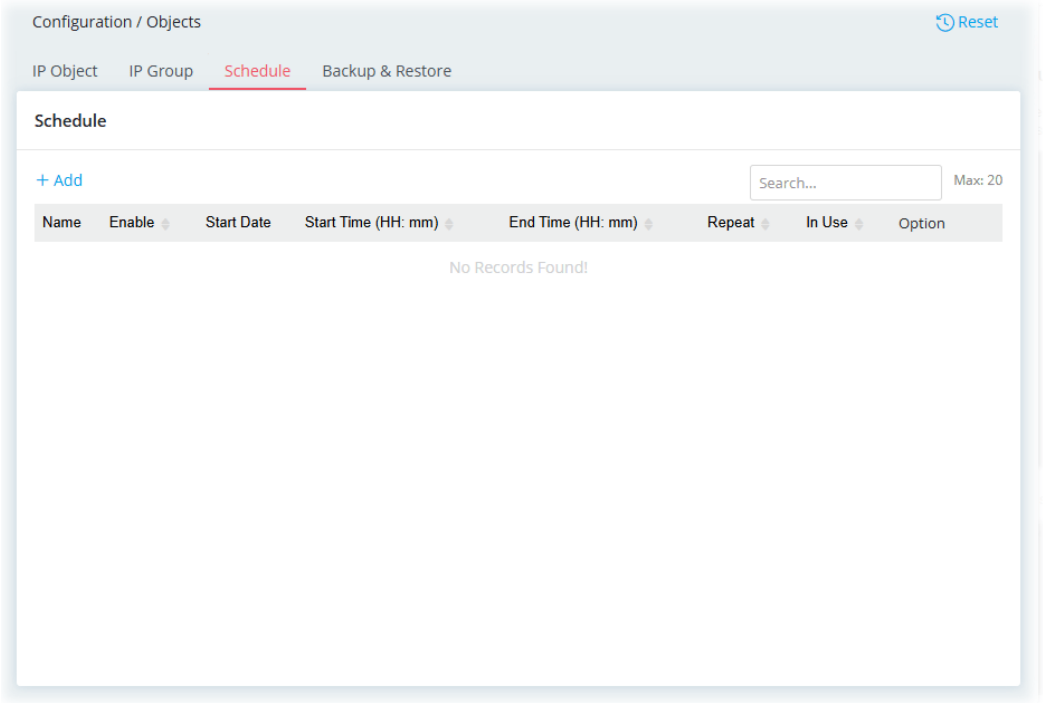
Item	Description
Group Name	Enter a name that identifies this profile.
Selected Objects	**+Add -** Click to open the page with available objects.
	Available Object
Search	Enter the IP object name or the IPv4/IPv6 Address to search related IP object(s).
Select Objects	Objects available for grouping will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

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

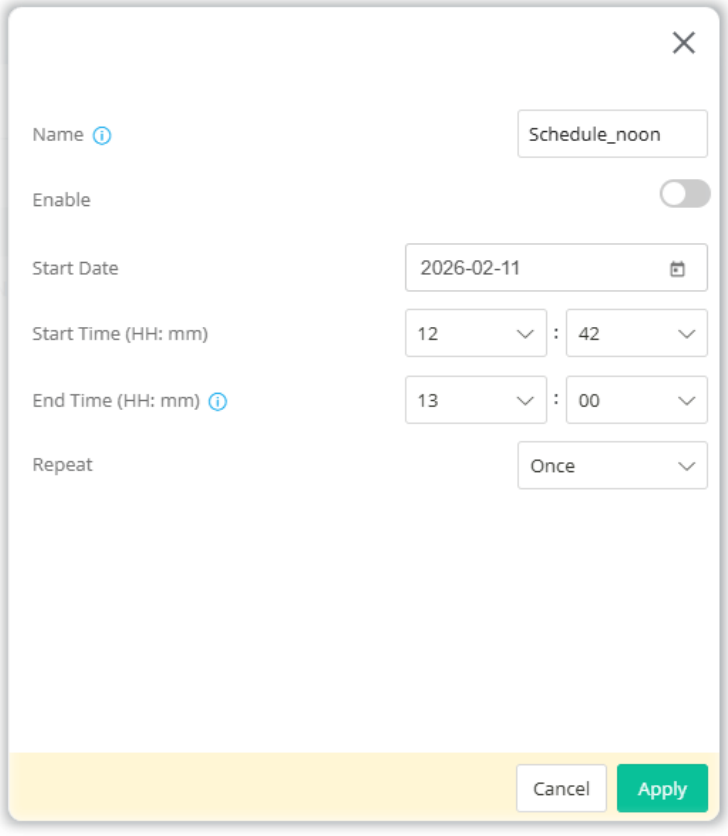


II-1-7-3 Schedule

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.



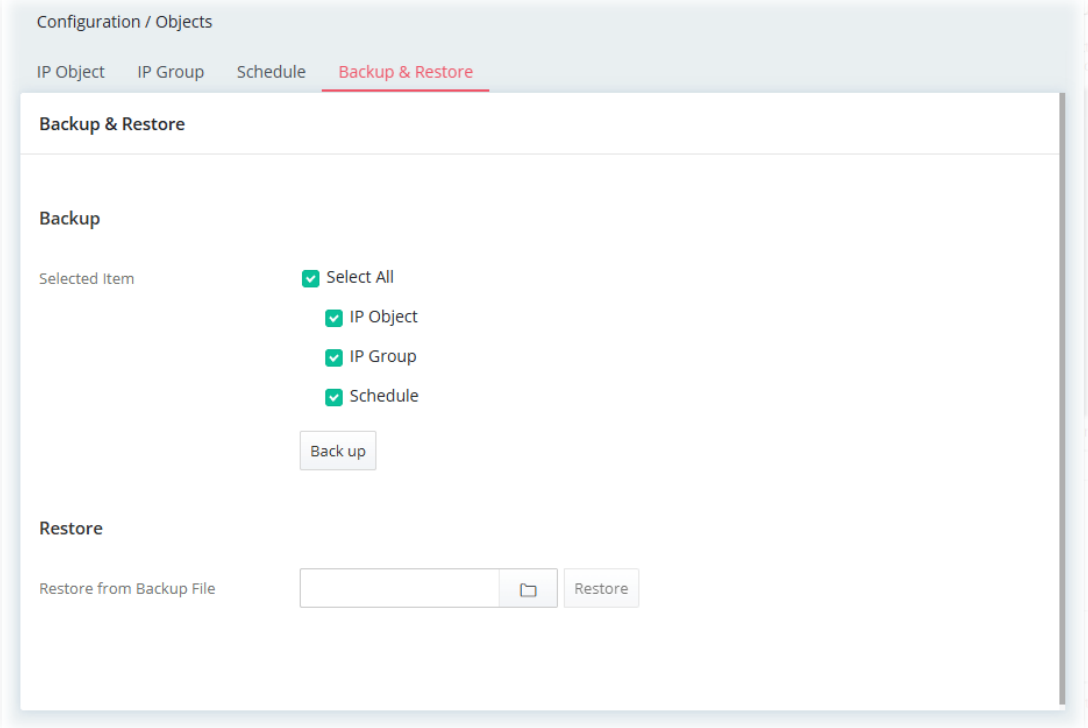
Available settings are explained as follows:

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

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

II-1-7-4 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. All the objects (or the template) can be saved and exported as a file by clicking Download. **Back up** – Click it to backup current objects to a file. Such file can be restored for future use.
Restore	**Restore from Backup File** – Click it to specify a file backed up previously. **Restore** – Click to execute the restoration.

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

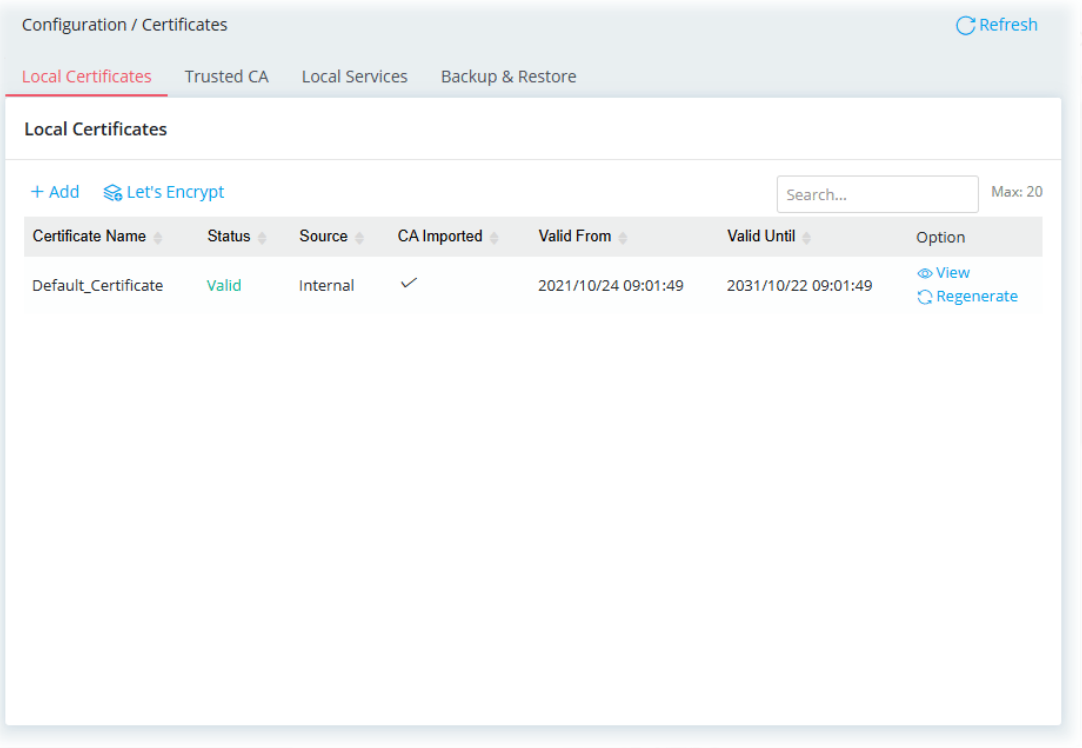
II-1-8 Certificates

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.

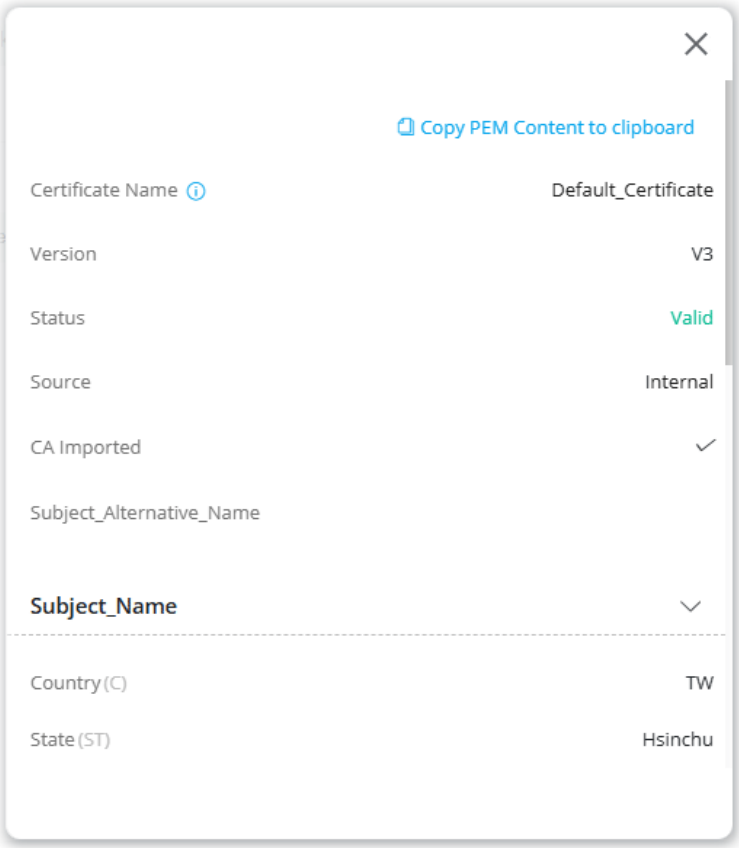
In this section, you can generate and manage local digital certificates, and import trusted CA certificates. Be sure that the system time is correct on the router so that certificates will not be erroneously considered to be invalid because of an incorrect system time falling outside of the certificate's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

II-1-8-1 Local Certificates

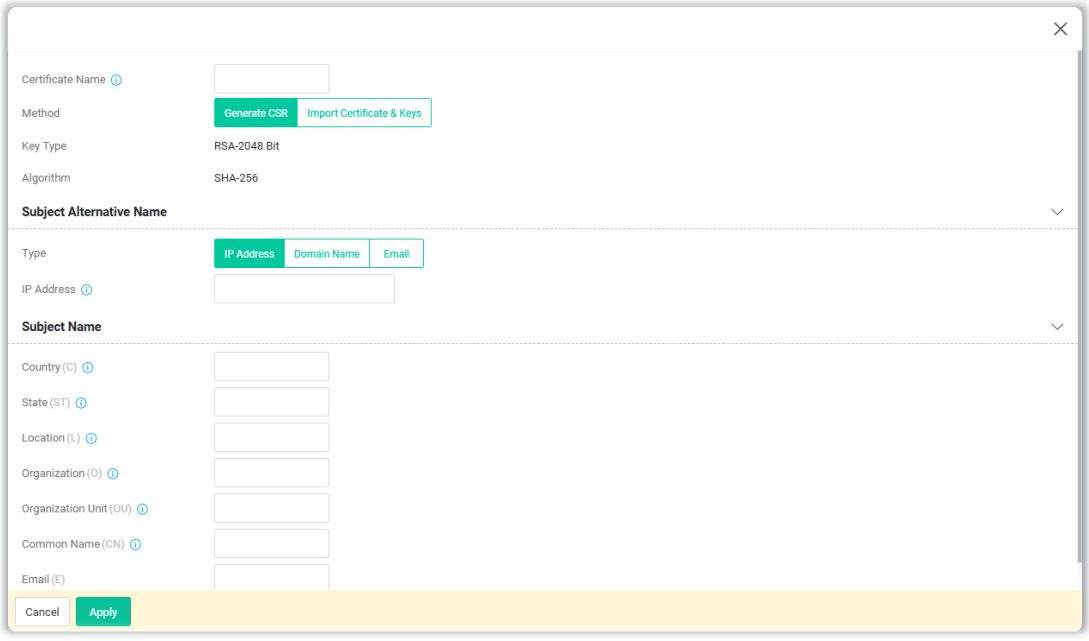
You can generate, import or view local certificates on this page.



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



To add a new certificate, 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.

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

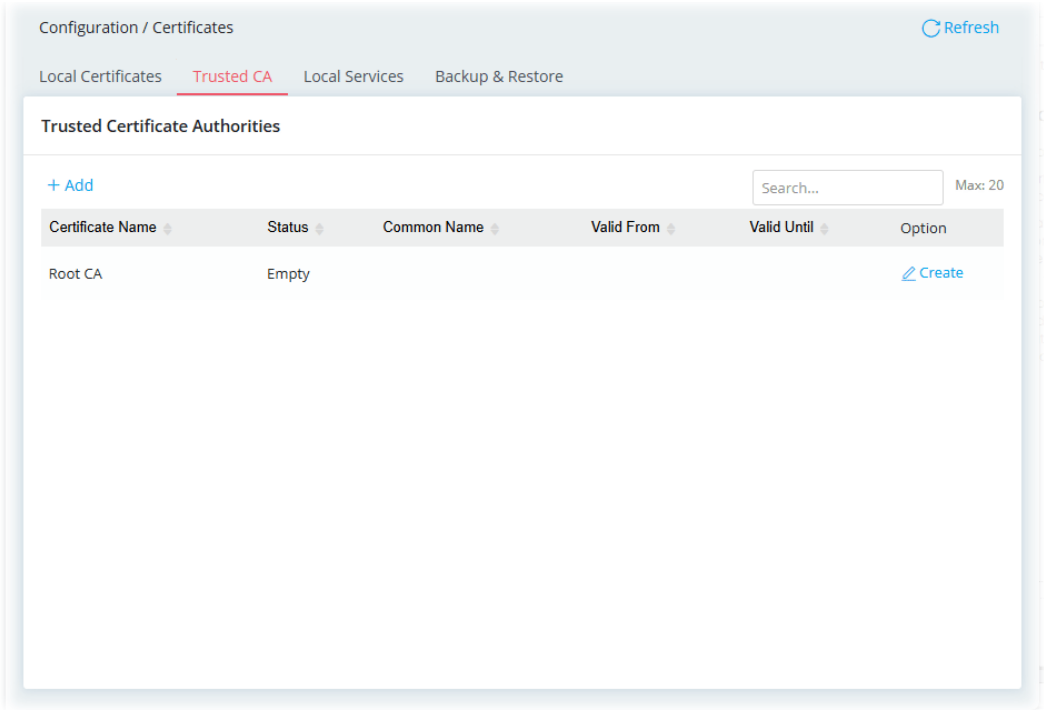
II-1-8-2 Trusted CA

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

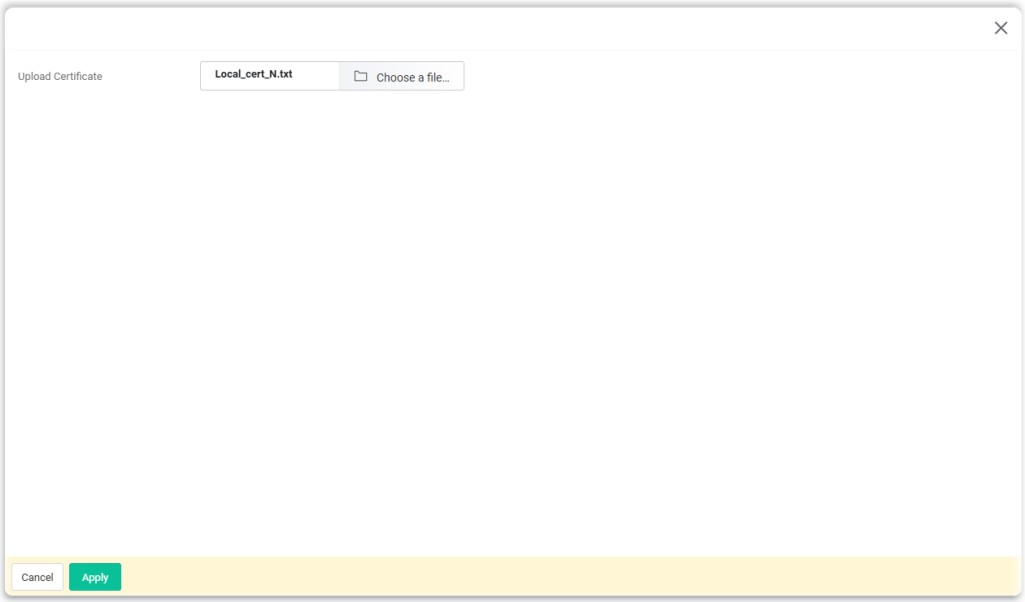
Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

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.



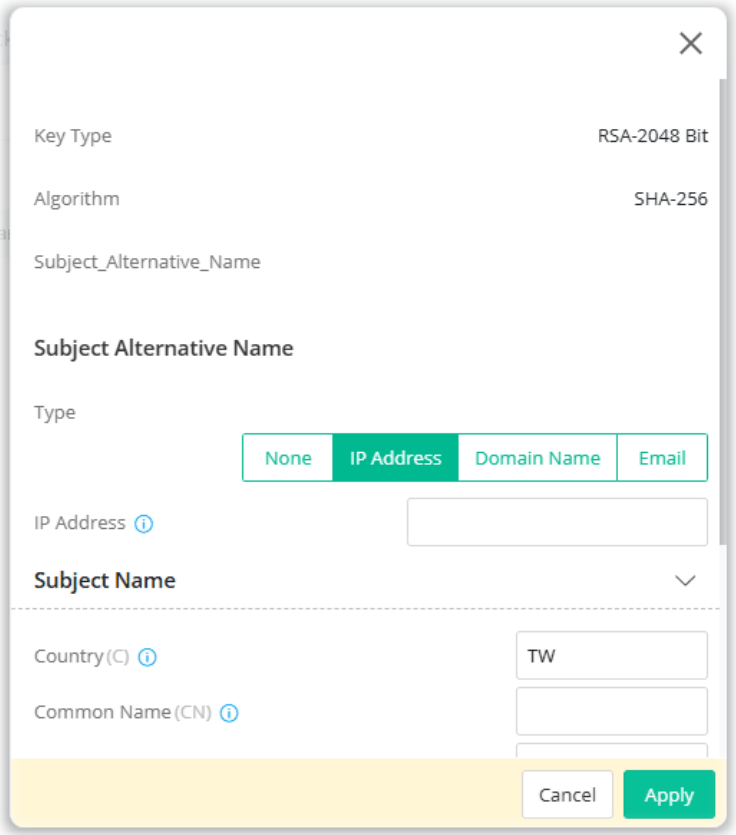
To import a RootCA to the Vigor router, click **+Add** to upload one certificate.



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.

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



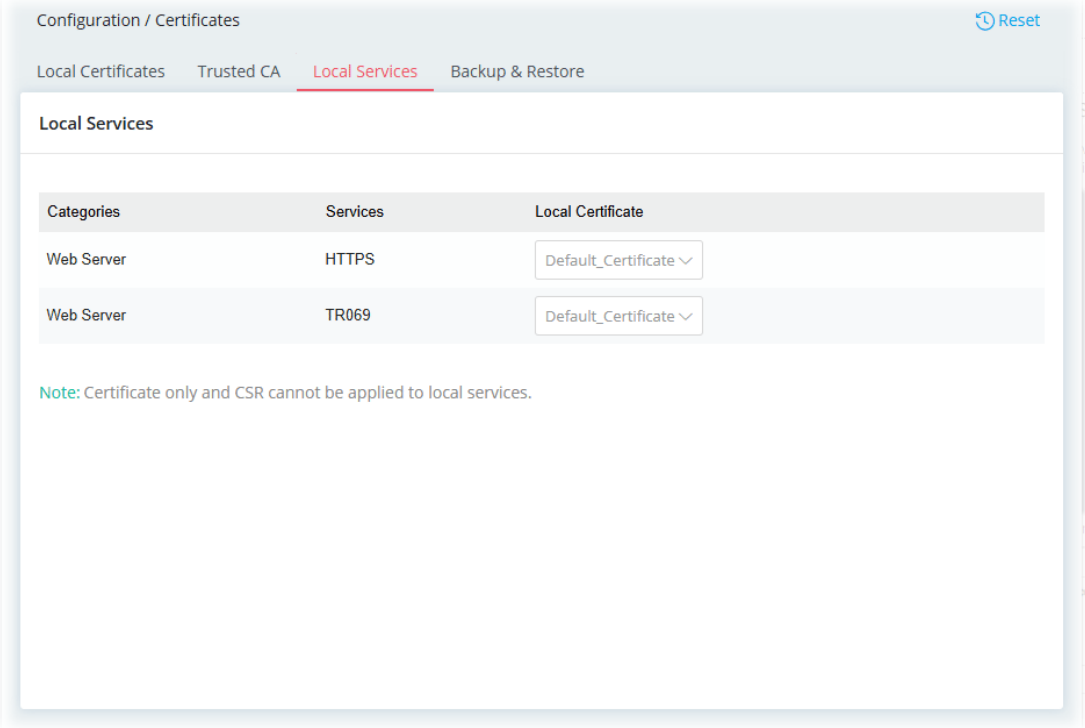
Available settings are explained as follows:

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 **Email**. 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.

II-1-8-3 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.



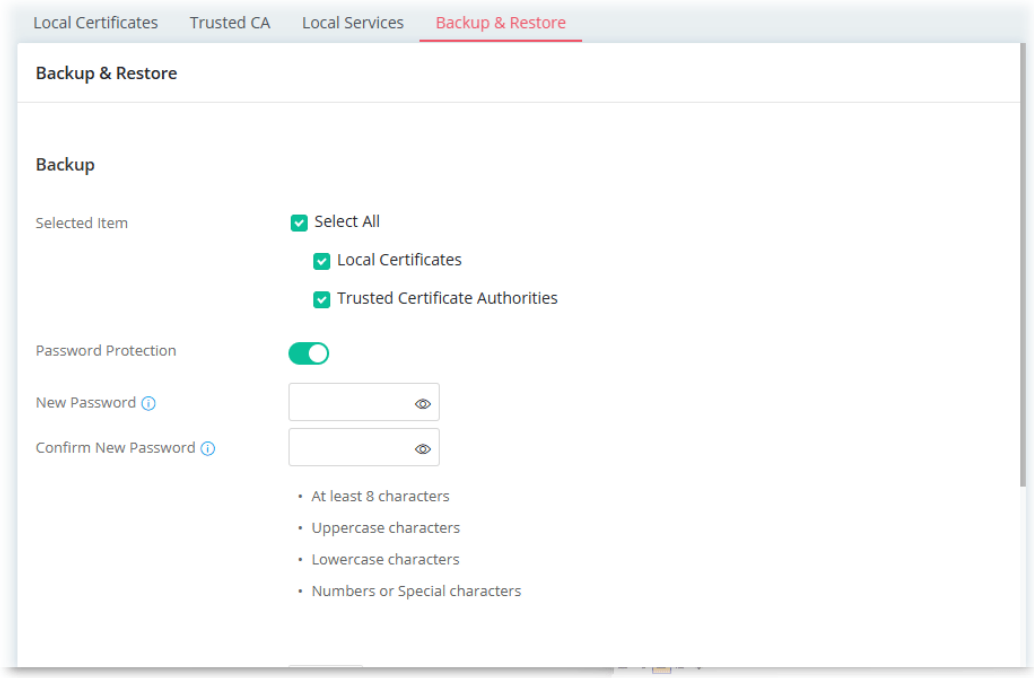
Available settings are explained as follows:

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.
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-1-8-4 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 certificates).
Password Protection	Switch the toggle to enable or disable the function. If enabled, set the following items: ● **New Password** - Enter the password with which you wish to encrypt the certificate. ● **Confirm New Password** - Enter the password again. **Back up** - Click to download the certificate.
	Restore
Restore from Backup file	Click to select the backup file you wish to restore. - Click to locate the file for restoring. **Restore** - Click to retrieve the certificate.
File has Password Protection	Switch the toggle to enable or disable the function. If enabled, set the following item: ● **Password** - Enter the password that was used to encrypt the certificates.

II-2 Security

II-2-1 Firewall Filters

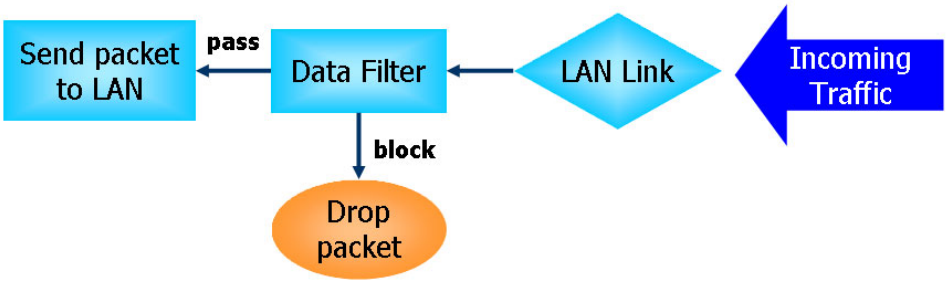
A network firewall monitors traffic travelling between networks, with the ability to selectively allow or block traffic using a predefined set of security rules. This helps to maintain the integrity of networks by stopping unauthorized access and the exchange of sensitive information.

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

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

Data Filter

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



Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

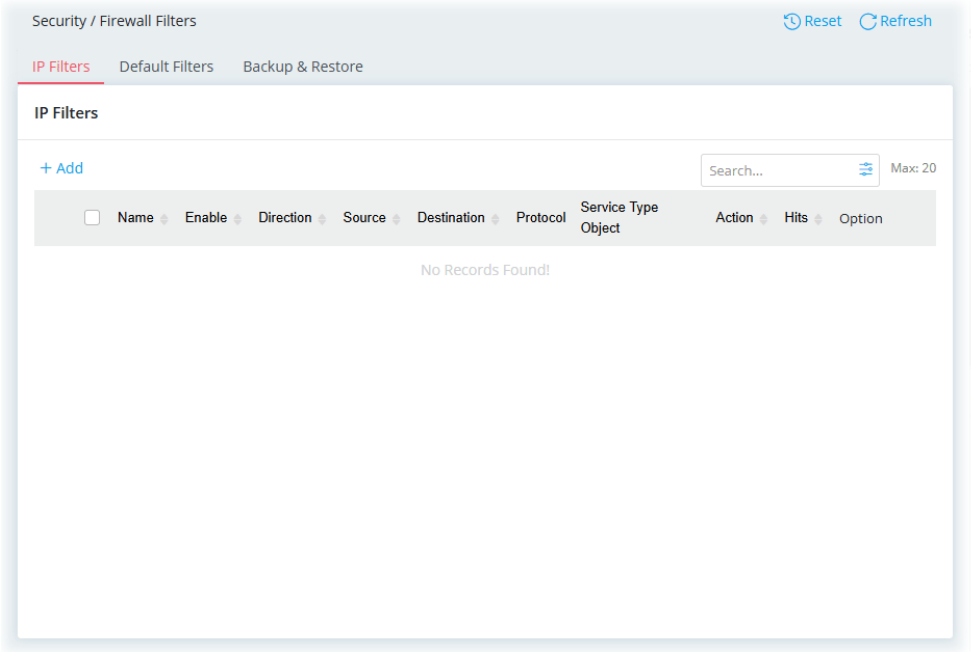
Vigor's DoS Defense functionality detects DoS attacks and mitigates their damage by inspecting every incoming packet, and malicious packets will be blocked. If Syslog is enabled, alert messages will also be sent. Abnormal traffic flow such as flood and port scan attacks that exceed allowable thresholds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

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

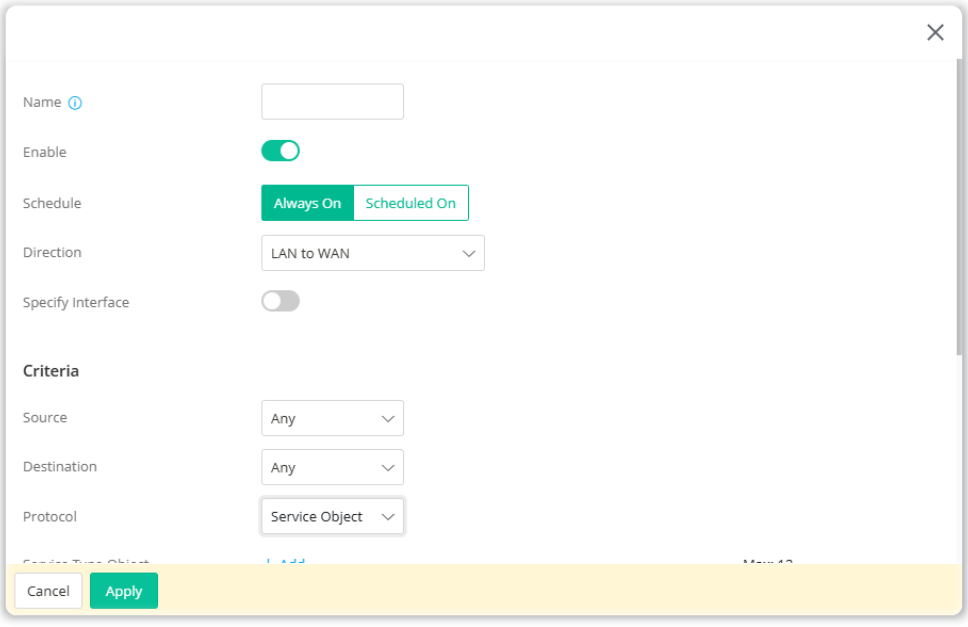
1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
9. SYN fragment
10. Fraggle attack
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unassigned Numbers

II-2-1-1 IP Filters

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

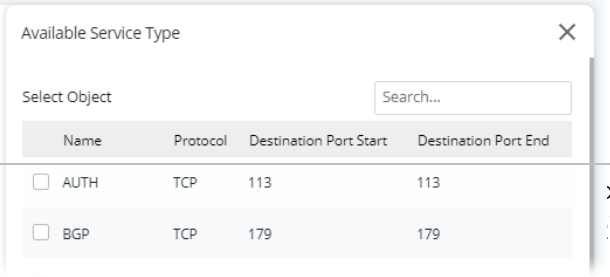


To add a new IP filter profile, click the **+Add** link to get the following page.



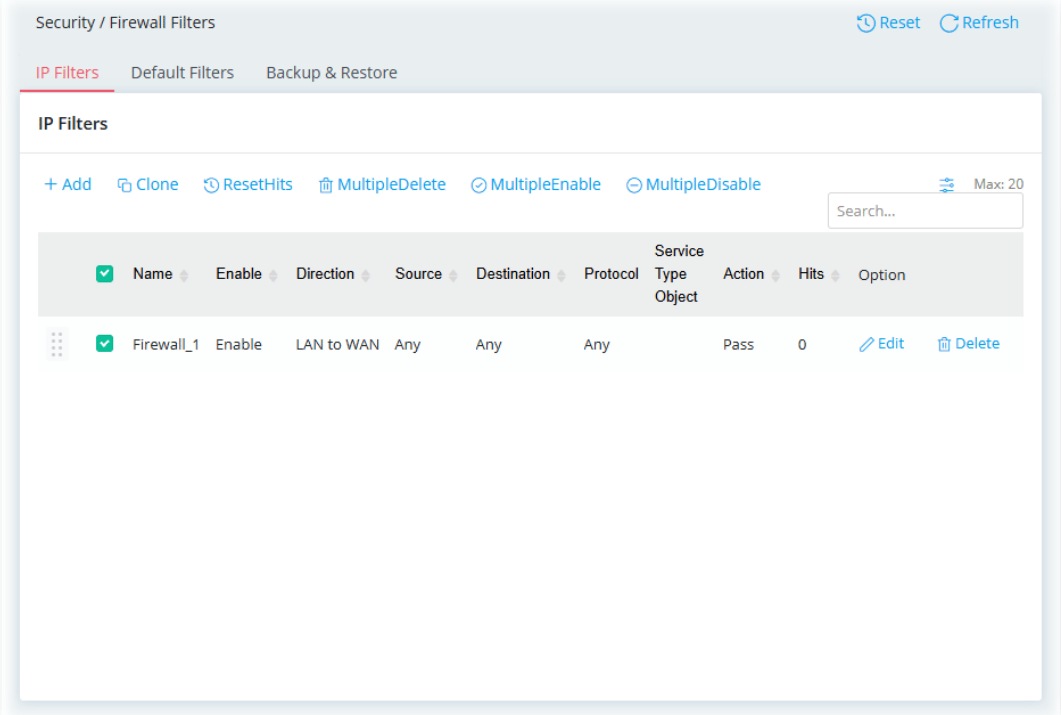
Available settings are explained as follows:

Item	Description
Name	Enter a name to identify the rule.
Enable	Switch the toggle to enable/disable this profile.
Schedule	**Always On** – This rule is enabled and active for always. **Scheduled On** - Select Schedule indexes to allow the rule to be enabled at specific times. You may choose up to 4 out of the 15 schedules in Configurations>>Objects>>Schedule. The rule is always enabled when no indexes have been selected. • **Clear Session when Schedule is On** - Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset.
Direction	Specify the direction of traffic flow to which this filter rule applies. • **LAN to WAN** • **WAN to LAN** • **LAN/VPN to LAN/VPN**
Specify Interface	Switch the toggle to enable/disable the function. If enabled, specify the interfaces for the traffic flow. **Source Interface** – Select the LAN interface(s). **Destination Interface** – Select the WAN interface(s).
Criteria	
Source	Configure the source IP addresses. To set the IP address manually, please choose **Any / IPv4 Address / IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group / MAC Object / MAC Group** as the source and enter required information. **Any** – All IP addresses **IPv4 Address**–Enter the IP address. • **Source IPv4 Address** – Click +Add to enter the IP address. **IPv4 Subnet**–Enter the IP Address and the Subnet Mask. • **Source IPv4 Subnet Address** - Click +Add to enter the IPv4 address with a subnet mask. **IPv6 Address**–Enter the IPv6 address. • **Source IPv6 Address** – Click +Add to enter the IPv6 address. **IPv6 Subnet**–Enter the IPv6 Address and the prefix length. • **Source IPv6 Subnet Address** - Click +Add to enter the IPv6 address with a subnet mask. **IP Object**–Allows selection of predefined IP Objects. • **Source IP Object** – Click +Add to select an IP object. **IP Group** –Allows selection of predefined IP Groups. • **Source IP Group** - Click +Add to select an IP group. **MAC Object**–Allows selection of predefined MAC Objects. • **Source MAC Object** – Click +Add to select an MAC object. **MAC Group** –Allows selection of predefined MAC Groups. • **Source MAC Group** - Click +Add to select an MAC group.
Destination	Configure the destination IP addresses. To set the IP address manually, please choose **Any / IPv4 Address /**

	IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group as the destination and enter required information. **Any** – All IP addresses **IPv4 Address**–Enter one IPv4 address. • **Destination IPv4 Address** – Click +Add to enter the IP address. **IPv4 Subnet**–Enter the IPv4 Address and the Subnet Mask. • **Destination IPv4 Subnet Address** - Click +Add to enter the IPv4 address with a subnet mask. **IPv6 Address**–Enter the IPv6 address. • **Destination IPv6 Address** – Click +Add to enter the IPv6 address. **IPv6 Subnet**–Enter the IPv6 Address and the prefix length. • **Destination IPv6 Subnet Address** - Click +Add to enter the IPv6 address with a subnet mask. **IP Object**–Allows selection of predefined IP Objects. • **Destination IP Object** – Click +Add to select an IP object. **IP Group** –Allows selection of predefined IP Groups. • **Destination IP Group** - Click +Add to select an IP group. **Country Object** –Allows selection of predefined Country Objects. • **Destination Country Object** – Select the object.
Protocol	Specify the protocol(s) which this filter rule will apply to. • Any • Service Object • TCP/UDP • TCP • UDP
Service Type Object	 col.) you want.
Specify Source Port	It is available when TCP or UDP or TCP/UDP is set as the Protocol. Switch the toggle to enable / disable the port settings. **Source Port** – If enabled, please provide the starting and ending port values.
Destination Port	It is available when TCP or UDP or TCP/UDP is set as the Protocol. To define a port range, please provide the starting and ending port values.
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.
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 IP filter profile is selected, click it to remove the items at one time.
MultipleEnable	When more than one IP filter profile is selected, click it to enable the profiles at one time.
MultipleDisable	When more than one IP filter profile is selected, click it to disable the profiles at one time.
Edit	Modify the selected IP filter profile.
Delete	Remove the selected IP filter profile.

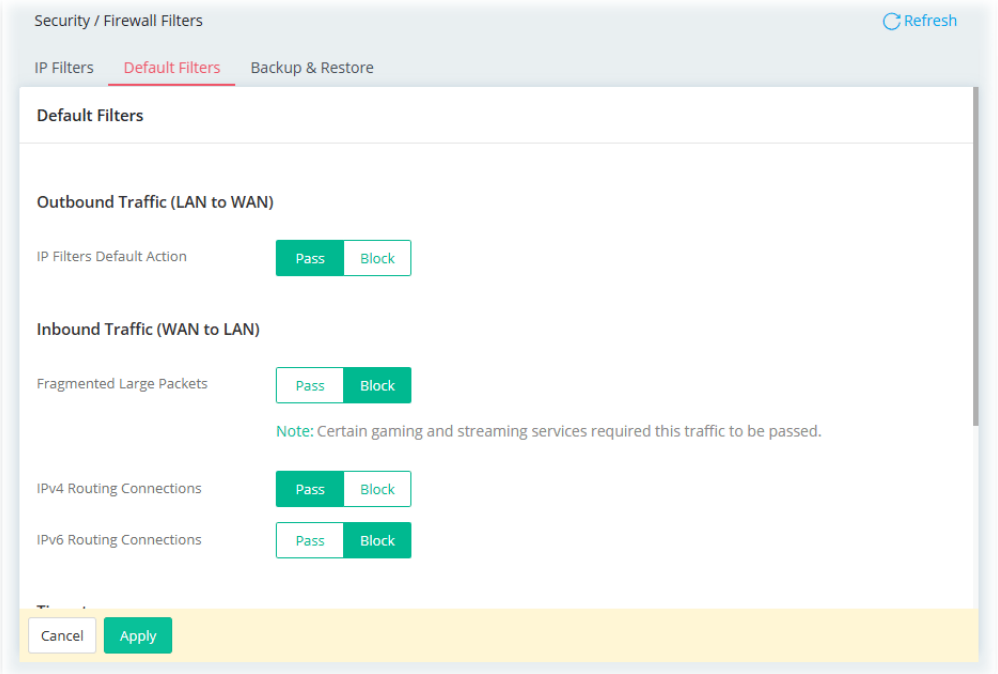
II-2-1-2 Default Filters

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)
IP Filters Default Action	Define the default action for the outgoing packets that do not match any IP filter rule. **Pass** –The packets that do not match any IP filter rule will be passed and next wait for the content filter. **Block** – The packets that do not match any IP filter rule will be blocked by Vigor system.
	Inbound Traffic (WAN to LAN)
Fragmented Large Packets	Certain games and video streaming service use fragmented UDP packets to transfer data. **Pass** - The router always passes fragmented packets without reassembling them, regardless of the size of the packet. **Block** - The router will attempt to reassemble fragmented packets up to a certain value (e.g., 15xx~2102) kilobytes long. Packets larger than the certain value will be discarded.
IPv4 Routing Connections	**Pass** – For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, select this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on

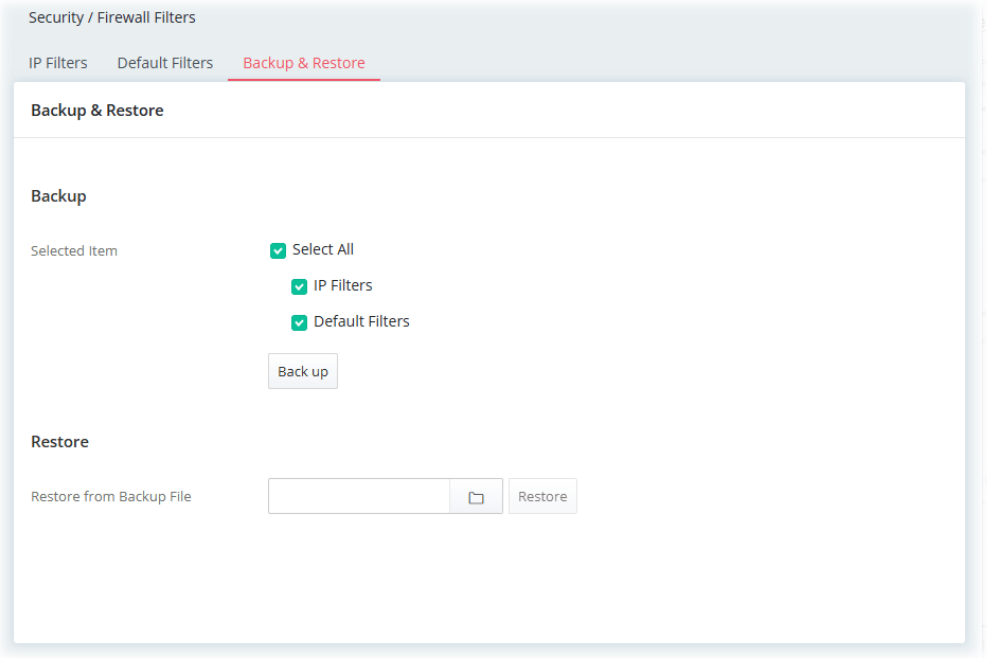
	private LAN subnets. **Block** - Block the LAN hosts from connecting to WAN hosts using IPv4.
IPv6 Routing Connections	**Pass** – IPv6 does not make use of Network Address Translation (NAT), so all LAN hosts receive public IPv6 IP addresses that are exposed to the WAN. **Block** - Block the WAN hosts from connecting to LAN hosts using IPv6.
ICMP Timestamp	**Pass** –Allows the router to reply to ICMP timestamp requests from other devices. It is useful for legacy network time synchronization and precise latency diagnostics. However, it may expose system uptime and clock information to potential attackers during network reconnaissance. **Block** - Prevents the router from replying to ICMP timestamp requests (Type 13). This helps protect the router by preventing external devices from learning its system time and uptime. Blocking these responses reduces the risk of attackers gathering information about the device during network scanning.
TCP Timestamp	**Pass** – Allows TCP packets to include timestamp information. Enables the inclusion of timing information in TCP headers to improve RTT (Round Trip Time) calculation and protection against wrapped sequence numbers. This is the standard setting for maintaining optimal network performance and stability in high-speed connections. **Block** - Removes timestamp information from TCP packets. It is used to prevent external scanners from estimating the system's uptime or boot time. This enhances device privacy and security by reducing the amount of diagnostic data exposed to the network.
Syslog	**Enable Syslog** – If enabled, the log related to default filter will be recorded to Syslog.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

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

II-2-1-3 Backup & Restore

This page allows the backup and restoration of router settings.

In addition to restoring Vigor180's own configuration backup, it is possible to restore backups from certain DrayTek routers on Vigor180.

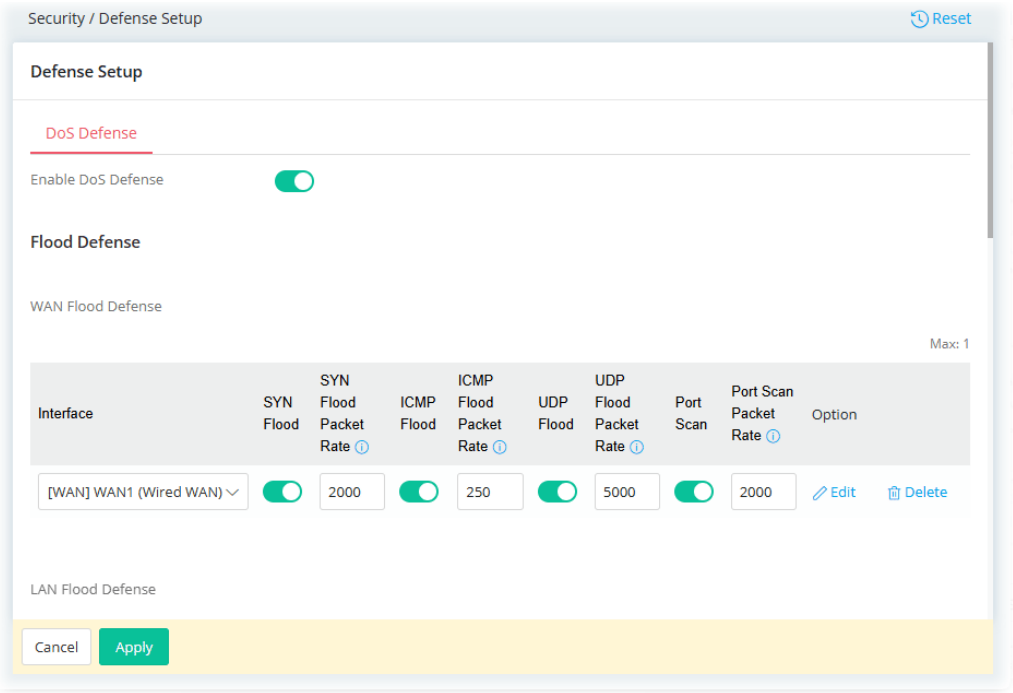


Available settings are explained as follows:

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

II-2-2 Defense Setup

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
Enable DoS Defense	Switch the toggle to enable/disable the DoS Defense.
	Flood Defense
WAN Flood Defense	**+Add** – Click it set profiles for flood defense. Up to 6 profiles can be created. **Interface** – Select a WAN interface. Set the packet rate values for WAN to meet your request. **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.
LAN Flood Defense	**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)

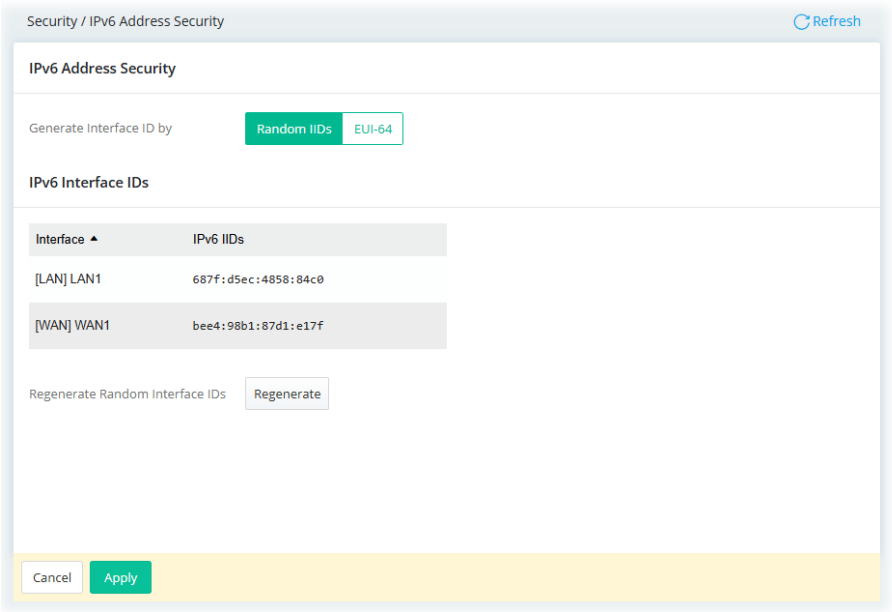
	parameters, a series of Internet addresses, routing messages, etc, which external eavesdroppers can use to discover details about the private network. **Block Land** – Enable to block LAND attacks. LAND attacks happen when an attacker sends spoofed SYN packets with both source and destination addresses 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.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings.

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

II-2-3 IPv6 Address Security

This page allows you to configure the IPv6 interface ID.



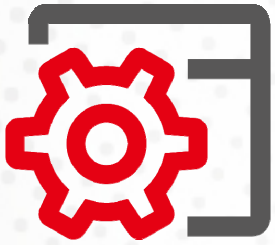
Available settings are explained as follows:

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 IDs	Display the interface and corresponding IPv6 IIDs.
Regenerate Random Interface IDs	**Regenerate** - Re-generate the random IIDs for all interfaces.
Cancel	Discard current settings.
Apply	Save the current settings.

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

This page is left blank.

Chapter III Management



III-1 System Maintenance

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

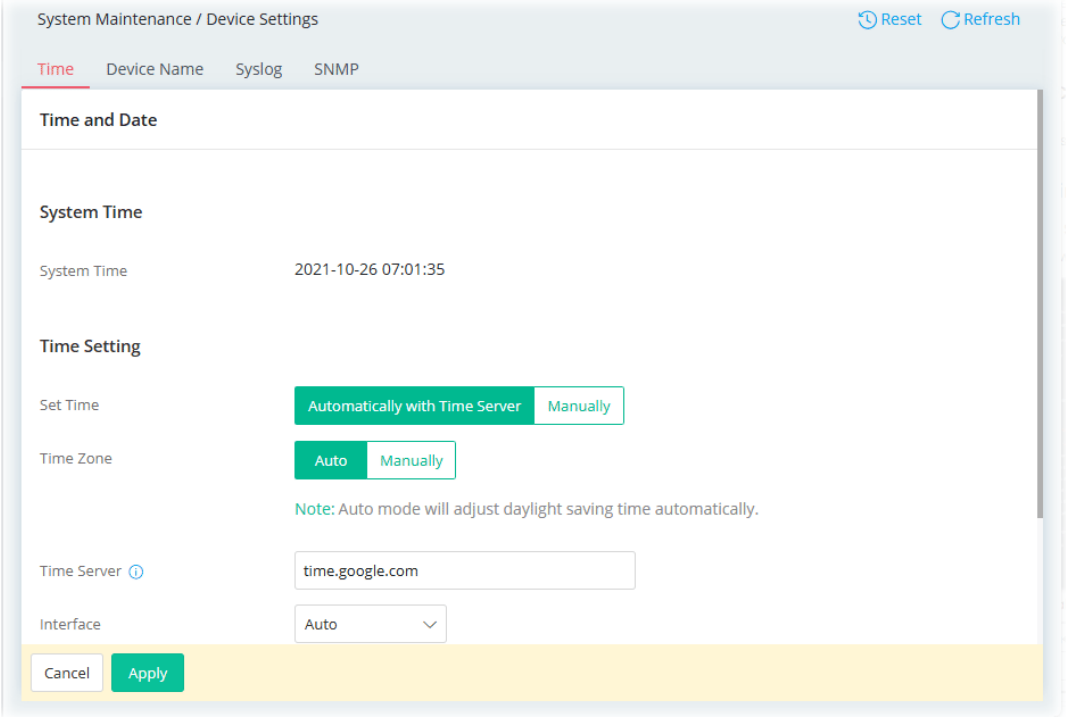
III-1-1 Device Settings

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

III-1-1-1 Time

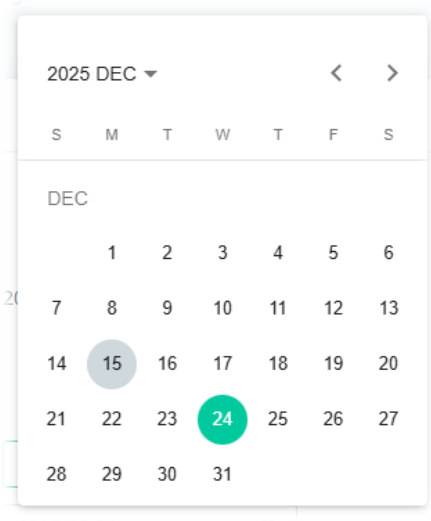
Open **System Maintenance>>Device Settings** and click the **Time** tab.

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



Available parameters are explained as follows:

Item	Description
	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	**Time Zone** - Select the time zone (Auto or Manually) where the

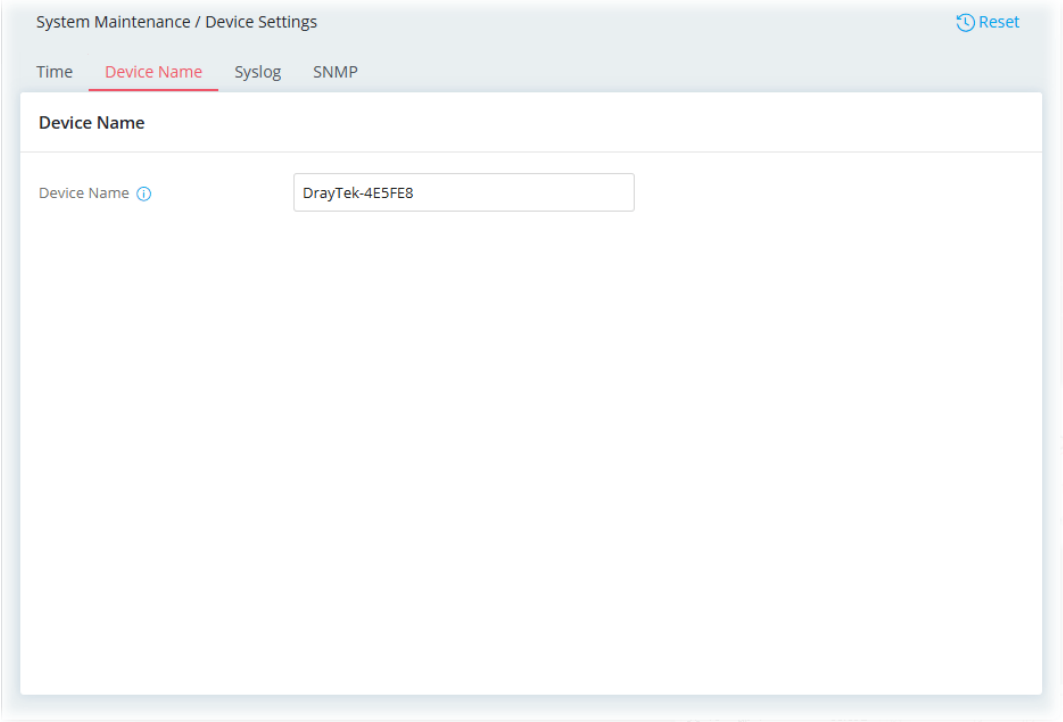
with Time Server is selected as Set Time	router is located. **Time Server** - Enter the web site of the primary time server. **Interface** - Renew the time through the selected WAN/LAN interface. If Auto is selected, the Vigor system will renew the time through WAN or LAN. **Test Time Server Connection** – Test if the time server works well. **Server Status** - Displays last update time status. **More Settings** - Click to open advanced settings for the time server. • **Auto Update Interval** - Select the time interval (e.g., 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** – It is available when **Manually** is selected as Time Zone. Switch the toggle to enable or disable the function. Enable Daylight Saving Time (DST) if it is applicable to your location if Manually is selected as Time Zone. • **Daylight Saving Period** - It is available when Daylight Saving is enabled. Specify the starting time and the ending time if "by Week" or "by Date" is selected.
When Manually is selected as Set Time	**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.
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.

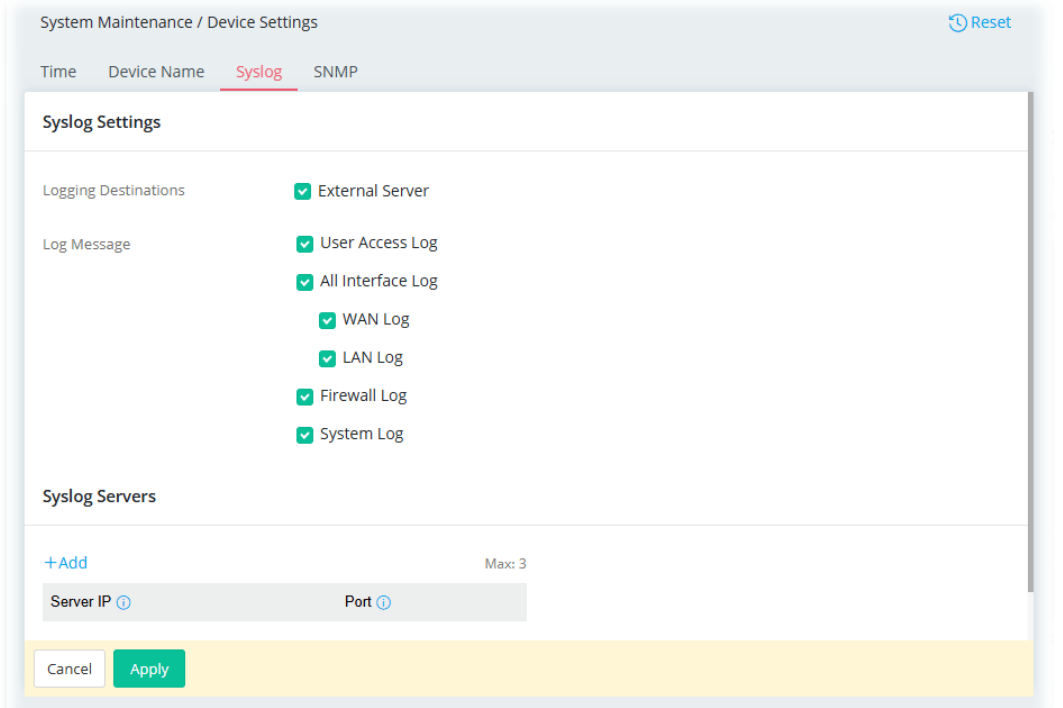
Open **System Maintenance>>Device Settings** and click the **Device Name** tab.



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	**External Server** - Select to set Log Message item(s) and configure Syslog Servers.
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 (1-65535) of the Syslog Server.
Option	**Delete** - Click it to remove the selected server profile.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

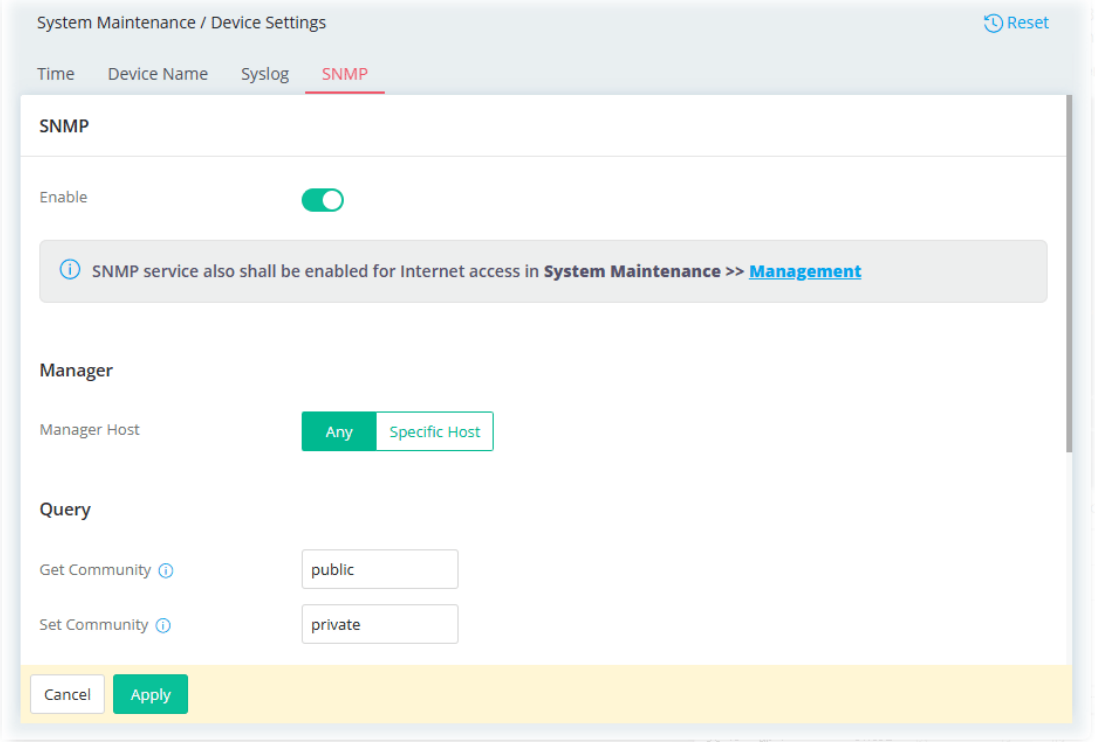
After finishing this web page configuration, please click **Apply** to save the settings.

III-1-1-4 SNMP

This section allows you to configure settings for SNMP services.

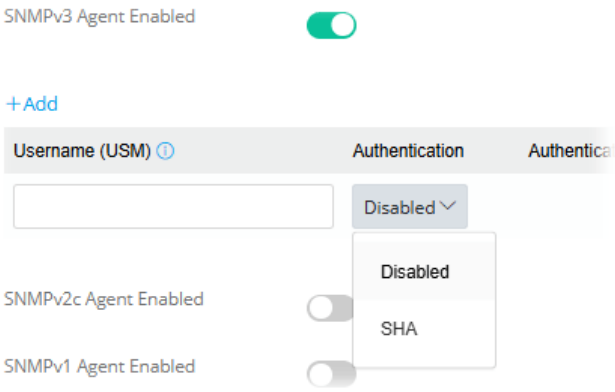
The SNMPv3 is more secure than SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.

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



Available parameters are explained as follows:

Item	Description

SNMP	
Enable	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.

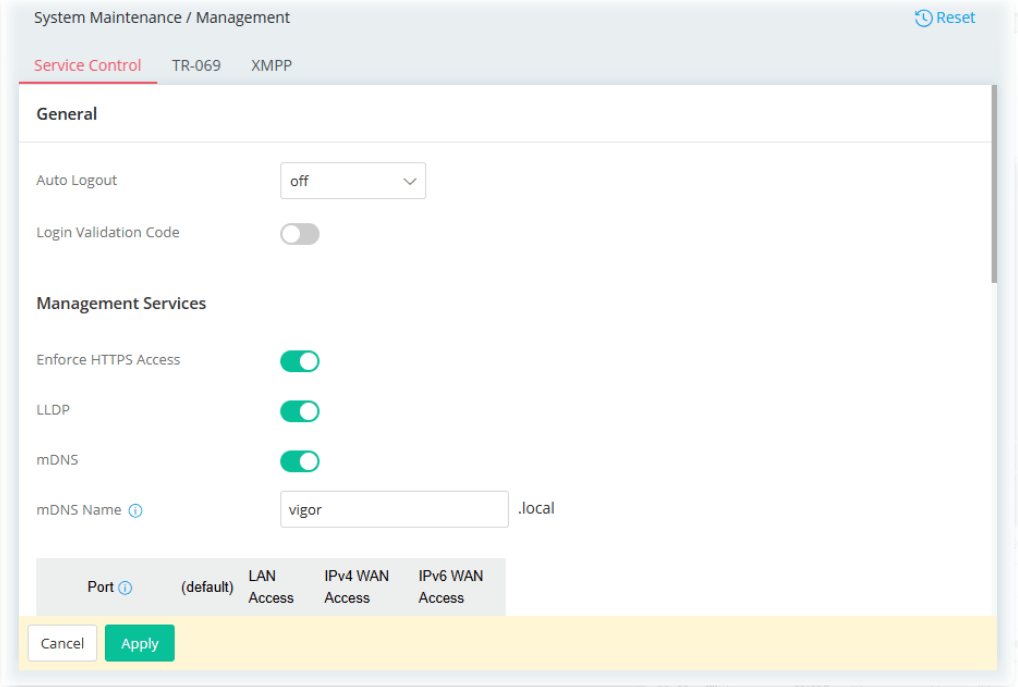
SNMPv1 Agent Enabled	Switch the toggle to enable/disable the SNMPv1 function.
Trap	
Enabled	Switch the toggle to enable/disable the Trap function.
Trap Version	Select the trap version. • V1 • V2c • V3
Trap Community	Enter the Trap Community string (for Trap Version V1/V2c). The default setting is public. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string. The maximum length of the text is 23 characters.
Trap Port	Enter the port number used for the Trap server.
Notification Host IP Type	Select the type of the notification host. • Both • IPv4 • IPv6
Notification Host(IPv4)	+Add - Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
Notification Host(IPv6)	+Add - Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
Trap Events	Select the event(s) to apply the settings configured in this page.
Apply	Save the current settings and exit the page.

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

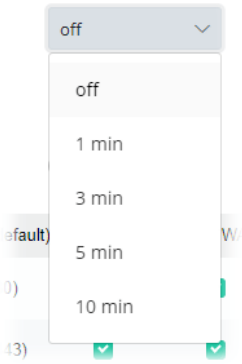
III-1-2 Management

III-1-2-1 Service Control

This page allows you to manage the general settings, management services, and TLS/SSL Encryption setup. After a user has been authenticated by means of a username and password, he or she can be granted Internet access, and optional firewall rules and WAN access policies can be applied.



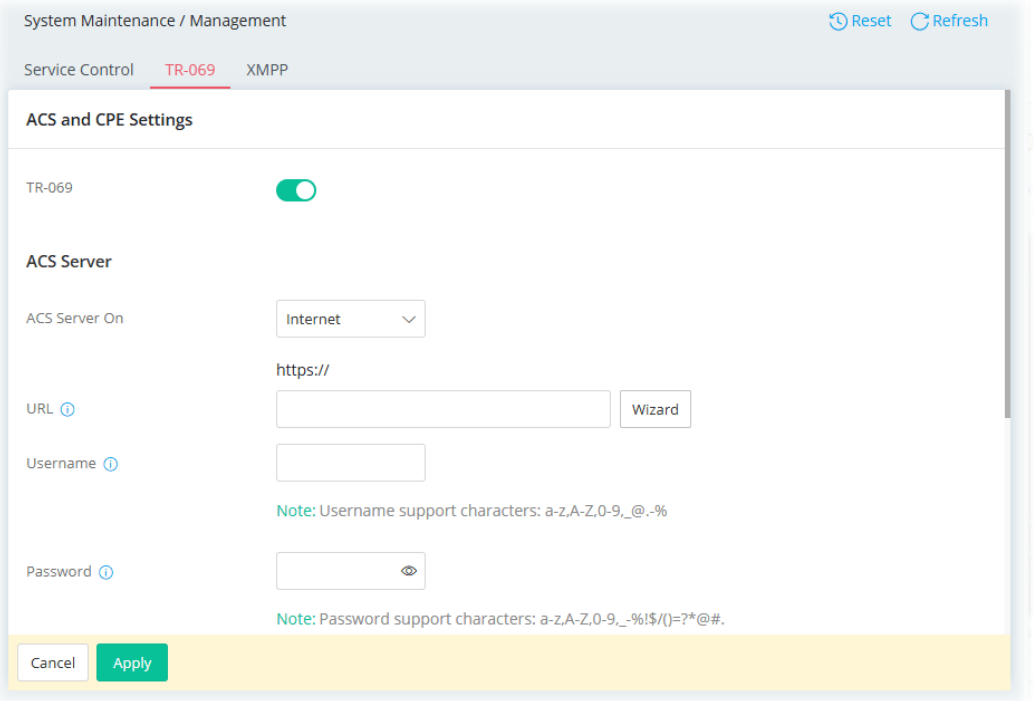
Available settings are explained as follows:

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. 
Login Validation Code	If enabled, the Vigor router will ask users to enter a validation code, as shown in the image, when they log in.
	Management Services
Enforce HTTPS Access	Switch the toggle to enable/disable the feature of allowing system administrators to login Vigor router via HTTPS.
LLDP	Switch the toggle to enable/disable the LLDP service.
mDNS	Switch the toggle to enable/disable the mDNS (Multicast Domain Name System) service.
mDNS Name	Enter a name as the identity in a local network that allows communication with other devices.
Port	Specify user-defined port numbers for the HTTP, HTTPS, SSH, Telnet and SNMP servers.
LAN Access	Select the checkbox to allow the system administrators to login

	from LAN interface. Later, configure the **LAN Access Control** below to determine who (the client) is able to access the LAN management services (HTTP, HTTPS, SSH, Telnet and SNMP).
IPv4/IPv6 WAN Access	Select the checkbox to allow the system administrators to login from IPv4/IPv6 WAN interface. Later, configure the **WAN Access Control** below to determine who (the client) is able to access the IPv4 WAN management services (HTTP, HTTPS, SSH, Telnet and SNMP).
TLS Encryption	
TLS 1.3/TLS 1.2	Switch the toggle to enable or disable the function.
Access Control List	
WAN Access Control	In general, all the clients via WAN interface can access the IPv4 WAN management services (based on the HTTP, HTTPS, SSH, Telnet and SNMP checkboxes selected). **WAN Access Control Mode –** Select Disabled or Allow List. • **Disabled** - The default is **Disabled**. • **Allow List** – Click **+Add** to have a new entry. The maximum number you can add is up to 6. Only the chosen IP objects within the selected IP group object can access the services listed on this page via the WAN interface.
LAN Access Control	In general, all the clients via LAN interface can access the LAN management services (based on the HTTP, HTTPS, SSH, Telnet and SNMP checkboxes selected). **LAN Access Control Mode** - Select Disabled or Allow List. • **Disabled** - The default is **Disabled**. • **Allow List** - Click **+Add** to have a new entry. The maximum number you can add is up to 6. Only the chosen IP objects within the selected IP group object can access the services listed on this page via the LAN interface.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

III-1-2-2 TR-069

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



Available settings are explained as follows:

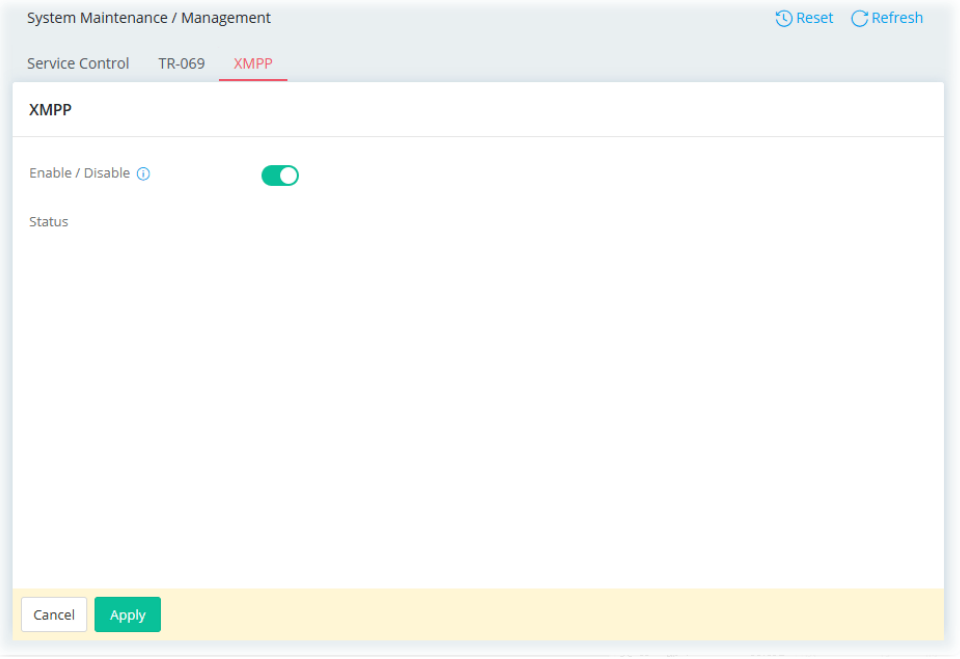
Item	Description
TR-069	Switch the toggle to enable or disable the function.
ACS Server	
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server.
URL	Enter the IP/domain for connecting to the ACS. **Wizard** - Click it to enter the IP address of VigorACS server, port number and the handler.
Username/Password	Enter the credentials required to connect to the ACS server.
Test Connection	
Event Code	Use the drop down menu to specify an event to perform the test. **Test With Inform** - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS server.
More settings	
CPE Client	This section specifies the settings of the CPE Client. **Protocol** - Select HTTPS if the connection is encrypted; otherwise select HTTP. **Port** - In the event of port conflicts, change the port number of the CPE. **Username / Password** - Enter the username and password that the VigorACS will use to connect to the CPE.

Periodic Inform Settings	**Enable / Disable** - Switch the toggle to enable or disable the function. The default setting is Enable, which means the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field. **Time Interval** - Set interval time or schedule time for the router to send notification to CPE.
STUN Settings	**Mode** - The default is **Auto**. If select **Enabled**, please enter the relational settings listed below: • **Server Address** - Enter the IP address of the STUN server. • **Server STUN Port** - Enter the port number (1-65535) of the STUN server. • **Minimum Keep Alive Period** - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". • **Maximum Keep Alive Period** - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
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.

III-1-2-3 XMPP

XMPP is an abbreviation of Extensible Messaging and Presence Protocol. If your device is registered with the XMPP server, it can help VigorACS manage the access point under NAT at any time without obstruction.



Switch the toggle of Enable/Disable to enable or disable the XMPP feature.

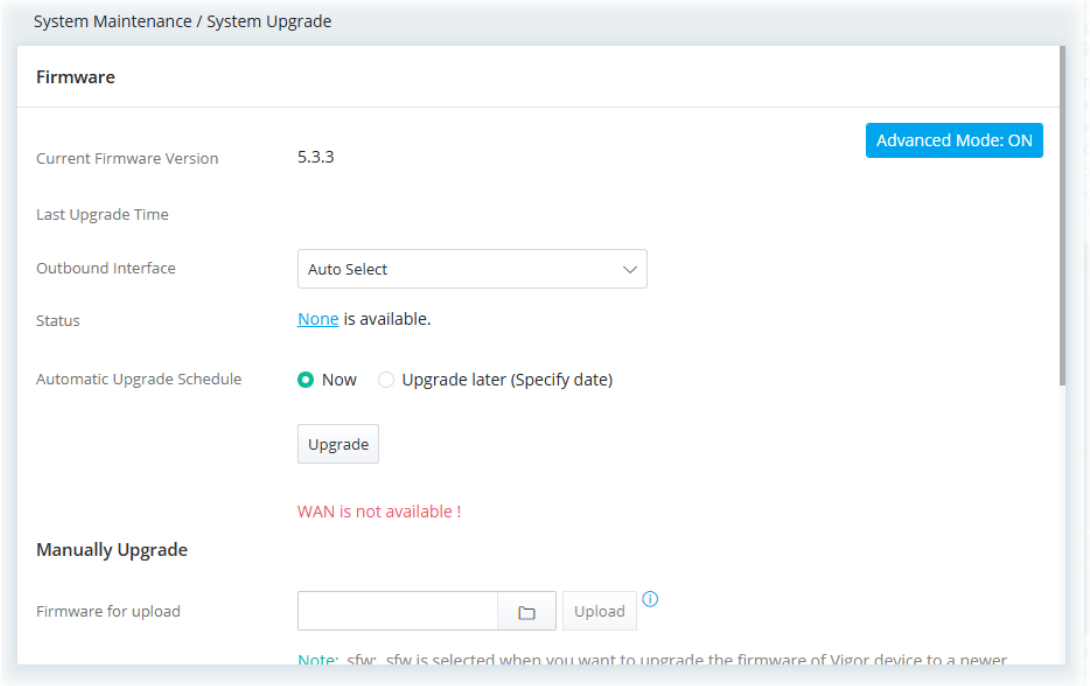
III-1-3 System Upgrade

III-1-3-1 Firmware

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

There are two methods to execute the firmware upgrade.

- **Manual Upgrade** - 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.
- **Automatic Upgrade** – The Vigor router system now offers automatic firmware upgrade feature (optionally, default is disabled), making it convenient for users to stay updated on crucial firmware changes, security issues, and significant bugs that necessitate immediate firmware update. With this feature, there is no need to download the latest firmware version yourself. The Vigor system will automatically detect the latest release, download it, and upgrade the router. This option is particularly beneficial for addressing critical security issues and fixing major bugs.



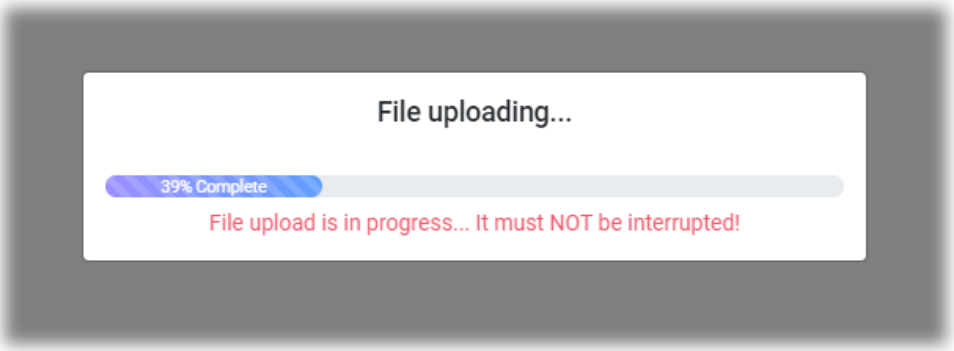
Available settings are explained as follows:

Item	Description
Advanced Mode: ON/OFF	Click to show or hide the advanced settings for system upgrade.
Current Firmware Version	Display current firmware version.
Outbound Interface	Select the WAN interface that will be used to download the firmware from the DrayTek website for automatic upgrade. Then select an IP or IP alias for the chosen WAN. The default is **Auto Select.**
Automatic Upgrade	**Now** – Select and click Upgrade to upgrade the firmware

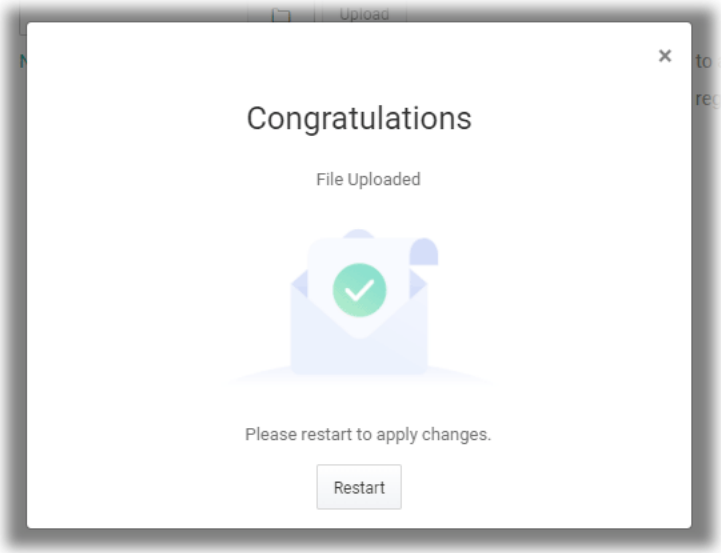
Schedule	immediately. **Upgrade later (Specify date) -** Upgrade the firmware at a specified time and date. • **Off** – Disable the function of scheduled update. • **Specify date** – Specify a date to upgrade the firmware. **Upgrade** – Click to upgrade the firmware immediately.
Manually Upgrade	
Firmware for upload	- Click to locate the firmware file for upgrade. **Upload** – Click to upload the selected file onto Vigor system.
Automatic Upgrade for General Updates	
Enabled Automatically Upgrade	Default is disabled. Switch the toggle to enable/disable automatic firmware upgrade within a designated time.
Upgrade Timing	Set the timing for the firmware upgrade. **In the middle of the night** – The firmware upgrade will take place at midnight. **Schedule Update** - The firmware upgrade will take place on a specified on one day and time in a week.
Automatic Upgrade for Critical Updates	
Enable Critical Security and Major Bug Fixes	Vigor router will perform the system upgrade automatically once receiving the newly firmware with critical security issue and major bug fixed. Default is disabled. Switch the toggle to enable/disable this feature.
Upgrade Timing	Set the timing for the firmware upgrade. **In the middle of the night** – The firmware upgrade will take place at midnight. **Schedule Update** - The firmware upgrade will take place on a specified on one day and time in a week.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

Click to locate the firmware from your host.

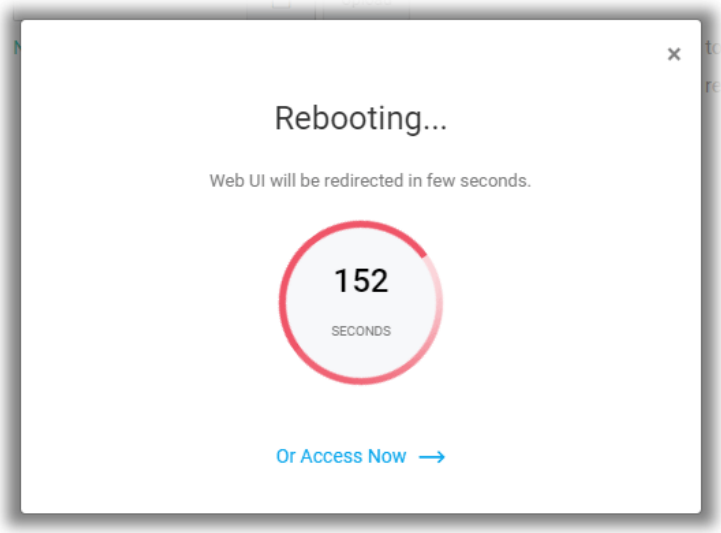
Then click **Upload** and wait for a few seconds.



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

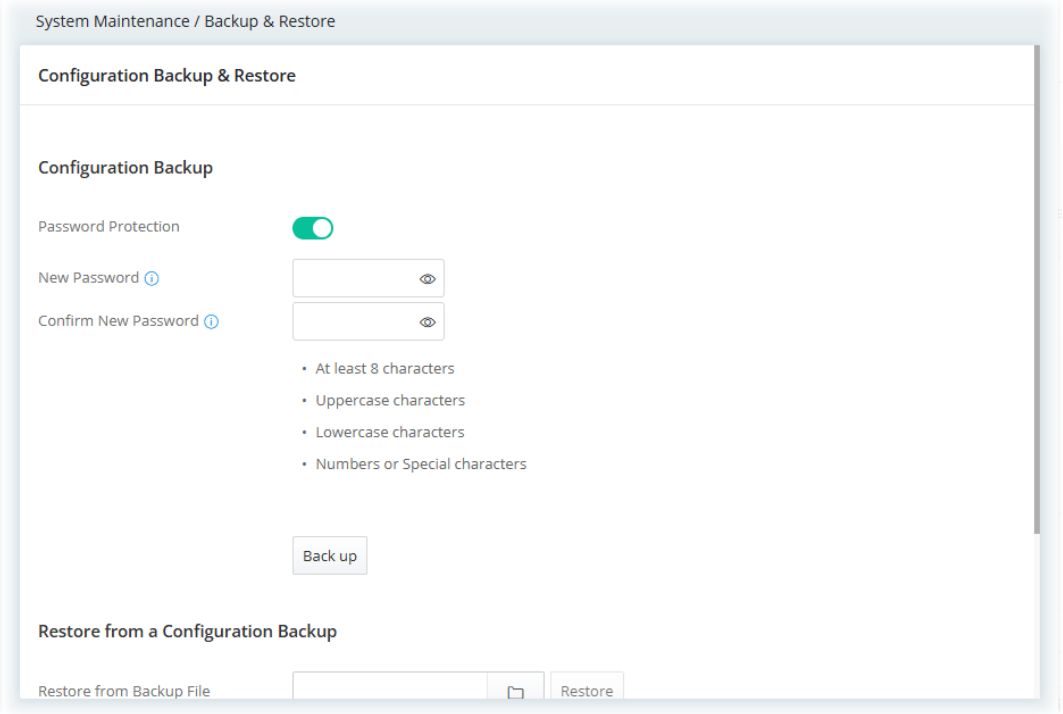


Wait for a while until the system finishes the rebooting.



III-1-4 Backup & Restore

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



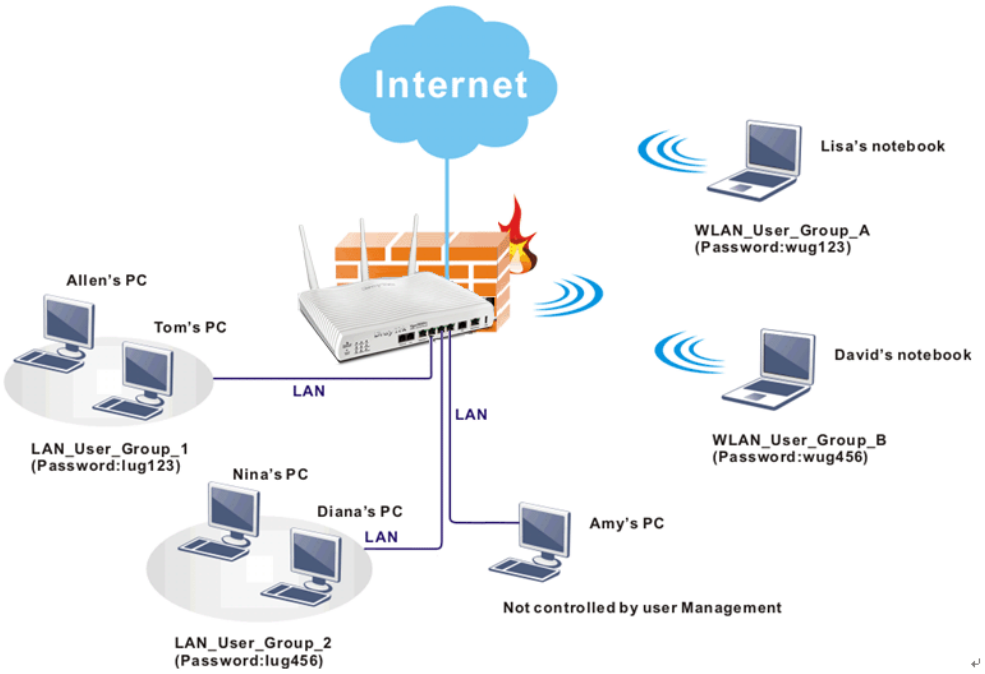
Available settings are explained as follows:

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

III-1-5 Accounts & Permission

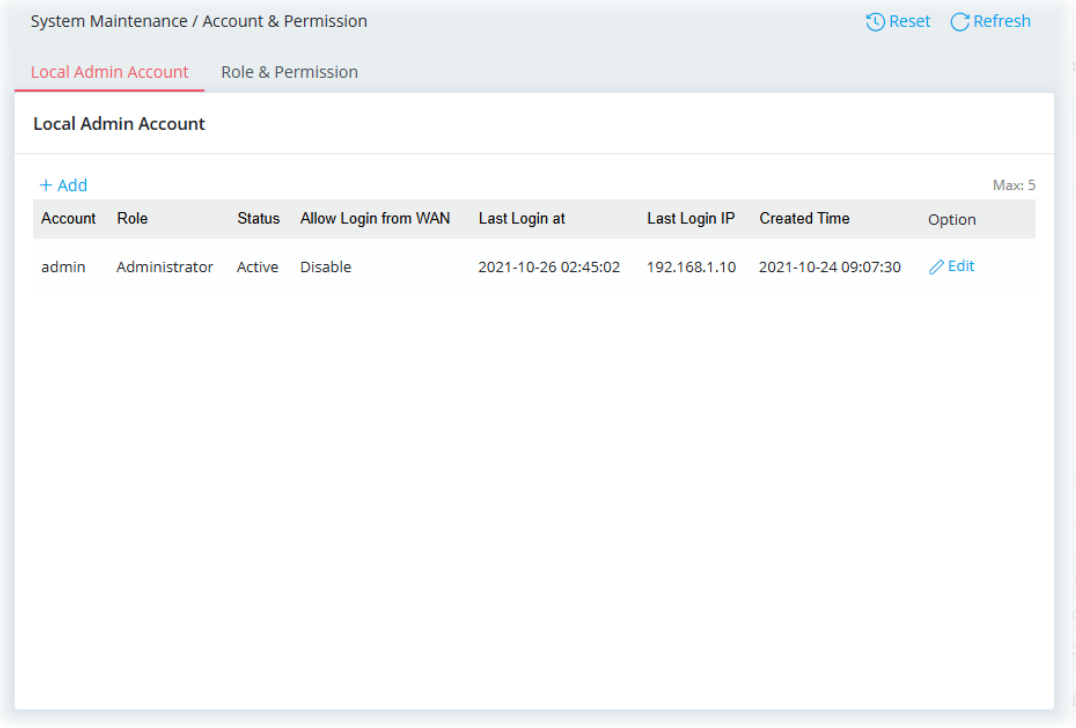
This page allows you to modify your current administration account and password.

It allows the network administrator to manage Internet access at the user level.



III-1-5-1 Local Admin Account

This page allows you to create up to five local admin account profiles.

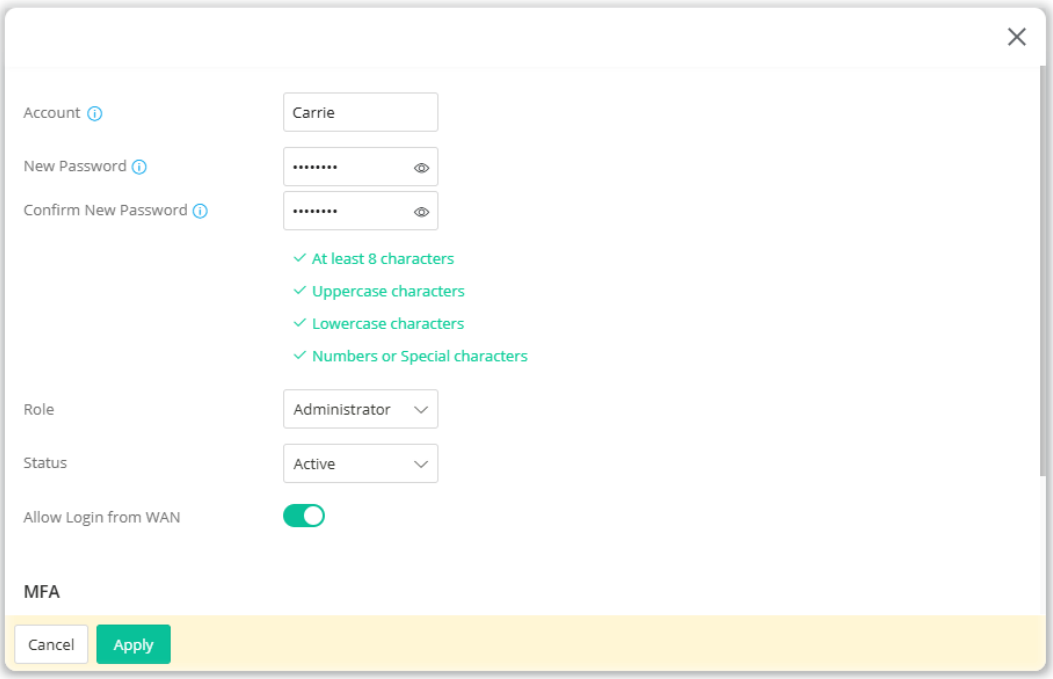


Available settings are explained as follows:

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** • **Users (created on the Role & Permission page)**
Status	**Active** - Enable the selected account profile. **Inactive** - Disable the selected account profile.
Allow Login from WAN	It is available if "Router Management" is selected as the usage. If enabled, the user can login from WAN by using this user account.
MFA	
Enable MFA	Switch the toggle to enable/disable the function of Multi-Factor Authentication (MFA). **Allowed MFA Method** - Select to require mOTP, TOTP, SMS or email authentication when logging in from the WAN.

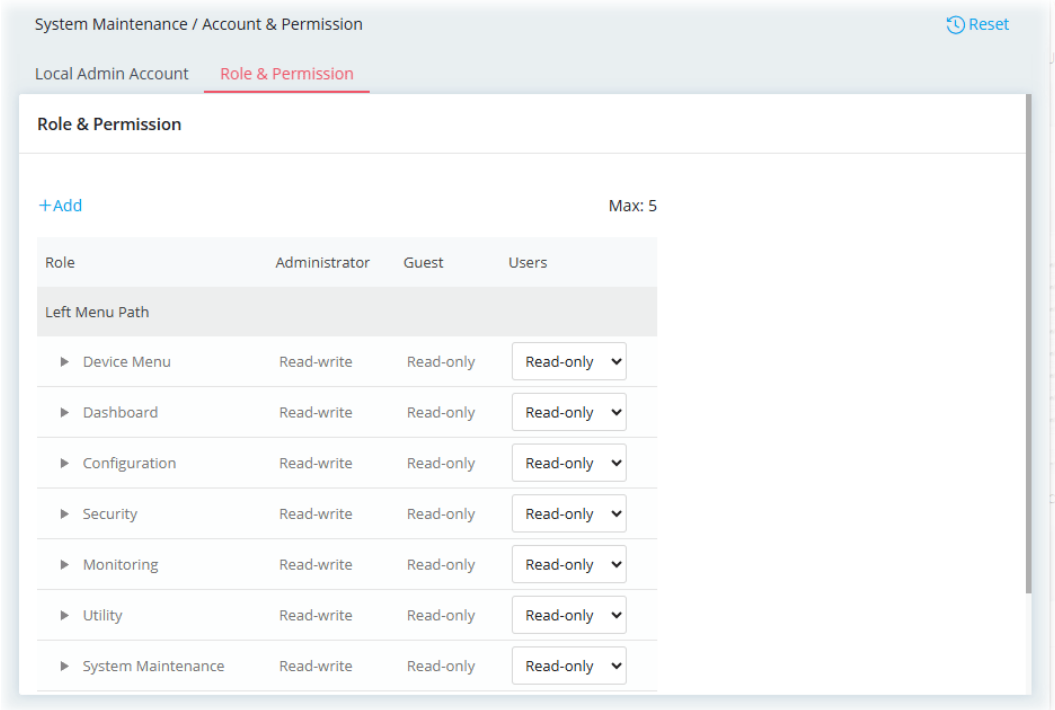
	TOTP – For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone. Select TOTP and click Apply. A pop-up dialog will appear as follows:  In the filed of Validation Code, enter the one-time password and click Verify. Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication. **SMS/Email** – The password will be sent via SMS or email as selected above. **mOTP** - Mobile one-Time Password (mOTP) allows the use of mOTP passwords. Enter the **PIN Code** and **Secret** settings for getting one-time passwords.
Account Info	
Created Time	Display the created time of the user account.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

Click **Apply** to save the settings.

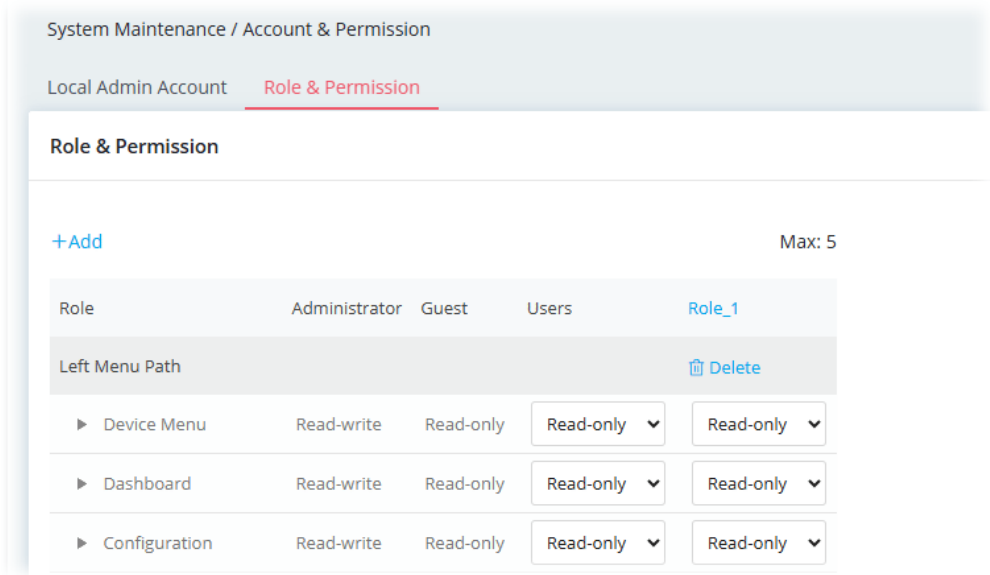
III-1-5-2 Role & Permission

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

The default roles are Administrator, Guest and Users.

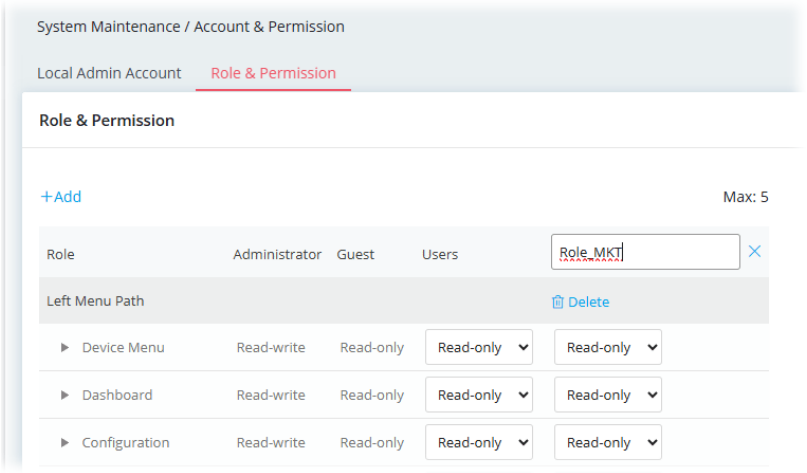
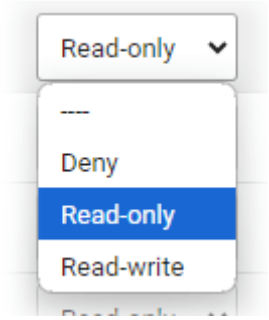


To create a new role profile, click **+Add**. A new role will be added on to the page.

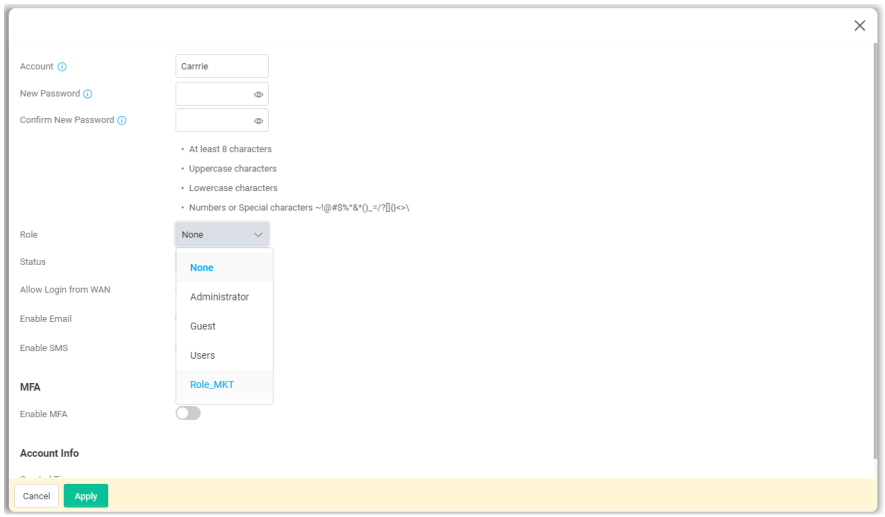


Available settings are explained as follows:

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).

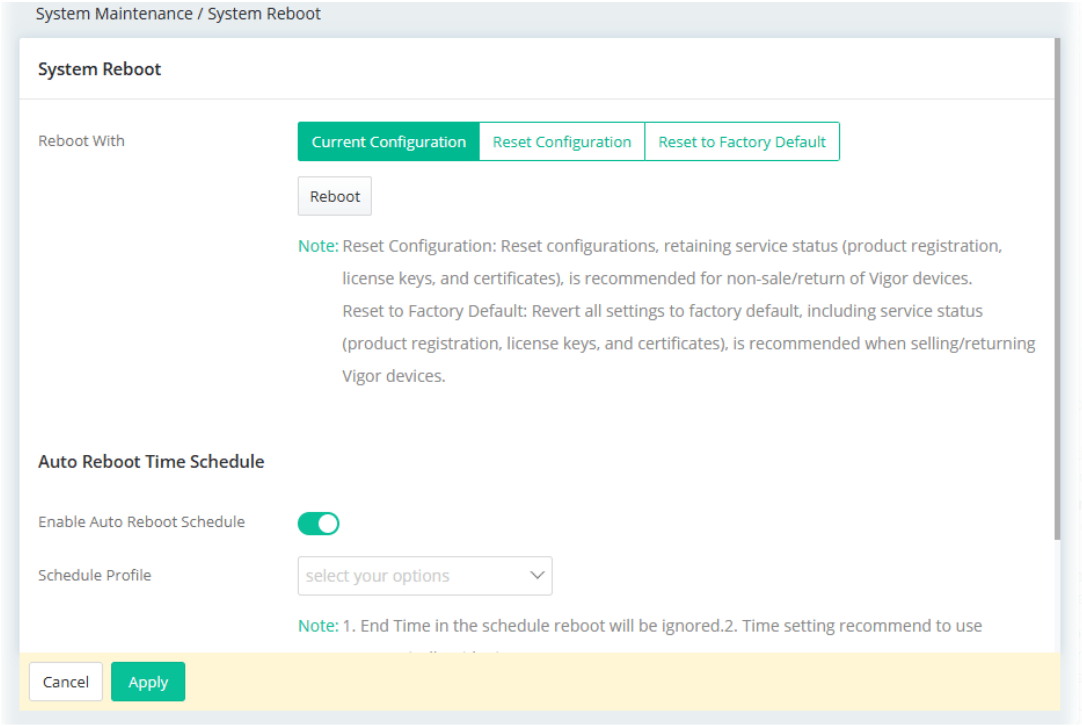
	
Left Menu Path	Lists all of the features that a role can have. The role of **Administrator** has the highest authority for accessing Vigor router. The role of **Guest/Users** has the lowest authority for accessing Vigor router. The permissions for user-defined roles are based on read-only or read-write 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**.



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.

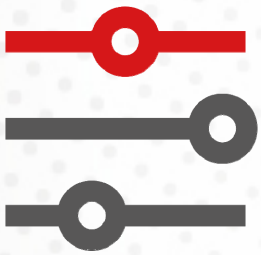


Available settings are explained as follows:

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. **Reset Configuration** – Select this option to reset the router while retaining service status (product registration, license keys, and certificates). **Reset to Factory Default** – Select this option to reset the router's configuration to the factory defaults before rebooting. **Reboot** – Click to reboot the router immediately.
Auto Reboot Time Schedule	**Enable Auto Reboot Schedule** – Switch the toggle to enable or disable the function. If enabled, Vigor router will reboot automatically based on the schedule profile. **Schedule Profile** – Use the drop-down list to select the profile(s).

This page is left blank.

Chapter IV Others

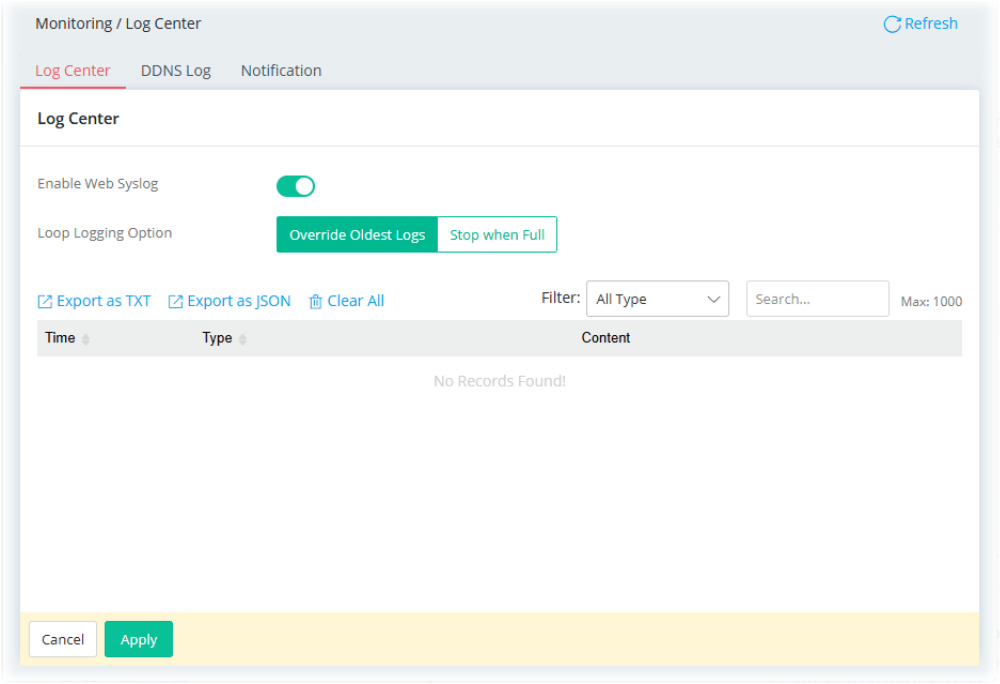


IV-1 Monitoring

IV-1-1 Log Center

IV-1-1-1 Log Center

Log related to setting configuration and/or actions performed by this device can be stored on web Syslog. Click **Refresh** to reload this page with the most up-to-date information.



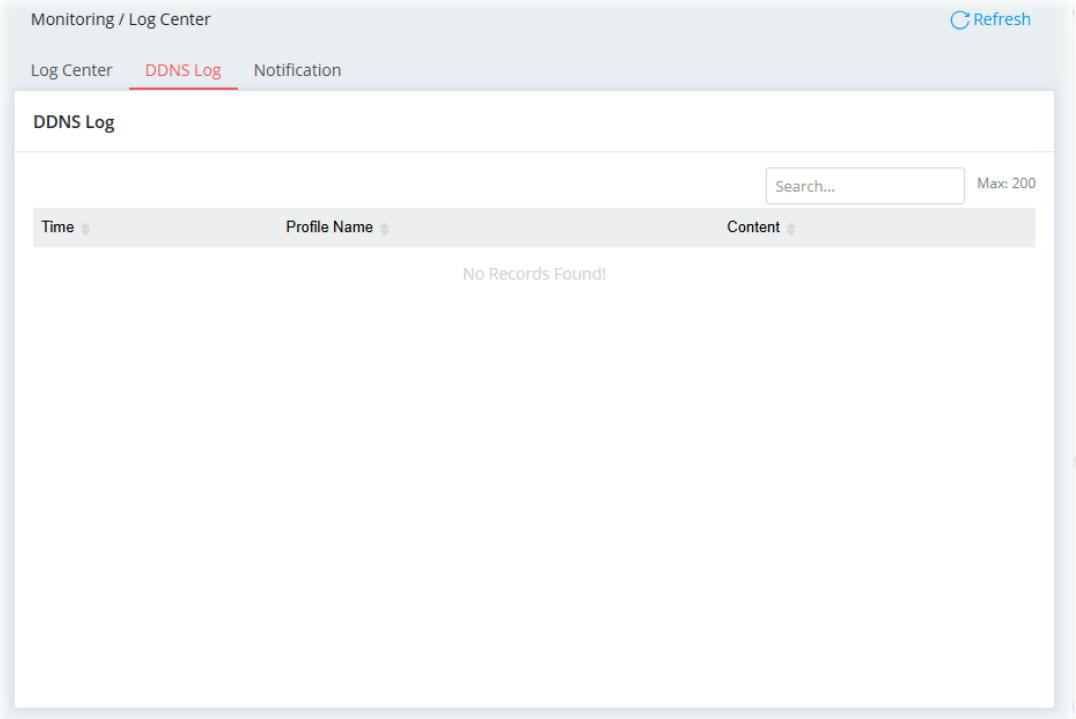
Available settings are explained as follows:

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

Click **Apply** to save the settings.

IV-1-1-2 DDNS Log

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

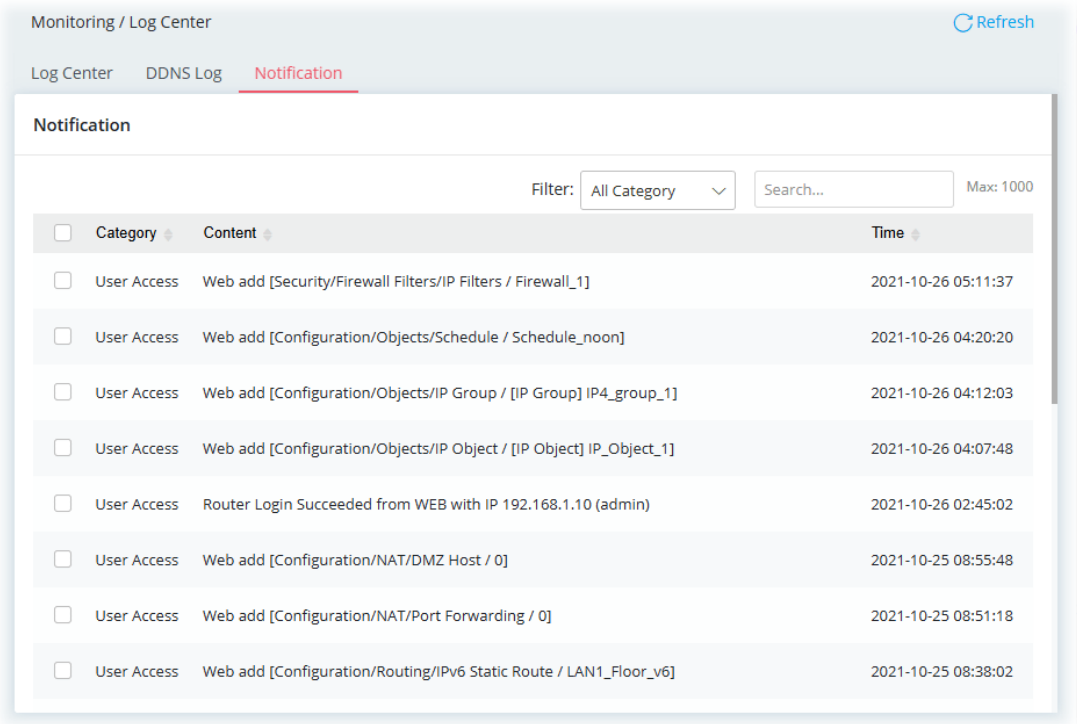


Click **Refresh** to reload this page with the most up-to-date information.

IV-1-1-3 Notification

This page displays important log information, including:

- important message
- the notification of SSH/Telnet Login, Web Login
- the notification of the firmware upgrade status
- the notification of configuration convert (restoration or update)


Monitoring / Log Center
Refresh
Log Center
DDNS Log
Notification
Notification
Filter:
All Category
Search...
Max: 1000
Category
Content
Time
User Access
Web add [Security/Firewall Filters/IP Filters / Firewall_1]
2021-10-26 05:11:37
User Access
Web add [Configuration/Objects/Schedule / Schedule_noon]
2021-10-26 04:20:20
User Access
Web add [Configuration/Objects/IP Group / [IP Group] IP4_group_1]
2021-10-26 04:12:03
User Access
Web add [Configuration/Objects/IP Object / [IP Object] IP_Object_1]
2021-10-26 04:07:48
User Access
Router Login Succeeded from WEB with IP 192.168.1.10 (admin)
2021-10-26 02:45:02
User Access
Web add [Configuration/NAT/DMZ Host / 0]
2021-10-25 08:55:48
User Access
Web add [Configuration/NAT/Port Forwarding / 0]
2021-10-25 08:51:18
User Access
Web add [Configuration/Routing/IPv6 Static Route / LAN1_Floor_v6]
2021-10-25 08:38:02

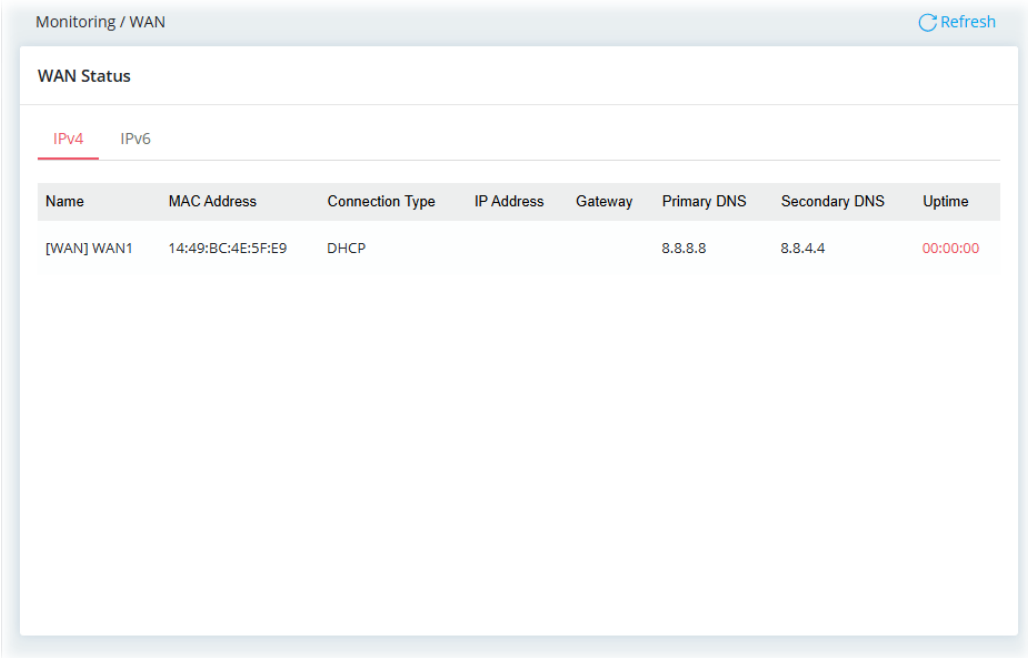
IV-1-2 WAN

This page can display the WAN connection status, including the connection interface, MAC address, connection type, connection IP address, connection gateway, primary DNS and secondary DNS server addresses, online Time, and so on.

IV-1-2-1 WAN Status

IPv4

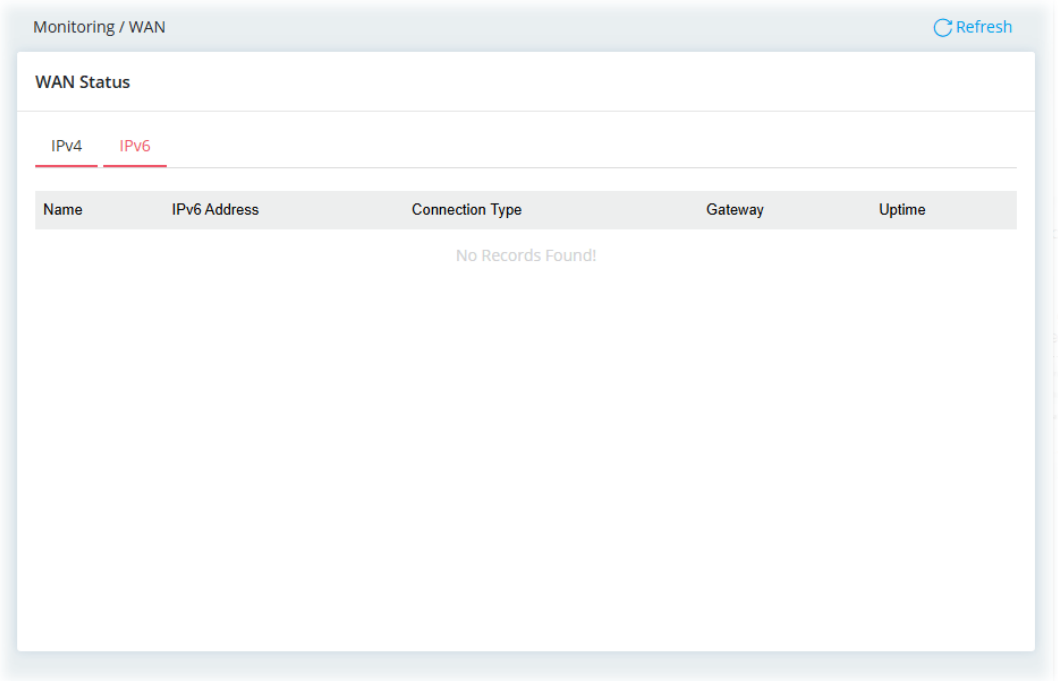
Select the IPv4 tab to display the IPv4 WAN connection status.



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

IPv6

Select the IPv6 tab to get the WAN connection information (e.g., name, IPv6 address, connection type, gateway and the uptime).



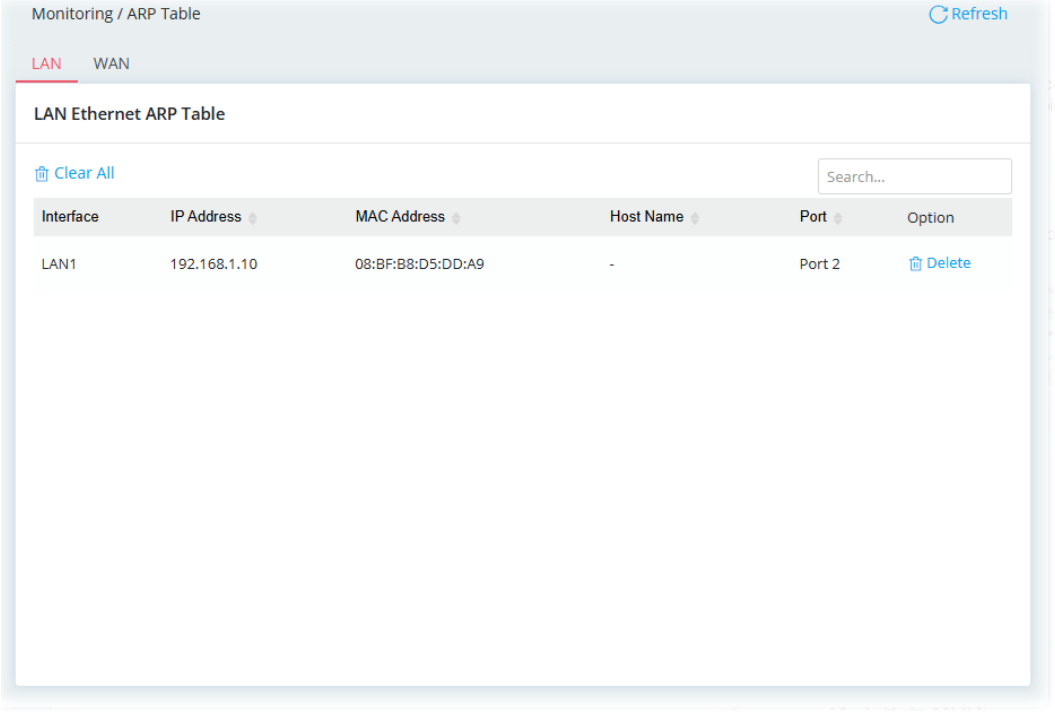
Click **Refresh** to reload this page with the most up-to-date information.

IV-1-3 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.

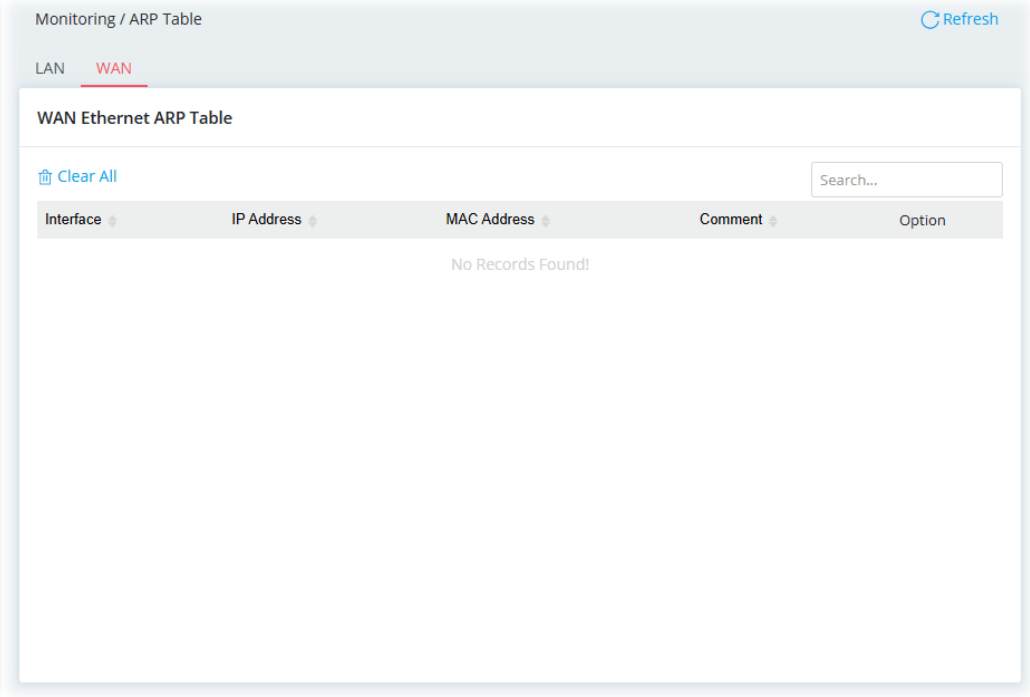
IV-1-3-1 LAN

Click **Refresh** to reload this page with the most up-to-date information of LAN Ethernet ARP table.



IV-1-3-2 WAN

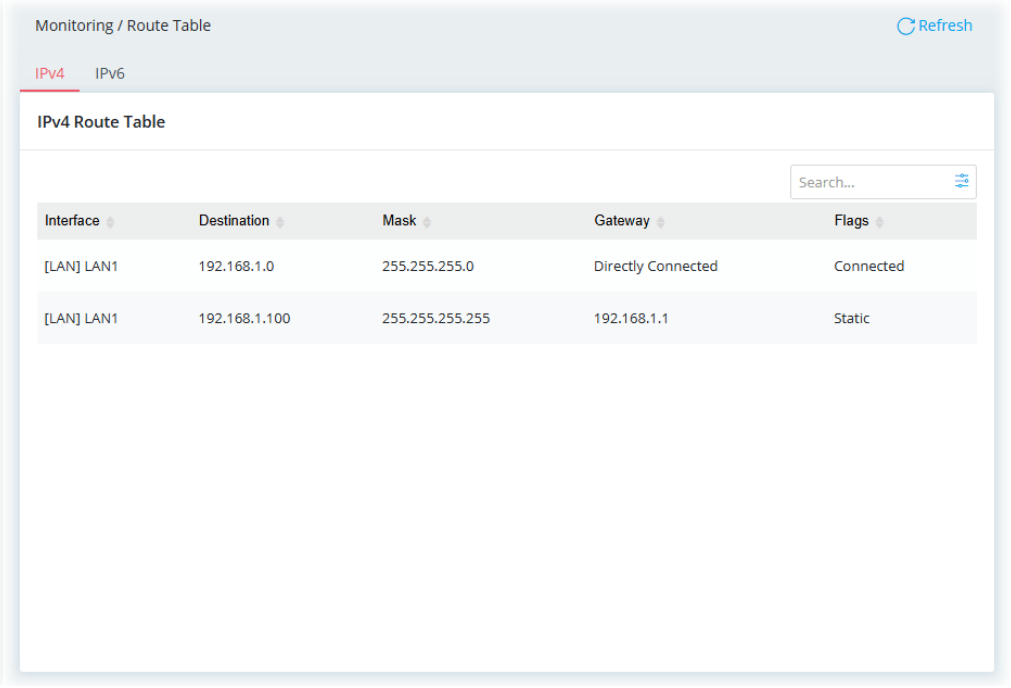
Click **Refresh** to reload this page with the most up-to-date information of WAN Ethernet ARP table.



IV-1-4 Route Table

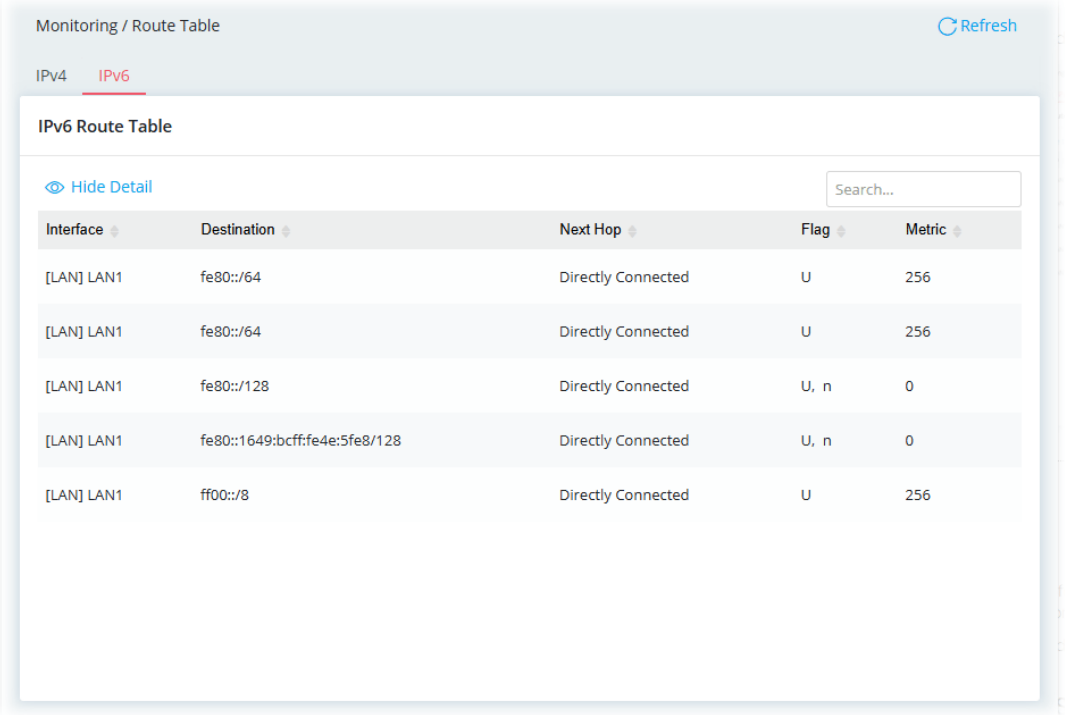
IV-1-4-1 IPv4

Click **Refresh** to reload this page with the most up-to-date IPv4 routing information.



IV-1-4-2 IPv6

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



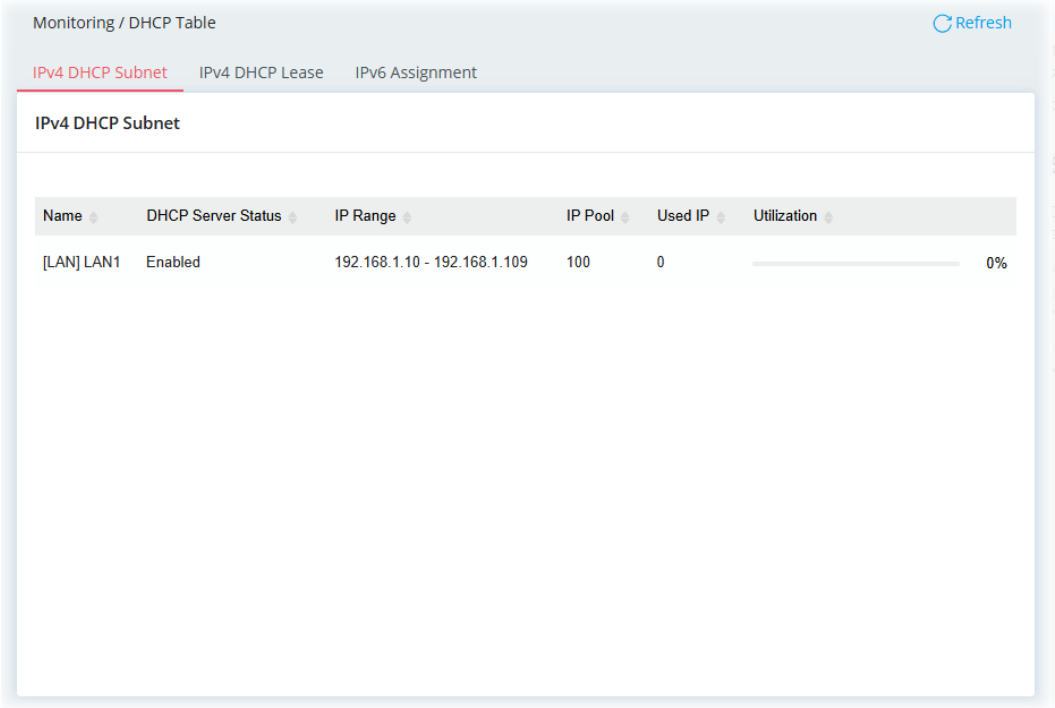
IV-1-5 DHCP Table

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.

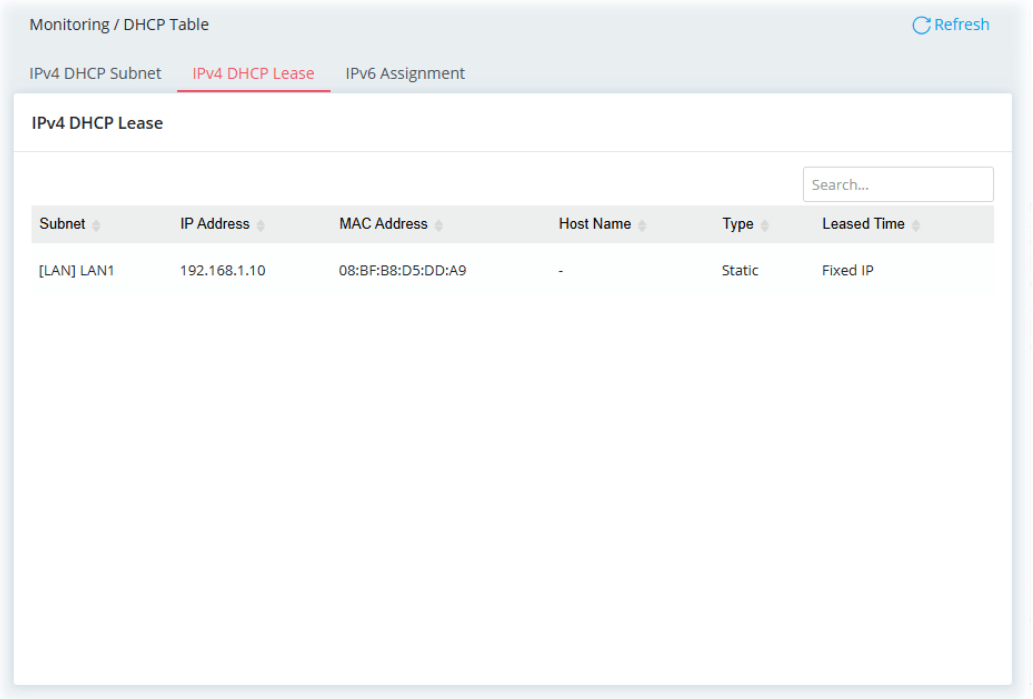
IV-1-5-1 IPv4 DHCP Subnet

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



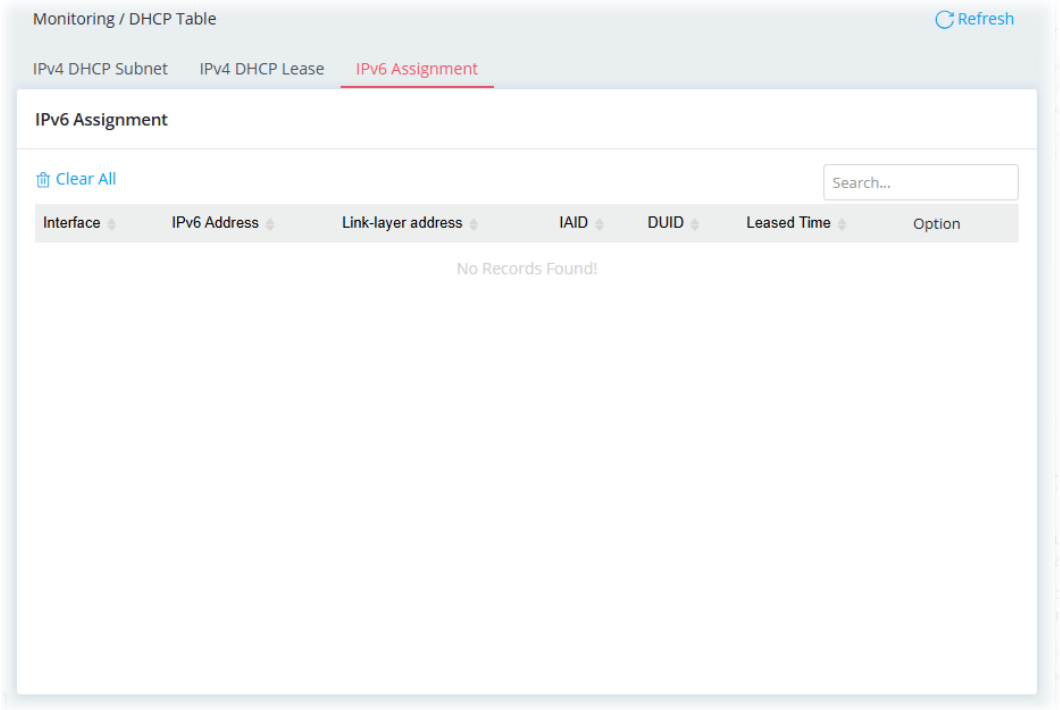
IV-1-5-2 IPv4 DHCP Lease

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


Monitoring / DHCP Table
Refresh
IPv4 DHCP Subnet
IPv4 DHCP Lease
IPv6 Assignment
IPv4 DHCP Lease
Search...
Subnet
IP Address
MAC Address
Host Name
Type
Leased Time
[LAN] LAN1
192.168.1.10
08:BF:B8:D5:DD:A9
-
Static
Fixed IP

IV-1-5-3 IPv6 Assignment

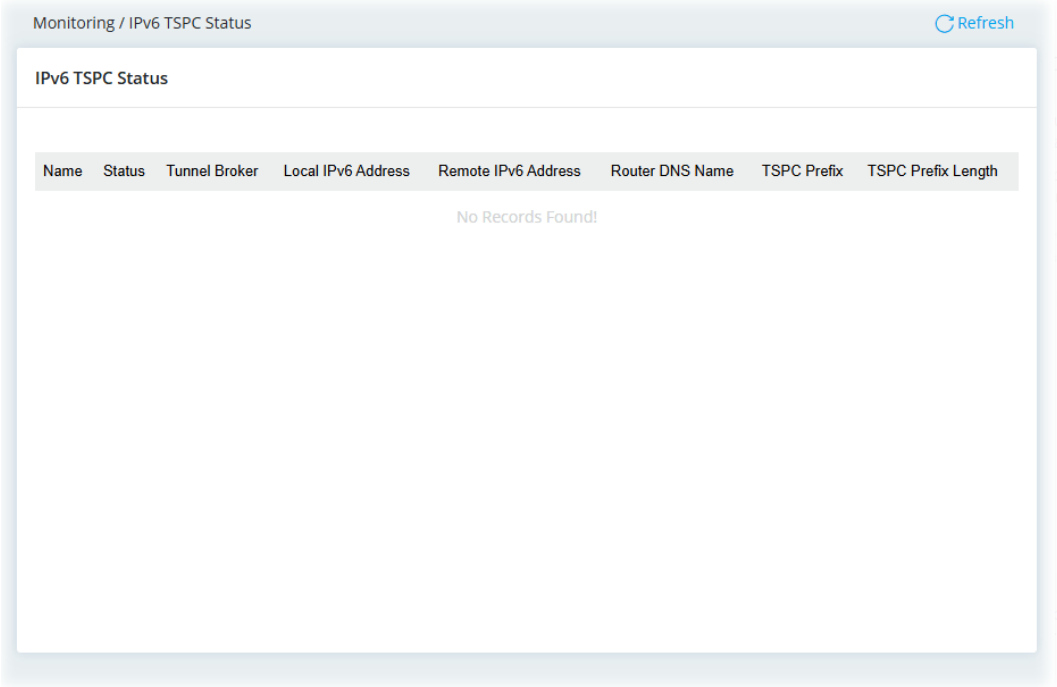
This page shows the remaining time of the IPv6 DHCP lease of the device.



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.

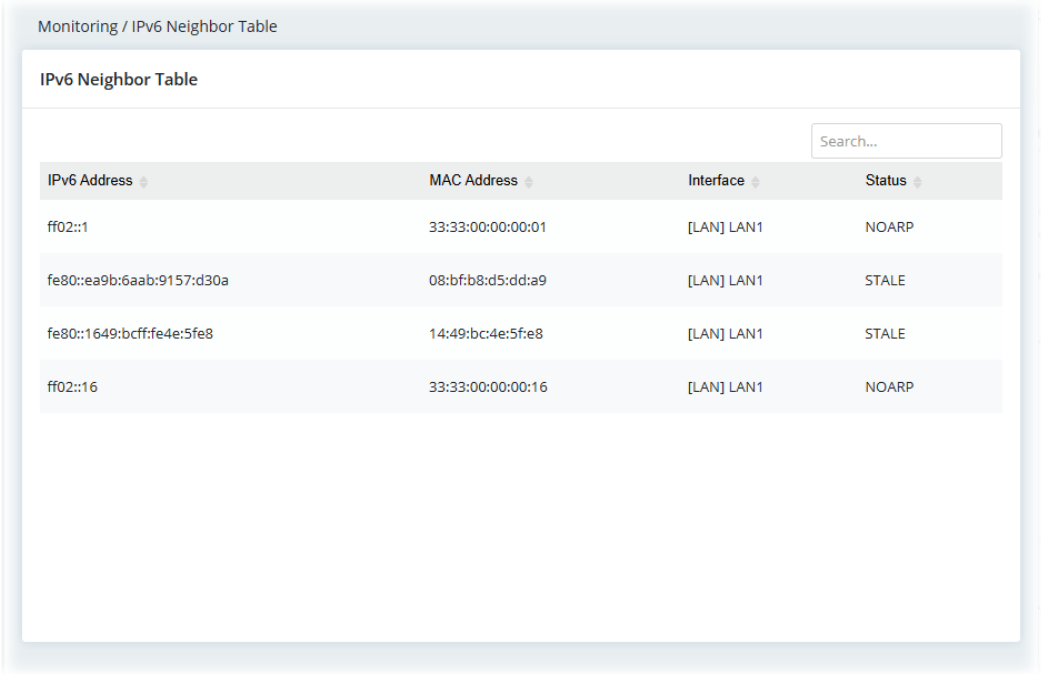
If TSPC is configured properly, the router will display the following when the router has connected to the tunnel broker successfully.



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

IV-1-7 IPv6 Neighbor Table

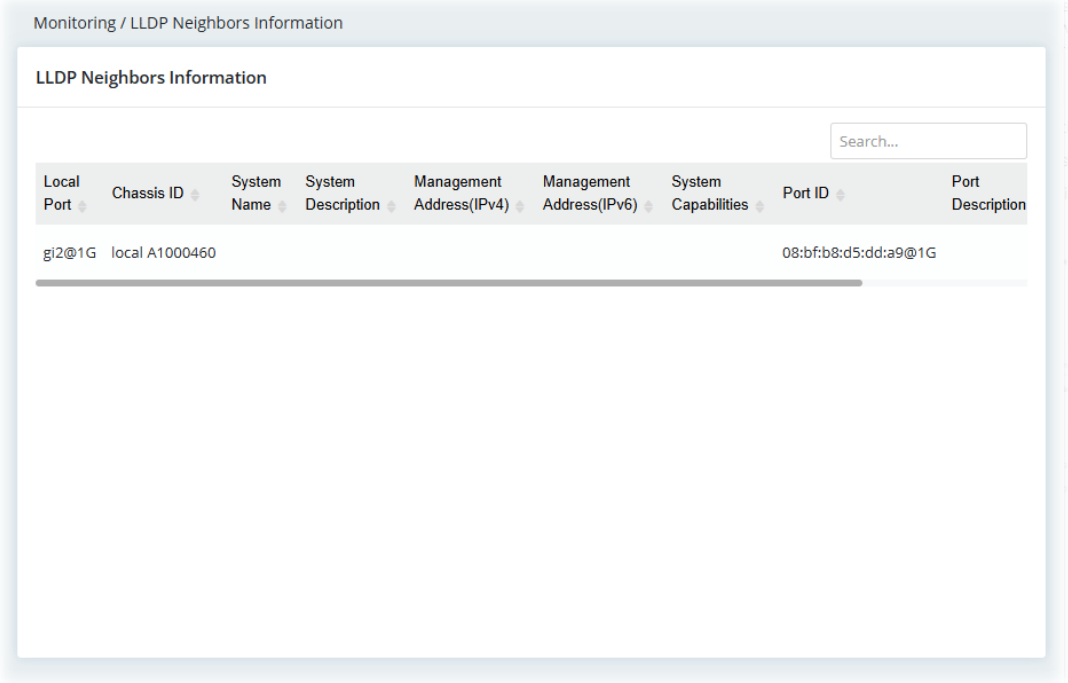
This page displays the mapping between Ethernet hardware addresses (MAC addresses) and the IPv6 addresses. This information is helpful in diagnosing network problems, such as IP address conflicts.



IV-1-8 LLDP Neighbors Information

This page allows the system administrator to understand the topology of network devices and the relationships between devices. Usually, information includes:

- Chassis ID
- System name
- System Description
- IPv4/IPv6 address (optional)
- System Capabilities
- Port ID
- Port Description
- Time
- Time to Live

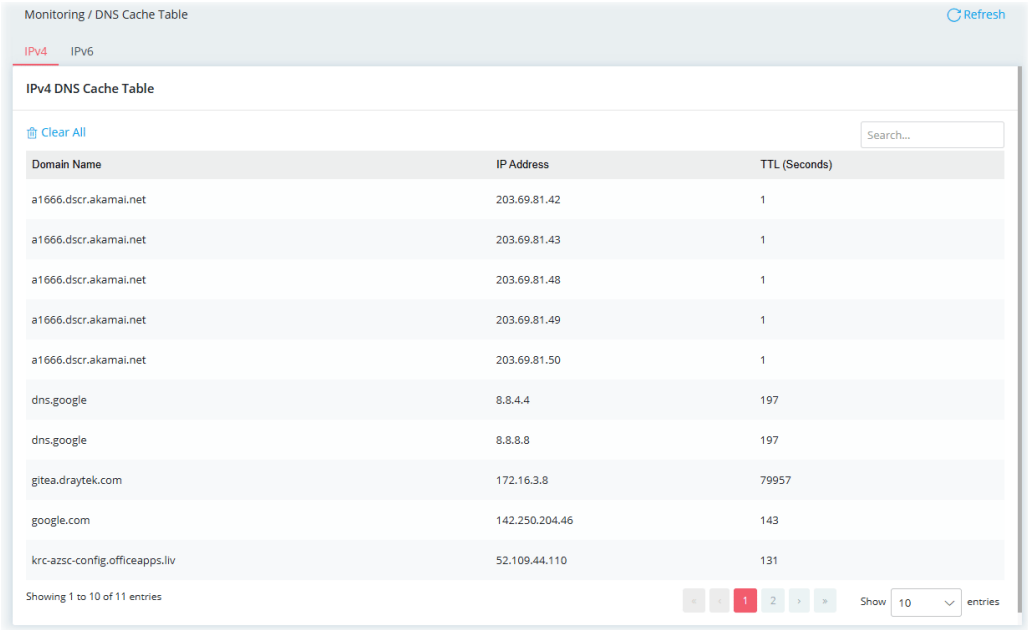


IV-1-9 DNS Cache Table

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

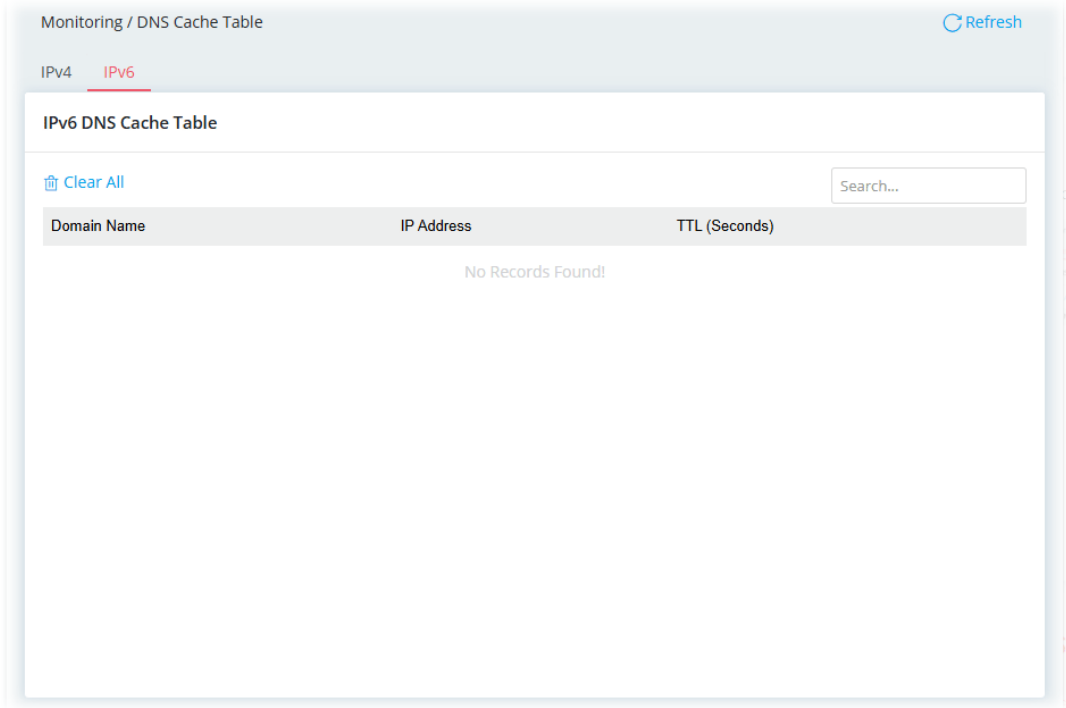
IV-1-9-1 IPv4

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



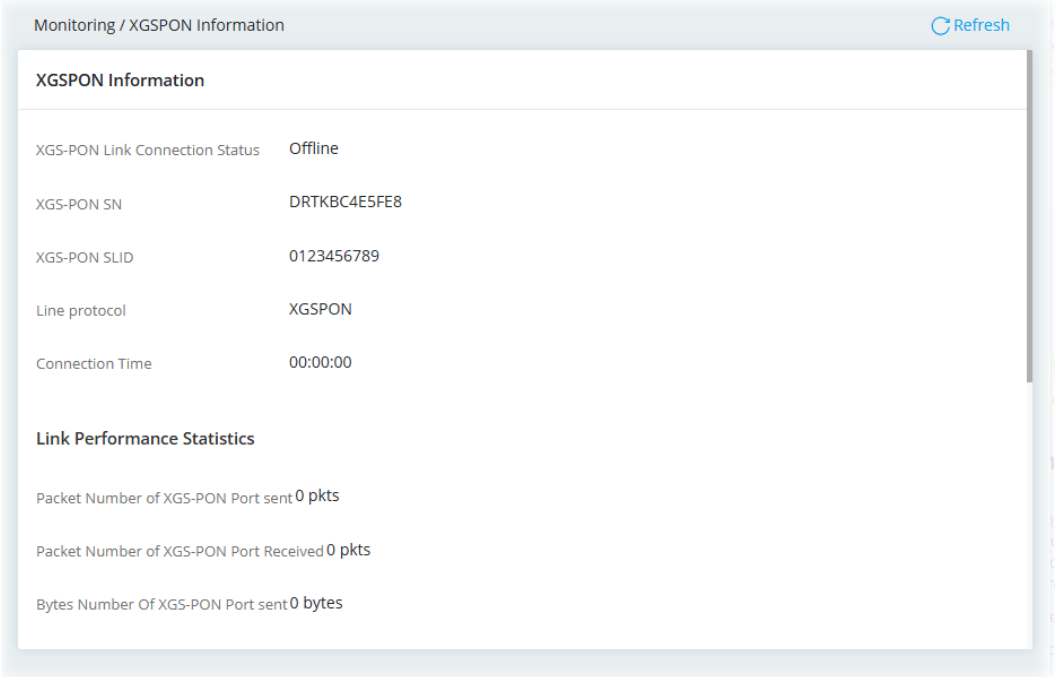
IV-1-9-2 IPv6

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



IV-1-10 XGSPON Status

This page displays detailed information about packets transmitted and received through the XGSPON port, including link performance statistics as well as SN and SLID information.

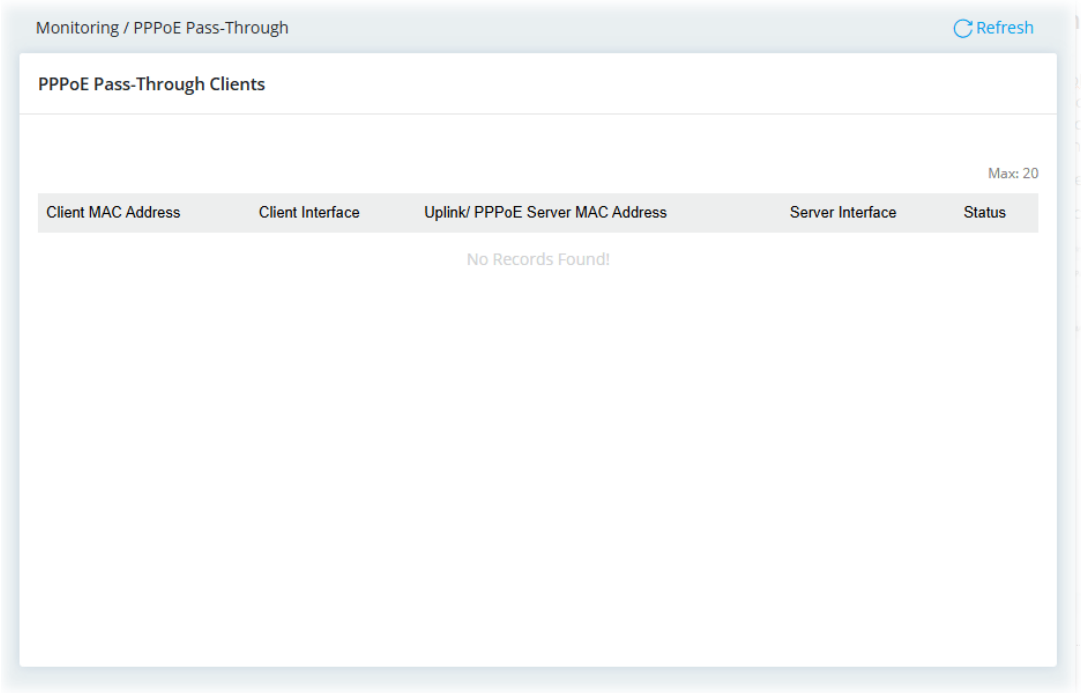


IV-1-11 PPPoE Pass-Through

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.

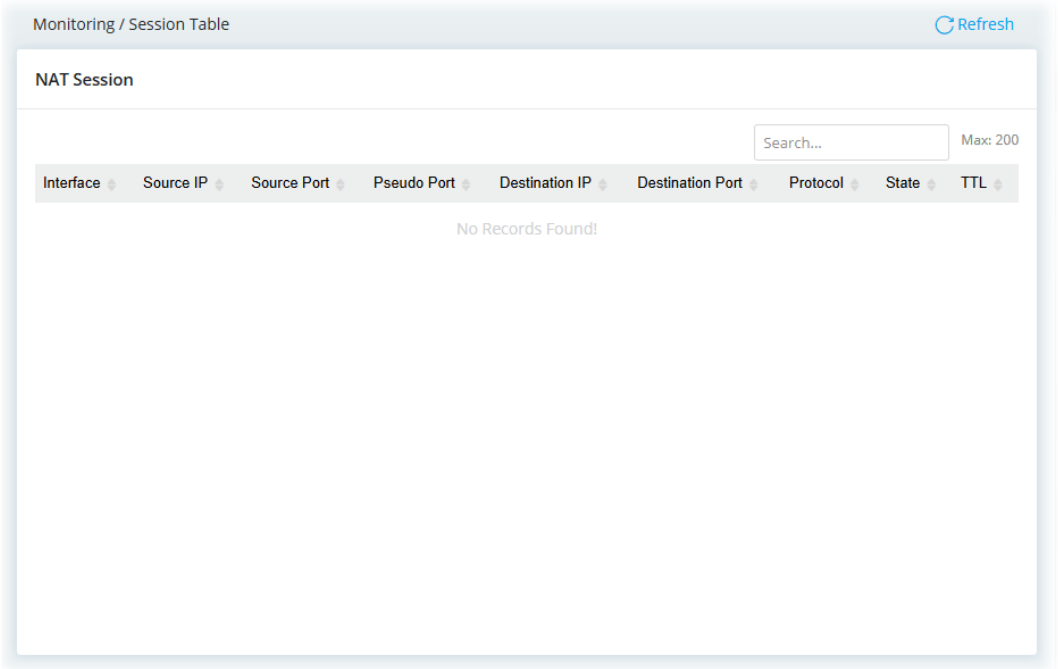
This page displays the results of performing PPPoE Pass-Through.

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


Monitoring / PPPoE Pass-Through
Refresh
PPPoE Pass-Through Clients
Max: 20
Client MAC Address
Client Interface
Uplink/ PPPoE Server MAC Address
Server Interface
Status
No Records Found!

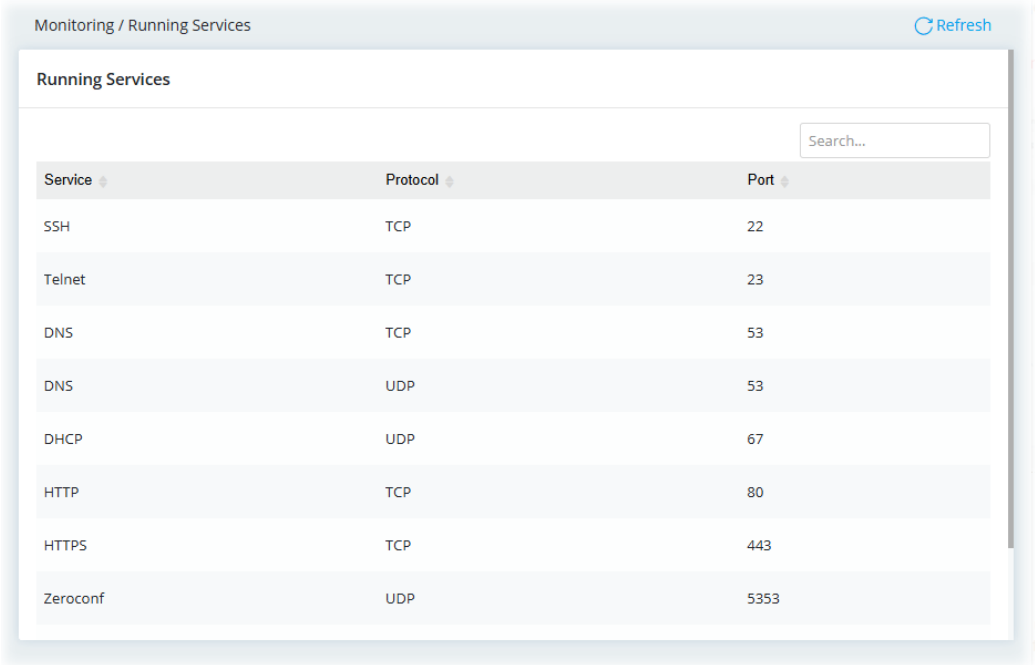
IV-1-12 Session Table

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-1-13 Running Services

This screen shows current running services (service name, protocol and the port number) for Vigor router.



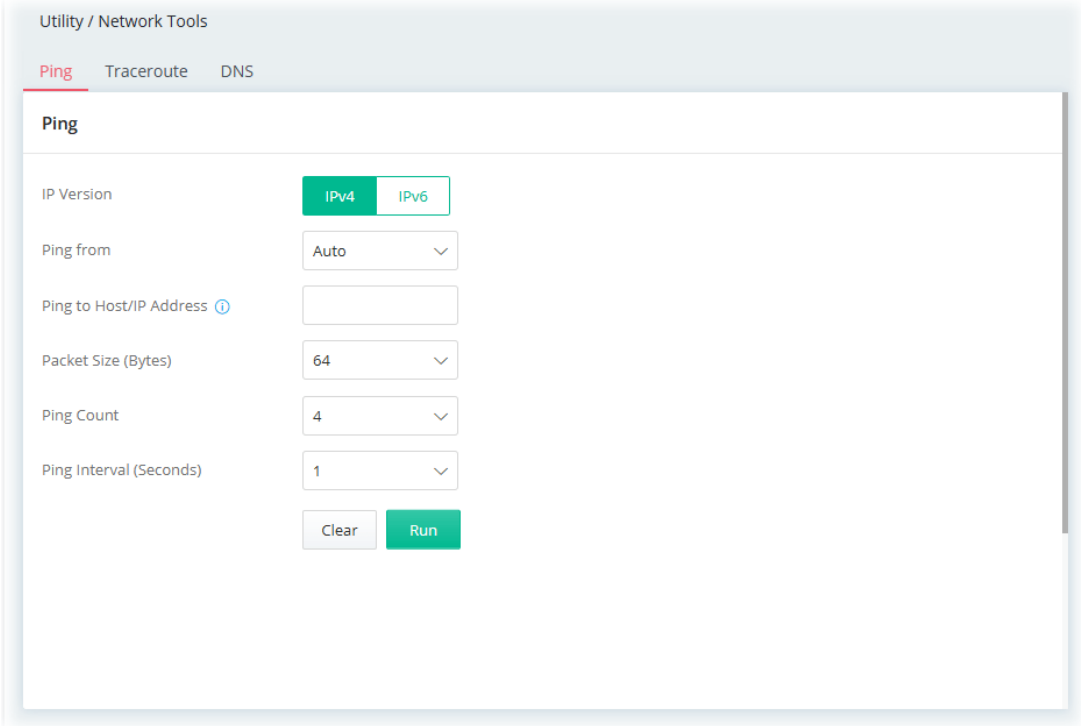
IV-2 Utility

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

IV-2-1 Network Tools

IV-2-1-1 Ping Tool

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



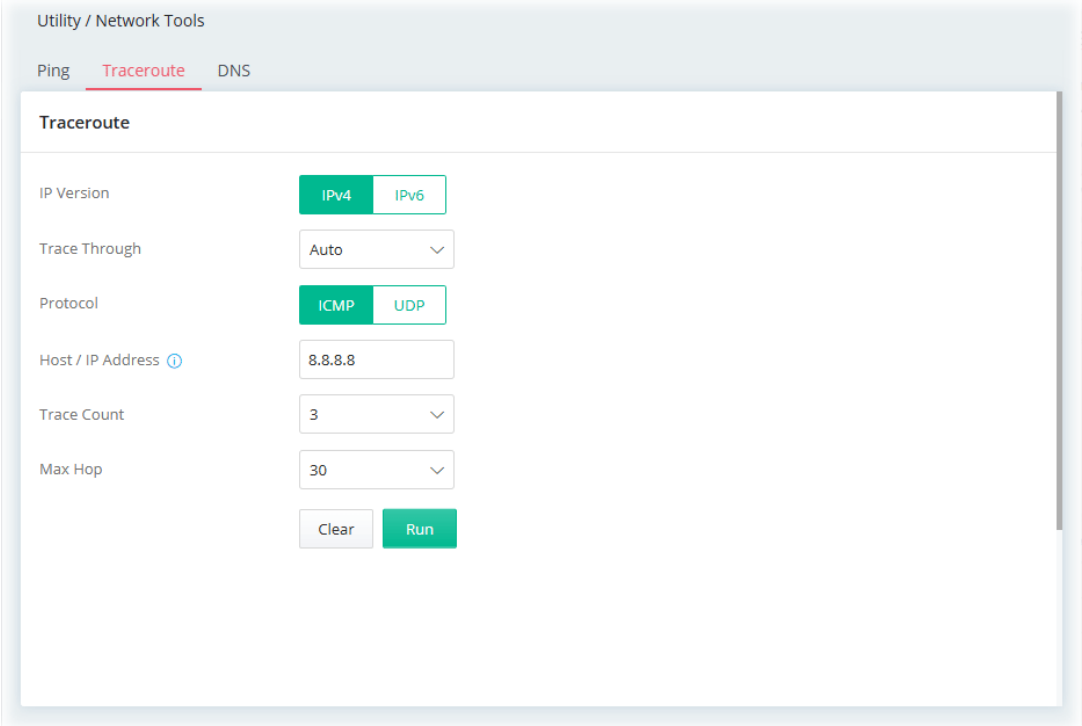
Available settings are explained as follows:

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-2-1-2 Traceroute

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

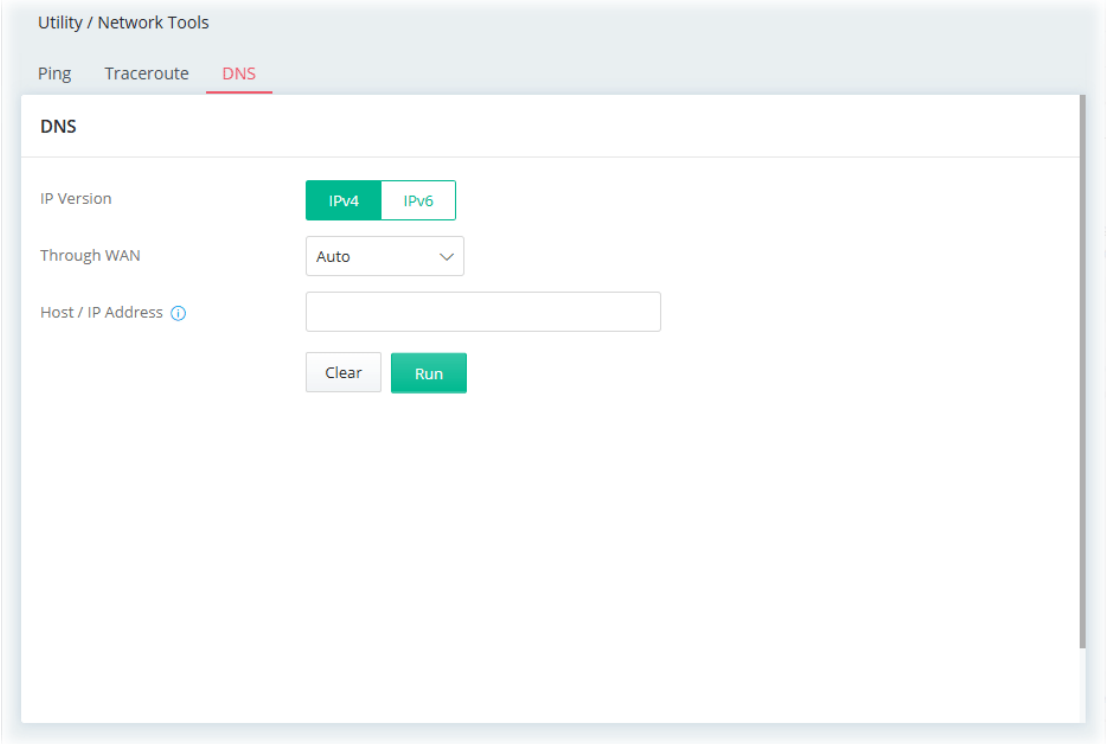


Available settings are explained as follows:

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 traceroute.
Trace Count	Select the max hops for traceroute, select none for unlimited.
Max Hop	Set the maximum number of hops to search for the target.
Clear	Remove the settings and return to the factory settings.
Run	Perform the job.

IV-2-1-3 DNS

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



Available settings are explained as follows:

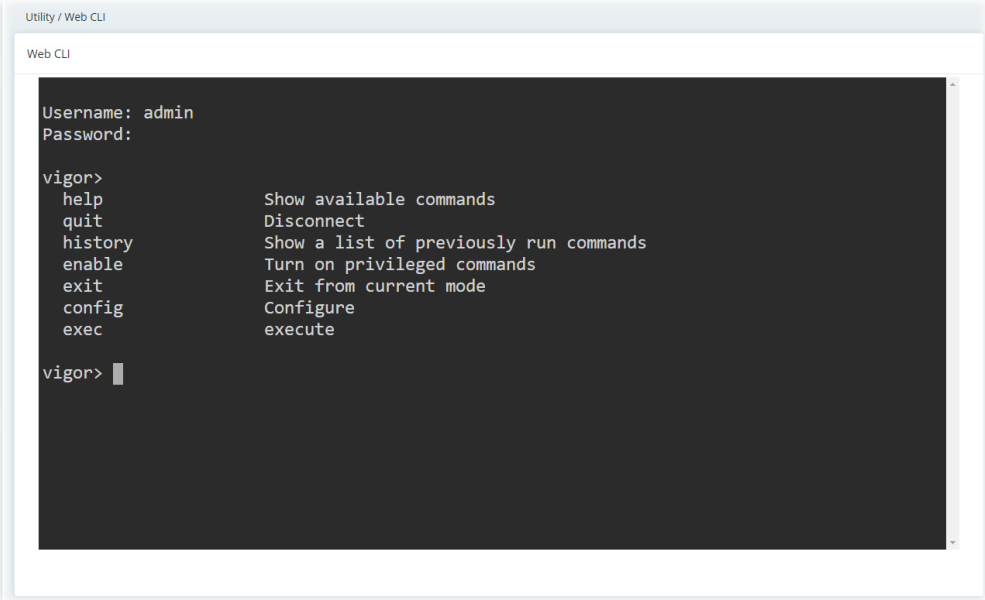
Item	Description
IP Version	Select the IP version for entering correct IP address.
Through WAN	Select an interface for DNS query.
Host/IP Address	Enter the domain name or IP address for DNS query to get corresponding information.
Clear	Remove the settings and return to the factory settings.
Run	Perform the job.

IV-2-2 Web CLI

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

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

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



This page is left blank.

Chapter V Troubleshooting

V-1 Checking the Hardware Status

Follow the steps below to verify the hardware status.

1. Check the power line and cable connections.
   Refer to "**I-2 Hardware Installation"** for details.
2. Power on the router. Make sure the **PWR** 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.

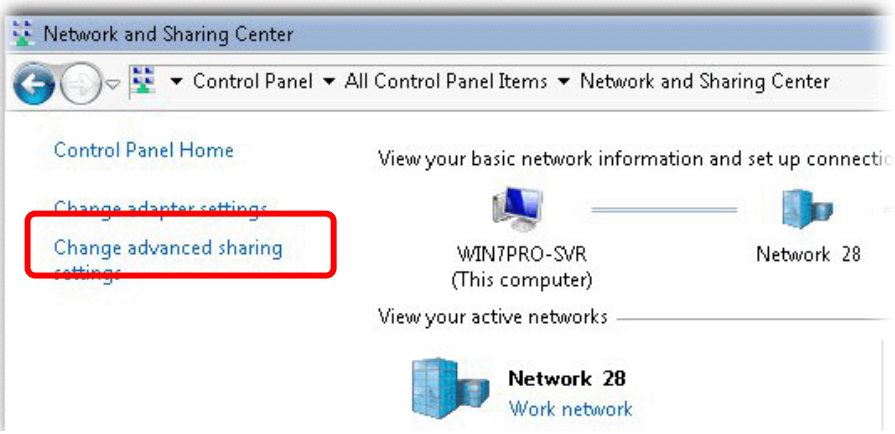
V-2-1 For Windows

Note:

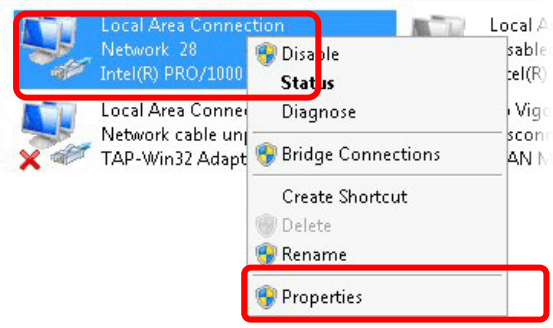
The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

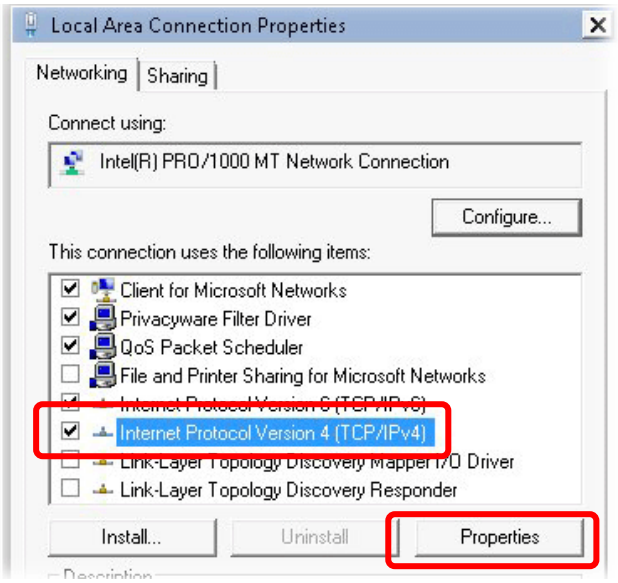
2. In the following window, click **Change adapter settings**.



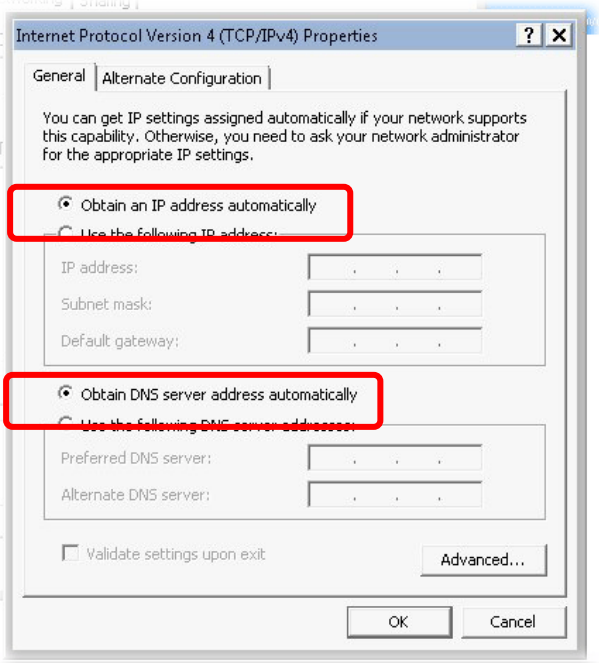
3. Icons of the network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

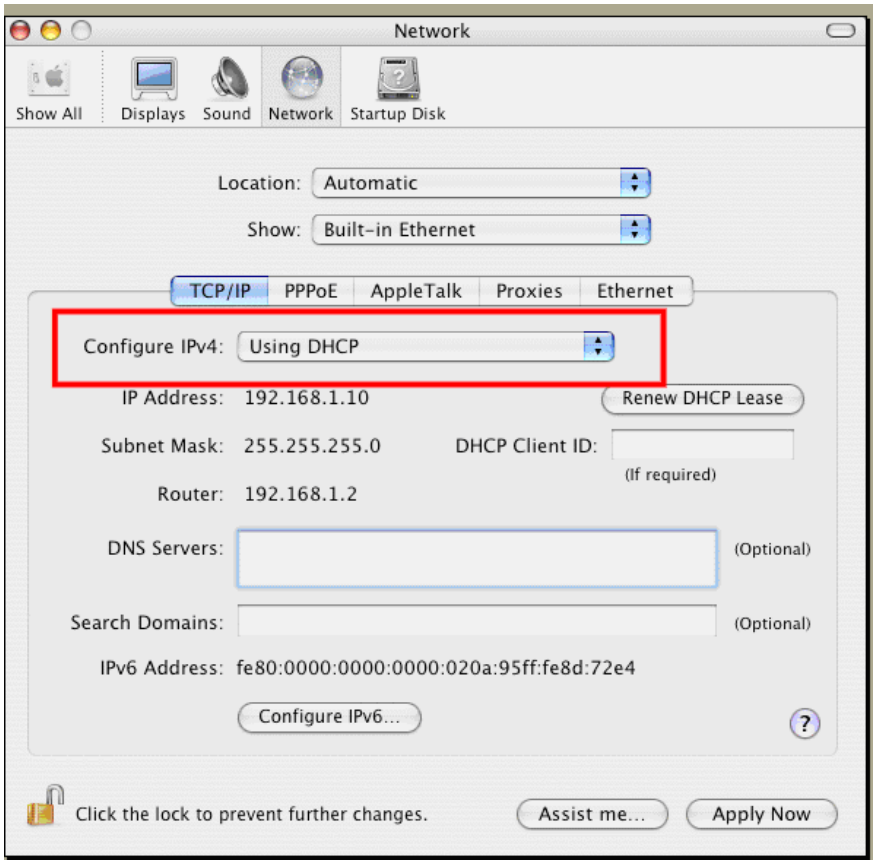


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



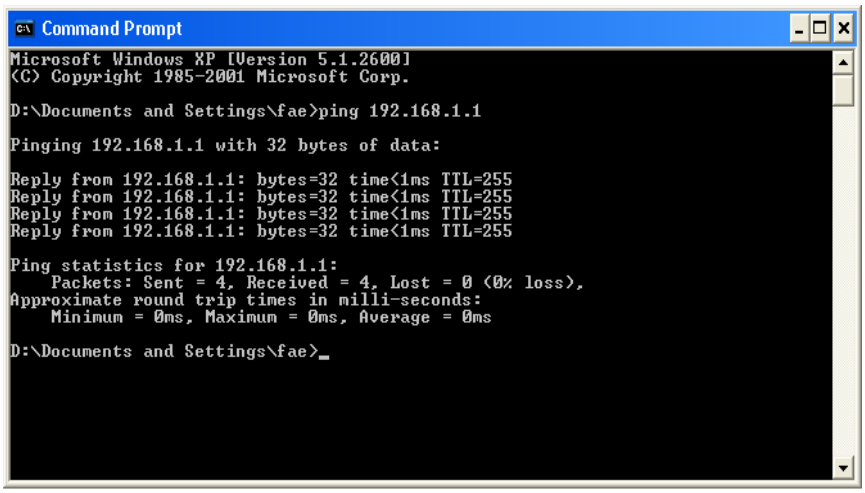
V-3 Pinging the Device

The default gateway IP address of the modem is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section V-2)

Please follow the steps below to ping the modem correctly.

V-3-1 For Windows

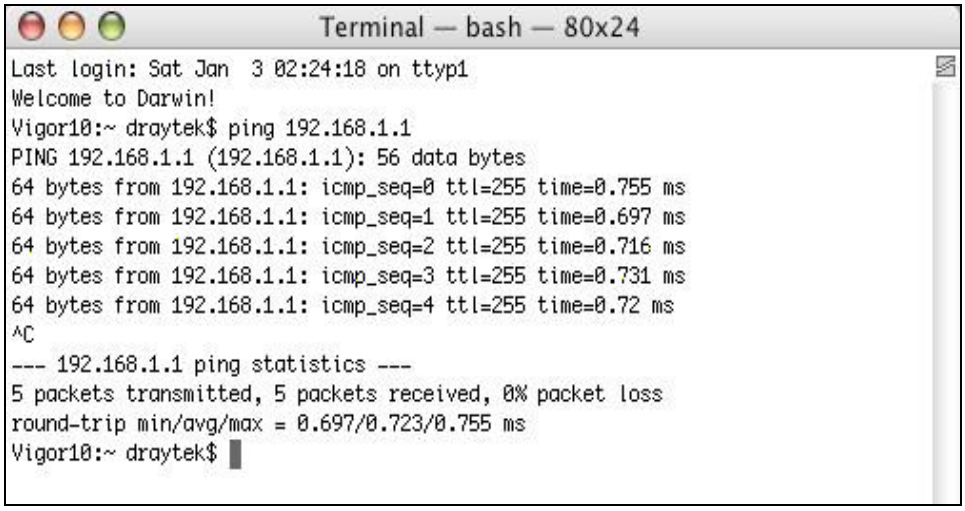
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **cmd**. The DOS command dialog will appear.



3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

V-3-2 For Mac Os (Terminal)

1. Double click on the current used Mac Os on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.


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:

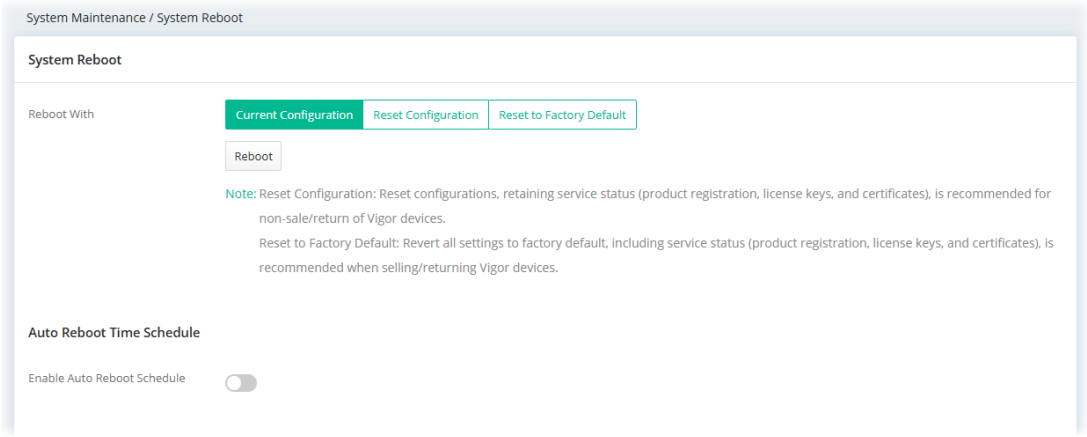
After using the factory default settings, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing.

V-4-1 Software Reset

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

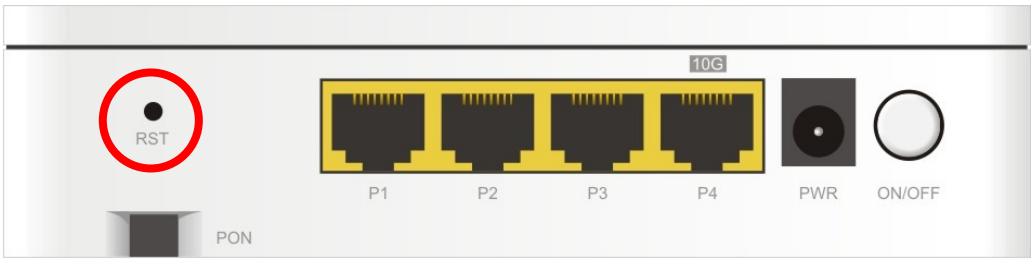
Go to **System Maintenance** and choose **System Reboot** on the web page. The following screen will appear. Choose **Factory Default** and click **Reboot**.

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.