DrayTek

VigorLTE 200 Series

LTE Router

USER'S GUIDE

V1.2

VigorLTE 200 Series
LTE Router

User's Guide

Version: 1.2

Firmware Version: V3.9.8.2

(For future update, please visit DrayTek web site)

Date: Dec. 12, 2022

Copyrights

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 8, 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

- 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 +5 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.
- 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 routers 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

Part I Installation i

I-1 Introduction 1

I-1-1 Indicators and Connectors 2

I-2 Hardware Installation 4

I-2-1 Network Connection via LTE 4

I-2-2 Wall-Mounted Installation 5

I-3 Accessing Web Page 6

I-4 Changing Password 8

I-5 Dashboard 9

I-5-1 Virtual Panel 10

I-5-2 Name with a Link 10

I-5-3 Quick Access for Common Used Menu 11

I-5-4 GUI Map 12

I-5-5 Web Console 13

I-5-6 Config Backup 13

I-5-7 Logout 14

I-5-8 Online Status 14

I-5-8-1 Physical Connection 14

I-5-8-2 Virtual WAN 16

I-6 Quick Start Wizard 17

I-6-1 LTE 18

I-6-2 WAN2 (Ethernet) 20

I-7 Service Activation Wizard 29

I-8 Registering Vigor Router 31

Part II Connectivity 35

II-1 LTE 36

Web User Interface 37

II-1-1 General Settings 37

II-1-1-1 SMS Quota 37

II-1-1-2 SMS Inbox Policy 38

II-1-2 SMS Inbox 39

II-1-3 Send SMS 42

II-1-4 SMS Gateway 43

II-1-5 Router Commands 47

II-1-6 Status 49

II-2 WAN 51

Web User Interface 52

II-2-1 General Setup 52

II-2-1-1 LTE 53

II-2-1-2 WAN2 53

II-2-2 Internet Access 55
II-2-2-1 Details Page for 3G/4G LTE Modem (DHCP mode) in LTE WAN *56*
II-2-2-2 Details Page for PPPoE in WAN2 ..... *61*
II-2-2-3 Details Page for Static or Dynamic IP in WAN2 ..... *63*
II-2-2-4 Details Page for PPTP *67*
II-2-2-5 Details Page for IPv6 – Offline *69*
II-2-2-6 Details Page for IPv6 – PPP *69*
II-2-2-7 Details Page for IPv6 – TSPC *70*
II-2-2-8 Details Page for IPv6 – AICCU *72*
II-2-2-9 Details Page for IPv6 – DHCPv6 Client *73*
II-2-2-10 Details Page for IPv6 – Static IPv6 ..... *74*
II-2-2-11 Details Page for IPv6 – 6in4 Static Tunnel *75*
II-2-2-12 Details Page for IPv6 – 6rd *77*
II-2-3 Multi-PVC/VLAN 79
II-2-4 WAN Budget 83
II-2-4-1 General Setup *83*
II-2-4-2 Status *85*
Application Notes 87
A-1 How to configure IPv6 on WAN interface? *87*
II-3 LAN 92
Web User Interface 94
II-3-1 General Setup 94
II-3-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup *96*
II-3-1-2 Details Page for LAN2 ..... *98*
II-3-1-3 Details Page for IP Routed Subnet *100*
II-3-1-4 Details Page for LAN IPv6 Setup *102*
II-3-1-5 DHCP Server Options *105*
II-3-2 VLAN 107
II-3-3 Bind IP to MAC 110
II-4 NAT 113
Web User Interface 114
II-4-1 Port Redirection 114
II-4-2 DMZ Host 118
II-4-3 Open Ports 121
II-4-4 ALG 123
II-5 Applications 125
Web User Interface 126
II-5-1 Dynamic DNS 126
II-5-2 Schedule 129
II-5-3 RADIUS 132
II-5-4 UPnP 134
II-5-5 IGMP 135
II-5-5-1 General Setting *135*
II-5-5-2 Working Group *136*
II-5-6 SMS Alert Service 137
Application Notes 138
A-1 How to use DrayDDNS? *138*
A-2 How to Configure Customized DDNS? *143*

II-6 Routing 147
Web User Interface 148
II-6-1 Static Route 148
II-5-2 Route Policy 153
II-5-3 BGP 162
II-5-3-1 Basic Settings 162
II-5-3-2 Static Network 163

Part III Wireless LAN 165

III-1 Wireless LAN 166
Web User Interface 170
III-1-1 Wireless Wizard 170
III-1-2 General Setup 173
III-1-3 Security 175
III-1-4 Access Control 177
III-1-5 WPS 179
III-1-6 WDS 180
III-1-7 Advanced Setting 183
III-1-8 AP Discovery 186
III-1-9 Station List 187

Part IV VPN 189

IV-1 VPN and Remote Access 190
Web User Interface 191
IV-1-1 VPN Client Wizard 191
IV-1-2 VPN Server Wizard 197
IV-1-3 Remote Access Control 200
IV-1-4 PPP General Setup 202
IV-1-5 IPsec General Setup 204
IV-1-6 IPsec Peer Identity 206
IV-1-7 VPN Matcher Setup 208
IV-1-8 OpenVPN 209
IV-1-8-1 OpenVPN Server Setup 209
IV-1-8-2 Client Config 212
IV-1-9 Remote Dial-in User 214
IV-1-10 LAN to LAN 217
IV-1-11 Connection Management 227
IV-2 SSL VPN 228
Web User Interface 229
IV-2-1 General Setup 229
IV-2-2 User Account 230
IV-2-3 SSL Portal Online User 234
IV-3 Certificate Management 235

Web User Interface 236
IV-3-1 Local Certificate 236
IV-3-2 Trusted CA Certificate 240
IV-3-3 Certificate Backup 242

Part V Security 243

V-1 Firewall 244
Web User Interface 246
V-1-1 General Setup 246
V-1-2 Filter Setup 251
V-1-3 DoS Defense 261
V-1-3-1 DoS Defense 261
V-1-3-2 Spoofing Defense 264
Application Notes 265
A-1 How to Configure Certain Computers Accessing to Internet 265
V-2 Central Security Management (CSM) 269
Web User Interface 270
V-2-1 APP Enforcement Profile 270
V-2-2 URL Content Filter Profile 272
V-2-3 Web Content Filter Profile 276
V-2-4 DNS Filter Profile 280
Application Notes 282
A-1 How to Create an Account for MyVigor 282
A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter 287

Part VI Management 293

VI-1 System Maintenance 294
Web User Interface 295
VI-1-1 System Status 295
VI-1-2 TR-069 297
VI-1-3 Administrator Password 300
VI-1-4 User Password 301
VI-1-5 Configuration Backup 303
VI-1-6 Syslog/Mail Alert 305
VI-1-7 Time and Date 307
VI-1-8 SNMP 308
VI-1-9 Management 310
VI-1-10 Panel Control 314
VI-1-11 Self-Signed Certificate 315
VI-1-12 Reboot System 316
VI-1-13 Firmware Upgrade 317
VI-1-14 Activation 318

VI-2 Bandwidth Management 320
Web User Interface 322
VI-2-1 Sessions Limit 322
VI-2-2 Bandwidth Limit 324
VI-2-3 Quality of Service 326
VI-3 Central Management (AP) 331
Web User Interface 332
VI-3-1 Dashboard 332
VI-3-2 Status 333
VI-3-3 WLAN Profile 334
VI-3-4 AP Maintenance 339
VI-3-5 Traffic Graph 340
VI-3-6 Temperature Sensor 341
VI-3-7 Event Log 341
VI-3-8 Total Traffic 342
VI-3-9 Station Number 342
VI-3-10 Load Balance 343
VI-3-11 Function Support List 345

Part VII Others 347

VII-1 Objects Settings 348
Web User Interface 349
VII-1-1 IP Object 349
VII-1-2 IP Group 353
VII-1-3 IPv6 Object 354
VII-1-4 IPv6 Group 356
VII-1-5 Service Type Object 357
VII-1-6 Service Type Group 359
VII-1-7 Keyword Object 361
VII-1-8 Keyword Group 363
VII-1-9 File Extension Object 364
VII-1-10 SMS Service Object 366
VII-1-11 Notification Object 369
VII-1-12 String Object 371
Application Notes 372
A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection 372

Part VIII Troubleshooting 377

VIII-1 Diagnostics 378
Web User Interface 379
VIII-1-1 Dial-out Triggering 379

VIII-1-2 Routing Table 380
VIII-1-3 ARP Cache Table 381
VIII-1-4 IPv6 Neighbour Table 382
VIII-1-5 DHCP Table 383
VIII-1-6 NAT Sessions Table 384
VIII-1-7 DNS Cache Table 385
VIII-1-8 Ping Diagnosis 386
VIII-1-9 Data Flow Monitor 387
VIII-1-10 Traffic Graph 389
VIII-1-11 Trace Route 390
VIII-1-12 Syslog Explorer 391
VIII-1-13 IPv6 TSPC Status 392
VIII-1-14 DoS Flood Table 393
VIII-2 Checking If the Hardware Status Is OK or Not 394
VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not 395
VIII-4 Pinging the Router from Your Computer 398
VIII-5 Checking If the ISP Settings are OK or Not 400
VIII-6 Backing to Factory Default Setting If Necessary 401
VIII-7 Contacting DrayTek 402

Part IX Telnet Commands 403

Accessing Telnet of VigorLTE 200 404

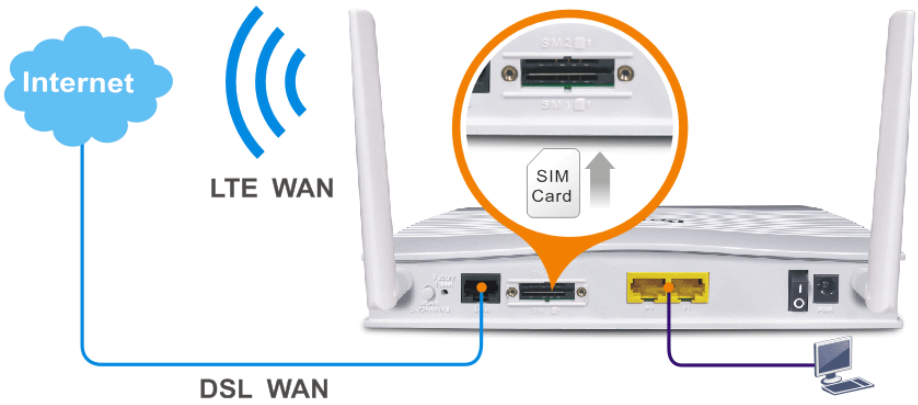
Part I Installation

This part will introduce Vigor router and guide to install the device in hardware and software.

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.

VigorLTE 200 series is a router equipped with an LTE module which allows you to access the Internet via a SIM card.



It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth. By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with VPN tunnels.

The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention and URL/Web content filter strengthen the security outside and control inside. Object-based firewall is flexible and allows your network be safe.

On the Wireless-equipped models each of the wireless SSIDs can also be grouped within one of the VLANs.

VigorLTE 200 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

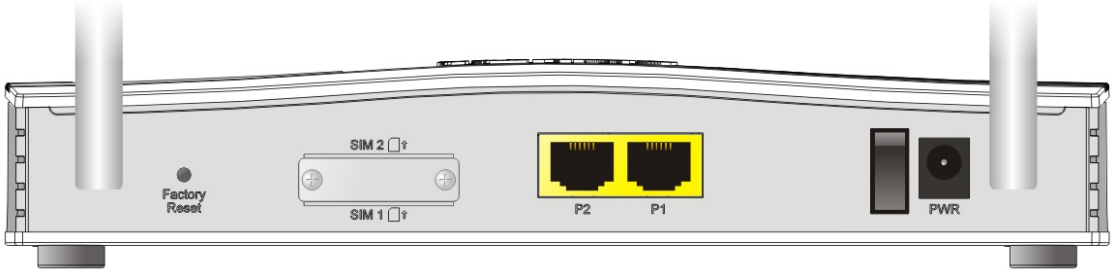
I-1-1 Indicators and Connectors

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

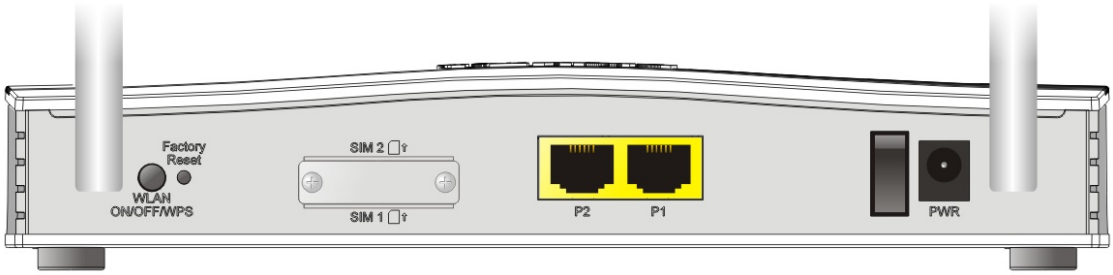
VigorLTE 200 / VigorLTE 200n

LED	Status	Explanation
	Off	The router is powered off.
	Blinking	The router is powered on and running normally.
	On	The router is ready to access Internet.
	Off	The router is not ready to access Internet.
	Blinking	Slowly: The DSL connection is ready. Quickly: The DSL connection is establishing.
	On	The LAN port is connected.
	Blinking	The data is transmitting through the LAN port.
	On	LTE device is connected and ready for use.
	Off	LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.).
	Blinking	Vigor device performs initial access procedure.
	On	SIM card is inserted into the slot and detected by Vigor device.
	Blinking	No SIM card in detected.
	On	Wireless function is enabled.
	Off	Wireless function is disabled.
	Blinking	The data is transmitting via wireless connection. Blinks with one second cycle for two minutes. The WPS function is active.

VigorLTE 200,



VigorLTE 200n,



Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
SIM2/SIM1	SIM card slot(s).
P2-P1	Connecters for local network devices.
ON/OFF	Power Switch.
PWR	Connecter for a power adapter.

I-2 Hardware Installation

I-2-1 Network Connection via LTE

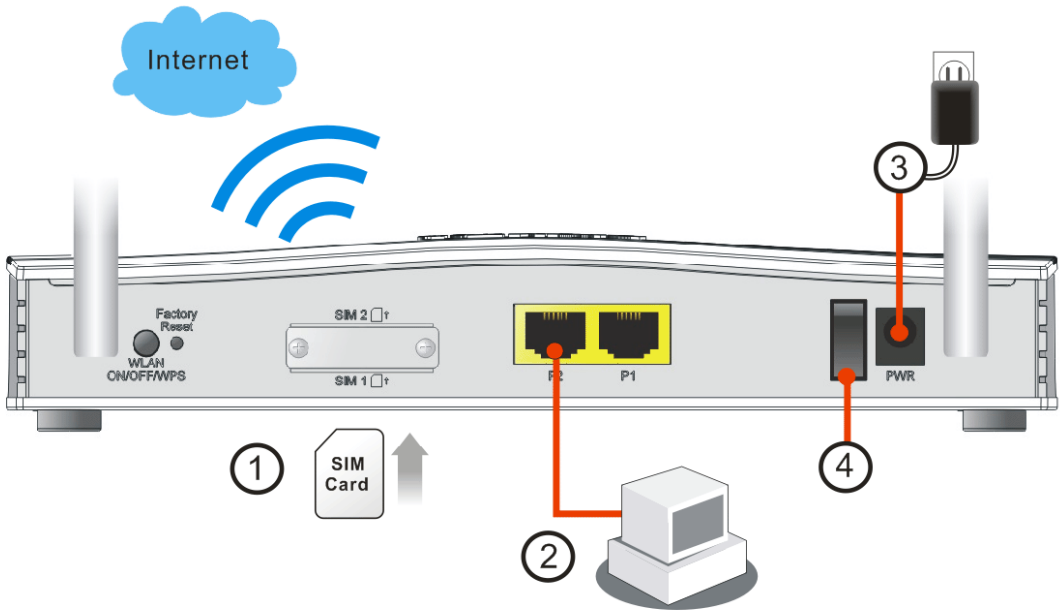
Before starting to configure the router, you have to connect your devices correctly. In this section, VigorLTE 200 is taken as an example.

1. Install the SIM card into the card slot. The back plate of the SIM card slot must be removed first and the direction of card notch must be on the left side.

After installing the SIM card, fasten the back plate again.

2. Connect to your computer with a RJ-45 cable.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the router.
5. Check the **power, LTE** and **LAN** LEDs to assure network connections.

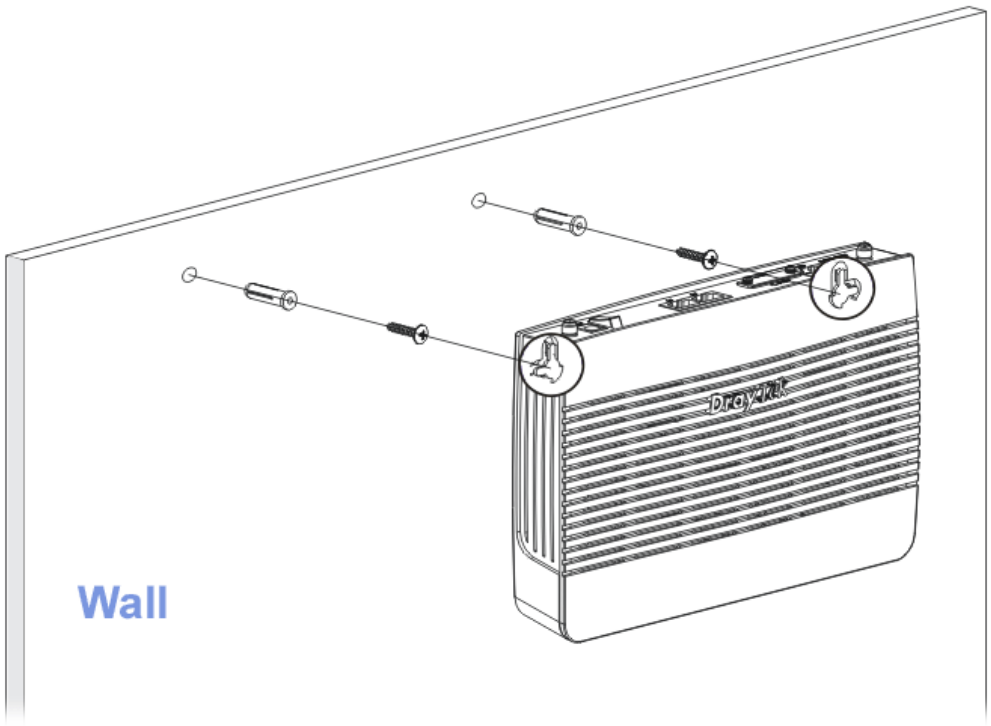
(For the hardware connection, we take *"n"* model as an example.)



I-2-2 Wall-Mounted Installation

VigorLTE 200 has keyhole type mounting slots on the underside.

1. A template is provided on the VigorLTE 200 packaging box to enable you to space the screws correctly on the wall.
2. Place the template on the wall and drill the holes according to the recommended instruction.
3. Fit screws into the wall using the appropriate type of wall plug.



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

4. When you finished about procedure, the router has been mounted on the wall firmly.

I-3 Accessing Web Page

1. Make sure your PC connects to the router correctly.

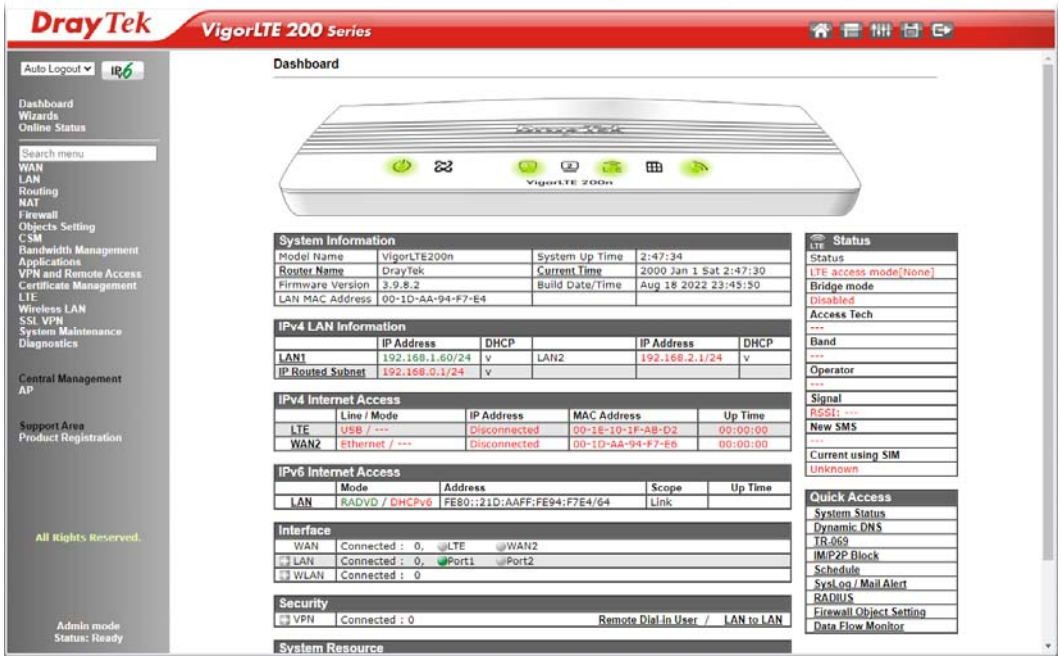
   You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.

3. Please type “admin/admin” as the Username/Password and click **Login**.

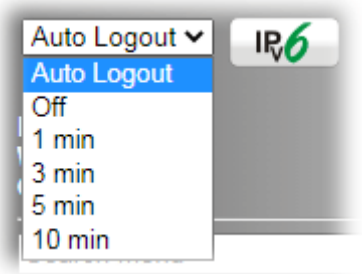
Info	If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

4. Now, the **Main Screen** will appear. Take VigorLTE 200n as as example.



Info	The home page will be different slightly in accordance with the type of the router you have.

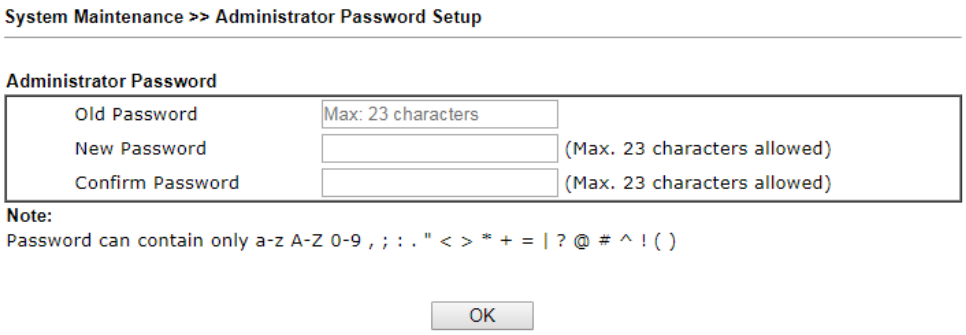
5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



I-4 Changing Password

Please change the password for the original security of the router.

1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.
2. Please type “admin/admin” as Username/Password for accessing into the web user interface with admin mode.
3. Go to **System Maintenance** page and choose **Administrator Password**.



4. Enter the login password (the default is “admin”) on the field of **Old Password**. Type **New Password** and **Confirm Password**. Then click **OK** to continue.

Info The maximum length of the password you can set is 23 characters.

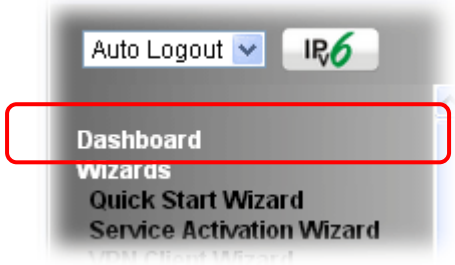
5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.

Info Even the password is changed, the Username for logging onto the web user interface is still “admin”.

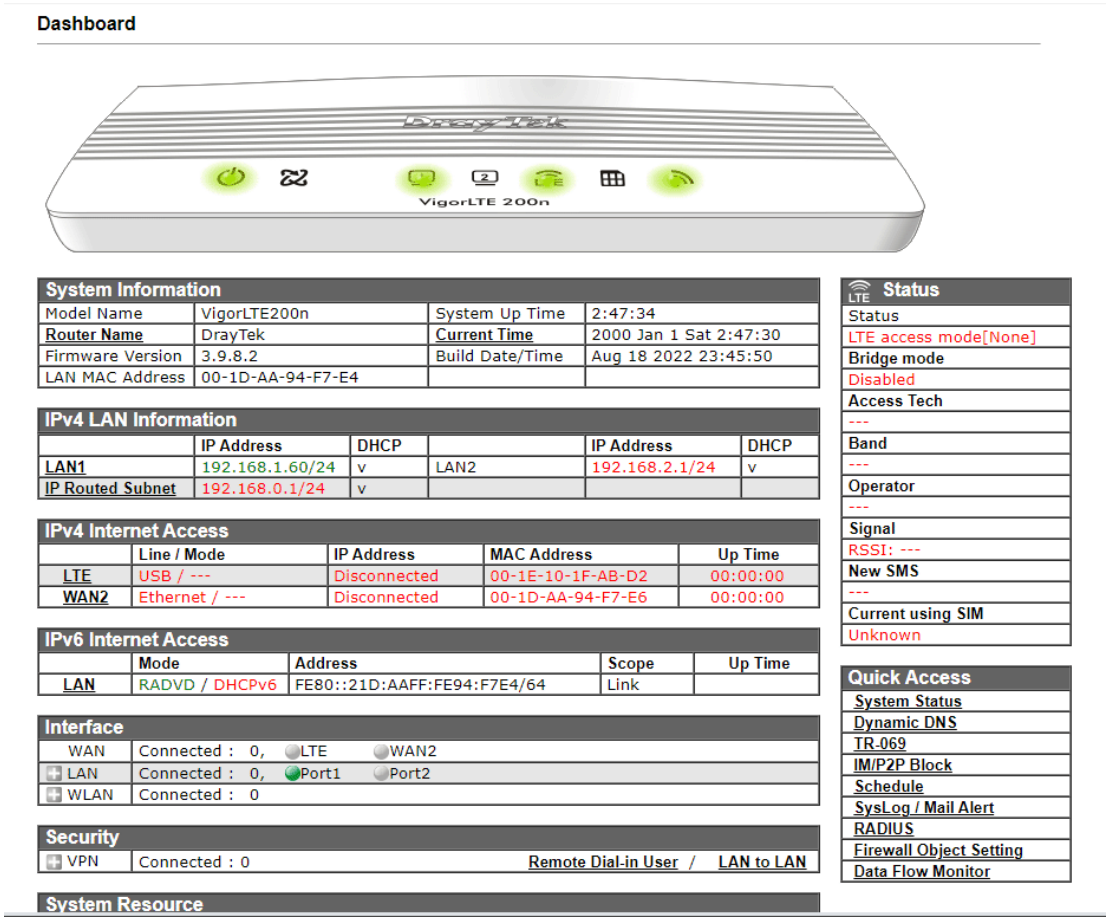
I-5 Dashboard

Dashboard shows the connection status including System Information, IPv4 Internet Access, IPv6 Internet Access, Interface (physical connection), Security and Quick Access.

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



A web page with default selections will be displayed on the screen. Refer to the following figure:



I-5-1 Virtual Panel

On the top of the Dashboard, a virtual panel (simulating the physical panel of the router) displays the physical interface connection. It will be refreshed every five seconds. When you move and click the mouse cursor on LEDs (except ACT), USB ports, or LAN1 – LAN4, related web setting page will be open for you to configure if required.

Port	Color	Description
LED	Black	It means the router or the function is not working.
	Green	It means the router or the function is working.

For detailed information about the LED display, refer to **I-1-1 LED Indicators and Connectors**.

I-5-2 Name with a Link

A name with a link (e.g., Router Name, Current Time, LTE and etc.) below means you can click it to open the configuration page for modification.

System Information

Model Name	VigorLTE200n	System Up Time	2:49:36
Router Name	DrayTek	Current Time	2000 Jan 1 Sat 2:49:32
Firmware Version	3.9.8.2	Build Date/Time	Aug 18 2022 23:45:50
LAN MAC Address	00-1D-AA-94-F7-E4		

IPv4 LAN Information

	IP Address	DHCP		IP Address	DHCP
LAN1	192.168.1.60/24	v	LAN2	192.168.2.1/24	v
IP Routed Subnet	192.168.0.1/24	v			

IPv4 Internet Access

	Line / Mode	IP Address	MAC Address	Up Time
LTE	USB / ---	Disconnected	00-1E-10-1F-AB-D2	00:00:00
WAN2	Ethernet / ---	Disconnected	00-1D-AA-94-F7-E6	00:00:00

IPv6 Internet Access

	Mode	Address	Scope	Up Time
LAN	RADVD / DHCPv6	FE80::21D:AAFF:FE94:F7E4/64	Link	

Interface

WAN	Connected : 0,	LTE	WAN2
LAN	Connected : 0,	Port1	Port2
WLAN	Connected : 0		

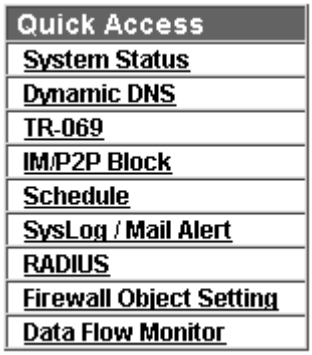
Security

VPN	Connected : 0	Remote Dial-in User / LAN to LAN

I-5-3 Quick Access for Common Used Menu

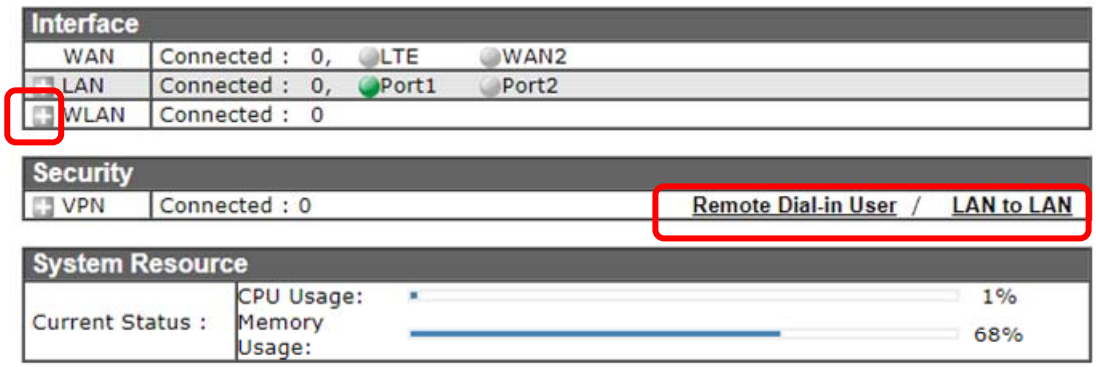
All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

Look at the right side of the Dashboard. You will find a group of common used functions grouped under **Quick Access**.



The function links of System Status, Dynamic DDNS, TR-069, IM/P2P Block, Schedule, Syslog/Mail Alert, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be open immediately.

In addition, quick access for VPN security settings such as **Remote Dial-in User** and **LAN to LAN** are located on the bottom of this page. Scroll down the page to find them and use them if required.



Note that there is a plus ( ) icon located on the left side of LAN/WLAN. Click it to review the LAN/WLAN connection(s) used presently.

Host connected physically to the router via LAN port(s) will be displayed with green circles in the field of Connected.

All of the hosts (including wireless clients) displayed with Host ID, IP Address and MAC address indicates that the traffic would be transmitted through LAN port(s) and then the WAN port. The purpose is to perform the traffic monitor of the host(s).

I-5-4 GUI Map

All the functions the router supports are listed with table clearly in this page. Users can click the function link to access into the setting page of the function for detailed configuration. Click the icon on the top of the main screen to display all the functions.

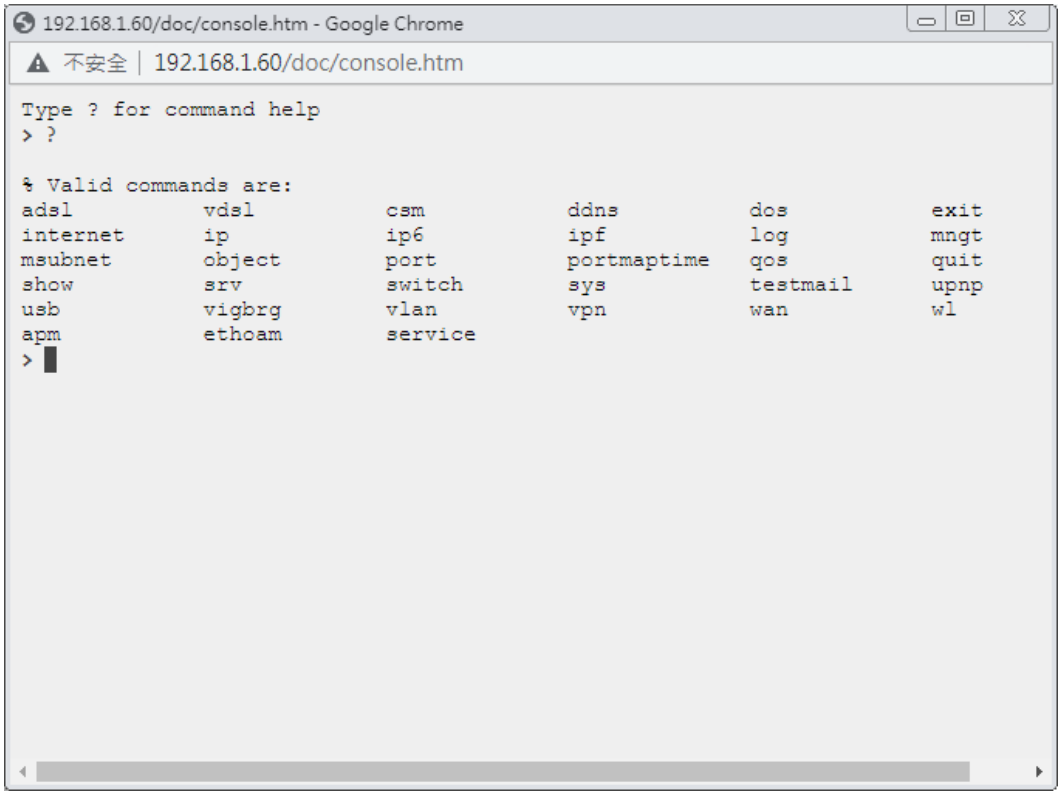
GUI Map

Wizards		**Certificate Management**	
	Quick Start Wizard		Local Certificate
	Service Activation Wizard		Trusted CA Certificate
	VPN Client Wizard		Certificate Backup
	VPN Server Wizard	**LTE**	
	Wireless Wizard		General Settings
Online Status			SMS Inbox
	Physical Connection		Send SMS
	Virtual WAN		SMS Gateway
WAN			Router Commands
	General Setup		Status
	Internet Access	**Wireless LAN**	
	Multi-PVC/VLAN		General Setup
	WAN budget		Security
LAN			Access Control
	General Setup		WPS
	VLAN		WDS
	Bind IP to MAC		Advanced Setting
Routing			AP Discovery
	Static Route		Station List
	Route Policy	**SSL VPN**	
	BGP		General Setup
NAT			User Account

I-5-5 Web Console

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.



I-5-6 Config Backup

There is one way to store current used settings quickly by clicking the **Config Backup** icon. It allows you to backup current settings as a file. Such configuration file can be restored by using **System Maintenance>>Configuration Backup**.

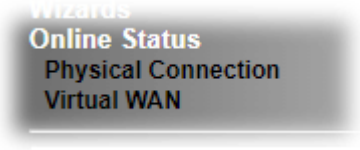
Simply click the icon on the top of the main screen and a pop up dialog will appear.

Click **Save** to store the setting.

I-5-7 Logout

Click this icon to exit the web user interface.

I-5-8 Online Status



I-5-8-1 Physical Connection

Such page displays the physical connection status such as LAN connection status, WAN connection status, ADSL information, and so on.

Physical Connection for IPv4 Protocol

Online Status

Physical Connection — **System Uptime: 0day 3:3:1**

IPv4 | IPv6

LAN Status

IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:
192.168.1.60	16,943	10,713	8.8.8.8	8.8.4.4

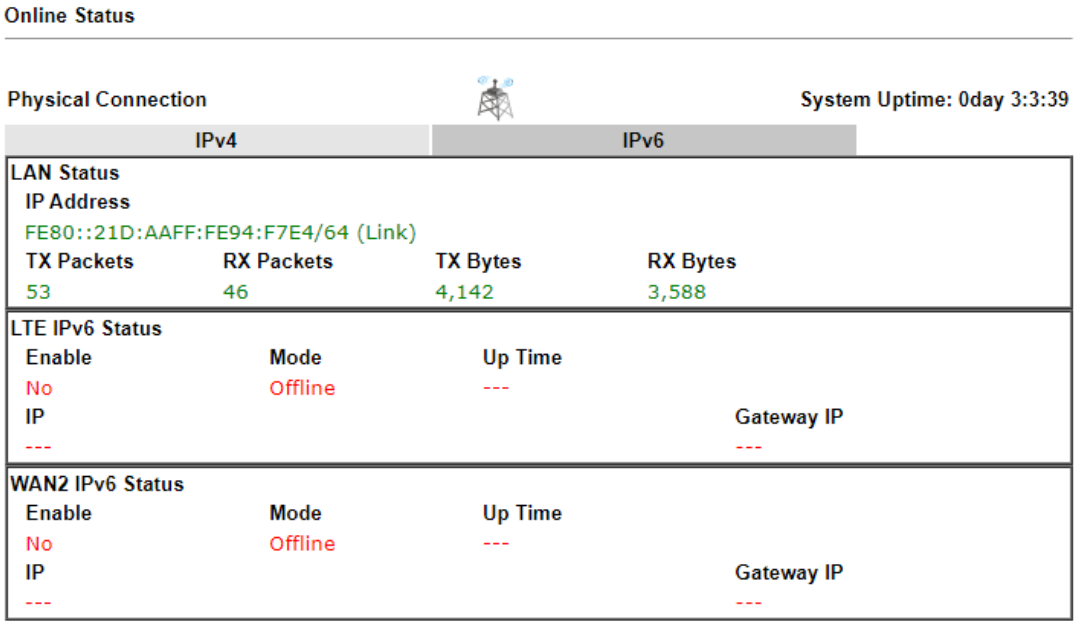
LTE Status (Using Unknown)

Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		---	00:00:00	-
IP	**GW IP**	**TX Packets**	**TX Rate(bps)**	**RX Packets**	**RX Rate(bps)**
---	---	0	0	0	0

WAN 2 Status

Enable	Line	Name	Mode	Up Time	
No	Ethernet		---	00:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(bps)**	**RX Packets**	**RX Rate(bps)**
---	---	0	0	0	0

Physical Connection for IPv6 Protocol



Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	**IP Address**-Displays the IP address of the LAN interface. **TX Packets**-Displays the total transmitted packets at the LAN interface. **RX Packets**-Displays the total received packets at the LAN interface.
LTE Status / WAN2 Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. **Line** – Displays the physical connection of this interface. **Name** – Display the name of the router. **Mode** - Displays the type of WAN connection (e.g., PPPoE). **Up Time** - Displays the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **GW IP** - Displays the IP address of the default gateway. **TX Packets** - Displays the total transmitted packets at the WAN interface. **TX Rate** - Displays the speed of transmitted octets at the WAN interface. **RX Packets** - Displays the total number of received packets at the WAN interface. **RX Rate** - Displays the speed of received octets at the WAN interface.

Detailed explanation (for IPv6) is shown below:

Item	Description
LAN Status	**IP Address**- Displays the IPv6 address of the LAN interface.. **TX Packets**-Displays the total transmitted packets at the LAN

Item	Description
	interface. **RX Packets**-Displays the total received packets at the LAN interface. **TX Bytes** - Displays the speed of transmitted octets at the LAN interface. **RX Bytes** - Displays the speed of received octets at the LAN interface.
LTE / WAN IPv6 Status	**Enable – No** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. No in red means such interface is not available. **Mode** - Displays the type of WAN connection (e.g., TSPC). **Up Time** - Displays the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **Gateway IP** - Displays the IP address of the default gateway.

Info

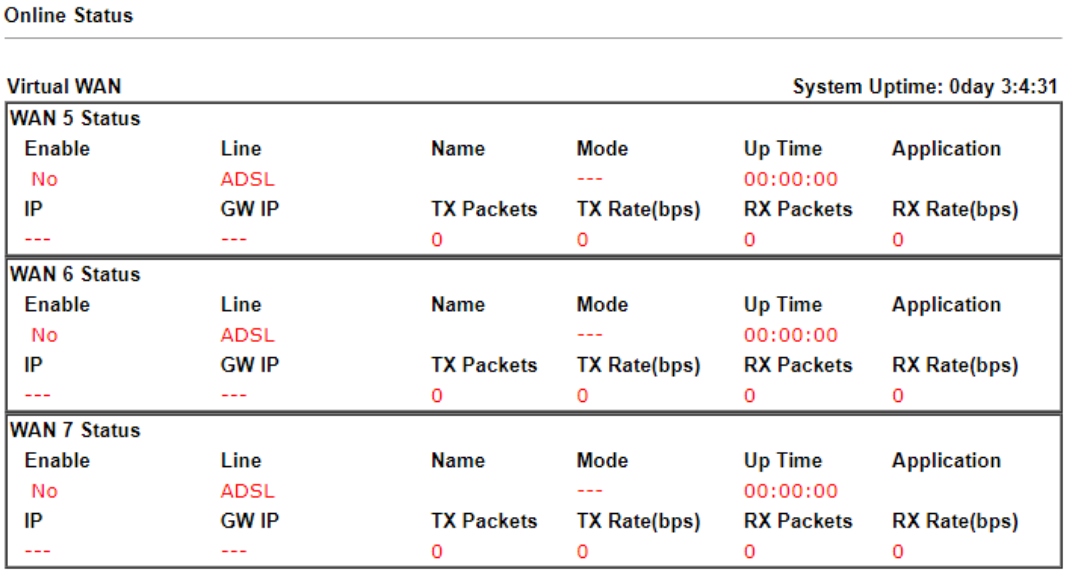
The words in green mean that the WAN connection of that interface is ready for accessing Internet; the words in red mean that the WAN connection of that interface is not ready for accessing Internet.

I-5-8-2 Virtual WAN

Such page displays the virtual WAN connection information.

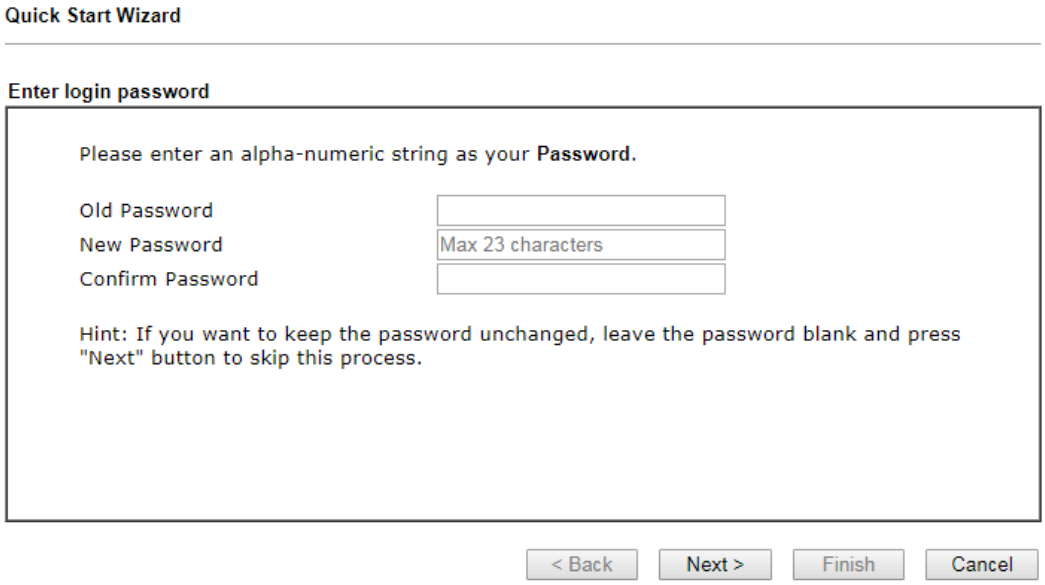
Virtual WAN are used by TR-069 management, and so on.

The field of Application will list the purpose of such WAN connection.

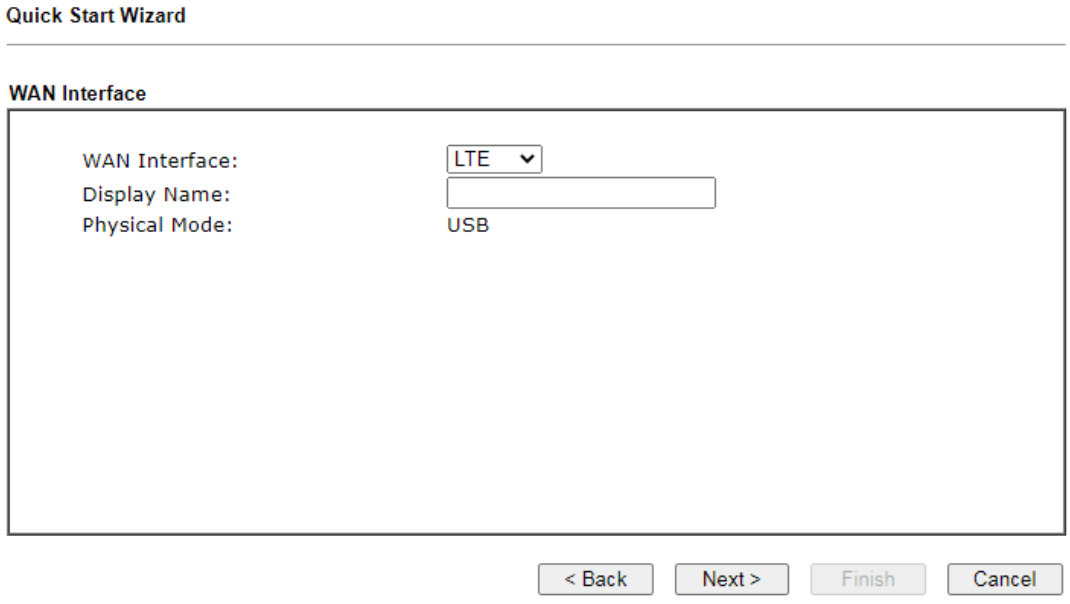


I-6 Quick Start Wizard

Quick Start Wizard can help you to deploy and use the router easily and quickly. Go to **Wizards>>Quick Start Wizard**. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.

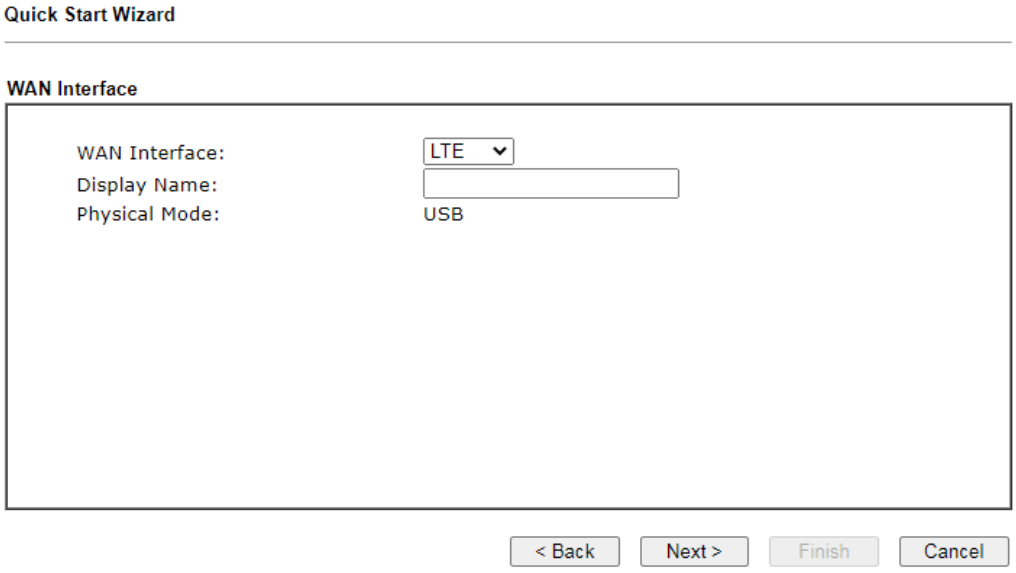


On the next page, please select the WAN interface that you use. If WAN interface is used, please choose WAN1; if USB interface is used, please choose LTE. Then click **Next** for next step. WAN2 and LTE will bring up different configuration page. Here, we take **LTE** as an example.

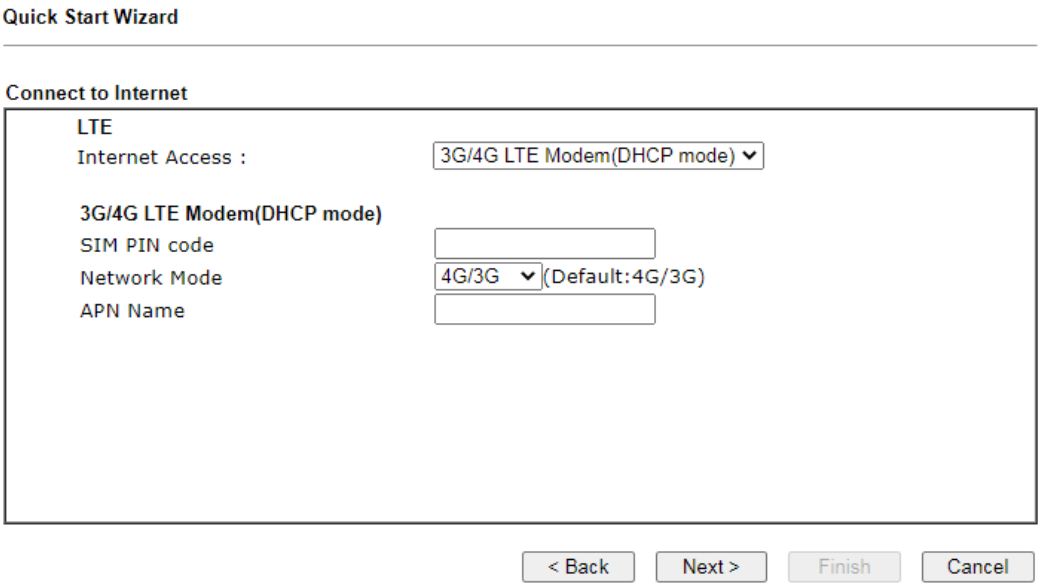


I-6-1 LTE

1. Choose **LTE**. Enter a string as Display Name (optional). Click **Next**.



2. After clicking **Next**, you will get the following web page.

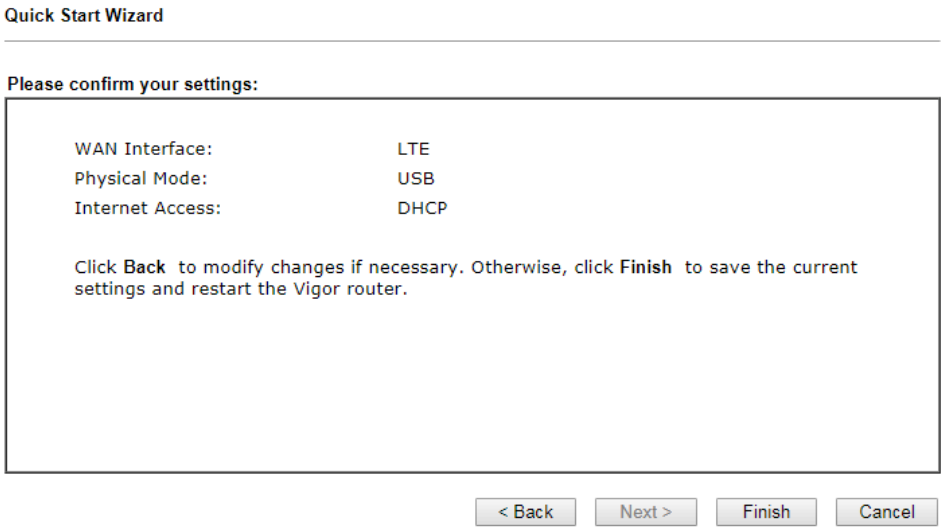


Available settings are explained as follows:

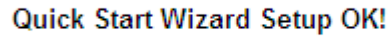
Item	Description
Internet Access	Specify a connection mode from the drop down menu.
SIM PIN code	Enter PIN code of the SIM card that will be used to access Internet.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs.

Item	Description
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Please manually enter the Username/Password provided by your ISP. Click **Next** for viewing summary of such connection.



4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.



5. Now, you can enjoy surfing on the Internet.

I-6-2 WAN2 (Ethernet)

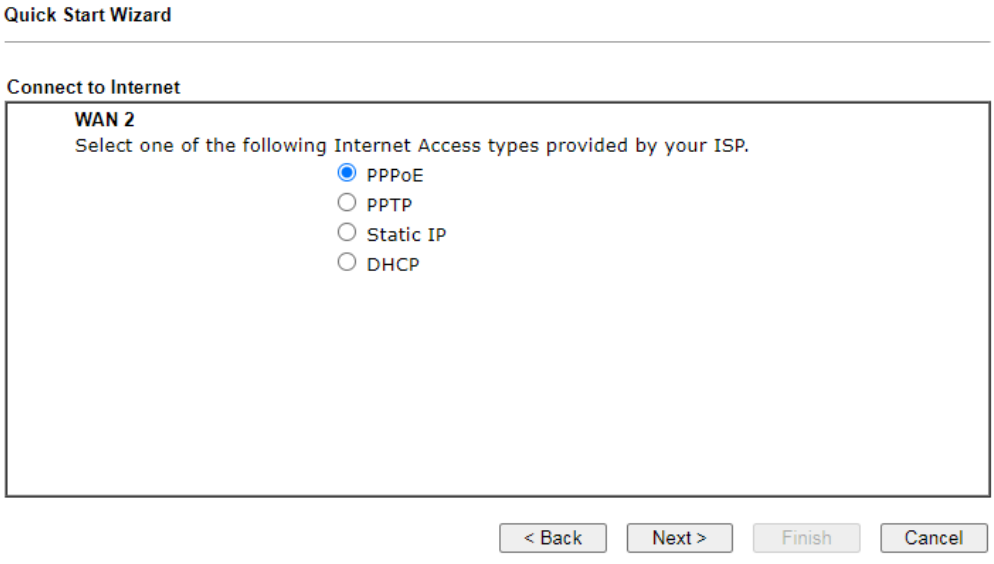
WAN2 can be configured for physical mode of Ethernet. If you choose Ethernet WAN2, please specify a physical type. Then, click **Next**.

Available settings are explained as follows:

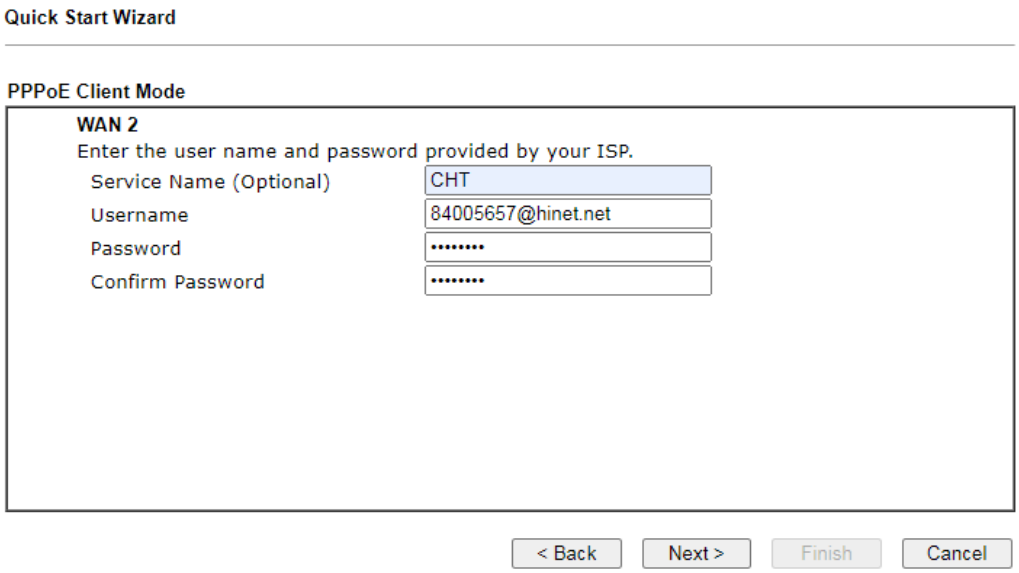
Item	Description
Display Name	Type a name for the router.
Physical Mode	Display the physical mode of this WAN interface.
Physical Type	This setting is available when **Ethernet** is selected as **Physical Mode**. In general, **Auto negotiation** is suggested.

PPPoE

1. Choose **WAN2** as the WAN Interface and choose **Ethernet** as the **Physical Mode**. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **PPPoE** as the Internet Access Type. Then click **Next** to get the following page.

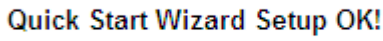


Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
Username	Assign a specific valid user name provided by the ISP. **Note:** The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. **Note:** The maximum length of the password you can set is 62 characters.
Confirm Password	ReEnter the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Please manually enter the Username/Password provided by your ISP. Click **Next** for viewing summary of such connection.

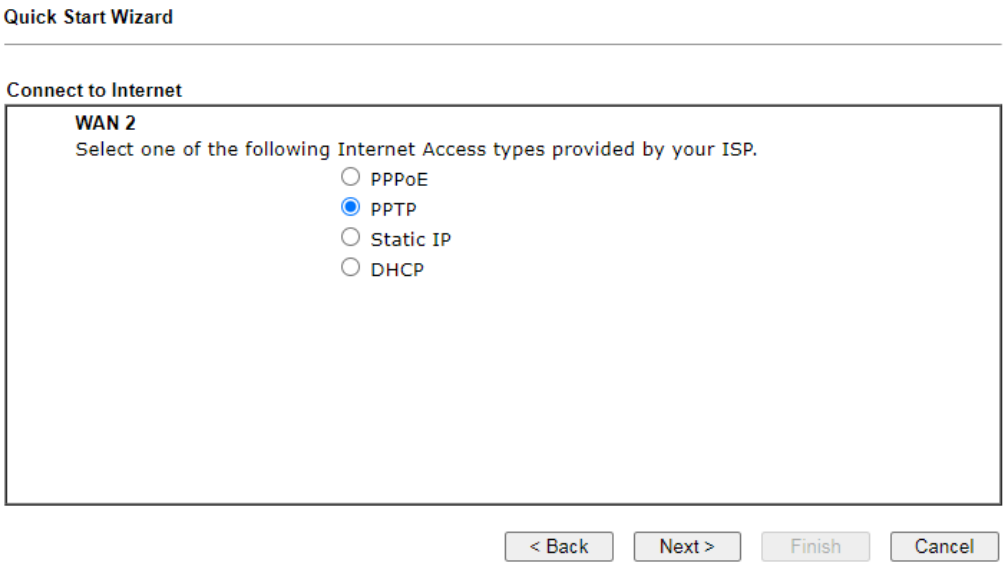
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.



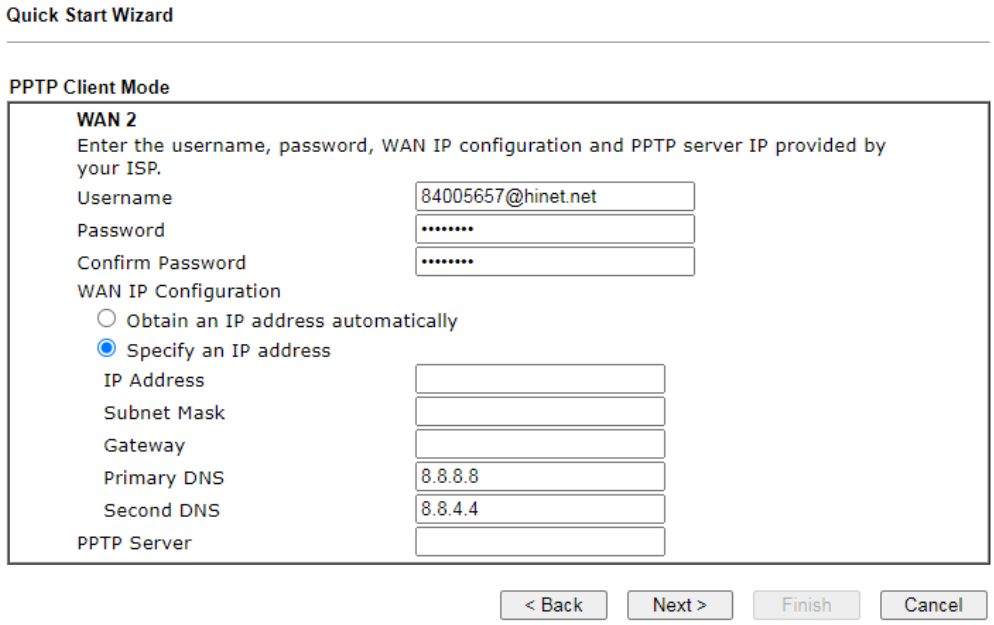
5. Now, you can enjoy surfing on the Internet.

PPTP

1. Choose **PPTP** as the WAN Interface and click the **Next** button.



2. The following page will be open for you to Enter all the information originally provided by your ISP.



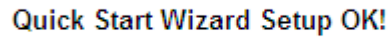
Available settings are explained as follows:

Item	Description
Username	Assign a specific valid user name provided by the ISP. **Note:** The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. **Note:** The maximum length of the password you can set is 62 characters.
Confirm Password	ReEnter the password.
WAN IP Configuration	**Obtain an IP address automatically** – the router will get an

	IP address automatically from DHCP server. **Specify an IP address** – you have to type relational settings manually. **IP Address** - Enter the IP address. **Subnet Mask** –Enter the subnet mask. Gateway – Enter the IP address of the gateway. **Primary DNS -** Enter the primary IP address for the router. **Secondary DNS -** Enter the secondary IP address for necessity in the future.
PPTP Server	Enter the IP address of the server.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Please Enter the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for viewing summary of such connection.

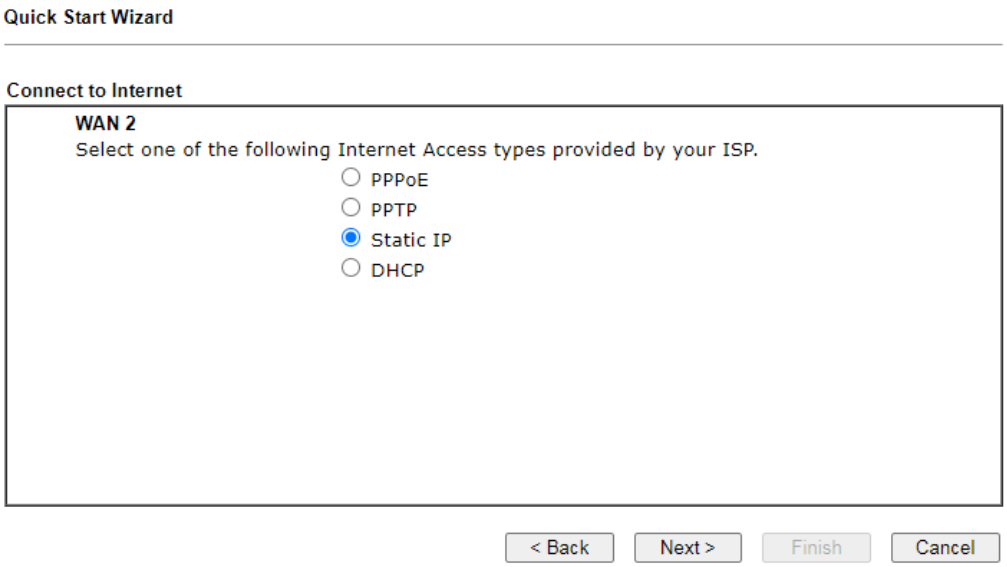
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



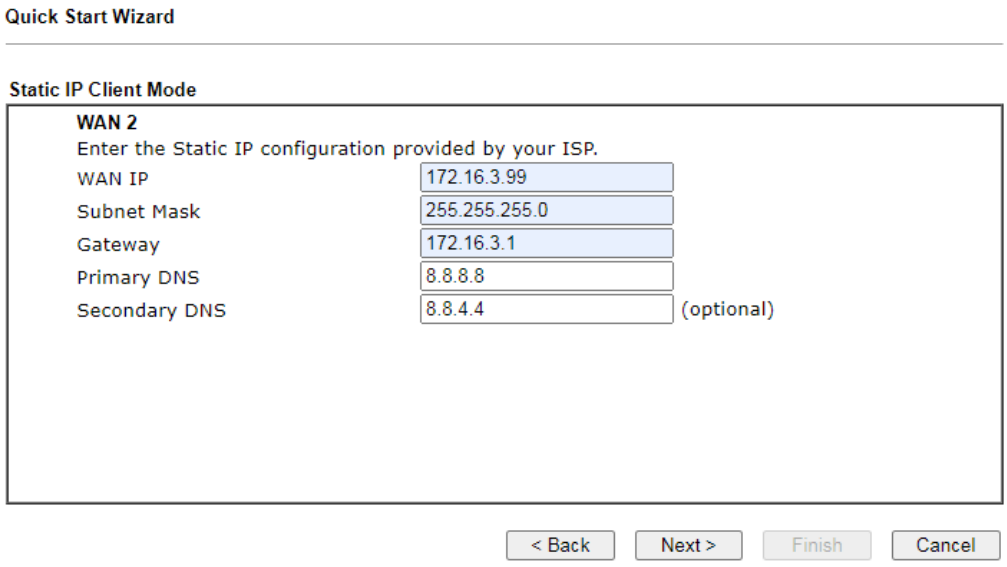
5. Now, you can enjoy surfing on the Internet.

Static IP

1. Click **Static IP** as the Internet Access type and click the **Next** button.



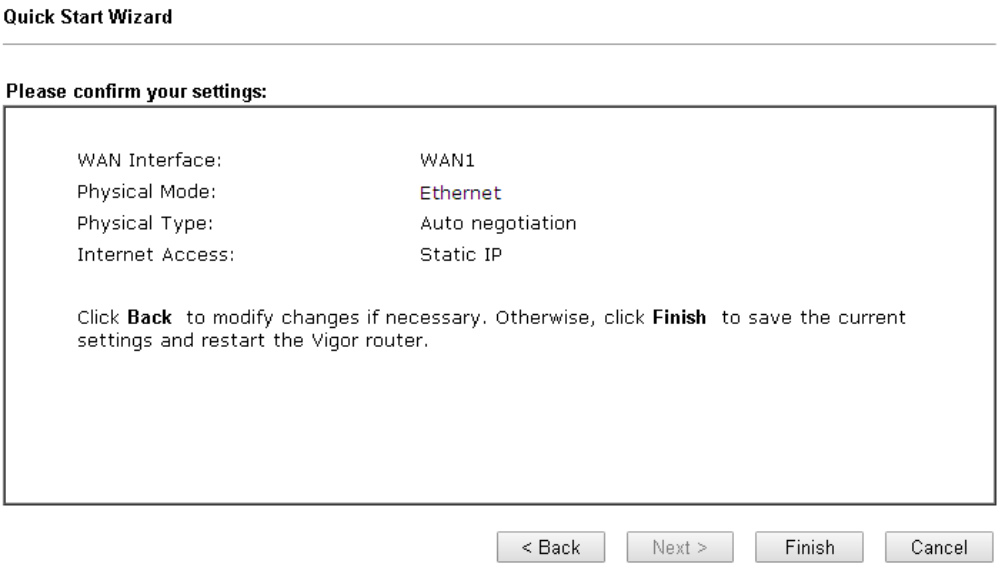
2. The following page will be open for you to Enter the IP address information originally provided by your ISP.



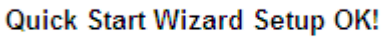
Available settings are explained as follows:

Item	Description
WAN IP	Enter the IP address.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the IP address of gateway.
Primary DNS	Enter the primary IP address for the router.
Secondary DNS	Enter secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Click **Next** for next step.



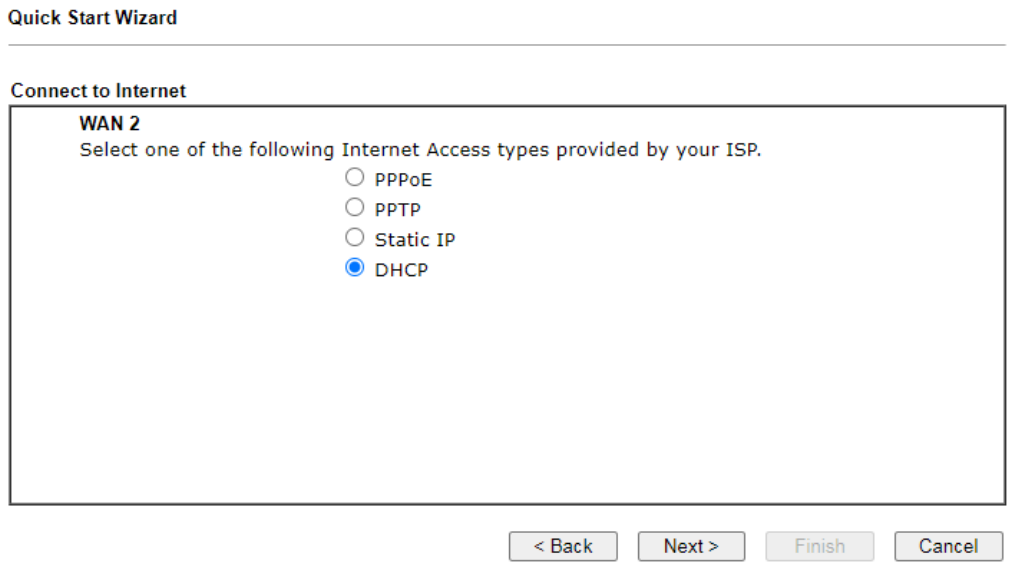
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.



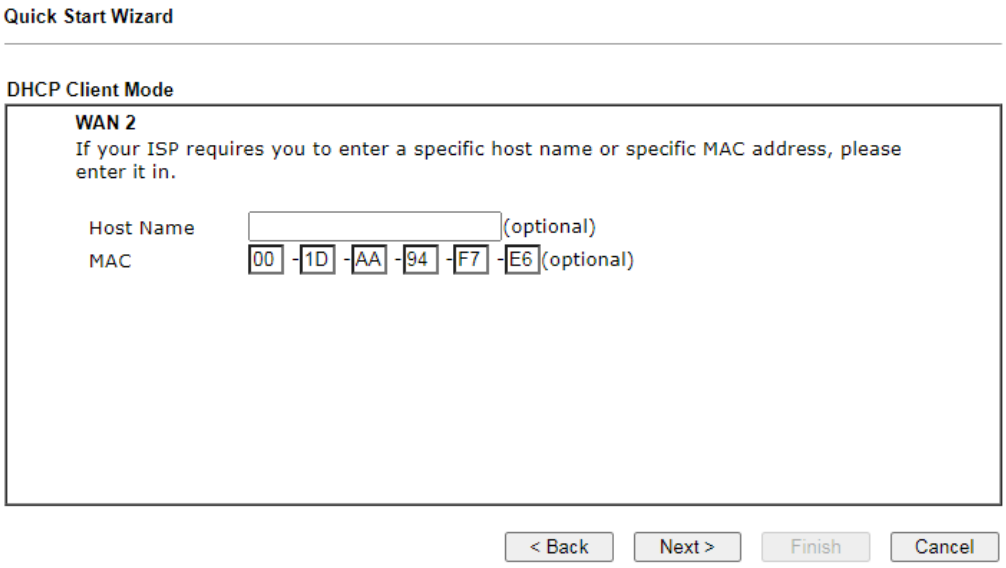
5. Now, you can enjoy surfing on the Internet.

DHCP

1. Click **DHCP** as the Internet Access type and click the **Next** button.



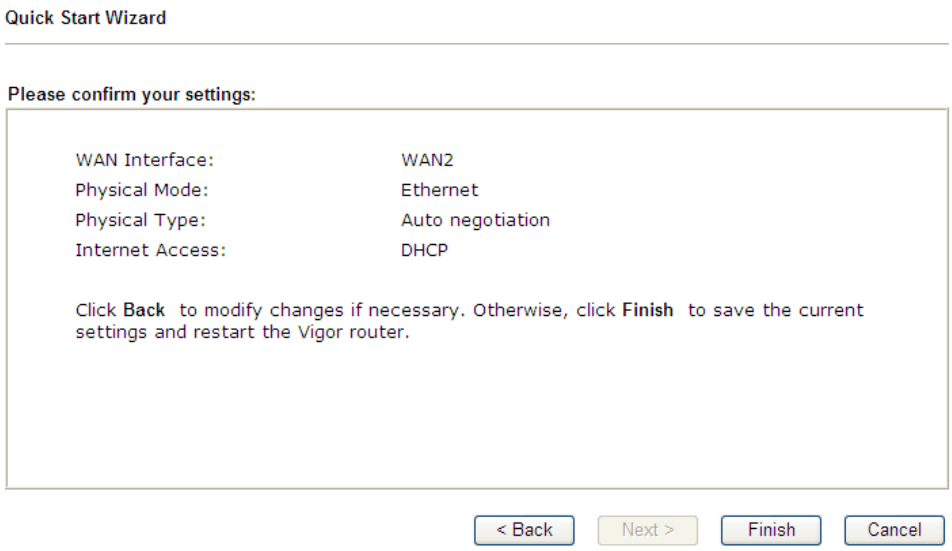
2. The following page will be open for you to Enter the IP address information originally provided by your ISP.



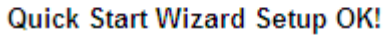
Available settings are explained as follows:

Item	Description
Host Name	Enter the name of the host. **Note:** The maximum length of the host name you can set is 39 characters.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. After finished the settings above, click **Next** for viewing summary of such connection.



4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



5. Now, you can enjoy surfing on the Internet.

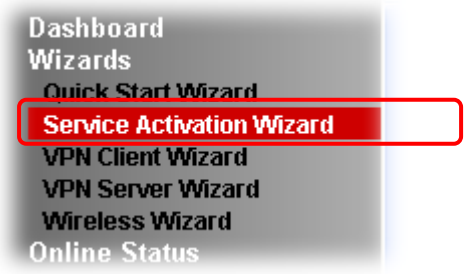
I-7 Service Activation Wizard

Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, please type "admin/admin" on Username/Password while Logging into the web user interface.**

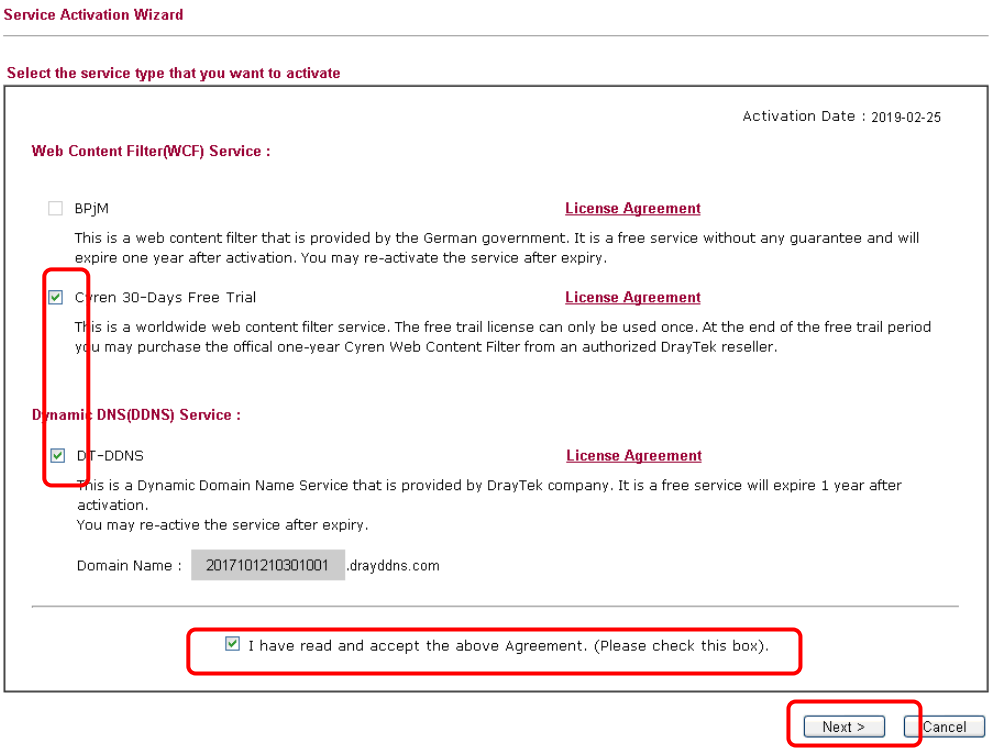
Service Activation Wizard is a tool which allows you to activate services without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com.

Info	Such function is available only for Admin Mode.

1. Open **Wizards>>Service Activation Wizard**.



2. In the following page, you can activate the Web content filter services and DNS service at the same time or individually. When you finish the selection, please click **Next**.



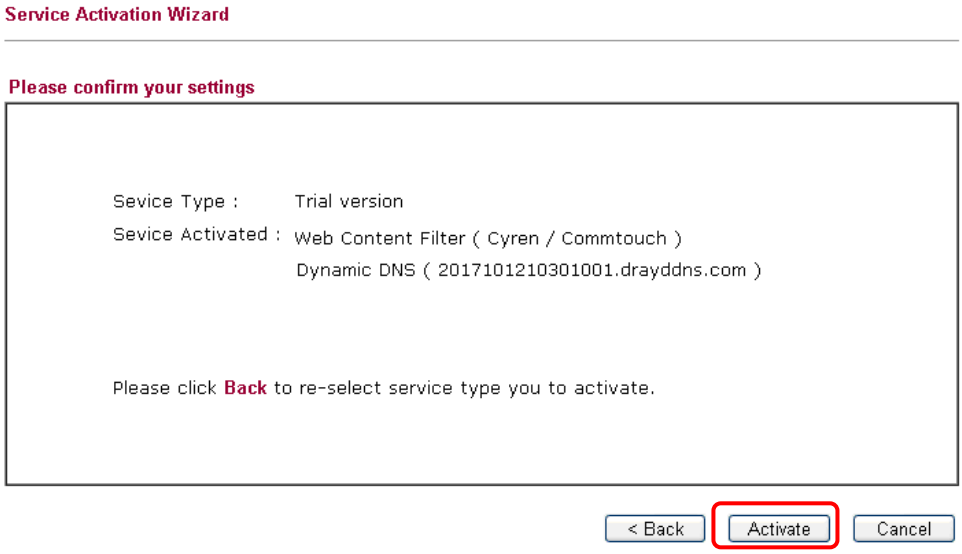
Info

BPjM is web content filter (WCF) for German Speaking users. It is ideal for your family to provide more Internet security for youngsters.

Cryan 30-day trial is WCF which offers 30-day trial period. After trial, you can purchase DrayTek's prepared Cryan GlobalView WCF package from retailing outlets.

DT-DDNS, developed by DrayTek, offers one year free charge service of dynamic DNS service for internal use.

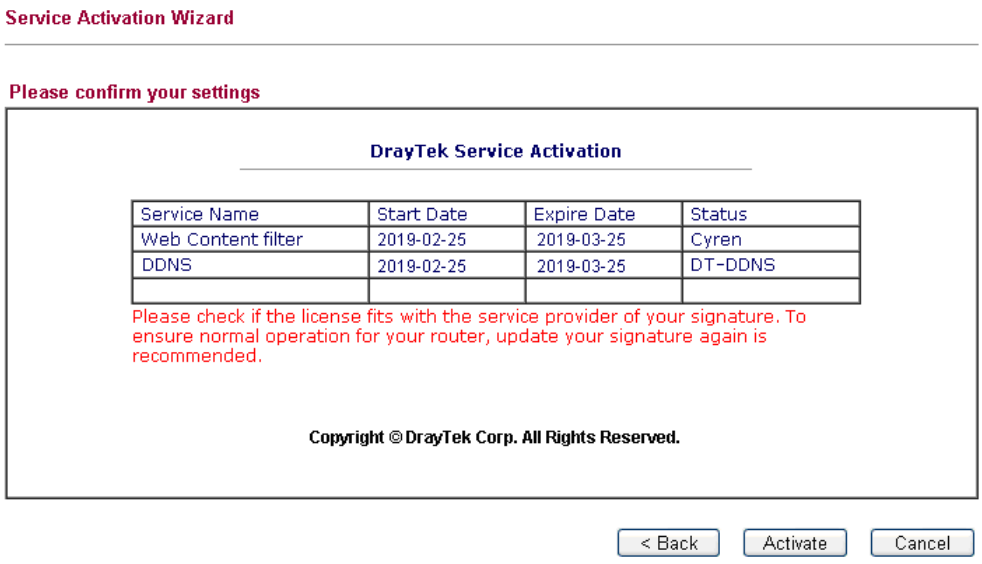
3. Setting confirmation page will be displayed as follows, please click **Activate**.



Info

The service will be activated and applied as the default rule configured in **Firewall>>General Setup**.

4. Now, the web page will display the service that you have activated according to your selection(s). The valid time for the free trial of these services is one month.



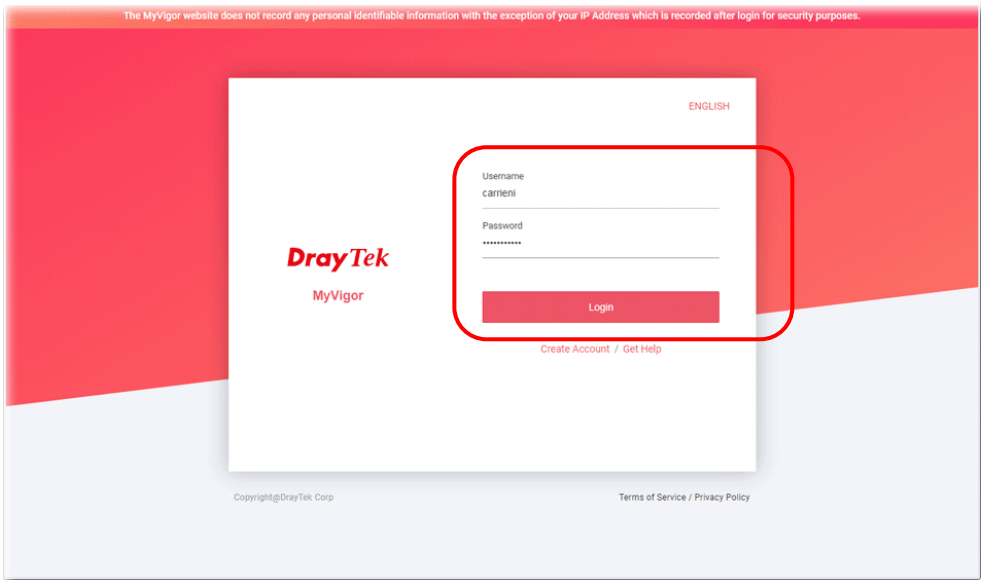
I-8 Registering Vigor Router

You have finished the configuration of Quick Start Wizard and you can surf the Internet at any time. Now it is the time to register your Vigor router to MyVigor website for getting more service. Please follow the steps below to finish the router registration.

1 Please login the web configuration interface of Vigor router by typing "**admin/admin**" as User Name / Password.

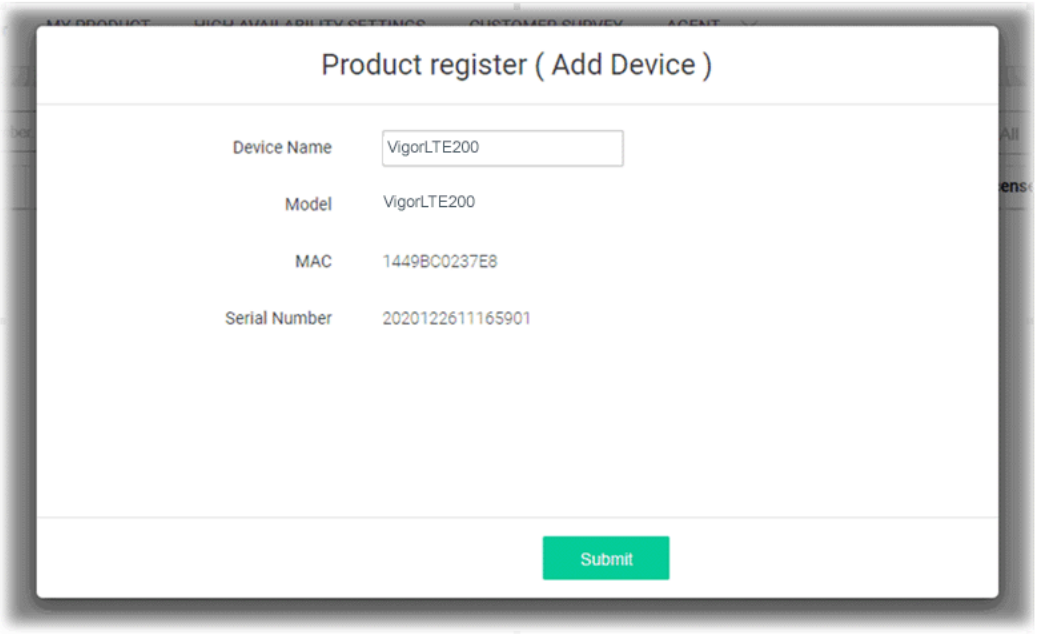
2 Click **Support Area>>Production Registration** from the home page.

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

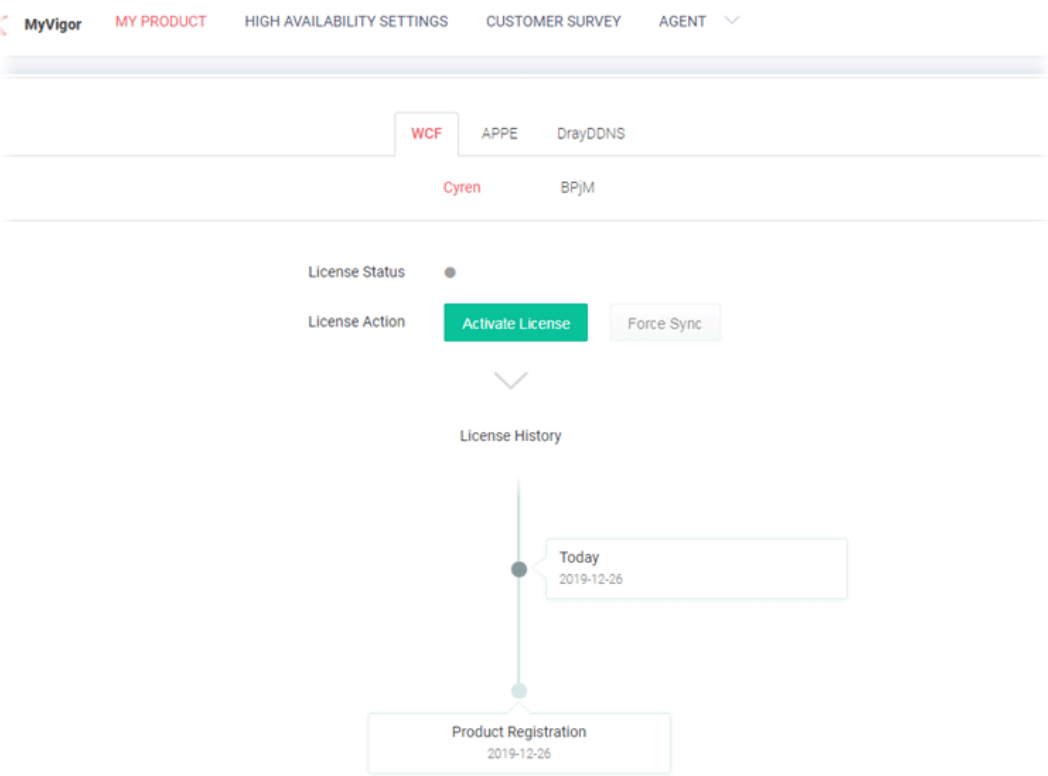


Info	If you haven't an accessing account, please refer to section Creating an Account for MyVigor to create your own one. Please read the articles on the Agreement regarding user rights carefully while creating a user account.

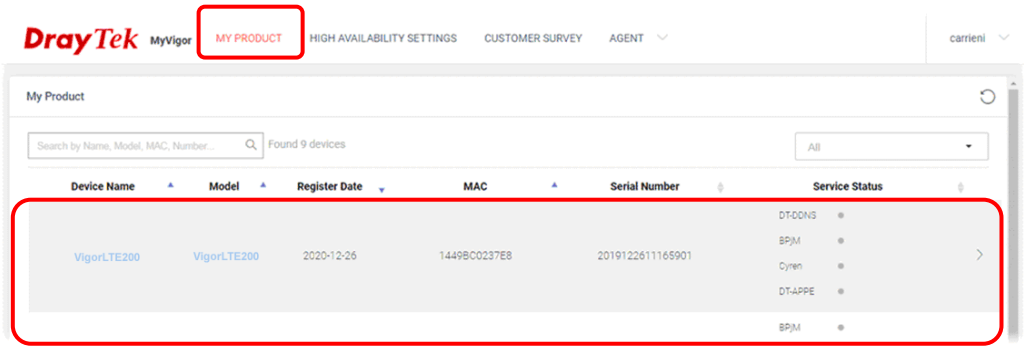
4 The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click **Submit**.



5 When the following page appears, your router information has been added to the database. Your router has been registered to *myvigor* website successfully.



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



This page is left blank.

Part II Connectivity

It means wide area network. Public IP will be used in WAN.

It means local area network. Private IP will be used in LAN. Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network.

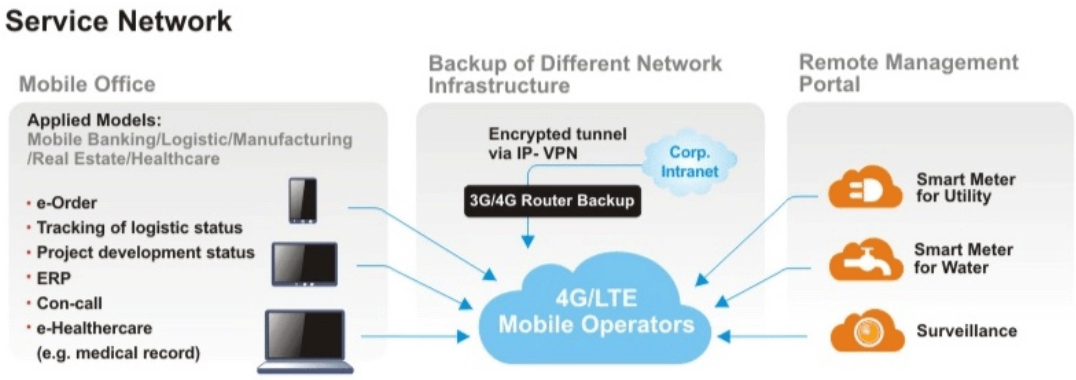
DNS, LAN DNS, IGMP, UPnP, WOL, RADIUS, SMS.

Static Route

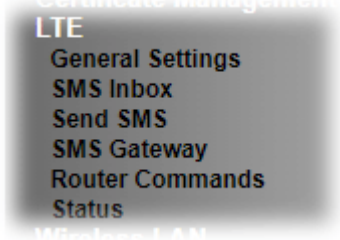
II-1 LTE

LTE WAN with SIM card can provide convinent Internet access for Vigor router. However, we can't stop thinking about what can Vigor router utilize this SIM card to provide more useful functions for user? Now, we have developed some useful functions for user, such as sending SMS from a router to report router status, rebooting router remotely via SMS with taking security into consideration, and so on.

This section can guide you to use the SIM card in LTE WAN to perform SMS related operations.



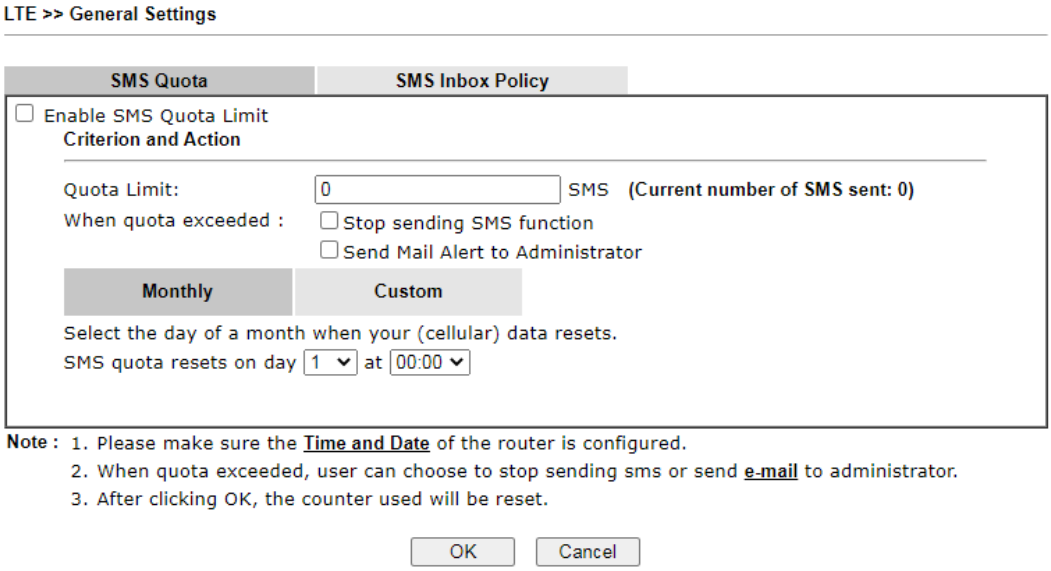
Web User Interface



II-1-1 General Settings

This page allows you to configure general settings for LTE. When SMS Quota Limit is enabled, you can specify the number of SMS quota, actions to perform when quota exceeded, and the period of resetting SMS quota used.

II-1-1-1 SMS Quota



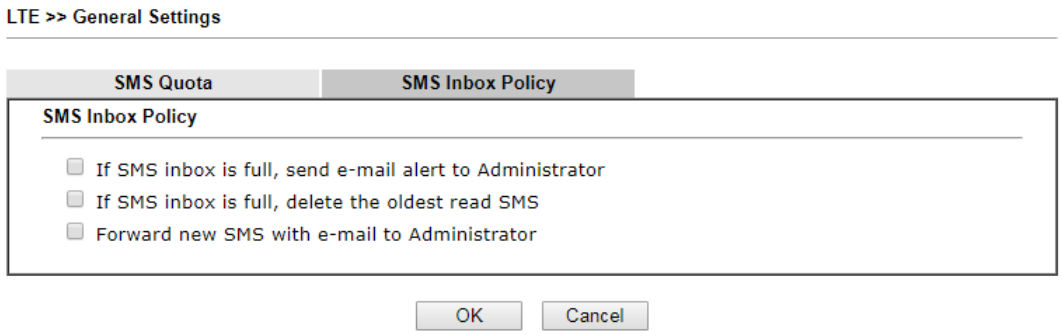
Available settings are explained as follows:

Item	Description
Enable SMS Quota Limit	Check the box to enable such feature.
Quota Limit	Specify the maximum number of sending SMS for LTE.
When quota exceeded	There are two actions to be performed when the quota limit is expired. **Stop sending SMS** – If it is checked, no SMS for LTE will be sent after the quota limit is expired. **Send Mail Alert to Administrator** – If it is checkd, a mail alert will be sent to the administrator when the quota limit is expired.
Monthly	This setting is to offer a mechanism of resetting the number of SMS sent record every month.

	SMS quota resets on day XX at XX … –You can determine the starting day in one month. The number of SMS sent will be reset.
Custom	This setting allows the user to define the billing cycle according to his request. The number of SMS sent will be reset with an interval of cycle duration. **Custom** – Monthly is default setting. If long period or a short period is required, use **Custom**. The period of reset is between 1 day and 60 days. You can determine the cycle duration by specifying the days and the hours. • **Cycle duration**: Specify the days to reset the number of SMS sent. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the number of SMS sent automatically. • **Today is day XX in the cycle** –Specify the day in the cycle duration as the starting point which Vigor router will reset the number of SMS sent. For example, 3 means the third day of the duration cycle.

II-1-1-2 SMS Inbox Policy

Such page allows you to determine which policy shall be used for SMS inbox/outbox.



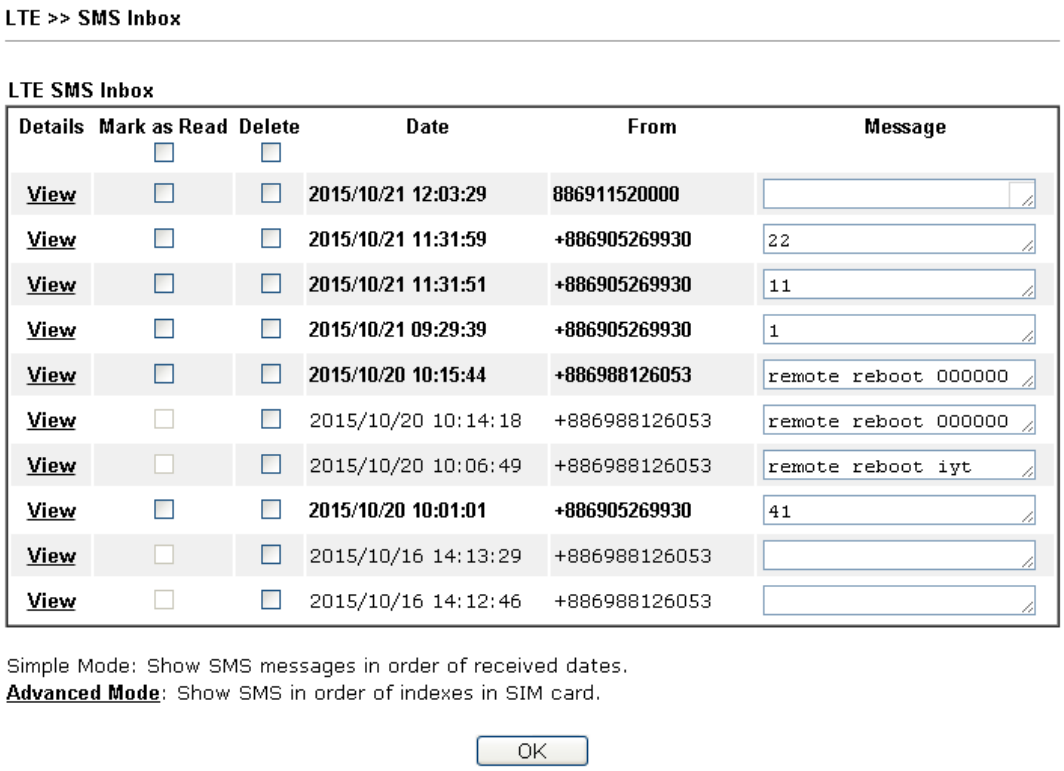
II-1-2 SMS Inbox

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

Since the data size of one SMS is limited, a long message will be sent by multiple SMS. For the convenience of users, we provide two modes. **Simple Mode** lists SMS messages in order for received time. **Advanced Mode** lists SMS in order for real index in the SIM card. Different SIM cards have different capacities. In general, it's around 30 to 40 SMS. Please note that the SIM card can not receive new SMS when all SMS indexes are occupied.

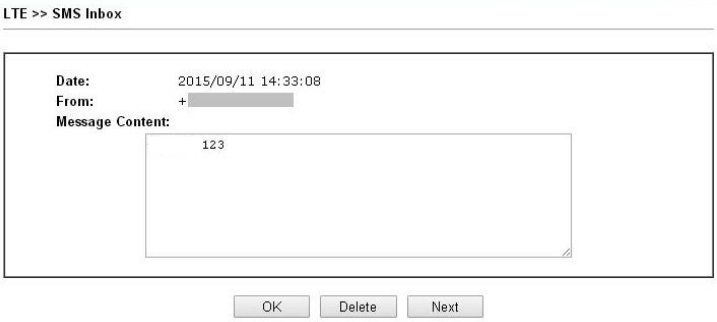
Click the Simple Mode link or the Advanced Mode link below to switch between these two modes.

II-1-2-1 Simple Mode



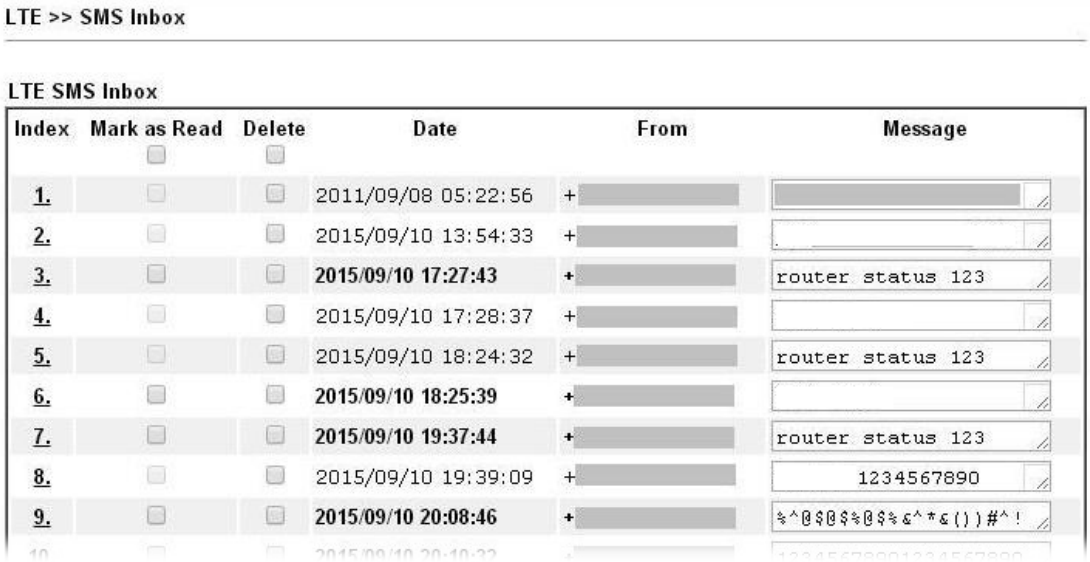
Available settings are explained as follows:

Item	Description
Mark as Read	Those messages in "unread" state are showed in bold text. If you want to change messages into "read" state, select them and click the OK button. Checking the checkbox in title will select all "unread" messages in this page.
Delete	If you want to delete messages, select them and click the OK button. Checking the checkbox in title will select all messages in this page.
Details	If you want to read the full content of the message, click the View link of that message to open the following page. It will change the message into "read" state.



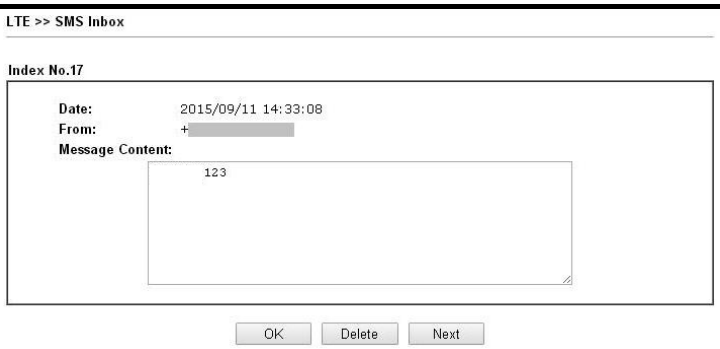
- **Message Content** - Display the full content of the message.
- **OK** - Return to previous page.
- **Delete** - Click it to delete this message and return to previous page.
- **Next** - Click it to see the content of next message.

II-1-2-1 Advanced Mode



Available settings are explained as follows:

Item	Description
Mark as Read	Those SMS in "unread" state are shown in bold text. If you want to change SMS into "read" state, select them and click the OK button. Checking the checkbox in title will select all "unread" SMS in this page.
Delete	If you want to delete SMS, select them and click the OK button. Checking the checkbox in title will select all SMS in this page.
Index	If you want to read the full content of the message of the SMS, click the index link of that SMS to open the following page. It will change all SMS of the message into "read" state.



Message Content - Display the full content of the message.

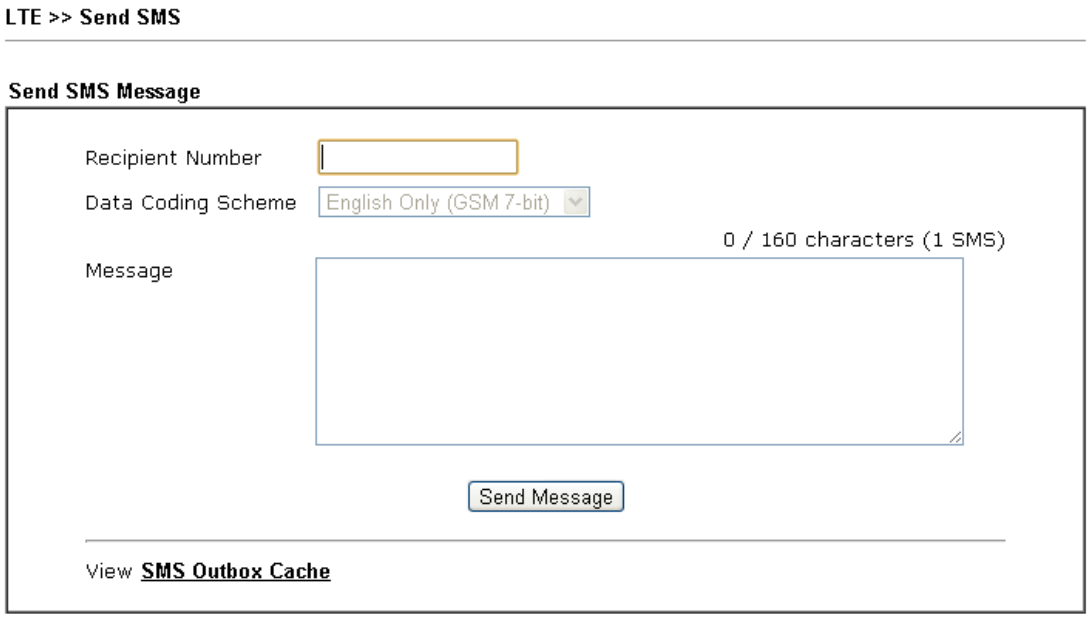
OK - Return to previous page.

Delete - Click it to delete all SMS of this message and return to previous page.

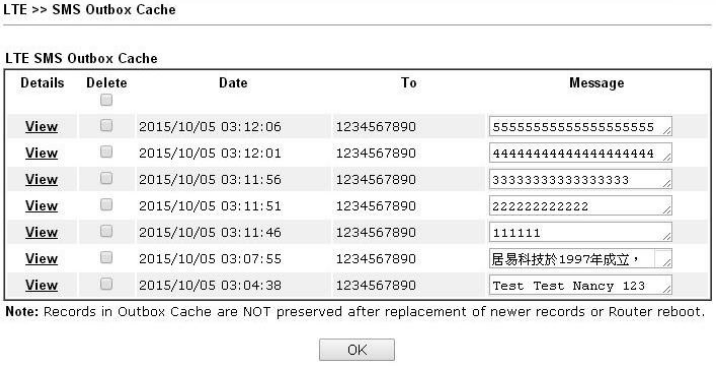
Next - Click it to see the content of next SMS index.

II-1-3 Send SMS

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



Available settings are explained as follows:

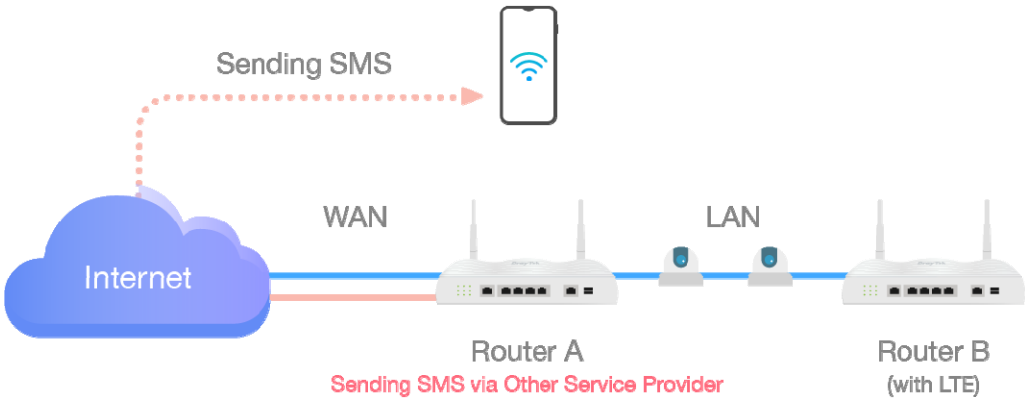
Item	Description
Recipient Number	Type the phone number of the recipient. The format can be an international phone number (+8869123455678) or a general phone number(0912345678).
Data Coding Scheme	The router will automatically select a suitable Data Coding Scheme according to the current content in Message. GSM 7-bit and UCS-2 are supported.
Message	Type in the message content to send. The total number of characters that you can type in this field is 1024.
Send Message	Click it to send this SMS message to the recipient immediately.
View SMS Outbox Cache	Display the record of SMS messages sent from the Router. 

II-1-4 SMS Gateway

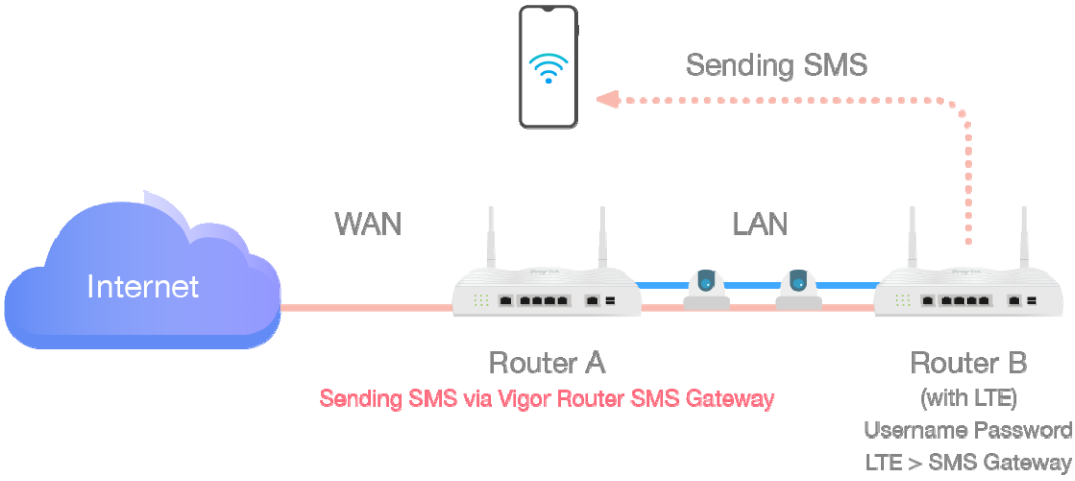
Vigor router can serve as an SMS Gateway for sending alerts via SMS to mobile phones.

Take a look at the following two pictures.

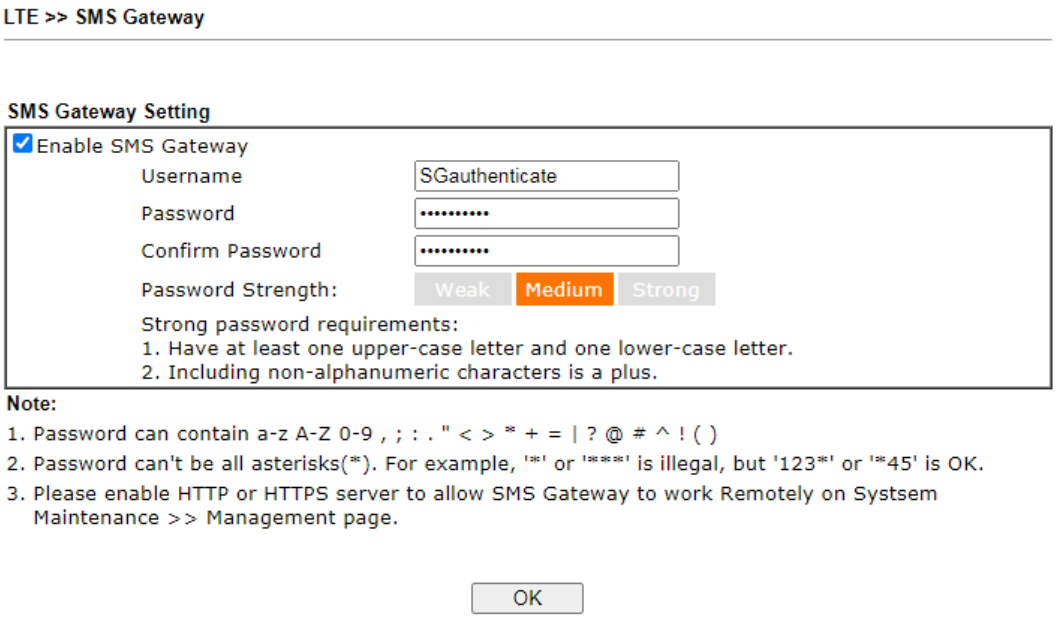
The IP cameras connect to Router A and Router B via LAN. Where there is something wrong with IP camera, Router A can only send the SMS with alerts/warning message via a specified service provider on Internet.



With the feature of SMS Gateway on Router B, even Router A is offline, router B could serve as an SMS Gateway that can send SMS (related to alerts or other events) to mobile phones directly.



For router B, simply open **LTE>>SMS Gateway** and set a pair of username and password.



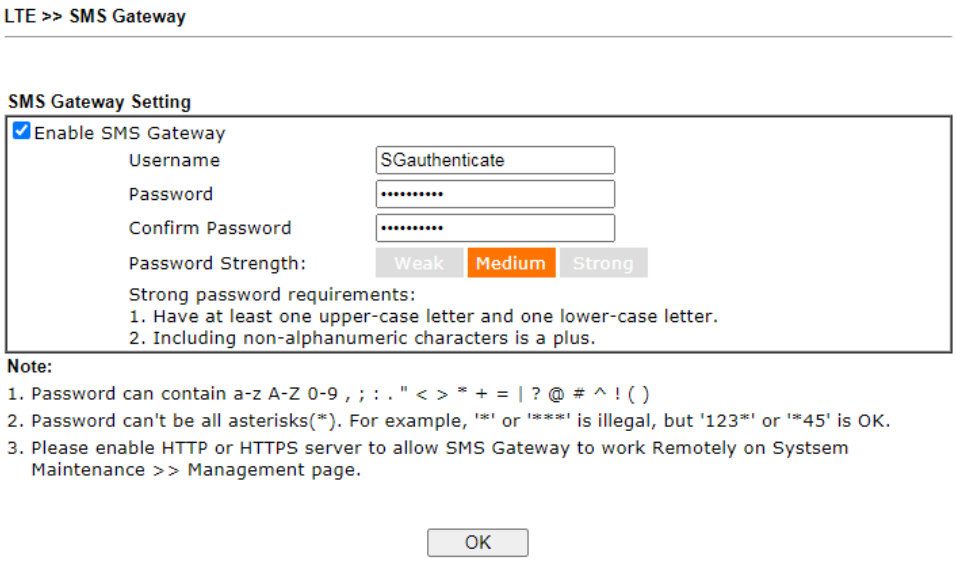
Available settings are explained as follows:

Item	Description
Enable SMS Gateway	Check the box to enable SMS gateway of this router.
Username	Define a username.
Password	Define a password.
Confirm Passowrd	Enter the password again.

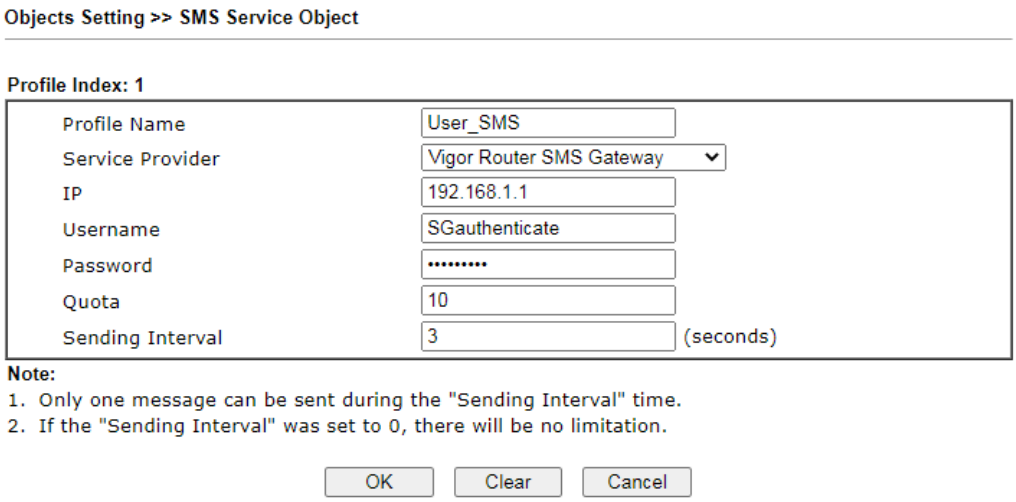
Below shows the settings configured on Router A and Router B.

1. Connect Router A and Router B (with LTE module).

2. On Router B, set a pair of username (e.g., SGauthenticate) and password on **LTE>>SMS Gateway**.

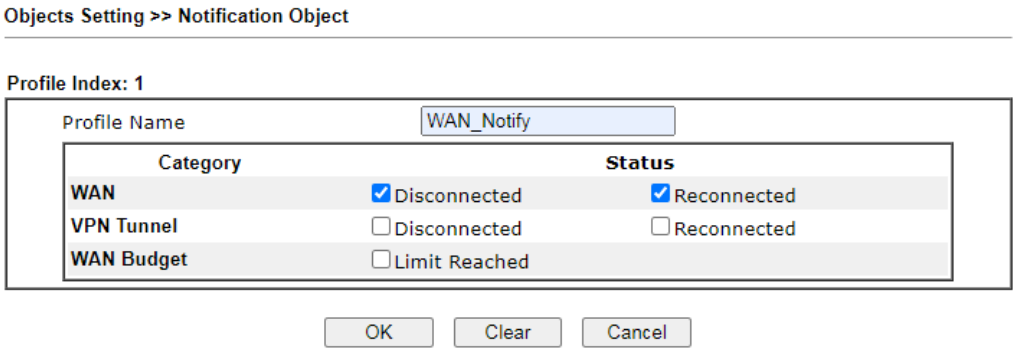


3. On Router A, open **Object Settings >> SMS Service Object>>Service Provider**. Click any index number (e.g., #1 in this case) to open the following page. Select **Vigor Router SMS Gateway** as the service provider. Set the WAN IP or LAN IP of this router in IP field.



As for username and password, please enter the same values as configured in Step 2.

4. Next, go to **Objects Setting >> Notification Object**. Select disconnection or connection of WAN, VPN tunnel and click **OK** to save the setting on Router A.



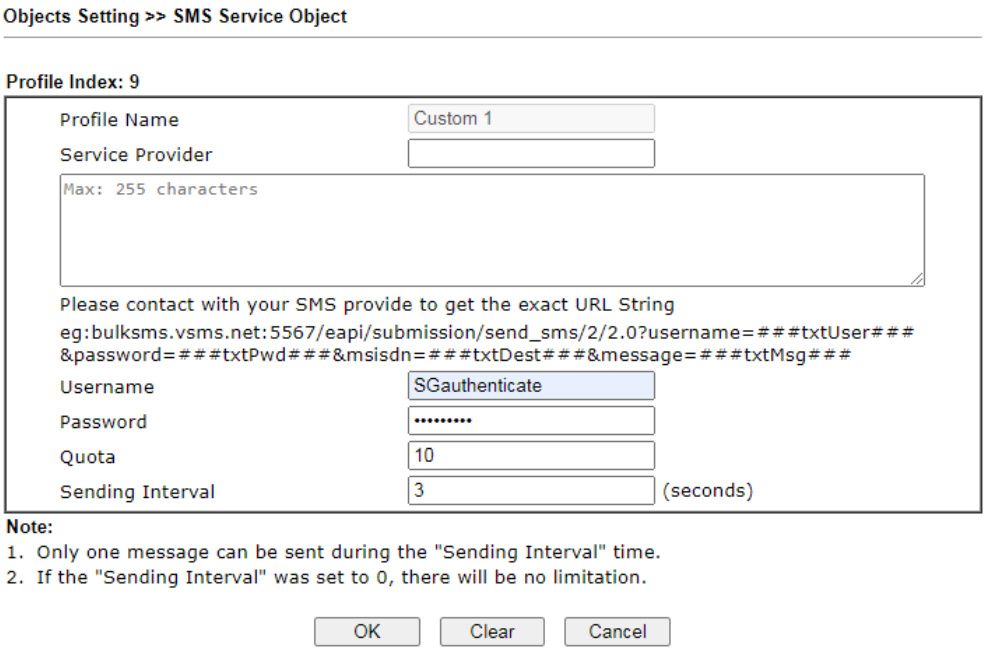
5. Once the router A encounters the condition set above, router B (as an SMS gateway) will send out an SMS to the recipient.

For a user who owns a non-DrayTek LTE router, there is one way to send the SMS to mobile phones through the non-DrayTek LTE router and DrayTek router.

1. Make sure the DrayTek router and the non-DrayTek LTE router are connected via LAN.

2. Obtain the exact URL string from non-DrayTek LTE router.

3. On DrayTek router, open **Objects Setting>>SMS Service Object** and click the number link #9 or #10 to customize SMS service object.



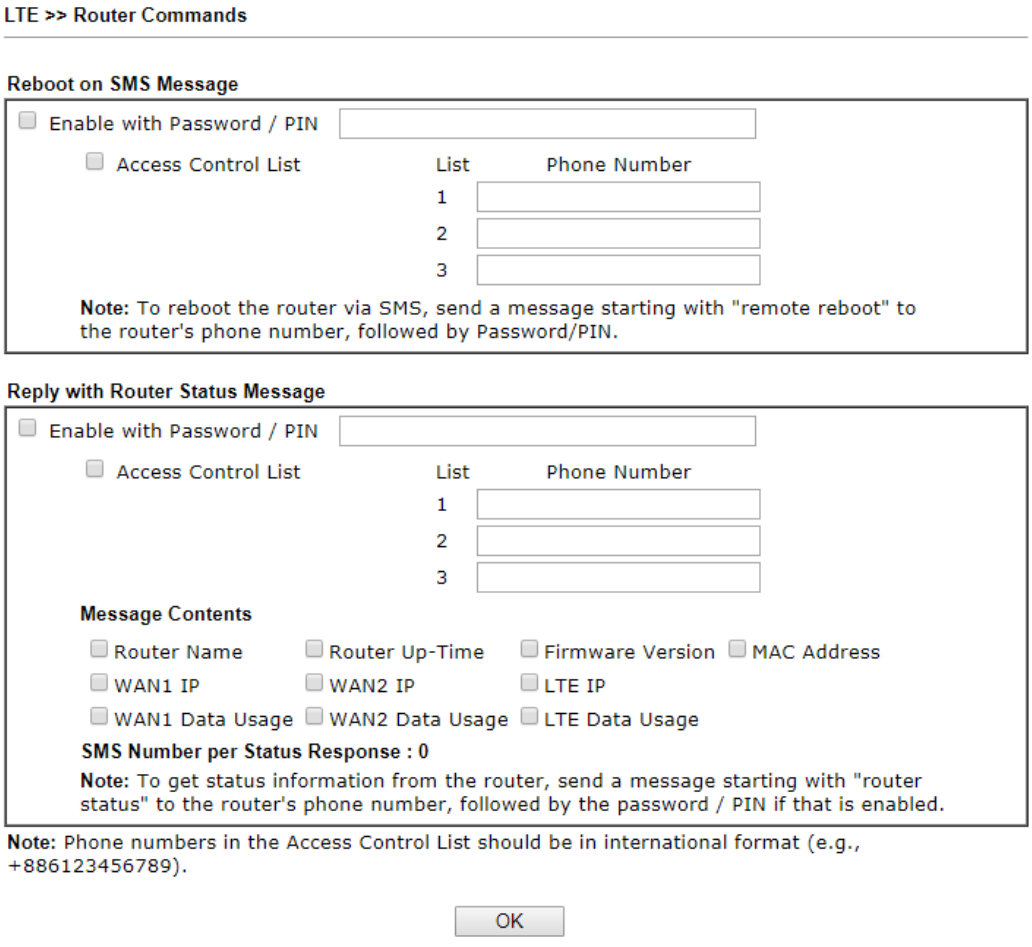
Enter the data coming from the non-DrayTek LTE router, e.g., the URL string, the username, password, and warning message on the entry box.

4. Click **OK** to save the settings.

II-1-5 Router Commands

This page allows the user to set function to reboot Vigor router remotely and get the router status via SMS.

Go to **LTE>>Router Commands** to get the following page.



Available settings are explained as follows:

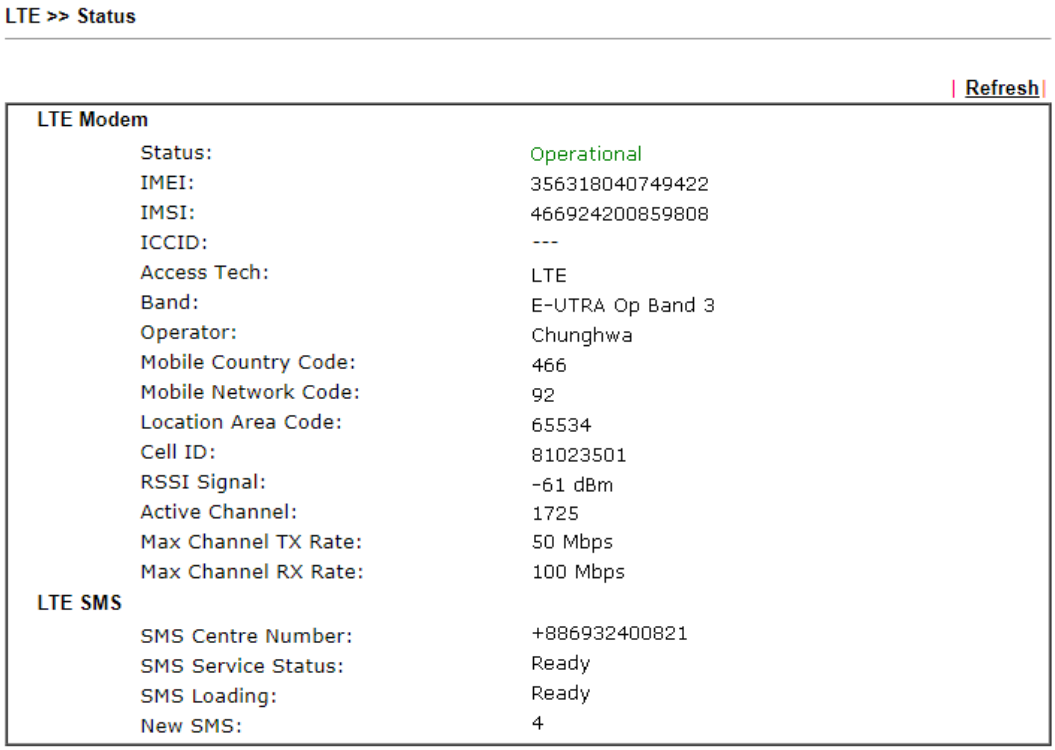
Item	Description
Reboot on SMS Message	
Enable with Password / PIN	To reboot Vigor router remotely via SMS, please check such box and type the password/PIN number (treated as

	authentication for any mobile phone). The password shall be composed by letters, numbers and baseline.
Access Control List	Check the box to type or modify (up to 3) phone numbers. The phone number specified here is capable of sending SMS to reboot such Vigor router remotely. **Note**: If such option is **enabled**, only mobile phones specified here are allowed to send SMS to reboot Vigor router if correct password is given. That is, if it is **disabled** (unchecked), any mobile phone can send SMS to reboot such Vigor router if correct password is given.
Reply with Router Status Message	
Enable with Password / PIN	Users can get the WAN data usage and basic information about Vigor router (e.g., IP address, MAC address) through the mobile phone by entering the password/PIN specified in this field. The password shall be composed by letters, numbers and baseline.
Access Control List	Check the box to type or modify (up to 3) phone numbers. The phone number specified here is capable of getting related information about Vigor router remotely. **Note**: If such option is **enabled**, only mobile phones specified here are allowed to obtaine related information about Vigor router if correct password is given. That is, if it is **disabled** (unchecked), any mobile phone can get the data of Vigor router if correct password is given.
Message Contents	There are several types of message contents for you to select. Choose and check the required item, then Vigor router will offer the status response about that item via SMS.
SMS messages per status response	Display the total number of the type for status response. Display the total number of SMS required to send the status message which contains the current selected Message Contents.

II-1-6 Status

Vigor router with LTE function is capable of accessing into Internet and able to send SMS to specified mobile phone.

This page will display basic information about the embedded LTE module and the current LTE connection.



Each item is explained as follows:

Item	Description
Status	LTE WAN status.
IMEI	International Mobile Equipment Identity of the embedded LTE module.
IMSI	International Mobile Subscripber Identity of the LTE SIM card.
Access Tech	Type of LTE connection (CDMA/GSM/WCDMA/LTE/TD-SCDMA).
Band	Band of LTE connection.
Operator	ISP name of LTE connection.
Mobile Country Code / Mobile Network Code / Location Area Code / Cell ID :	Base station information.
RSSI Signal	Signal strength of LTE connection.
Active Channel	Frequency of LTE connection.
Max Channel TX Rate /	Maximum TX/RX link rate of LTE connection.

Max Channel RX Rate	
SMS Centre Number	The phone number for SMS service of the LTE SIM card.
SMS Service status	Whether the SMS service of the LTE SIM card is ready.
SMS Loading	Whether the received SMS messages in the LTE SIM card have been loaded to the Router.
New SMS	The number of unread SMS in SMS Inbox.

II-2 WAN

It allows users to access Internet.

Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as *private* IP addresses, and are listed in the following ranges:

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

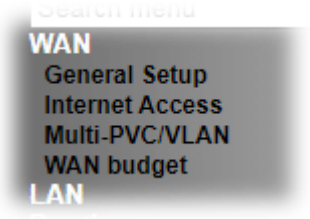
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

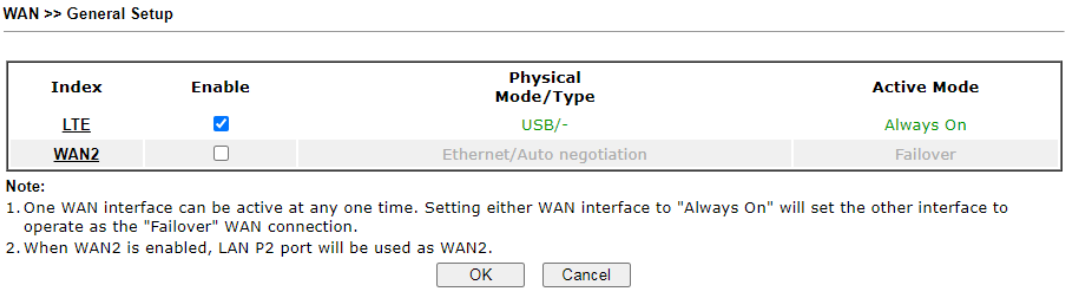
When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

Web User Interface



II-2-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for LTE/WAN in details.

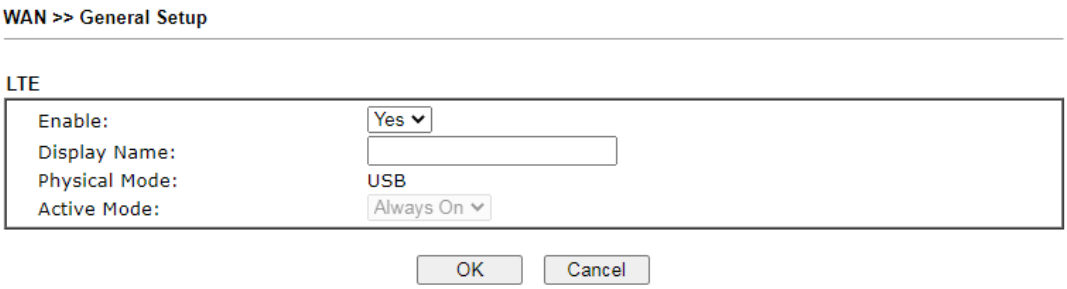


Available settings are explained as follows:

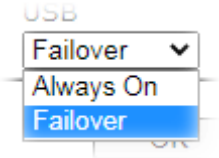
Item	Description
Index	Click the LTE/ WAN interface link under Index to access into the WAN configuration page.
Enable	**V** means such WAN interface is enabled and ready to be used.
Physical Mode / Type	Display the physical mode and physical type of such WAN interface.
Active Mode	Display whether such WAN interface is Active device or backup device.

II-2-1-1 LTE

To use LTE network connection through LTE module, please configure **LTE** interface.



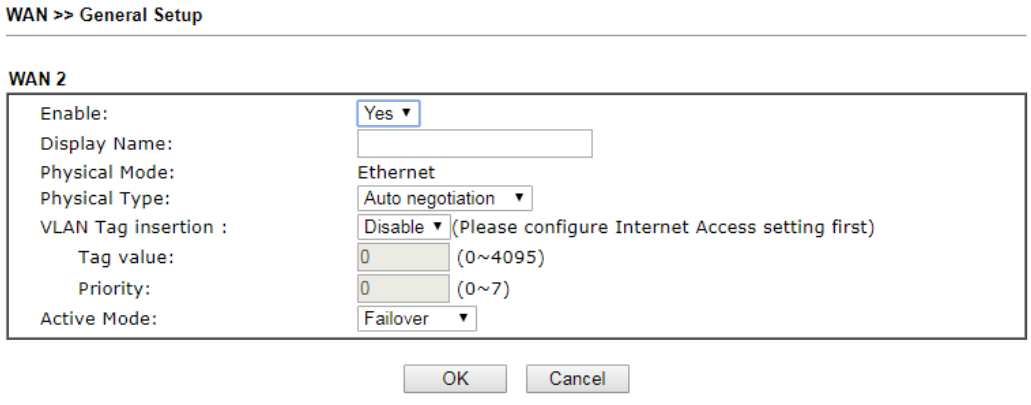
Available settings are explained as follows:

Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Enter the description for such WAN interface.
Physical Mode	Display the physical mode of this WAN interface.
Active Mode	In general, LTE WAN is main interface and is always on for Internet connection. However, if WAN2 is enabled and set as Always On, the LTE WAN can be treated as backup WAN and allowed to be set as Always On or Failover.  **Always On -** Make the LTE connection being activated always. **Failover** – Choose it to make the LTE connection as a backup connection.

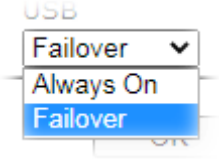
After finished the above settings, click **OK** to save the settings.

II-2-1-2 WAN2

Click WAN2 link to get the following page:



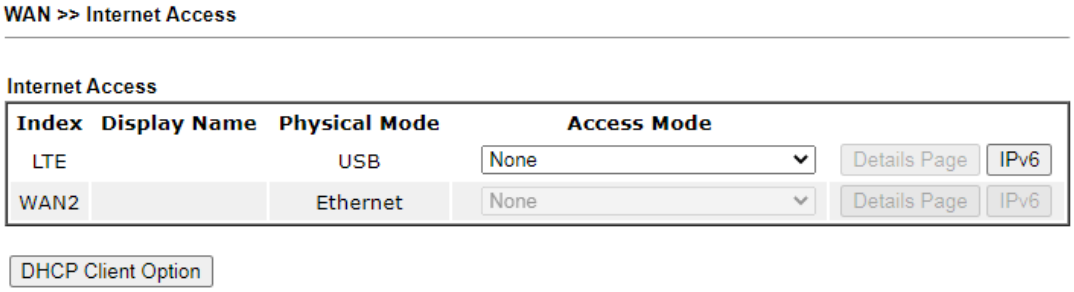
Available settings are explained as follows:

Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Enter the description for such WAN interface.
Physical Mode	Display the physical mode of this WAN interface.
VLAN Tag insertion	**Enable** – Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please Enter the tag value and specify the priority for the packets sending by WAN interface. **Disable** – Disable the function of VLAN with tag. **Tag value** – Enter the value as the VLAN ID number. The range is from 0 to 4095. **Priority** – Enter the packet priority number for such VLAN. The range is from 0 to 7.
Active Mode	Choose **Always On** to make the WAN connection being activated always.  **Failover** – Choose it to make the WAN connection as a backup connection.

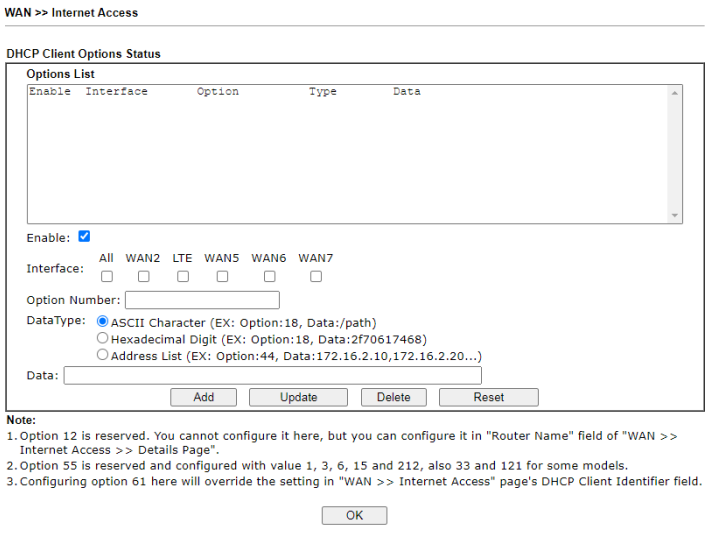
After finished the above settings, click **OK** to save the settings.

II-2-2 Internet Access

This page allows you to set WAN configuration with different modes.



Available settings are explained as follows:

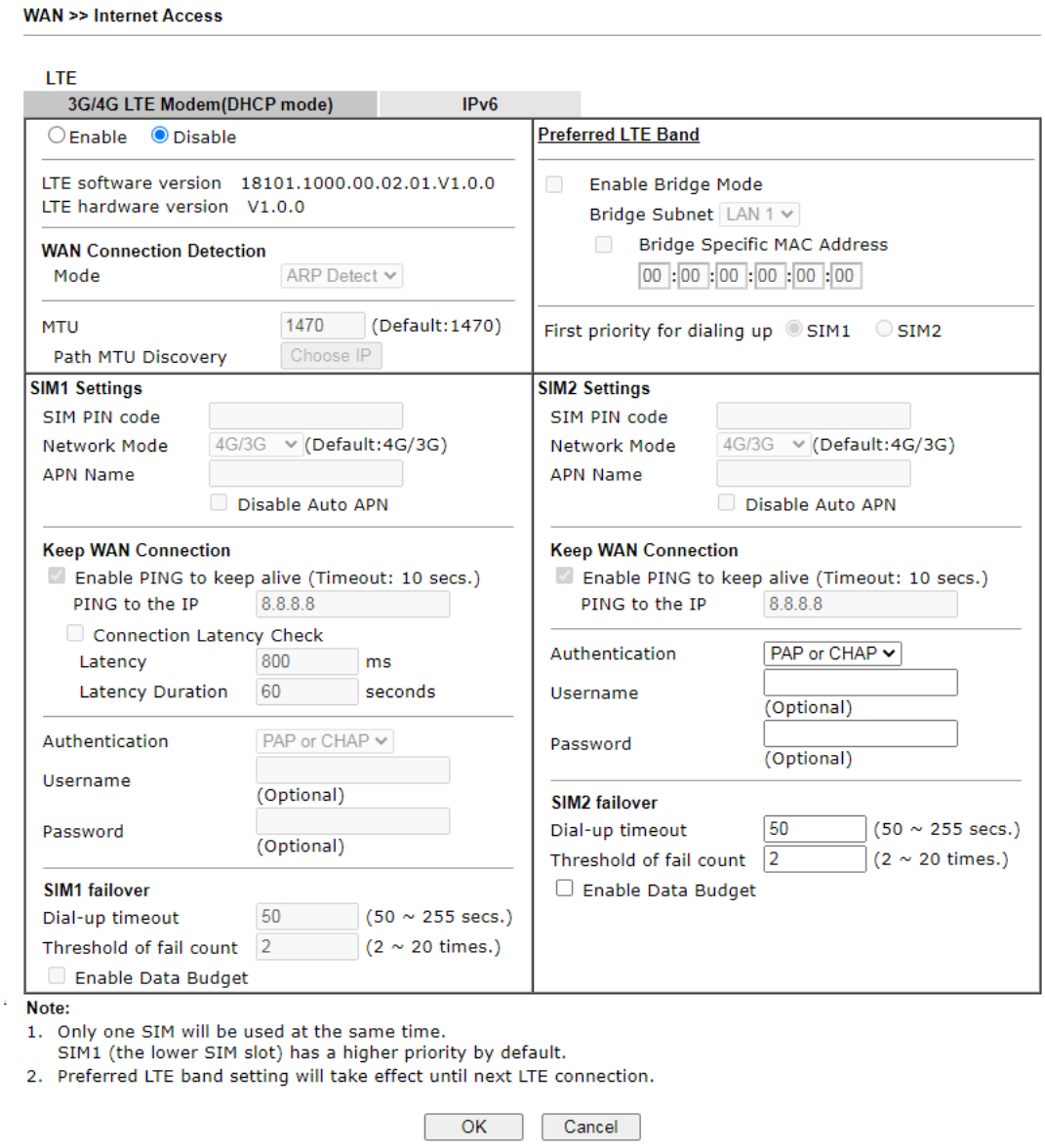
Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/LTE that entered in general setup.
Physical Mode	It shows the physical connection for WAN (Ethernet or fiber) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click **Details Page** for accessing the page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.
DHCP Client Option	This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.  **Enable** – Check the box to enable the function of DHCP

	Option. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets. **Interface** – Specify the WAN interface(s) that will be overwritten by such function. WAN5 ~ WAN6 can be located under **WAN>>Multi-PVC/VLAN**. **Option Number** – Type a number for such function. **Note:** If you choose to configure option 61 here, the detailed settings in **WAN>>Interface Access** will be overwritten. **DataType** – Choose the type (ASCII or Hex) for the data to be stored. **Data** – Enter the content of the data to be processed by the function of DHCP option.

II-2-2-1 Details Page for 3G/4G LTE Modem (DHCP mode) in LTE WAN

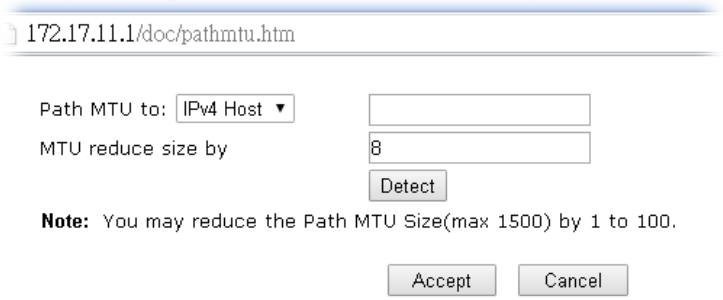
LTE WAN uses the embedded LTE module to access internet.

To use **3G/4G LTE Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G LTE Modem (DHCP mode)** for LTE. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Enable	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
LTE hardware version	The hardware version of the embedded LTE module.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use 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)** – Set TTL value of PING operation. ● **Ping Interval –** Type the interval for the system to execute the PING operation. ● **Ping Retry –** Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Choose IP** to open the following dialog.  ● **Path MTU to** – Type the IP address as the specific transmit path. ● **MTU reduce size by** – It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● **Detect** – Click it to detect a suitable MTU value. ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
Preferred LTE Band	Click the link to open a pop-up dialog. Different ISPs can offer various LTE bands. Available legal bands will be shown on the screen based on the operational bands offered by YOUR ISP. In default, all the bands are enabled. Choose one or multiple bands if you want to change. If not, keep the default configuration. **Enable Bridge Mode (Use LAN Port P1)** - DHCP client (a PC or other router) connected to LAN Port P1 is able to get WAN IP to access Internet from LTE WAN interface. ● **Bridge Specific MAC Address** - Enter the MAC address of the DHCP client (a PC or a router) manually to get the WAN IP. **First priority for dialing up -** Select SIM1 or SIM2 as the first priority for dialing up. The default setting is SIM1.
SIM1 Settings	
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 19

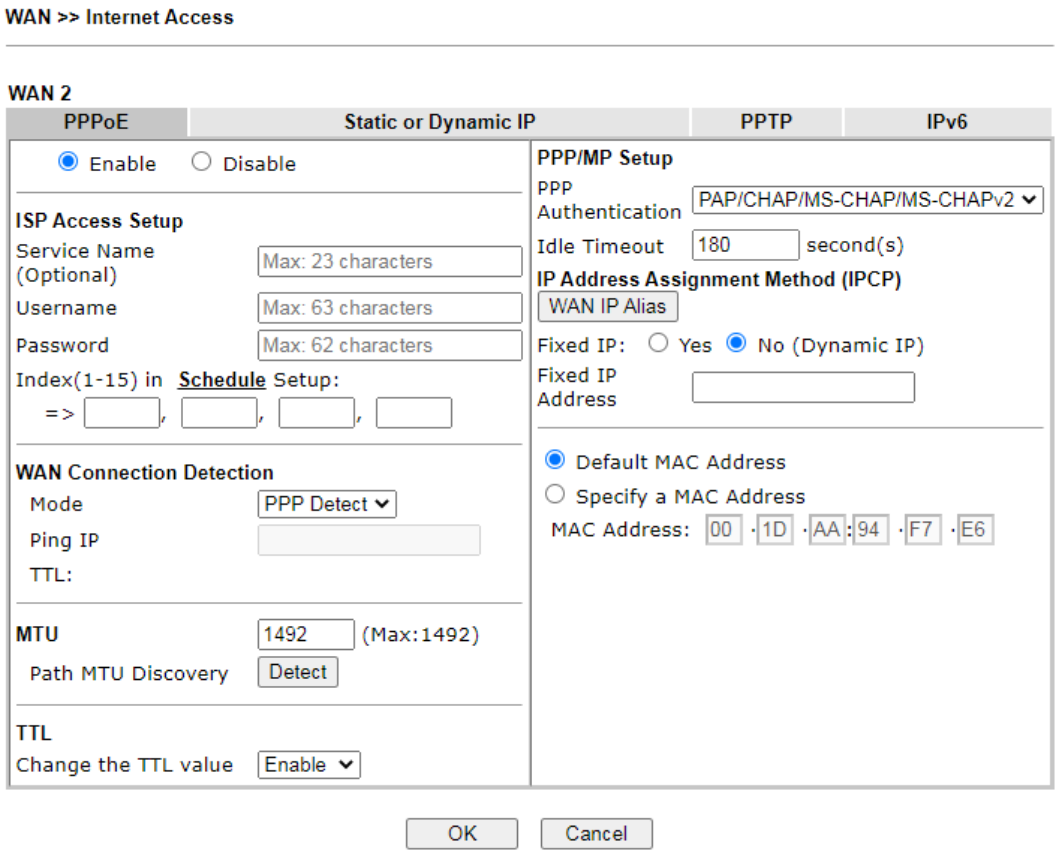
	characters.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click **Apply.** The maximum length of the name you can set is 47 characters.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. **Enable PING to Keep alive** – If you enable the PING function, please specify an IP address for the system to PING it for keeping alive. Vigor system will send a packet per second to the specified IP address. If the system does not receive any reply from that IP within 10 seconds, Vigor system will reboot LTE module until successfully set LTE connection. ● **PING to the IP** – Enter an IP address. **Connection Latency Check** - Enable the latency time setting for packet reply. If it is enabled (checked), Vigor system will wait for the packet reply from the specified IP address. When the time of waiting packet reply reaches the time threshold (defined in Latency) and continues for a period of time (defined in Latency Duration), Vigor system will reboot LTE module until successfully set LTE connection. ● **Latency** – Set a time threshold for packet reply. Default value is 800 (unit: micro-second). ● **Latency Duration** – Set a time period. Default value is 60 (unit: second). **Authentication -** Select **None** or **PAP or CHAP**. **UserName -** Enter the username (optional). The maximum length of the name you can set is 47 characters. **Password -** Enter the password (optional). The maximum length of the password you can set is 62 characters.
SIM2 Settings	
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 19 characters.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click **Apply.** The maximum length of the name you can set is 47 characters.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function.

	Enable PING to Keep alive – If you enable the PING function, please specify an IP address for the system to PING it for keeping alive. Vigor system will send a packet per second to the specified IP address. If the system does not receive any reply from that IP within 10 seconds, Vigor system will reboot LTE module until successfully set LTE connection. ● **PING to the IP** – Enter an IP address. **Authentication -** Select **None** or **PAP or CHAP**. **UserName -** Enter the username (optional). The maximum length of the name you can set is 47 characters. **Password -** Enter the password (optional). The maximum length of the password you can set is 62 characters.
SIM1/SIM2 failover	**Dial-up timeout** - Set the time out interval (50 to 255 seconds). **Threshold of fail count** - Set the maximum times (2 to 20) of failed dial-ups. After that, the system will stop dial-up and use another SIM card for dial-up instead. **Enable Data Budget** - When selected, WAN Budget is enabled for this WAN. ● **Quota Limit** - Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify. ● **When quota exceeded: Shutdown WAN interface** - All the outgoing traffics through the WAN interface will be terminated. ● **Send alert SMS to** - The system will send out a warning message to a specified mail address when the quota is running out. However, the connection charges will be calculated continuously. ● **Quota resets on day** - Some ISP might apply for the network limitation based on the traffic limit per month. This setting is to offer a mechanism for resetting the traffic record every month. You can determine the starting day in one month.

After finishing all the settings here, please click **OK** to activate them.

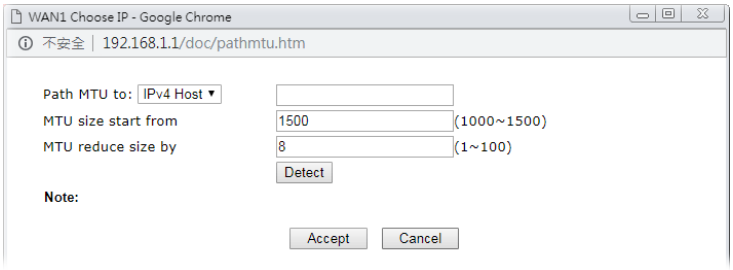
II-2-2-2 Details Page for PPPoE in WAN2

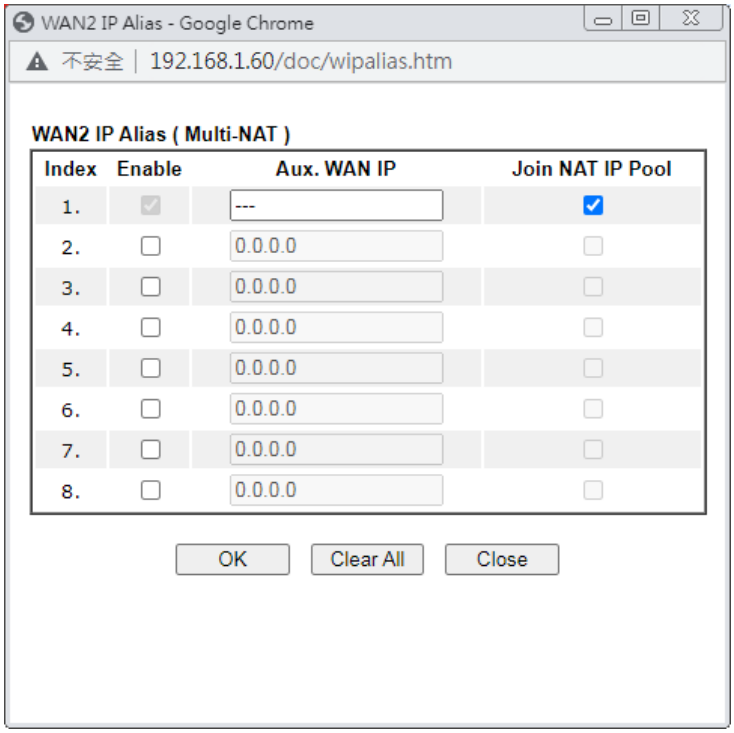
To choose PPPoE as the accessing protocol of the Internet, please select **PPPoE** from the **WAN>>Internet Access >>WAN2** page. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Enable/Disable	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. **Service Name** - Enter the description of the specific network service. **Username** – Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. **Password** – Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. **Index (1-15)** - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through PPP Detect or Ping Detect.

	Mode – Choose **PPP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use 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)** – Set TTL value of PING operation. ● **Ping Interval –** Type the interval for the system to execute the PING operation. ● **Ping Retry –** Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Detect** to open the following dialog.  ● **Path MTU to** – Type the IP address as the specific transmit path. ● **MTU size start from** – Determine the starting point value of the packet. Default setting is 1500. ● **MTU reduce size by** – It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● **Detect** – Click it to detect a suitable MTU value ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
TTL	**Change the TTL value –** Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router. ● **Enable** - TTL value will be reduced (-1) when it passess through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0". ● **Disable** – TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.

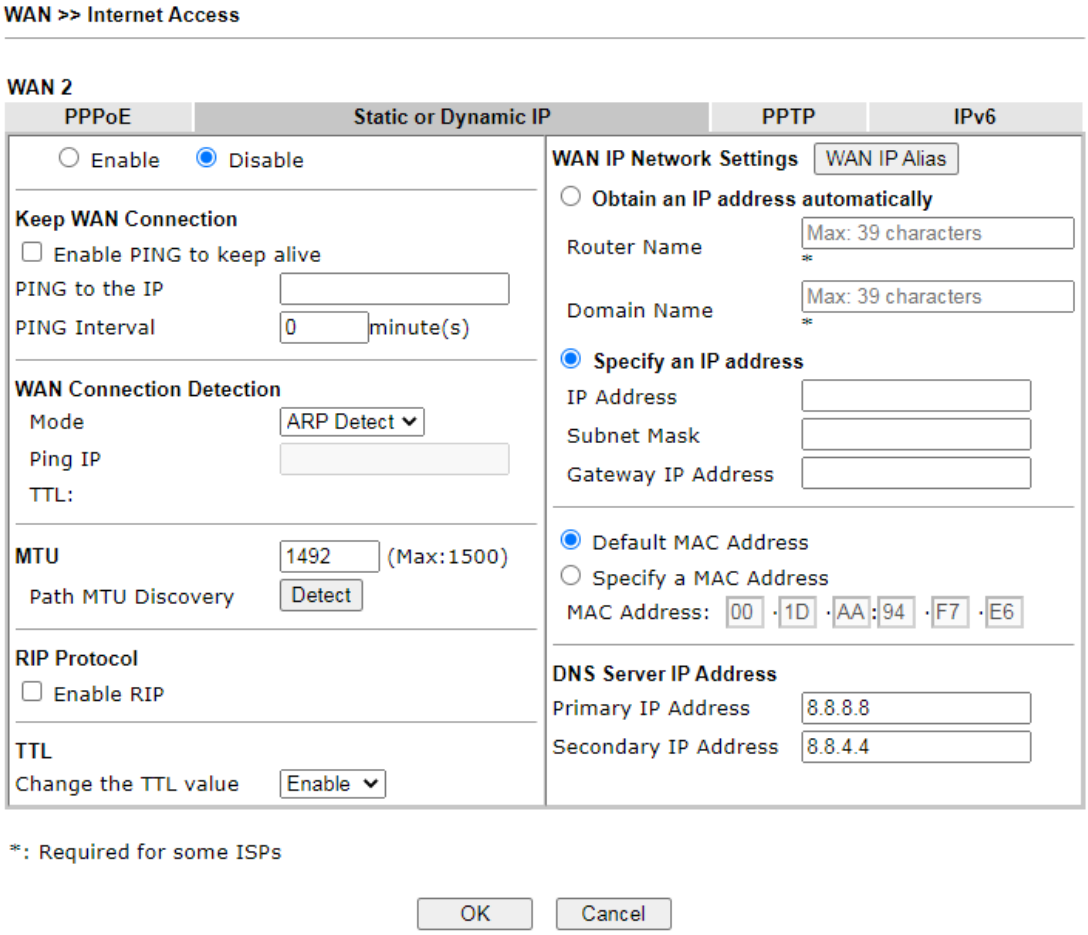
PPP/MP Setup	**PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. **Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action. **IP Assignment (IPCP)-** Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. **WAN IP 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. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click **OK** to exit the dialog.  **Fixed IP Address** – Type in a fixed IP address. **Default MAC Address** – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router. **Specify a MAC Address –** Type the MAC address for the router manually.

After finishing all the settings here, please click **OK** to activate them.

II-2-2-3 Details Page for Static or Dynamic IP in WAN2

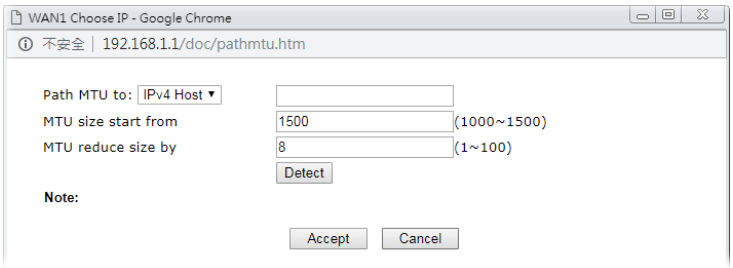
For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you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

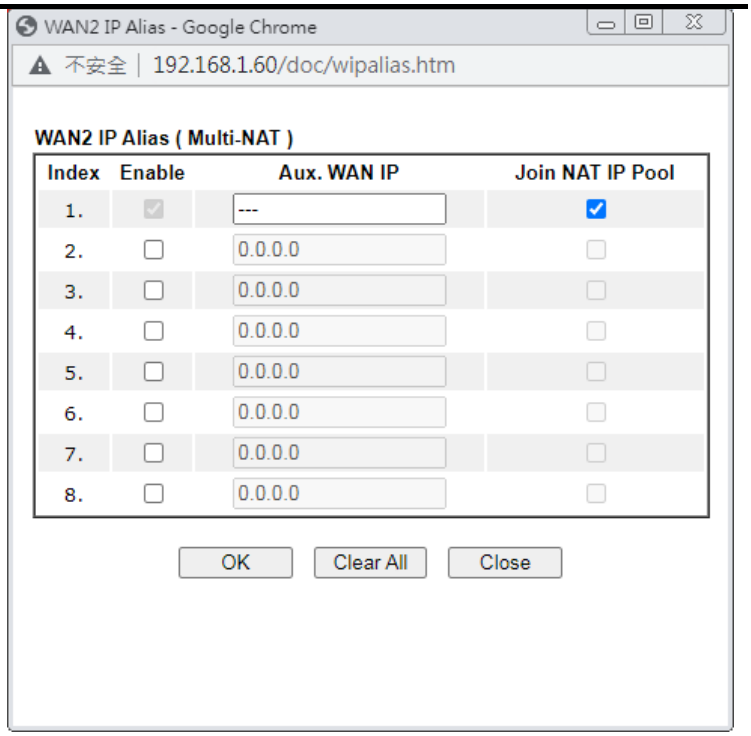
To use **Static or Dynamic IP** as the accessing protocol of the internet, please click the **Static or Dynamic IP** tab. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Enable / Disable	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. **PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval** - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect, Ping Detect** or **Always On** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use 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)** – Set TTL value of PING operation. ● **Ping Interval –** 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	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Detect** to open the following dialog.  ● **Path MTU to** – Choose the destination as the specific transmit path and Enter the IP address. ● **MTU size start from** - Determine the starting point value of the packet. ● **MTU reduce size by** – It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● **Detect** – Click it to detect a suitable MTU value ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
RIP Protocol	Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.
TTL	**Change the TTL value –** Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router. **Enable** - TTL value will be reduced (-1) when it passess through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0". **Disable** – TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you Enter IP address manually. **WAN IP 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.



Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.

- **Router Name**: Enter the router name provided by ISP.
- **Domain Name**: Enter the domain name that you have assigned.

Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.

- **IP Address**: Enter the IP address.
- **Subnet Mask**: Enter the subnet mask.
- **Gateway IP Address**: Enter the gateway IP address.

Default MAC Address: Click this radio button to use default MAC address for the router.

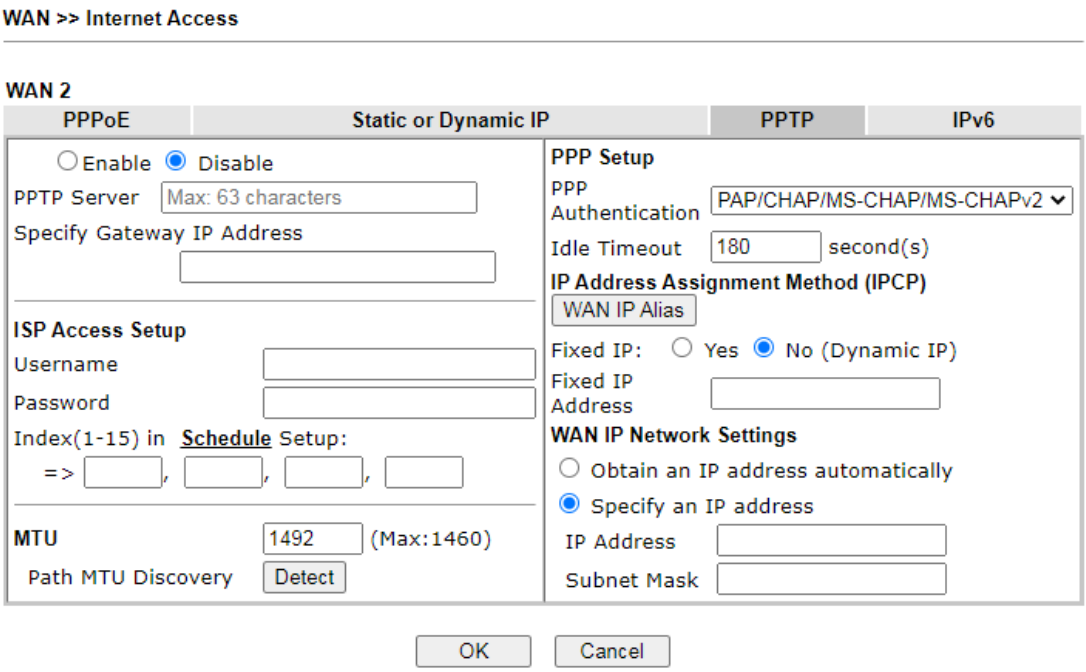
Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IP Address	Enter the primary IP address for the router if you want to use **Static IP** mode. If necessary, Enter secondary IP address for necessity in the future.

After finishing all the settings here, please click **OK** to activate them.

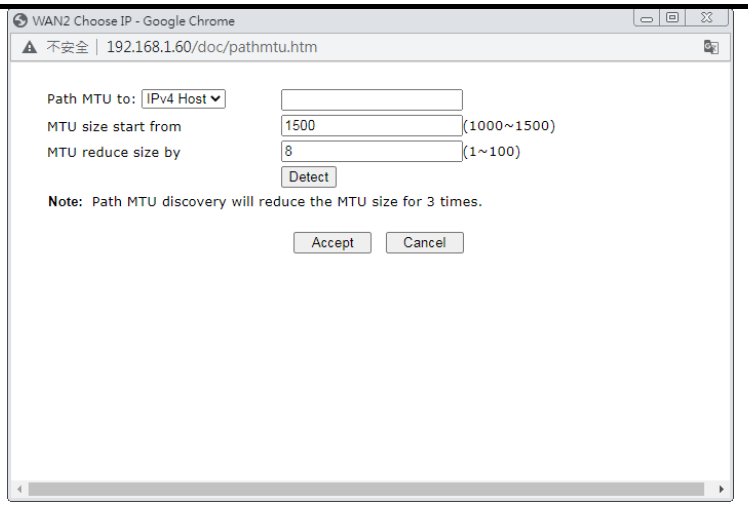
II-2-2-4 Details Page for PPTP

To use **PPTP** as the accessing protocol of the internet, please click the **PPTP** tab. The following web page will be shown.



Available settings are explained as follows:

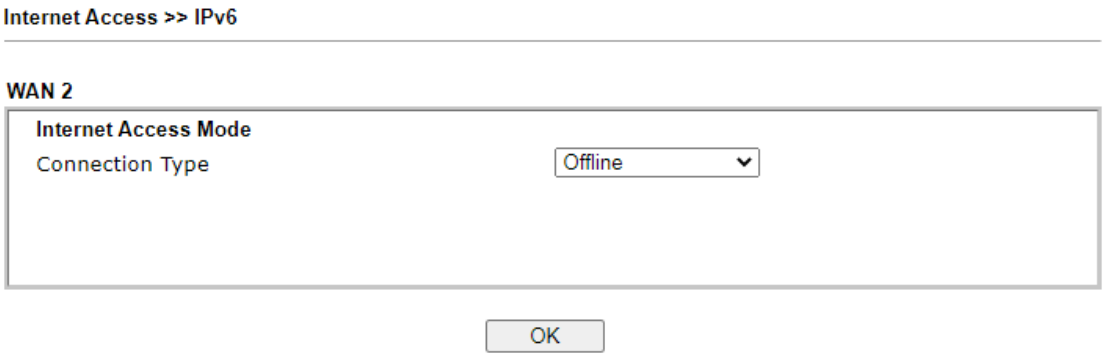
Item	Description
PPTP	**Enable -** Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface. **Disable** – Click this radio button to close the connection through PPTP. **PPTP Server** - Specify the IP address of the PPTP server if you enable PPTP client mode. **Specify Gateway IP Address** – Specify the gateway IP address for DHCP server.
ISP Access Setup	**Username** -Enter the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. **Password** -Enter the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. **Index (1-15) in Schedule Setup -** You can Enter four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Detect** to open the following dialog.

	 ● **Path MTU to** – Choose the destination as the specific transmit path and Enter the IP address. ● **MTU size start from** - Determine the starting point value of the packet. ● **MTU reduce size by** – It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● **Detect** – Click it to detect a suitable MTU value ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
PPP Setup	**PPP Authentication** - Select **PAP only** or **PAP or CHAP** for PPP. **Idle Timeout** - Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method(IPCP)	**WAN IP 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. **Fixed IP** - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and Enter a fixed IP address in the box. **Fixed IP Address -**Type a fixed IP address.
WAN IP Network Settings	**Obtain an IP address automatically** – Click this button to obtain the IP address automatically. **Specify an IP address** – Click this radio button to specify some data. ● **IP Address** – Enter the IP address. ● **Subnet Mask** – Enter the subnet mask.

After finishing all the settings here, please click **OK** to activate them.

II-2-2-5 Details Page for IPv6 – Offline

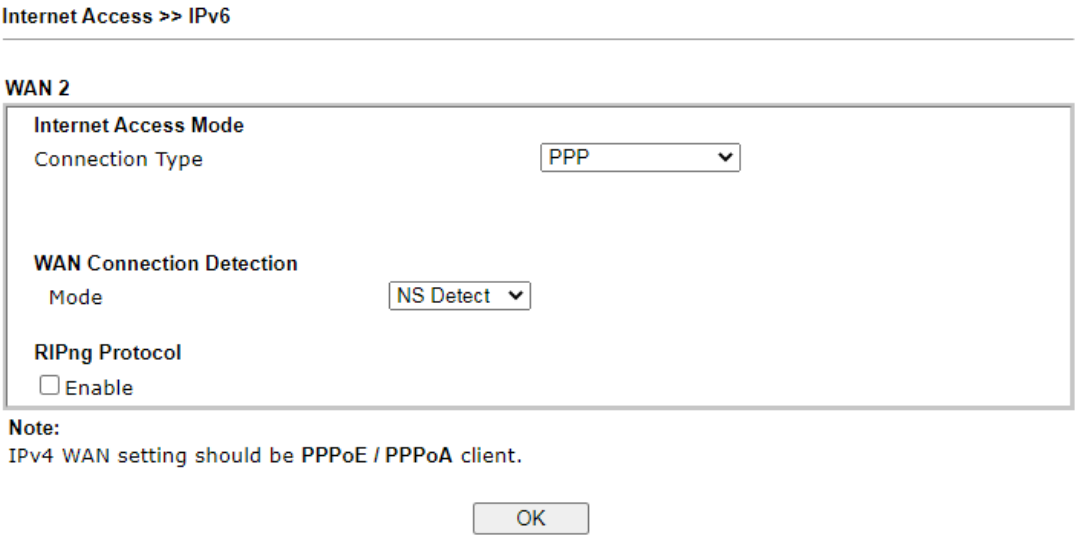
When Offline is selected, the IPv6 connection will be disabled.



II-2-2-6 Details Page for IPv6 – PPP

During the procedure of IPv4 PPPoE connection, we can get the IPv6 Link Local Address between the gateway and Vigor router through IPv6CP. Later, use DHCPv6 or accept RA to acquire the IPv6 prefix address (such as: 2001:B010:7300:200::/64) offered by the ISP. In addition, PCs under LAN also can have the public IPv6 address for Internet access by means of the generated prefix.

No need to type any other information for PPP mode.

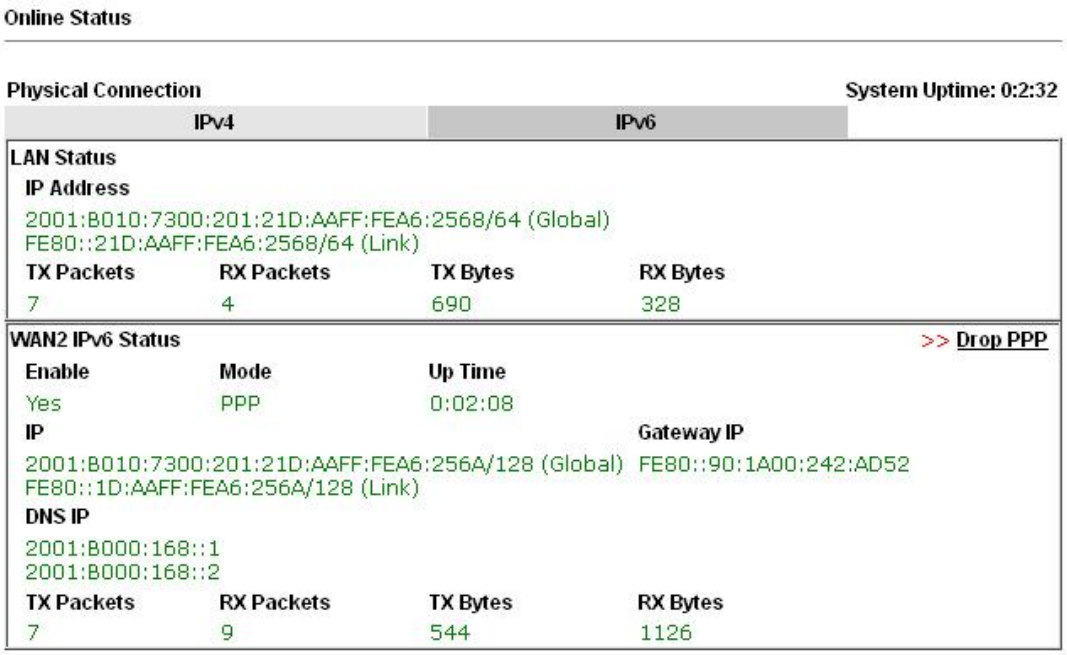


Available settings are explained as follows:

Item	Description
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **NS Detect**, **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

Below shows an example for successful IPv6 connection based on PPP mode.



Info

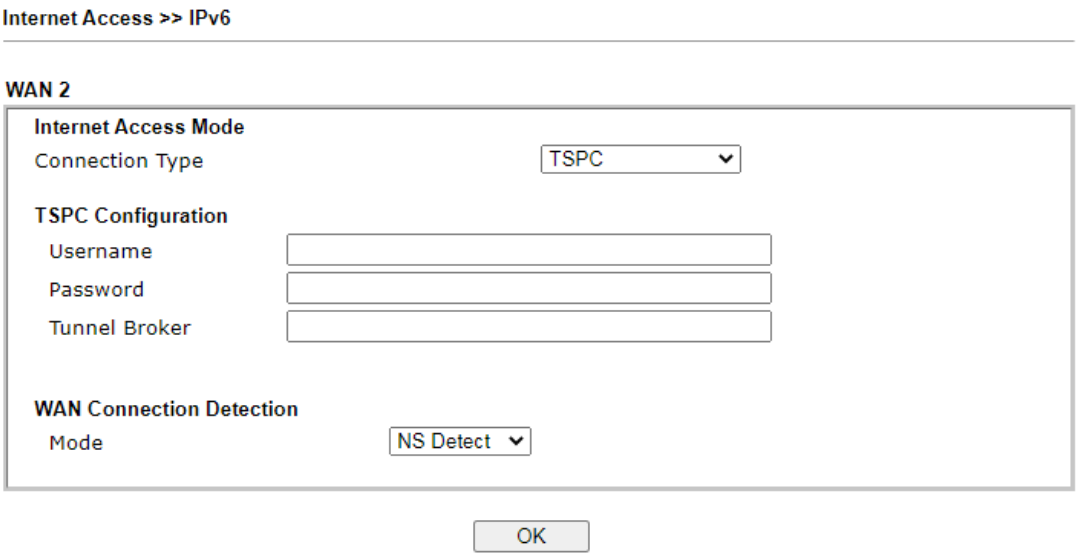
At present, the IPv6 prefix can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

II-2-2-7 Details Page for IPv6 – 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.

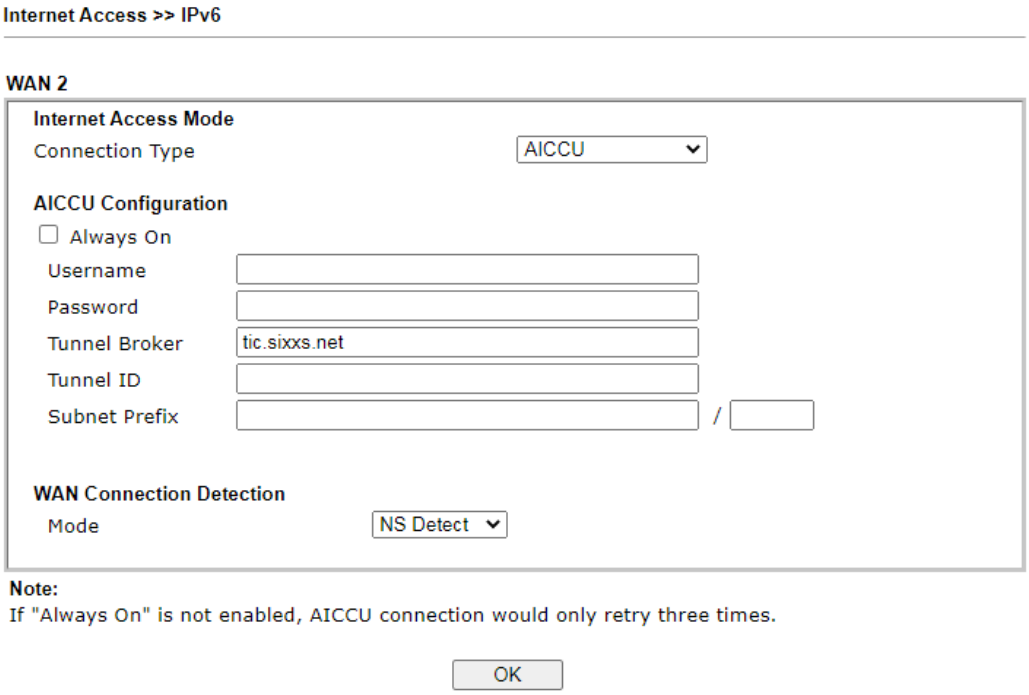


Available settings are explained as follows:

Item	Description
Username	Enter the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account. The maximum length of the name you can set is 63 characters.
Password	Enter the password assigned with the user name. The maximum length of the name you can set is 19 characters.
Tunnel Broker	Enter the address for the tunnel broker IP, FQDN or an optional port number.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **NS Detect**, **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

After finished the above settings, click **OK** to save the settings.

II-2-2-8 Details Page for IPv6 – AICCU



Available settings are explained as follows:

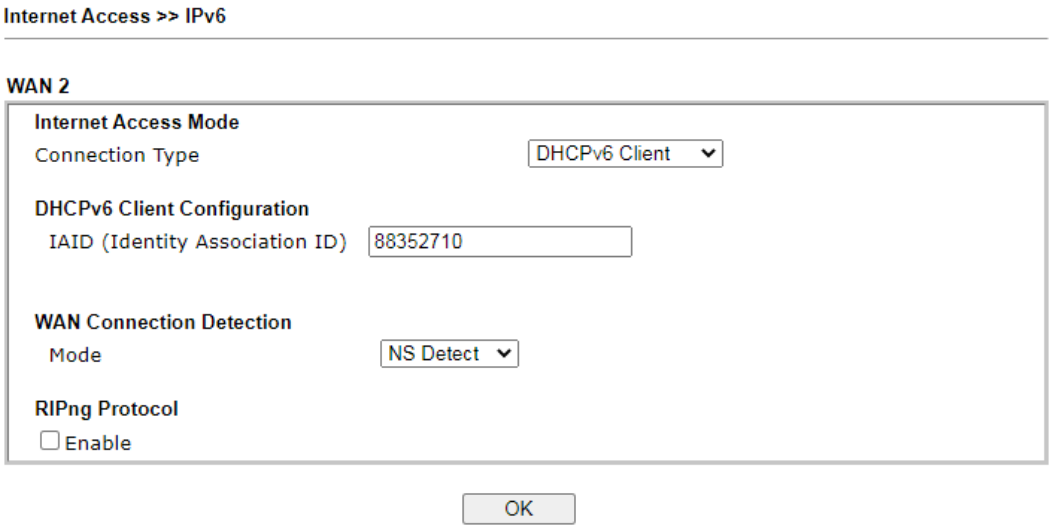
Item	Description
Always On	Check this box to keep the network connection always.
Username	Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password. The maximum length of the name you can set is 19 characters.
Password	Enter the password assigned with the user name. The maximum length of the password you can set is 19 characters.
Tunnel Broker	It means a server of AICCU. The server can provide IPv6 tunnels to sites or end users over IPv4. Enter the address for the tunnel broker IP, FQDN or an optional port number.
Tunnel ID	One user account may have several tunnels. And, each tunnel shall have one specified tunnel ID (e.g., T115394). Enter the ID offered by Tunnel Broker.
Subnet Prefix	Enter the subnet prefix address obtained from service provider. The maximum length of the prefix you can set is 128 characters.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **NS Detect**, **Always On** or **Ping Detect** for the system to execute for WAN detection. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field

	for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

After finished the above settings, click **OK** to save the settings.

II-2-2-9 Details Page for IPv6 – DHCPv6 Client

DHCPv6 client mode would use DHCPv6 protocol to obtain IPv6 address from server.



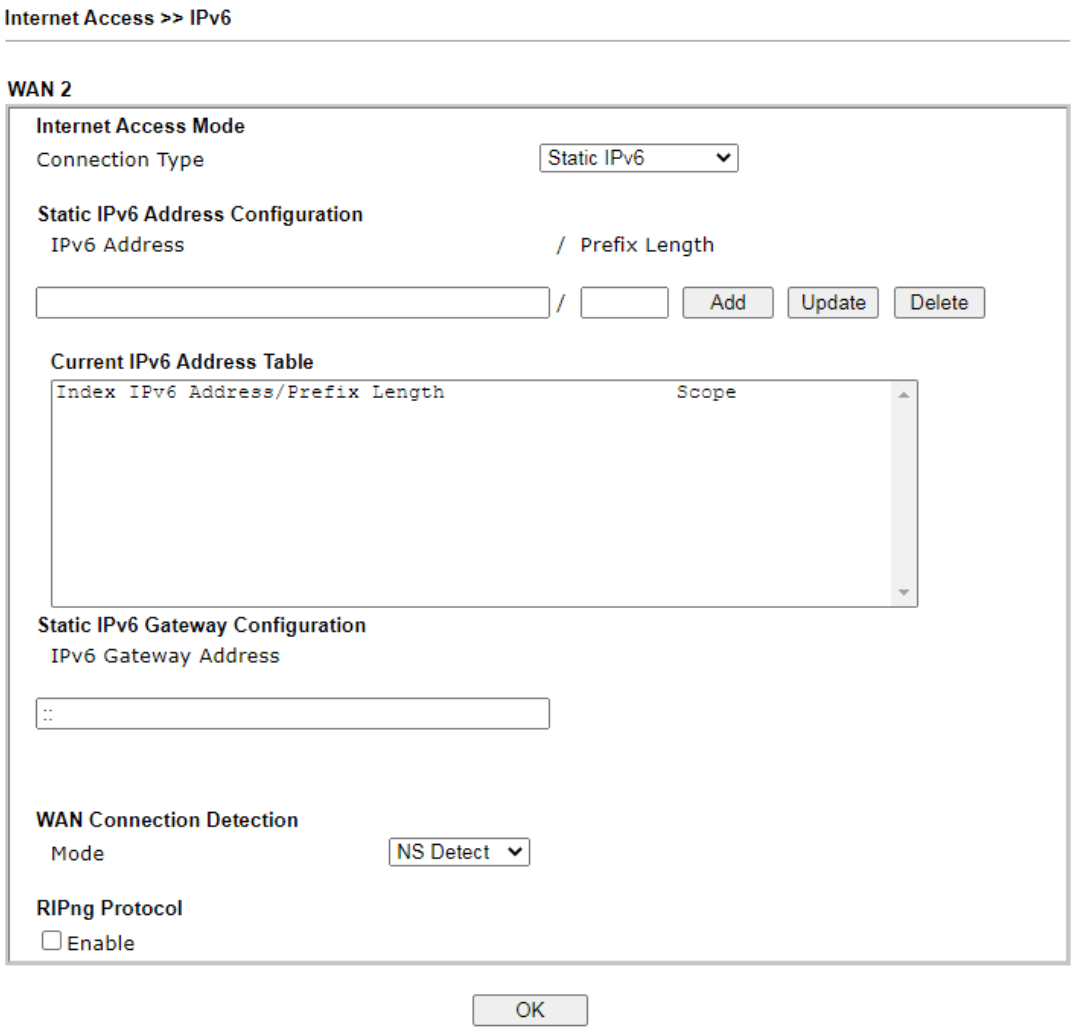
Available settings are explained as follows:

Item	Description
DHCPv6 Client Configuration	**IAID** - Type a number as IAID.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect. **Mode** – Choose **Always On**, **Ping Detect** or **NS Detect** for the system to execute for WAN detection. With **NS Detect** mode, the system will check if network connection is established or not, like IPv4 ARP Detect. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

After finished the above settings, click **OK** to save the settings.

II-2-2-10 Details Page for IPv6 – Static IPv6

This type allows you to setup static IPv6 address for WAN interface.



Available settings are explained as follows:

Item	Description
Static IPv6 Address configuration	**IPv6 Address –** Enter the IPv6 Static IP Address. **Prefix Length –** Enter the fixed value for prefix length. **Add –** Click it to add a new entry. **Update** – Click it to modify an existed entry. **Delete –** Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.
Static IPv6 Gateway Configuration	**IPv6 Gateway Address -** Type your IPv6 gateway address here.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **NS Detect, Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always.

	● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

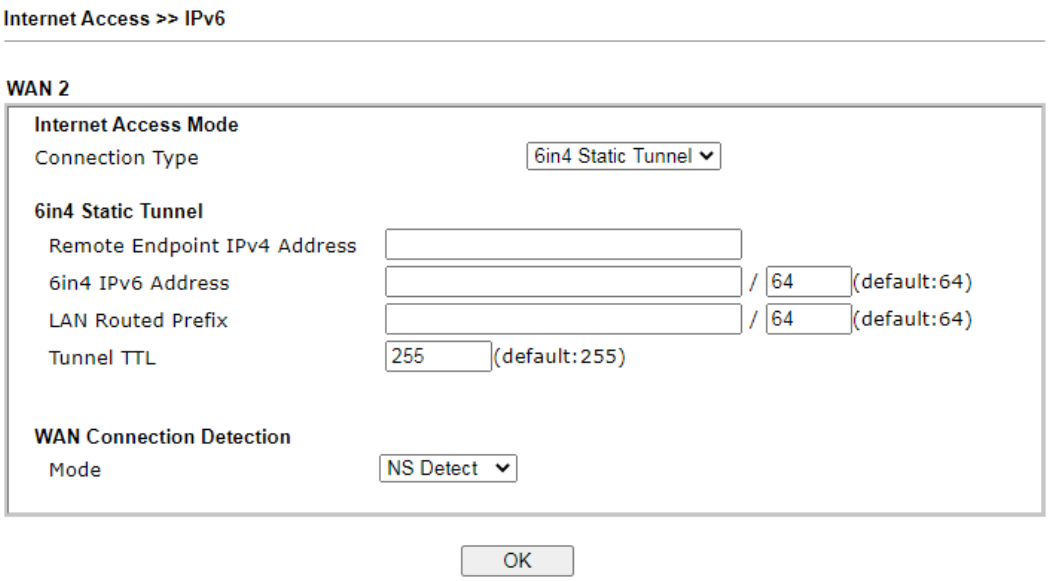
After finished the above settings, click **OK** to save the settings.

II-2-2-11 Details Page for IPv6 – 6in4 Static Tunnel

This type allows you to setup 6in4 Static Tunnel for WAN interface.

Such mode allows the router to access IPv6 network through IPv4 network.

However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than anycast endpoint. The mode has more reliability.



Available settings are explained as follows:

Item	Description
Remote Endpoint IPv4 Address	Enter the static IPv4 address for the remote server.
6in4 IPv6 Address	Enter the static IPv6 address for IPv4 tunnel with the value for prefix length.
LAN Routed Prefix	Enter the static IPv6 address for LAN routing with the value for prefix length.
Tunnel TTL	Enter the number for the data lifetime in tunnel.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **NS Detect, Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field

	for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

After finished the above settings, click **OK** to save the settings.

Below shows an example for successful IPv6 connection based on 6in4 Static Tunnel mode.

Online Status

Physical Connection **System Uptime: 0day 0:4:16**

IPv4 | IPv6

LAN Status

IP Address

2001:4DD0:FF00:83E4:21D:AAFF:FE83:11B4/64 (Global)
FE80::21D:AAFF:FE83:11B4/64 (Link)

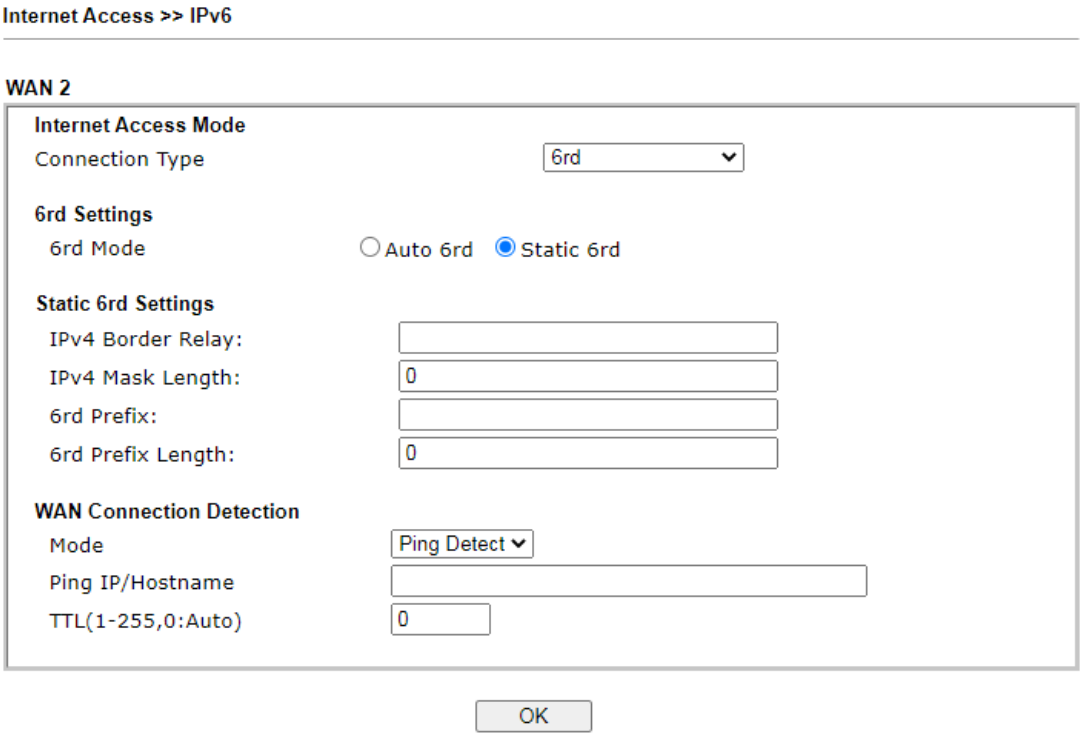
TX Packets	RX Packets	TX Bytes	RX Bytes
14	80	1244	6815

WAN1 IPv6 Status

Enable	Mode	Up Time	
Yes	6in4 Static Tunnel	0:04:07	
IP			**Gateway IP**
2001:4DD0:FF10:83E4::2131/64 (Global) FE80::C0A8:651D/128 (Link)			---
TX Packets	**RX Packets**	**TX Bytes**	**RX Bytes**
3	26	211	2302

II-2-2-12 Details Page for IPv6 – 6rd

This type allows you to setup 6rd for WAN interface.

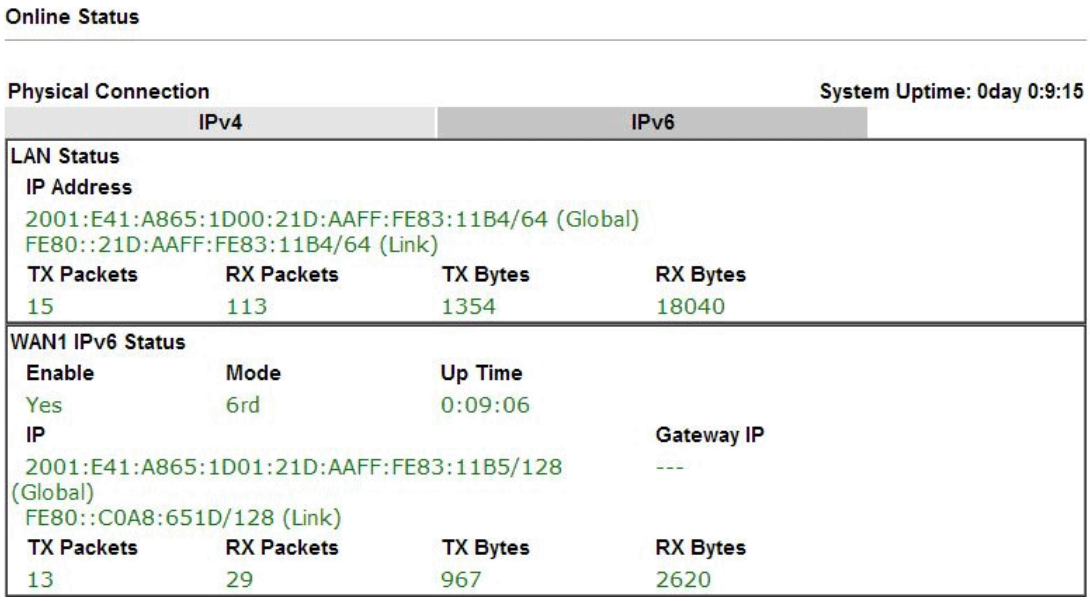


Available settings are explained as follows:

Item	Description
6rd Mode	**Auto 6rd –** Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". **Static 6rd -** Set 6rd options manually.
IPv4 Border Relay	Enter the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.
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 Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **NS Detect, Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

After finished the above settings, click **OK** to save the settings.

Below shows an example for successful IPv6 connection based on 6rd mode.



II-2-3 Multi-PVC/VLAN

Multi-VLAN allows users to create profiles for specific WAN interface and bridge connections for user applications that require very high network throughput. Simply go to **WAN** and select **Multi-VLAN**.

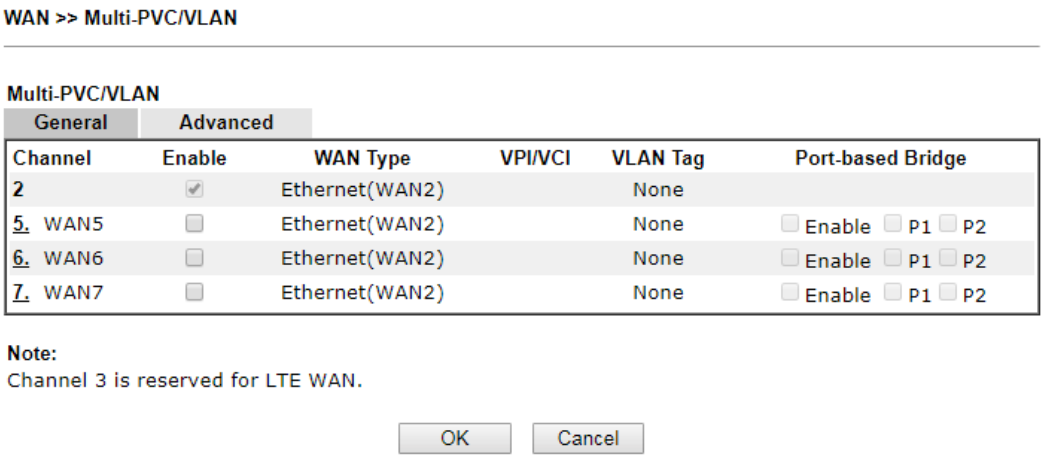
Channel 2 has the following fixed assignment and cannot be altered.

- Channel 2: Ethernet on WAN2 (based on the model)

Channels 5 through **7** can be configured as virtual WANs (WAN5 through WAN7).

General

This page shows the basic configurations used by every channel.

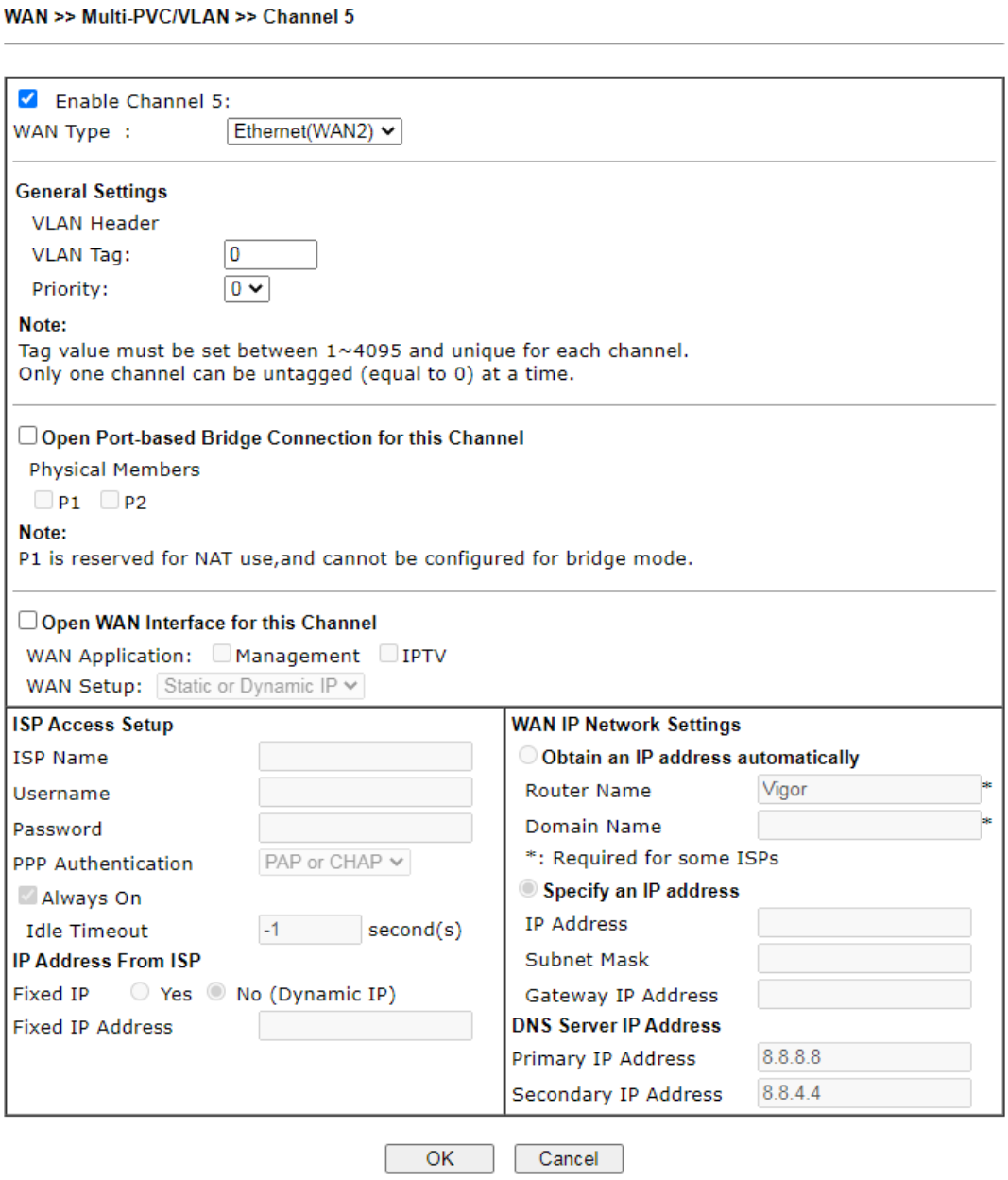


Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 2 is used by the Internet Access web user interface and can not be configured here. Channels 5 ~ 7 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.
Port-based Bridge	The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. **Enable** - Check this box to enable the port-based bridge function on this channel. **P1 ~ P2** – Check the box(es) to build bridge connection on LAN.

To configure a PVC channel, click its channel number.

WAN links for Channel 5, 6 and 7 are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 5, 6 and 7 to configure your router.



Available settings are explained as follows:

Item	Description
Enable Channel 4/5/6	**Enable –** Select to enable this channel. **Disable –** Select to disable this channel.
General Settings	**VLAN Tag –** Enter the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. **Priority –** Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
Open Port-based Bridge	The settings here will create a bridge between the LAN ports

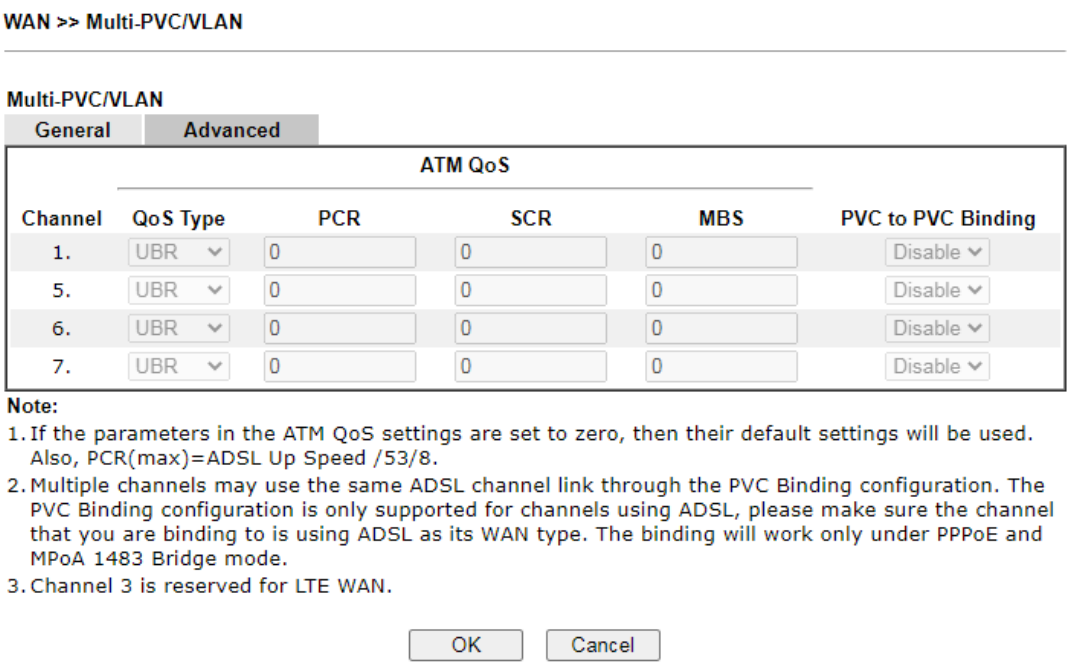
Connection for this Channel	selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured. **Physical Members –** Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection. **Note:** LAN port P1 is reserved for NAT use and cannot be selected for bridging.
Open WAN Interface for this Channel	Check the box to enable relating function. **WAN Application** ● **Management** can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069. ● **IPTV** - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers. **WAN Setup -** Choose **PPPoE/PPPoA** or **Static or Dynamic IP** to determine what WAN settings must be configured.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. **ISP Name** – PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank. **Username** – Name provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters. **Password** – Password provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters. **PPP Authentication** –The protocol used for PPP authentication. ● **PAP only**- Only PAP (Password Authentication Protocol) is used. ● **PAP or CHAP**- Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. **Always On** – If selected, the router will maintain the PPPoE/PPPoA connection. **Idle Timeout** – Maximum length of time, in seconds, of idling allowed (no traffic) before the connection is dropped. **IP Address From ISP** - Specifies how the WAN IP address of the channel configured. ● **Fixed IP** **Yes** - IP address entered in the Fixed IP Address field will be used as the IP address of the virtual WAN. **No** - Virtual WAN IP address will be assigned by the ISP's PPPoE/PPPoA server.
WAN IP Network Settings	**Obtain an IP address automatically** – Select this option if the router is to receive IP configuration information from a DHCP server. ● **Router Name** – Sets the value of DHCP Option 12, which is used by some ISPs. ● **Domain Name** – Sets the value of DHCP Option 15,

	which is used by some ISPs. **Specify an IP address** – Select this option to manually enter the IP address. ● **IP Address** – Type in the IP address. ● **Subnet Mask** – Type in the subnet mask. ● **Gateway IP Address** – Type in gateway IP address. **DNS Server IP Address -** Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

After finished the above settings, click **OK** to save the settings and return to previous page.

Advanced

Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information.



Available settings are explained as follows:

Item	Description
QoS Type	Select a proper QoS type for the channel according to the information that your ISP provides.
PCR	It represents Peak Cell Rate. The default setting is “0”.
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.
PVC to PVC Binding	It allows the enabled PVC channel to use the same ADSL connection settings of another PVC channel. Please choose the PVC channel via the drop down list.

After finished the above settings, click **OK** to save the settings.

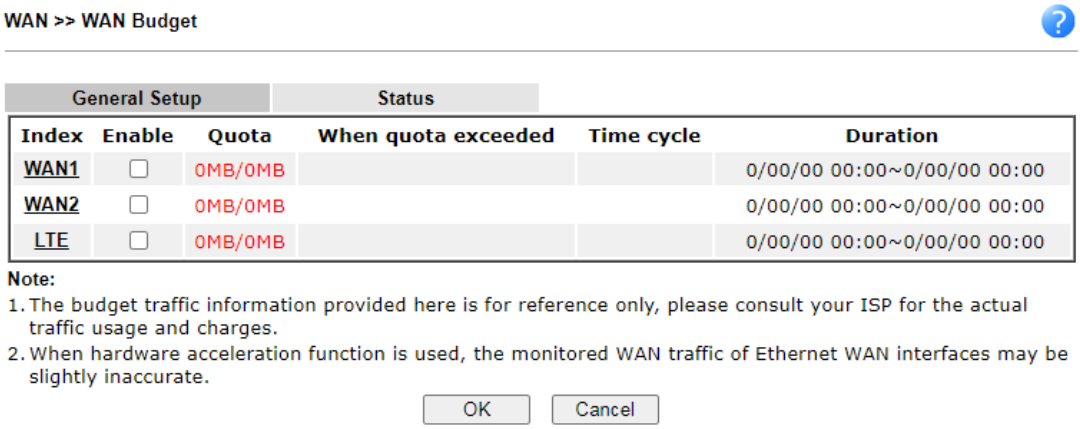
II-2-4 WAN Budget

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

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

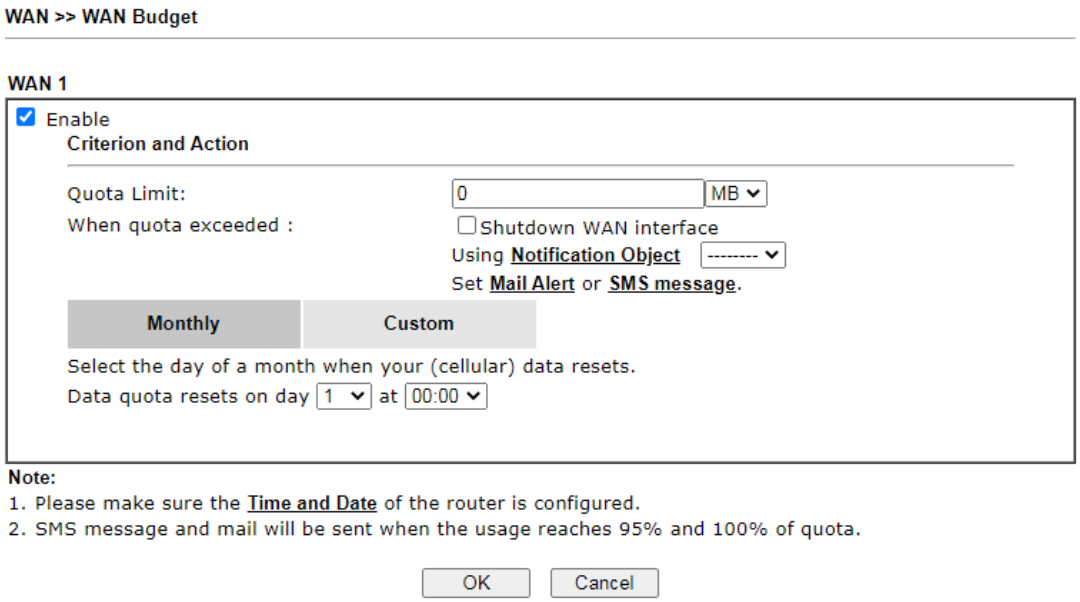
- set up calendar cycles to monitor;
- limit your Internet usage according to your ISP's quota;
- set up action(s) to take when the quota is exceeded.

II-2-4-1 General Setup



Item	Description
Index	The WAN port. Click to configure WAN Budget for a particular WAN.
Enable	**v -** WAN Budget is enabled on this WAN. **x -** WAN Budget is disabled on this WAN.
Quota	The current cycle's Internet usage is expressed as *x/y* where *x* is the cumulative usage and *y* is the upper limit. For example, 100MB/200MB means the usage thus far in this cycle is 100MB, and the upper limit is 200MB.
When quota exceeded	Actions to be taken once the quota is reached. **Shutdown** – WAN will be disabled. **Mail Alert** – Email will be sent to the administrator.
Time cycle	Reset frequency of the usage data. **Monthly** – The Monthly option in the **Criterion and Action** tab was used to set up the usage quota. **User Define**d: The User Defined option in the **Criterion and Action** tab was used to set up the usage qota.
Duration	Start and end timestamps of the current cycle.

Click WAN1 (to WAN6) link to open the following web page.

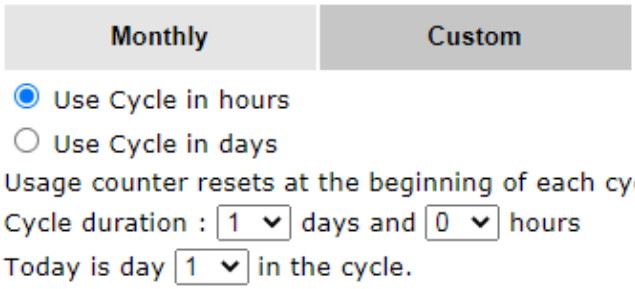


Available settings are explained as follows:

Item	Description
Enable	When selected, WAN Budget is enabled for this WAN.
Quota Limit	Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify.
When quota exceeded	Check the box(es) as the condition(s) for the system to perform when the traffic has exceeded the budget limit. **Shutdown WAN interface** – All the outgoing traffic through such WAN interface will be terminated. ● **Using Notification Object** – The system will send out a notification based on the content of the notification object. ● **Set Mail Alert** – The system will send out a warning message to the administrator when the quota is running out. However, the connection charges will be calculated continuously. ● **Set SMS message** - The system will send out SMS message to the administrator when the quota is running out.
Monthly	Some ISP might apply for the network limitation based on the traffic limit per month. This setting is to offer a mechanism of resetting the traffic record every month. Monthly Custom Select the day of a month when your (cellular) data resets. Data quota resets on day 1 at 00:00 **Data quota resets on day ...** – You can determine the starting day in one month.
Custom	This setting allows the user to define the billing cycle according to his request. The WAN budget will be reset with an interval of billing cycle. Monthly is default setting. If long period or a short period is required, use **Custom**. The period of cycle duration is between 1 day and 60 days. You can determine the cycle

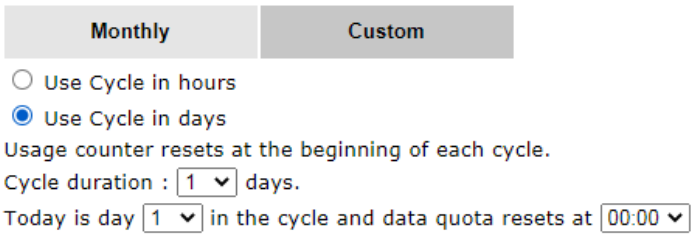
duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.

Use Cycle in hours –



- **Cycle duration**: Specify the days and hours to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically.
- **Today is day** – Specify the day in the cycle as the starting point which Vigor router will reset the traffic record. For example, "3" means the third day of the cycle duration.

Use Cycle in days -

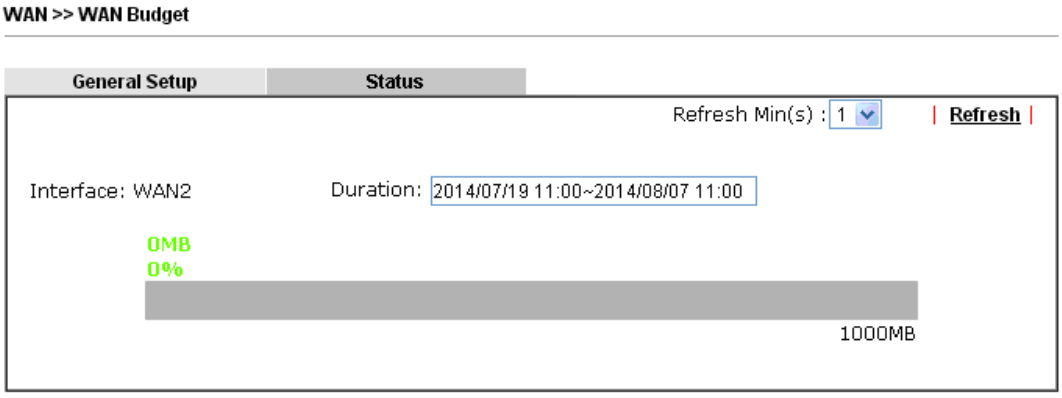


- **Cycle duration**: Specify the days to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically.
- **Today is day** – Specify the day and time for data quota rest in the cycle as the starting point which Vigor router will reset the traffic record. For example, "3" means the third day of the cycle duration.

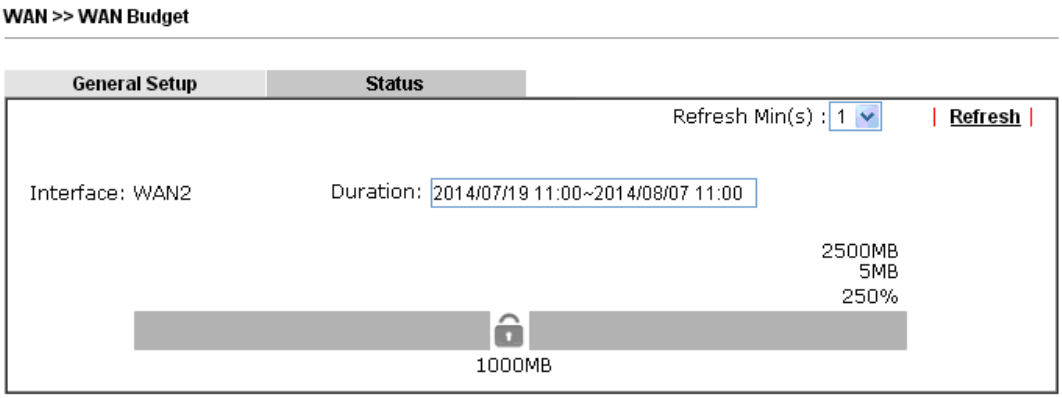
After finished the above settings, click **OK** to save the settings.

II-2-4-2 Status

The status page displays the status WAN budget, including the duration and the usage.



If the WAN budget is exhausted, a lock will be displayed on the page if **Shutdown WAN interface** is selected. Which means no data transmission will be carried out. Moreover, the system will send out a warning message to the administrator if **Mail Alert** is selected**.** Or, the system will send out SMS message to the administrator if **SMS message** is selected.

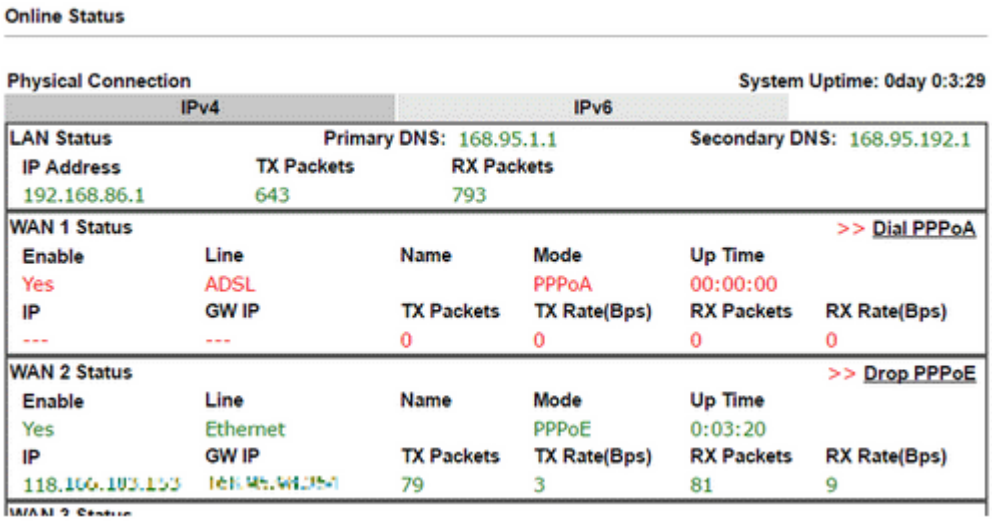


Application Notes

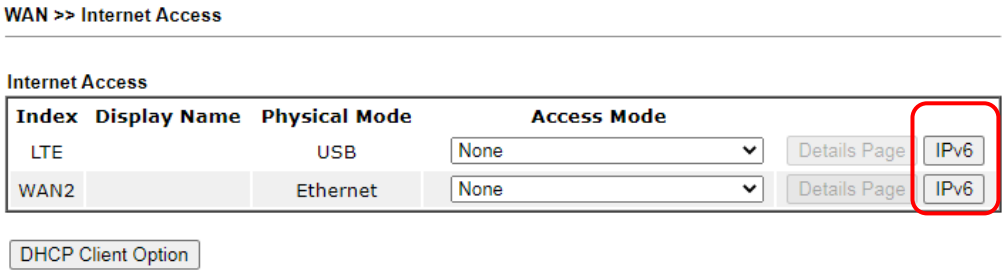
A-1 How to configure IPv6 on WAN interface?

This document is going to demonstrate how to implement an IPv6 address on Vigor Router's WAN.

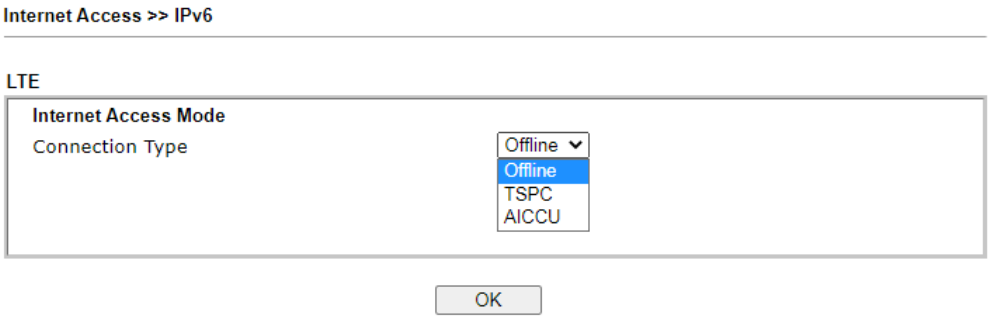
1. Before configuring IPv6 on WAN, please make sure the router is connected to the IPv4 Internet.



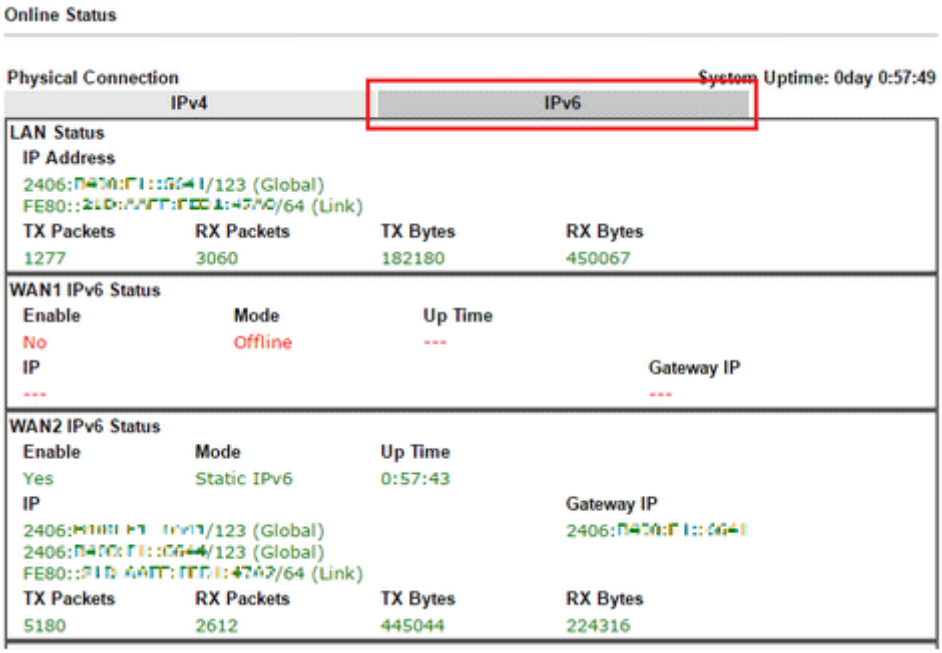
2. Go to **WAN >> Internet Access**, click on IPv6 of the WAN interface that you would like to configure an IPv6 address.



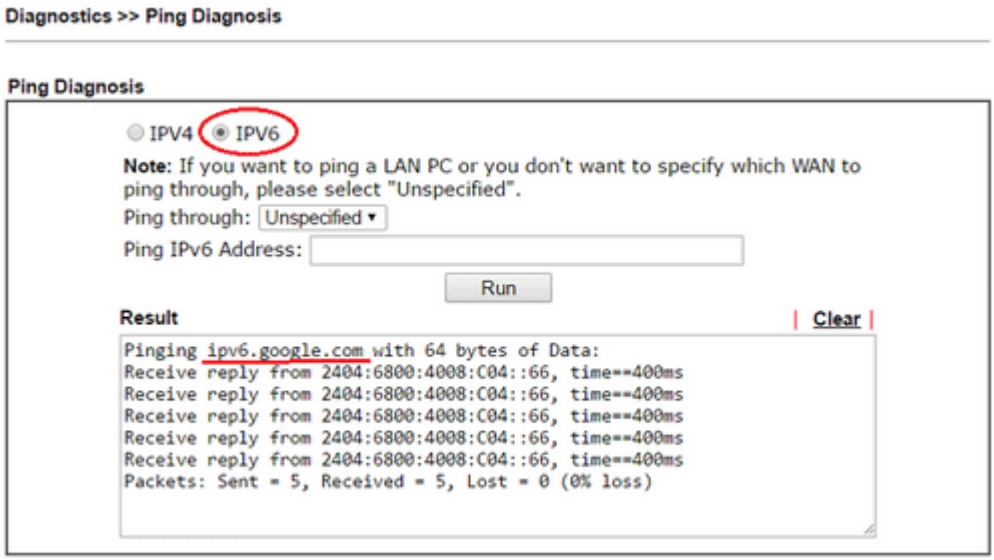
3. Select a **Connection Type** from the drop-down list, enter the required parameters. Then click **OK** and reboot the router to apply the settings.



4. After accomplishing the configurations, Network Administrator may check the status from the IPv6 tab on **Online Status >> Physical Connection** page.



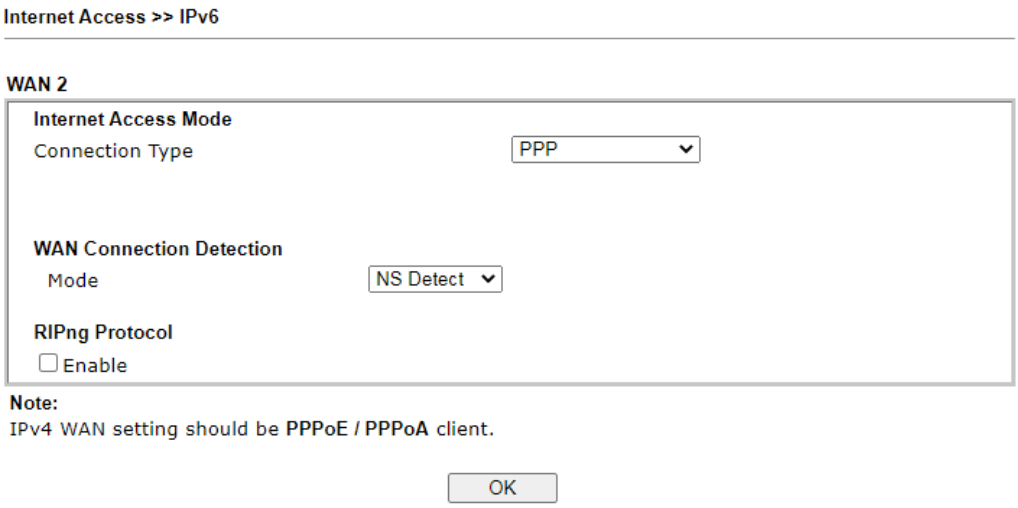
5. Furthermore, Network Administrator may test the connectivity of IPv6 from the router by going to **Diagnostics >> Ping Diagnosis** and selecting "IPv6".



Below we will provide some examples of configuring IPv6 with different connection types.

PPP (Point-to-Point Protocol)

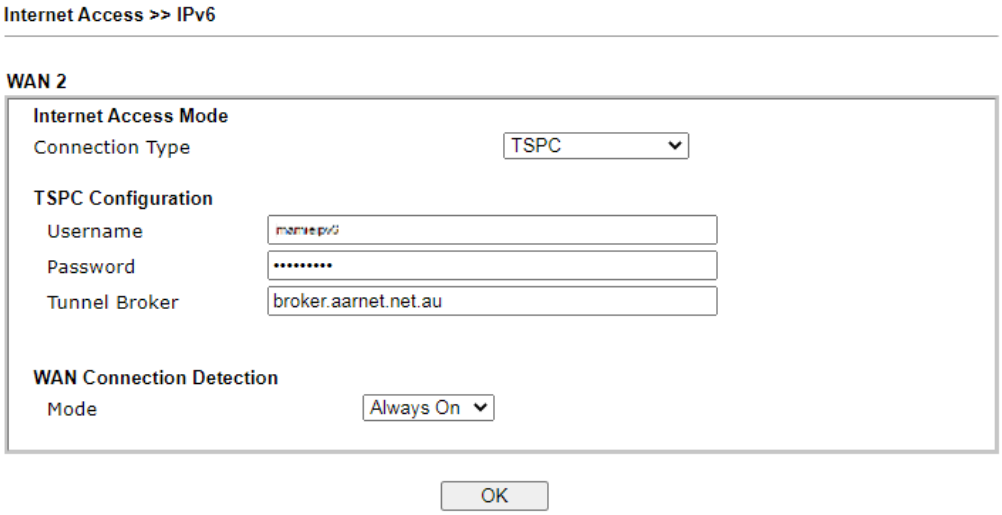
This applies if the IPv4 access mode is PPPoE, and the IPv4 ISP also provides an IPv6 address. To use IPv6 PPP, you just need to choose the **Connection Type** to "PPP", no other setting is required.



TSPC (Tunnel Setup Protocol Client)

In this mode, the IPv6 connectivity is provided by a tunnel broker on the IPv4 Internet through a tunnel set up by Tunnel Setup Protocol (TSP). To use TSPC, you'll need to sign up for a tunnel broker service and get a username and password first, then, configure the router as follows:

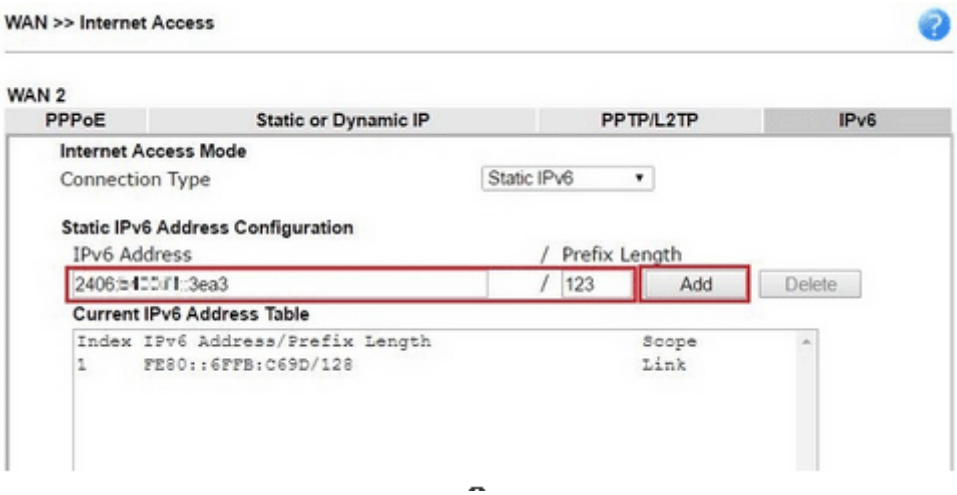
1. Set Connection Type to TSPC.
2. Enter the Username and Password registered at the TSP server.
3. Enter the IP or Domain Name of the TSPC server for **Tunnel Broker**.



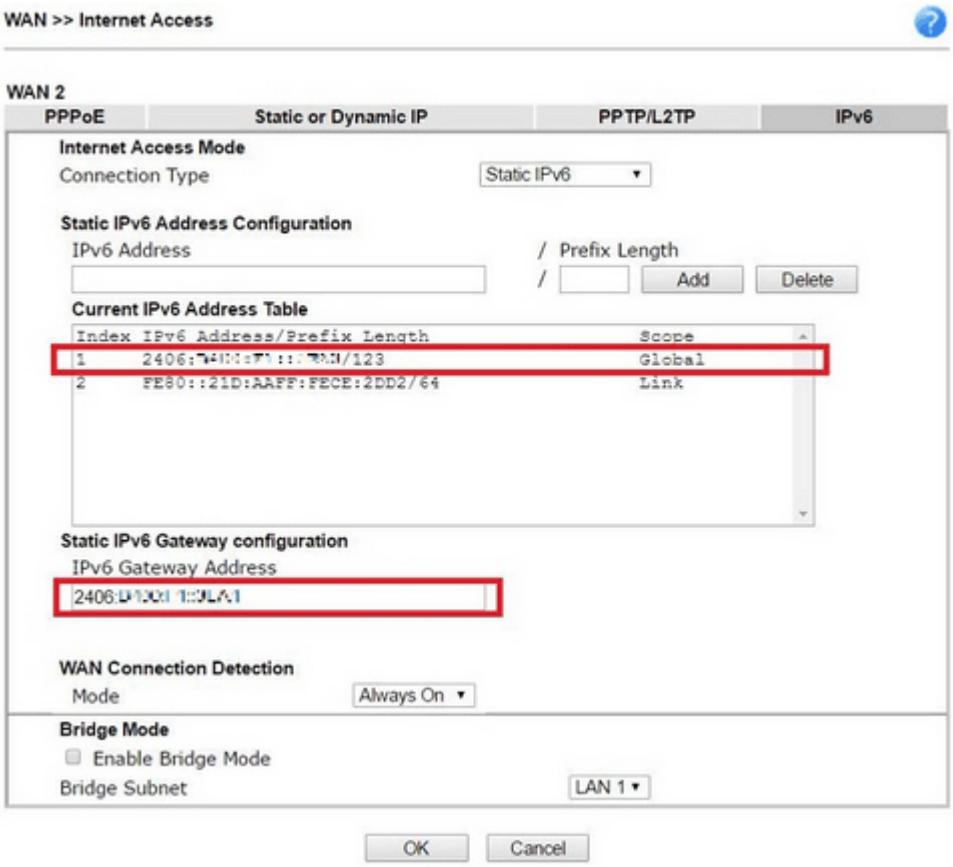
Static IPv6

If your ISP provides a static IPv6 address for you, you may configure that IPv6 address for WAN by doing the following steps:

1. Set **Connection Type** to Static IPv6.
2. Enter the IPv6 address and Prefix Length which provided by the ISP, and click **Add**.



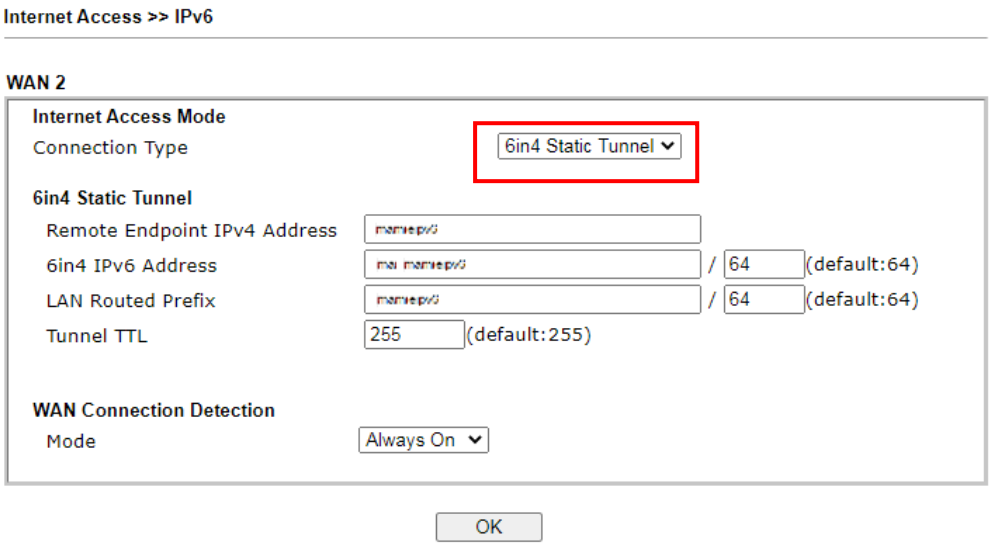
3. You should see the IPv6 address in **Current IPv6 Address Table**. Then, specify the IP address of IPv6 Gateway.



6in4 Static Tunnel

In this mode, the IPv6 connectivity is provided by a tunnel broker on the IPv4 Internet through a tunnel configured manually. To use 6in4 Static Tunnel, you need sign up for a tunnel broker service and get an IPv6 address and routed IPv6 prefixes first. Then, configure the router as follows:

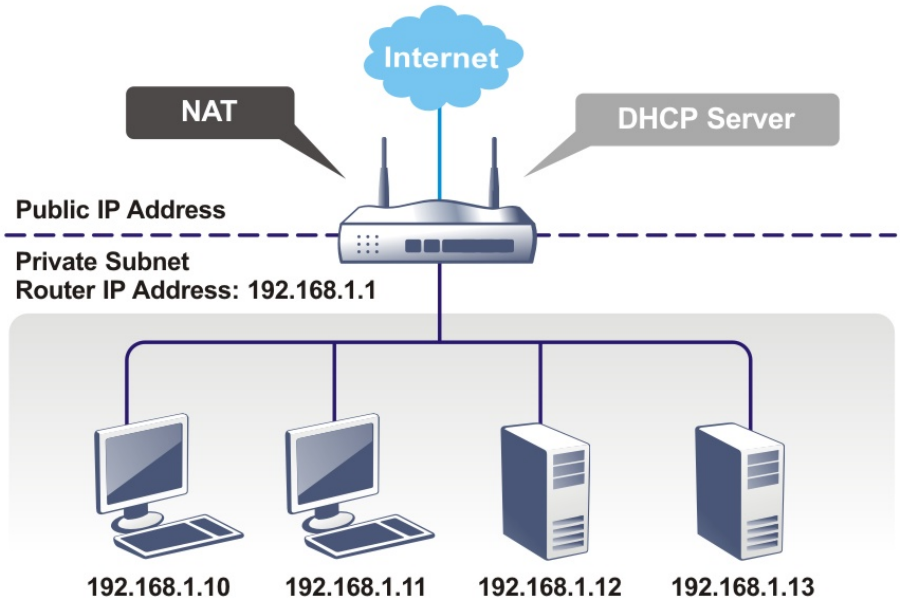
1. Set Connection Type to 6in4 Static Tunnel.
2. Enter the tunnel server's IPv4 address in Remote Endpoint IPv4 Address.
3. Enter the router's IPv6 address in 6in4 IPv6 Address.
4. Enter the routed IPv6 prefix in LAN Routed Prefix.



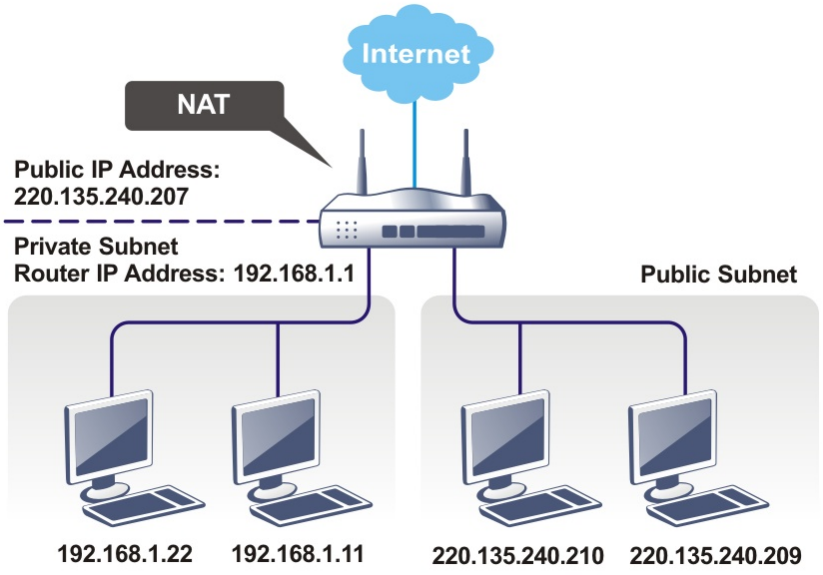
II-3 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



What is Routing Information Protocol (RIP)

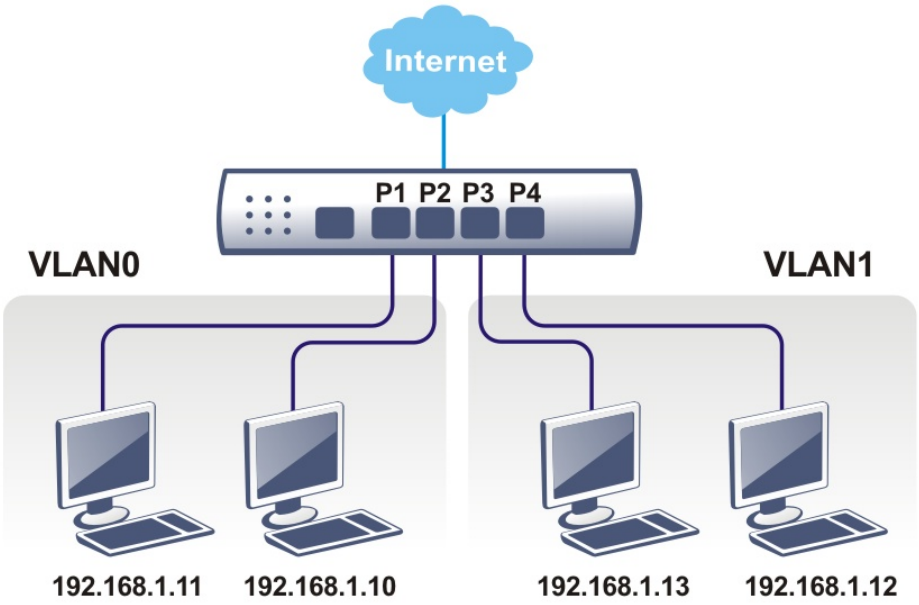
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 8 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.

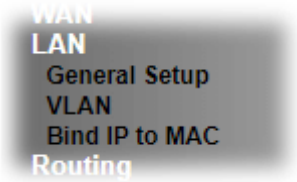


Web User Interface

A LAN 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.

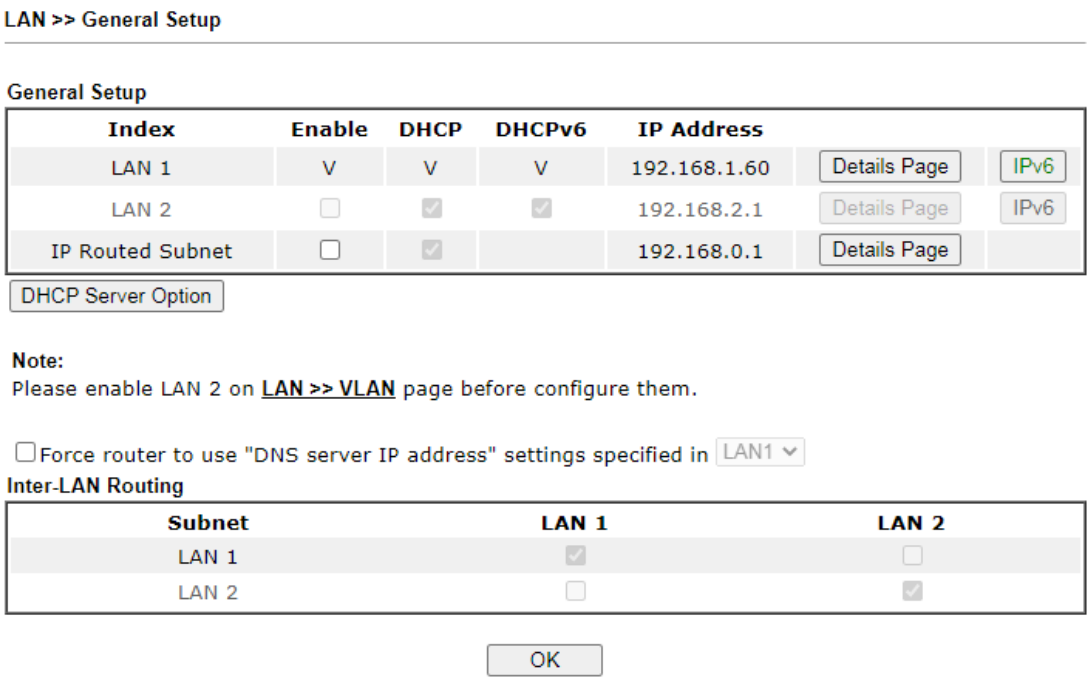
To communicate with the hosts outside of the LAN, LAN clients have to go through a network gateway, which in most cases is a router that sits between the LAN and the ISP network, which is the WAN. The router acts as a director to ensure traffic between the LAN and the WAN reach their intended destinations.



II-3-1 General Setup

This page provides you the general settings for LAN. Click **LAN** to open the LAN settings page and choose **General Setup**.

There are four subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN2). In addition, different subnets can link for each other by configuring **Inter-LAN Routing**. At present, LAN1 setting is fixed with NAT mode only. LAN2 – LAN4 can be operated under **NAT** or **Route** mode. IP Routed Subnet can be operated under Route mode.



Available settings are explained as follows:

Item	Description
General Setup	Allow to configure settings for each subnet respectively. **Index -** Display all of the LAN items. **Enable-** Basically, LAN1 status is enabled in default. LAN2 and IP Routed Subnet can be observed by checking the Enable box. **DHCPv6-** LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN. **IP Address -** Display the IP address for each LAN item. Such information is set in default and you can not modify it. **Details Page -** Click it to access into the setting page. Each LAN will have different LAN configuration page. **Each LAN must be configured in different subnet.** **IPv6 –** Click it to access into the settings page of IPv6.
DHCP Server Option	DHCP packets can be processed by adding option number and data information when such function is enabled. For detailed information, refer to later section.
Force router to use "DNS server IP address" …..	Force Vigor router to use DNS servers configured in LAN1/LAN2 instead of DNS servers given by the Internet Access server (PPPoE, PPTP or DHCP server).
Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN). Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. Refer to section II-2-2 VLAN on how to set up VLANs. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

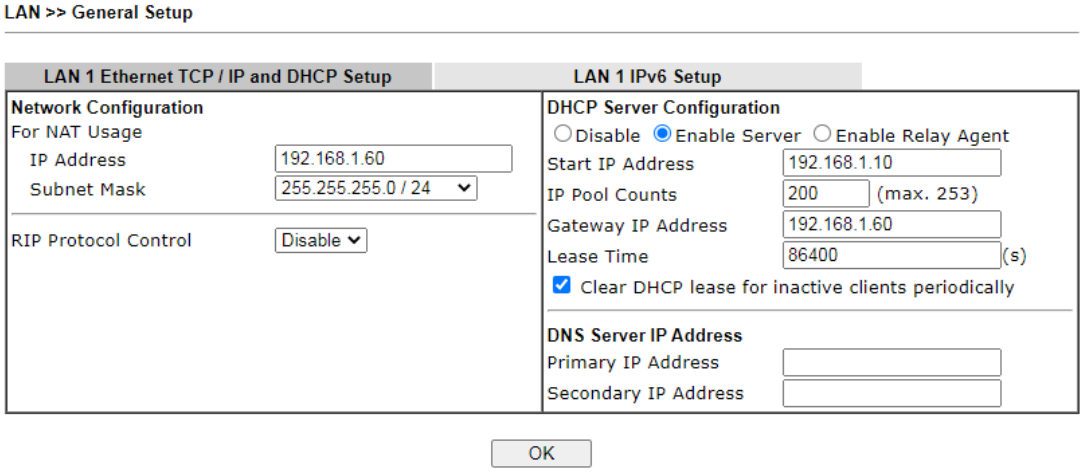
When you finish the configuration, please click **OK** to save and exit this page.

Info

To configure a subnet, select its Detials Page button to bring up the LAN **Details Page**.

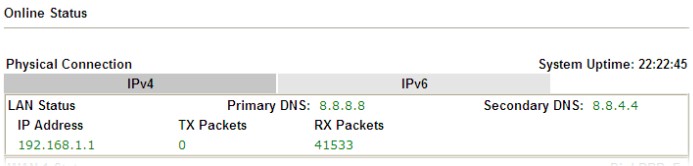
II-3-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information.



Available settings are explained as follows:

Item	Description
Network Configuration	**For NAT Usage,** **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24). **RIP Protocol Control,** **Enable -** When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
DHCP Server Configuration	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. **Disable -** Let you manually assign IP address to every host in the LAN. **Enable Server -** Let the router assign IP address to every host in the LAN. ● **Start IP Address -** The beginning LAN IP address that is given out to LAN DHCP clients. ● **IP Pool Counts -** The maximum number of IP addresses to be handed out by DHCP. The default value is 200.

	Valid range is between 1 and 253. The actual number of IP addresses available for assignment is the IP Pool Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller. ● **Gateway IP Address -** The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **Network Configuration** section above. ● **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. ● **Clear DHCP lease for inactive clients periodically -** If selected, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool. **Note**: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following: ■ Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30 ■ Clear DHCP lease when the client is not responding ARP replies. **Enable Relay Agent –** 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. ● **DHCP Server IP Address –** It is available when **Enable Relay Agent** is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
DNS Server IP Address	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. **Primary 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 IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. The default DNS Server IP address can be found via Online Status:  If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable)

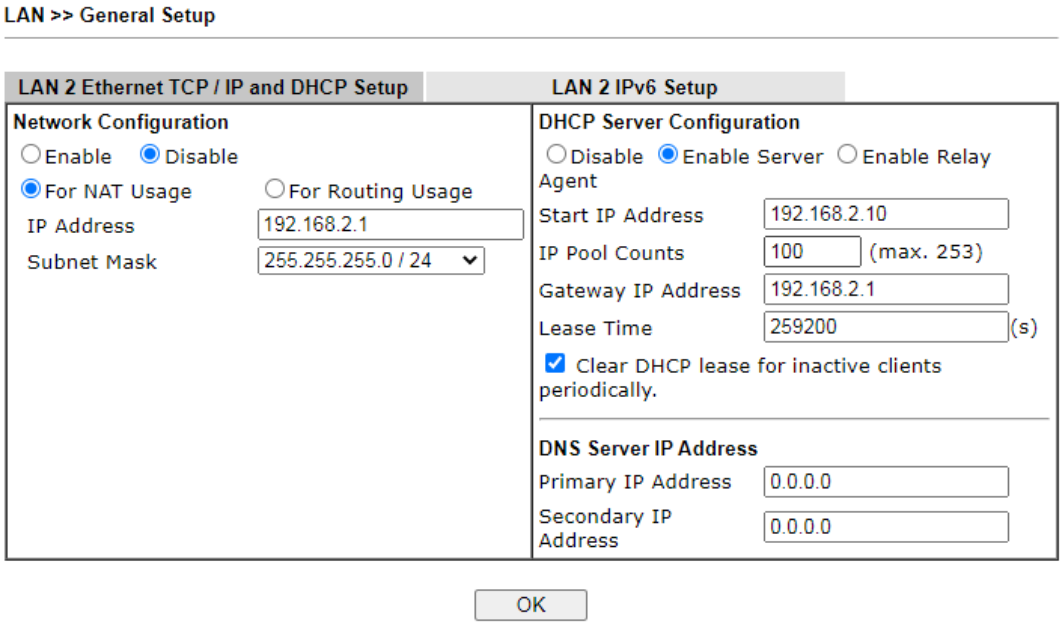
	connection.

When you finish the configuration, please click **OK** to save and exit this page.

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.

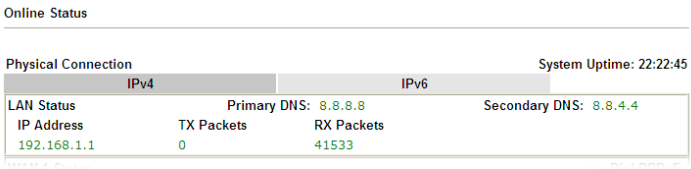
II-3-1-2 Details Page for LAN2



Available settings are explained as follows:

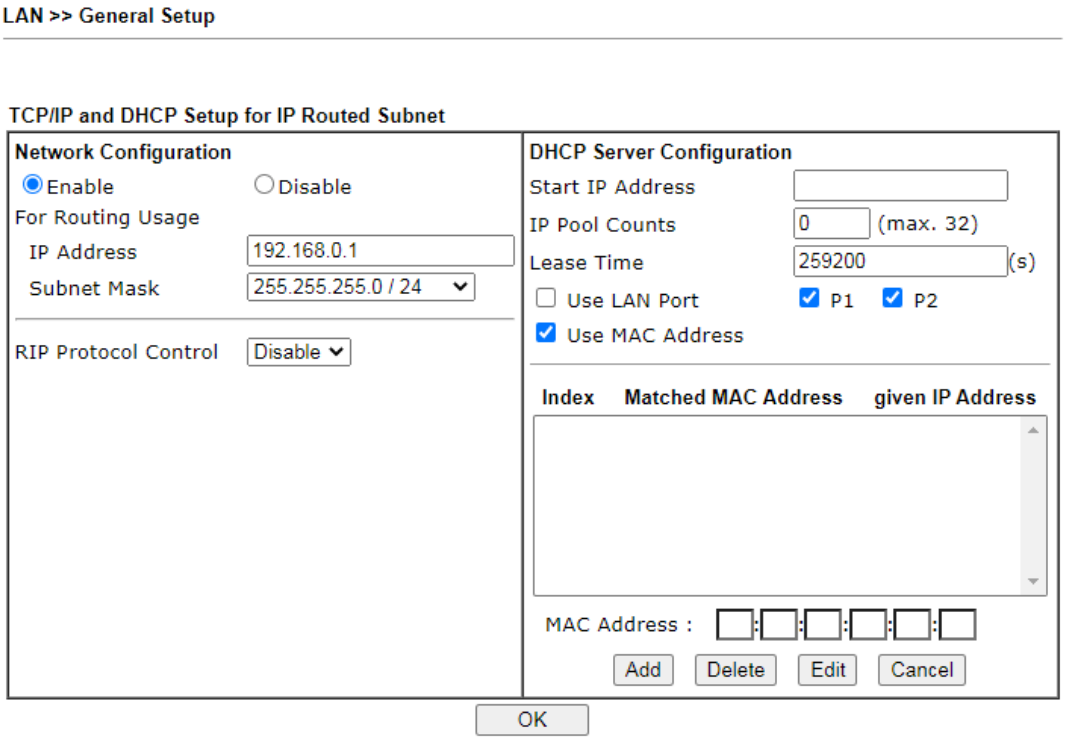
Item	Description
Network Configuration	**Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration. **For NAT Usage -** Click this radio button to invoke NAT function. **For Routing Usage -** Click this radio button to invoke this function. **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch 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. **Disable Server –** Let you manually assign IP address to every host in the LAN. **Enable Server -** Let the router assign IP address to every host in the LAN. ● **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. The actual number of IP addresses available for assignment is the IP Pool Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller. ● **Gateway IP Address -** The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **Network Configuration** section above. ● **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. ● **Clear DHCP lease for inactive clients periodically -** If selected, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool. **Note**: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following: ■ Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30 ■ Clear DHCP lease when the client is not responding ARP replies. **Enable Relay Agent –** 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. ● **DHCP Server IP Address –** It is available when **Enable Relay Agent** is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
DNS Server IP Address	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. **Primary 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 IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. The default DNS Server IP address can be found via Online Status:

	 If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

When you finish the configuration, please click **OK** to save and exit this page.

II-3-1-3 Details Page for IP Routed Subnet



Available settings are explained as follows:

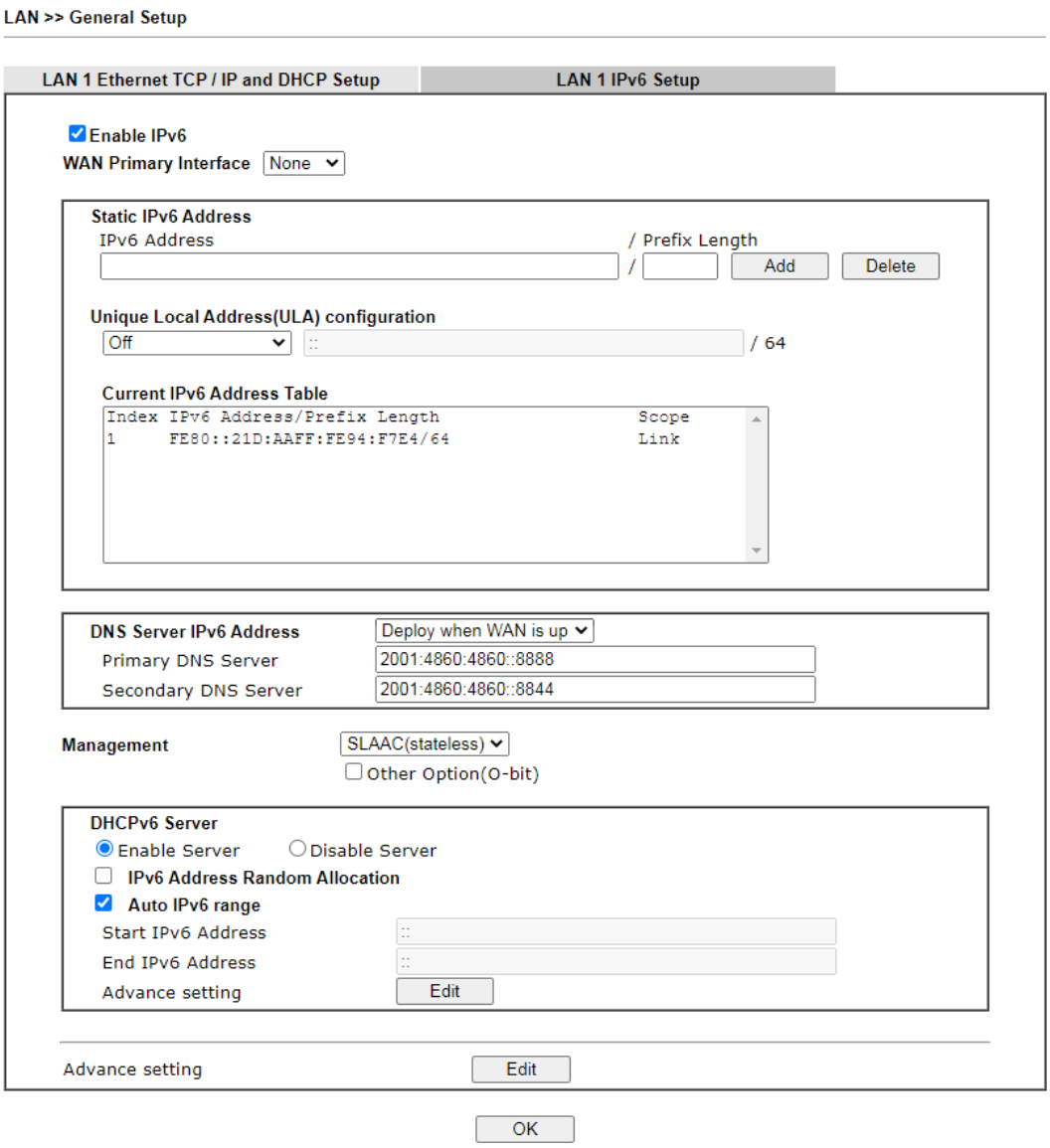
Item	Description
Network Configuration	**Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration. **For Routing Usage,** **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24). **RIP Protocol Control,** **Enable –** When Enabled, the router will attempt to exchange routing information with neighbouring routers using the

	Routing Information Protocol**.**
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch 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. **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. The actual number of IP addresses available for assignment is the IP Pool Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller. **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. **Use LAN Port –** Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2. **Use MAC Address -** Check such box to specify MAC address. ● **MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts which can be assigned, deleted or edited from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet. **Add –** Enter the MAC address in the boxes and click this button to add. **Delete** – Click it to delete the selected MAC address. **Edit** – Click it to edit the selected MAC address. **Cancel** – Click it to cancel the job of adding, deleting and editing.

When you finish the configuration, please click **OK** to save and exit this page.

II-3-1-4 Details Page for LAN IPv6 Setup

There are two configuration pages for each LAN. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.

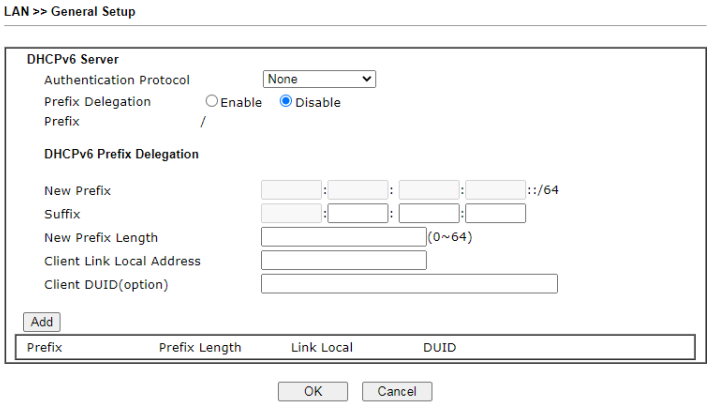


It provides 2 daemons for LAN side IPv6 address configuration. One is **SLAAC**(stateless) and the other is **DHCPv6** (Stateful) server.

Available settings are explained as follows:

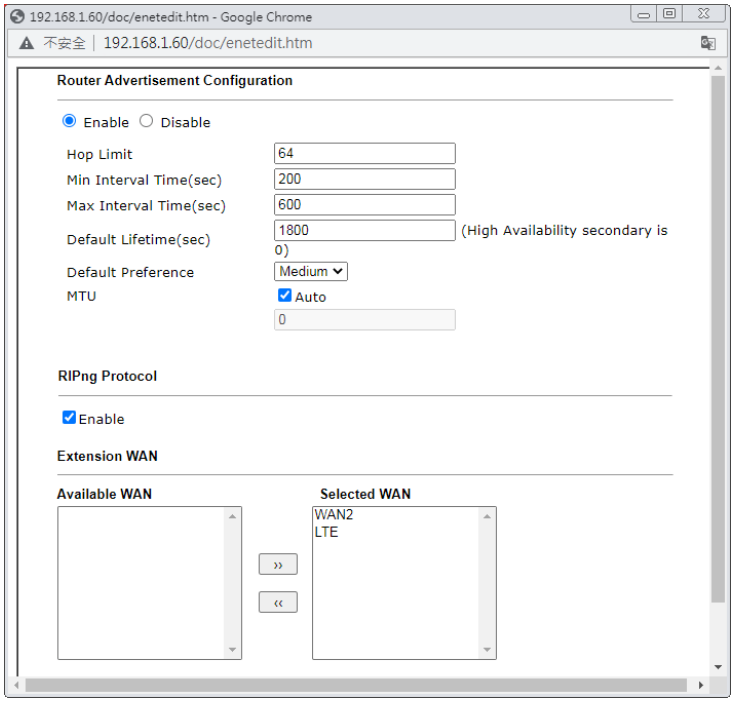
Item	Description
Enable IPv6	Check the box to enable the configuration of LAN 1 IPv6 Setup.
WAN Primary Interface	Use the drop down list to specify a WAN interface for IPv6.
Static IPv6 Address	**IPv6 Address** –Type static IPv6 address for LAN. **Prefix Length –** Enter the fixed value for prefix length. **Add –** Click it to add a new entry. **Delete –** Click it to remove an existed entry.
Unique Local Address (ULA) configuration	Unique Local Addresses (ULAs) are private IPv6 addresses assigned to LAN clients.

	Off - ULA is disabled. **Manually ULA Prefix -** LAN clients will be assigned ULAs generated based on the prefix manually entered. **Auto ULA Prefix -** LAN clients will be assigned ULAs using an automatically-determined prefix.
Current IPv6 Address Table	Display current used IPv6 addresses.
DNS Server IPv6 Address	**Deploy when WAN is up –** The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up. **Enable** – The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not. ● **Primary DNS Sever** – Enter the IPv6 address for Primary DNS server. ● **Secondary DNS Server** –Type another IPv6 address for DNS server if required. **Disable** – DNS server will not be used.
Management	Configures the Managed Address Configuration flag (M-bit) in Route Advertisements. ● **Off** - No configuration information is sent using Route Advertisements. ● **SLAAC(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 Vigor2860, or a separate DHCPv6 server.
Other Option(O-bit)	When selected, the **Other Configuration** flag is set, which indicates to LAN clients that IPv6 configuration information besides LAN IPv6 addresses is available from a DHCPv6 server. Setting the M-bit (see **Management** above) has the same effect as implicitly setting the O-bit, as DHCPv6 supplies all IPv6 configuration information, including what is indicated as available when the O-bit is set.
DHCPv6 Server	**Enable Server** –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration. **Disable Server** –Click it to disable DHCPv6 server. **IPv6 Address Random Allocation** - **Auto IPv6 range –** After check the box, Vigor router will assign the IPv6 range automatically. **Start IPv6 Address** / **End IPv6 Address** –Enter the start and end address for IPv6 server. **Advance setting** – Click the Edit button to configure advanced IPv6 settings for DHCPv6 server.



Advance setting

The Advanced Settings page has additional settings for Router Advertisement and enabling multiple WANs for IPv6 traffic.



Router Advertisement Configuration – Click **Enable** to enable router advertisement server. 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.

Disable – Click it to disable router advertisement server.

Hop Limt – The value is required for the device behind the router when IPv6 is in use.

Min/Max Interval Time (sec) – It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets.

Default Lifetime (sec) -Within such period of time, VigorLTE 200 can be treated as the default gateway.

Default Preference – It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted.

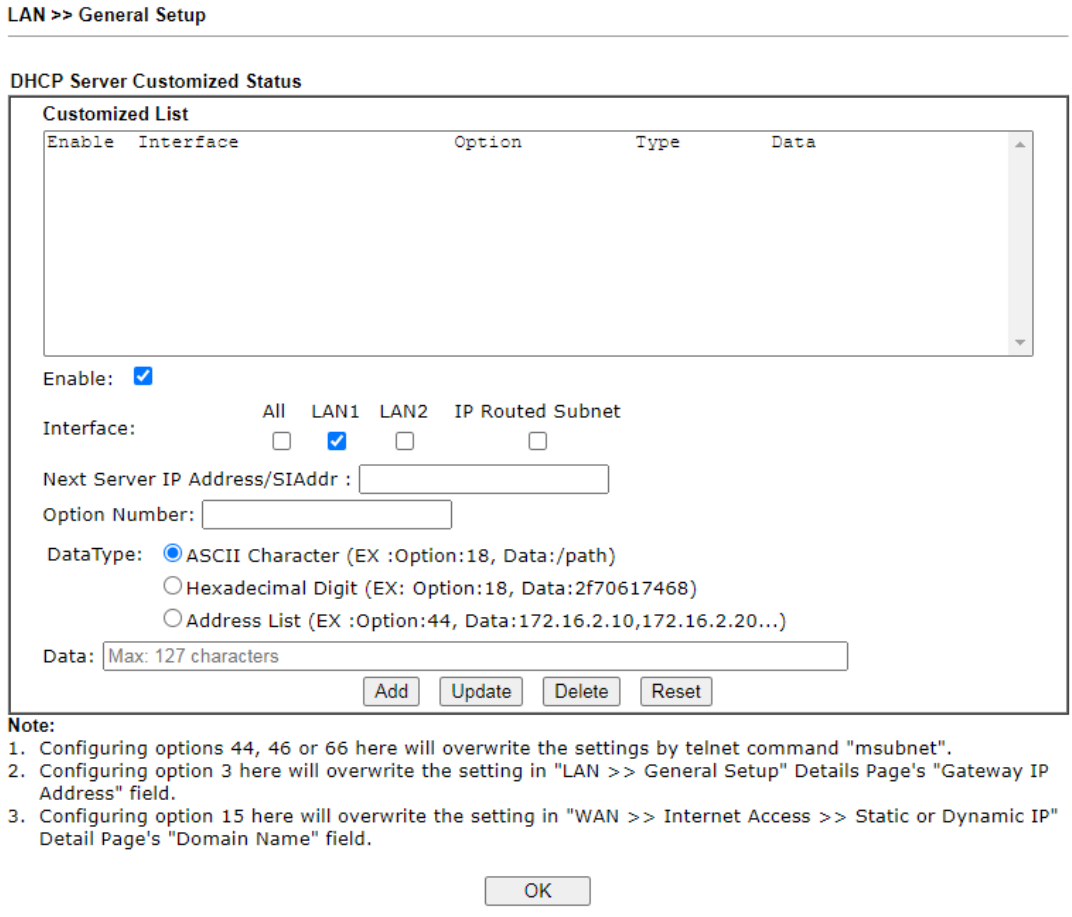
MTU – It means Max Transmit Unit for packet. If **Auto** is

	selected, the router will determine the MTU value for LAN. **RIPng Protocol -**RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2. **Extension WAN –** In addition to the default WAN used for IPv6 traffic specified in the WAN Primary Interface in the LAN IPv6 Setup page, additional WANs can be selected to carry IPv6 traffic by enabling them in the Extension WAN section. **Available WAN** – Additional WANs available but not currently selected to carry IPv6 traffic. **Selected WAN** – Additional WANs selected to carry IPv6 traffic.

After making changes on the Advance setting page, click the **OK** button to retain the changes and return to the LAN IPv6 Setup page. Be sure to click OK on the LAN IPv6 Setup page or else changes made on the Advance setting page will not be saved.

II-3-1-5 DHCP Server Options

DHCP Options can be configured by clicking the Advanced button on the LAN General Setup screen.



Available settings are explained as follows:

Item	Description
Customized List	Shows all the DHCP options that have been configured in the system.
Enable	If selected, DHCP option entry is enabled. If unselected, DHCP option entry is disabled.

Interface	LAN interface(s) to which this entry is applicable.
Next Server IP Address/SIAddr	Overrides the DHCP Next Server IP address (DHCP Option 66) supplied by the DHCP server.
Option Number	DHCP option number (e.g., 100).
DataType	Type of data in the Data field: **ASCII Character** - A text string. Example: /path. **Hexadecimal Digit -** A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468. **Address List -** One or more IPv4 addresses, delimited by commas.
Data	Data of this DHCP option.

To add a DHCP option entry from scratch, clear the data entry fields (**Enable, Interface, Option Number, DataType** and **Data**) by clicking Reset. After filling in the values, click **Add** to create the new entry.

To add a DHCP option entry modeled after an existing entry, click the model entry in **Customized List**. The data entry fields will be populated with values from the model entry. After making all necessary changes for the new entry, click **Add** to create it.

To modify an existing DHCP option entry, click on it in **Customized List**. The data entry fields will be populated with the current values from the entry. After making all necessary changes, click **Update** to save the changes.

To delete a DHCP option entry, click on it in **Customized List**, and then click **Delete**.

II-3-2 VLAN

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

Select **LAN>>VLAN** from the menu bar of the Web UI to bring up the VLAN Configuration page.

Tagged VLAN

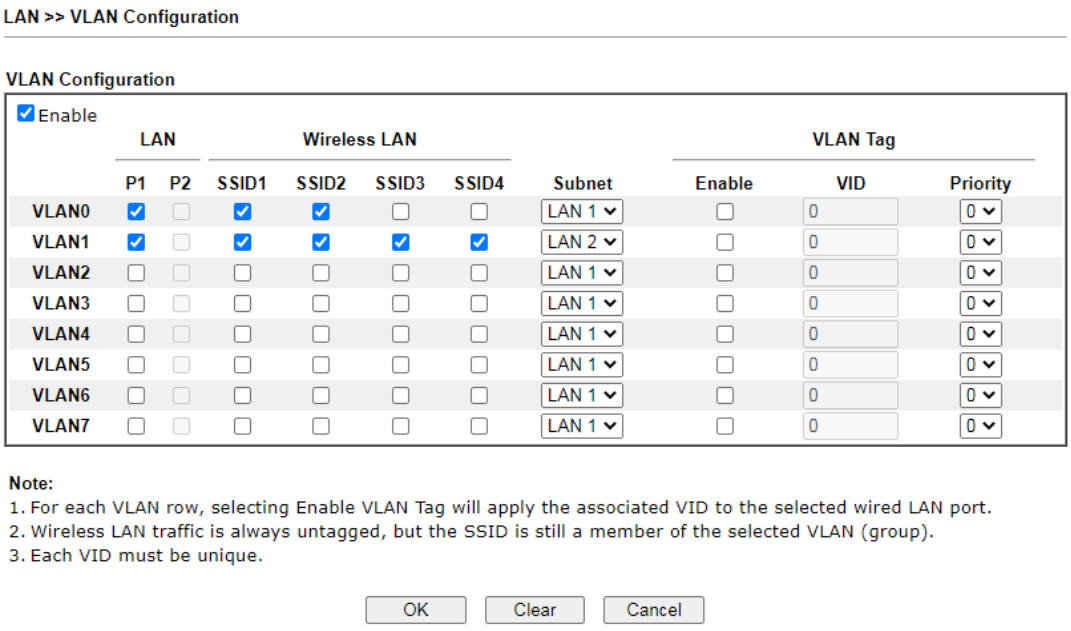
The tagged VLANs (802.1q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each of VLANs to each of the different IP subnets that the router may also be operating, to provide even more isolation. The said functionality is **tag-based multi-subnet**.

Port-Based VLAN

Relative to tag-based VLAN which groups clients with an identifier, port-based VLAN uses physical ports (P1 ~ P2) to separate the clients into different VLAN group.

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. The multi-subnet can let a small businesses have much better isolation for multi-occupancy applications. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

Below is an example page in VigorLTE 200Ln:



Info	Settings in this page only applied to LAN port but not WAN port.

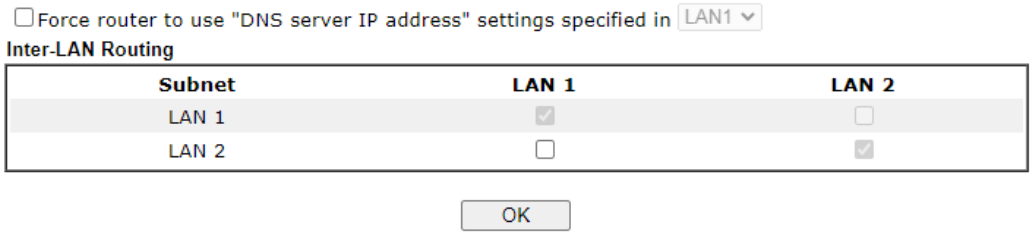
Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	**P1 - P2**- Check the LAN port(s) to group them under the selected VLAN.
Wireless LAN	**SSID1 - SSID4 -** Check the SSID boxes to group them under the selected VLAN.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet.
VLAN Tag	**Enable** – Check the box to enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the LAN while sending them out. Please Enter the tag value and specify the priority for the packets sending by LAN. **VID** – Enter the value as the VLAN ID number. The range is form 0 to 4095. VIDs must be unique. **Priority** – Valid values are from 0 to 7, where 1 has the lowest priority, followed by 0, and finally from 2 to 7 in increasing order of priority.

Info	Leave one VLAN untagged at least to prevent from not connecting to Vigor router due to unexpected error.

The Vigor router supports up to 8 VLANs. Each VLAN can be set up to use one or more of the Ethernet ports and wireless LAN Service Set Identifiers (SSIDs). Within the grid of VLANs (horizontal rows) and LAN interfaces (vertical columns),

- all hosts within the same VLAN (horizontal row) are visible to one another
- all hosts connected to the same LAN or WLAN interface (vertical column) are visible to one another if
  - they belong to the same VLAN, or
  - they belong to different VLANs, and inter-LAN routing (**LAN>>General Setup**) between them is enabled (see below).

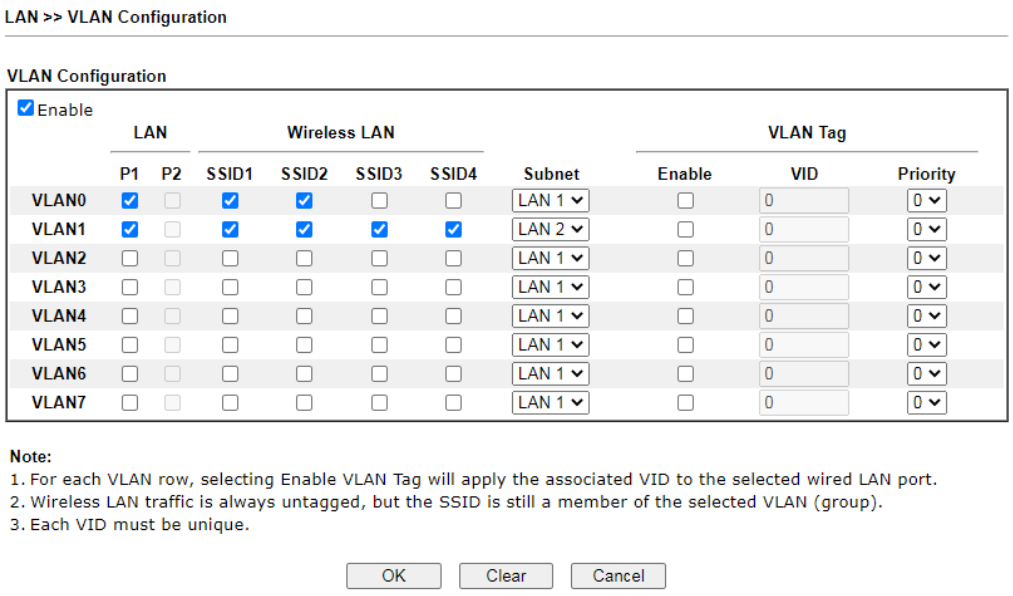


Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

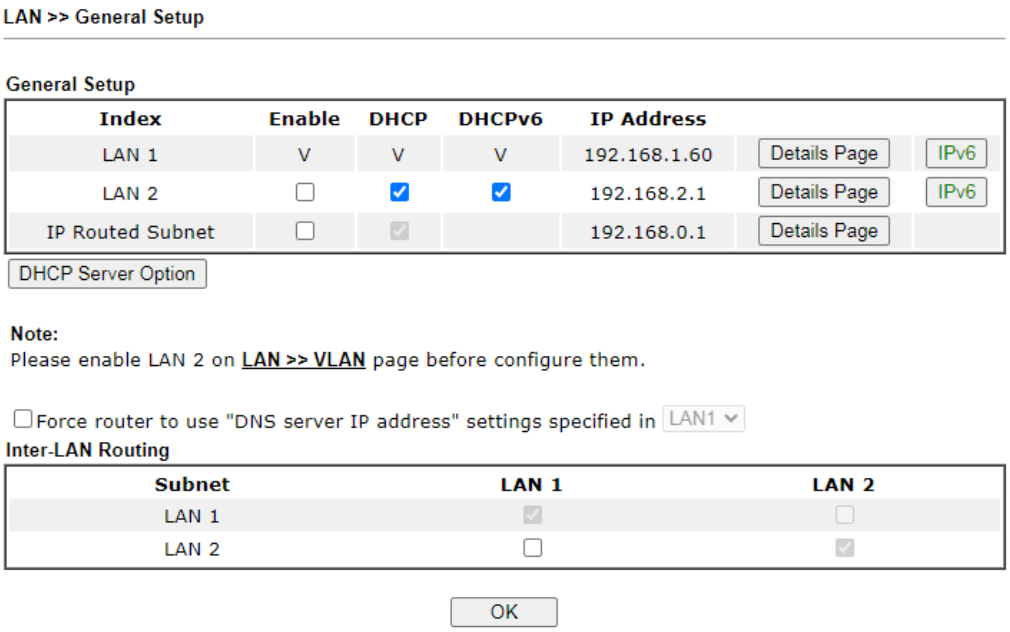
VigorLTE 200 series features a hugely flexible VLAN system. In its simplest form, each of the Gigabit LAN ports can be isolated from each other, for example to feed different companies or departments but keeping their local traffic completely separated.

Configuring port-based VLAN for wireless and non-wireless clients

1. All the wire network clients are categorized to group VLAN0 in subnet 192.168.1.0/24 (LAN1).
2. All the wireless network clients are categorized to group VLAN1 in subnet 192.168.2.0/24 (LAN2).
3. Open **LAN>>VLAN**. Check the boxes according to the statement in step 1 and Step 2.



4. Click **OK**.
5. Open **LAN>>General Setup**. If you want to let the clients in both groups communicate with each other, simply activate **Inter-LAN Routing** by checking the box between **LAN1** and **LAN2.**



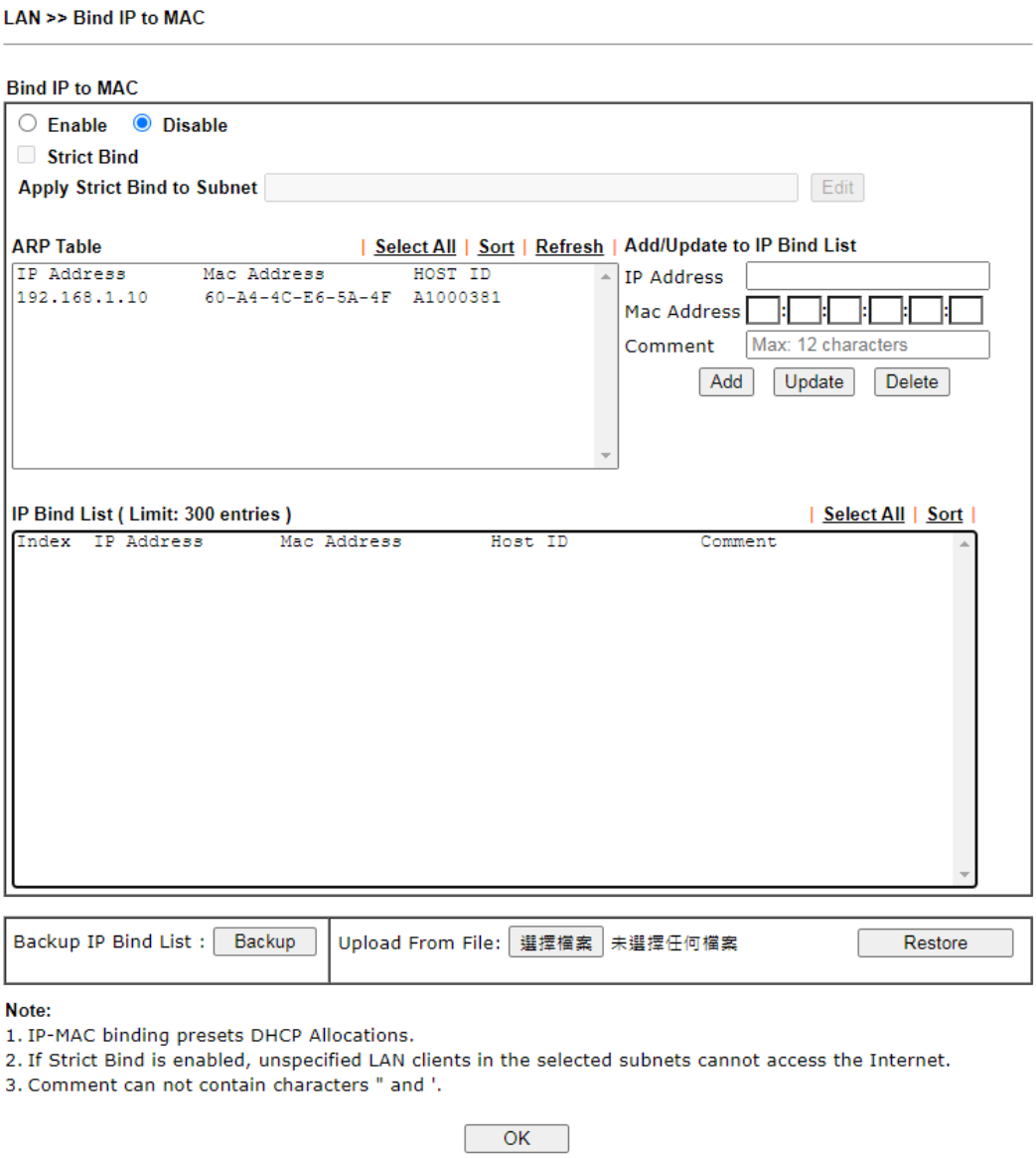
Vigor router supports up to six private IP subnets on LAN. Each can be independent (isolated) or common (able to communicate with each other). This is ideal for departmental or multi-occupancy applications.

Info	As for the VLAN applications, refer to "Appendix I: VLAN Application on Vigor Router" for more detailed information.

II-3-3 Bind IP to MAC

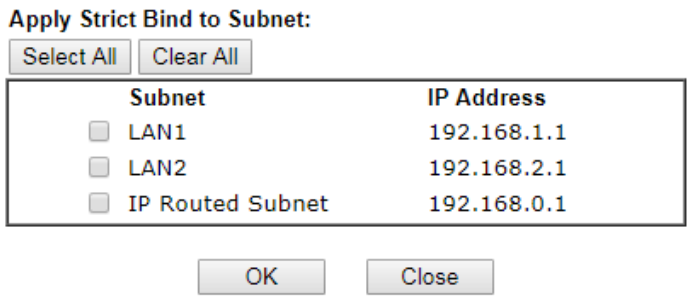
This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

Click **LAN** and click **Bind IP to MAC** to open the setup page.



Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Check the box to block the connection of the IP/MAC which is not listed in IP Bind List. LAN clients will be assigned IP addresses according to the MAC-to-IP address associations on this page. LAN client whose MAC address has not been bound to an IP address will be denied network access. **Note**: Before selecting **Strict Bind**, make sure at least one valid MAC address has been bound to an IP address. Otherwise no LAN clients will have network access, and it will not be possible to connect to the router to make changes to its configuration. **Apply Strict Bind to Subnet** – Choose the subnet(s) for

	applying the rules of Bind IP to MAC. 
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.
Select All	Select all entries in the ARP Table for manipulation.
Sort	Reorder the entry based on the IP address.
Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
Add / Update to IP Bind List	**IP Address** – Enter the IP address to be associated with a MAC address. **Mac Address** – Enter the MAC address of the LAN client's network interface. **Comment** – Type a brief description for the entry. **Add** - It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**. **Update** - It allows you to edit and modify the selected IP address and MAC address that you create before. **Delete** - You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Delete**. The selected item will be removed from the **IP Bind List**.
IP Bind List	It displays a list for the IP bind to MAC information.
Backup IP Bind List	Click **Backup** and enter a filename to back up IP Bind List to a file.
Upload From File	Click **Browse…** to select an IP Bind List backup file. Click **Restore** to restore the backup and overwrite the existing list.

Info	Before you select Strict Bind, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web user interface of the router might not be accessed.

When you finish the configuration, click **OK** to save the settings.

II-4 NAT

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.

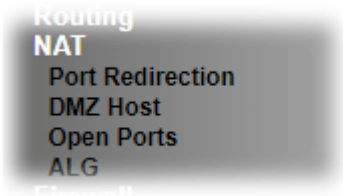
The benefit of the NAT includes:

- **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.

Info

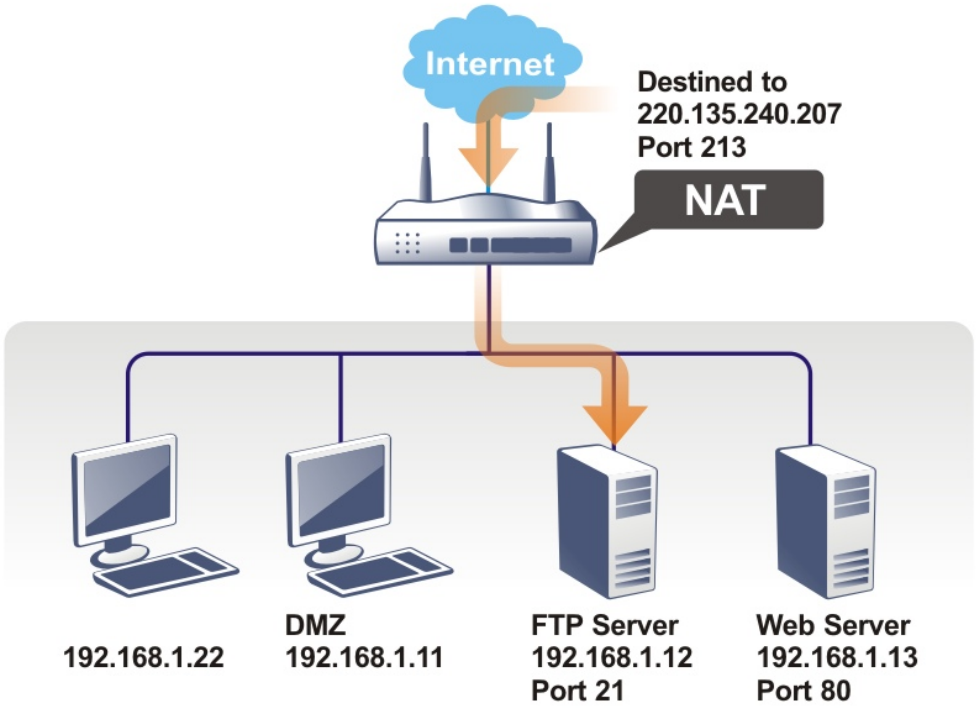
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

Web User Interface



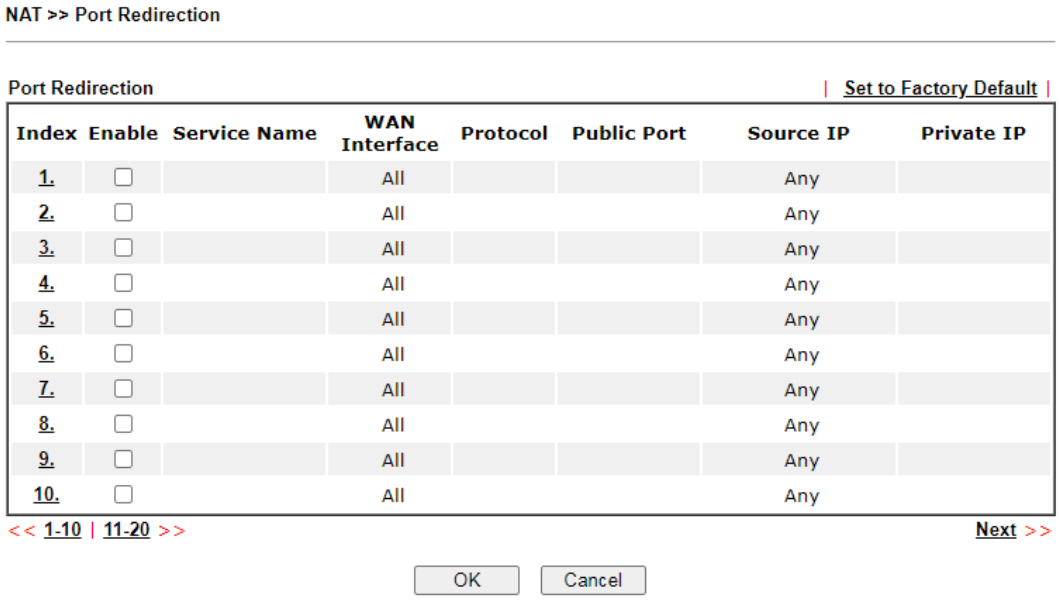
II-4-1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

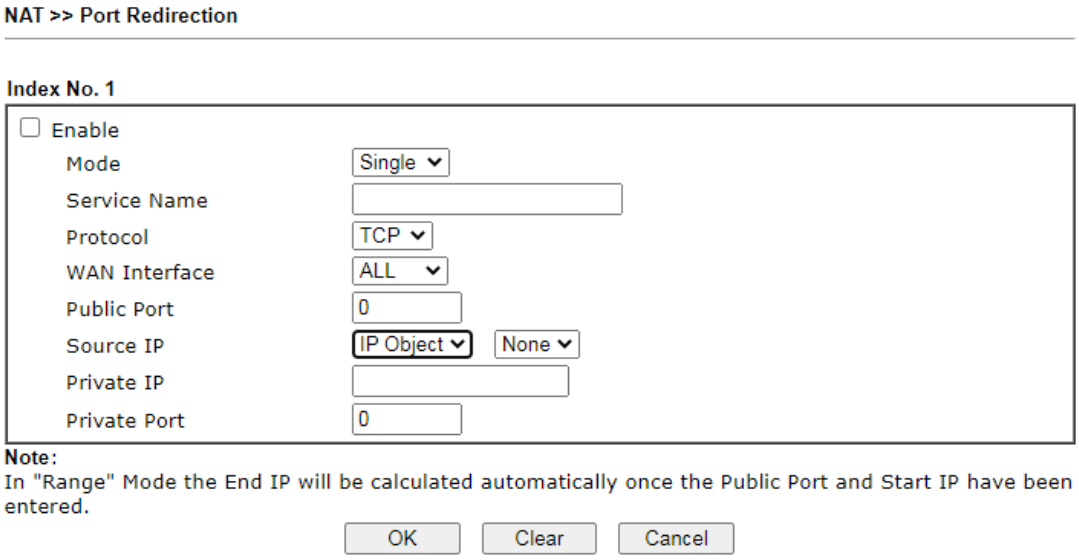
To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 40 port-mapping entries for the internal hosts.



Each item is explained as follows:

Item	Description
Index	Display the number of the profile.
Enable	Check the box to enable the profile.
Service Name	Display the description of the specific network service.
WAN Interface	Display the WAN IP address used by the profile.
Protocol	Display the transport layer protocol (TCP or UDP).
Public Port	Display the port number which will be redirected to the specified **Private IP and Port** of the internal host.
Source IP	Display the source IP address or object.
Private IP	Display the IP address of the internal host providing the service.

Press any number under Index to access into next page for configuring port redirection.



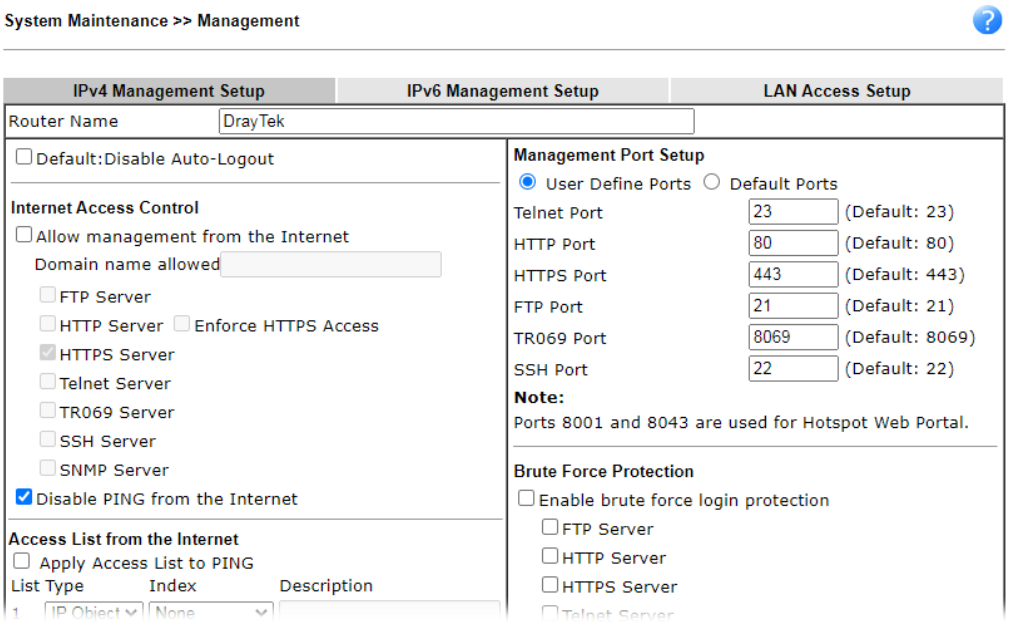
Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN Interface	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to all intefaces.
Public Port	Specify which port can be redirected to the specified **Private IP** and **Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Enter the required number on the first box (as the starting port) and the second box (as the ending port).
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
Private IP	Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point). The second one will be assigned automatically later.
Private Port	Specify the private port number of the service offered by the internal host.

After finishing all the settings here, please click **OK** to save the configuration.

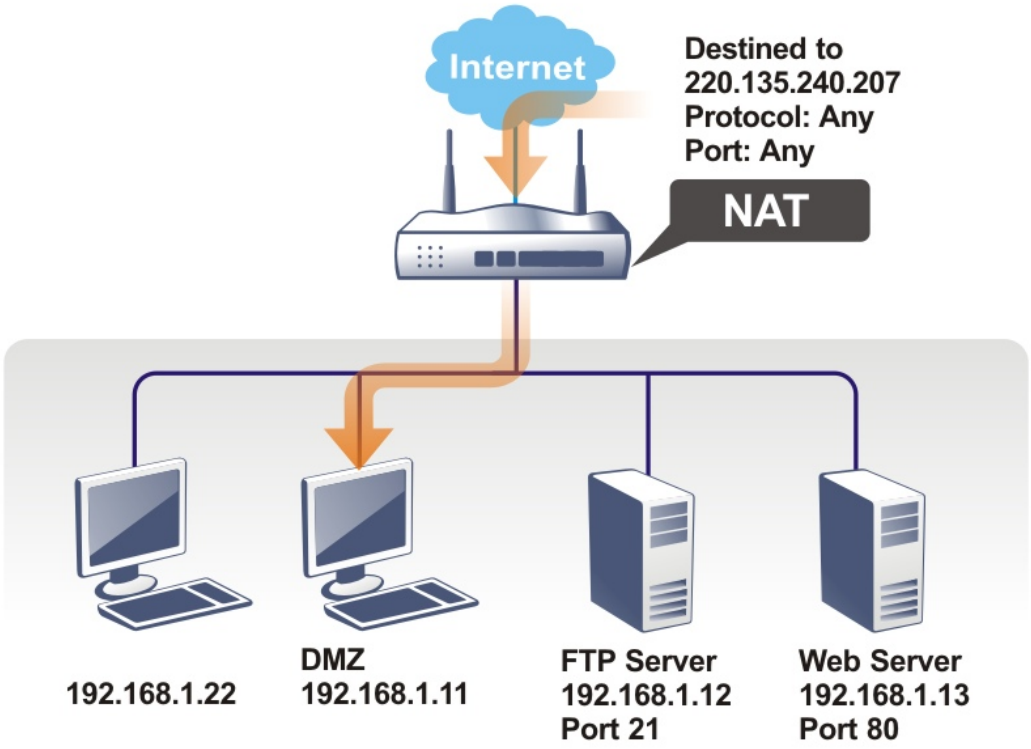
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

For example, the built-in web user interface in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.



II-4-2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. 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.

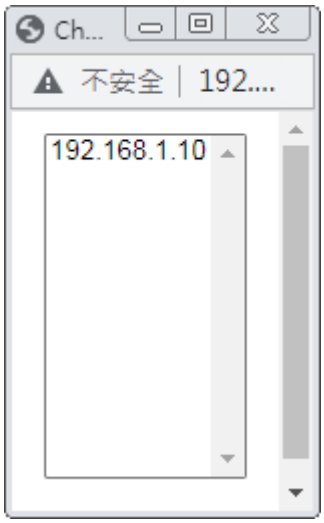


The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

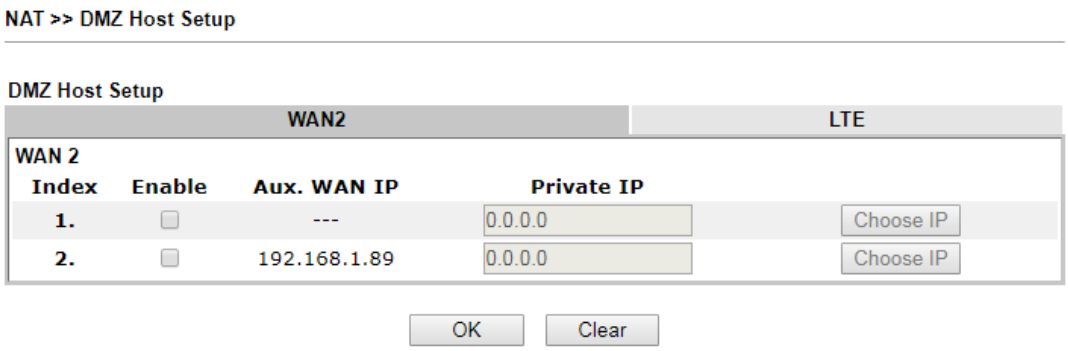
Click **DMZ Host** to open the following page. You can set different DMZ host for each WAN interface. Click the WAN tab to switch into the configuration page for that WAN.

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable the DMZ function.
Private IP	Enter the private IP address of the DMZ host, or click Choose IP to select one.

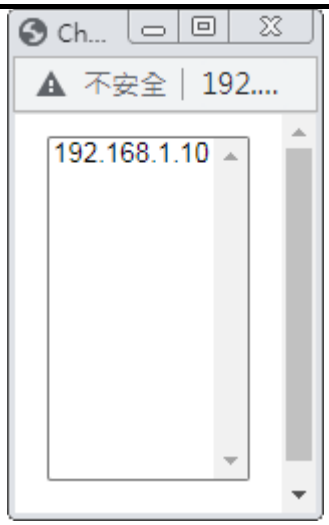
Choose IP	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.  When you have selected one private IP from the above dialog, the IP address will be shown on the screen. Click **OK** to save the setting.

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN interface**,** you will find them in **Aux. WAN IP** for your selection.



Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose IP to select one.
Choose IP	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.

	 When you have selected one private IP from the above dialog, the IP address will be shown on the screen. Click **OK** to save the setting.

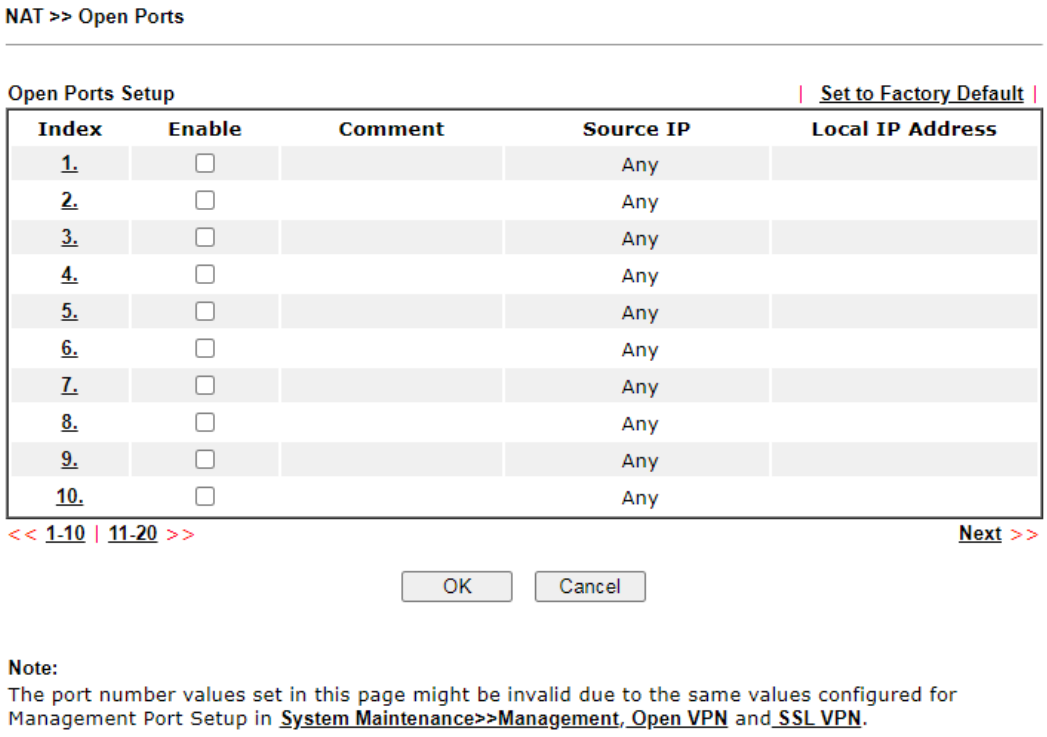
After finishing all the settings here, please click **OK** to save the configuration.

II-4-3 Open Ports

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

Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

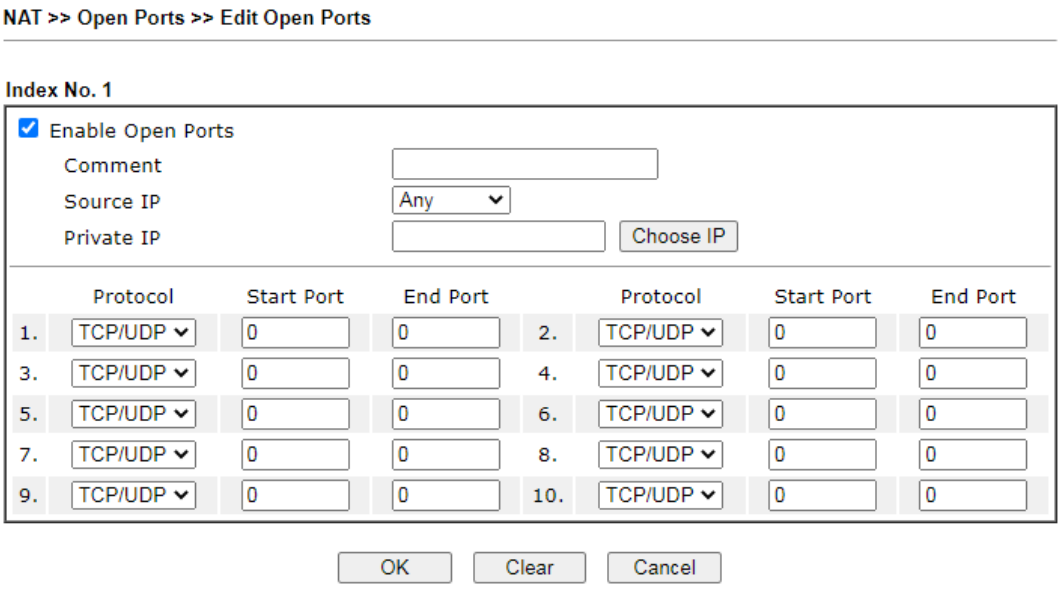
Click **Open Ports** to open the following page:



Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Enable	Check the box to enable the open port profile.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface used by such index.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.
Source IP	Display the name of source IP object.
Local IP Address	Display the private IP address of the local host offering the service.

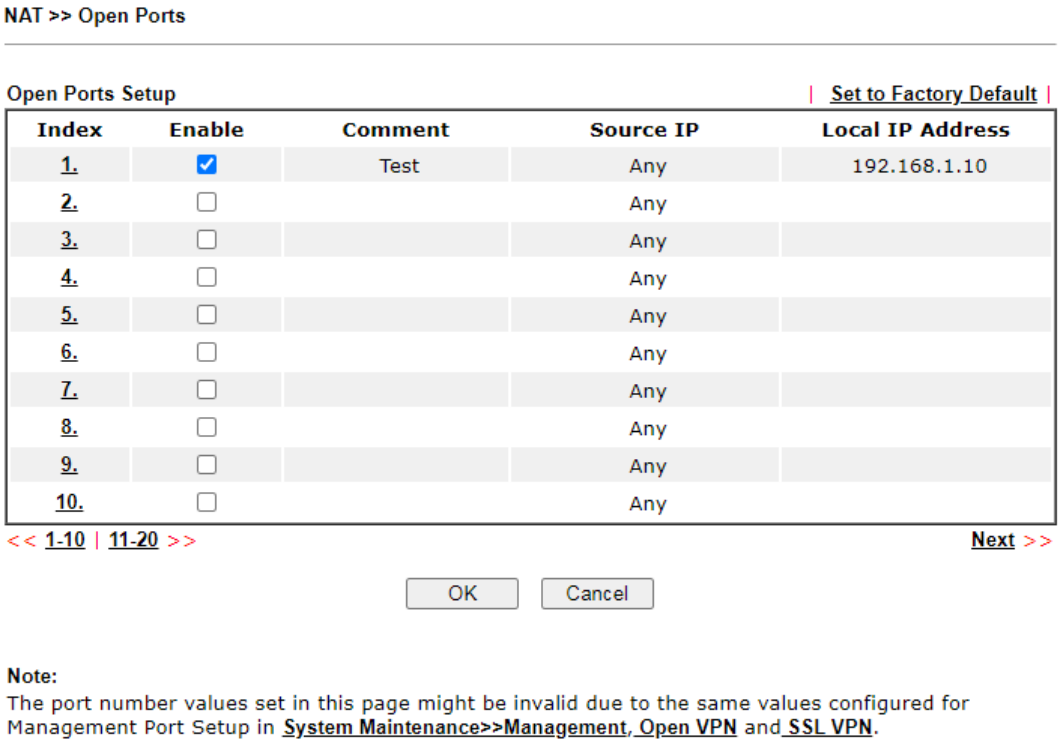
To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.



Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
Private IP	Enter the private IP address of the local host or click **Choose IP** to select one. **Choose IP -** Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or **-----** (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

After finishing all the settings here, please click **OK** to save the configuration.



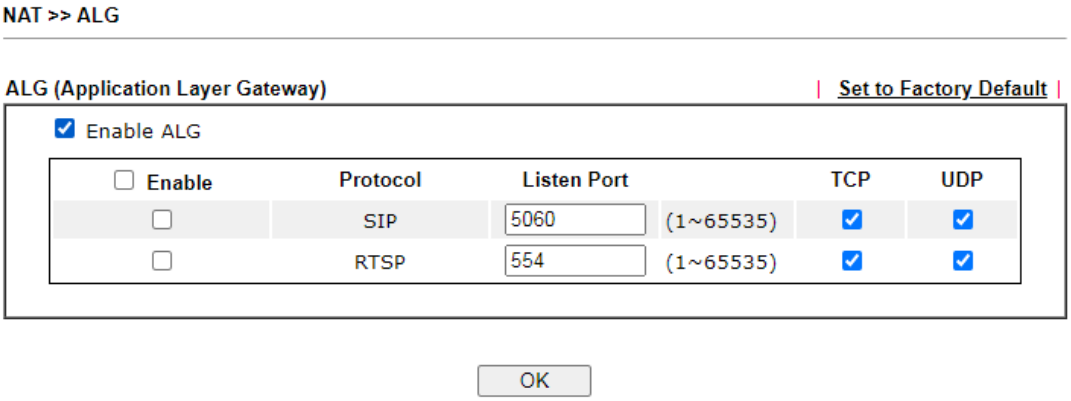
Note:
The port number values set in this page might be invalid due to the same values configured for Management Port Setup in **System Maintenance>>Management**, **Open VPN** and **SSL VPN**.

II-4-4 ALG

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

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

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



Available settings are explained as follows:

Item	Description
Enable ALG	Check to enable such function.
Listen Port	Type a port number for SIP or RTSP protocol.

TCP	Check the box to make correspond protocol message packet from TCP transmit and receive via NAT.
UDP	Check the box to make correspond protocol message packet from UDP transmit and receive via NAT.

II-5 Applications

Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** You should visit their websites to register your own domain name for the router.

Schedule

The Vigor router has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

RADIUS

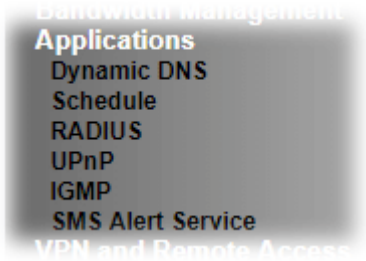
Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network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

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

UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a router.

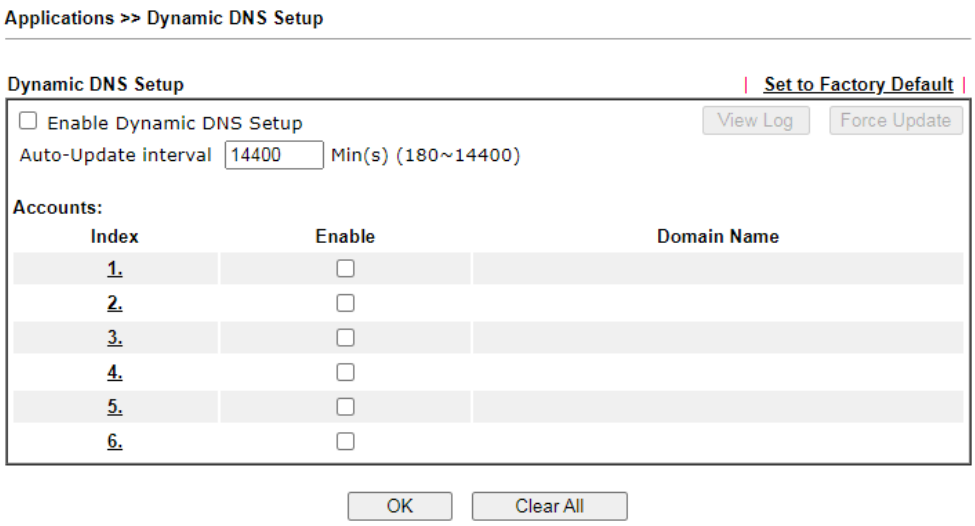
Web User Interface



II-5-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
2. Open **Applications>>Dynamic DNS**.
3. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.

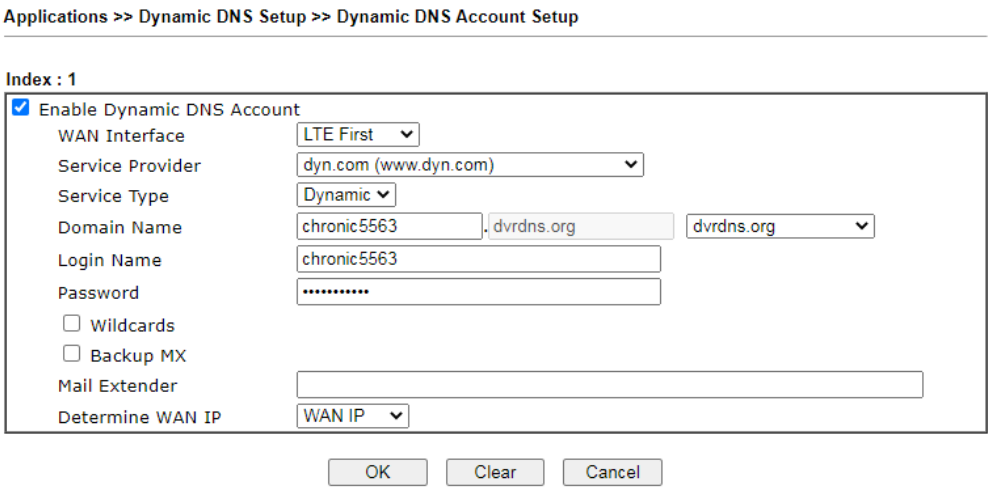


Available settings are explained as follows:

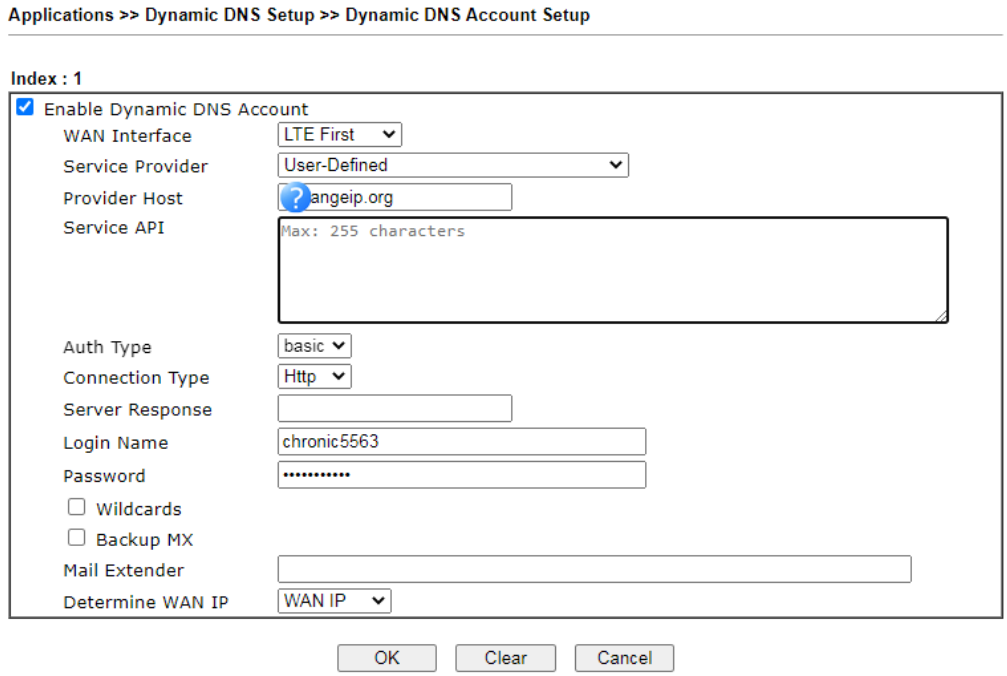
Item	Description
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).

Enable	Check the box to enable this account.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.

4. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, Enter the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.



If **User-Defined** is specified as the service provider, the web page will be changed slightly as follows:



Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.

Provider Host	Enter the IP address or the domain name of the host which provides related service. Note that such option is available when Customized is selected as Service Provider.
Service API	Enter the API information obtained from DDNS server. Note that such option is available when Customized is selected as Service Provider. (e.g: /dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j*****.changeip.org&ip=###IP### &cmd=update&offline=0)
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. (e.g., http://ns1.vigorddns.com/ddns.php?username=xxxx&password=xxxx&domain=xxxx.vigorddns.com) Note that such option is available when Customized is selected as Service Provider.
Connection Type	There are two connection types (HTTP and HTTPs) to be specified. Note that such option is available when Customized is selected as Service Provider.
Server Response	Type any text that you want to receive from the DDNS server. Note that such option is available when Customized is selected as Service Provider.
Login Name	Enter the login name that you set for applying domain.
Password	Enter the password that you set for applying domain.
Wildcard	The Wildcard feature is not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please Enter the name in this area. Such mail server will be used as backup mail exchange.
Determine WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: ● **WAN IP** - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● **Internet IP** – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.

5. Click **OK** button to activate the settings. You will see your setting has been saved.

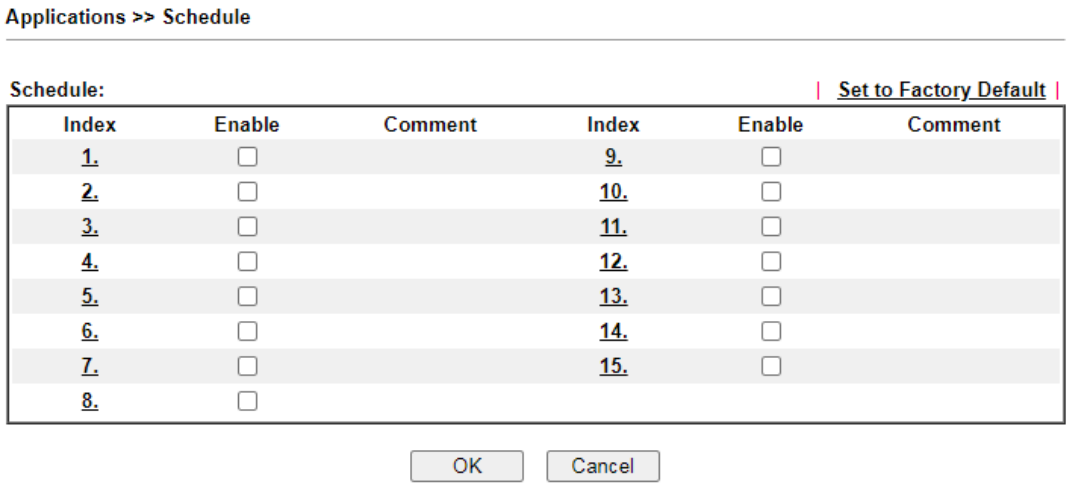
Disable the Function and Clear all Dynamic DNS Accounts

Uncheck **Enable Dynamic DNS Setup**, and click **Clear All** button to disable the function and clear all accounts from the router.

II-5-2 Schedule

The Vigor router has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.



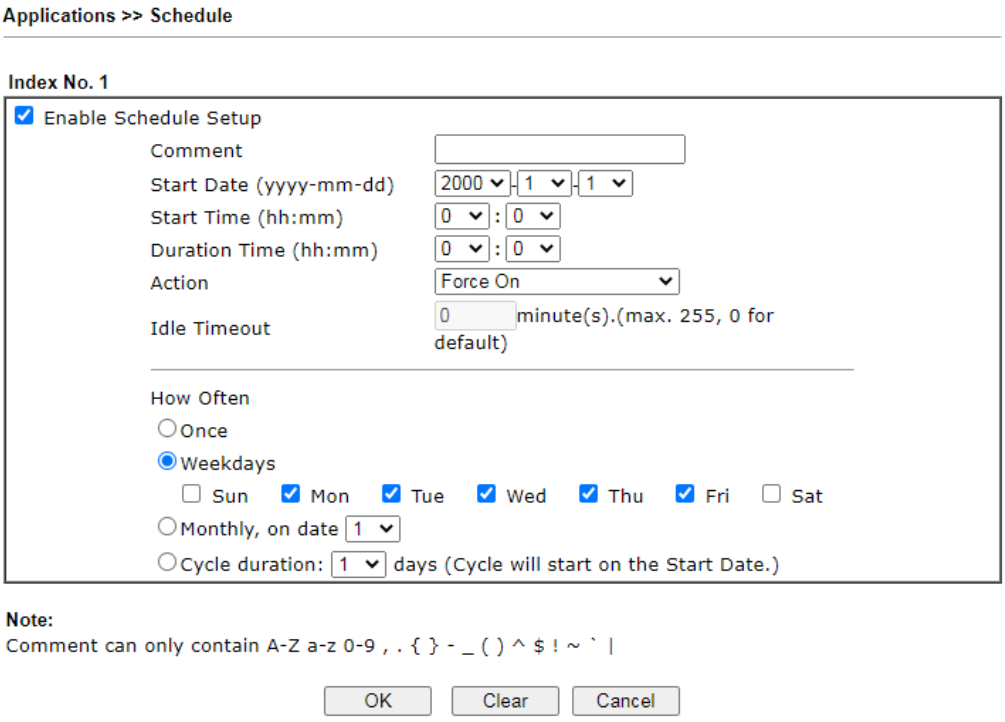
Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the index number link to access into the setting page of schedule.
Enable	Click the box to enable such schedule profile.
Comment	Display the name of the time schedule.

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN and Remote Access >> LAN to LAN** settings.

To add a schedule:

1. Click any index, say Index No. 1.
2. The detailed settings of the schedule with index 1 will be shown below.



Available settings are explained as follows:

Item	Description
Enable Schedule Setup	Check to enable the schedule.
Comment	Type a short description for such schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
Action	Specify which action Call Schedule should apply during the period of the schedule. **Force On -**Force the connection to be always on. **Force Down -**Force the connection to be always down. **Enable Dial-On-Demand -**Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field. **Disable Dial-On-Demand -**Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule.
How Often	Specify how often the schedule will be applied. ● **Once -**The schedule will be applied just once ● **Weekdays -**Specify which days in one week should perform the schedule. ● **Monthly, on date –** The router will only execute the action applied such schedule on the date (1 to 28) of a month.

	● **Cycle duration –** Type a number as cycle duration. Then, any action applied such schedule will be executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date.

3. Click **OK** button to save the settings.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).

Office Hour:

(Force On)

Mon - Sun **9:00 am** **to** **6:00 pm**

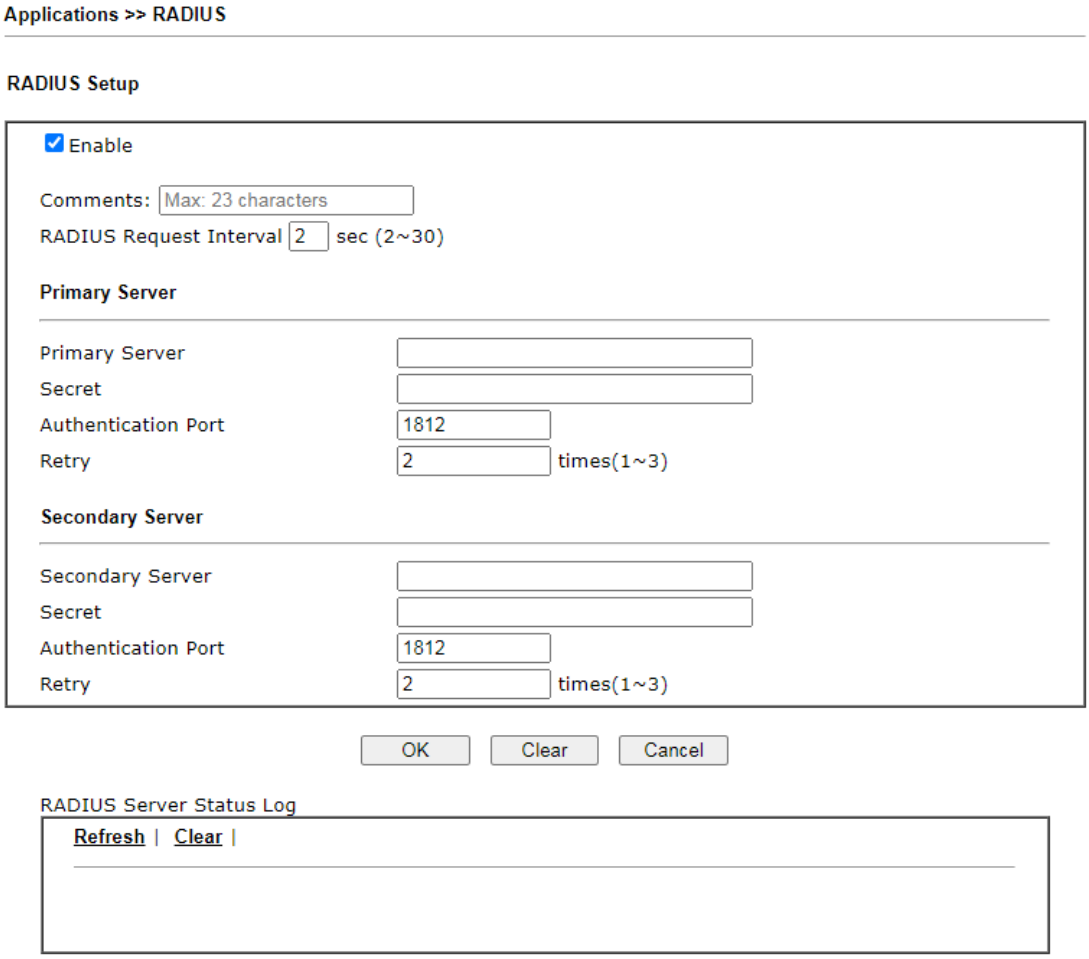
1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

II-5-3 RADIUS

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

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

Vigor router can be operated as a RADIUS client. Therefore, this page is used to configure settings for external RADIUS server. Then LAN user of Vigor router will be authenticated by such server for network application.



Available settings are explained as follows:

Item	Description
Enable	Check to enable RADIUS client feature. RADIUS Accounting is a network customer billing mechanism for RADIUS server. If enabled, Vigor router will deliver accounting request (e.g., IP address, traffic from the client) to the specified RADIUS server periodically. **Comments** - Enter a brief description for this profile. **RADIUS Request Interval** - Set a timeout value for the router

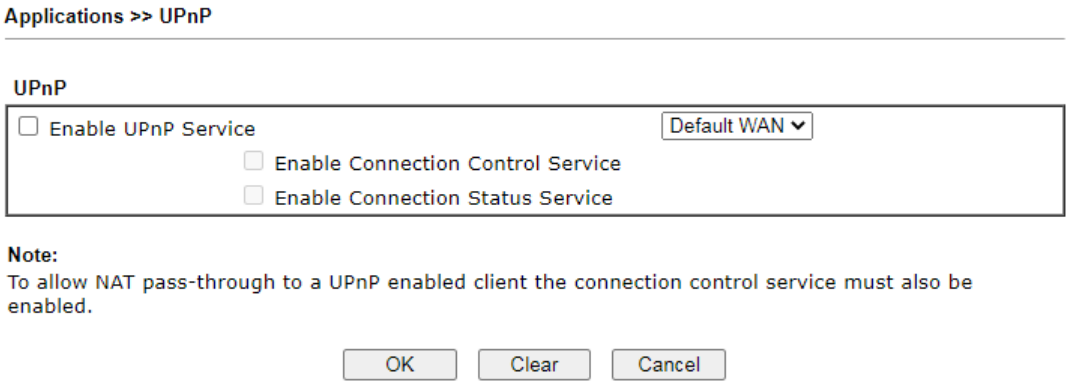
	waiting for a response from the RADIUS server. If no response, Vigor router will send the authentication request again.
Primary Server	**Primary Server** - Enter the IP address of the RADIUS server. **Secret** - The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters. **Authentication Port** - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138. **Retry** - Set the number of attempts to perform reconnection with RADIUS server. If the connection (with the Primary Server) still fails, stop the connection attempt and begin to make connection with the secondary server.
Secondary Server	**Secondary Server** - Enter the IP address of RADIUS server. **Secret** - The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters. **Authentication Port** - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138. **Retry** - Set the number of attempts to perform reconnection. If the connection (with the Secondary Server) still fails, stop the connection attempt. The client authentication would be determined as "failed".

After finished the above settings, click **OK** button to save the settings.

II-5-4 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router.

Info	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.



Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

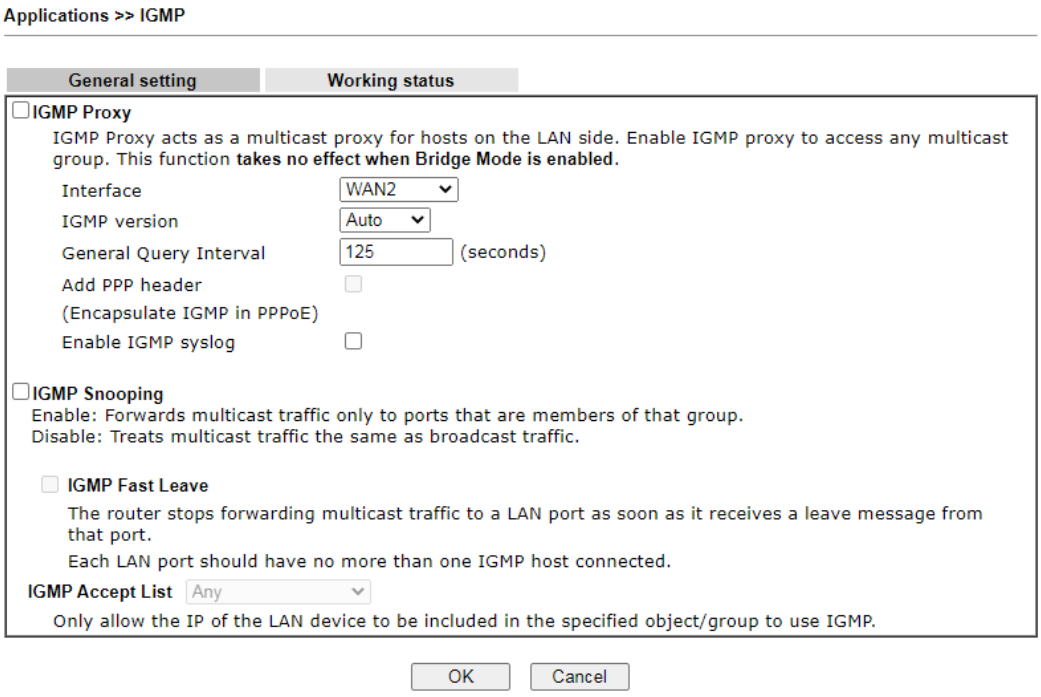
- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

II-5-5 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

II-5-5-1 General Setting



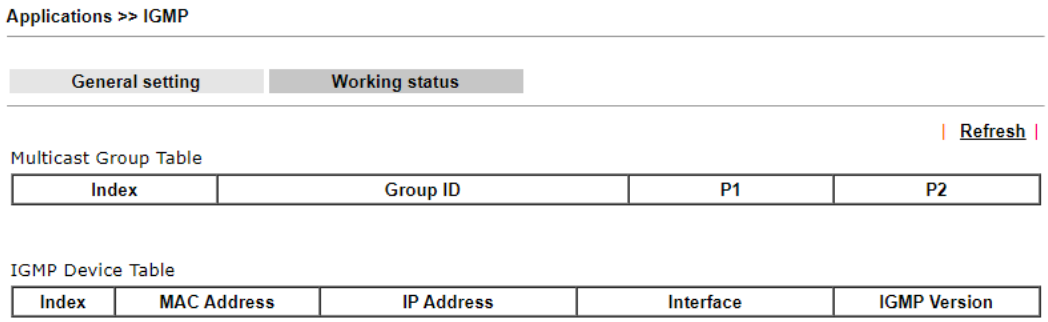
Available settings are explained as follows:

Item	Description
IGMP Proxy	Check this box to enable this 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. **IGMP version** – At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe. **General 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. **Add PPP header** – Check this box if the interface type for IGMP is PPPoE. It depends on the specifications regulated by each ISP. If you have no idea to enable or disable, simply contact your ISP providers. **Enable IGMP syslog** - Check the box to store the IGMP status onto Syslog.

IGMP Snooping	Select to enable IGMP Snooping so that multicast traffic are forwarded to IGMP clients that have joined a multicast group. **IGMP Fast Leave** - This option is shown only when IGMP Snooping is enabled. Select to enable IGMP Fast Leave. Normally when the router receives a "leave" message from an IGMP host, it will send a last member query message to see if there are still members within the multicast group. When Fast Leave is enabled, multicast for a group is immediately terminated when the last host in that group sends a "leave" message. **IGMP Accept List** - Only the device with the IP address specified here is able to use IGMP.

After finishing all the settings here, please click **OK** to save the configuration.

II-5-5-2 Working Group



Available settings are explained as follows:

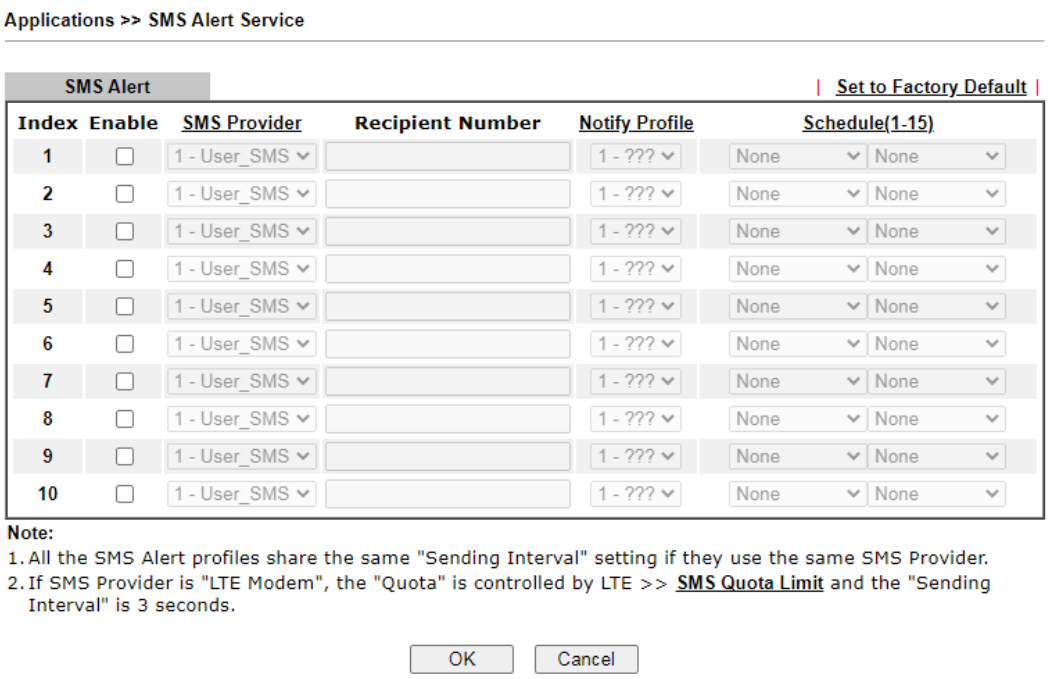
Item	Description
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P2	It indicates the LAN port used for the multicast group.

II-5-6 SMS Alert Service

The function of SMS (Short Message Service) Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.

This page allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.



Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click **SMS Provider** link to define the SMS server.
Recipient Number	Enter the phone number of the one who will receive the SMS.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the **Notify Profile** link to define the content of the SMS.
Schedule (1-15)	Enter the schedule number that the SMS will be sent out. You can click the **Schedule(1-15)** link to define the schedule.

After finishing all the settings here, please click **OK** to save the configuration.

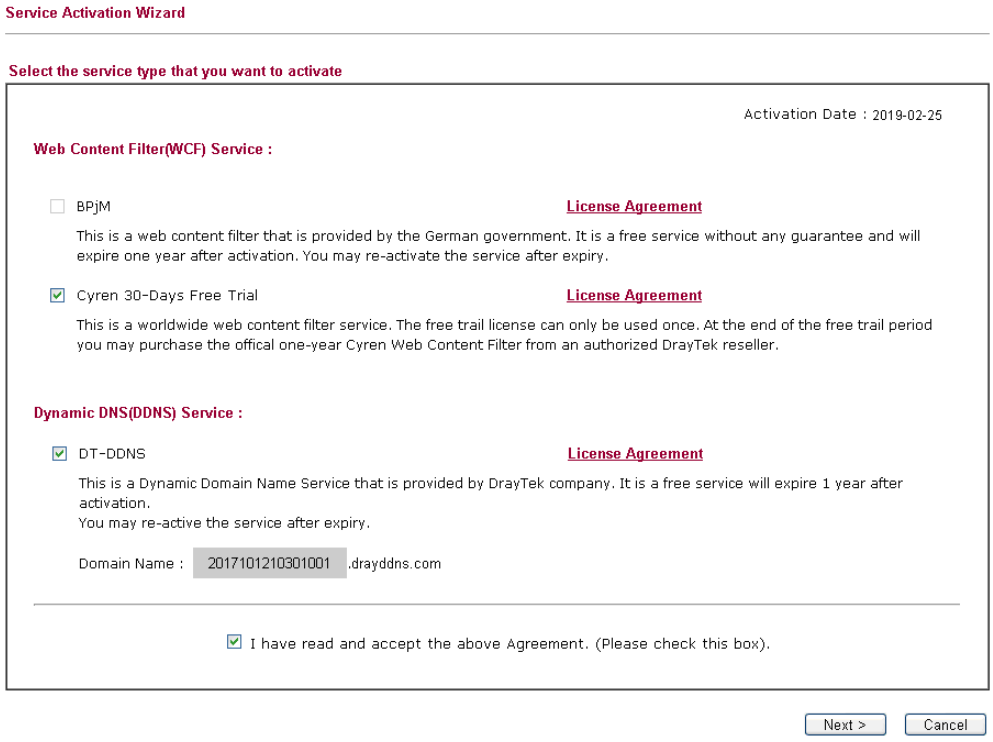
Application Notes

A-1 How to use DrayDDNS?

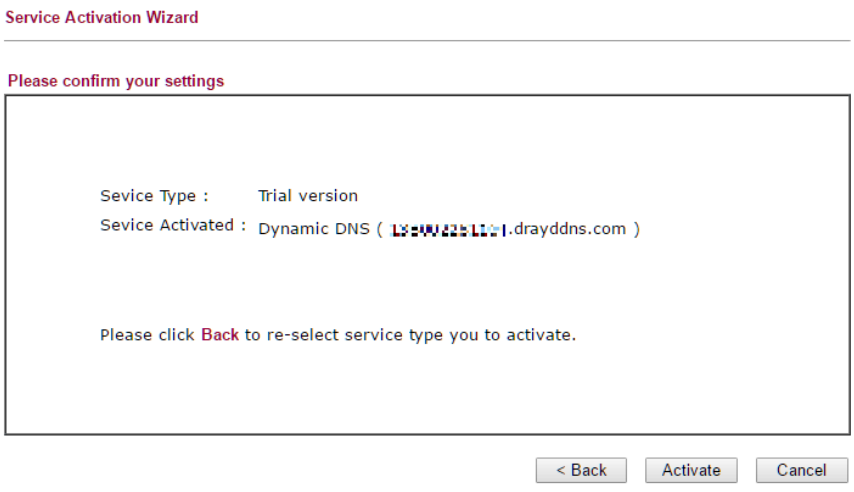
Vigor router supports various DDNS service providers, user can set up user-defined profile to update the DDNS even the service provider is not on the list. Now, DrayTek starts to support our own DDNS service - DrayDDNS. We will provide a domain name for each Vigor Router, this single domain name can record IP addresses of all WAN.

Activate DrayDDNS License

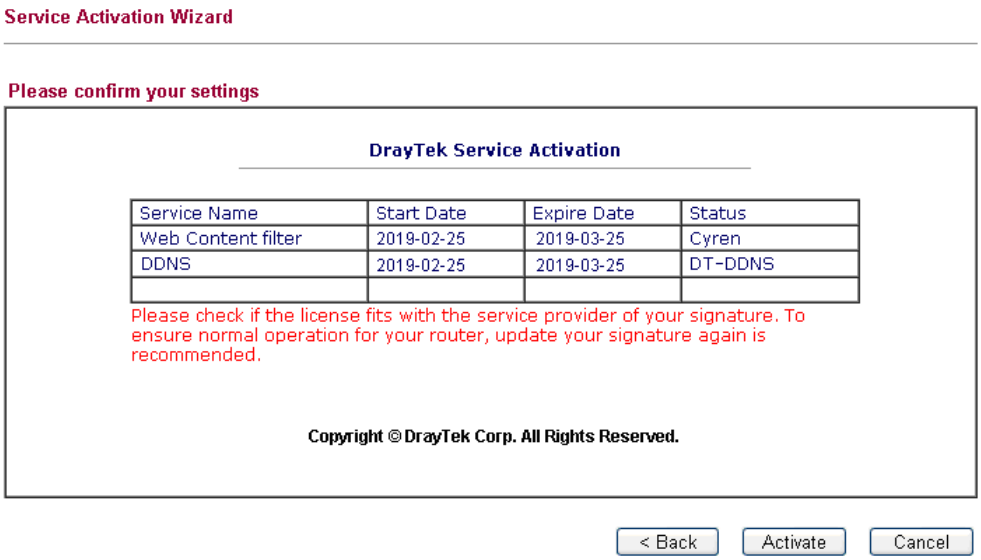
1. Go to **Wizards >> Service Activation Wizard**, wait for the router to connect to MyVigor server, then tick **DT-DDNS** and **I have read and accept the above Agreement**, click **Next**.



2. Confirm the information, then click **Activate**.



3. MyVigor server will reply with the service activation information.



Configure DDNS Profile

1. Go to **Applications >> Dynamic DNS Setup**,

   a. Tick **Enable Dynamic DNS Setup**

   b. Click an available profile index

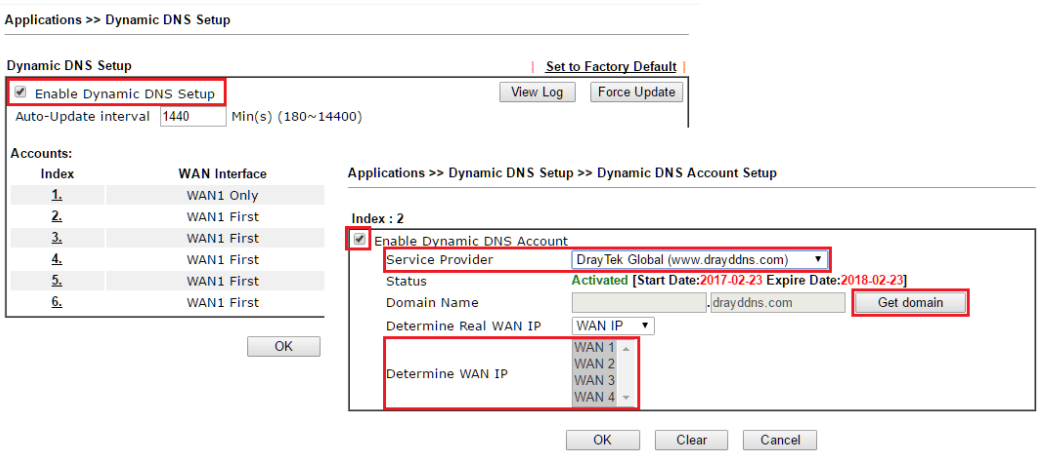
   c. Tick **Enable Dynamic DNS Account**

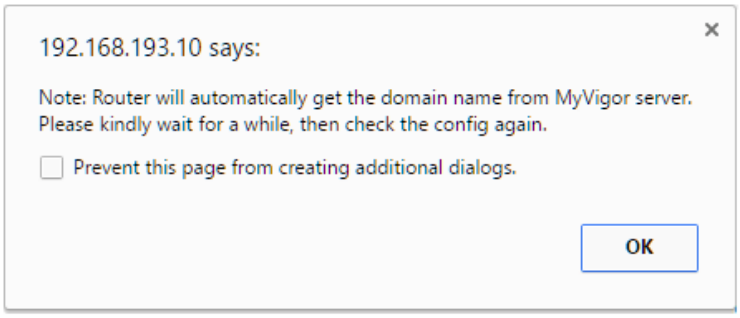
   d. Select **DrayTek Global (www.drayddns.com)** as **Service Provider**

   e. Select the WAN you would like to upload the IP to DDNS server

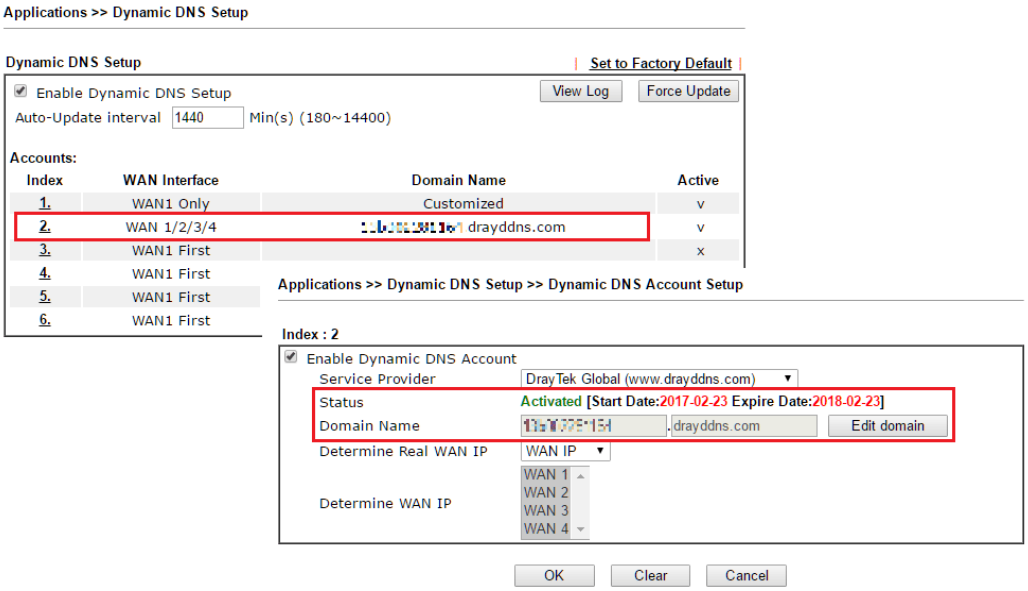
   f. Click **Get domain**

   g. Click **OK** on the pop up notification window





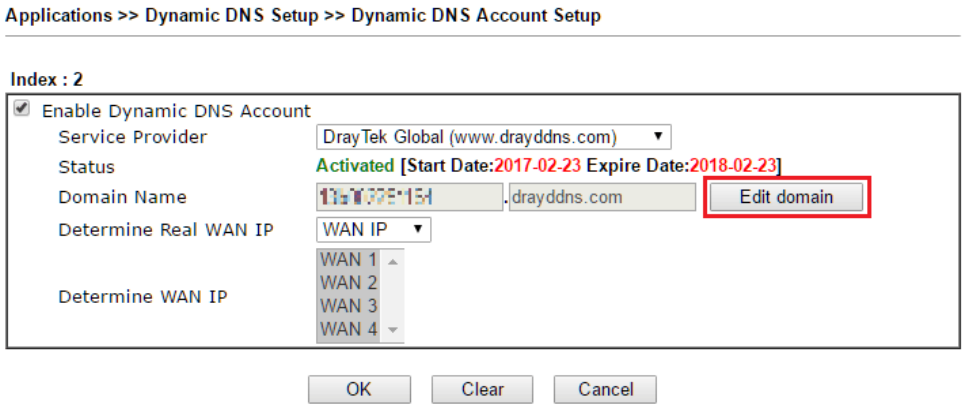
2. Wait few seconds for router to get the domain name, then, we can click the profile to check the information of license and domain name.



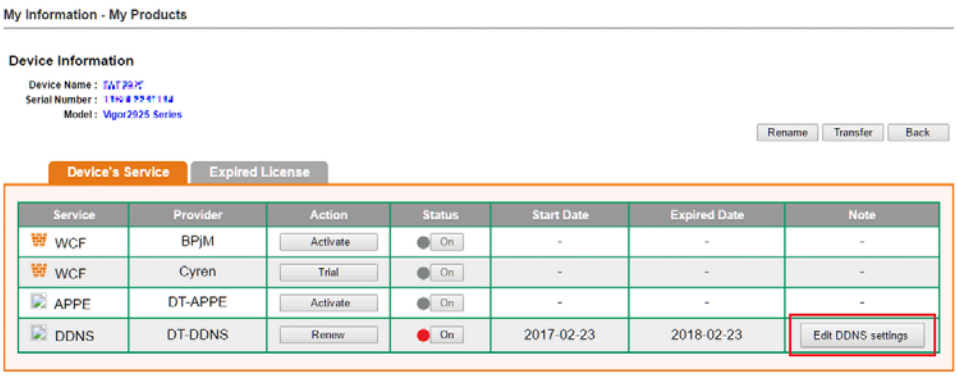
Modify Domain Name

Currently, only the domain name is allowed to be modified MyVigor website. We will need to register the router to MyVigor server, and log in to MyVigor website to modify it.

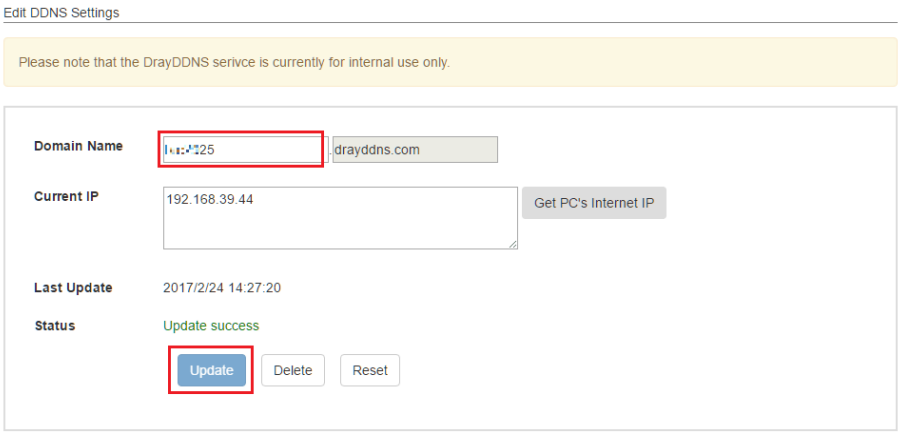
1. Please visit https://myvigor.draytek.com/ or go to **Applications >> Dynamic DNS Setup >> DrayDDNS** profile and click **Edit domain**.



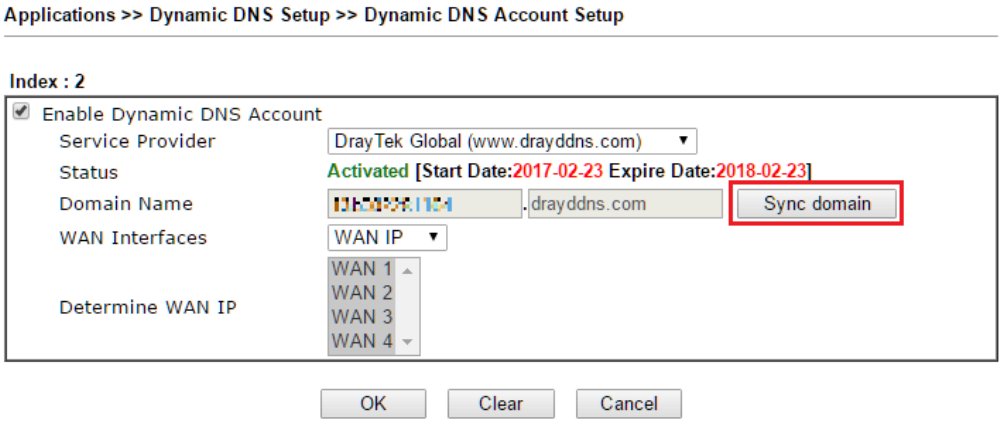
2. Log in to MyVigor Website, choose the profile, then click **Edit DDNS settings**.



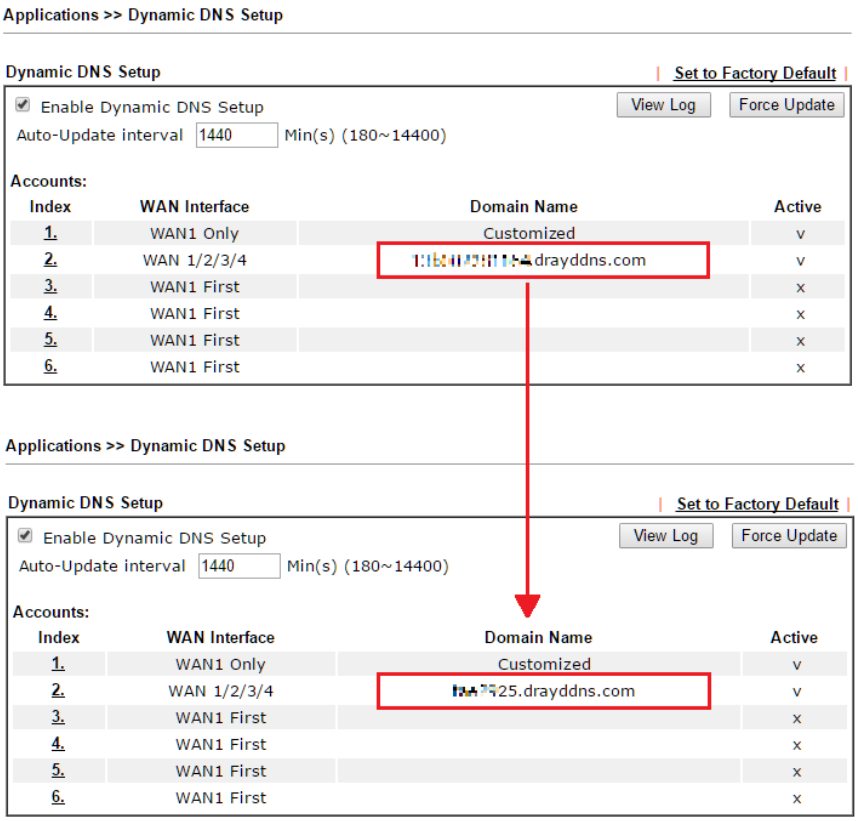
3. Input the desired **Domain name (e.g., XXXX25)** and click **Update.**



4. Vigor router will get the modified domain name when the it performs next DDNS updating. We can click **Sync domain** to accelerate this process.



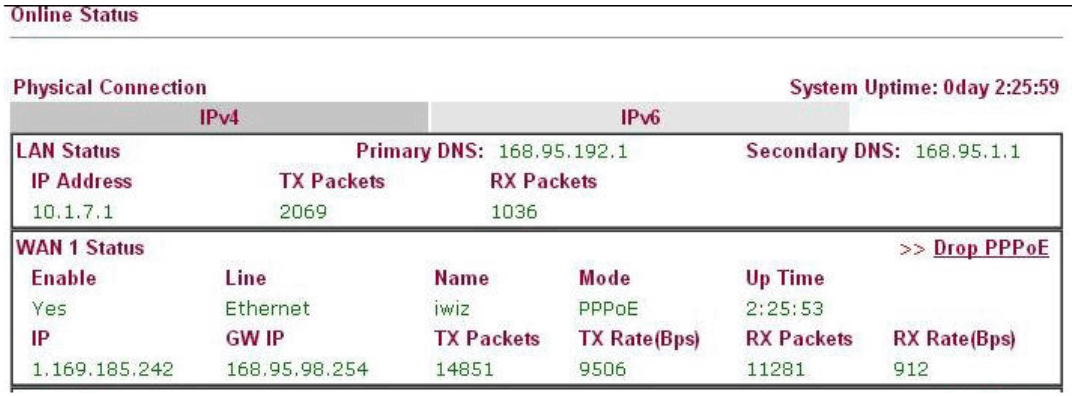
After few seconds, the router will get the new domain name and print it on the profiles list.


Applications >> Dynamic DNS Setup
Dynamic DNS Setup
Set to Factory Default
Enable Dynamic DNS Setup
View Log
Force Update
Auto-Update interval 1440 Min(s) (180~14400)
Accounts:
Index WAN Interface Domain Name Active
1. WAN1 Only Customized v
2. WAN 1/2/3/4 drayddns.com v
3. WAN1 First x
4. WAN1 First x
5. WAN1 First x
6. WAN1 First x
Applications >> Dynamic DNS Setup
Dynamic DNS Setup
Set to Factory Default
Enable Dynamic DNS Setup
View Log
Force Update
Auto-Update interval 1440 Min(s) (180~14400)
Accounts:
Index WAN Interface Domain Name Active
1. WAN1 Only Customized v
2. WAN 1/2/3/4 25.drayddns.com v
3. WAN1 First x
4. WAN1 First x
5. WAN1 First x
6. WAN1 First x

A-2 How to Configure Customized DDNS?

This article describes how to configure customized DDNS on Vigor routers to update your IP to the DDNS server. We will take "Changeip.org" and "3322.net" as example. Before setting, please make sure that the WAN connection is up.

Part A : Changeip.org



Note that,

Username: jo***

Password: jo********

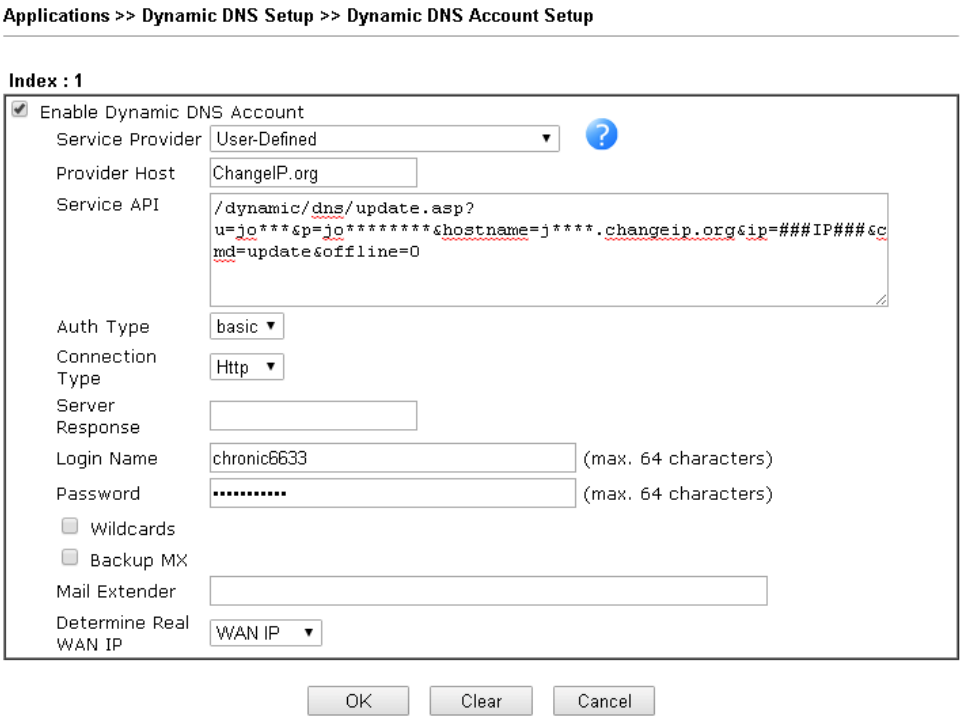
Host name: j*****.changeip.org

WAN IP address: 1.169.185.242

Following is the screenshot of editing the HTML script on the browser to update your IP to the DDNS server.

Now we have to configure the router so it can do the same job for us automatically.

1. Please go to **Applications >> Dynamic DNS** to create a profile for user-defined DDNS client.



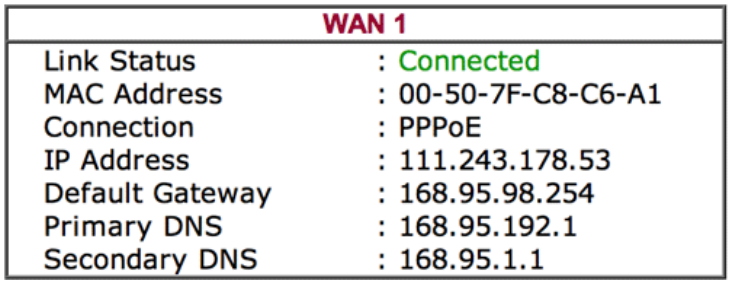
2. Set the Service Provider as **User-Defined**.

3. Set the Service API as:
/dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j****.changeip.org&ip=###IP### &cmd=update&offline=0

   In which, ###IP### is a value which will be replaced with the current interface IP address automatically when DDNS service is running. In this case the IP will be 1.169.185.242.

4. After setting, the Customized DDNS service will be up, and our IP will be updated to the DDNS server.

Part B : 3322.net



Username: bi*******

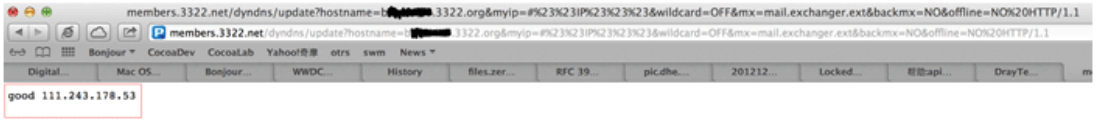
Password: 88********

Host name: bi*******.3322.org

WAN IP address: 111.243.178.53

To update the IP to the DDNS server via editing the HTML script, we can Enter the following script on the browser:

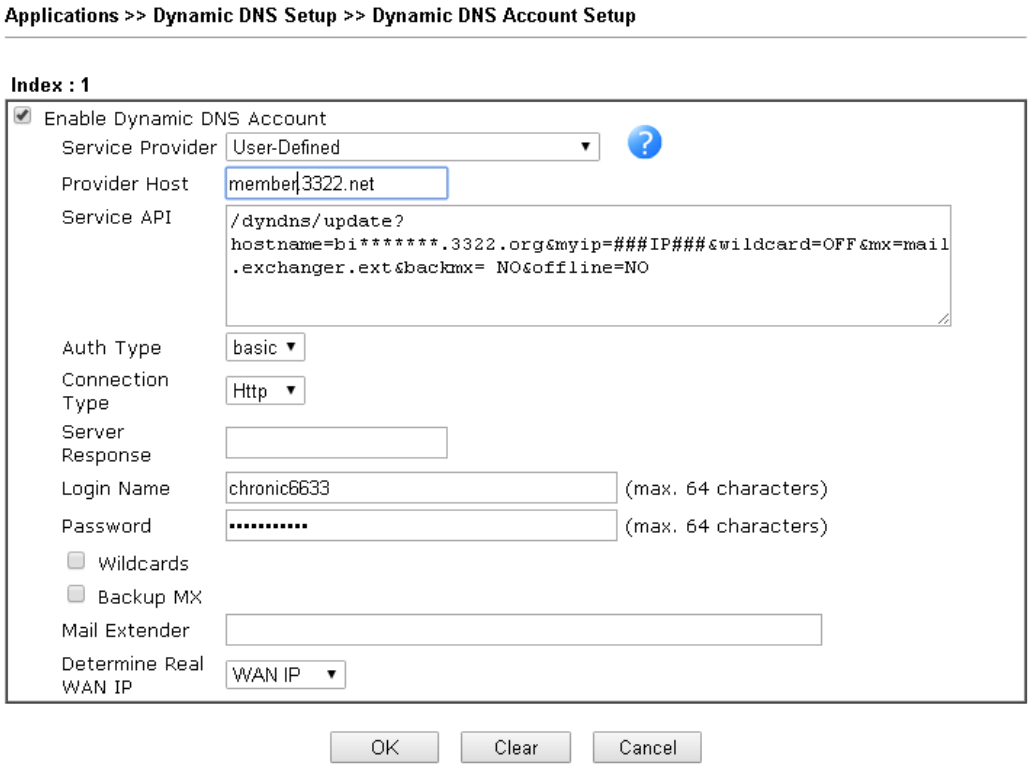
And the result will be :



"good 111.243.178.53" means our IP has been updated to the server successfully.

Now we have to configure the router so it can do the same job for us automatically.

1. Please go to **Applications >> Dynamic DNS** to create a profile for User-Defined DDNS client.



2. Set the Service Provider as **User-Defined**.

3. Set the Provider Host as **member.3322.net**.

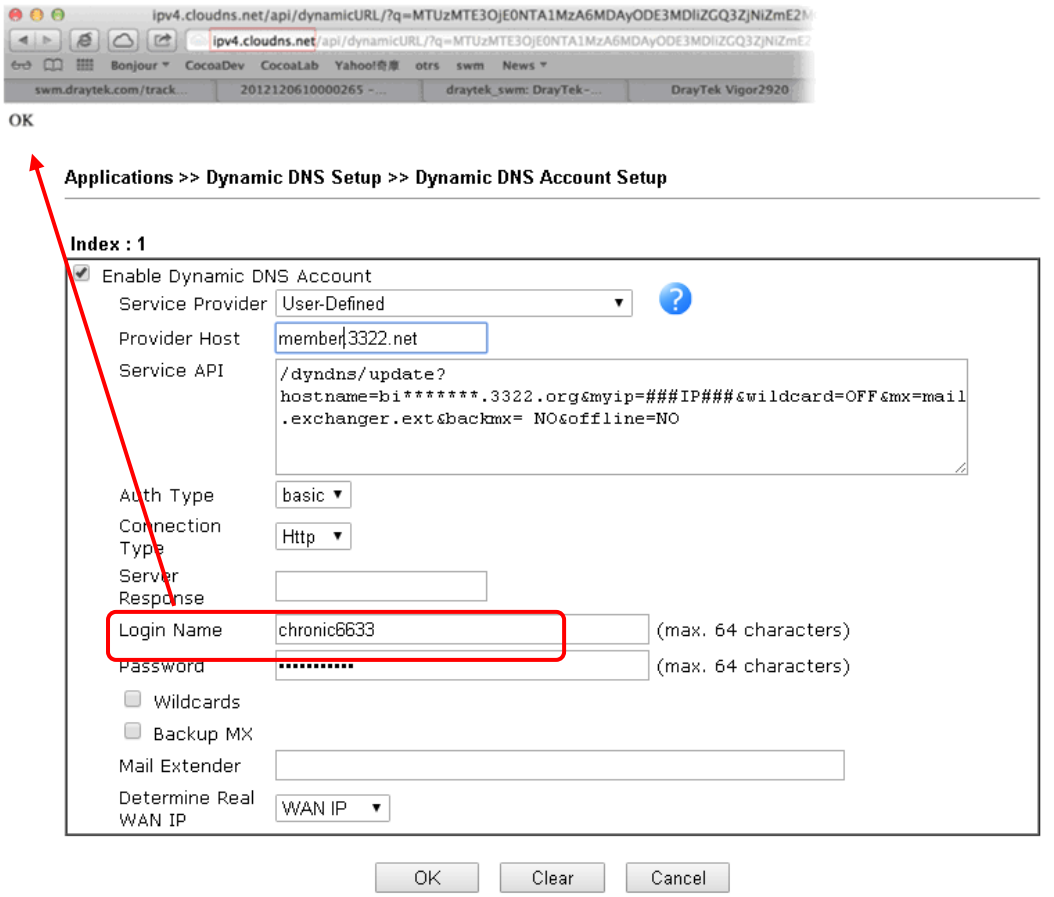
4. Set the Service API as:
/dyndns/update?hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail.exchanger.ext&backmx=NO&offline=NO

5. Enter your account and password.

6. After the setting, the Customized DDNS service will be up, and our IP will be updated to the DDNS server automatically.

Part C : Extend Note

The customized Service Provider is also eligible with the ClouDNS.net.



II-6 Routing

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

Through protocol, IP address, port number and interface configuration, Route Policy can be used to configure any routing rules to fit actual request. In general, Route Policy can easily reach the following purposes:

Specify Interface

Through dedicated interface (WAN/LAN/VPN), the data can be sent from the source IP to the destination IP.

Address Mapping

Allows you specify the outgoing WAN IP address (es) for an internal private IP address or a range of internal private IP addresses.

Priority

The router will determine which policy will be adopted for transmitting the packet according to the priority of Static Route and Route Policy.

Failover to/Failback

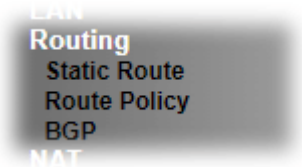
Packets will be sent through another Interface or follow another Policy when the original interface goes down (**Failover to**). Once the original interface resumes service (**Failback**), the packets will be returned to it immediately.

Other routing

Specify routing policy to determine the direction of the data transmission.

Info	For more detailed information about using policy route, refer to **Support >>FAQ/Application Notes** on www.draytek.com.

Web User Interface

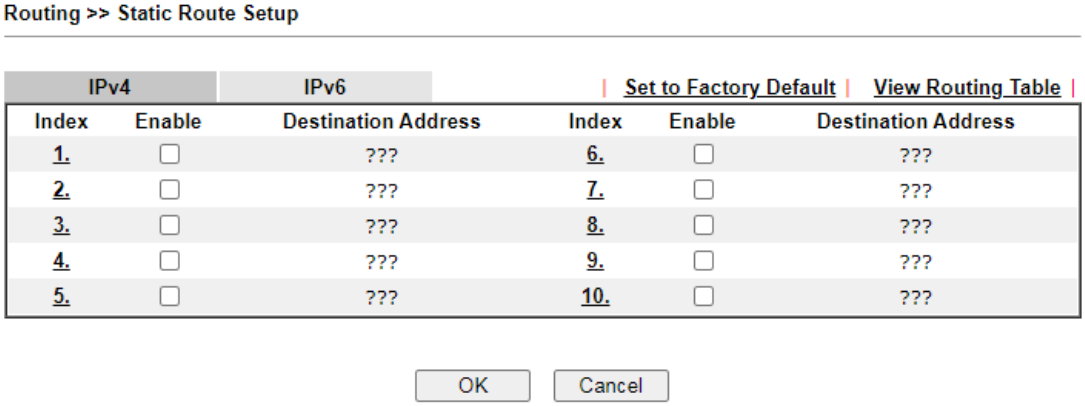


II-6-1 Static Route

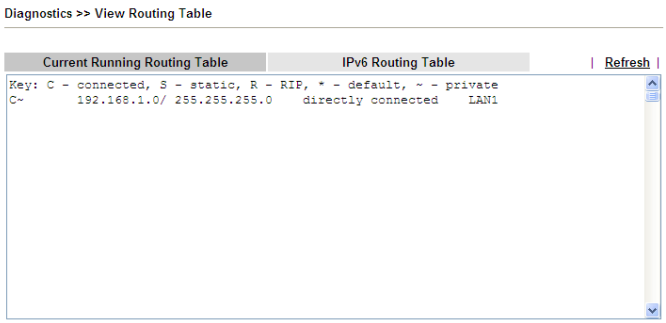
Static routing is an alternative to dynamic routing. It is a process that the system network administrator can configure network routers with all the required information for packet forwarding.

Go to **Routing** >> **Static Route**. The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

Static Route for IPv4



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing Routing Table	Displays the routing table for your reference. 
Index	The number (1 to 30) under Index allows you to open next page to set up static route.
Enable	Check the box to enable such route.

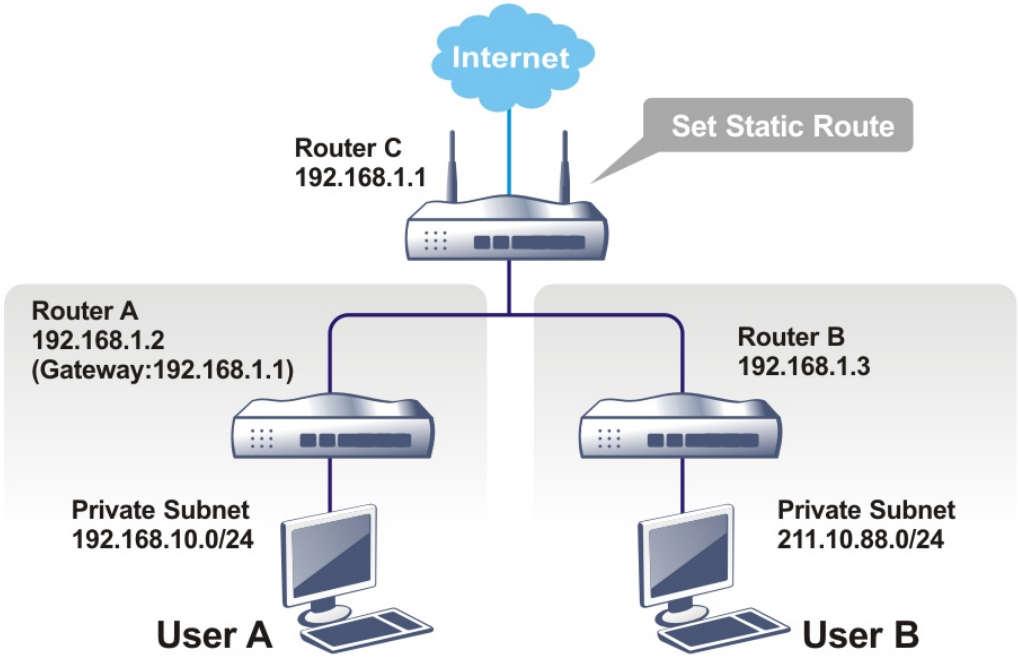
Destination Address	Displays the destination address of the static route.

Add Static Routes to Private and Public Networks

Here is an example (based on IPv4) of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

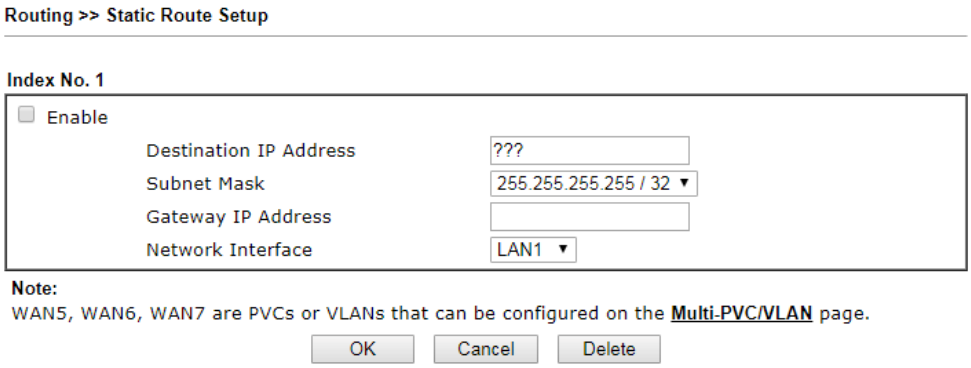
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

Info	There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via the router, and continuously exchange of IP routing information with different subnets.

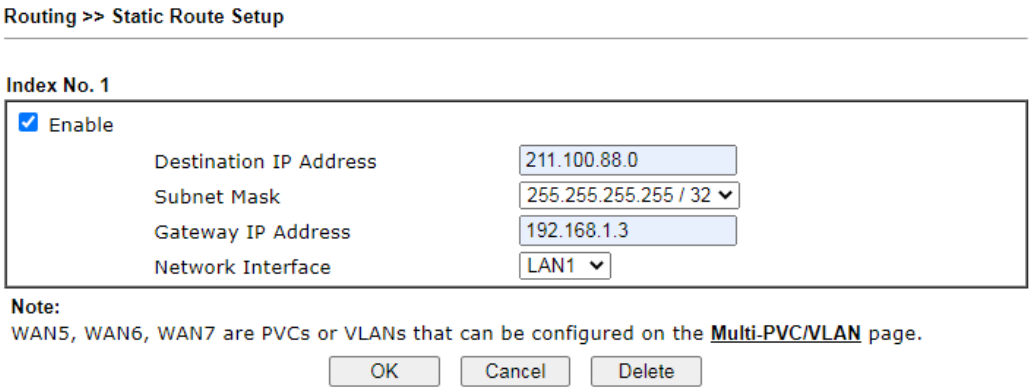
2. Click the **LAN >> Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



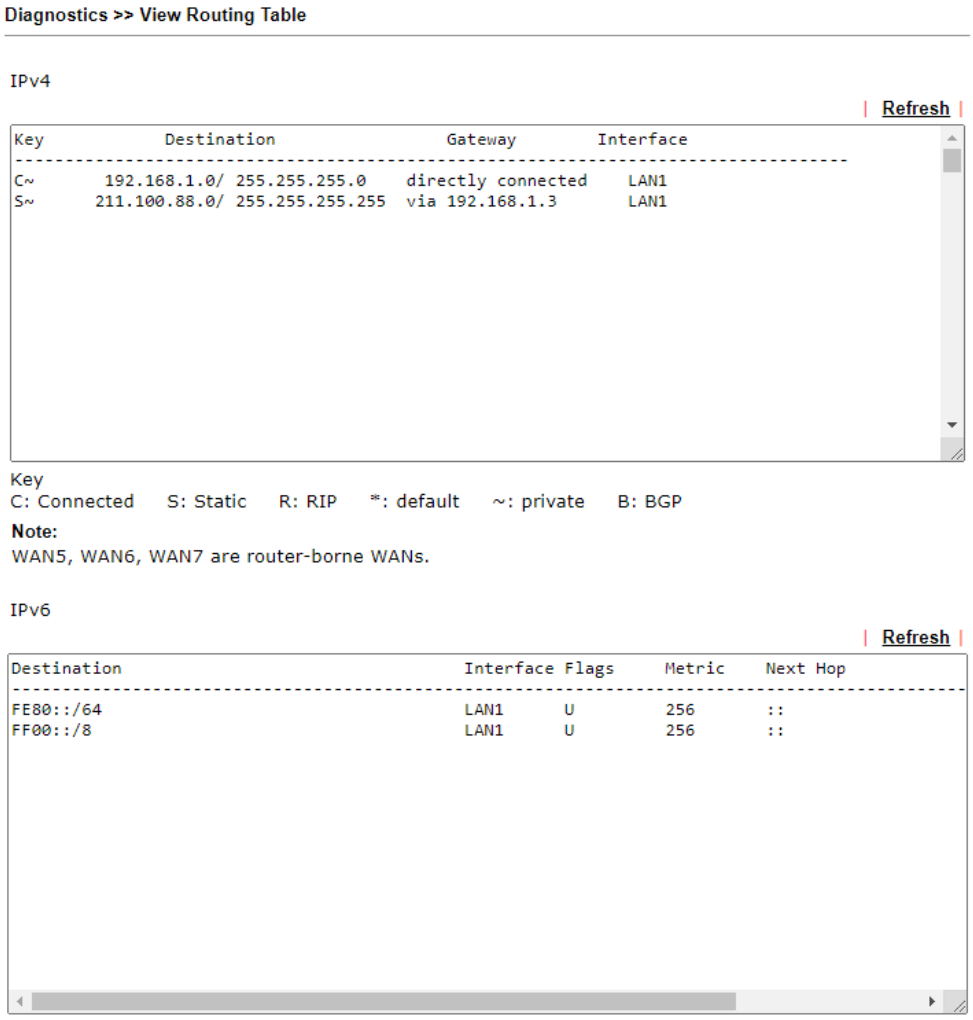
Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.
Destination IP Address	Type an IP address as the destination of such static route.
Subnet Mask	Enter the subnet mask for such static route.
Gateway IP Address	Enter the IP address of the gateway.
Network Interface	Use the drop down list to specify an interface for such static route.

3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3. Click **OK**.

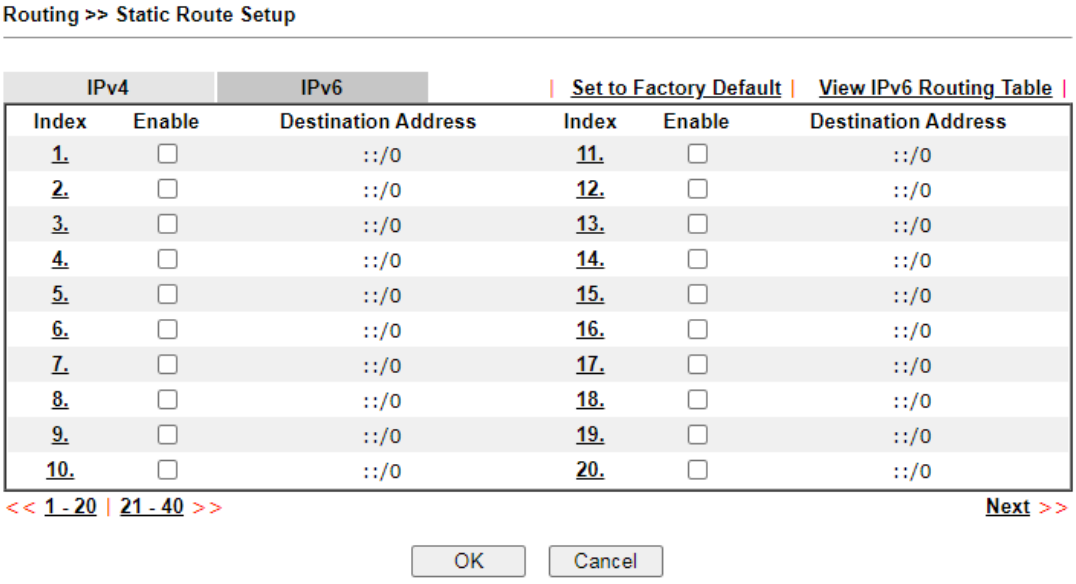


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



Static Route for IPv6

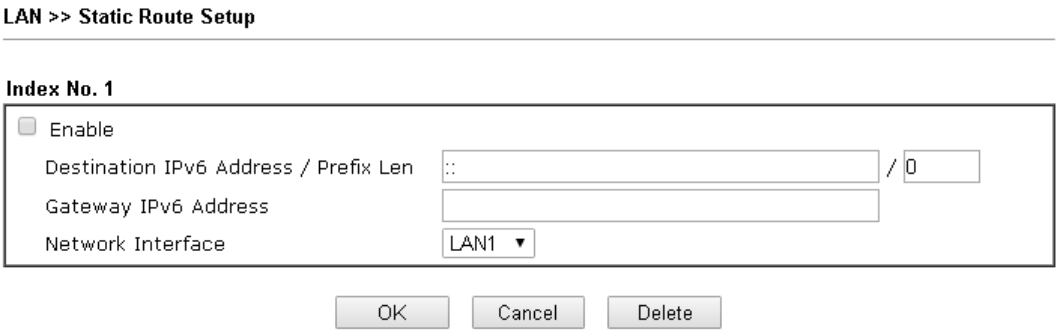
You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing IPv6 Routing Table	Displays the routing table for your reference.
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Enable	Check the box to enable such static route.
Destination Address	Displays the destination address of the static route.

Click any underline of index number to get the following page.



Available settings are explained as follows:

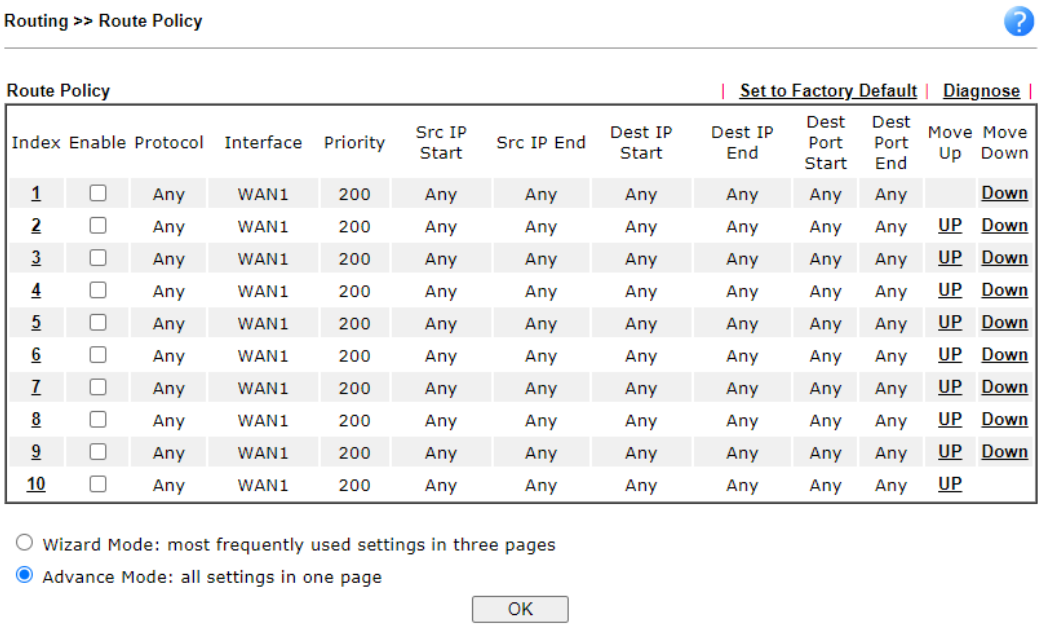
Item	Description
Enable	Click it to enable this profile.
Destination IPv6 Address / Prefix Len	Enter the IP address with the prefix length for this entry.
Gateway IPv6 Address	Enter the gateway address for this entry.
Network Interface	Use the drop down list to specify an interface for this static route.

When you finish the configuration, please click **OK** to save and exit this page.

II-5-2 Route Policy

TheRoute Policy feature gives you control over how different types of outbound traffic are routed, through any of the LANs, WANs or VPNs. The policy set in Route Policy always has higher priority than **Default Route**, and always has lower priority than the **Firewall** Rules. Administrator may also define a priority to this policy.

To add, delete or modify load balance or route policies, select **Routing >> Route Policy** from the menu bar.



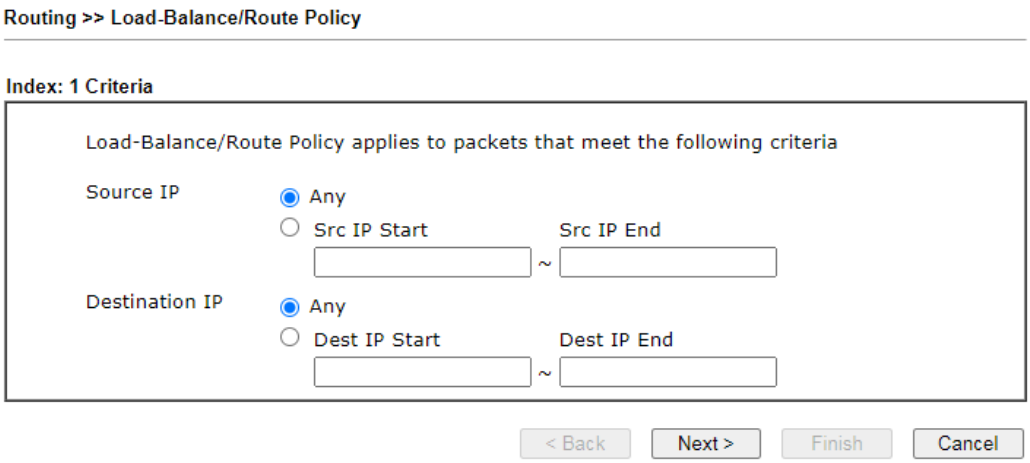
Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear the settings of all Load-Balance and Route Policy rules.
Index	Rule index. Click to bring up the configuration page of the rule.
Enable	Select to enable this rule.
Protocol	Protocol(s) to which this rule applies.
Interface	LAN, IP Routed Subnet, WAN or VPN interface that the traffic described by this rule is to be directed.
Priority	The priority of this rule.
Src IP Start	The beginning source IP address.
Src IP End	The ending source IP address.
Dest IP Start	The beginning destination IP address.
Dest IP End	The ending destination IP address.
Dest Port Start	The beginning destination port number.
Dest Port End	The ending destination port number.
Move UP/Move Down	Click to shift priority of rule up/down by one.
Wizard Mode	The setup wizard will present the most-commonly used rule settings in three steps.

Advance Mode	All the rule settings will be shown on one configuration page.

If Wizard Mode is selected, you will be guided through the configuration process in three steps. Only the most commonly used settings will be shown.

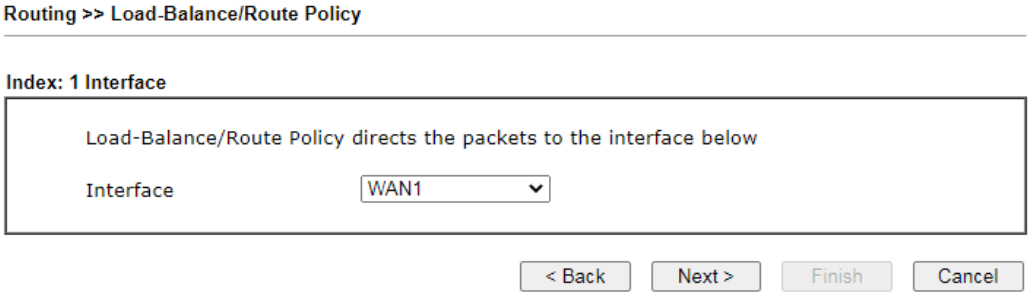
1. Click the **Wizard Mode** radio button.
2. Click **Index 1**. The setting page will appear as follows:



Available settings are explained as follows:

Item	Description
Source IP	Source IP addresses to which this rule is to be applied. **Any** - This rule applies to all source IP addresses. **Src IP Start, Src IP End** - This rule applies to the specified range of source IP addresses. If there is only one source IP address, enter the address in both the Start and End fields.
Destination IP	Destination IP addresses to which this rule is to be applied. **Any** - This rule applies to all destination IP addresses. **Dest IP Start, Dest IP End** - This rule applies to the specified range of destination IP addresses. If there is only one destination IP address, enter the address in both the Start and End fields.

3. Click **Next** to get the following page.



Available settings are explained as follows:

Item	Description
Interface	You can select an interface from one of the following: WAN, LAN, VPN, IP Routed Subnet, and LTE. Packets match with the above criteria will be transferred to the interface

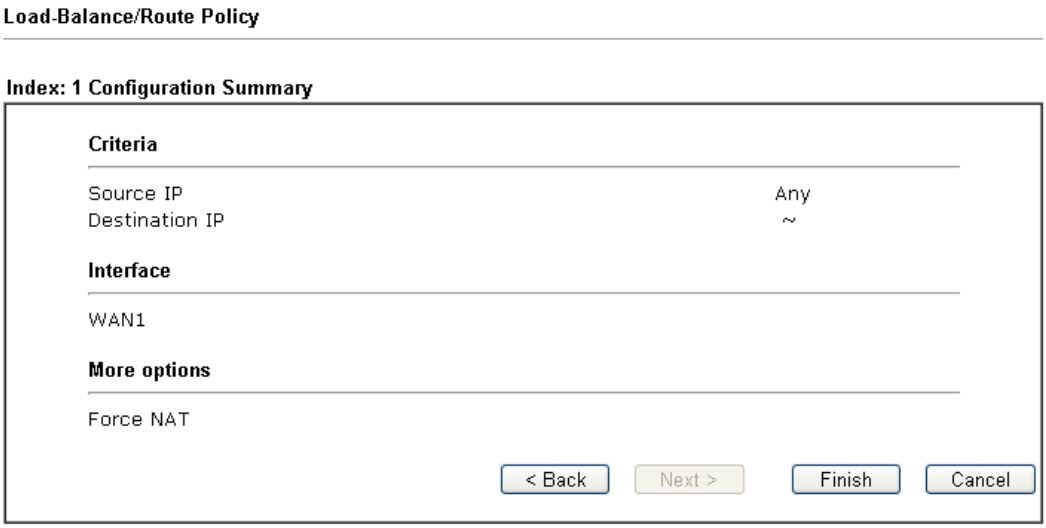
	chosen here. Select an interface from the list.

4. Specify an interface and click **Next.** The following page will appear only if you choose WAN1 ~WAN7 as Interface.

Available settings are explained as follows:

Item	Description
Force NAT /Force Routing	It determines which mechanism that the router will use to forward the packet to WAN.

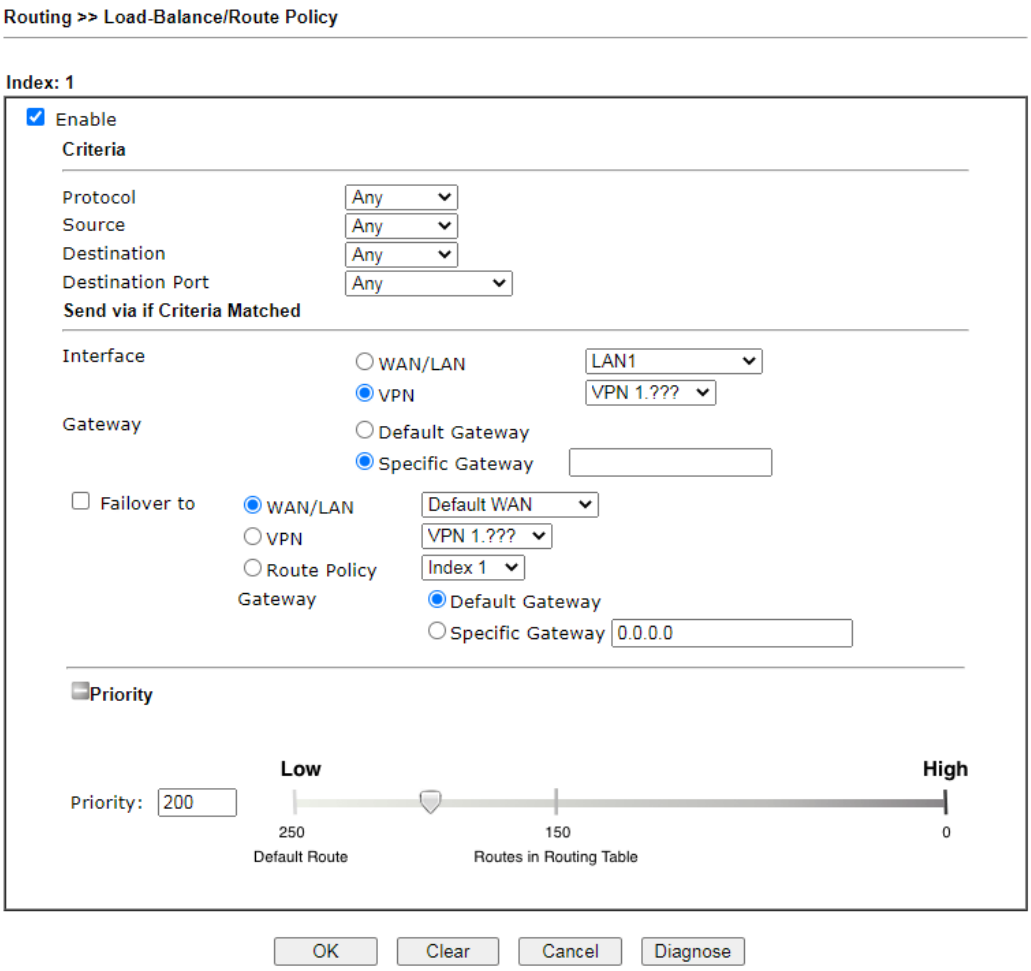
5. After choosing the mechanism, click **Next** to get the summary page for reference.



6. If there is no error, click **Finish** to complete wizard setting. To make changes, click **Back** to return to the previous pages. To discard all changes, click **Cancel**.

If **Advance Mode** is selected, you will be presented with a single page with all the configurable settings for the rule.

1. Click the **Advance Mode** radio button.
2. Click **Index 1** to access into the following page.



Available settings are explained as follows:

Item	Description
Enable	Select to enable rule and unlock all fields for configuration.
Criteria	Router examines outgoing LAN traffic to find the first rule whose criteria are satisfied. **Protocol -** Use the drop-down menu to choose a proper protocol for the WAN interface. **Source -** Source IP addresses to which this rule is to be applied. ● **Any** – This rule applies to all source IP addresses. ● **IP Range** –This rule applies to the specified range of source IP addresses. - **Start** - Enter an address as the starting IP for such profile. - **End** - Enter an address as the ending IP for such profile. ● **IP Subnet** - This rule applies to source IP addresses defined by the specified network IP address and subnet mask.

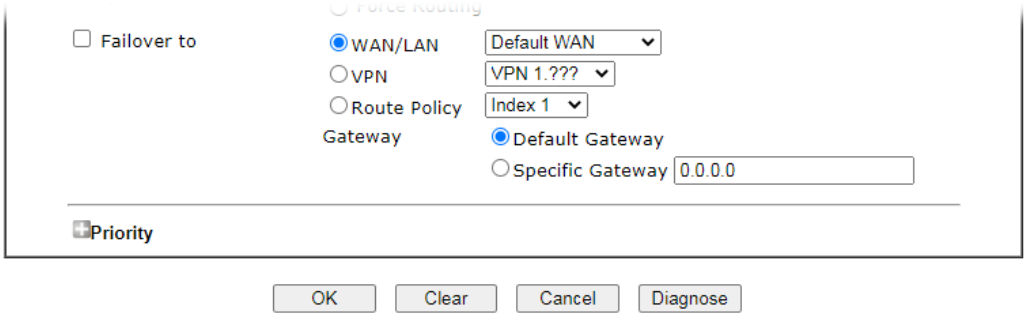
	- **Network** – Enter an IP address here. - **Mask** – Use the drop down list to choose a suitable mask for the network. ● **IP Object / IP Group** – Use the drop down list to choose a preconfigured IP object/group. **Destination -** Destination IP addresses to which this rule is to be applied. ● **Any** – This rule applies to all source IP addresses. ● **IP Range** –This rule applies to the specified range of destination IP addresses. - **Start -** Enter an address as the starting IP for such profile. - **End -** Enter an address as the ending IP for such profile. ● **IP Subnet** - This rule applies to destination IP addresses defined by the specified network IP address and subnet mask. - **Network** – Enter an IP address here. - **Mask** – Use the drop down list to choose a suitable mask for the network. ● **Domain Name** – Specify a domain name as the destination. - **Select** – Click it to choose an existing domain name defined in Objects Setting>>String Object. - **Delete** – Remove current used domain name. - **Add** – Create a new domain name as the destination. ● **IP Object / IP Group** – Use the drop down list to choose a preconfigured IP object/group. **Destination Port** - Destination port numbers to which this rule is to be applied. As only TCP and UDP protocols use port numbers, this setting does not apply to the ICMP protocol. ● **Any** - This rule applies to all destination ports. ● **Dest Port Range** - This rule applies to the specified range of destination ports. - **Start -** Enter the destination port start for the destination IP. - **End -** Enter the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.
Send to if criteria matched	If criteria are matched, the traffic will be sent to the designated interface and gateway. **Interface** – Packets match with the above criteria will be transferred to the interface chosen here. Select an interface from the list (WAN/LAN: A WAN or LAN interface; VPN: A Virtual Private Network; PVC). **Interface Mode** - It is available if WAN is selected as the Interface. **Gateway** – Select a gateway. ● **Default Gateway** - Traffic will be sent to the default gateway address of the specified interface. ● **Specific Gateway** - Traffic will be sent to the

	specified gateway address instead of the default gateway address. **Failover to** – If the interface specified above loses connection, traffic can be forwarded to an alternate interface or be scrutinized by an alternate route policy. ● **WAN/LAN –** Use the drop down list to choose an interface as an auto failover interface. ● **VPN –** Use the drop down list to choose a VPN tunnel as a failover tunnel. ● **Route Policy –** Use the drop down list to choose an existed route policy profile. ● **Gateway** – The failed-over traffic can be sent to the Default Gateway of the alternate interface/route policy, or a Specific Gateway at the specified IP address. **Failback**- When **Failover to** option is enabled, Administrator could also enable **Failback** to clear the existing session on Failover interface and return to the original interface immediately once the original interface resume its service. When Failback is not enabled, the router will only stop sending packets via the Failover interface when the existing sessions are cleared, and this might take a long time because some application will keep sending packet once a while. Therefore, Failback option is recommended if Administrator wants the traffic to go via the primary interface as soon as possible.
Priority	Specifies the priority of the rule in relation to other rules. Lowering the priority value increases the priority of the rule, and vice versa. Routes in the routing table have a priority value of 150, whereas the default routes have a priority value of 250. The default priority value of Load Balance/Route Policy rules is 200. To change the priority, move the slider or enter a value.

3. When you finish the configuration, please click **OK** to save and exit this page.

Diagnose for Route Policy

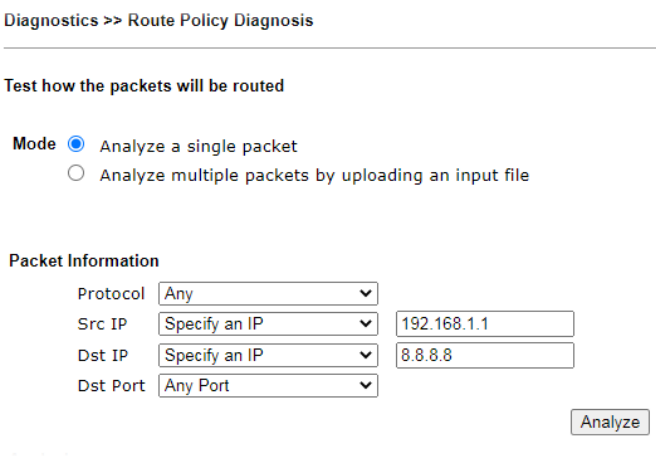
The Diagnose function allows you to determine how a specific type of traffic from a host to a destination will be routed, and which routes, route policies and load balance rules match the criteria of the traffic.



Click **Diagnose**.

Analyze a single packet

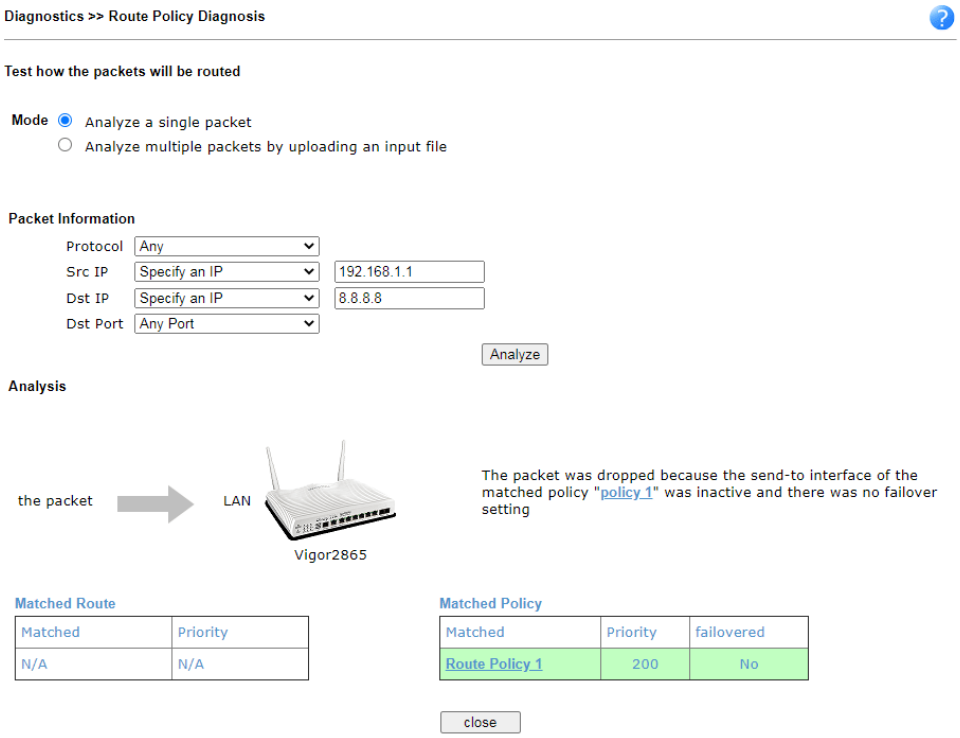
Select this mode to make Vigor router analyze how a single packet will be sent by a route policy.



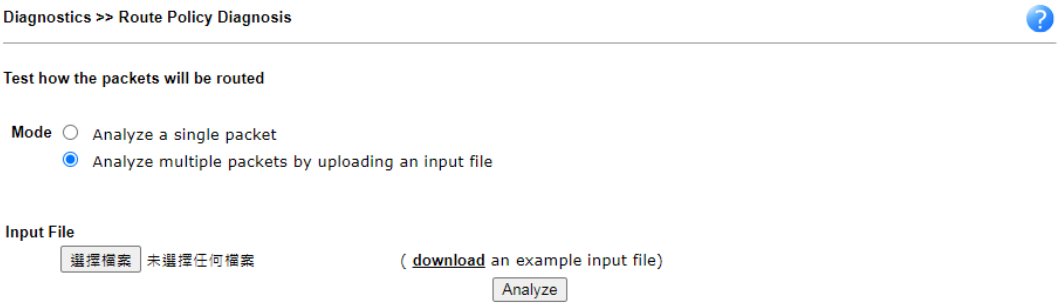
Available settings are explained as follows:

Item	Description
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. **Protocol -** Specify a protocol for diagnosis. **Src IP** – IP address of host where the traffic originates. ● **Specify an IP** - One source IP address. ● **Any IP**- Source IP address is not specified. Any IP from LAN X/IP Routed Subnet. ● **Subnet/IP Routed Subnet** - Any source IP address on the specified subnet. **Dst IP** – IP address of the destination host. ● **Specify an IP** - One destination IP address. ● **Any IP** - Destination IP address is not specified. **Dst Port** – Number of port to which the traffic is sent. This setting is only applicable to UDP and TCP protocols. Use the drop down list to specify the destination port. **Analyze** – Click to analyze and display routes, route policies and load balance rules with matching criteria. If required, click **export analysis** to export the result as a file.

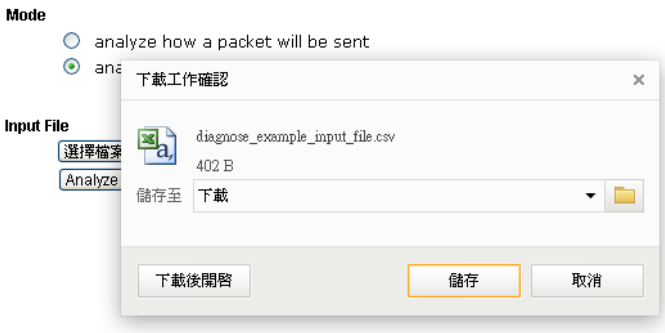
The following shows an analysis example. The packet matched the criteria of one route policy.



Analyze multiple packets by uploading an input file



Available settings are explained as follows:

Item	Description
Input File	**Browse** – Click to browse folder structure and select an input file. **Download and example input file** - Click to download a sample input file (blank ".csv" file). Then, click the Browse button to select that blank ".csv" file for saving the result of analysis.  **Analyze** – After selecting input file, click to start the

	analysis process. Click the **export** button to export the result as a file. Note that the analysis was based on the current "load-balance/route policy" settings, we do not guarantee it will be 100% the same as the real case.

The following shows the analysis of the sample input file. The matched routes and policies are highlighted in green. The Final Result column shows the outcome.

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

Mode ○ Analyze a single packet
● Analyze multiple packets by uploading an input file

Input File
選擇檔案 未選擇任何檔案 (**download** an example input file)
Analyze

Analysis export

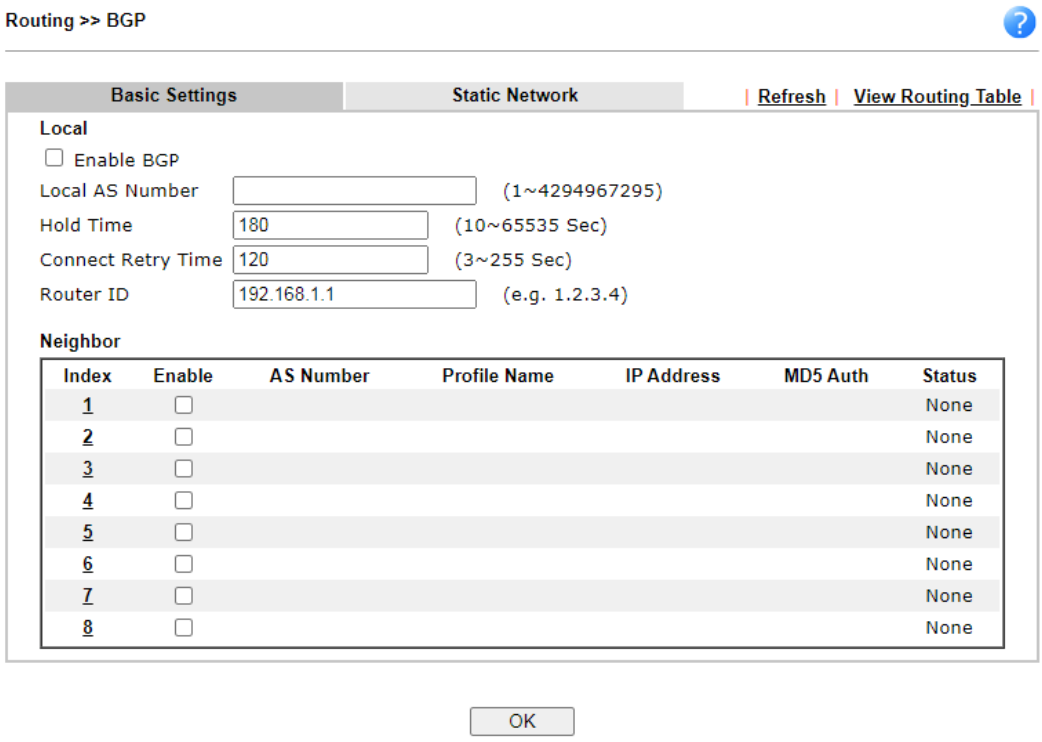
	Input Packet Information				Matched Route		Matched Policy			Final Result	
Profile	Proto	Src IP	Dst IP	Dst Port	Route	Priority	Policy	Priority	failovered	Interface	Reason
LA-branch	ICMP	192.168.1.10	10.10.10.10	Any	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because neither "route" or "policy" was matched
NY-branch	TCP	192.168.1.20	20.20.20.20	5060	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because neither "route" or "policy" was matched
NZ	UDP	192.168.1.20	20.20.20.20	5060	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because

II-5-3 BGP

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

II-5-3-1 Basic Settings

Set general settings for for local router and neighboring routers.



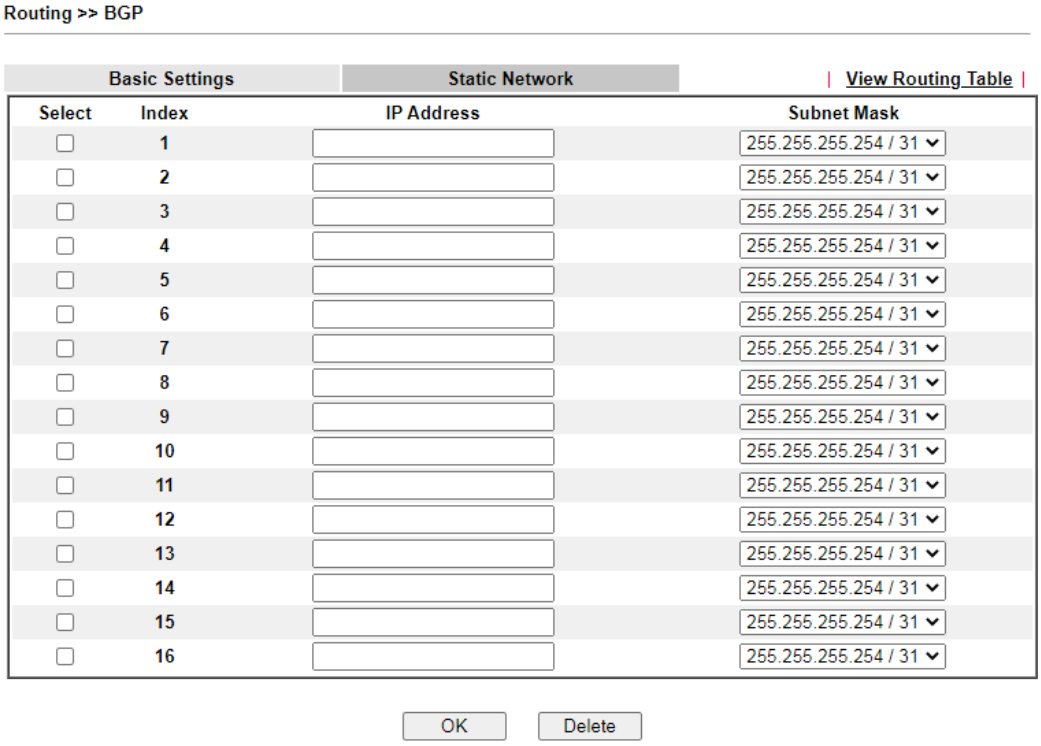
Available settings are explained as follows:

Item	Description
Local	
Enable BGP	Check the box to enable basic BGP function for local router.
Local AS Number	Set the AS number for local router.
Hold Time	Set the time interval (in seconds) to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time.
Connect Retry Time	If the router fails to connect to neighboring router, it requires a period of time to reconnect. Set the time interval to do reconnection.
Router ID	Specify the LAN subnet for the router.
Neighbor	
Enable	Check the box to enable the basic BGP function for neighboring router.
Index	Click the index number link to configure neighbor profile.

AS Number	Display the AS Number for neighboring router.
Profile Name	Display the name of the neighboring profile.
IP Address	Display the IP address specified for the neighboring profile.
MD5 Auth	Display the status (enabled or disabled) of MD5 authentication.
Status	Display the connection status for local router and neighboring router.

II-5-3-2 Static Network

This page allows you to configure up to eight neighboring routers for exchanging the routing information with the local router.



Available settings are explained as follows:

Item	Description
Select	Check the box to enable the configuration for the selected index entry.
IP Address	Enter the IP address for a router.
Subnet Mask	Use the drop down list to specify a subnet mask for the IP address.

This page is left blank.

Part III Wireless LAN

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

III-1 Wireless LAN

This function is used for "n" model only.

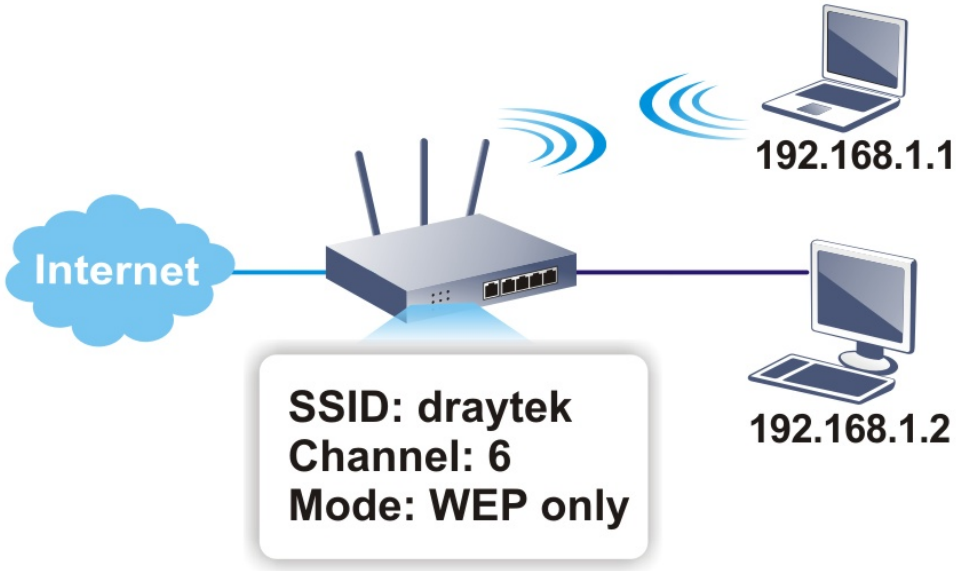
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The VigorLTE 200 wireless series router (with "n", or "ac" in model name) is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

VigorLTE 200 wireless router is a highly integrated wireless local area network (WLAN) for 5 GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80 MHz at 5 GHz. VigorLTE 200 "ac" series router can support data rates up to 1.3 Gbps in 802.11ac 80 MHz channels. VigorLTE 200 "n" series router supports 802.11n up to 300 Mbps for 40 MHz channel operations.

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

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Multiple SSIDs

Vigor router supports four SSID settings for wireless connections. Each SSID can be defined with different name and download/upload rate for selecting by stations connected to the router wirelessly.

Real-time Hardware Encryption

Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

Complete Security Standard Selection

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

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

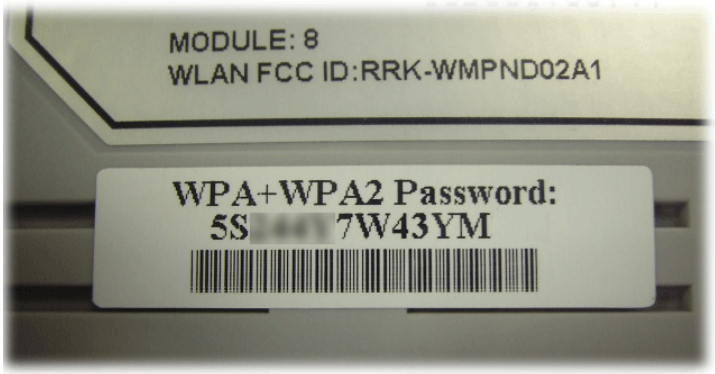
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Info

The password (PSK) of default security mode is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



Separate the Wireless and the Wired LAN- WLAN Isolation

It enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List

It will display all the stations in your wireless network and the status of their connection.

WPS

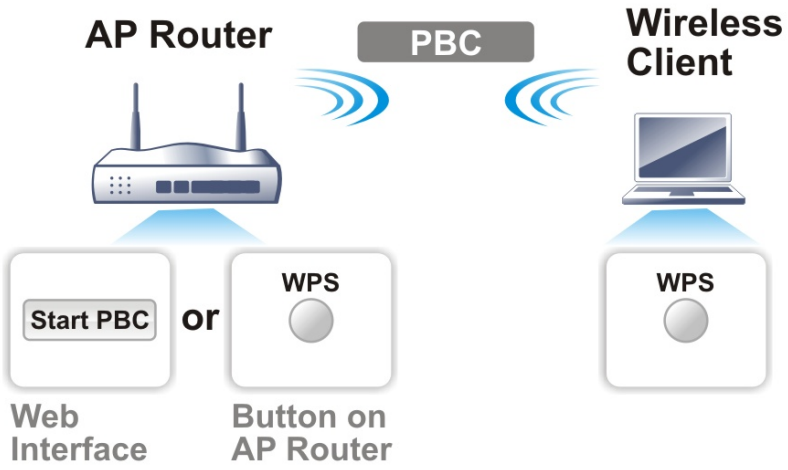
WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

Info	WPS is available for the wireless station with WPS supported.

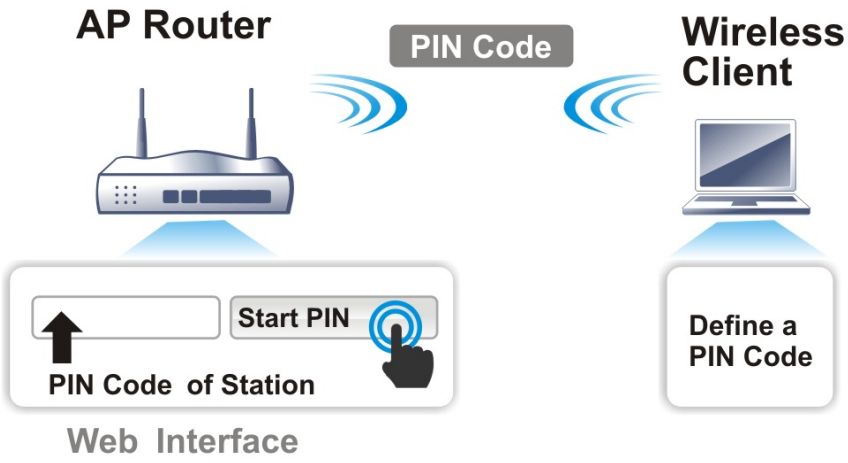
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

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

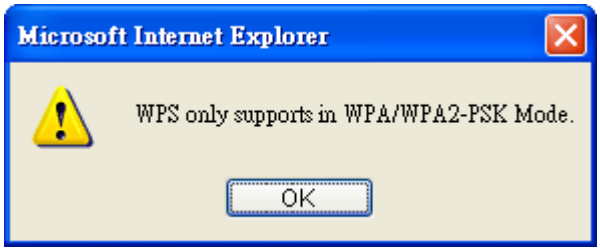
- On the side of VigorLTE 200 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



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

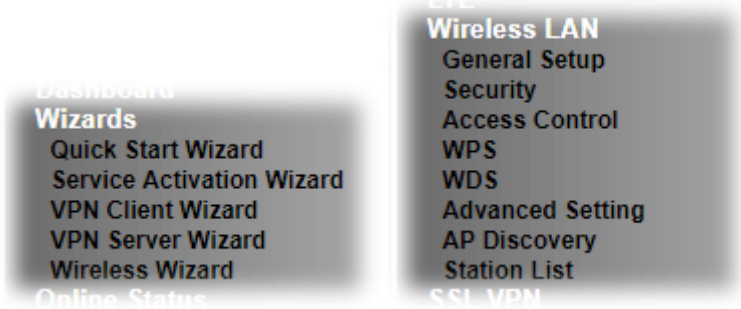


For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

Web User Interface

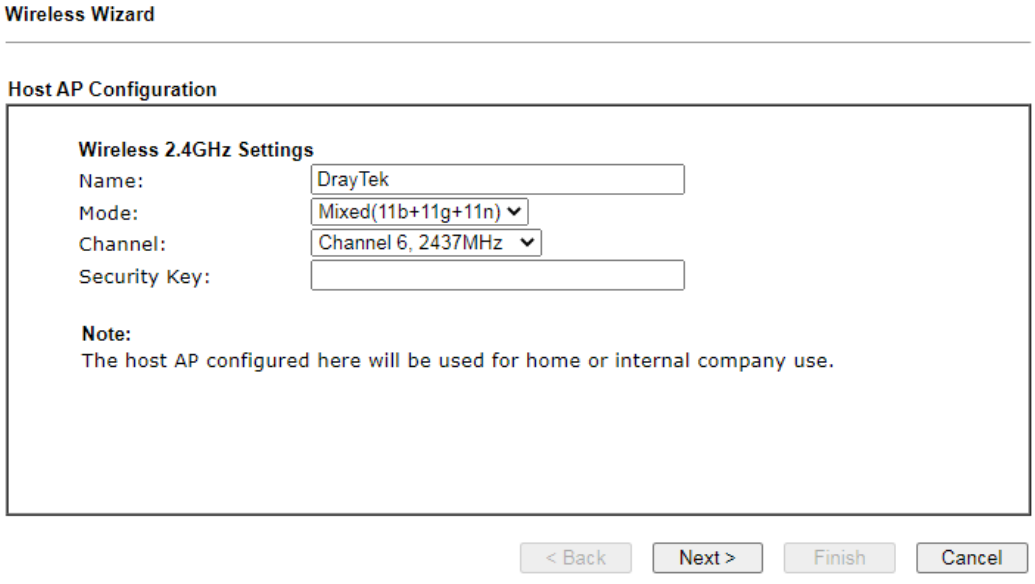


III-1-1 Wireless Wizard

The wireless wizard allows you to configure settings specified for a host AP (for home use or internal use for a company) and specified for a guest AP (for any wireless clients accessing into Internet).

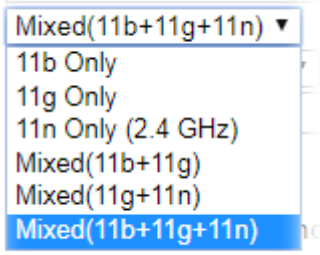
Follow the steps listed below:

1. Open **Wizards>>Wireless Wizard**.
2. The screen of wireless wizard will be shown as follows. This page will be used for internal users in a company or your home. Besides, the settings will change based on different model of VigorLTE 200 series. In this case, VigorLTE 200Ln is used as an example.

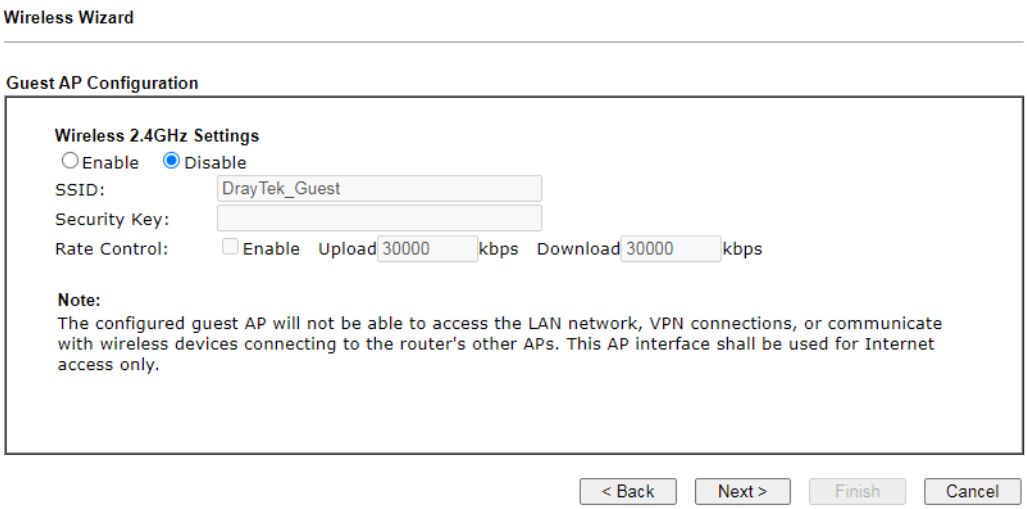


Available settings are explained as follows:

Item	Description
Name	Enter the SSID name of this router for wireless connection. The default name is defined with DrayTek. Change the name if required.
Mode	At present, the router can connect to 11b Only, 11g Only, 11n Only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed

	(11b+11g+11n) mode. 
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde…").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

3. After typing the required information, click **Next**. The settings in the page limit the wireless station (guest) accessing into Internet but not being allowed to share the LAN network and VPN connection.



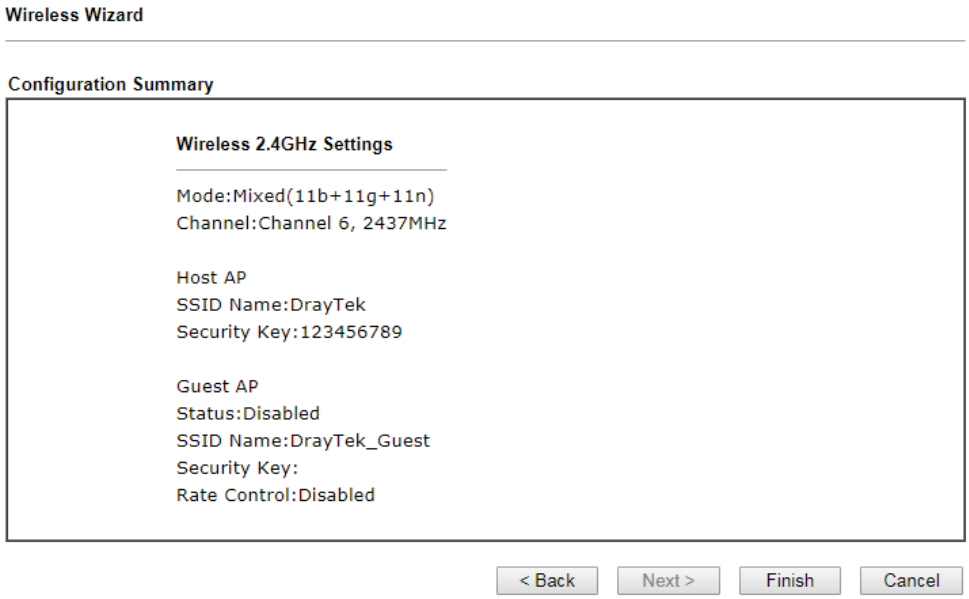
Available settings are explained as follows:

Item	Description
Enable/Disable	Click it to enable or disable settings in this page.
SSID	Enter the SSID name of this router. (SSID1)
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered

	manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Rate Control	Check the box to enable the rate control function. **Upload / Download** - Enter the values as the limits for data upload and data download.
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

4. After typing the required information, click **Next**.

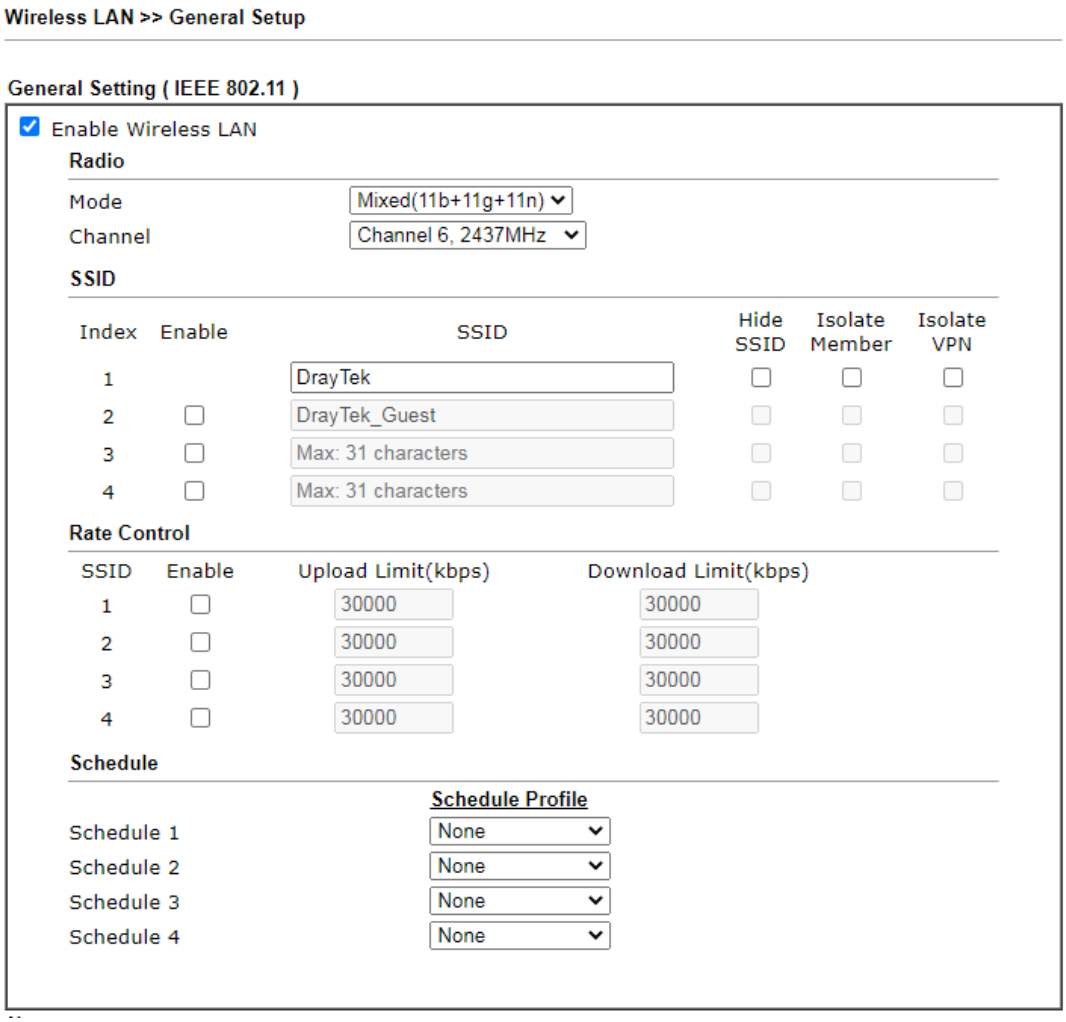
5. The following page will display the configuration summary for wireless setting.



6. Click **Finish** to complete the wireless settings configuration.

III-1-2 General Setup

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



Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	For 2.4GHz: At present, the router can connect to 11b Only, 11g Only, 11n Only(2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN.

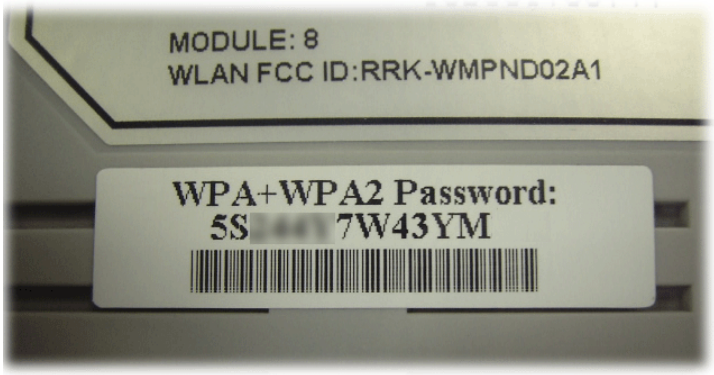
	Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
Isolate	**Member** –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. **VPN** – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.
Rate Control	**Enable** – Check the box to set the rate limit for data transmission in upload and download. It controls the data transmission rate through wireless connection. **Upload** – Check Enable and enter the transmitting rate for data upload. Default value is 30,000 kbps. **Download** – Enter the transmitting rate for data download. Default value is 30,000 kbps.
Schedule Profile	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.

After finishing all the settings here, please click **OK** to save the configuration.

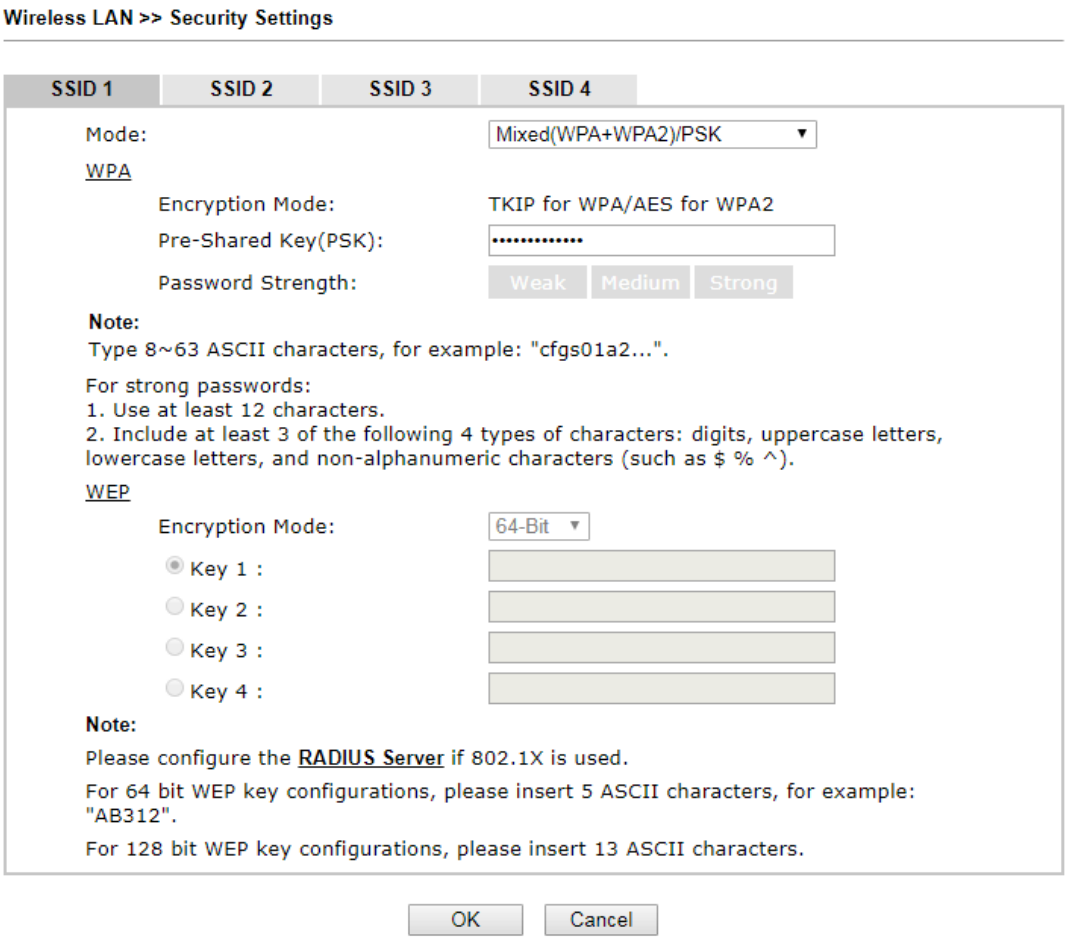
III-1-3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

The password (PSK) of default security mode is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



By clicking the **Wireless LAN>>Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.



Available settings are explained as follows:

Item	Description

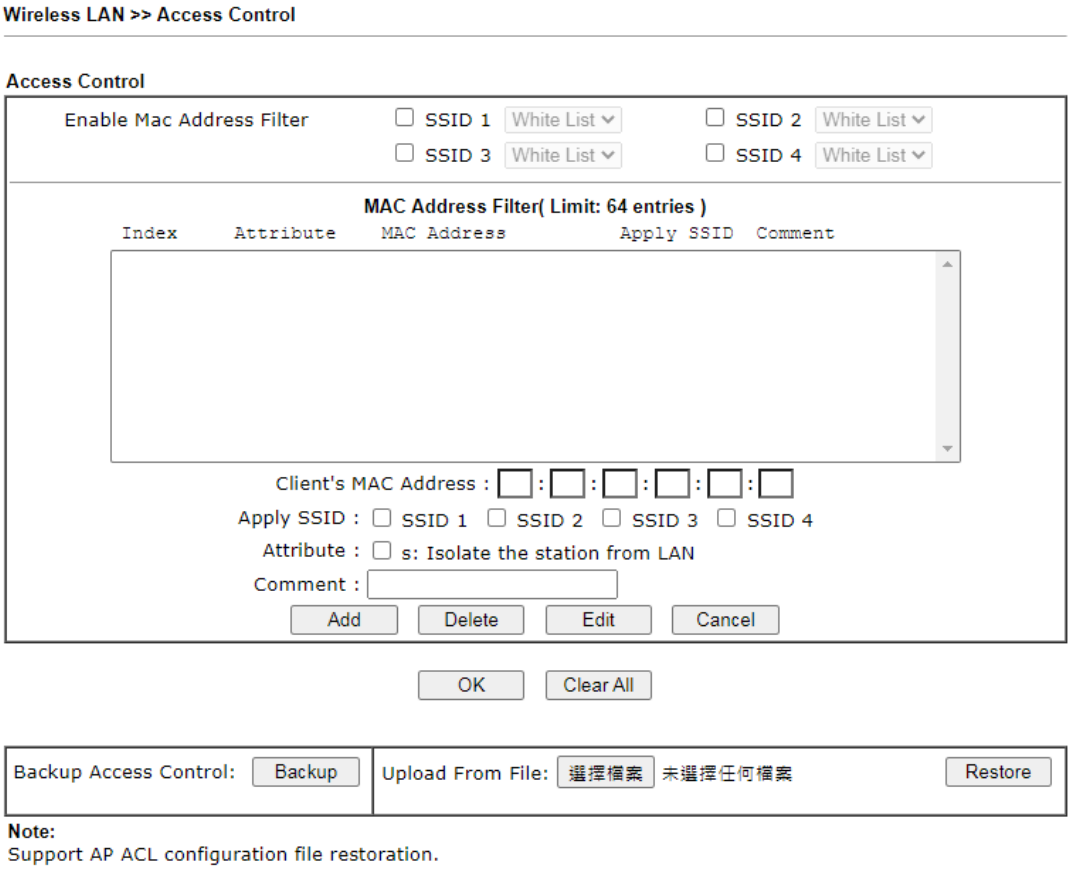
Mode	There are several modes provided for you to choose.  **Info** You should also set **RADIUS Server** simultaneously if 802.1x mode is selected. **Disable** - Turn off the encryption mechanism. **WEP -** Accepts only WEP clients and the encryption key should be entered in WEP Key. **WEP/802.1x Only -** Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **WPA/802.1x Only -** Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **WPA2/802.1x Only -** Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **Mixed (WPA+WPA2/802.1x only) -** Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **WPA/PSK -** Accepts only WPA clients and the encryption key should be entered in PSK. **WPA2/PSK -** Accepts only WPA2 clients and the encryption key should be entered in PSK. **Mixed (WPA+ WPA2)/PSK -** Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). **Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). **Password Strength** – The system will display the password strength (represented with the word of weak, medium or strong) of the PSK specified above.
WEP	**64-Bit** - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.) **128-Bit** - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D). All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

After finishing all the settings here, please click **OK** to save the configuration.

III-1-4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.



Available settings are explained as follows:

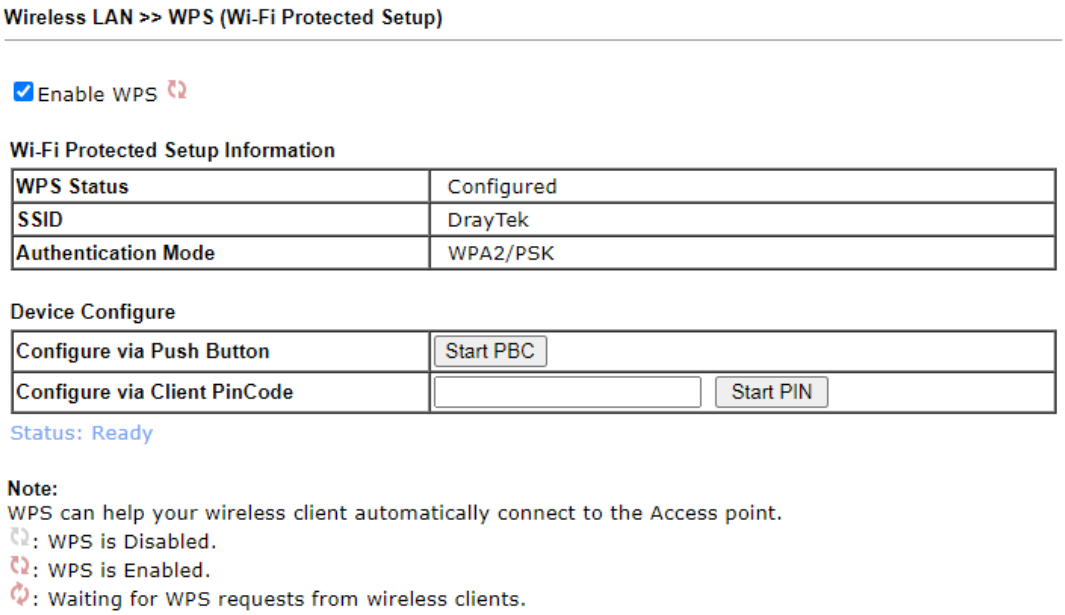
Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	**s: Isolate the station from LAN -** select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Comment	Enter a brief description for the specified client's MAC

	address.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.
Backup Access Control	Settings on this web page can be saved as a file which can be restored in the future by this device or other device.
Upload From File	Restore wireless access control settings and applied onto this device.

After finishing all the settings here, please click **OK** to save the configuration.

III-1-5 WPS

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



Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

III-1-6 WDS

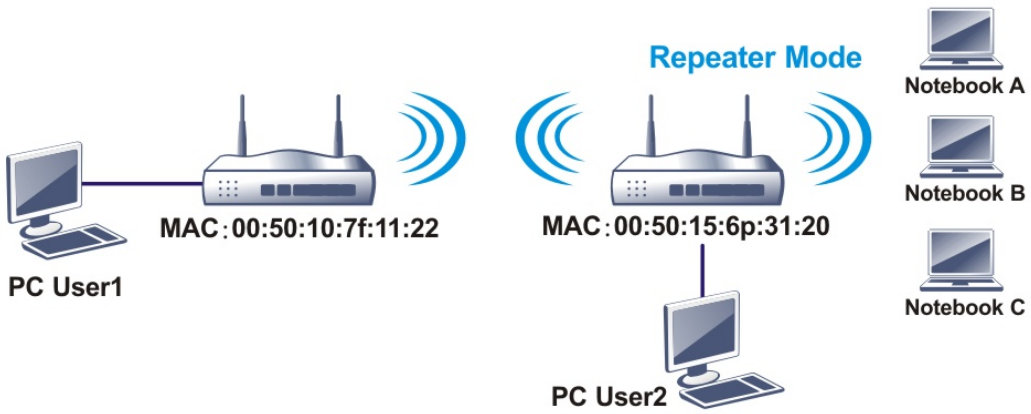
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

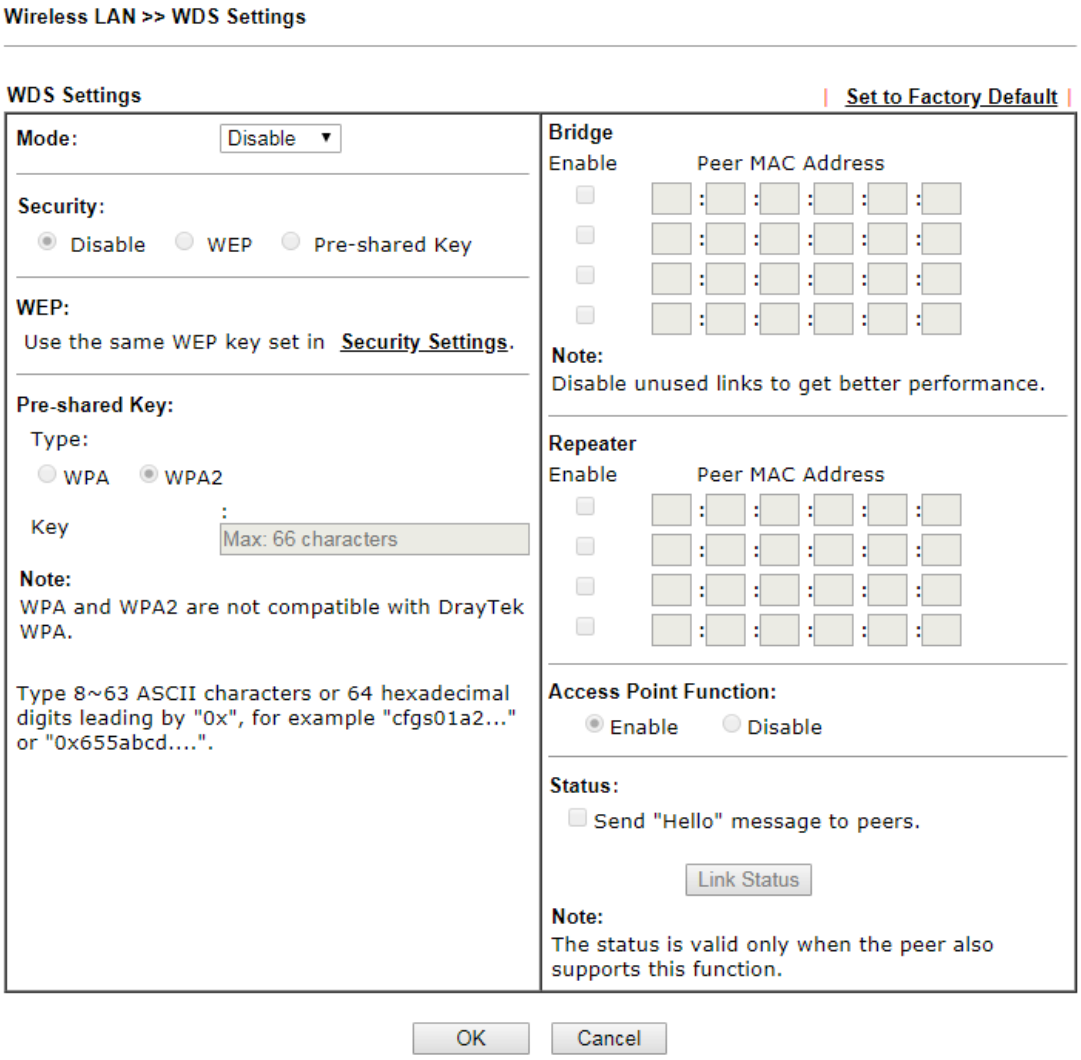
Refer to the following table:

WDS Mode	Wireless Signal	Comparisons
Bridge	Limited	● Wireless stations (clients) within the effective range of wireless signal can access into Internet through the router /AP. ● Wireless stations (clients) out of the effective range of wireless signal **cannot** access into Internet through the router /AP with Bridge mode configured. ● The packets received from a WDS link will only be forwarded to local wired or wireless hosts.
Repeater	Extended	● Wireless stations (clients) within the effective range of wireless signal can access into Internet through the router /AP. ● Wireless stations (clients) out of the effective range of wireless signal **can access** into Internet through the router /AP with Repeater mode configured. ● The packets received from one Vigor router can be repeated to another AP (remotely) through WDS links. ● Only Repeater mode can do WDS-to-WDS packet forwarding.

The WDS - Repeater mode is implemented in Vigor router. The application for the WDS-Repeater mode is depicted as below:



Click **WDS** from **Wireless LAN** menu. The following page will be shown.



Available settings are explained as follows:

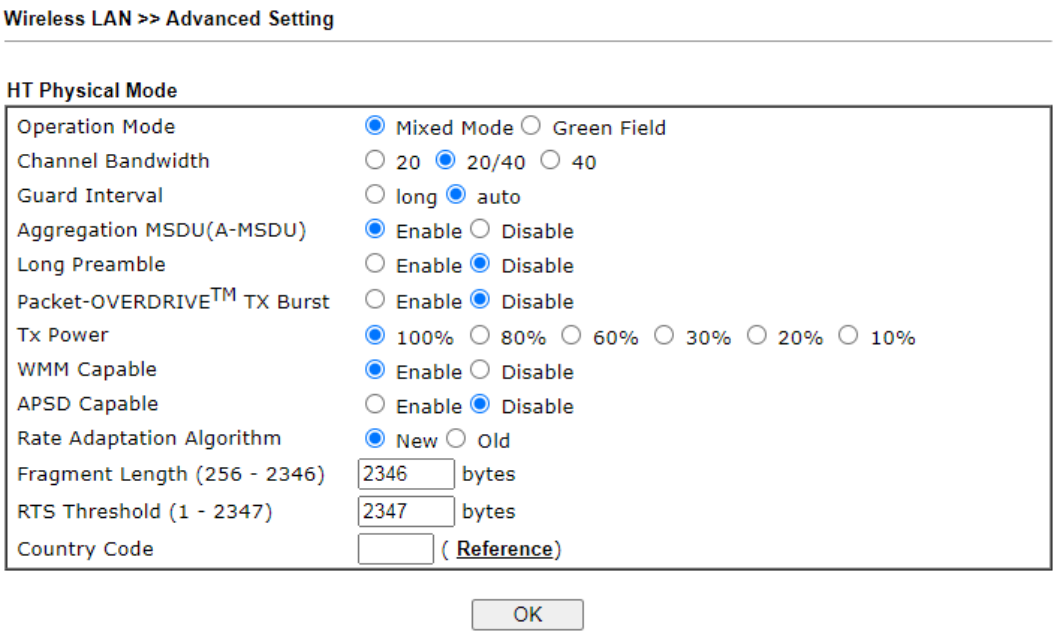
Item	Description
Mode	Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Repeater** mode is for the second one.
Security	There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
Pre-shared Key	When **Pre-Shared Key** is selected as Security above, configure the following settings if required. **Type –** There are some types for you to choose. **WPA** and **WPA2** are used for WDS devices (e.g.2925n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. **Key –** Set the encryption key in this field. Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.
Bridge	If you choose Bridge as the connecting mode, please Enter the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better

	performance. If you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.
Repeater	If you choose **Repeater** as the connecting mode, please Enter the peer MAC address (of VigorAP/Vigor router required to make connection with such Vigor router and used to extend the wireless signal) in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.
Access Point Function	Click **Enable** to make this router serve as an access point. When **Repeater** is set as WDS Mode, click **Enable** to use such function. Click **Disable** if **Bridge** is set as WDS Mode.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

After finishing all the settings here, please click **OK** to save the configuration.

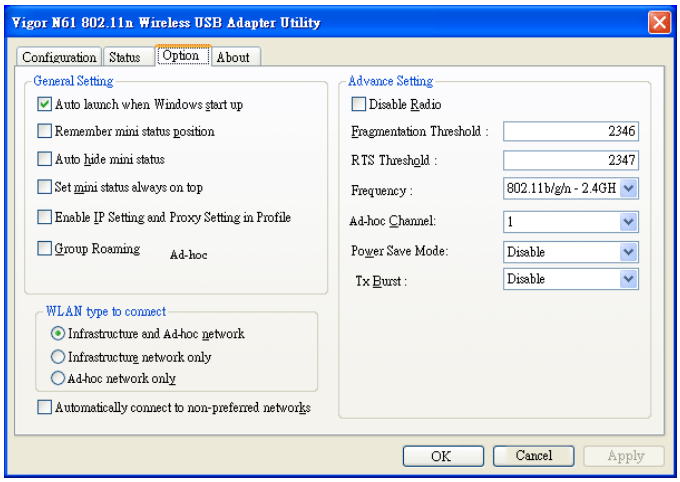
III-1-7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.



Available settings are explained as follows:

Item	Description
Operation Mode	**Mixed Mode** – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected. **Green Field** – to get the highest throughput, please choose such mode. Such mode can make the data transmission happen between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.
Channel Bandwidth	Vigor router will use 20MHz/40MHz/80MHz for data transmission and receiving between the AP and the stations. **20/40-** Vigor Router will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose **auto** as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is **Enable.**
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click **Enable** to

	use **Long Preamble** if needed to communicate with this kind of devices.
Packet-OVERDRIVE TX Burst	This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too. Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose Enable for TxBURST on the tab of Option). 
TX Power	Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be.
WMM Capable	WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM. To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
APSD Capable	APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. The default setting is **Disable**.
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.
Fragment Length (256 - 2346)	Set the Fragment threshold. Do not modify default value if you don’t know what it is, default value is 2346.
RTS Threshold (1 - 2347)	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold. Do not modify default value if you don’t know what it is, default value is 2347.

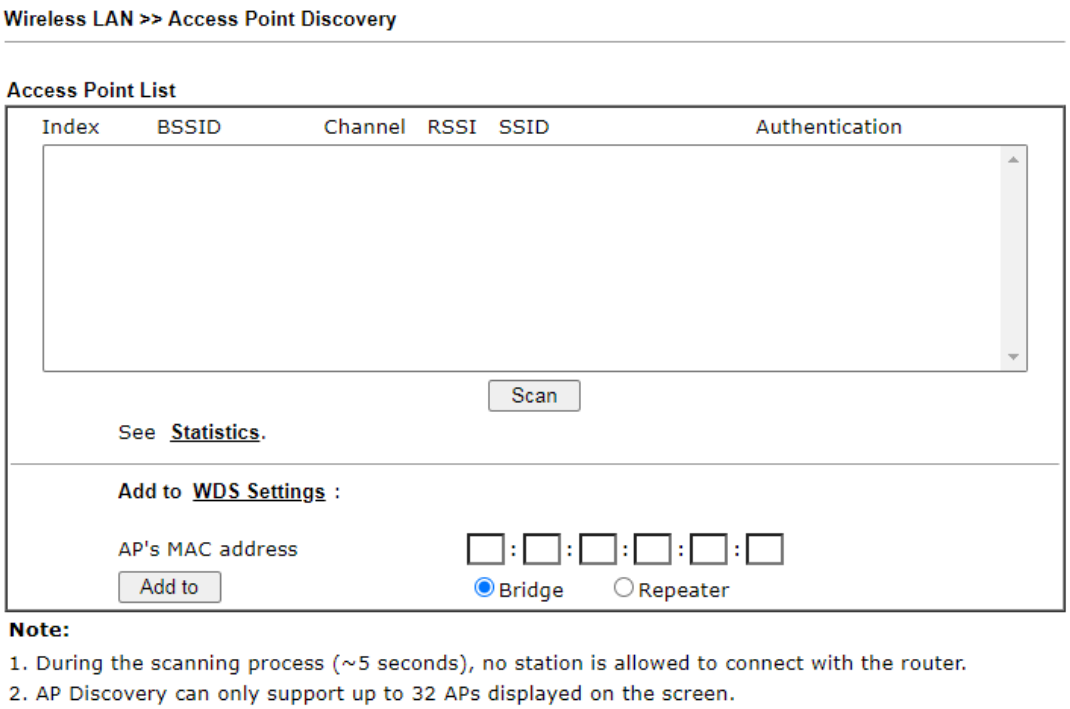
Country Code	Vigor router broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.

After finishing all the settings here, please click **OK** to save the configuration.

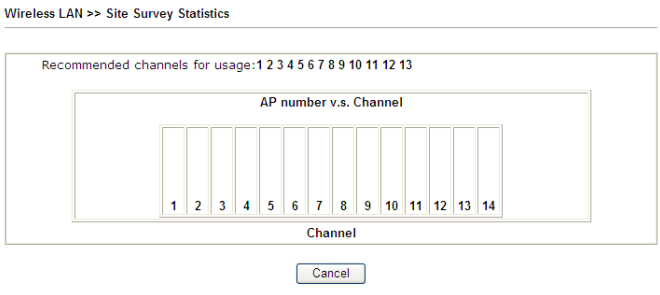
III-1-8 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

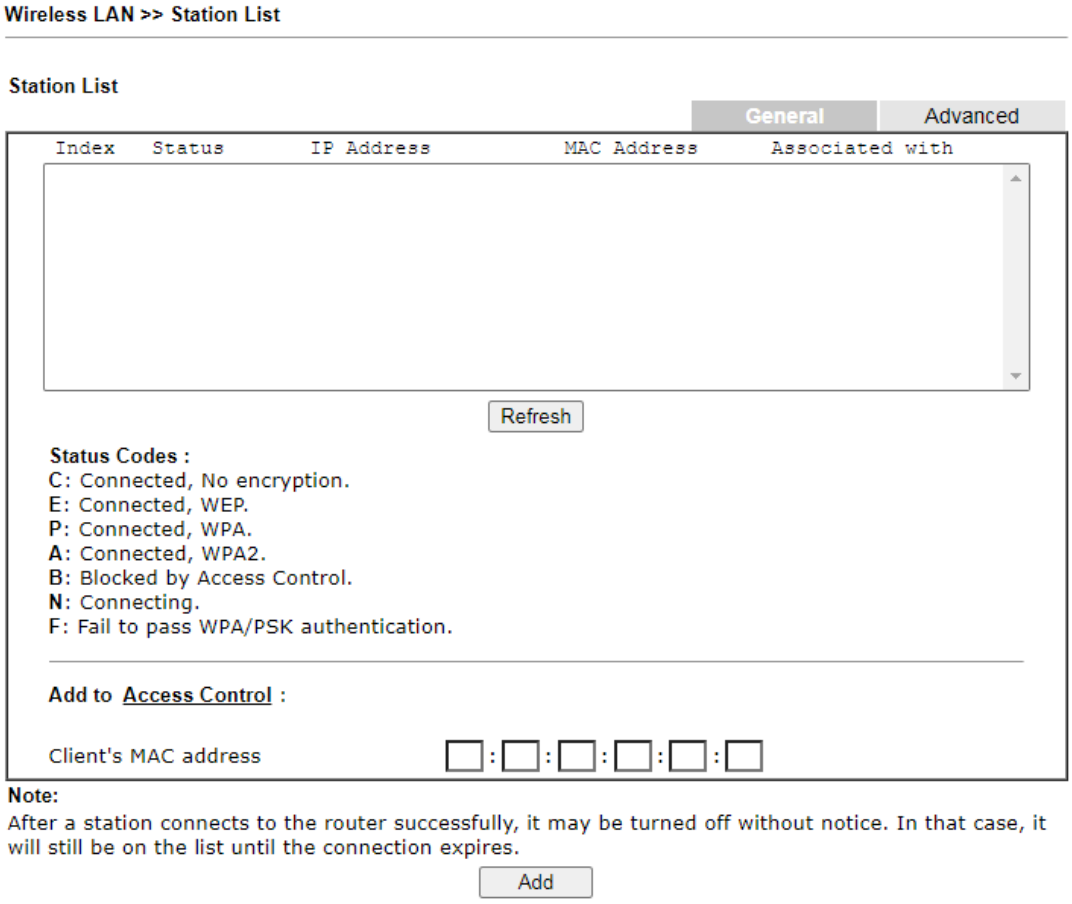


Available settings are explained as follows:

Item	Description
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs. 
Add to	If you want the found AP applying the WDS settings, please Enter the AP's MAC address on the bottom of the page and click Repeater. Next, click **Add to**. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

III-1-9 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.



Available settings are explained as follows:

Item	Description
Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into **Access Control.**

This page is left blank.

Part IV VPN

VPN

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

SSL VPN

It is a form of VPN that can be used with a standard Web browser.

Certificate Management

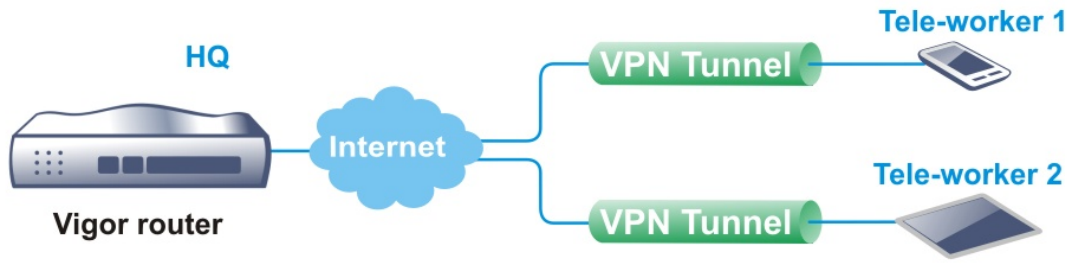
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

IV-1 VPN and Remote Access

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

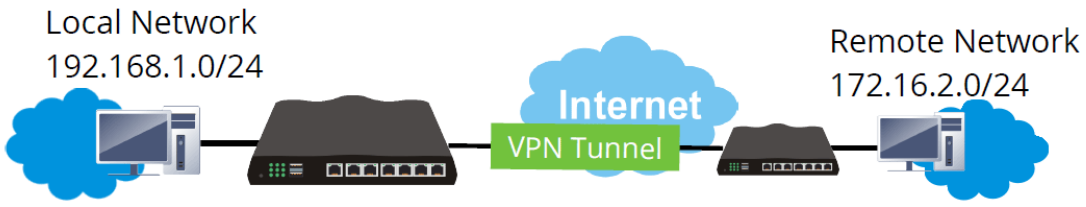
The VPN built is suitable for:

- Communication between home office and customer
- Secure connection between Teleworker, staff on business trip and main office
- Exchange data between remote office and main office
- POS between chain store and headquarters



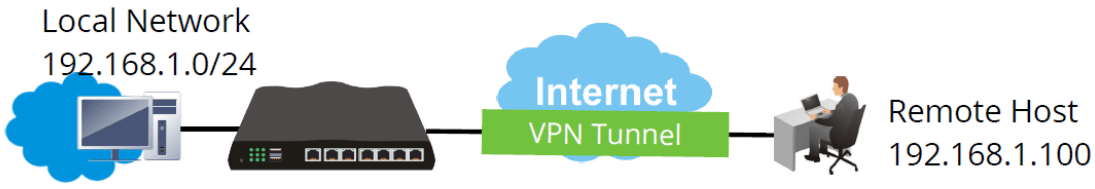
Site-to-Site (LAN-to-LAN)

- A connection between two router's LAN networks.
- Allows employees in branch offices and head office to share the same network resources.

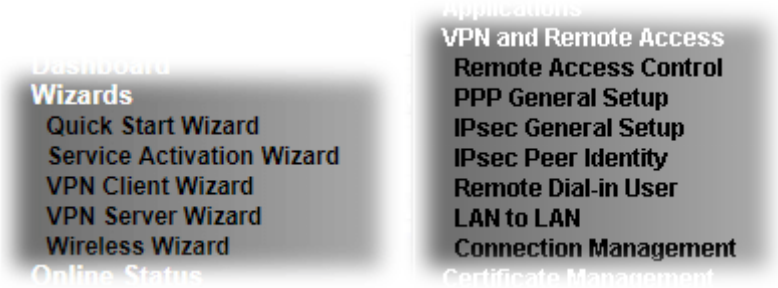


Remote Access (Remote Dial-in)

- A connection between the remote host and router's LAN network. The host will use an IP address in the local subnet.
- Allows employees to access the company's internal resources when they are traveling.



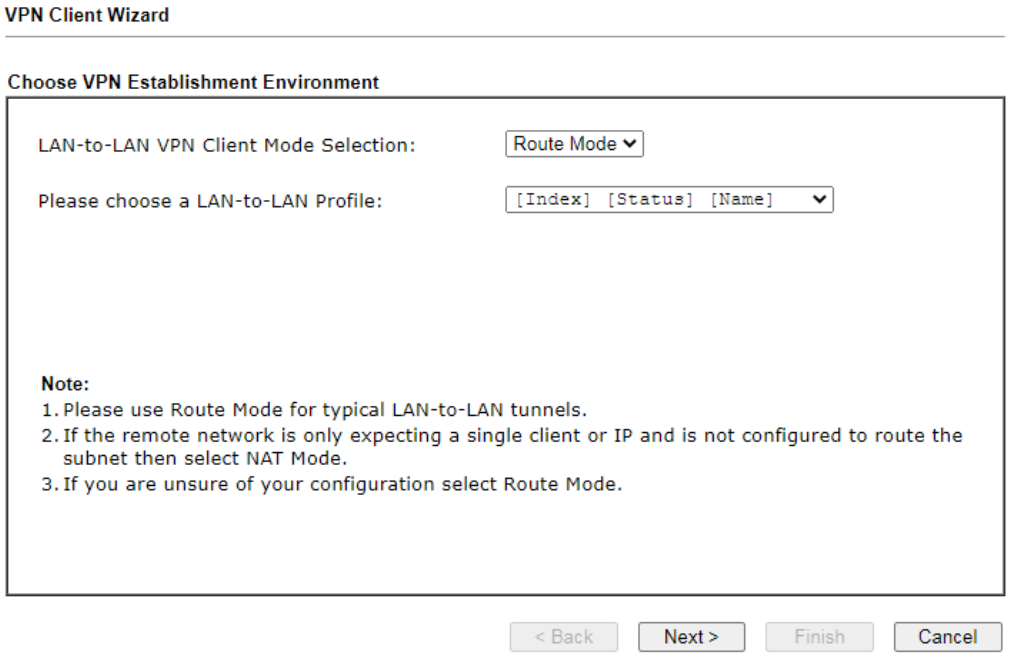
Web User Interface



IV-1-1 VPN Client Wizard

Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

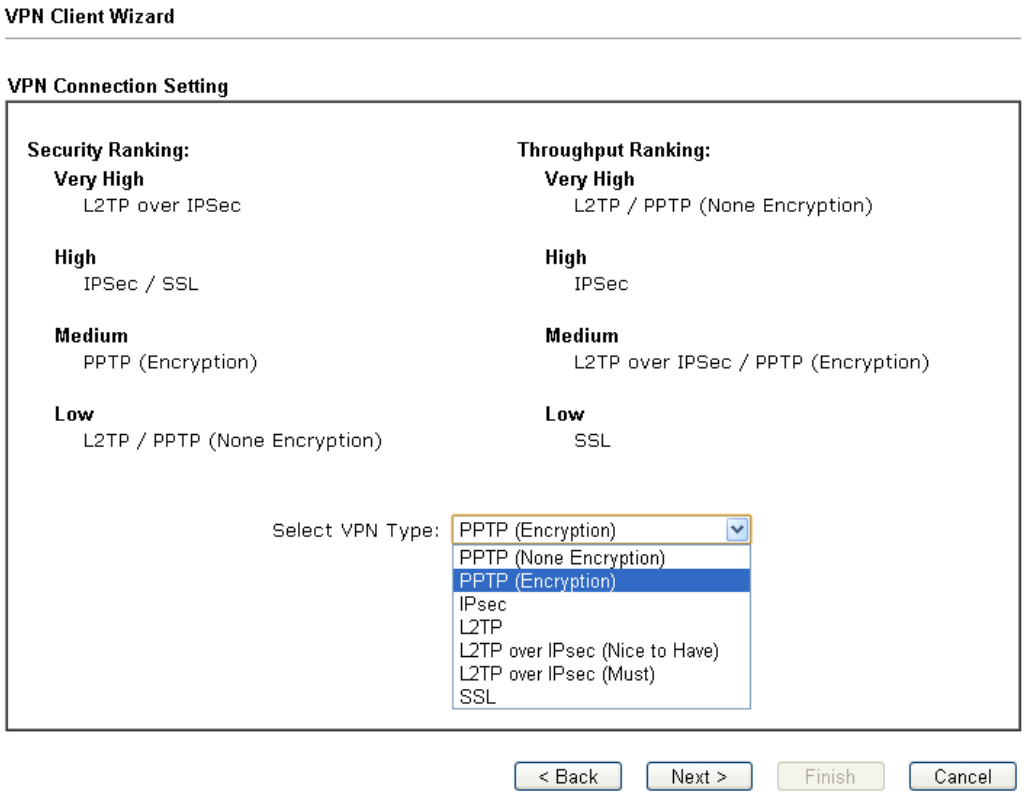
1. Open **Wizards>>VPN Client Wizard**. The following page will appear.



Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. **Route Mode/NAT Mode** – If the remote network only allows you to dial in with single IP, please choose NAT mode, otherwise please choose Route Mode.
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.

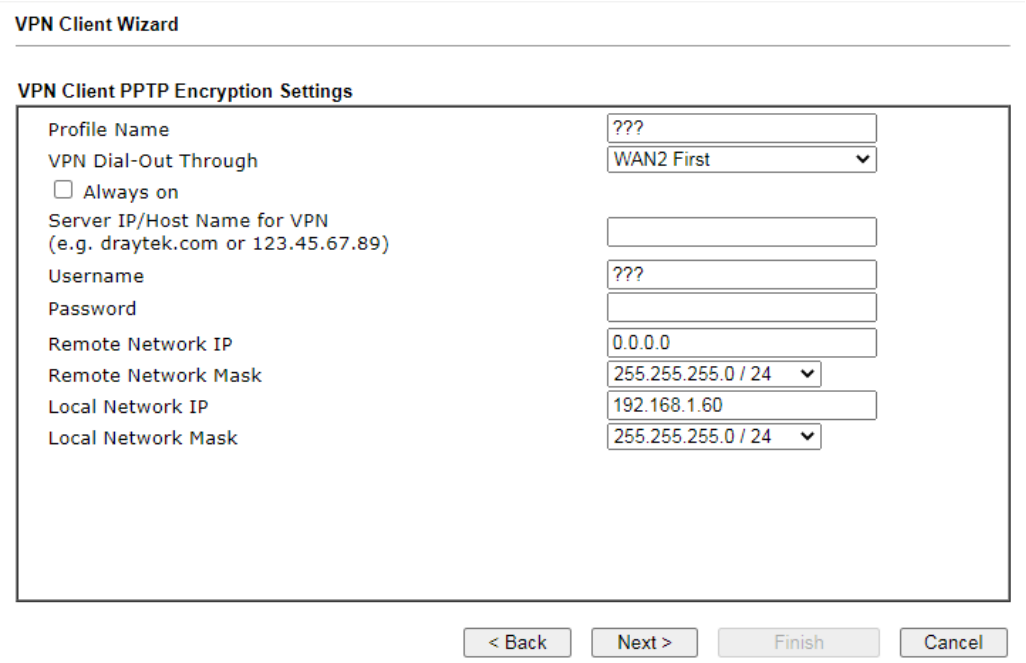
2. When you finish the mode and profile selection, please click **Next** to open the following page.



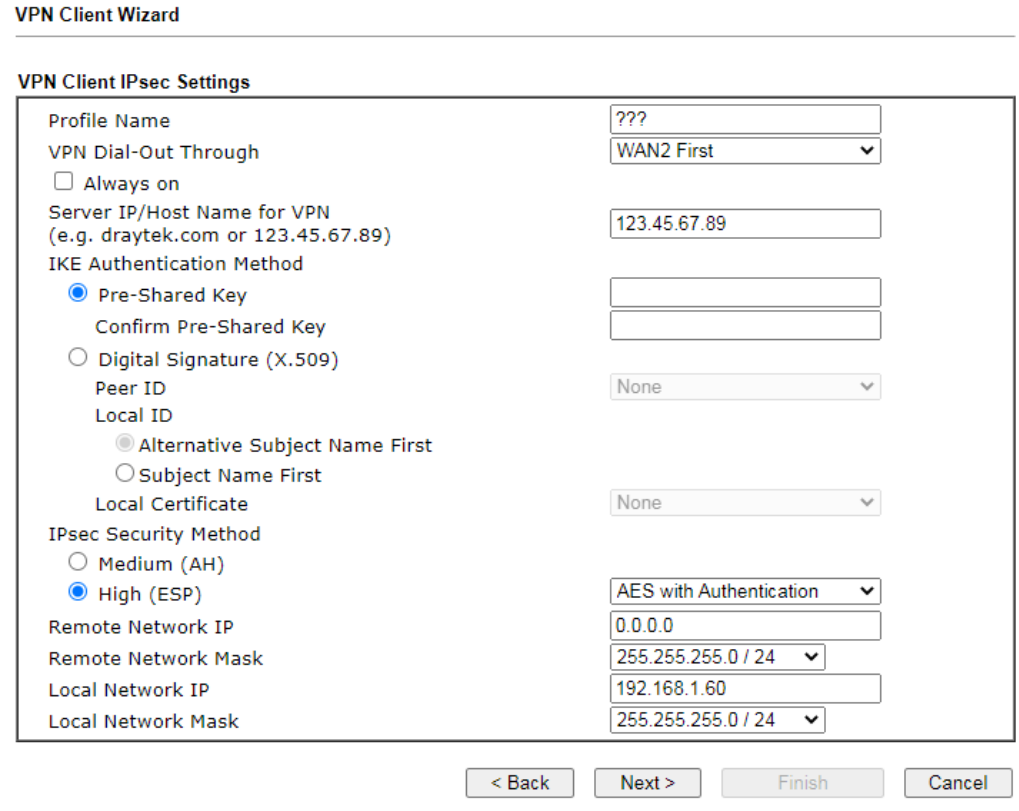
In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

Info	The following descriptions for VPN Type are based on the Route Mode specified in LAN-to-LAN Client Mode Selection.

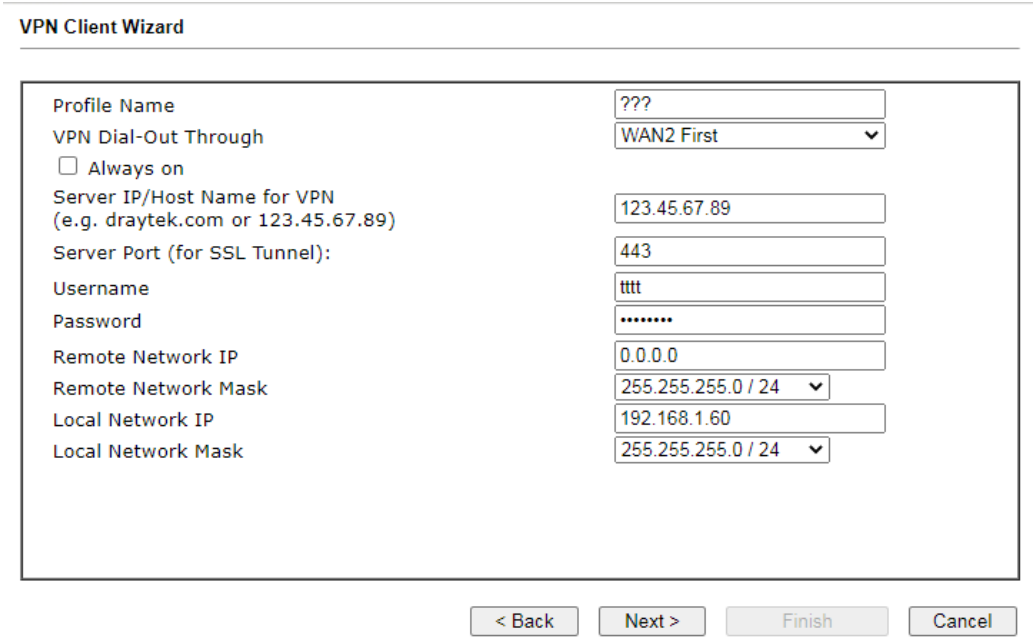
When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:



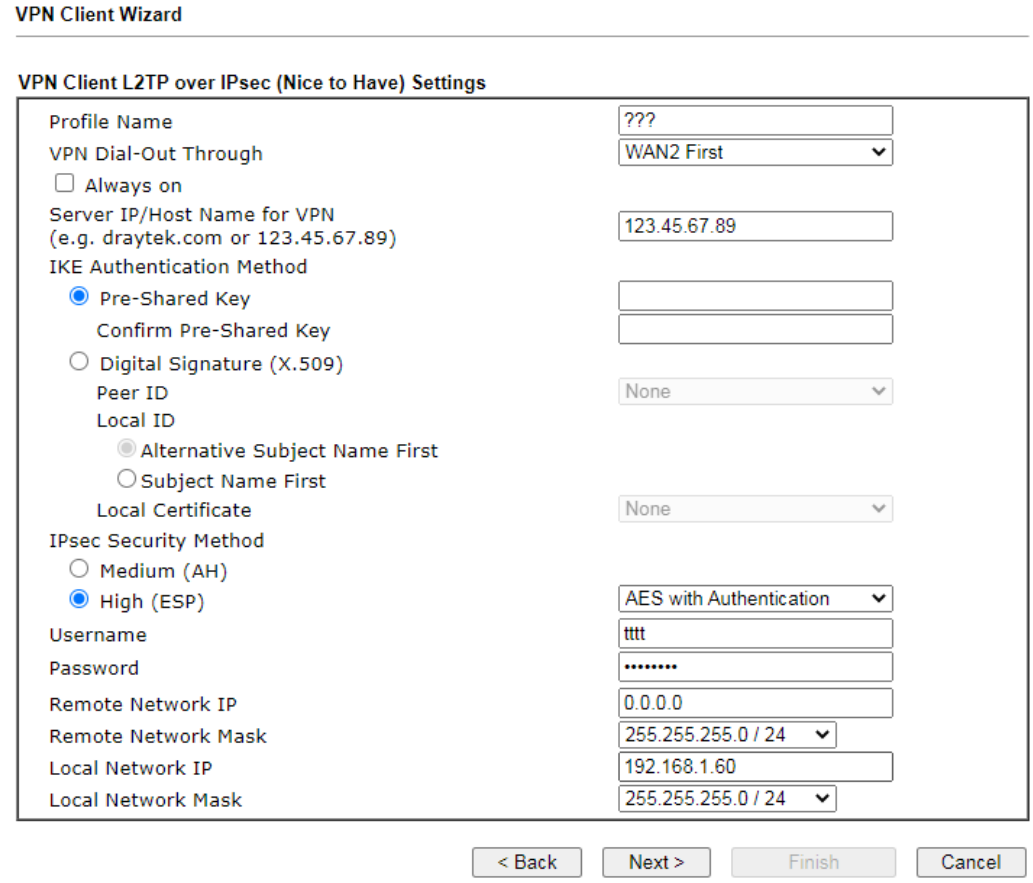
When you choose **IPsec**, you will see the following graphic:



When you choose **SSL**, you will see the following graphic:



When you choose **L2TP over IPsec (Nice to Have)** or **L2TP over IPsec (Must),** you will see the following graphic:

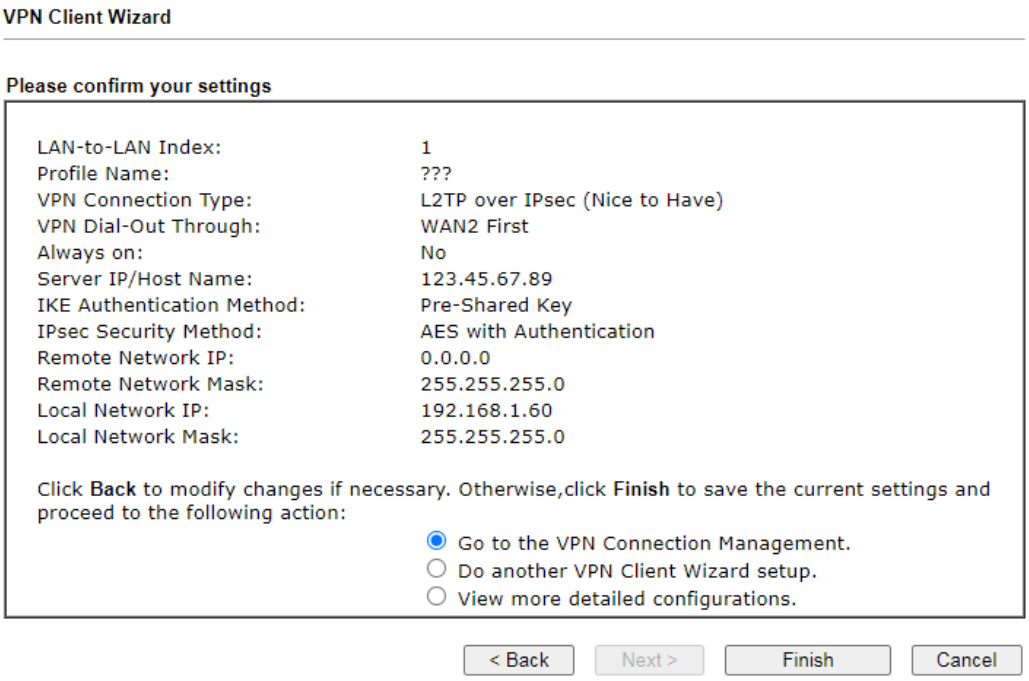


Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited

	to 10 characters.
Always On	Check to enable router always keep VPN connection.
Server IP/Host Name for VPN	Enter the IP address of the server or Enter the host name for such VPN profile.
IKE Authentication Method	IKE Authentication Method usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. **Pre-Shared Key-** Specify a key for IKE authentication. **Confirm Pre-Shared Key-**Confirm the pre-shared key.
Digital Signature (X.509)	Click **Digital Signature** to invoke this function. **Peer ID** – Choose the peer ID selection from the drop down list. **Local ID** – Choose **Alternative Subject Name First** or **Subject Name First**. **Local Certificate** – Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in **Certificate Management >> Local Certificate.** Otherwise, the setting you choose here will not be effective.
IPsec Security Method	**Medium** - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **High** - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the user name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please Enter the network mask (according to the real location of the remote host) for building VPN connection.
Local Network IP	Enter the local network IP for TCP / IP configuration.
Local Network Mask	Enter the local network mask for TCP / IP configuration.

3. After finishing the configuration, please click **Next.** The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.



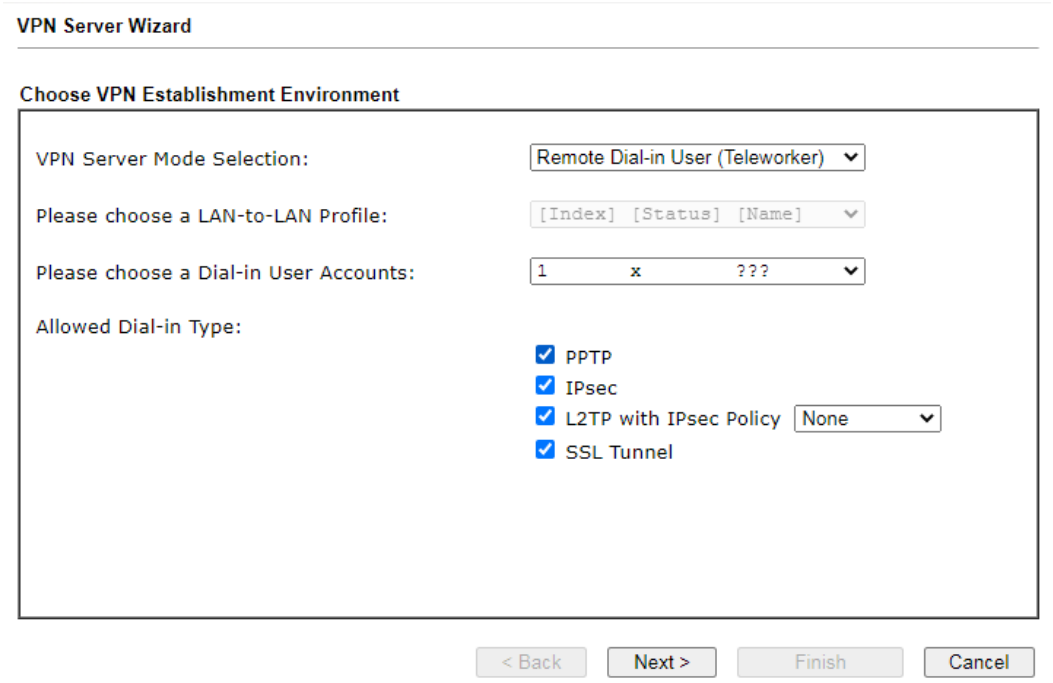
Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access **VPN and Remote Access>>Connection Management** for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access **VPN and Remote Access>>LAN to LAN** for viewing detailed configuration.

IV-1-2 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

1. Open **Wizards>>VPN Server Wizard**. The following page will appear.

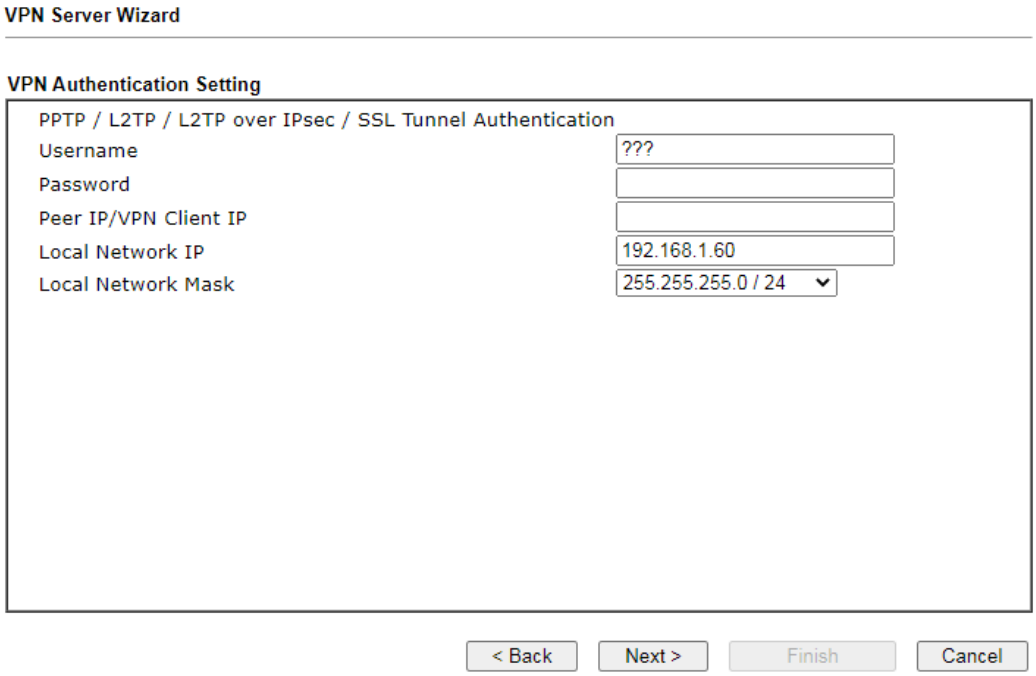


Available settings are explained as follows:

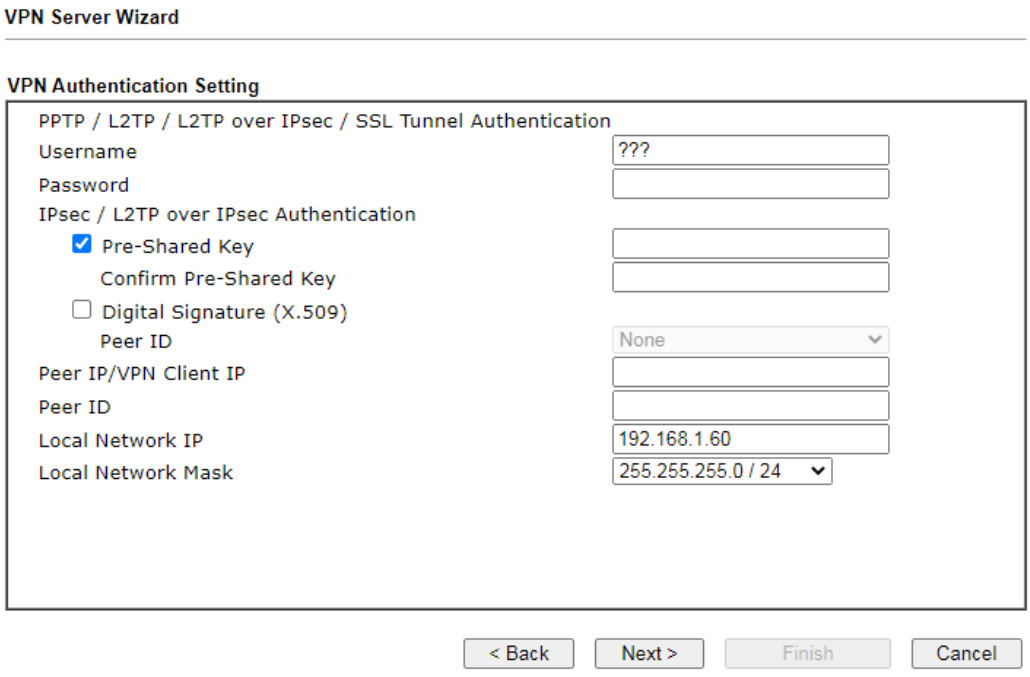
Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. **Site to Site VPN** – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. **Remote Dial-in User** –You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection.
Please choose a LAN-to-LAN Profile	This item is available when you choose **Site to Site VPN** (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.
Please choose a Dial-in User Accounts	This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.
Allowed Dial-in Type	This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard). Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (**Site to Site VPN** and **Remote Dial-in User**) selected.

2. After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made. Here we take the examples of choosing **Site-to-Site VPN** as the **VPN Server Mode**.

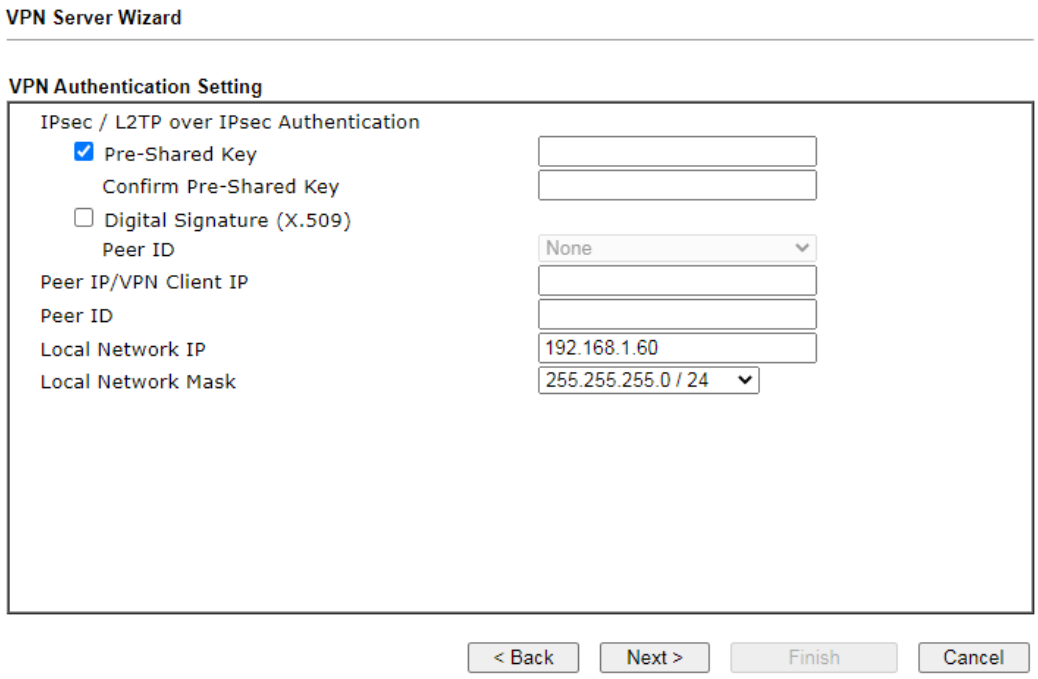
When you check **PPTP/SSL**, you will see the following graphic:



When you check **PPTP & IPsec & L2TP** (three types) or **PPTP & IPsec** (two types) or **L2TP with Policy (Nice to Have/Must)**, you will see the following graphic:



When you check **IPsec**, you will see the following graphic:

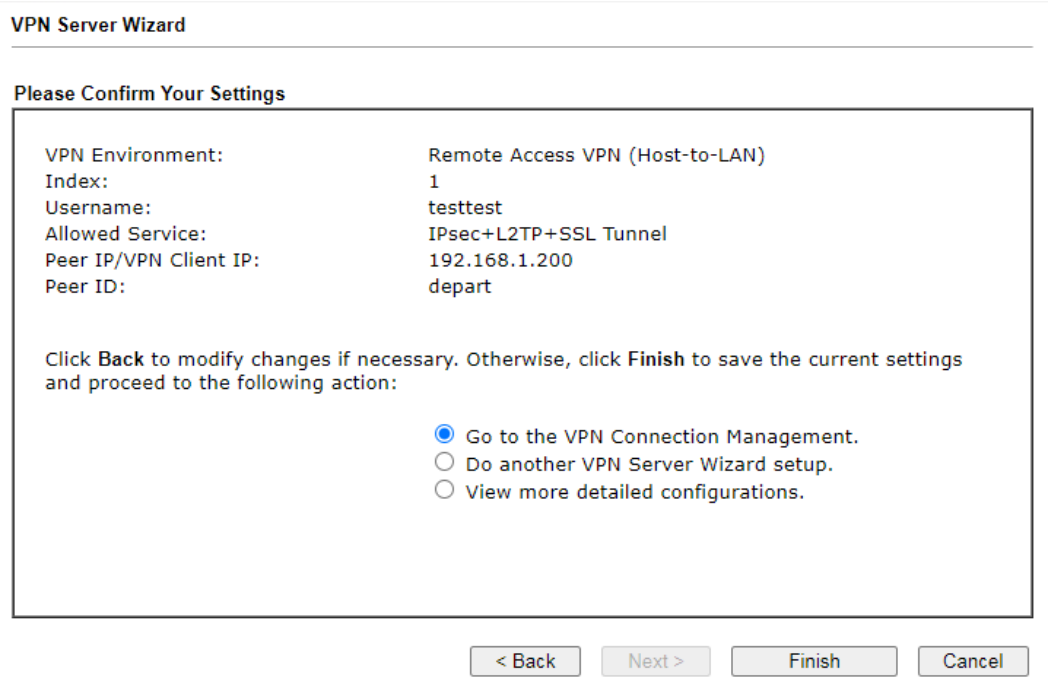


Available settings are explained as follows:

Item	Description
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Pre-Shared Key	For IPsec/L2TP IPsec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Enter the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. **Peer ID** – Choose the peer ID selection from the drop down list. **Local ID** – Choose **Alternative Subject Name First** or **Subject Name First**.
Peer IP/VPN Client IP	Enter the WAN IP address or VPN client IP address for the remote client.
Peer ID	Enter the ID name for the remote client. The length of the name is limited to 47 characters.
Remote Network IP	It is available for Site to Site VPN (LAN-to-LAN). Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	It is available for Site to Site VPN (LAN-to-LAN). Please Enter the network mask (according to the real

	location of the remote host) for building VPN connection.
Local Network IP	Enter the local network IP for TCP / IP configuration.
Local Network Mask	Enter the local network mask for TCP / IP configuration.

3. After finishing the configuration, please click **Next.** The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.



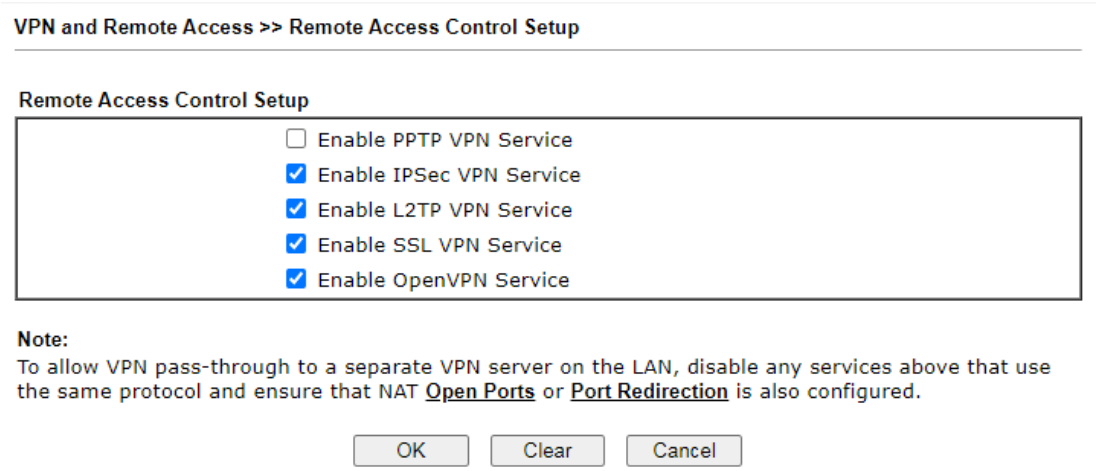
Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access **VPN and Remote Access>>Connection Management** for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access **VPN and Remote Access>>LAN to LAN** for viewing detailed configuration.

IV-1-3 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

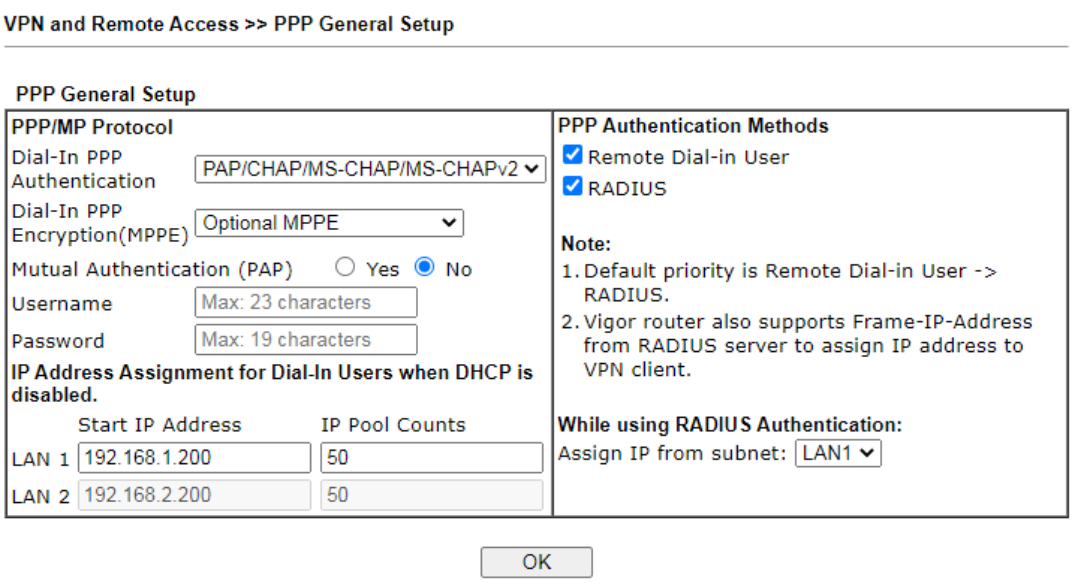
Open **VPN and Remote Access>>Remote Access Control**.



After finishing all the settings here, please click **OK** to save the configuration.

IV-1-4 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.



Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	**PAP Only** - elect this option to force the router to authenticate dial-in users with the PAP protocol. **PAP/CHAP/MS-CHAP/MS-CHAPv2** - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE)	**Optional MPPE** - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit “no MPPE encrypted packets”. Otherwise, the MPPE encryption scheme will be used to encrypt the data. ● **Require MPPE (40/128bits) -** Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. ● **Maximum MPPE -** This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name**

	and **Password** of the mutual authentication peer. The length of the name/password is limited to 23/19 characters.
IP Address Assignment for Dial-In Users	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. You can configure up to four start IP addresses for LAN1 ~ LAN4.
PPP Authentication Methods	Select the method(s) to be used for authentication in PPP connection. **PPP Authentication Methods** ☑ Remote Dial-in User ☑ RADIUS
While using Radius Authentication	If PPP connection will be authenticated via RADIUS server, it is necessary to specify the LAN profile for the dial-in user to get IP from.

IV-1-5 IPsec General Setup

In **IPsec General Setup,** there are two major parts of configuration.

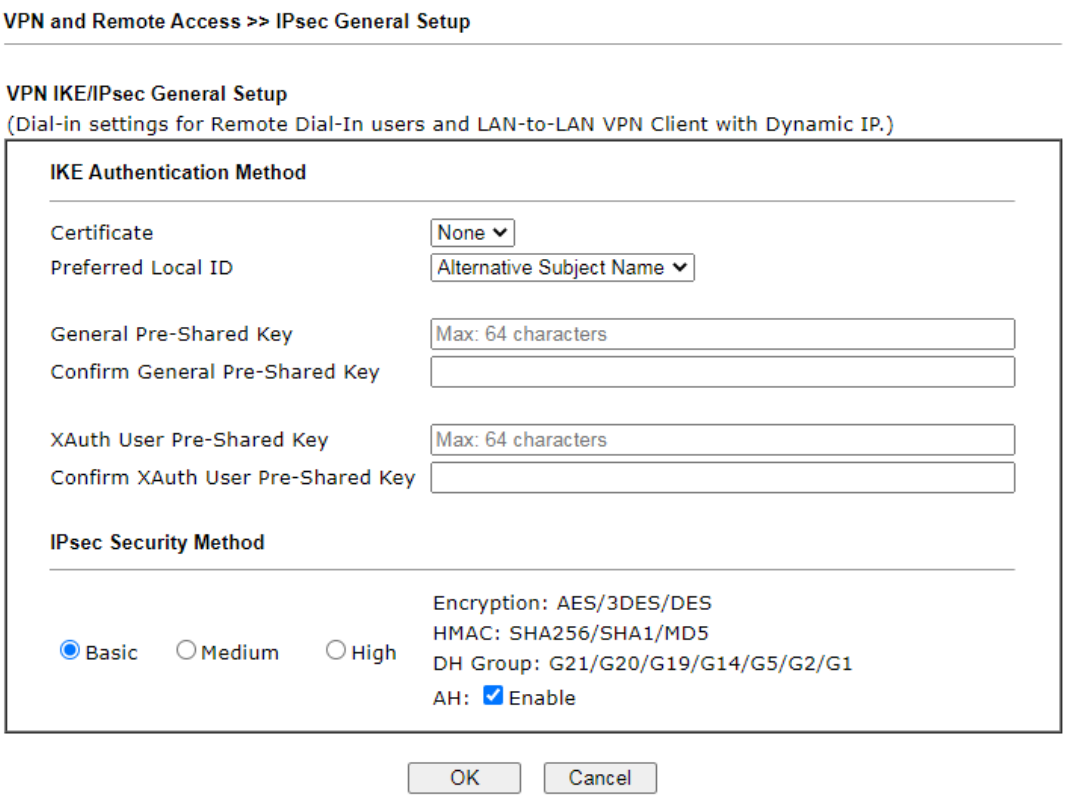
There are two phases of IPsec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPsec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPsec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPsec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.



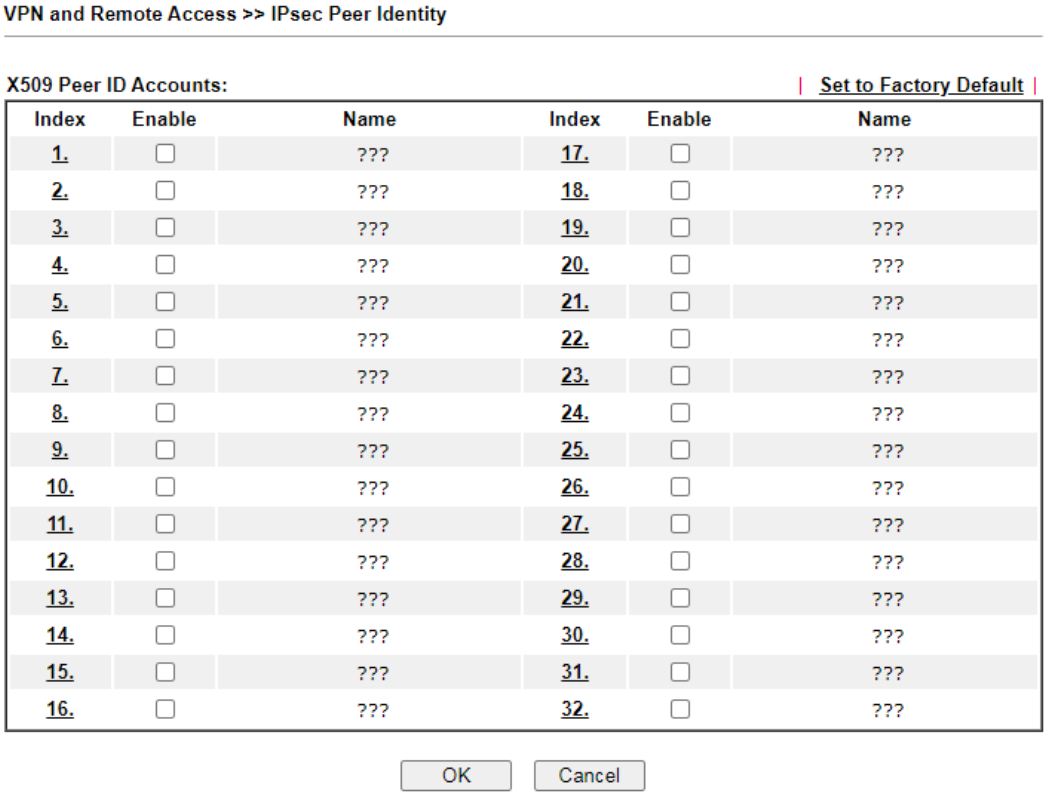
Available settings are explained as follows:

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, **Certificate (X.509)** and **Pre-Shared Key**. **Certificate** – X.509 certificates can be used for IKE authentication. To set up certificates on the router, go to the Certificate Management section. **Preferred Local ID** - Specify the preferred local ID information **(Alternative Subject Name First** or **Subject Name First**) for IPsec authentication while the client is using the general setting (without a specific Peer IP or ID in the VPN profile). **General Pre-Shared Key-** Define the PSK key for general authentication. **Confirm General Pre-Shared Key-** Re-enter the characters to confirm the pre-shared key. **XAuth User Pre-Shared Key -** Define the PSK key for IPsec XAuth authentication. **Confirm XAuth User Pre-Shared Key-** Re-enter the characters to confirm the pre-shared key for IPsec XAuth authentication. **Note**: Any packets from the remote dial-in user which does not match the rule defined in **VPN and Remote Access>>Remote Dial-In User** will be applied with the method specified here.
IPsec Security Method	Available mthods include **Basic, Medium** and **High**. Each method offers different encryption, HMAC and DH Group. **Basic -** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **Medium -** When this option is selected, the Authentication Header (AH) protocol can be used to provide authentication to IPsec traffic. **High** - When this option is selected, the Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security.

After finishing all the settings here, please click **OK** to save the configuration.

IV-1-6 IPsec Peer Identity

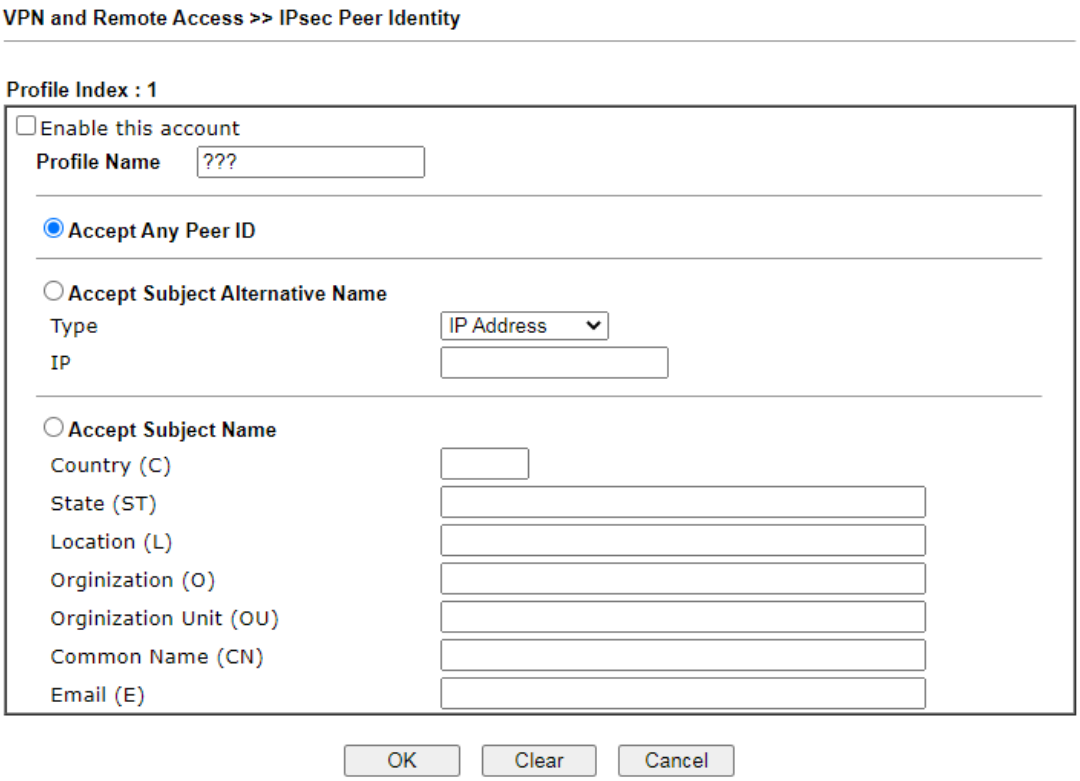
To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **32** entries of digital certificates for peer dial-in users.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPsec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.



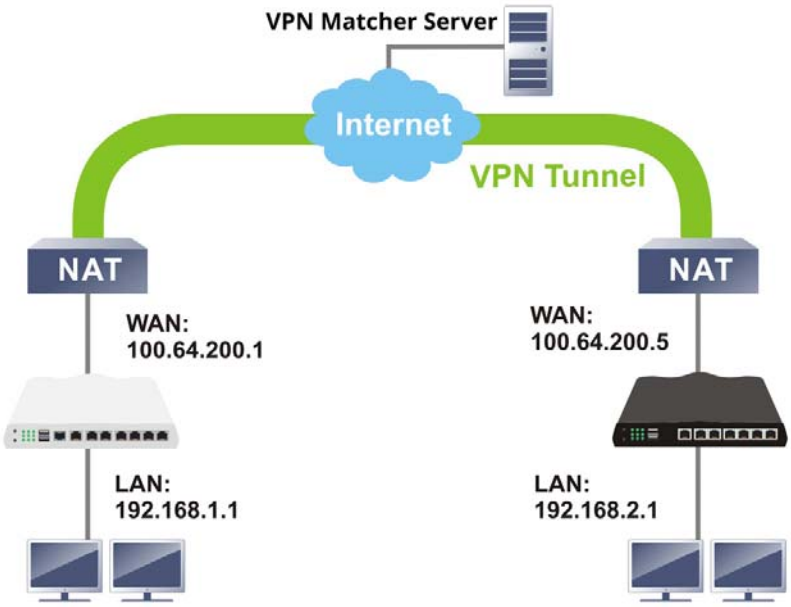
Available settings are explained as follows:

Item	Description
Profile Name	Enter the name of the profile. The maximum length of the name you can set is 32 characters.
Enable this account	Check it to enable such account profile.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail**. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN),** and **Email (E)**.

After finishing all the settings here, please click **OK** to save the configuration.

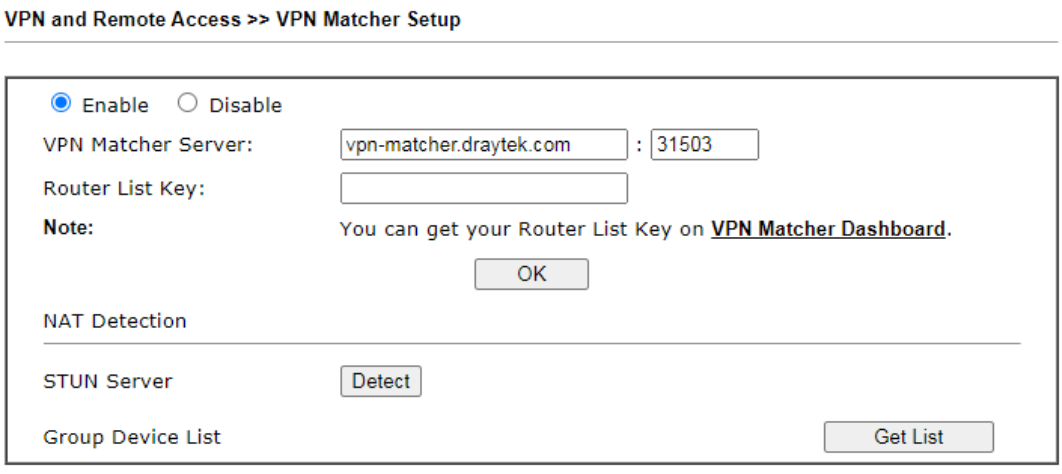
IV-1-7 VPN Matcher Setup

Normally, to establish VPN connection, at least one peer must have a public IP address. The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other. Refer to the following figure.



There is one limitation for the VPN connection. Both routers must be behind a cone NAT, but not symmetric NAT.

Go to **VPN and Remote Access>>VPN Matcher Setup** to open the following page.



Available settings are explained as follows:

Item	Description
Enable / Disable	Click to enable / disable the function of VPN Matcher Setup.
VPN Matcher Server	The IP address of the DrayTek VPN Matcher server is defined as "vpn-matcher.draytek.com" with the port nubmer "31503".
Router List Key	Enter the authentication key for finding a Vigor router with the same group of this device from the VPN matcher server. Then set a VPN link between Vigor routers on both ends via

	VPN wizard.
OK	Click to save the settings.
STUN Server	**Detect** - Click to check if the NAT used by Vigor router is core NAT or not. If not, no VPN can be established.
Group Device List	**Get List** - After entering the Authkey above, click to get available Vigor router which is within the same group as this device.

IV-1-8 OpenVPN

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

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

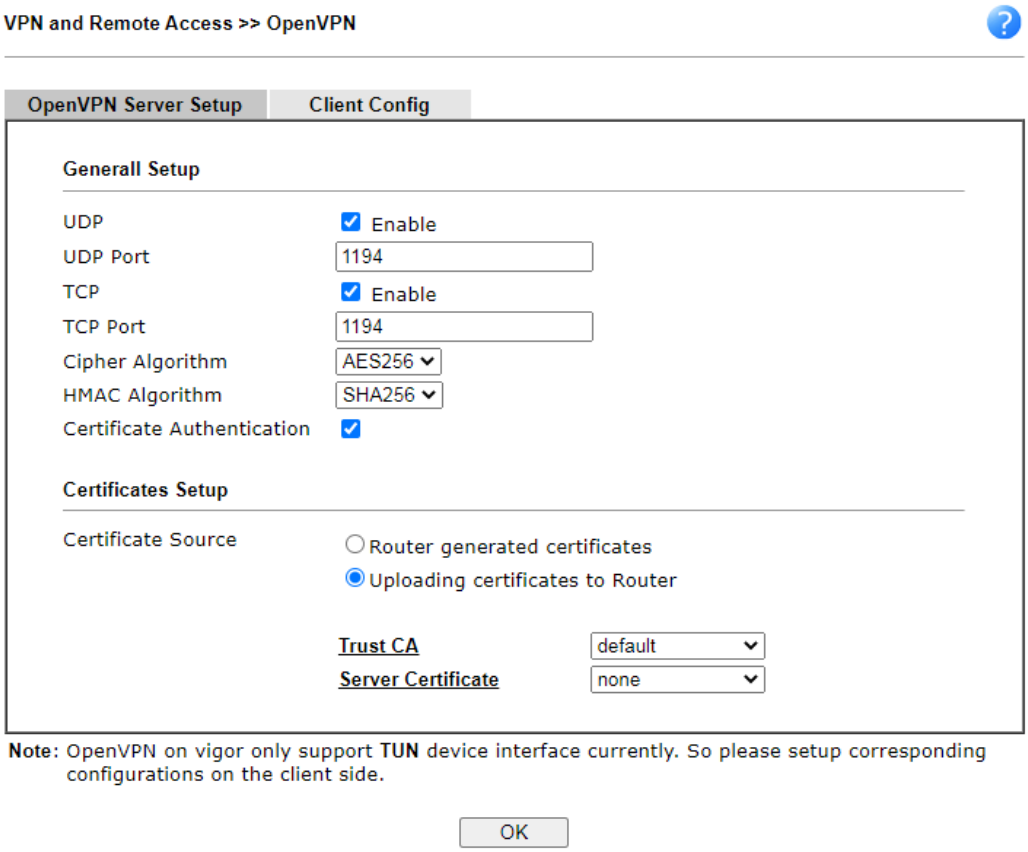
OpenVPN offers a convenient way for users to build a VPN between the local end and the remote end. There are two advantages of OpenVPN:

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

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

IV-1-8-1 OpenVPN Server Setup

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



Available settings are explained as follows:

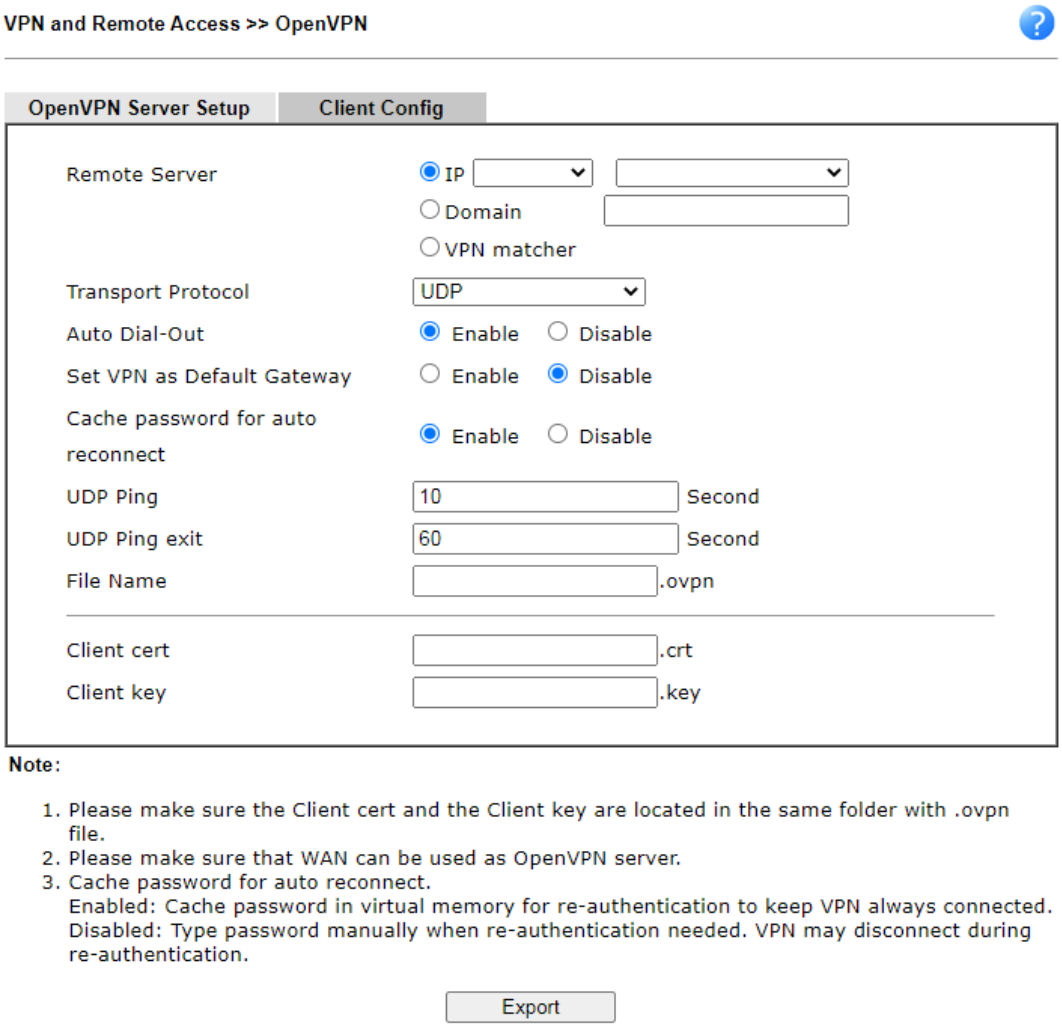
Item	Description
General Setup	
UDP	**Enable -** Select checkbox to enable UDP protocol for OpenVPN connections. **UDP Port** – Enter the UDP port number.
TCP	**Enable -** Select checkbox to enable TCP protocol for OpenVPN connections. **TCP Port** – Enter the TCP port number.
Cipher Algorithm	Select the desired cipher algorithm. Two encryption algorithms are supported: AES128 and AES256. AES256 is more secure than AES128 but may result in lower performance because it incurs higher computational overhead.
HMAC Algorithm	HMAC stands for Hash-based Message Authentication Code. It is used to validate the data integrity and authenticity of the VPN data. Select the desired HMAC hash algorithm. Two hash algorithms, SHA1 and SHA256, are supported. SHA256 is preferred as it is more robust and reliable than SHA1.
Certificate Authentication	Select this checkbox if you would like to validate that the client certificate was issued by a trusted CA.
Certificate Setup	
Certificate Source	Select a source for the certificate to be used for OpenVPN. **Router generated certificates** - Router-generated

	certificates that will be used for OpenVPN. • **GENERATE** - Click to generate a certificate. • **Delete all certificate** - Click to remove all certificates generated by the router. **Uploading certificates to Router** - Third-party certificates will be used for OpenVPN. • **Trust CA** - Use the dropdown list to select a trusted CA certificate that has already been uploaded to the router. To upload Trusted CA certificates to the router, click the Trust CA label and you will be taken to the **Certificate Management >> Trusted CA Certificate** page to perform the operation. • **Server Certificate** - Use the dropdown list to select a server certificate that has already been uploaded to the router. To upload server certificates to the router, click the Server Certificate label and you will be taken to the **Certificate Management >> Local Certificate** page to perform the operation.

After finishing all the settings here, please click **OK** to save the configuration.

IV-1-8-2 Client Config

On this page, you can create and export the configuration required for a remote OpenVPN client to connect to the router.



Available settings are explained as follows:

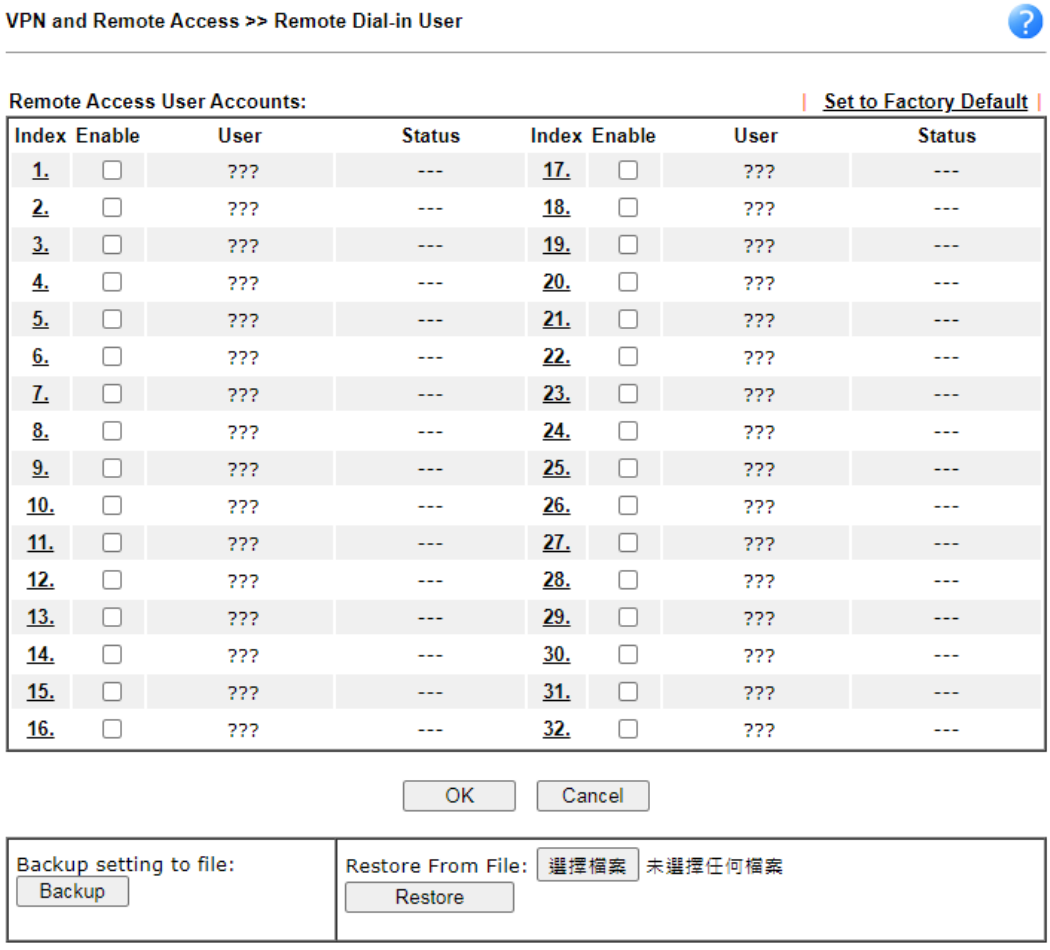
Item	Description
Remote Server	The OpenVPN client will use the IP address or domain name to connect to the router. Select either IP or Domain. **IP** – The OpenVPN configuration file will use the numeric IP address as the server address. **Domain** – The OpenVPN configuration file will use the domain as the server address. You need to ensure that the domain resolves to the IP address of a router WAN port. **VPN matcher** - The OpenVPN configuration file will use the VPN matcher as the server address.
Transport Protocol	Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router.
Auto Dial-Out	**Enable** - If selected, the remote client can auto-dial to this Vigor router to build an OpenVPN tunnel. **Disable** - Select to disable the function.
Set VPN as Default	**Enable** - If selected, the Vigor router will be treated as a

Gateway	"default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel. **Disable** - Select to disable the function.
Cache password for auto reconnect	**Enable** - The default setting. Save the config information with the password required for the OpenVPN tunnel connection. **Disable** - Save the config information without the password information. If it is selected, the user must re-enter the password for authentication while setting the network connection via OpenVPN tunnel.
UDP Ping	Ping remote device over the UDP control channel, if no packets have been sent for the number of seconds configured here.
UDP Ping exit	Let OpenVPN exit after the seconds set here if no reception of a ping or other packet from the remote device.
File Name	Enter the filename of the configuration file to be downloaded from the router.
CA cert	Enter the certificate authority (CA) file name obtained from 3rd party provider.
Client cert	Enter the filename of the client certificate obtained from 3rd party provider.
Client key	Enter the filename of the private key obtained from the 3rd party provider.
Export	Click this button to download the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections.

IV-1-9 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

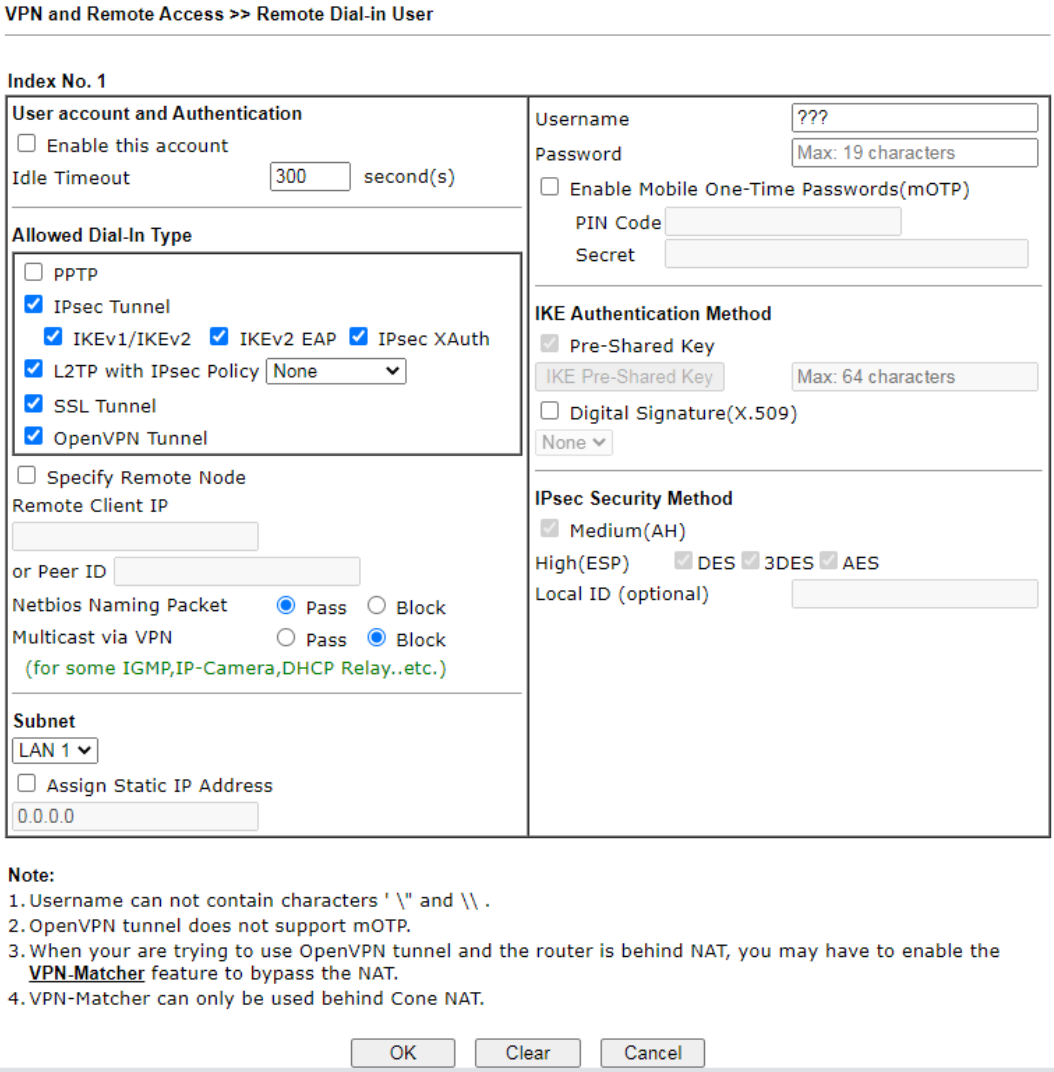
The router provides multiple access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
Enable	Check the box to enable the profile.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.



Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Check the box to enable this function. **Idle Timeout-** If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
Allowed Dial-In Type	**PPTP** - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. **IPsec Tunnel** - Allow the remote dial-in user to make an IPsec VPN connection through Internet. **L2TP with IPsec Policy** - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: ● **None -** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.

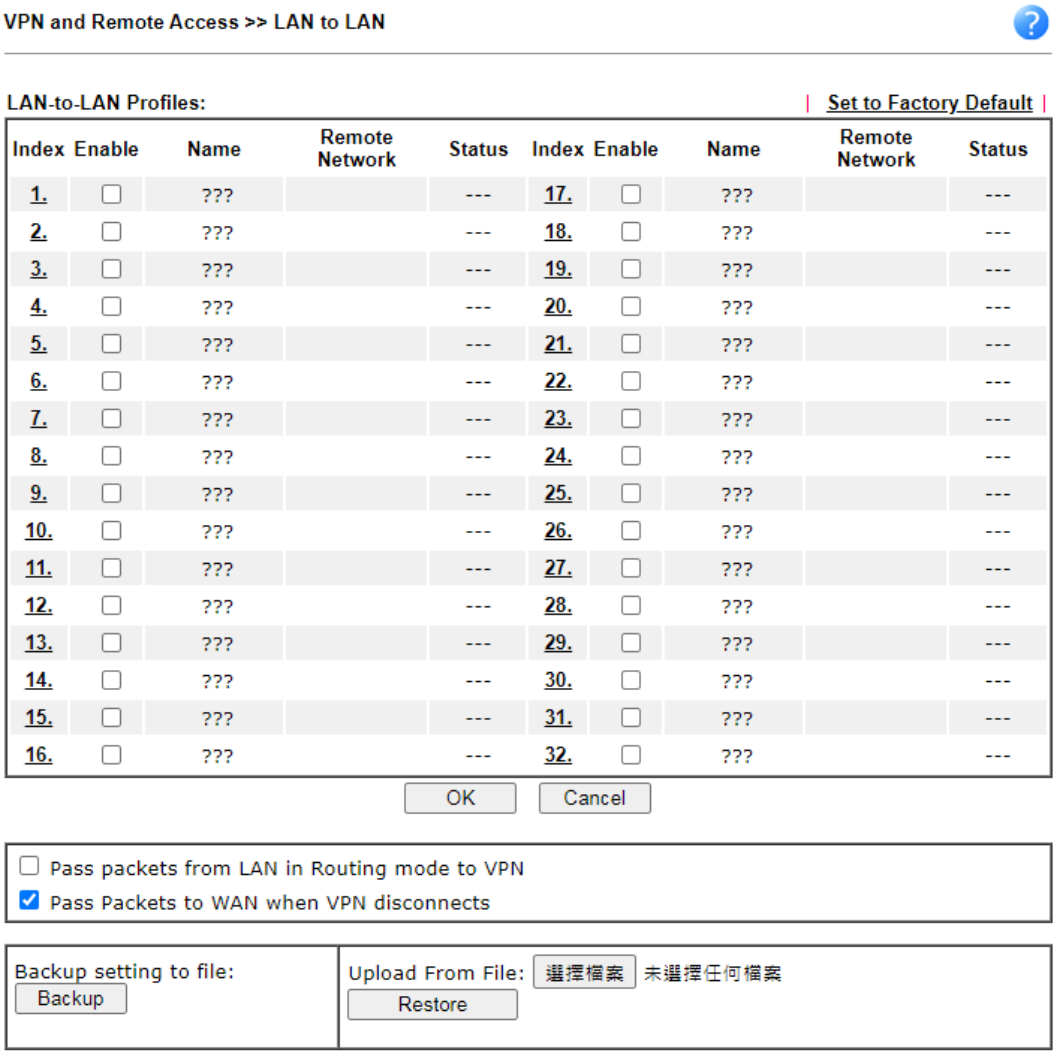
	• **Nice to Have -** Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. • **Must -**Specify the IPsec policy to be definitely applied on the L2TP connection. **SSL Tunnel –** Allow the remote dial-in user to make an SSL VPN connection through Internet. **Specify Remote Node -**You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the **general settings**. **Netbios Naming Packet -** • **Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. • **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. **Multicast via VPN** - Some programs might send multicast packets via VPN connection. • **Pass** – Click this button to let multicast packets pass through the router. • **Block** – This is default setting. Click this button to let multicast packets be blocked by the router. **User Name** - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 23 characters. **Password** - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 19 characters. **Enable Mobile One-Time Passwords (mOTP) -** Check this box to make the authentication with mOTP function. **PIN Code** – Enter the code for authentication (e.g, 1234). **Secret** – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Subnet	Chose one of the subnet selections for such VPN profile. **Assign Static IP Address –** Please type a static IP address for the subnet you specified.
IKE Authentication Method	This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specifying the IP address of the remote node. **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and Enter the required characters (1-63) as the pre-shared key. **Digital Signature (X.509) –** Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity.**
IPsec Security Method	This group of fields is a must for IPsec Tunnels and L2TP with

	IPsec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **Medium-Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. **High-Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. **Local ID (Optional)-** Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

After finishing all the settings here, please click **OK** to save the configuration.

IV-1-10 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

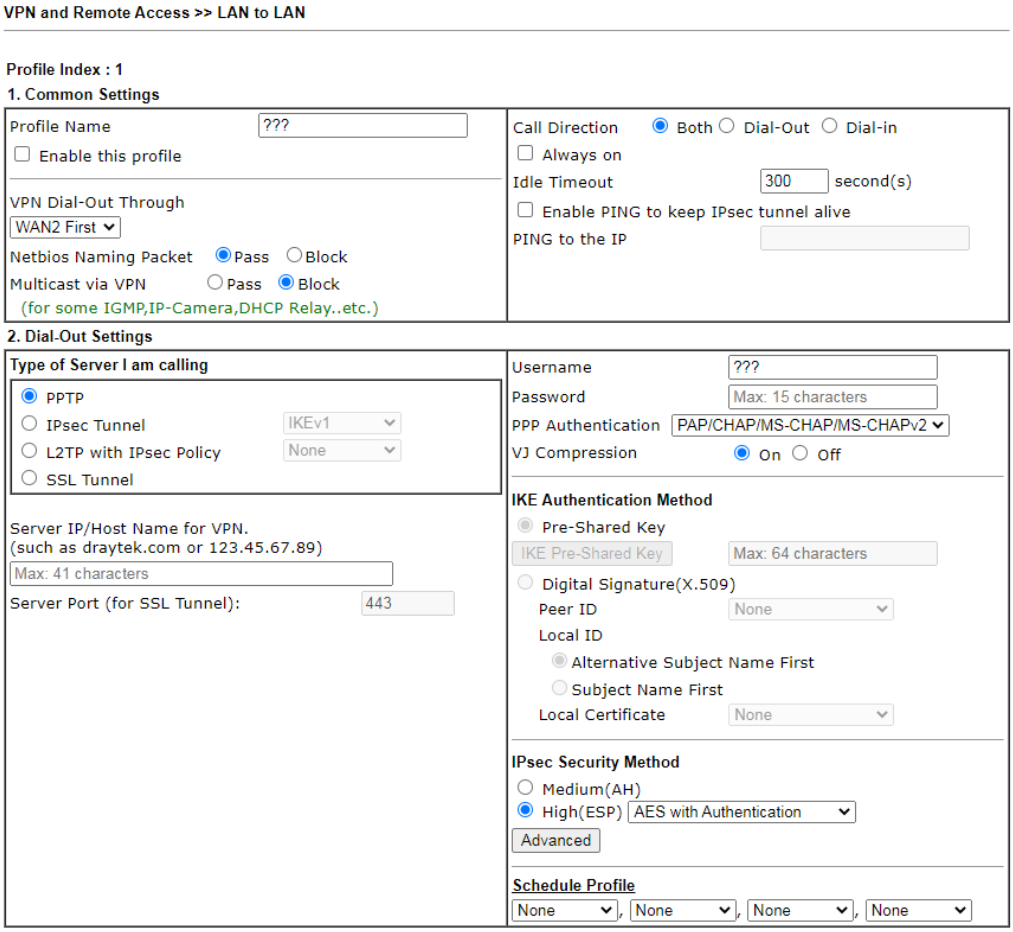


Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number link to access into the setting page of a VPN profile.
Enable	Check it to enable such LAN to LAN profile.
Name	Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Remote Network	Display the IP address with the netmask of remote network.
Status	Online – means such LAN to LAN profile is in use. Offline – means such LAN to LAN profile isn't in use even if the profile has been enabled.

To edit each profile:

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.



Available settings are explained as follows:

Item	Description
Common Settings	**Profile Name –** Specify a name for the profile of the LAN-to-LAN connection.

	Enable this profile - Check here to activate this profile. **VPN Dial-Out Through -** Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only. ● **WAN2 First/ LTE First** - While connecting, the router will use WAN2 or LTE as the first channel for VPN connection. If WAN2 or LTE fails, the router will use another WAN interface instead. ● **WAN2 Only/ LTE Only** - While connecting, the router will use WAN2 or LTE as the only channel for VPN connection. **Netbios Naming Packet** ● **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. **Multicast via VPN -** Some programs might send multicast packets via VPN connection. ● **Pass** – Click this button to let multicast packets pass through the router. ● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router. **Call Direction -** Specify the allowed call direction of this LAN-to-LAN profile. ● **Both**:-initiator/responder ● **Dial-Out**- initiator only ● **Dial-In-** responder only. **Always On-**Check to enable router always keep VPN connection. **Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection. **Enable PING to keep IPsec tunnel alive -** This function is to help the router to determine the status of IPsec VPN connection, especially useful in the case of abnormal VPN IPsec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address. This function is used to handle abnormal IPsec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnects without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection). **PING to the IP -** Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

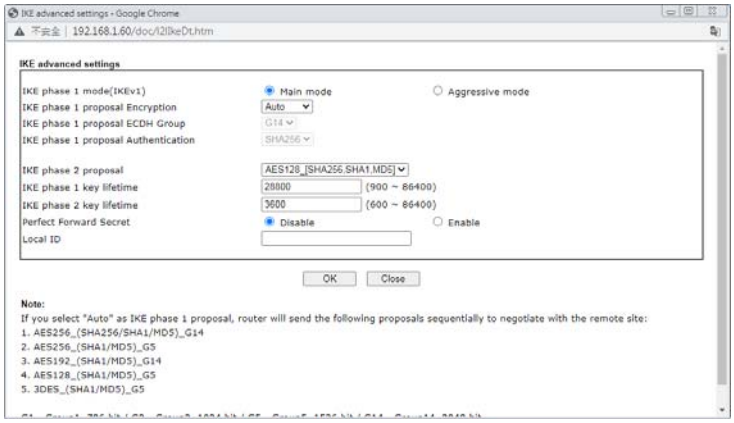
Dial-Out Settings	**Type of Server I am calling - PPTP** - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server. **IPsec Tunnel** - Build an IPsec VPN connection to the server through Internet. **L2TP with IPsec Policy -** Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: ● **None:** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ● **Nice to Have:** Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. ● **Must:** Specify the IPsec policy to be definitely applied on the L2TP connection. **SSL Tunnel** - Build an SSL VPN connection to the server through Internet. **User Name -** This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 49 characters. **Password -** This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 15 characters. **PPP Authentication -** This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP/MS-CHAP/MS-CHAPv2 is the most common selection due to compatibility. **VJ compression -** This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **On** to improve bandwidth utilization. **IKE Authentication Method -** This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy. ● **Pre-Shared Key** - Input 1-63 characters as pre-shared key. ● **Digital Signature (X.509)** - Select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity**. **Peer ID -** Select one of the predefined Profiles set in **VPN and Remote Access >>IPsec Peer Identity.** **Local ID –** Specify a local ID **(Alternative Subject Name First** or **Subject Name First)** to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode. ● **Local Certificate –** Select one of the profiles set in **Certificate Management>>Local Certificate**. **IPsec Security Method -** This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy. ● **Medium AH (Authentication Header)** means data will be authenticated, but not be encrypted. By default, this option is active. ● **High (ESP-Encapsulating Security Payload)-** means payload (data) will be encrypted and authenticated.

Select from below:

- **DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme.
- **DES with Authentication-**Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
- **3DES without Authentication**-Use triple DES encryption algorithm and not apply any authentication scheme.
- **3DES with Authentication-**Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
- **AES without Authentication**-Use AES encryption algorithm and not apply any authentication scheme.
- **AES with Authentication-**Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.

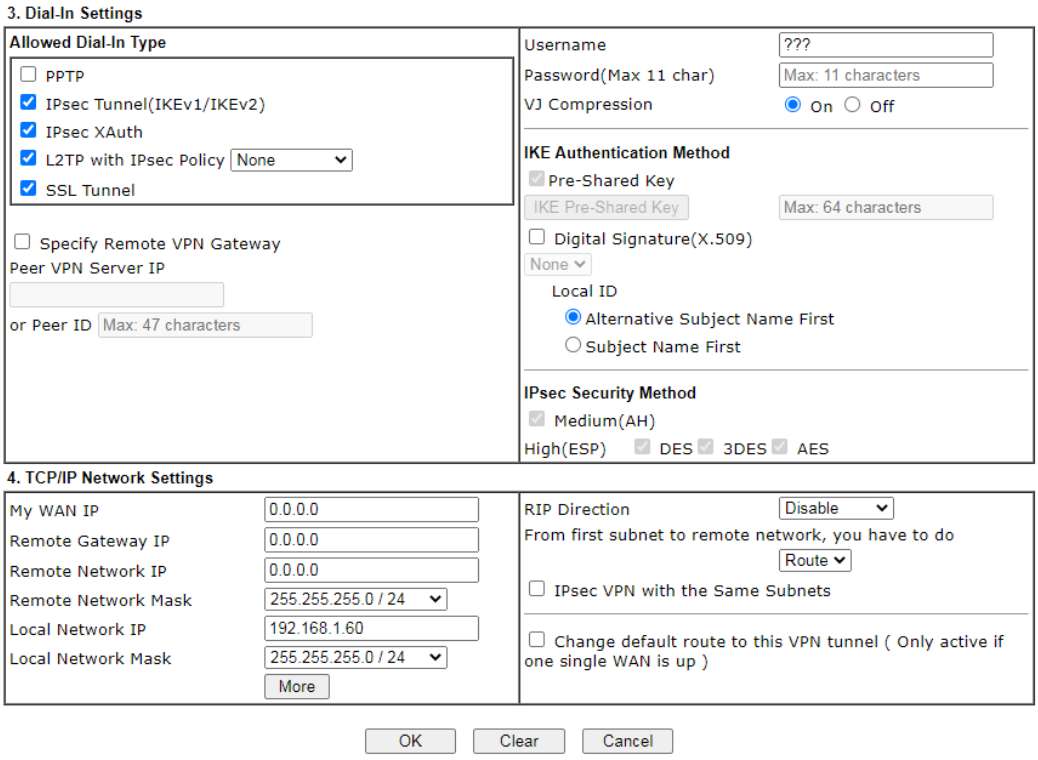
The window of advance setup is shown as below:



IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

- **IKE phase 1 proposal-**To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.
- **IKE phase 2 proposal-**To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.
- **IKE phase 1 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.

	● **IKE phase 2 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds. ● **Perfect Forward Secret (PFS)-**The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function. **Local ID-**In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters. **Schedule Profile -** Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.



Available settings are explained as follows:

Item	Description
Dial-In Settings	**Allowed Dial-In Type -** Determine the dial-in connection with different types. ● **PPTP -** Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. ● **IPsec Tunnel-** Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● **L2TP with IPsec Policy -** Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:

- **None -** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.
- **Nice to Have** - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.
- **Must -** Specify the IPsec policy to be definitely applied on the L2TP connection.

- **SSL Tunnel-** Allow the remote dial-in user to trigger an SSL VPN connection through Internet.

Specify Remote VPN Gateway - You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side.

If you uncheck the checkbox**,** the connection type you select above will apply the authentication methods and security methods in the general settings.

Username - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.

Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.

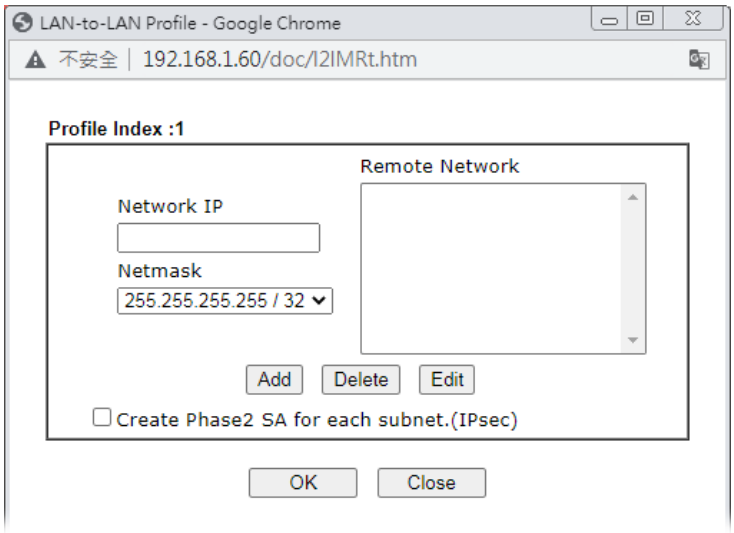
VJ Compression - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above.

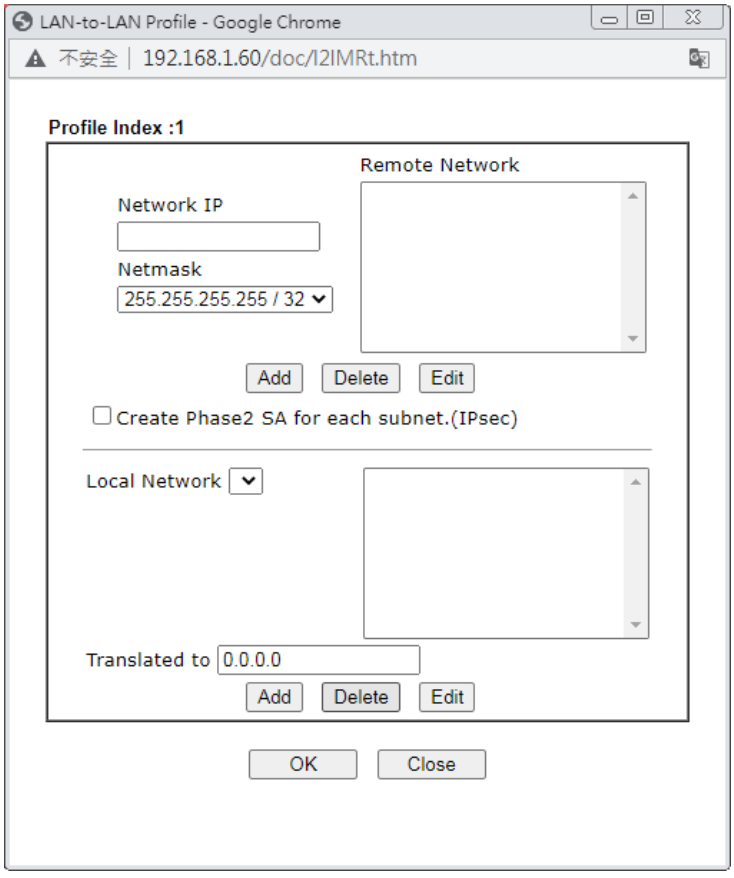
IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node.

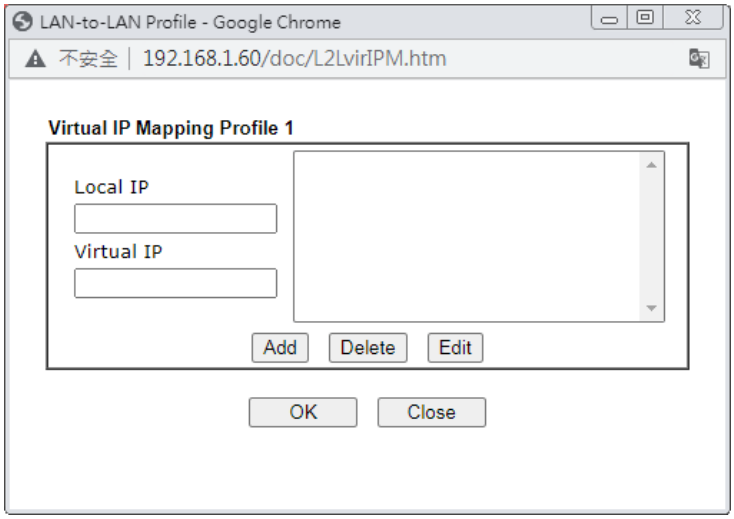
- **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and Enter the required characters (1-63) as the pre-shared key.
- **Digital Signature (X.509) -**Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity**.
  - **Local ID** – Specify which one will be inspected first.
  - **Alternative Subject Name First** – The alternative subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.
  - **Subject Name First** – The subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.

IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.

- **Medium-** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default,

	this option is active. ● **High-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
TCP/IP Network Settings	**My WAN IP –**This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP. **Remote Gateway IP -** This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP. **Remote Network IP/ Remote Network Mask -** Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode. **Local Network IP / Local Network Mask -** Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required. **More -** Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Masks through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.  **RIP Direction -** The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable. **From first subnet to remote network, you have to do -** If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**. **Change default route to this VPN tunnel -** Check this box to

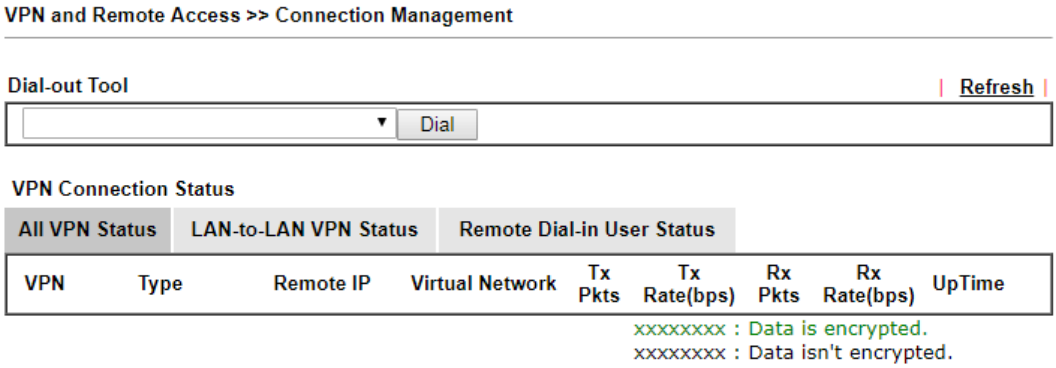
	change the default route with this VPN tunnel.
IPSec VPN with the Same subnet	For both ends (e.g., different sections in a company) are within the same subnet, there is a function which allows you to build Virtual IP mapping between two ends. Thus, when VPN connection established, the router will change the IP address according to the settings configured here and block sessions which are not coming from the IP address defined in the Virtual IP Mapping list. After checking the box of **IPSec VPN with the Same subnet**, the options under **TCP/IP Network Settings** will be changed as shown below:  **Remote Network IP/ Remote Network Mask -** Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode. **Translated Local Network –** This function is enabled in default. Use the drop down list to specify a LAN port as the transferred direction. Then specify an IP address. Click **Advanced** to configure detailed settings if required. **Advanced** – Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.  **Translated Type –** There are two types for you to choose.

	• **Whole Subnet** • **Specific IP Address** **Virtual IP Mapping –** A pop up dialog will appear for you to specify the local IP address and the mapping virtual IP address. 

2. After finishing all the settings here, please click **OK** to save the configuration.

IV-1-11 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.



Available settings are explained as follows:

Item	Description
Dial-out Tool	This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function. **Dial -** Click this button to execute dial out function.

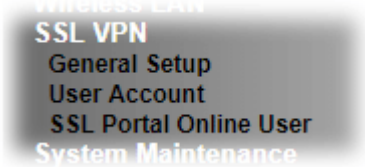
IV-2 SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.

There are two benefits that SSL VPN provides:

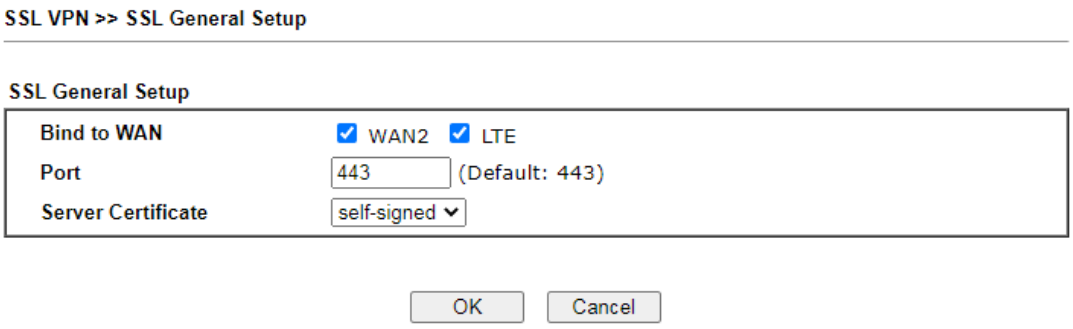
- It is not necessary for users to preinstall VPN client software for executing SSL VPN connection.
- There are less restrictions for the data encrypted through SSL VPN in comparing with traditional VPN.

Web User Interface



IV-2-1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.



Available settings are explained as follows:

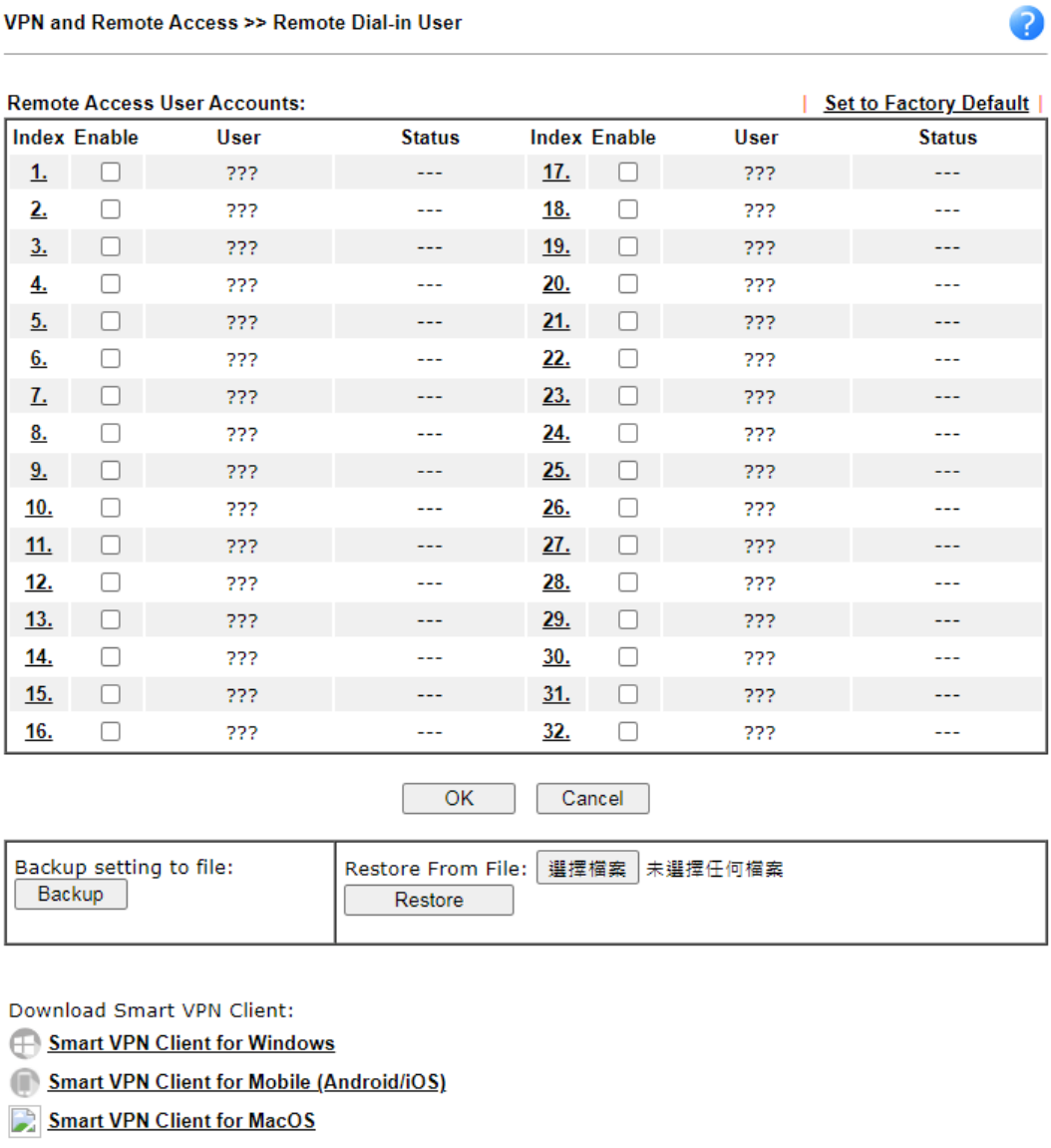
Item	Description
Bind to WAN	Choose and check WAN interface(s) for SSL VPN tunnel establishment.
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in **System Maintenance>>Management**. In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose **Self-signed** to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

After finishing all the settings here, please click **OK** to save the configuration.

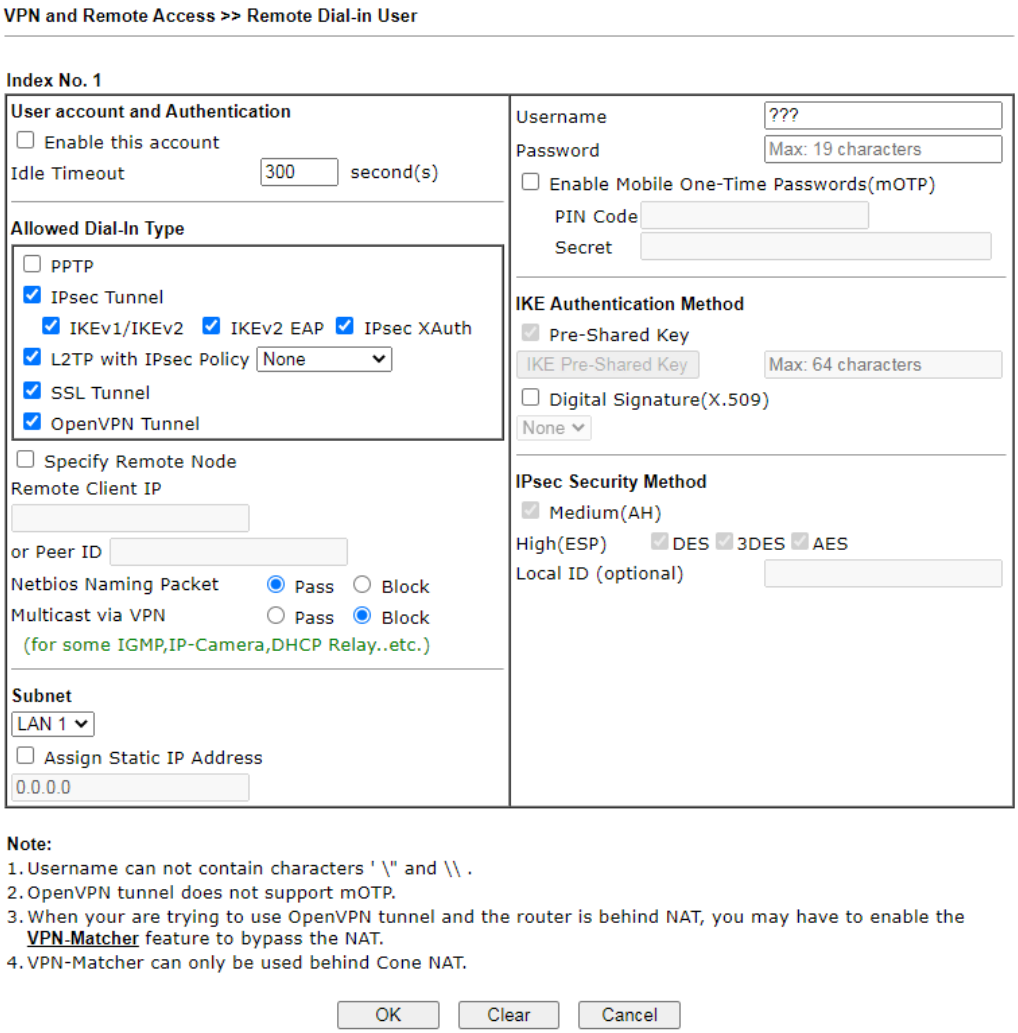
IV-2-2 User Account

With SSL VPN, VigorLTE 200 series let teleworkers have convenient and simple remote access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe. The SSL technology is the same as the encryption that you use for secure web sites such as your online bank. The SSL VPN can be operated in either full tunnel mode or proxy mode. Now, VigorLTE 200 series allows up to 16 simultaneous incoming users.

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item will guide to access into **VPN and Remote Access>>Remote Dial-in user**.



Click each index to edit one remote user profile.



Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Check the box to enable this function. **Idle Timeout-** If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds. **Username** - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 23 characters. **Password** - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 19 characters. **Enable Mobile One-Time Passwords (mOTP) -** Check this box to make the authentication with mOTP function. **PIN Code** – Enter the code for authentication (e.g, 1234). **Secret** – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Allowed Dial-In Type	**PPTP** - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. **IPSec Tunnel** - Allow the remote dial-in user to make an IPSec

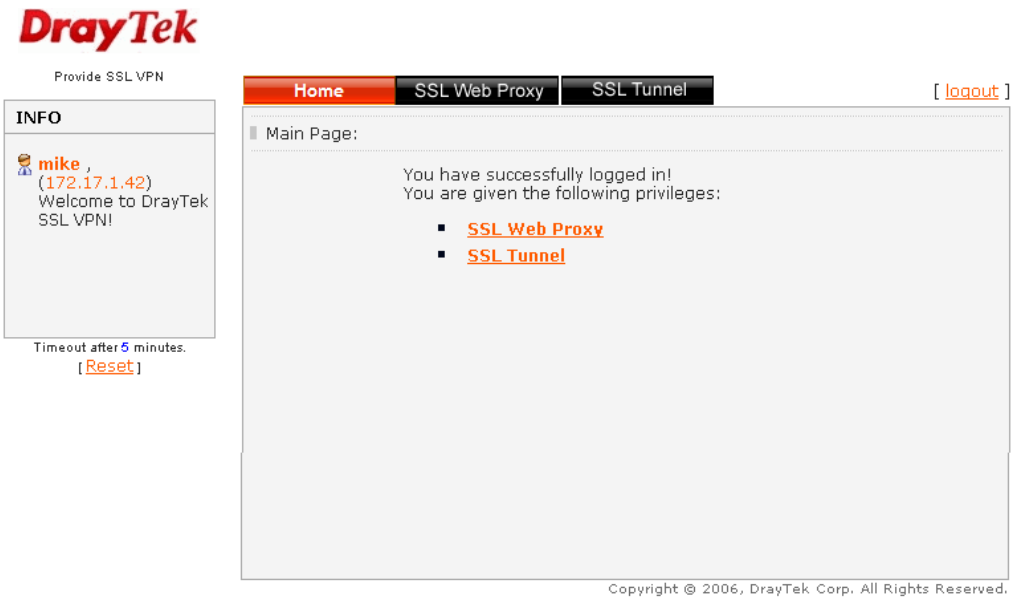
Item	Description
	VPN connection through Internet. **L2TP with IPSec Policy** - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: ● **None -** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ● **Nice to Have -** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● **Must -**Specify the IPSec policy to be definitely applied on the L2TP connection. **SSL Tunnel -** It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP / L2TP / IPSec). If you check this box, the function of SSL Tunnel for this account will be activated immediately. **IPsec XAuth** – Allow the remote dial-in user to make an IPsec VPN connection through XAuth server in Internet. **Specify Remote Node -** Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the **general settings**. **Netbios Naming Packet** ● **Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. **Multicast via VPN** - Some programs might send multicast packets via VPN connection. ● **Pass** – Click this button to let multicast packets pass through the router. ● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.
Subnet	Chose one of the subnet selections for such VPN profile. **Assign Static IP Address –** Please type a static IP address for the subnet you specified.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and Enter the required characters (1-63) as the pre-shared key. **Digital Signature (X.509) –** Check the box of Digital Signature to invoke this function and Select one predefined Profiles set

Item	Description
	in the **VPN and Remote Access >>IPSec Peer Identity.**
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **Medium-Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. **High(ESP-Encapsulating Security Payload)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. **Local ID -** Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

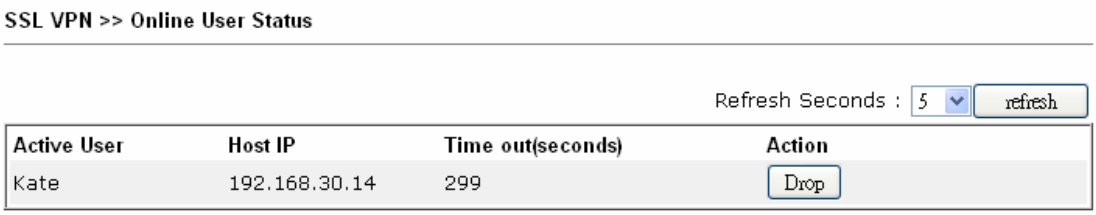
After finishing all the settings here, please click **OK** to save the configuration.

IV-2-3 SSL Portal Online User

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into **DrayTek SSL VPN portal** interface.



Next, users can open **SSL VPN>> Online Status** to view logging status of SSL VPN.



Available settings are explained as follows:

Item	Description
Active User	Display current user who visits SSL VPN server.
Host IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.
Action	You can click **Drop** to drop certain login user from the router's SSL Portal UI.

IV-3 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your 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. Here Vigor router support digital certificates conforming to standard X.509.

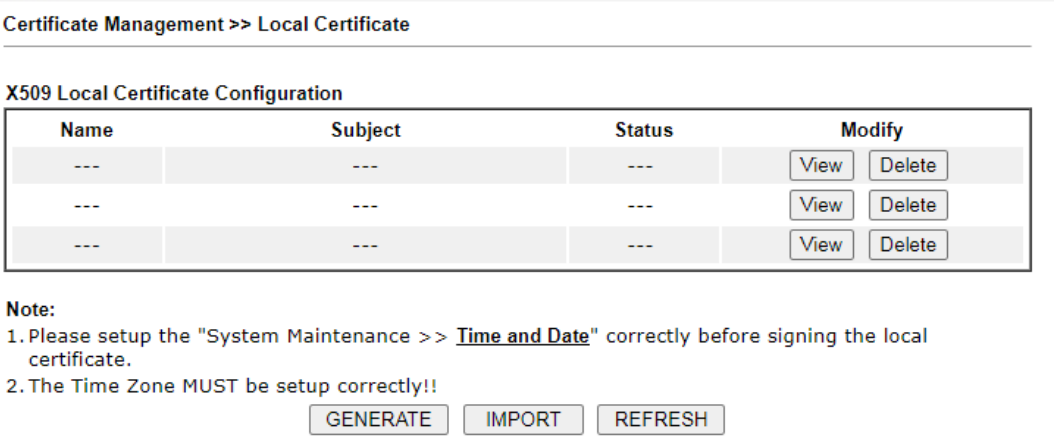
Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

Web User Interface

IV-3-1 Local Certificate

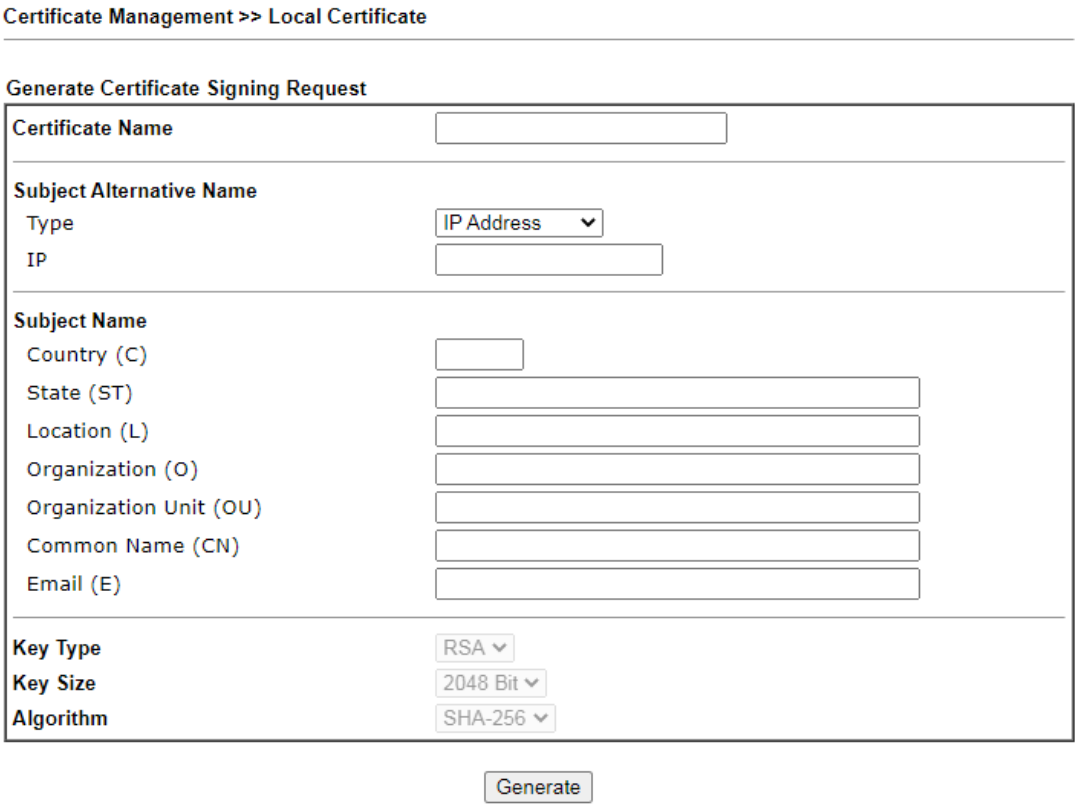


Available settings are explained as follows:

Item	Description
Generate	Click this button to open **Generate Certificate Request** window. Enter all the information that the window requests. Then click **Generate** again.
Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.
Delete	Click this button to delete selected name with certification information.

GENERATE

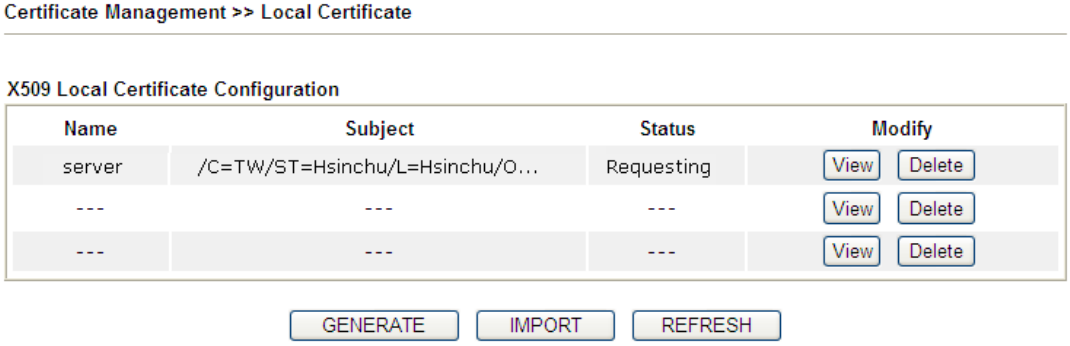
Click this button to open **Generate Certificate Signing Request** window. Enter all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.



Info

Please be noted that "Common Name" must be configured with router's WAN IP or domain name.

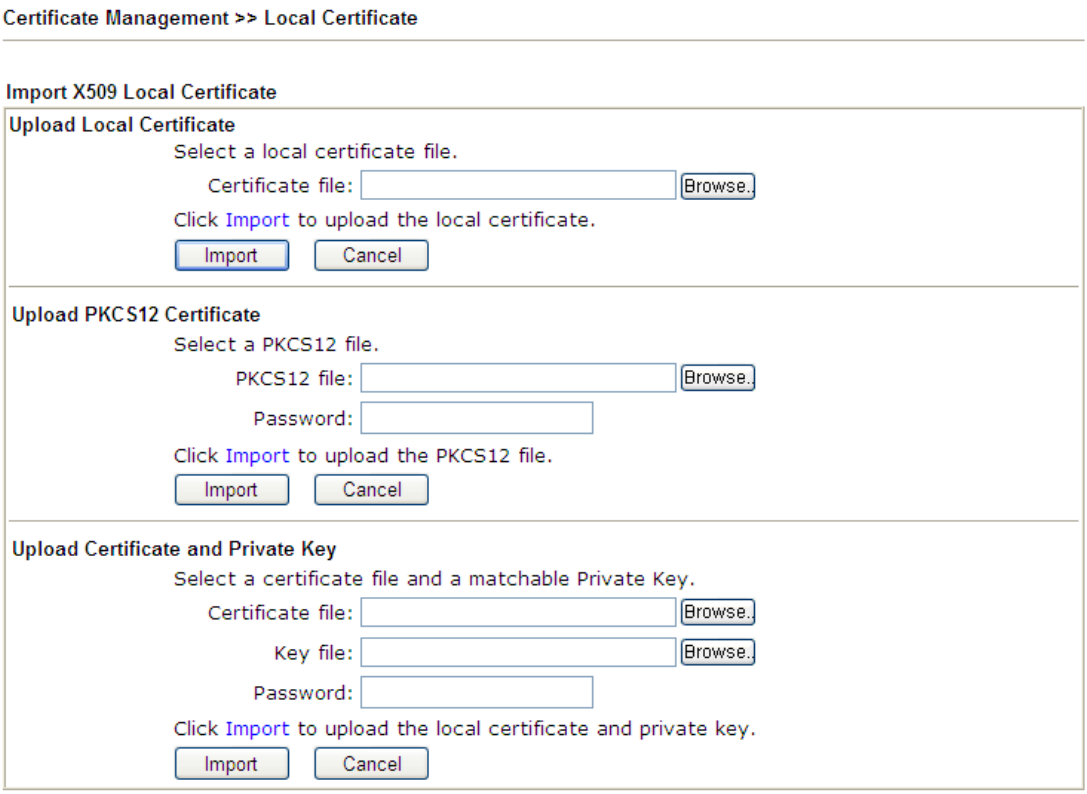
After clicking **GENERATE**, the generated information will be displayed on the window below:



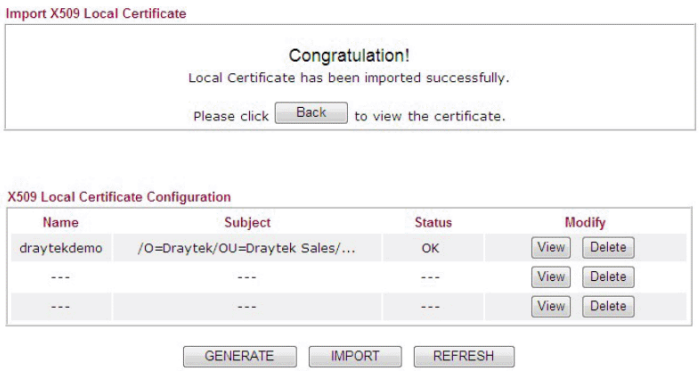
IMPORT

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.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.



Available settings are explained as follows:

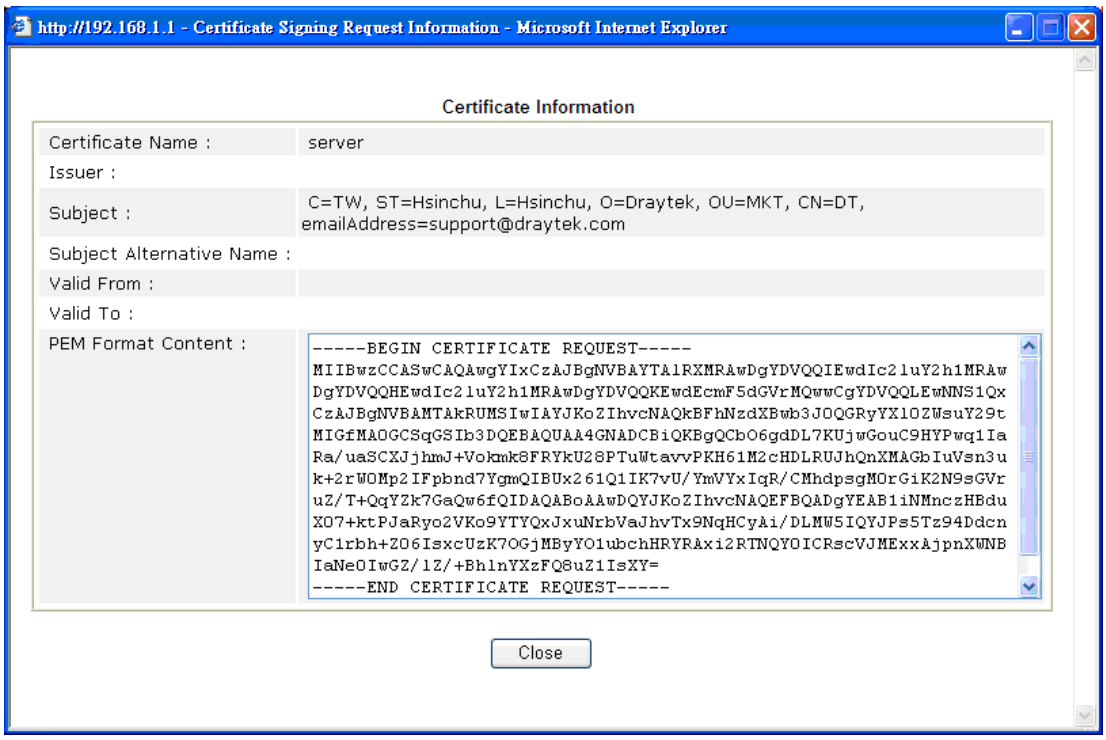
Item	Description
Upload Local Certificate	It allows users to import the certificate which is generated by Vigor router and signed by CA server. If you have done well in certificate generation, the Status of the certificate will be shown as "**OK**". 
Upload PKCS12 Certificate	It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords. Note that PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.



Info	You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

Delete

Click this button to remove the selected certificate.

IV-3-2 Trusted CA Certificate

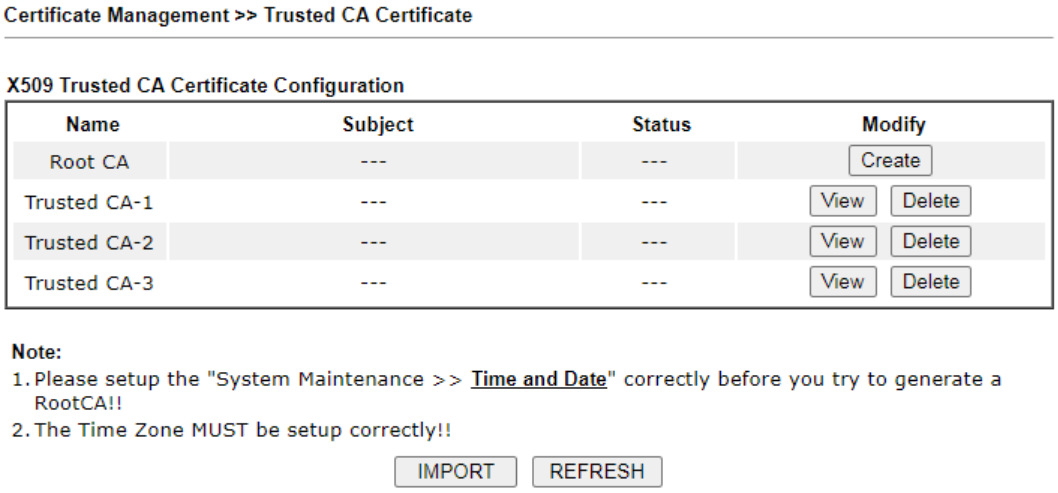
Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

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.

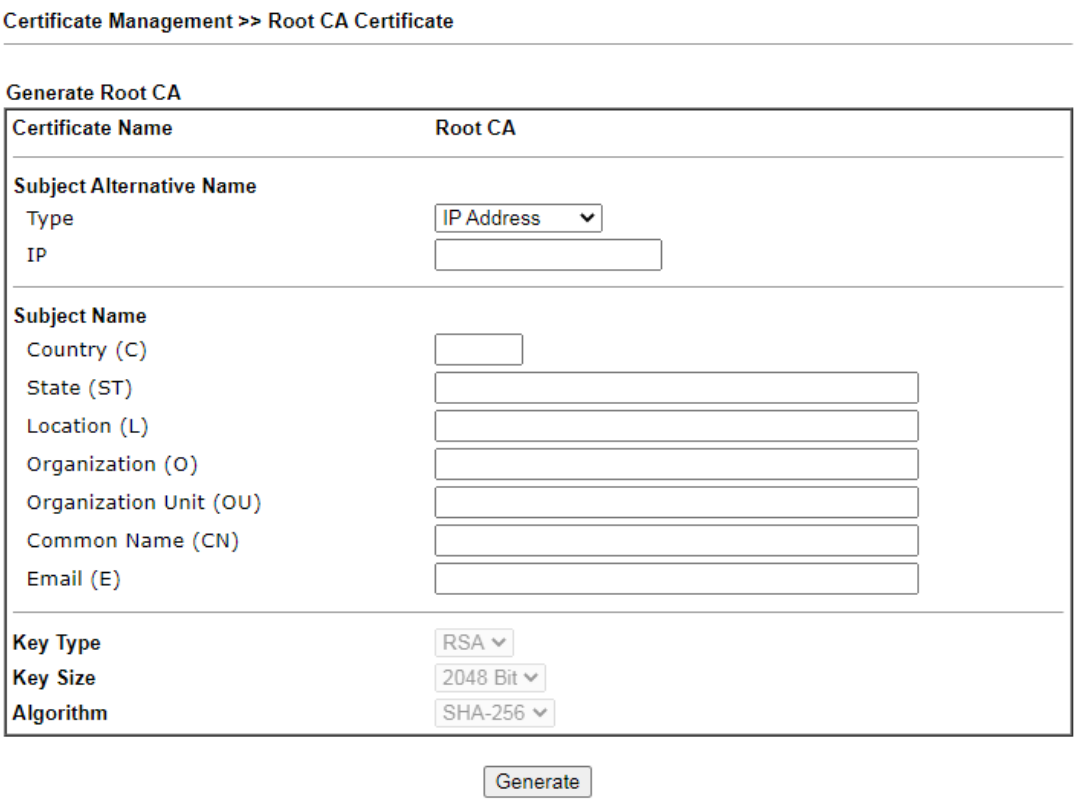
Info

Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.



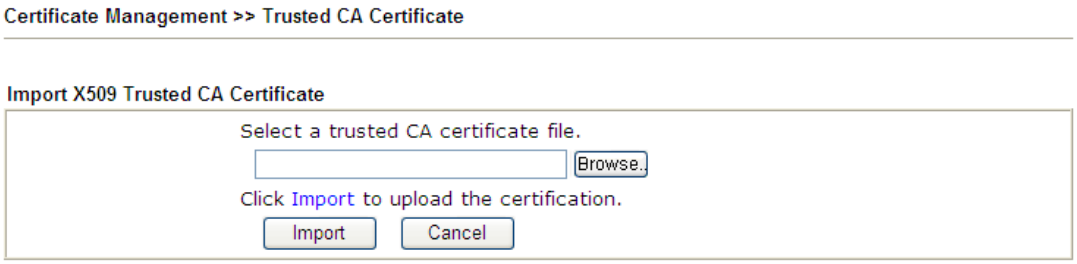
Creating a Root CA

Click **Create** to open the following page. Enter all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **Generate** again.

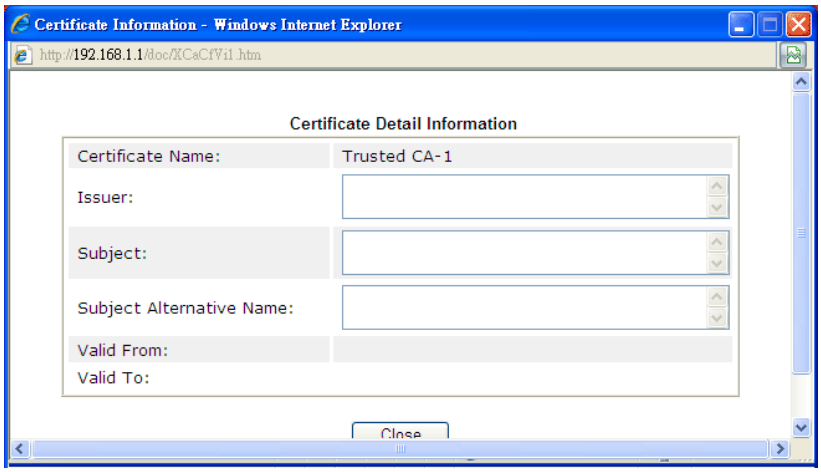


Importing a Trusted CA

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse…** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window.



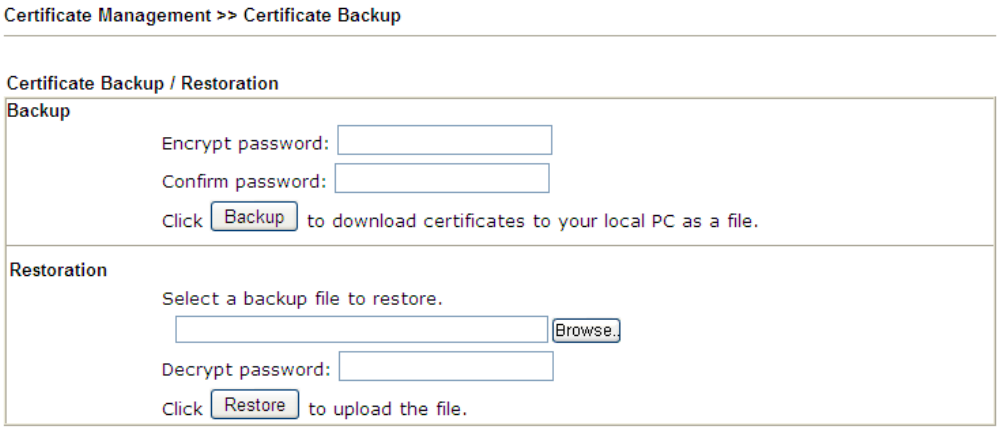
For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



IV-3-3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Confirm password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.



Available settings are explained as follows:

Item	Description
Backup	
Encrypt password/Confirm password	Enter the password with which you wish to encrypt the certificate.
Backup	Click to download the certificate.
Restoration	
Select a backup file to restore	Click Browse to select the backup file you wish to restore.
Decrypt password	Enter the password that was used to encrypt the certificates.
Restore	Click to retrieve the certificate.

Part V Security

Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet.

CSM

CSM is an abbreviation of Central Security Management which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

V-1 Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

Firewall Facilities

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

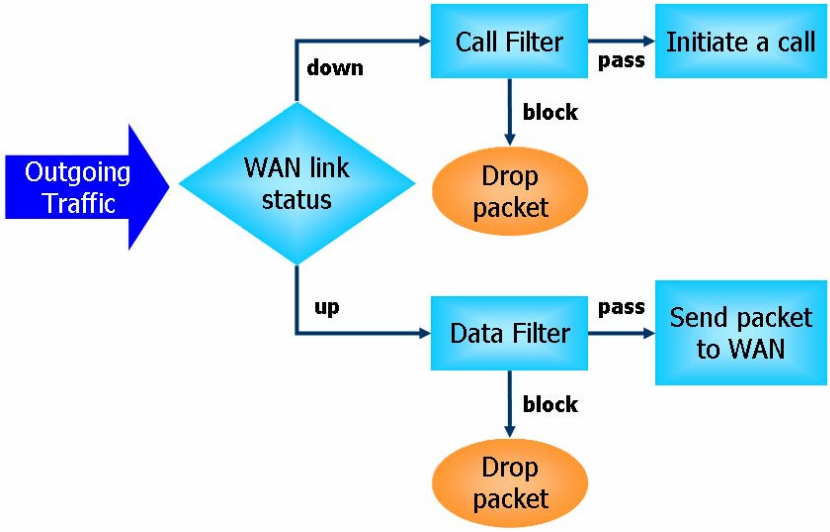
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

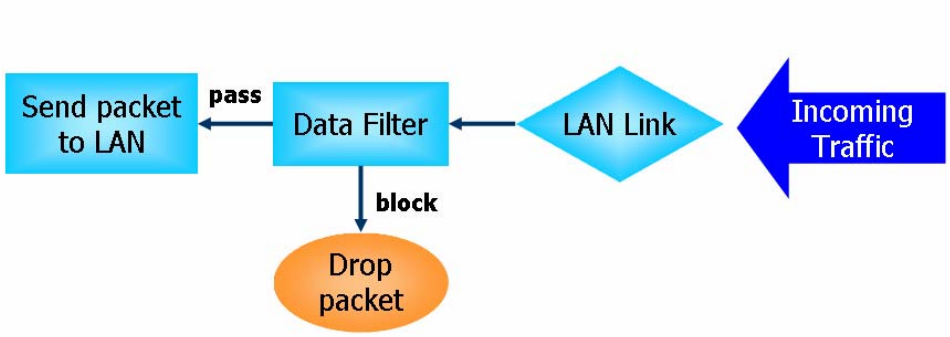
IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter -** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.





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

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

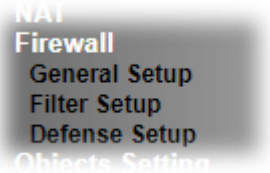
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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

Web User Interface

Below shows the menu items for Firewall.



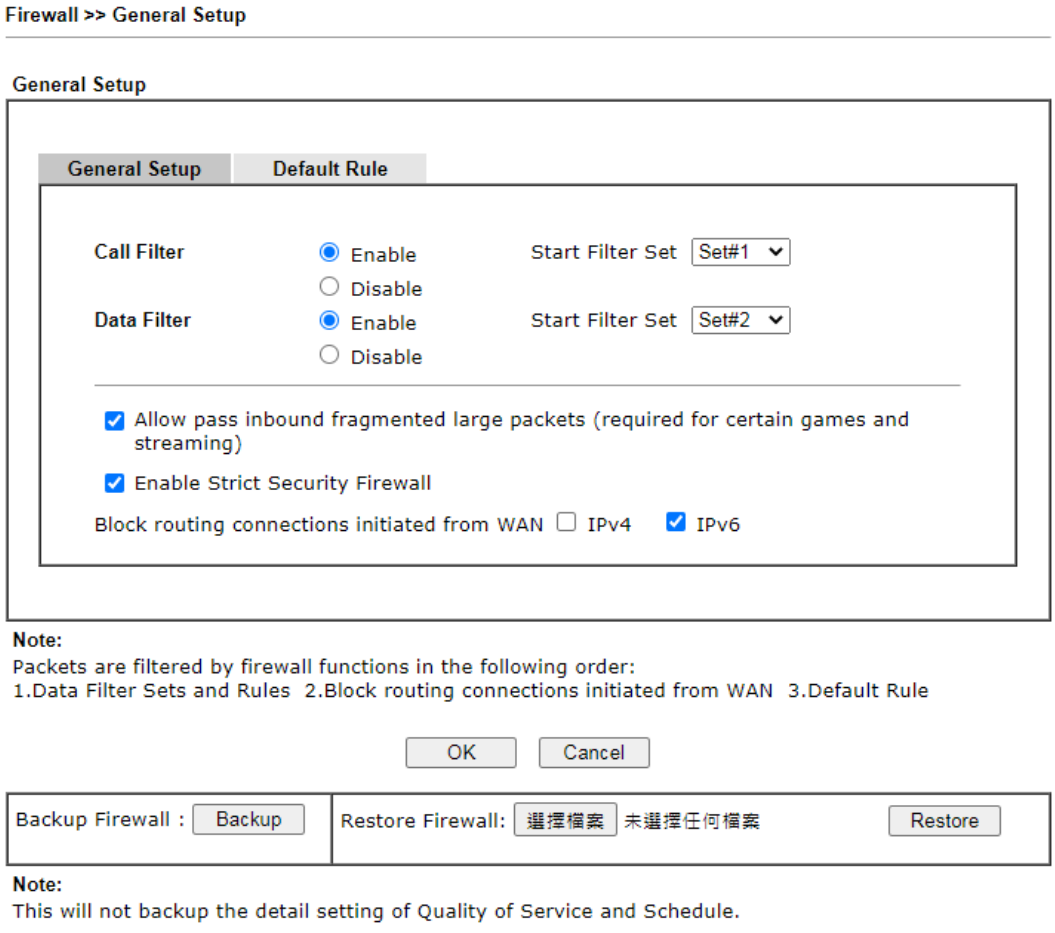
V-1-1 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

Click **Firewall** and click **General Setup** to open the general setup page.

General Setup Page

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.

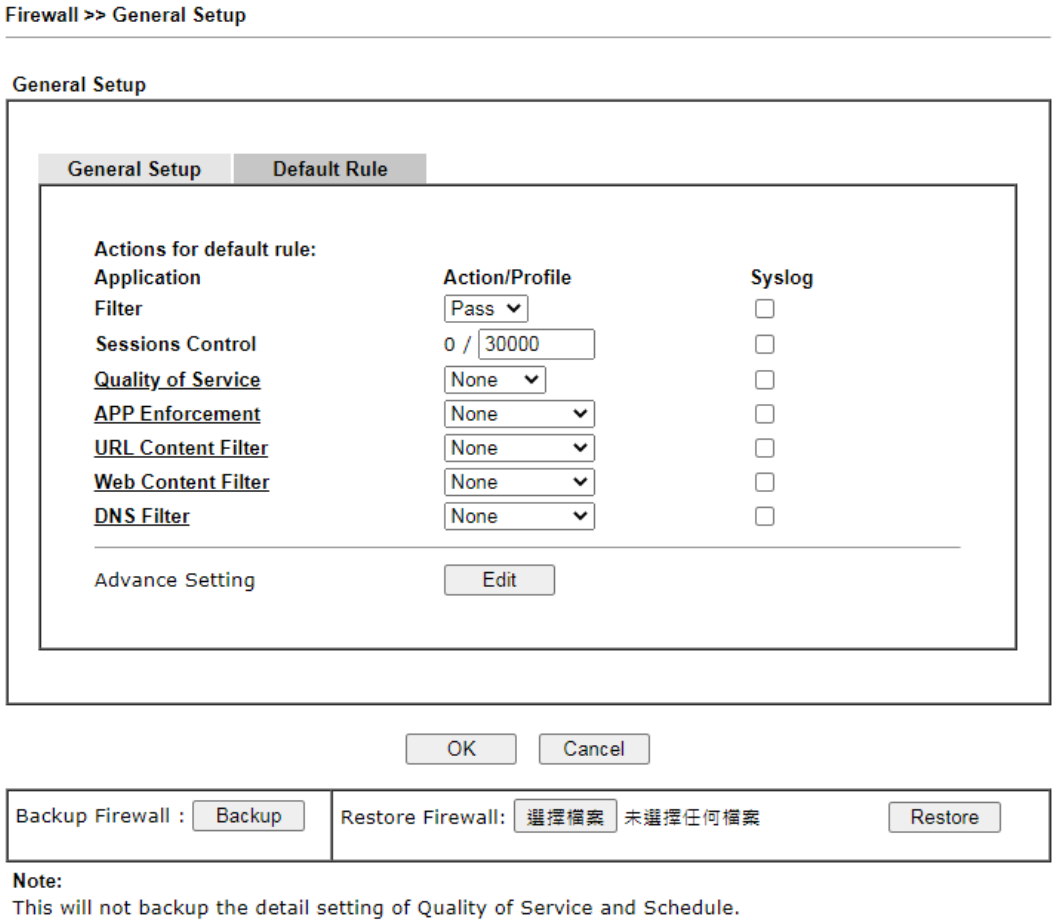


Available settings are explained as follows:

Item	Description
Call Filter	Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.
Always pass inbound fragmented large packets…	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Always pass inbound fragmented large packets…**". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "**Always pass inbound fragmented large packets…**".
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router's firewall will block the packets directly.
Block routing connections initiated from WAN	Usually, IPv6 network sessions/traffic from WAN to LAN will be accepted by IPv6 firewall in default. **IPv6** - To prevent remote client accessing into the PCs on LAN, check the box to make the packets (routed from WAN to LAN) via IPv6 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT. **IPv4** - To prevent remote client accessing into the PCs on LAN, check the box to make the incoming packets via IPv4 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.
Backup Firewall	Click **Backup** to save the firewall configuration.
Restore Firewall	Click **Select** to choose a firewall configuration file. Then click **Restore** to apply the file.

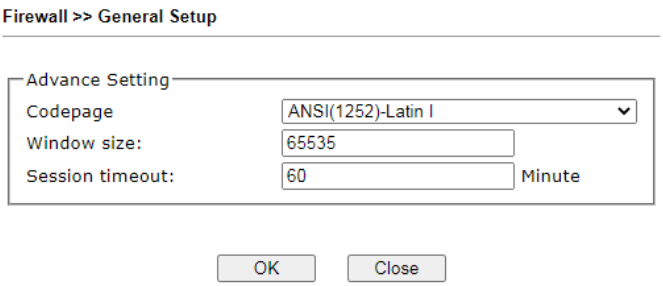
Default Rule Page

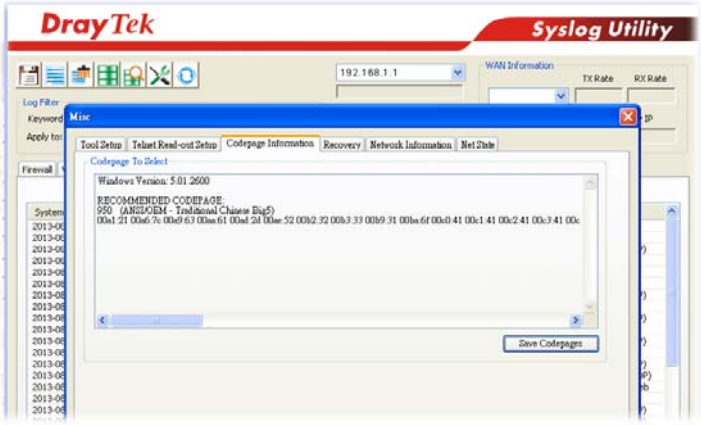
Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor router.



Available settings are explained as follows:

Item	Description
Filter	Select **Pass** or **Block** for the packets that do not match with the filter rules.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.
APP Enforcement	Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed

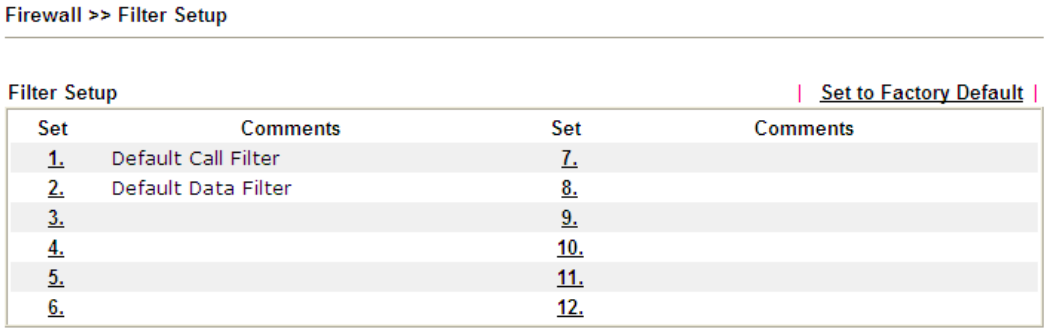
	information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
DNS Filter	Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. **Syslog** - Select to allow DNS Filter to log messages in Syslog. Logging action is configured at the profile level in the DNS Filter Profile Table section in CSM>>DNS Filter Profile, SysLog.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtain correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

	 **Window size** – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper. **Session timeout** – Setting timeout for sessions can make the best utilization of network resources.
Backup Firewall	Click **Backup** to save the firewall configuration.
Restore Firewall	Click **Select** to choose a firewall configuration file. Then click **Restore** to apply the file.

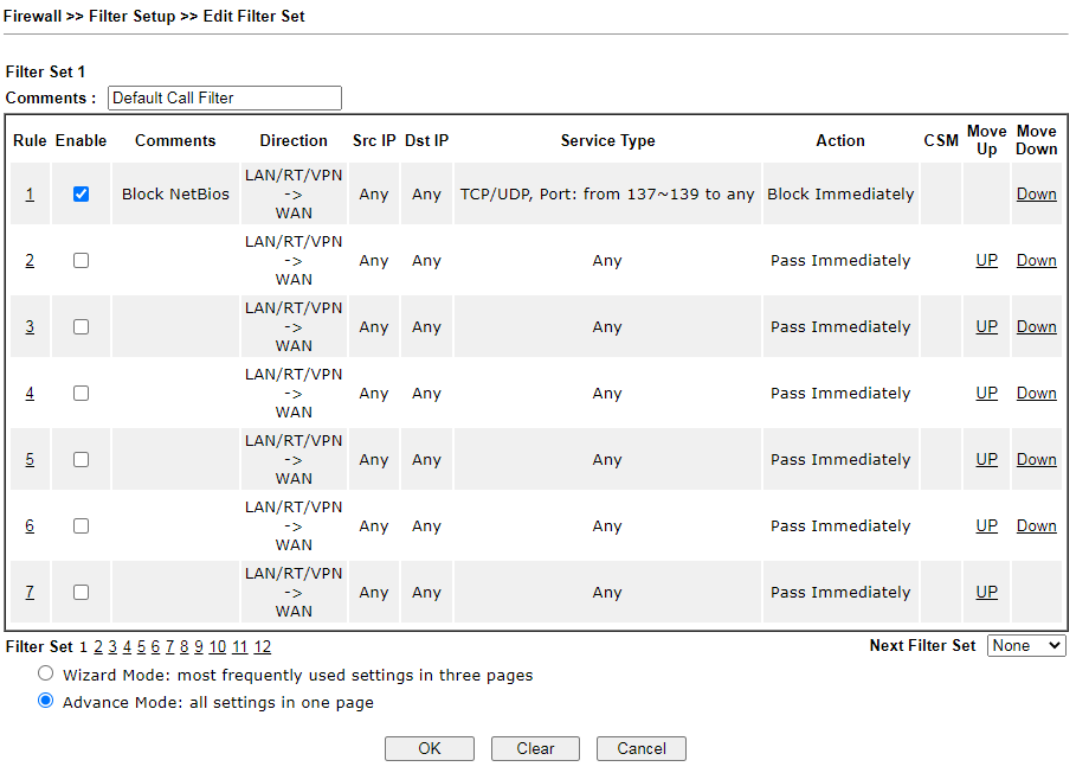
After finishing all the settings here, please click **OK** to save the configuration.

V-1-2 Filter Setup

Click **Firewall** and click **Filter Setup** to open the setup page.



To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.



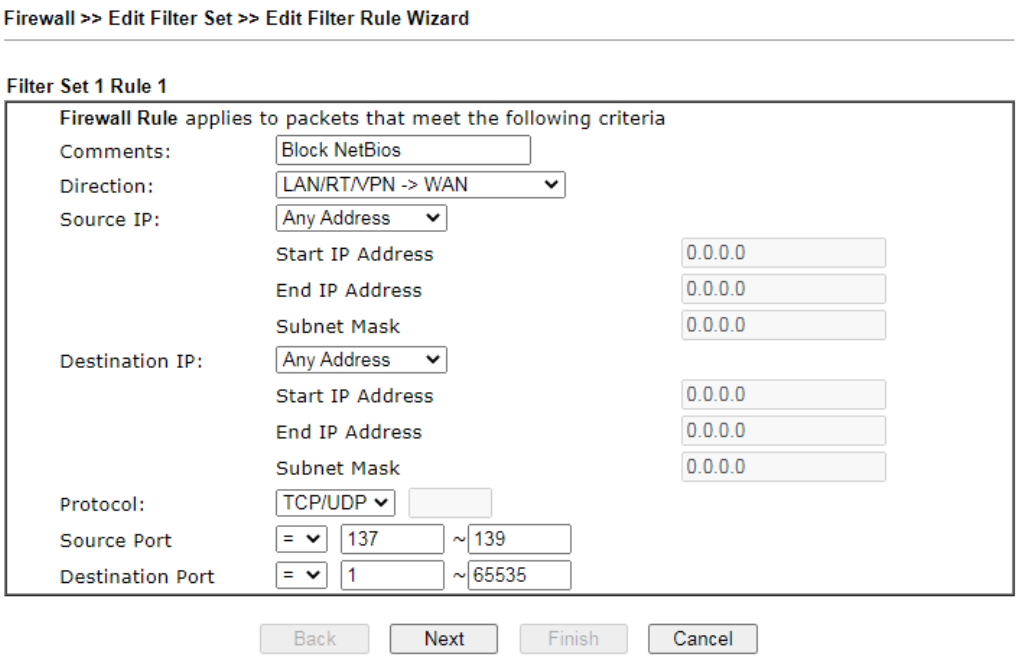
Available settings are explained as follows:

Item	Description
Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Enable	Check the box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 23-character long.
Direction	Display the direction of packet.
Src IP / Dst IP	Display the IP address of source /destination.

Service Type	Display the type and port number of the packet.
Action	Display the packets to be passed /blocked.
CSM	Display the content security managed
Move Up/Down	Use **Up** or **Down** link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.
Wizard Mode	Allow to configure frequently used settings for filter rule via several setting pages.
Advance Mode	Allow to configure detailed settings of filter rule.

To use Wizard Mode, simple do the following steps:

1. Click the **Wizard Mode** radio button.
2. Click **Index 1**. The setting page will appear as follows:



Available settings are explained as follows:

Item	Description
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Direction	Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic. **Note:** RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and Enter them in this dialog.
Protocol	Specify the protocol(s) which this filter rule will apply to.

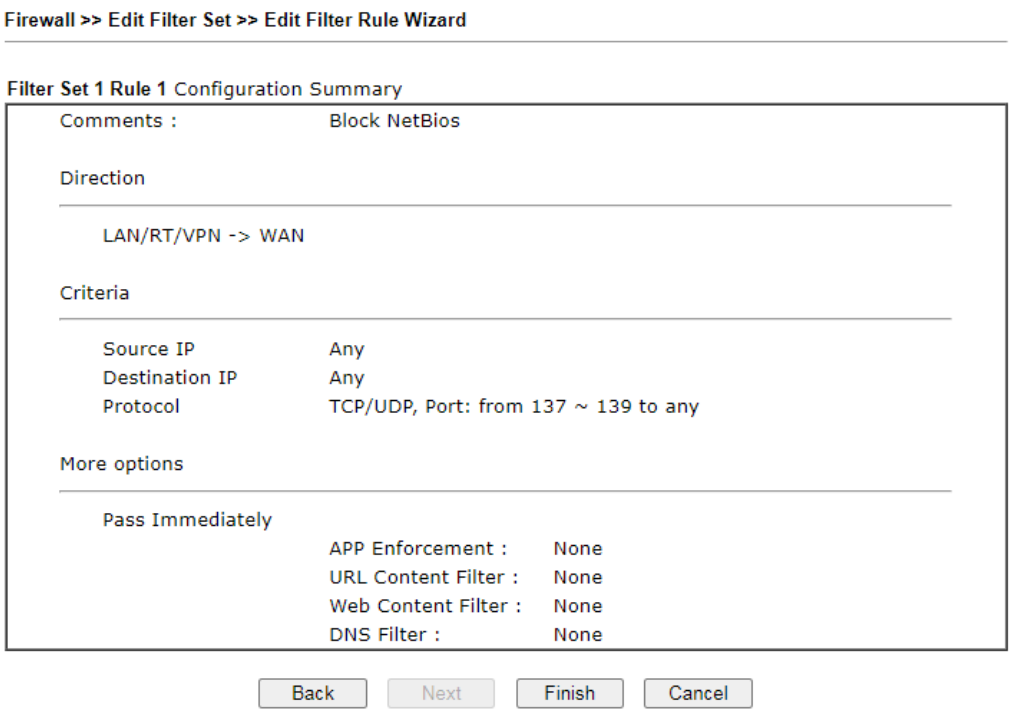
Source Port / Destination Port	*(=)* – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. *(!=)* – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. *(>)* – the port number greater than this value is available. *(<)* – the port number less than this value is available for this profile.

3. Click **Next** to get the following page.

Available settings are explained as follows:

Item	Description
Pass Immediately	Packets matching the rule will be passed immediately. **APP Enforcement -** Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. Refer to the chapter on APP Enforcement for more details on the feature. **URL Content Filter -** Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. Refer to the chapter on URL Content Filter for more details on the feature. **Web Content Filter -** Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. **DNS Filter -** Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile.
Block Immediately	Packets matching the rule will be dropped immediately.

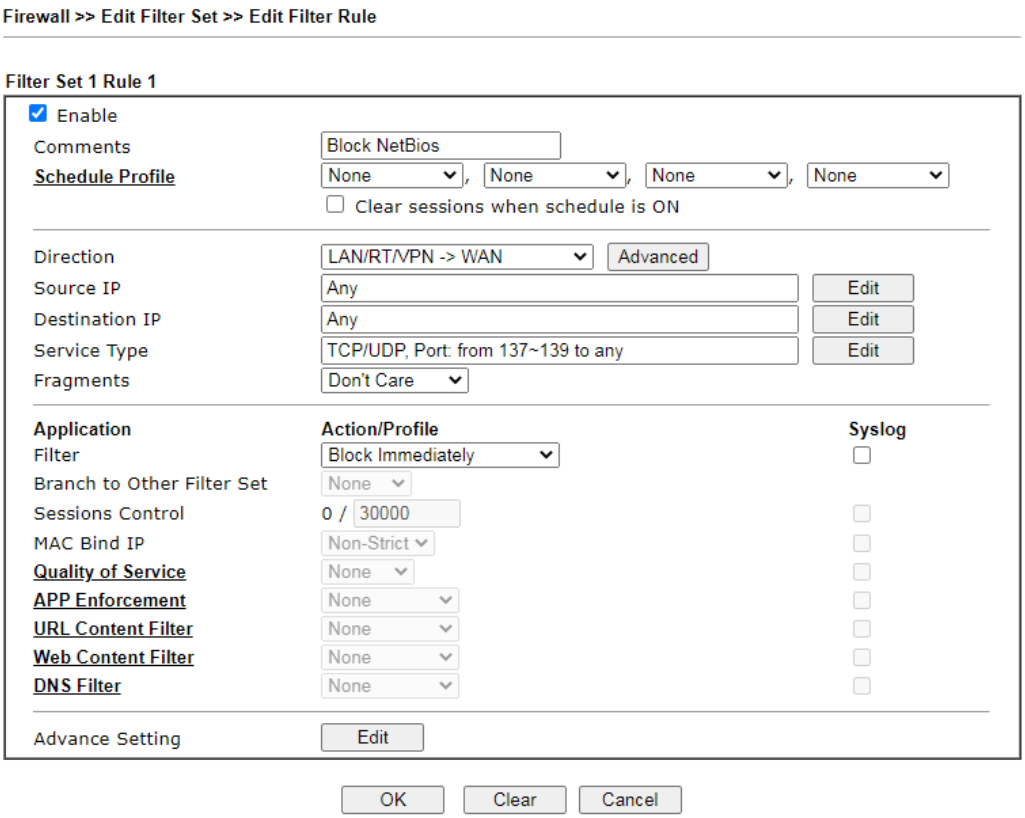
4. After choosing the mechanism, click **Next** to get the summary page for reference.



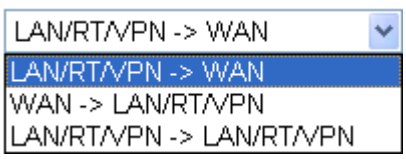
5. If there is no error, click **Finish** to complete wizard setting.

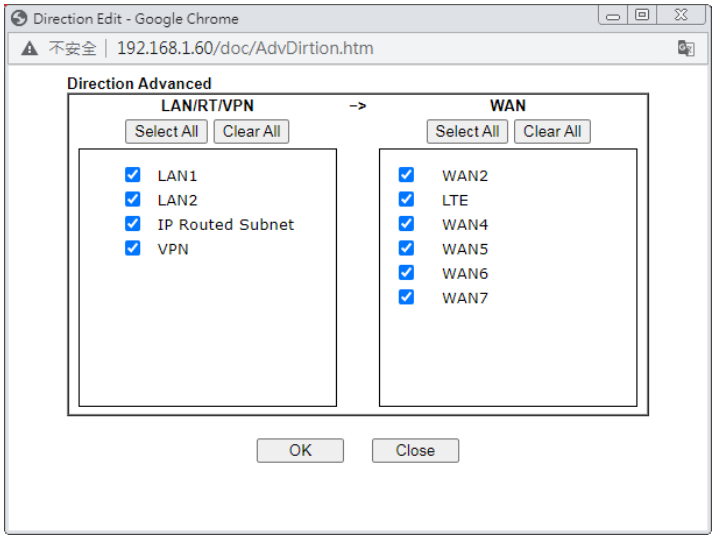
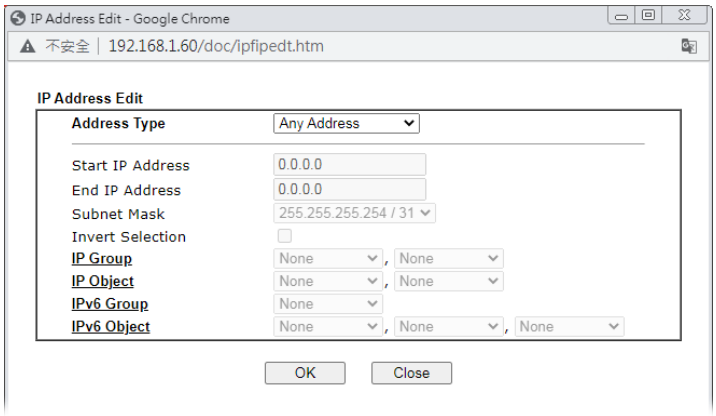
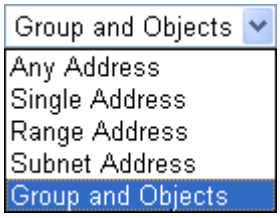
To use **Advance** Mode, do the following steps:

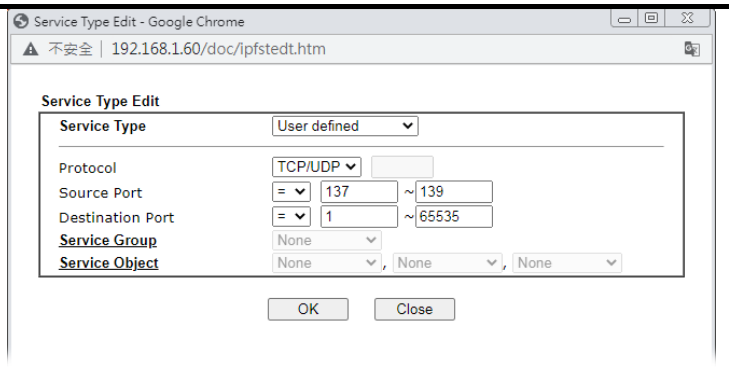
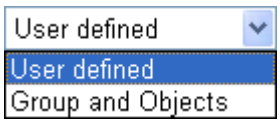
1. Click the **Advance Mode** radio button.
2. Click **Index 1** to access into the following page.

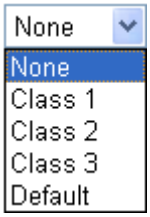


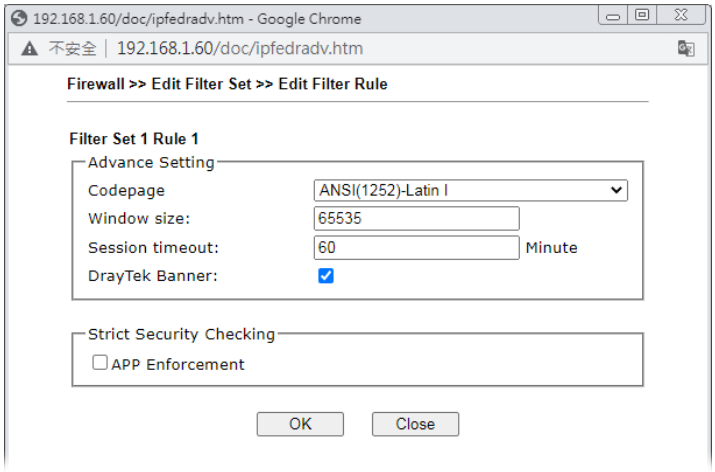
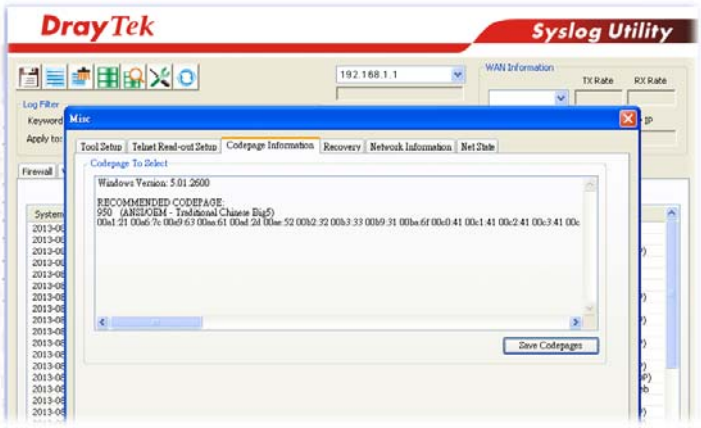
Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Schedule Profile	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
Direction	Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic.  **Note:** RT means routing domain for 2nd subnet or other LAN. **Advanced** - After choosing the direction, click the

	Advanced button to specify interfaces for traffic flow. 
Source/Destination IP	Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.  To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.  From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.
Service Type	Click **Edit** to access into the following dialog to choose a suitable service type.

	 To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.  **Protocol -** Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -** *(=)* – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. *(!=)* – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. *(>)* – the port number greater than this value is available. *(<)* – the port number less than this value is available for this profile. **Service Group/Object** - Use the drop down list to choose the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for **Data Filter** only. *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.
Filter	Specifies the action to be taken when packets match the rule. **Block Immediately -** Packets matching the rule will be dropped immediately. **Pass Immediately -** Packets matching the rule will be passed immediately. **Block If No Further Match -** A packet matching the rule, and that does not match further rules, will be dropped. **Pass If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through.

Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	**Strict** – Make the MAC address and IP address settings configured in **IP Object** for **Source IP** and **Destination IP** are bound for applying such filter rule. **No-Strict -** no limitation.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. 
APP Enforcement	Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
DNS Filter	Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. **Syslog** - Select to allow DNS Filter to log messages in Syslog. Logging action is configured at the profile level in the DNS

	Filter Profile Table section in CSM>>DNS Filter Profile, SysLog.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.  **Window size** – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper. **Session timeout**–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule. **DrayTek Banner** – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.

	 **Strict Security Checking** - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router. When the resource is inadequate, the packets will be blocked if Strict Security Checking is enabled. If Strict Security Checking is not enabled, then the packets will pass through the router.

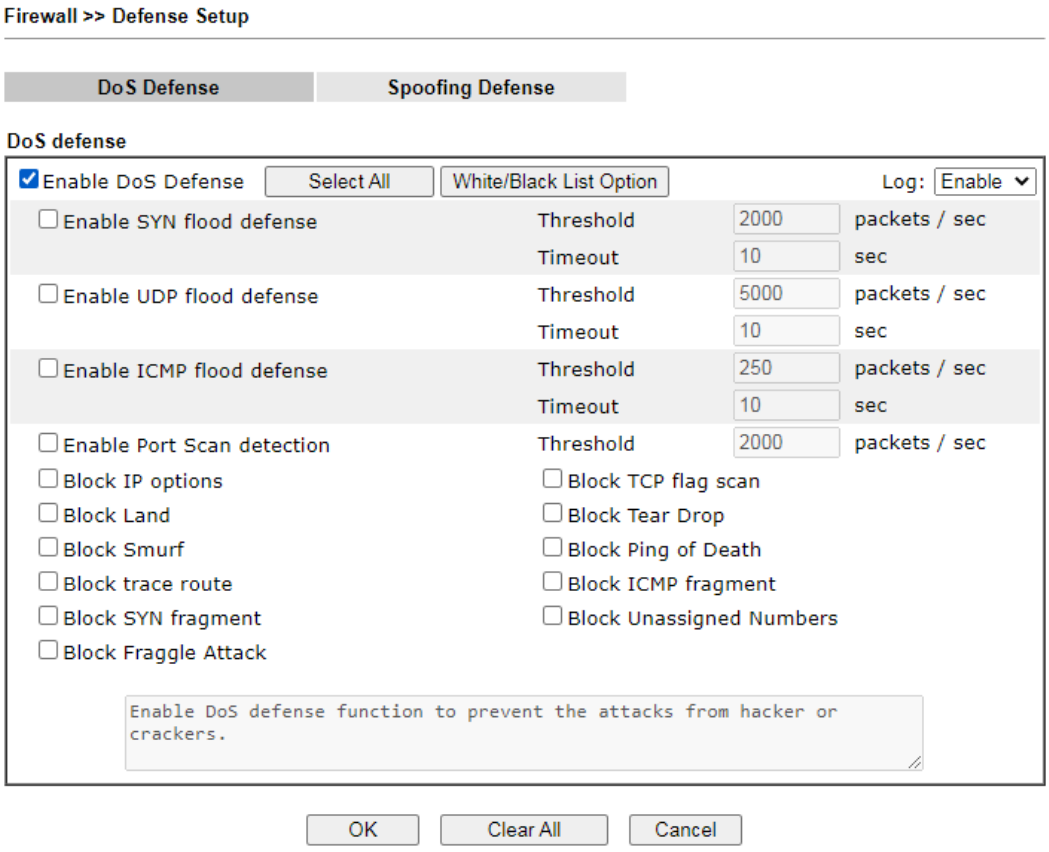
3. When you finish the configuration, please click **OK** to save and exit this page.

V-1-3 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

V-1-3-1 DoS Defense

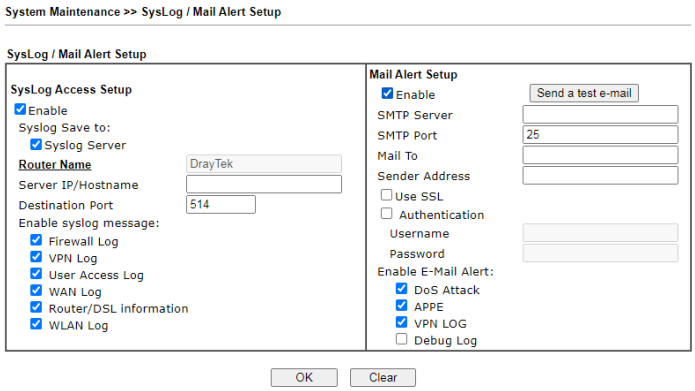
Click **Firewall** and click **DoS Defense** to open the setup page.

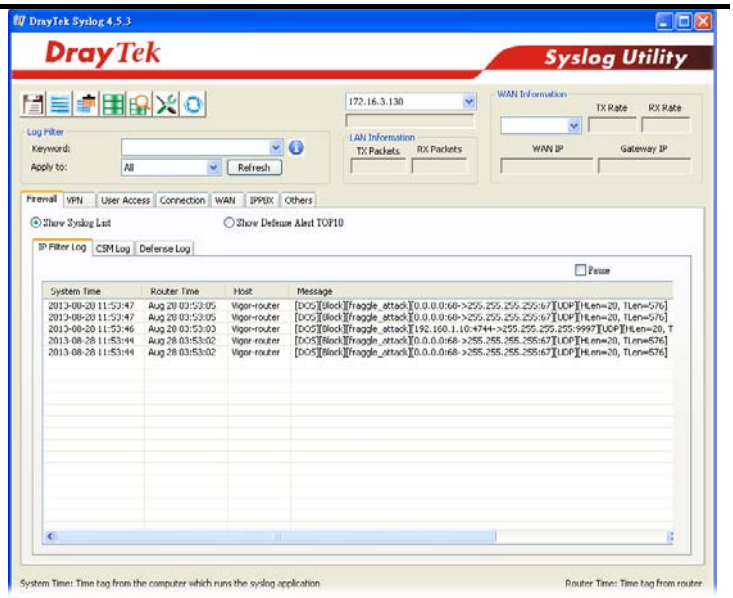


Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality. **Select All -** Click this button to select all the items listed below. **White/Black List Option** – Set white/black list of IPv4/IPv6 address.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be

	paused for 10 seconds.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable Port Scan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as "attack event".
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace route	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is

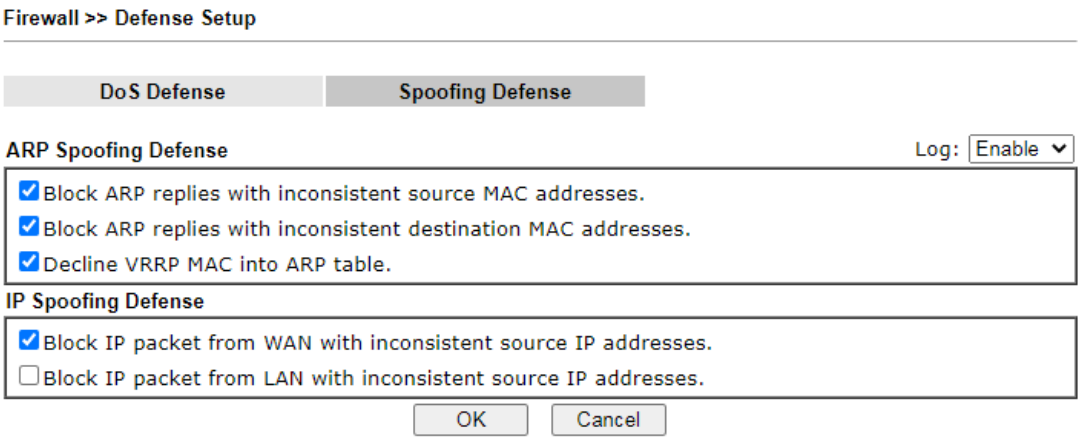
	blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. 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.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected. 



After finishing all the settings here, please click **OK** to save the configuration.

V-1-3-2 Spoofing Defense

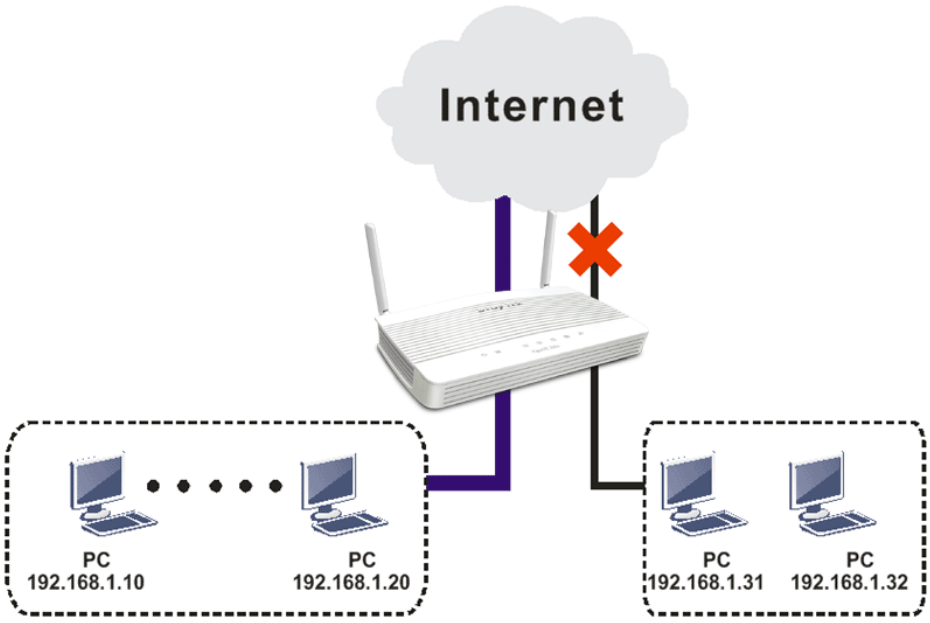
Click the **Spoofing Defense** tab to open the setup page.



Application Notes

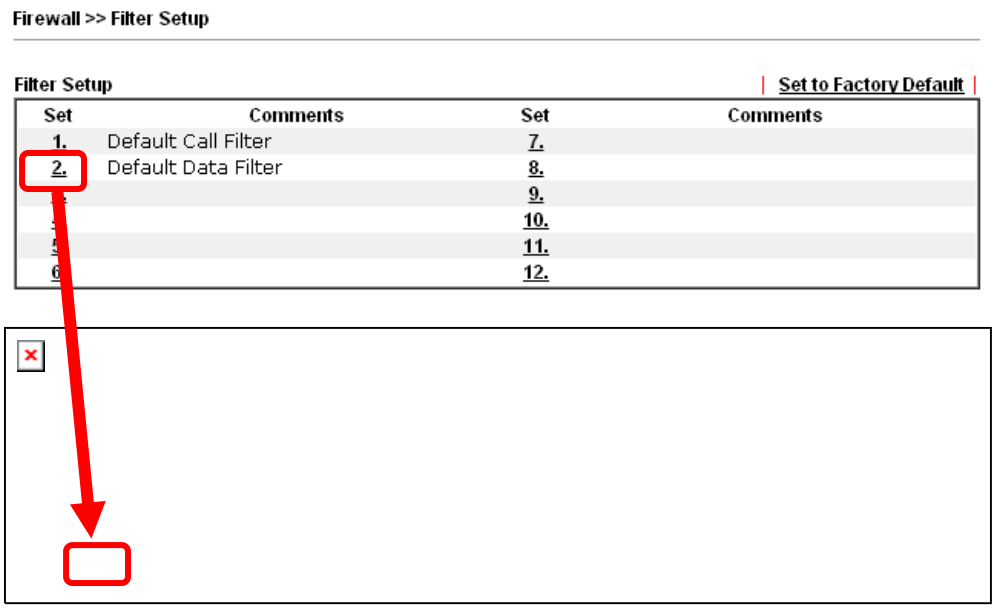
A-1 How to Configure Certain Computers Accessing to Internet

We can specify certain computers (e.g., 192.168.1.10 ~ 192.168.1.20) accessing to Internet through Vigor router. Others (e.g., 192.168.1.31 and 192.168.1.32) outside the range can get the source from LAN only.

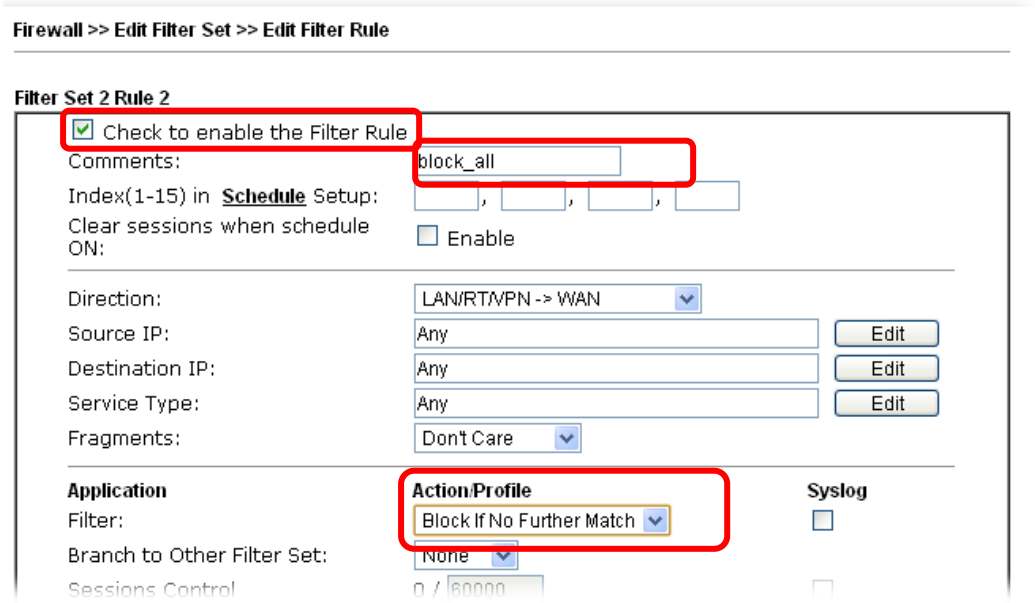


The way we can use is to set two rules under **Firewall**. For **Rule 1** of **Set 2** under **Firewall>>Filter Setup** is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

1. Access into the web user interface of Vigor router.
2. Open **Firewall>>Filter Setup**. Click the **Set 2** link, choose **Advance** Mode and choose the **Filter Rule 2** button.



3. Check the box of **Check to enable the Filter Rule**. Enter the comments (e.g., **block_all**). Choose **Block If No Further Match** for the **Filter** setting. Then, click **OK**.

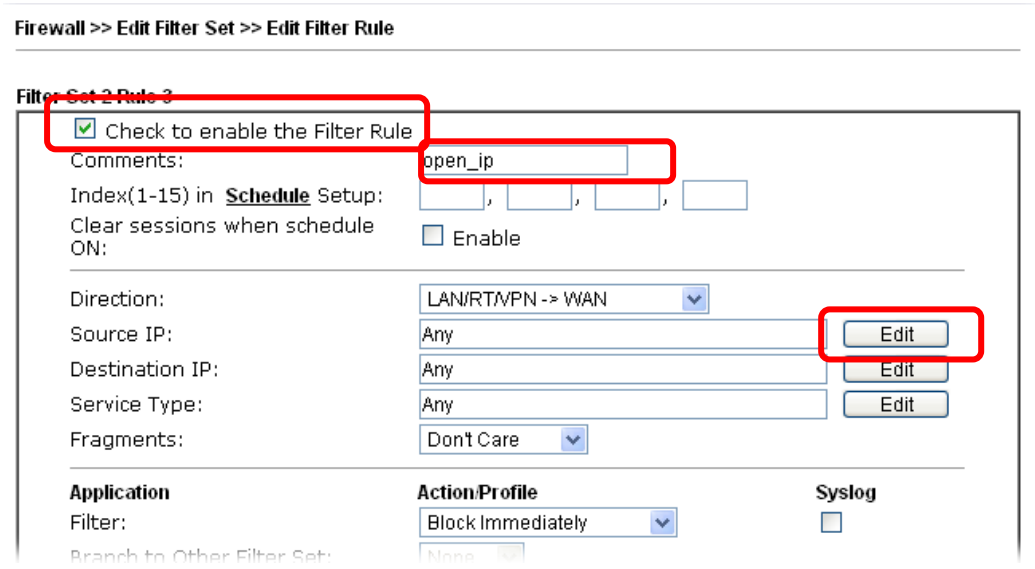


Info

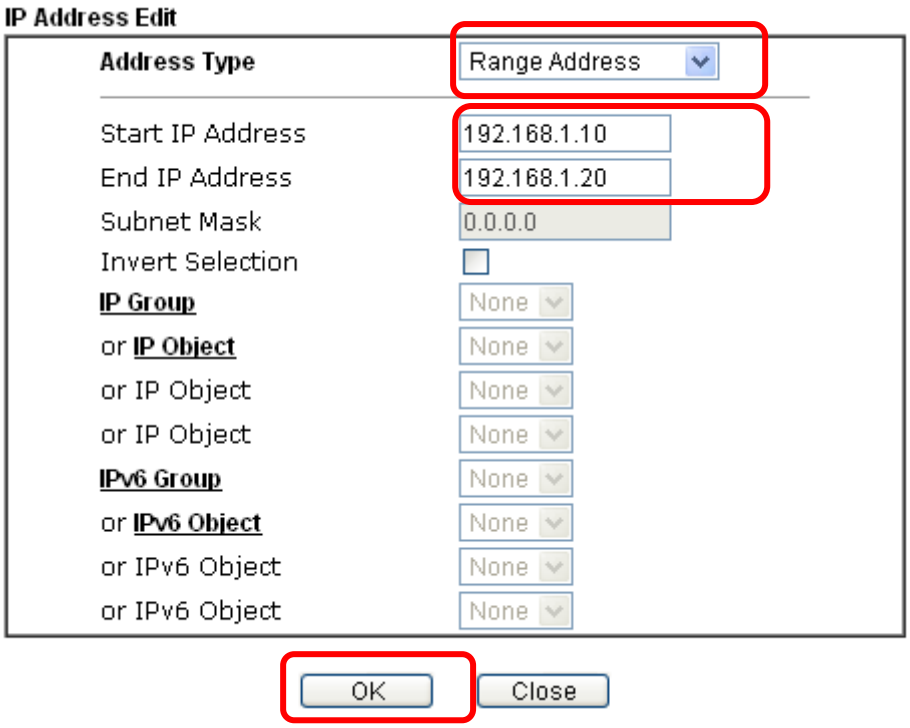
In default, the router will check the packets starting with Set 2, Filter Rule 2 to Filter Rule 7. If Block If No Further Match for is selected for Filter, the firewall of the router would check the packets with the rules starting from Rule 3 to Rule 7. The packets not matching with the rules will be processed according to Rule 2.

4. Next, set another rule. Just open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 3** button.

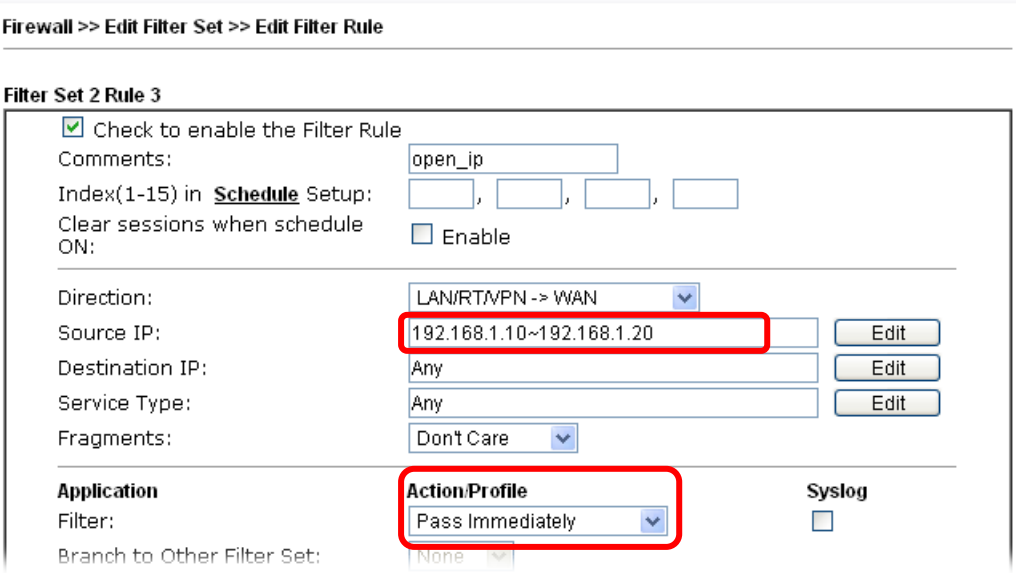
5. Check the box of **Check to enable the Filter Rule**. Enter the comments (e.g., **open_ip**). Click the **Edit** button for **Source IP**.



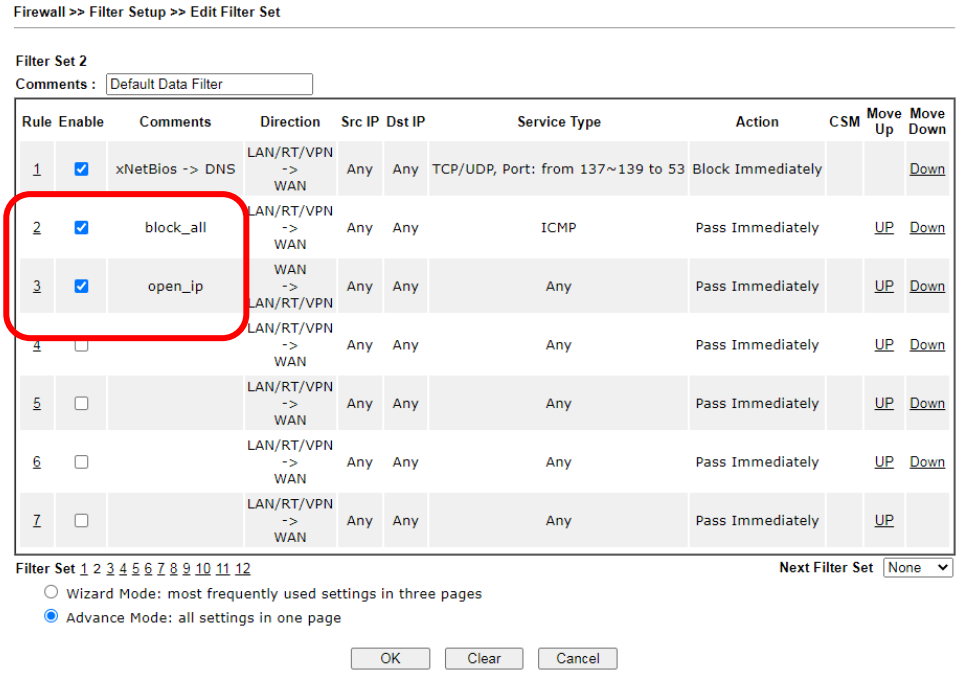
6. A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.



7. Now, check the content of **Source IP** is correct or not. The action for **Filter** shall be set with **Pass Immediately.** Then, click **OK** to save the settings.



8. Both filter rules have been created. Click **OK**.



Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments : Default Data Filter

Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	☑	xNetBios -> DNS	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53	Block Immediately			Down
2	☑	block_all	LAN/RT/VPN -> WAN	Any	Any	ICMP	Pass Immediately		UP	Down
3	☑	open_ip	WAN -> LAN/RT/VPN	Any	Any	Any	Pass Immediately		UP	Down
4	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12 Next Filter Set None

○ Wizard Mode: most frequently used settings in three pages

◉ Advance Mode: all settings in one page

OK Clear Cancel

Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

V-2 Central Security Management (CSM)

CSM is an abbreviation of **Central Security Management** which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

APP Enforcement Filter

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserved attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user Enter or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

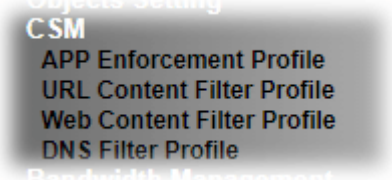
Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

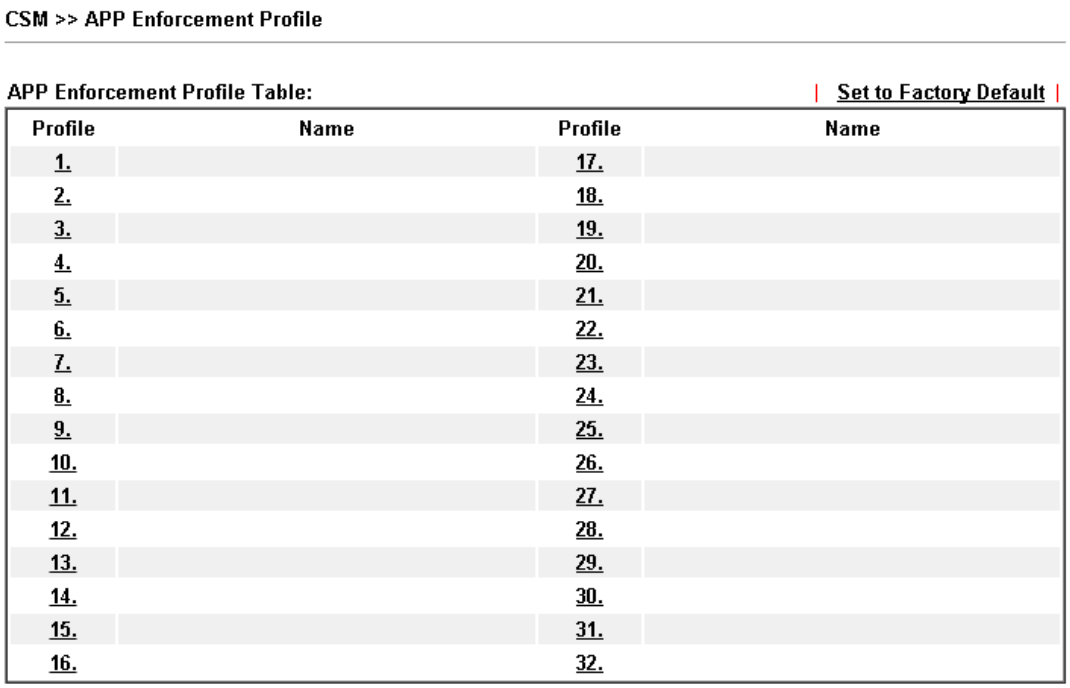
Info	The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface



V-2-1 APP Enforcement Profile

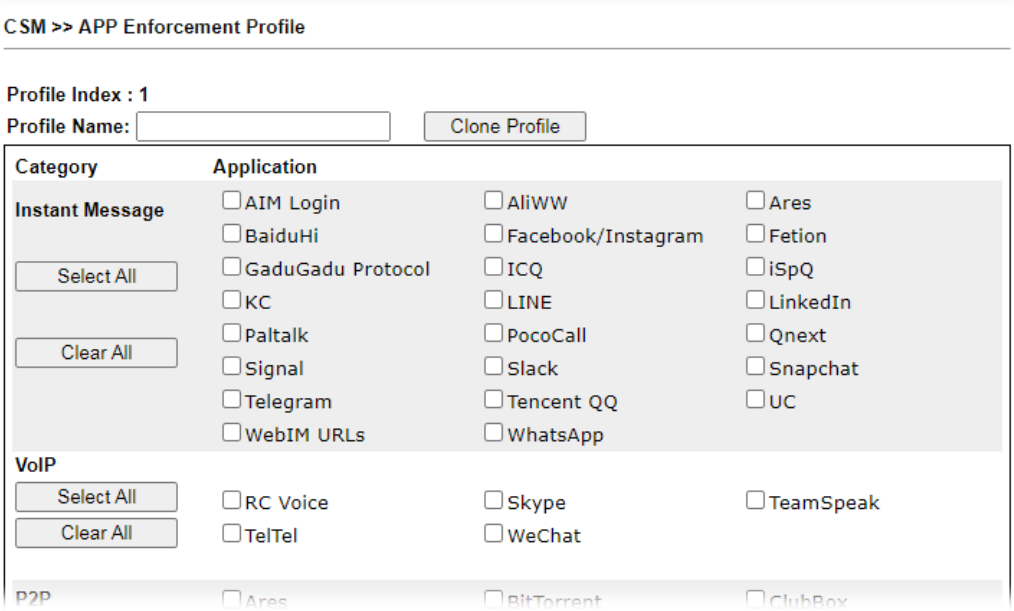
You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/Misc application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the APP Enforcement Profile.

Click the number under Index column for settings in detail.



Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.
Enable	Check the box to select the APP to be blocked by Vigor router.

The profiles configured here can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

V-2-2 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

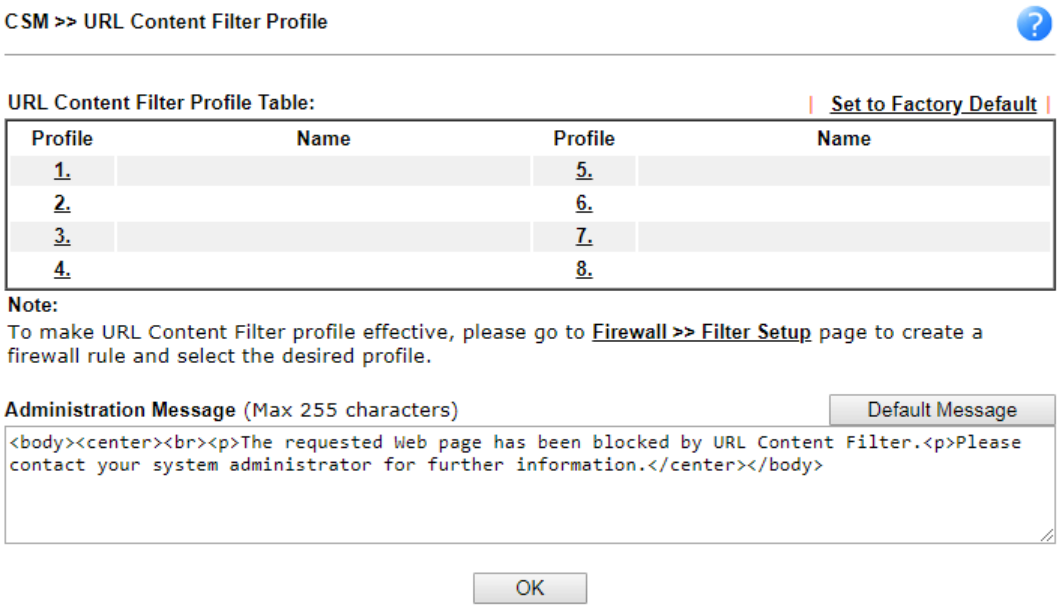
Once a user Enter or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click **CSM** and click **URL Content Filter Profile** to open the profile setting page.

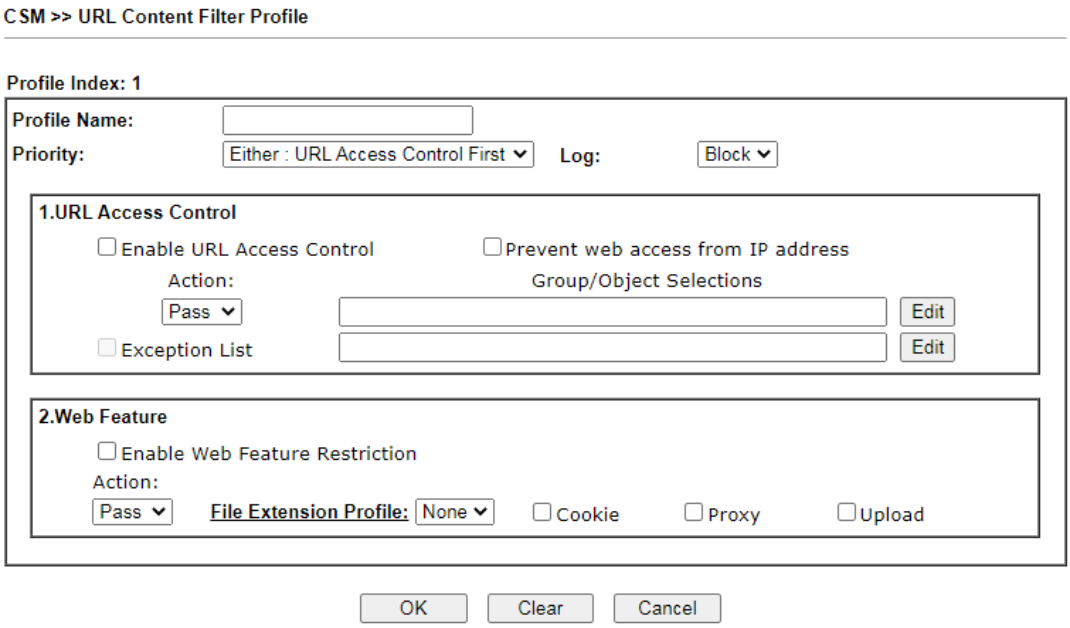


Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.

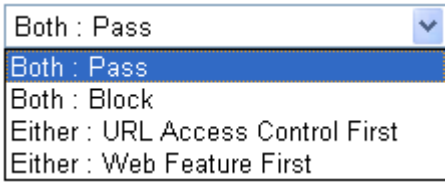
Administration Message	You can Enter the message manually for your necessity. **Default Message** - You can Enter the message manually for your necessity or click this button to get the default message which will be displayed on the field of **Administration Message**.

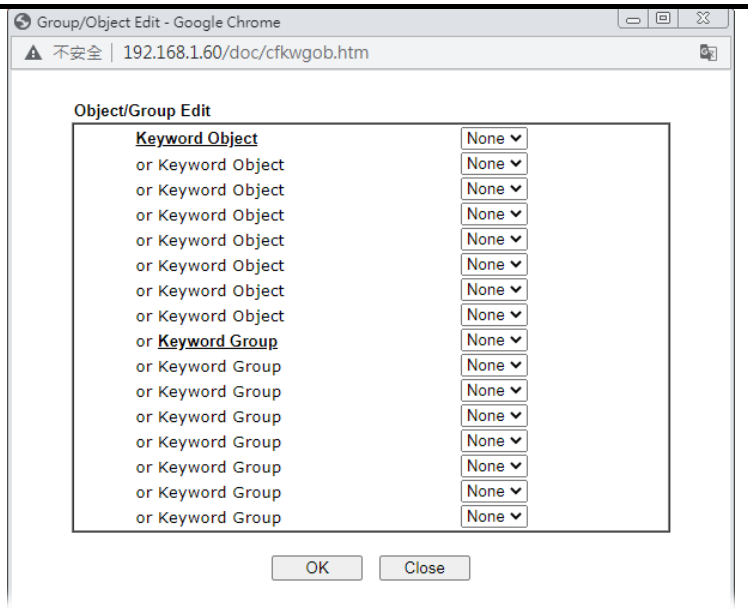
You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.

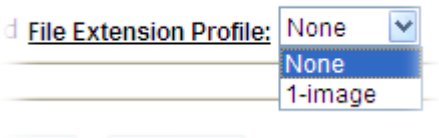


Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	It determines the action that this router will apply. **Both: Pass** – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. **Both:Block** –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. **Either: URL Access Control First** – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second. **Either: Web Feature First** –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.

	
Log	**Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog.
URL Access Control	**Enable URL Access Control** - Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature. **Prevent web access from IP address** - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before. **Action** – This setting is available only when **Either : URL Access Control First** or **Either : Web Feature First** is selected. ● *Pass* - Allow accessing into the corresponding webpage with the keywords listed on the box below. ● *Block* - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. **Exception List** – Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above. **Group/Object Selections** – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.



Web Feature	**Enable Web Feature Restriction-** Check this box to make the keyword being blocked or passed. **Action -** This setting is available only when **Either: URL Access Control First** or **Either: Web Feature First** is selected. *Pass* **-** Allow accessing into the corresponding webpage with the keywords listed on the box below. *Block* **-** Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. **File Extension Profile –** Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.  **Cookie** - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. **Proxy** - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. **Upload** – Check the box to block the file upload by way of web page.

After finishing all the settings, please click **OK** to save the configuration.

V-2-3 Web Content Filter Profile

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

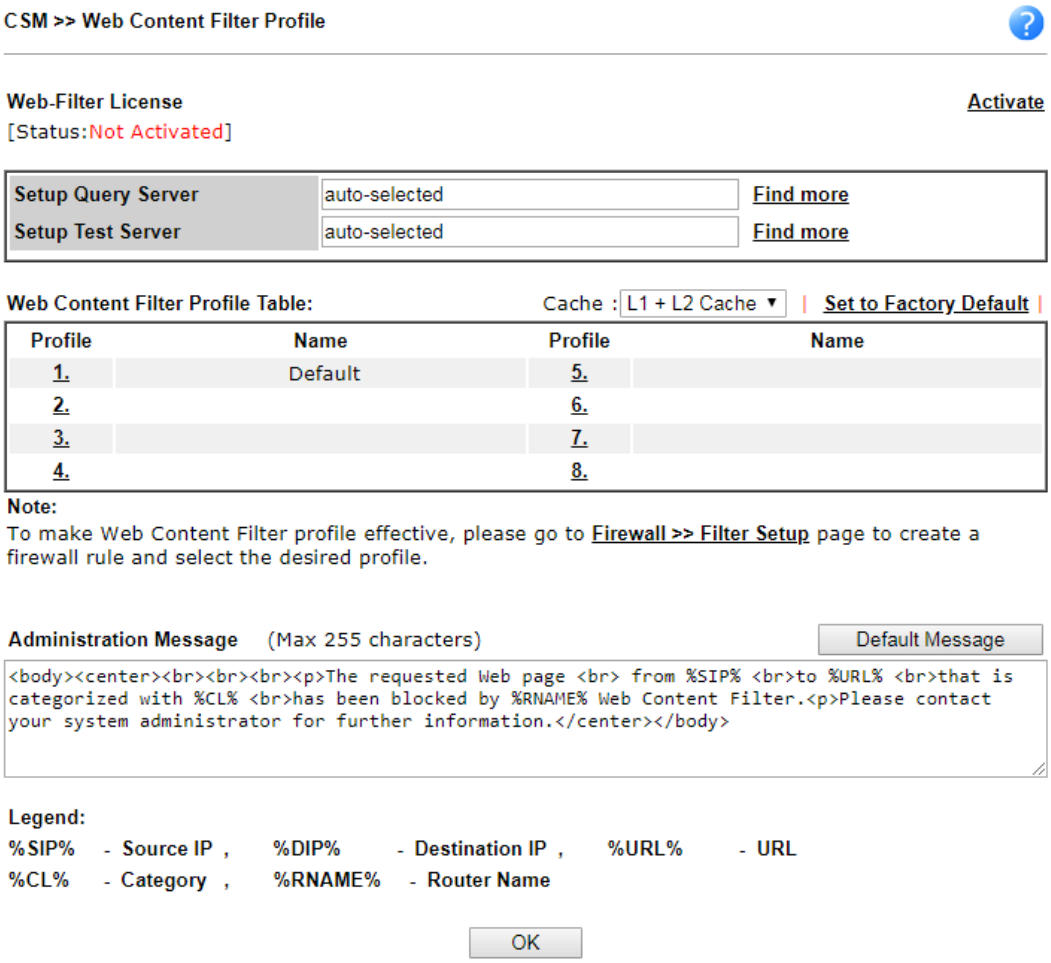
Service Activation Wizard allows you to use trial version of WCF directly without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (***MyVigor***) located on http://myvigor.draytek.com. Therefore, you need to register an account on http://myvigor.draytek.com for using corresponding service. Please refer to section of creating MyVigor account.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with Vigor router currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open http://myvigor.draytek.com for searching another qualified and suitable one.

Info 1	Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by Commtouch. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.
Info 2	Commtouch is merged by Cyren, and GlobalView services will be continued to deliver powerful cloud-based information security solutions! Refer to: http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

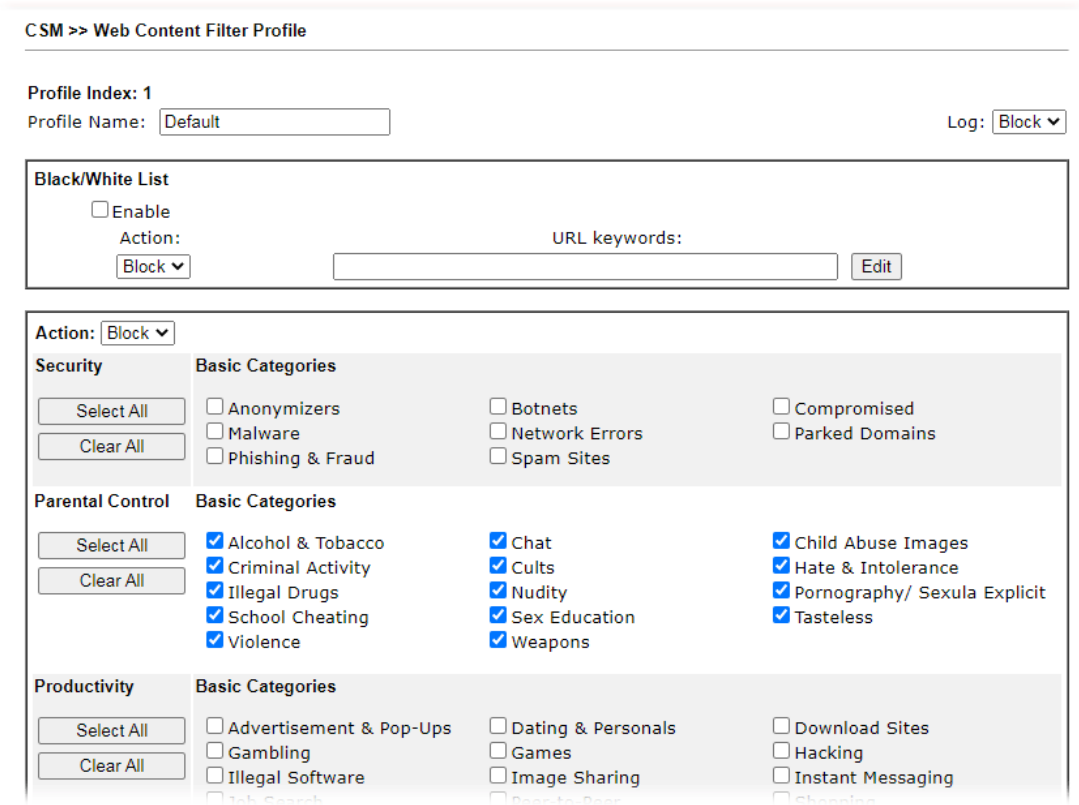


Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile. **Find more -** Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Setup Test Server	It is recommended for you to use the default setting, auto-selected. **Find more -** Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Cache	**None** – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching. **L1** – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate. **L2** – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized

	for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate. **L1+L2 Cache** – the router will check the URL with fast processing rate combining the feature of L1 and L2.
Set to Factory Default	Click this link to retrieve the factory settings.
Administration Message	You can Enter the message manually for your necessity or click **Default Message** button to get the default text displayed on the field of **Administration Message**.

Eight profiles are provided here as Web content filters. Simply click the index number under Profile to open the following web page. The items listed in Categories will be changed according to the different service providers. If you have and activate another web content filter license, the items will be changed simultaneously. All of the configuration made for web content filter will be deleted automatically. Therefore, please backup your data before you change the web content filter license.



Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Log	**Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog.
Black/White List	**Enable –** Activate white/black list function for such profile. **URL keywords –** Click **Edit** to choose the group or object profile as the content of white/black list.

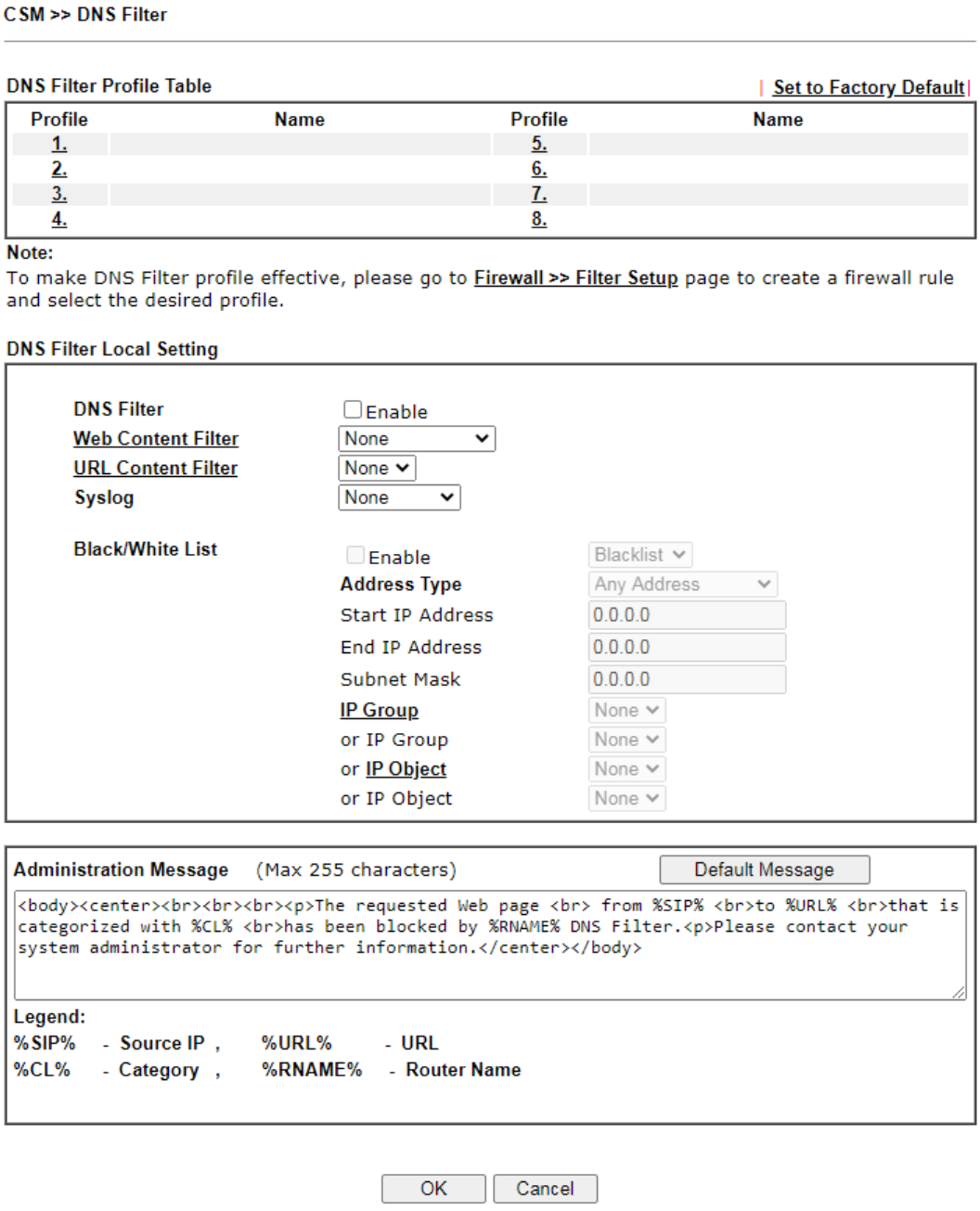
	Pass - **allow** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. **Block** - **restrict** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.
Action	**Pass** - allow accessing into the corresponding webpage with the categories listed on the box below. **Block** - restrict accessing into the corresponding webpage with the categories listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action.

After finishing all the settings, please click **OK** to save the configuration.

V-2-4 DNS Filter Profile

DNS Filter blocks or allows traffic to the WAN by intercepting DNS queries, and applying UCF and WCF rules to hostnames. DNS filtering is especially useful when you wish to restrict access of protocols other than HTTP, such as HTTPS. Note that a WCF license must have already been activated before WCF rules could be used.

To configure DNS Filter Profiles, select **CSM >> Web Content Filter Profile** from the main menu.



Available settings are explained as follows:

Item	Description
DNS Filter Profile Table	DNS Filter Profiles take effect when DNS servers on the WAN are used for DNS queries. The router intercepts all outgoing DNS queries on UDP port 53 and applies WCF and UCF rules

	on the domain names before passing the queries to the DNS servers. IP addresses of the domains are then blocked or allowed as per applicable WCF and UCF rules. DNS Filter Profiles can be applied by selecting from Firewall filter rules. **Profile -** Index number of the profile. Click to bring up the configuration page for the profile entry. **Name -** Name that identifies the profile.
Set to Factory Default	Clear all DNS Filter profile settings.
DNS Filter Local Setting	By setting the IP address of the DNS lookup server to the router's address, the router serves as a DNS lookup proxy server. When DNS Filter Local Setting is enabled, all DNS queries sent to the router will have WCF and UCF rules applied to the hostnames, and access to the resolved IP addresses will be allowed or blocked as configured in the rules. **DNS Filter -** Select to enable DNS Filter Local Setting. **Web Content Filter -** Select a WCF profile. **URL Content Filter** - Select a UCF profile. **Syslog -** The filtering result can be recorded according to the setting selected for Syslog. ● **None –** No log file will be created for this profile. ● **Pass –** Only passed access attempts will be recorded in Syslog. ● **Block –** Only blocked access attempts will be recorded in Syslog. ● **Both –** Both passed and blocked access attempts will be recorded in Syslog. **Black/White List –** Specify IP address, subnet mask, IP object, or IP group as a black list or white list for DNS packets passing through or blocked by Vigor router.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box. You can embed the following variables in the message: ● %SIP% – The source IP address that attempted the HTTP access. ● %DIP% – The destination IP address to which access was attempted. ● %URL% – The URL of the destination website. ● %CL% – The category to which the URL belongs. ● %RNAME% – The name of the router. **Default Message** - Click to reset the administration message to the factory default.

To save changes on the page, click **OK**. To discard changes, click **Cancel**.

Application Notes

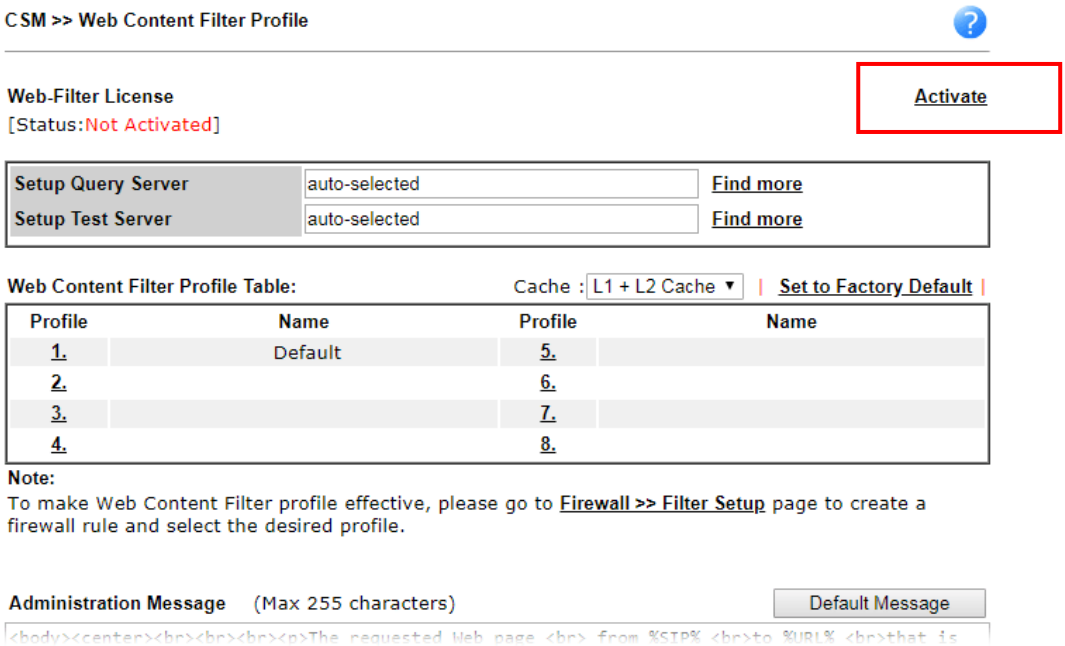
A-1 How to Create an Account for MyVigor

The website of MyVigor (a server located on http://myvigor.draytek.com) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor.

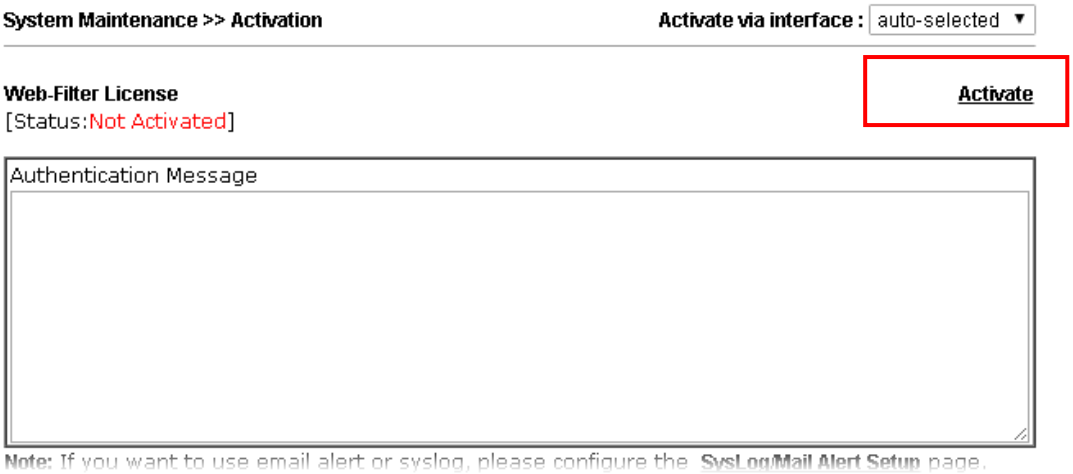
Create an Account via Vigor Router

1. Click **CSM>> Web Content Filter Profile**. The following page will appear.

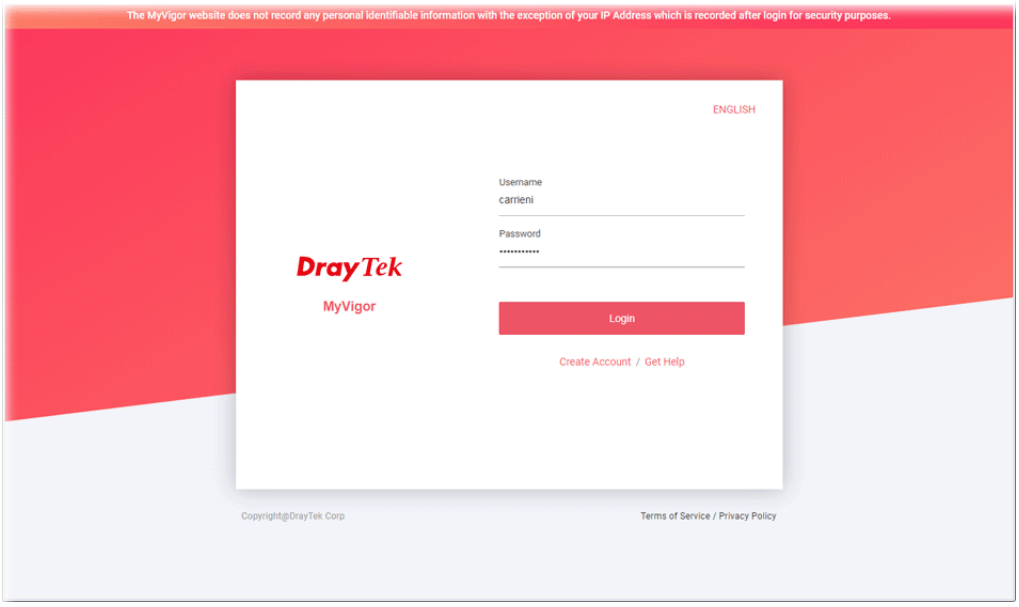


Or

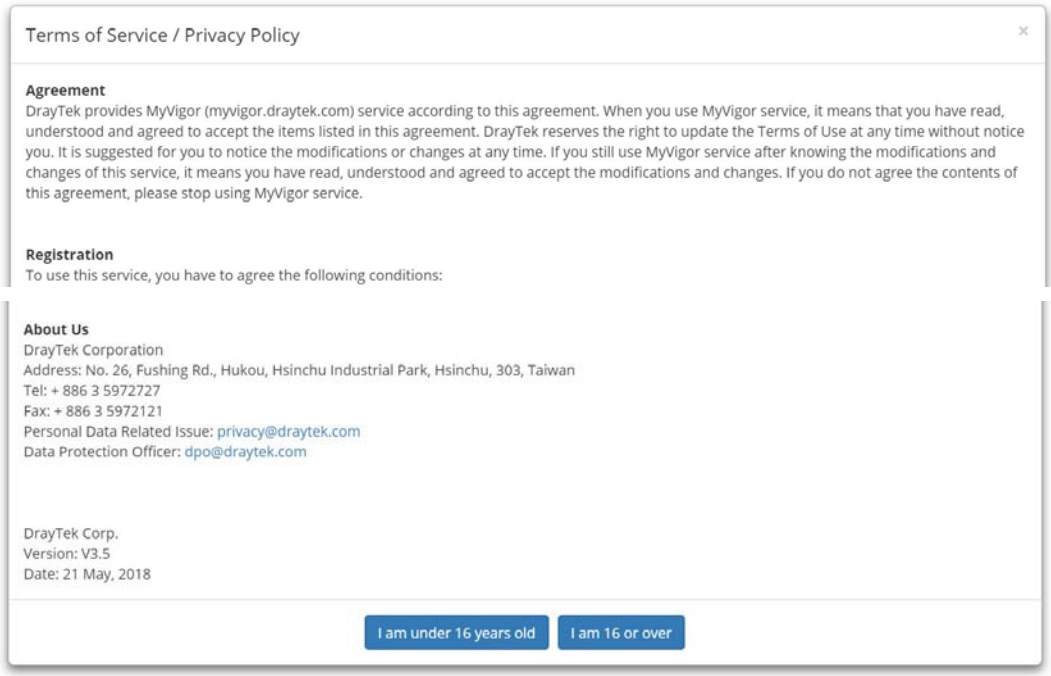
Click **System Maintenance>>Activation** to open the following page.



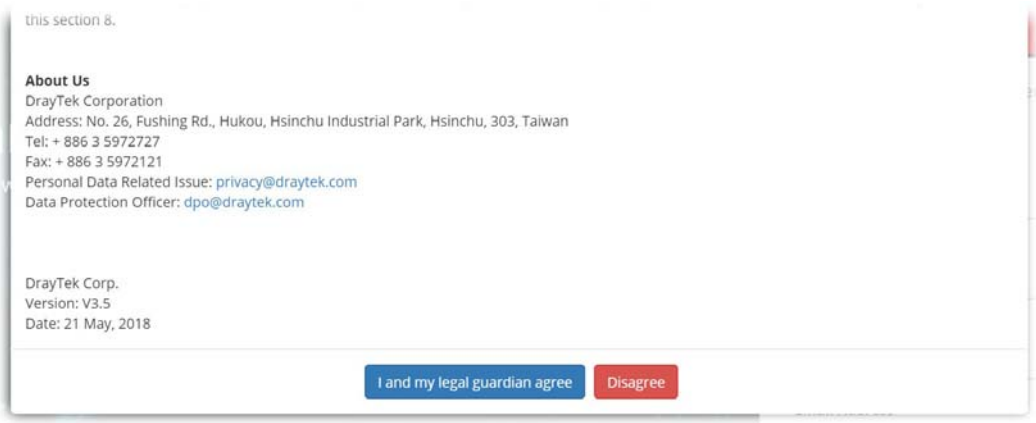
2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.



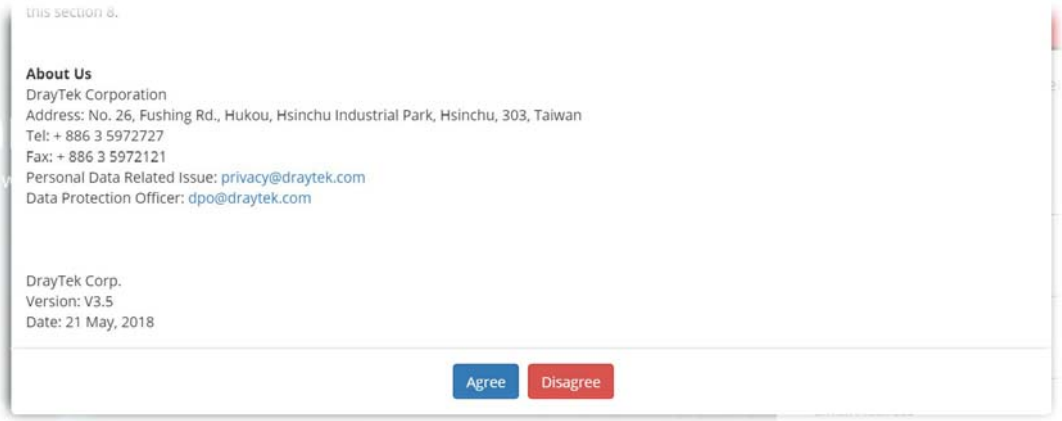
3. Click the link of **Create an account now**.
4. The system will ask if you are 16 years old or over.
   - If yes, click **I am 16 or over**.



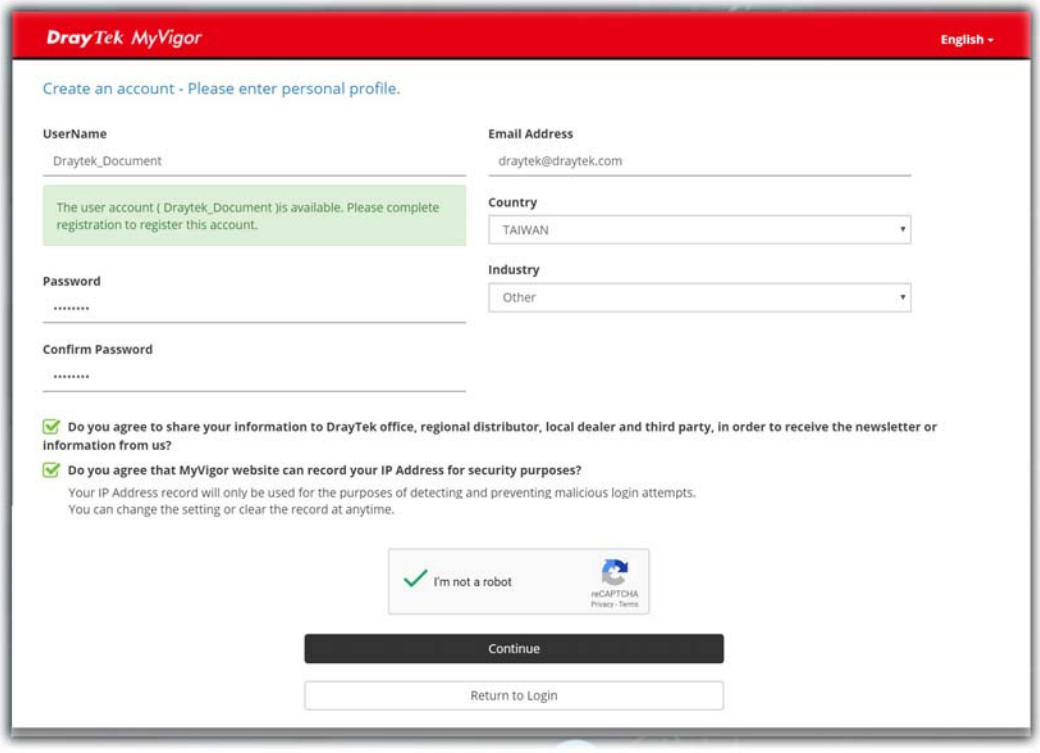
- If not, click **I am under 16 years old** to get the following page. Then, click **I and my legal guardian agree**.



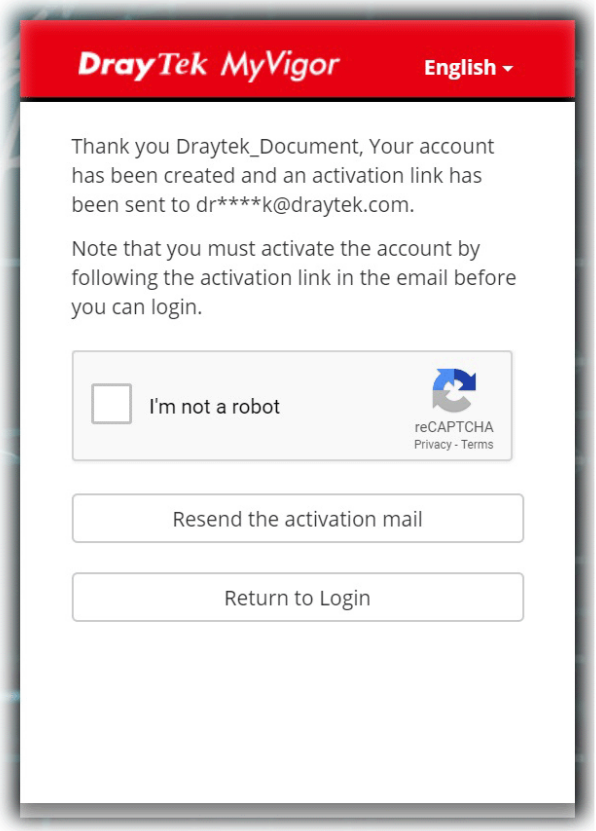
5. After reading the terms of service/privacy policy, click **Agree**.



6. In the following page, enter your personal information in this page and then click **Continue**.



7. Choose proper selection for your computer and click **Continue**.



8. Now you have created an account successfully.
9. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

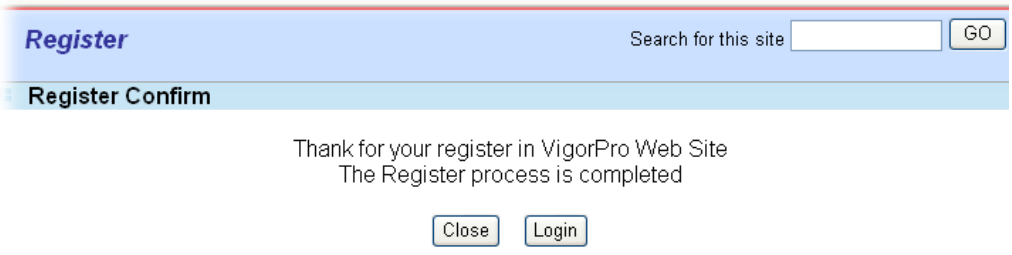
****** This is an automated message from myvigor.draytek.com. ******

Thank you (**Mary**) for creating an account.

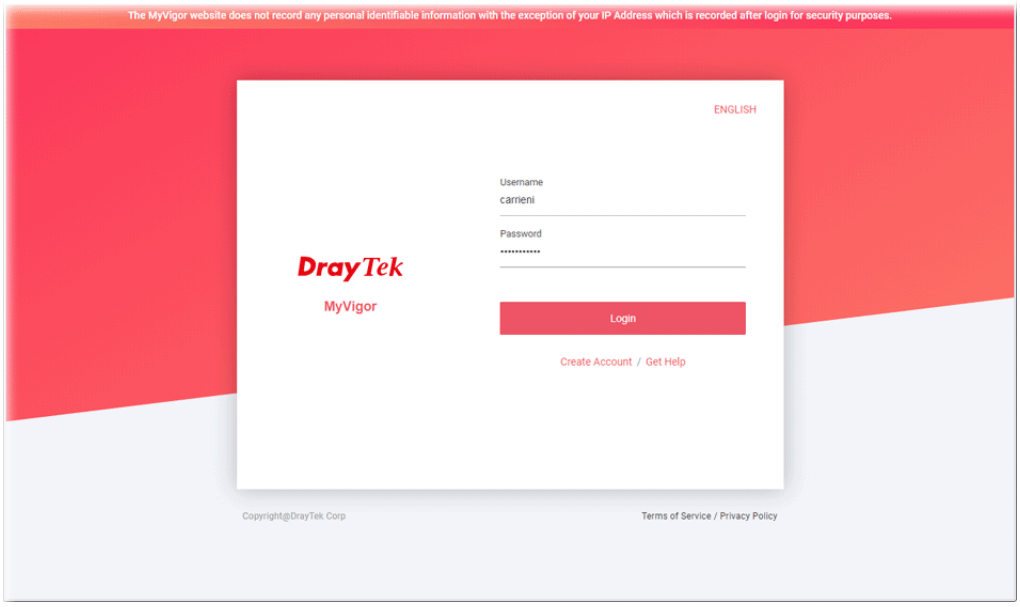
Please click on the activation link below to activate your account

Link : Activate my Account

10. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



11. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.



12. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

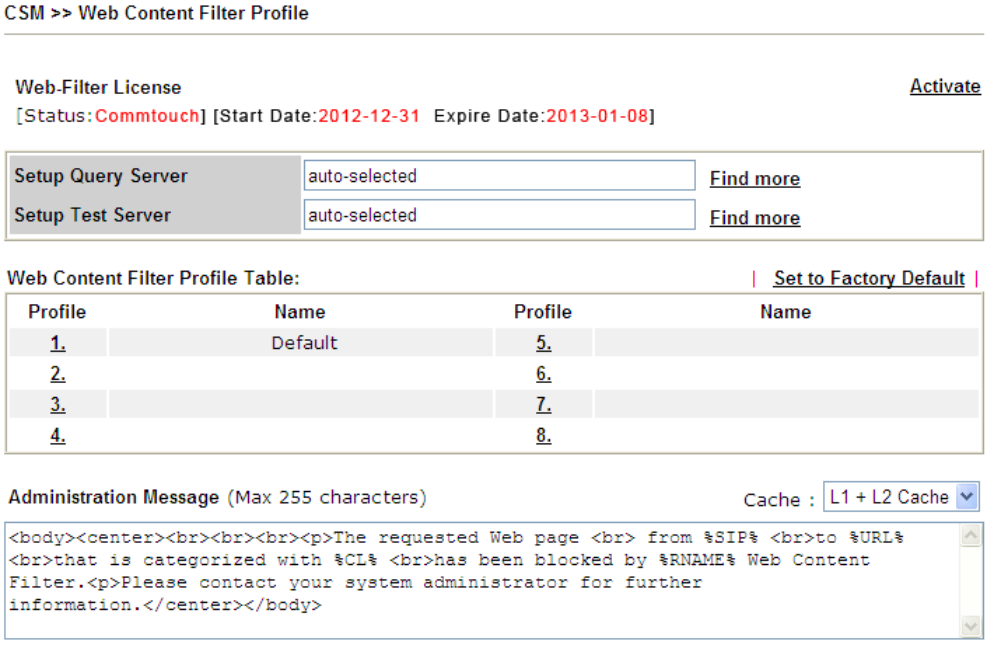
URL Content Filter,

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

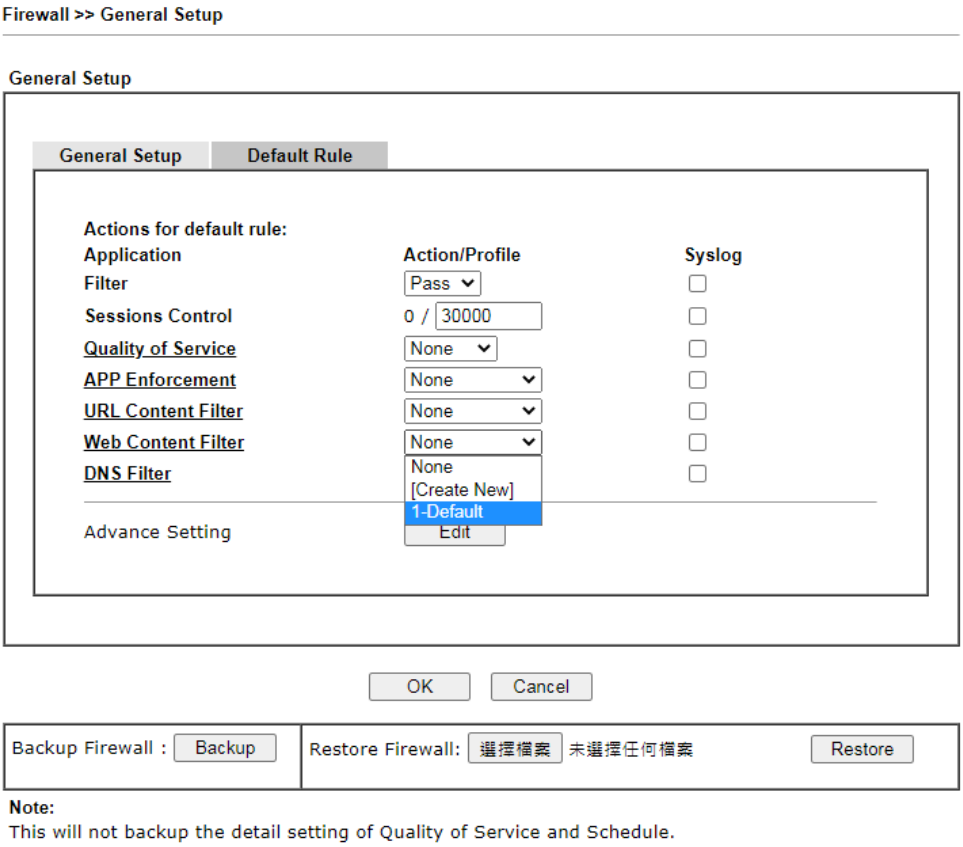
I. Via Web Content Filter

1. Make sure the Web Content Filter (powered by Commtouch) license is valid.



2. Open **CSM >> Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with Action**, Block**.

3. Enable this profile in **Firewall>>General Setup>>Default Rule**.

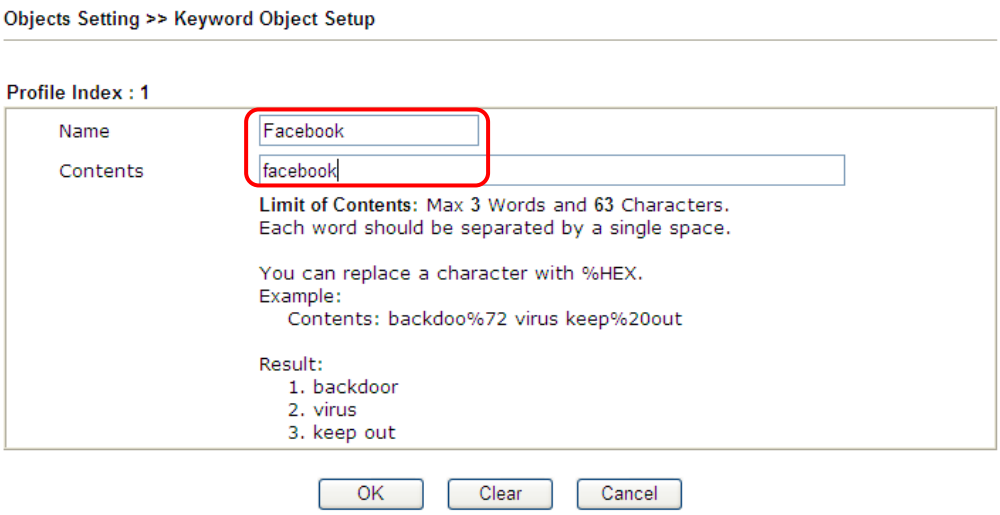


4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

II. Via URL Content Filter

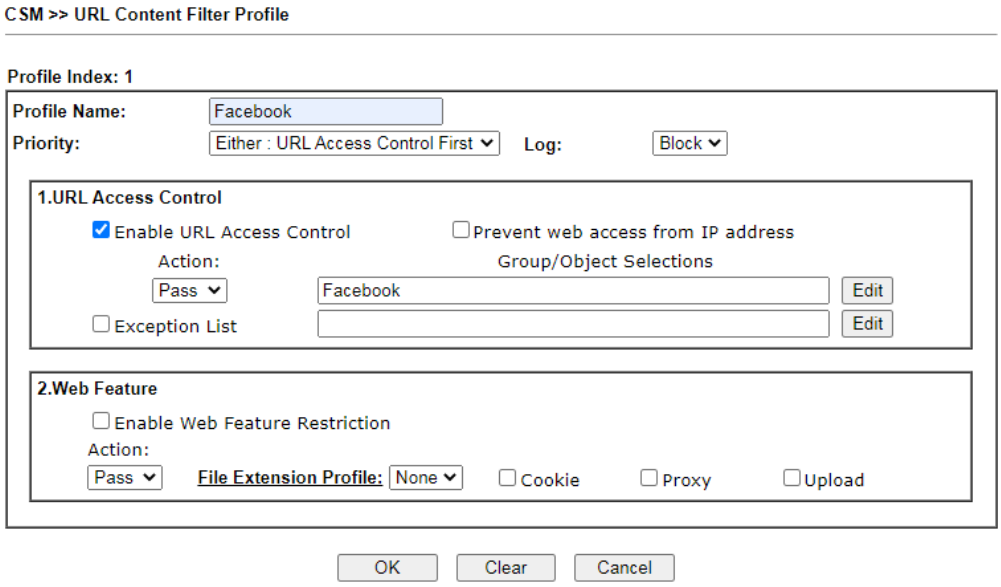
A. Block the web page containing the word of "Facebook"

1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
2. In the field of **Contents**, please type *facebook*. Configure the settings as the following figure.



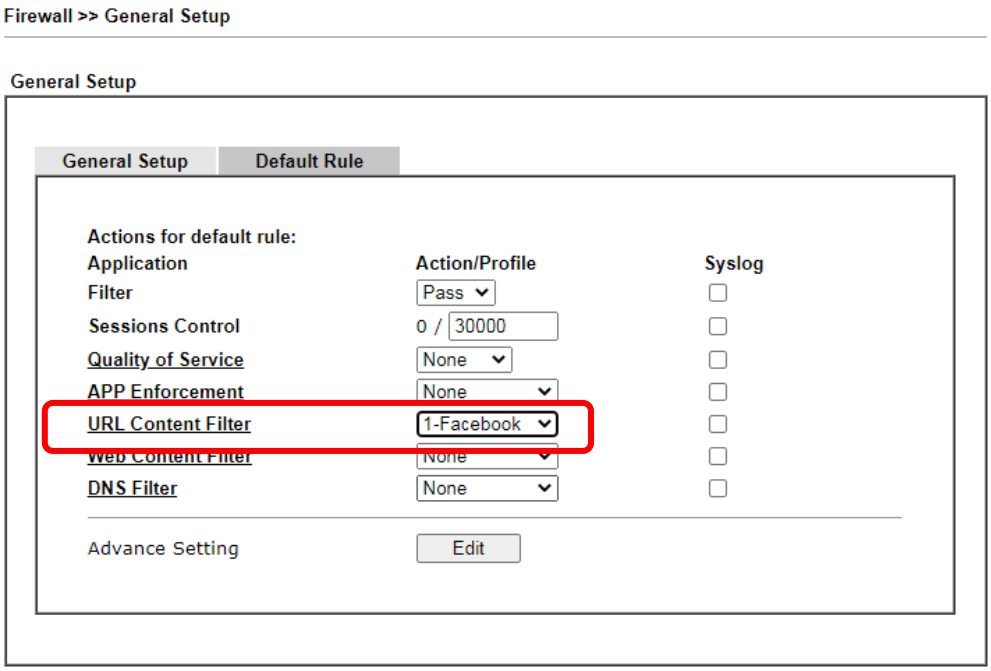
3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.



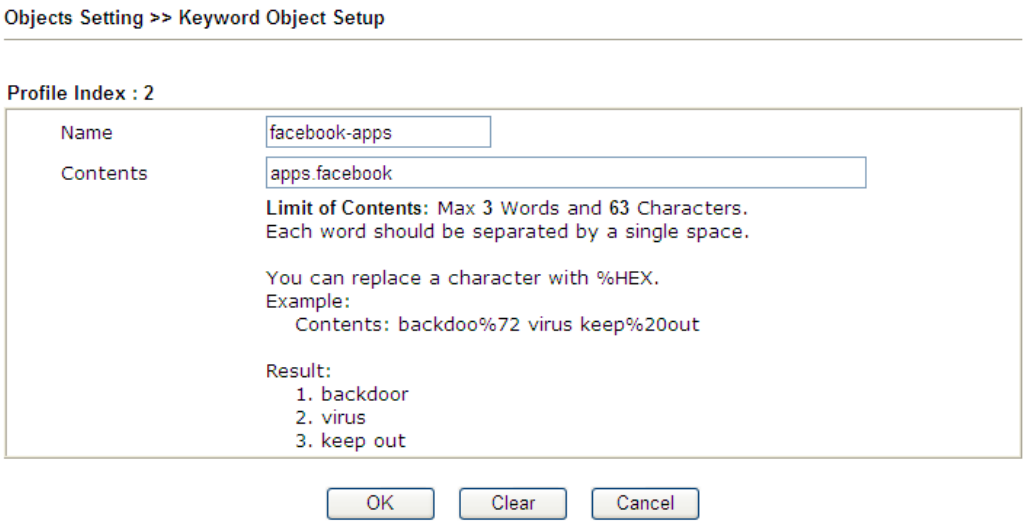
5. When you finished the above steps, click **OK**. Then, open **Firewall>>General Setup**.

6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word "facebook" inside.

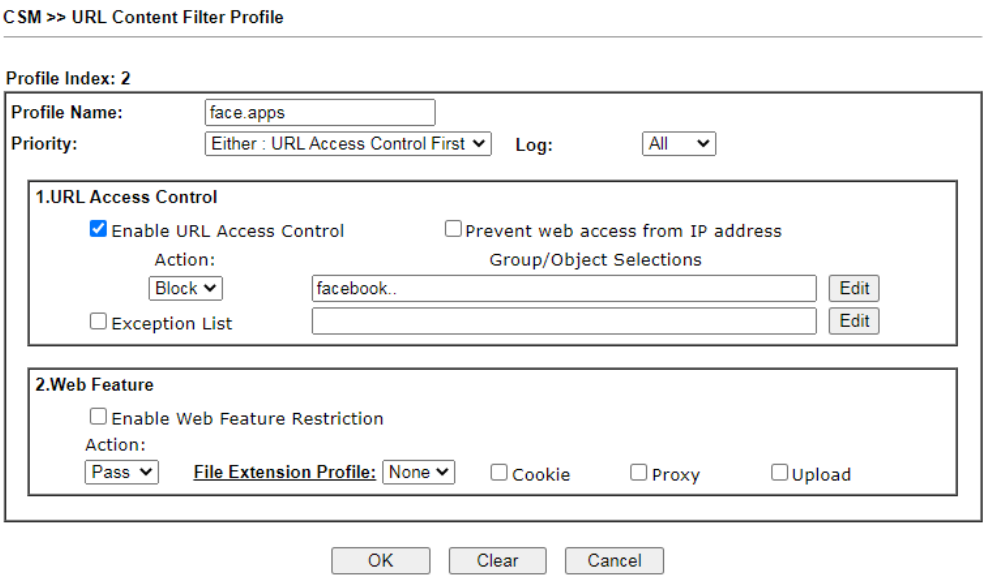


B. Disallow users to play games on Facebook

1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
2. In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.

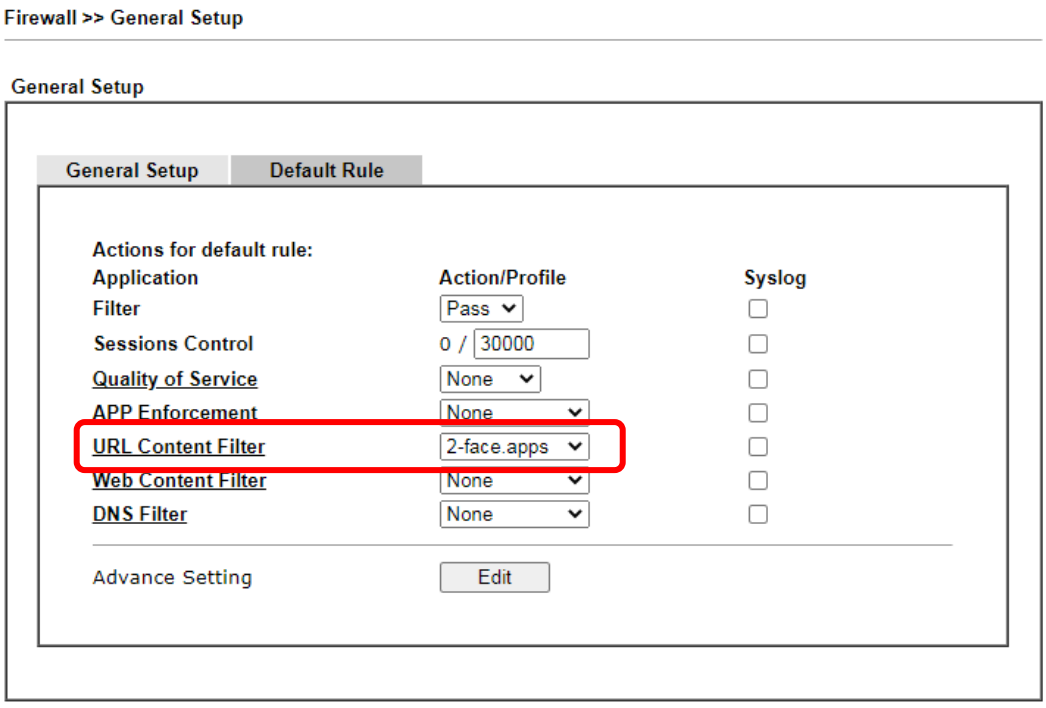


3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.
4. Configure the settings as the following figure.



5. When you finished the above steps, please open **Firewall>>General Setup**.

6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.



This page is left blank.

Part VI Management

System Maintenance

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, User Password, Configuration Backup, Syslog /Mail Alert, Time and Date, SNMP, Management, Panel Control, Self-Signed Certificate, Reboot System, Firmware Upgrade, and Activation.

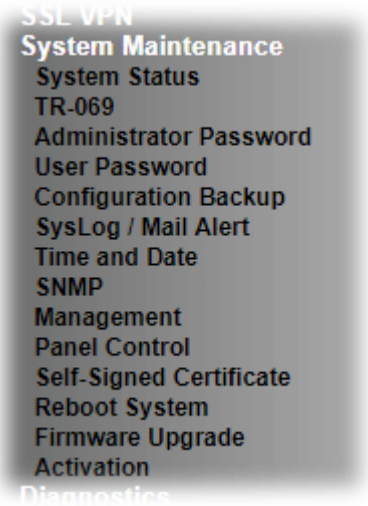
Bandwidth Management

It is used to control the bandwith of data transmission through configuration of Sessions Limit, Bandwidth Limit, and Quality of Servie (QoS).

VI-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Configuration Backup, Syslog /Mail Alert, Time and Date, SNMP, Management, Panel Control, Self-Signed Certificate, Reboot System, Firmware Upgrade and Activation.

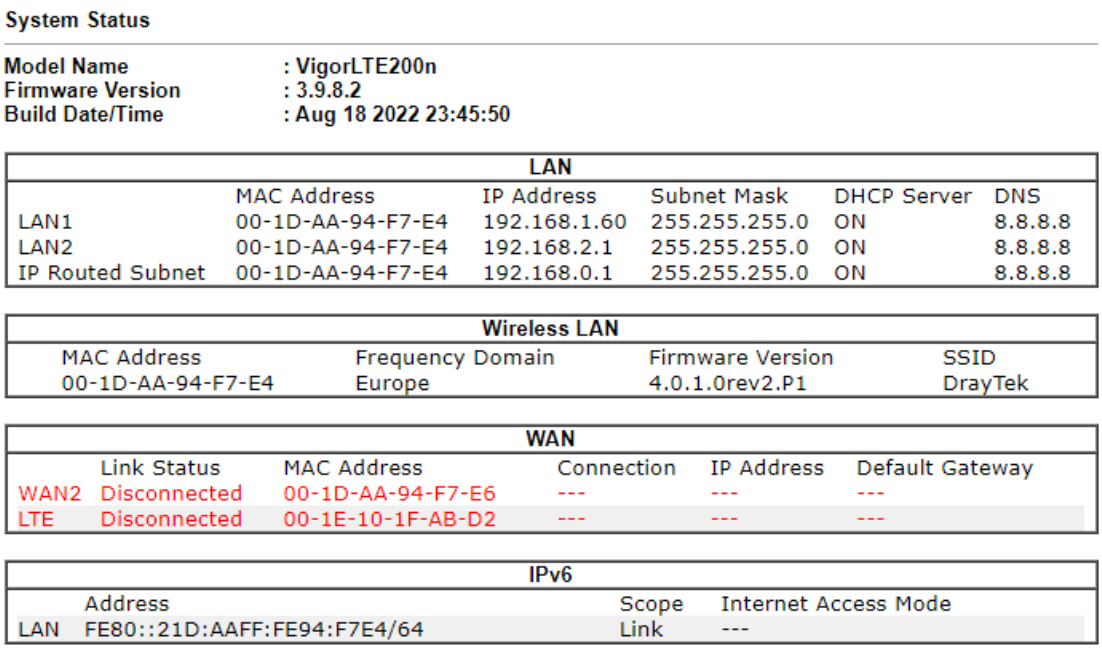
Below shows the menu items for System Maintenance.



Web User Interface

VI-1-1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.



System Status

Model Name : **VigorLTE200n**
Firmware Version : **3.9.8.2**
Build Date/Time : **Aug 18 2022 23:45:50**

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-94-F7-E4	192.168.1.60	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-94-F7-E4	192.168.2.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-94-F7-E4	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-94-F7-E4	Europe	4.0.1.0rev2.P1	DrayTek

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN2	Disconnected	00-1D-AA-94-F7-E6	---	---	---
LTE	Disconnected	00-1E-10-1F-AB-D2	---	---	---

IPv6

	Address	Scope	Internet Access Mode
LAN	FE80::21D:AAFF:FE94:F7E4/64	Link	---

User Mode is OFF now.

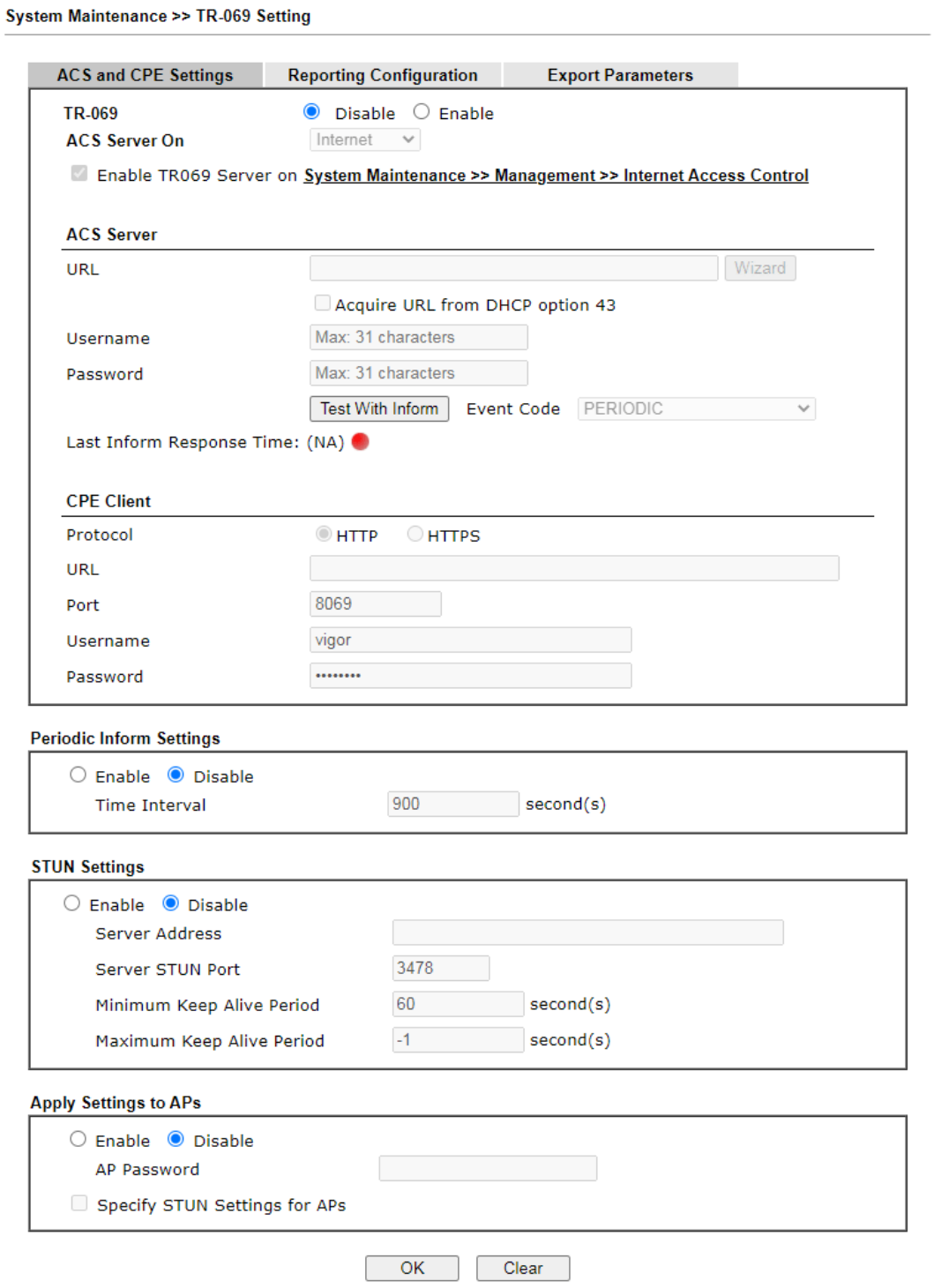
Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	**MAC Address** - Display the MAC address of the LAN Interface. **IP Address** - Display the IP address of the LAN interface. **Subnet Mask** - Display the subnet mask address of the LAN interface. **DHCP Server** - Display the current status of DHCP server of the LAN interface. **DNS** - Display the assigned IP address of the primary DNS.
WAN	**Link Status** - Display current connection status.

	MAC Address **-** Display the MAC address of the WAN Interface. **Connection** **-** Display the connection type. **IP Address** **-** Display the IP address of the WAN interface. **Default Gateway** **-** Display the assigned IP address of the default gateway.
IPv6	**Address -** Display the IPv6 address for LAN. **Scope -** Display the scope of IPv6 address. For example, IPv6 **Link Local** could only be used for direct IPv6 link. It can't be used for IPv6 internet. **Internet Access Mode –** Display the connection mode chosen for accessing into Internet.

VI-1-2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.



Available settings are explained as follows:

Item	Description
TR-069	Click **Enable** to activate the settings on this page.

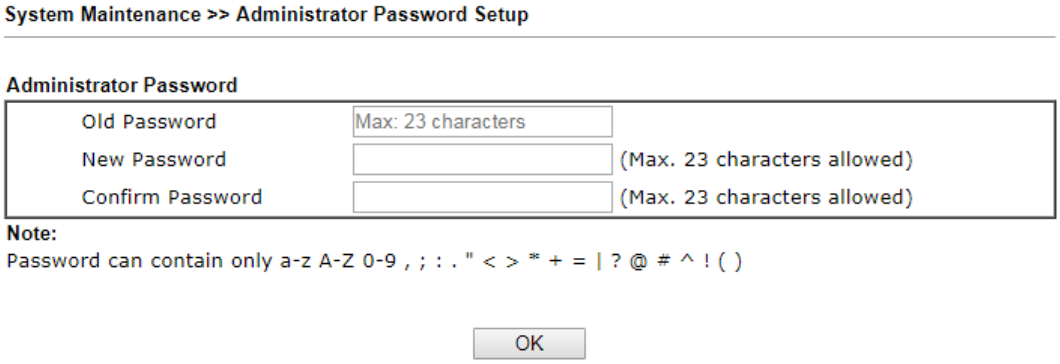
ACS Server On	Choose the interface for the router connecting to ACS server.
Enable TR069 Server on ...	**Enable TR069 Server on System Maintenance>>Management>>Internet Access Control** - If enabld, a user will be allowed to access into TR-069 from WAN.
ACS Server	**URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information. **Wizard** – Click it to enter the IP address of VigorACS server, port number and the handler. **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 SI server. **Event Code** – Use the drop down menu to specify an event to perform the test. **Last Inform Response Time** – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
CPE Client	Such information is useful for Auto Configuration Server. **Enable/Disable** – Allow/Deny the CPE Client to connect with Auto Configuration Server. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. **Username and Password** – Enter the username and password that VigorACS can use to access into such CPE.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the router to send notification to CPE. Or click **Disable** to close the mechanism of notification.
STUN Settings	The default is **Disable**. If you click **Enable**, please Enter the relational settings listed below: **Server Address –** Enter the IP address of the STUN server. **Server Port –** Enter the port number of the STUN server. **Minimum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Apply Settings to APs	This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by VigorLTE 200 at the same time. **Disable** – Related settings will not be applied to VigorAP. **Enable** – Above STUN settings will be applied to VigorAP after clicking **OK**. If such feature is enabled, you have to Enter the password for accessing VigorAP. **AP Password** – Enter the password of the VigorAP that you want to apply VigorLTE 200's TR-069 settings. **Specific STUN Settings to APs** – After clicking the **Enable**

	radio button for **Apply Settings to APs**, if you want to apply specific STUN settings (not the STUN Settings configured for VigorLTE 200) to VigorAPs to meet specific requirements, simply check this box. Then, Enter the server IP address, server port, minimum keep alive period and maxmum keep alive period respectively.

After finishing all the settings here, please click **OK** to save the configuration.

VI-1-3 Administrator Password

This page allows you to set new password.



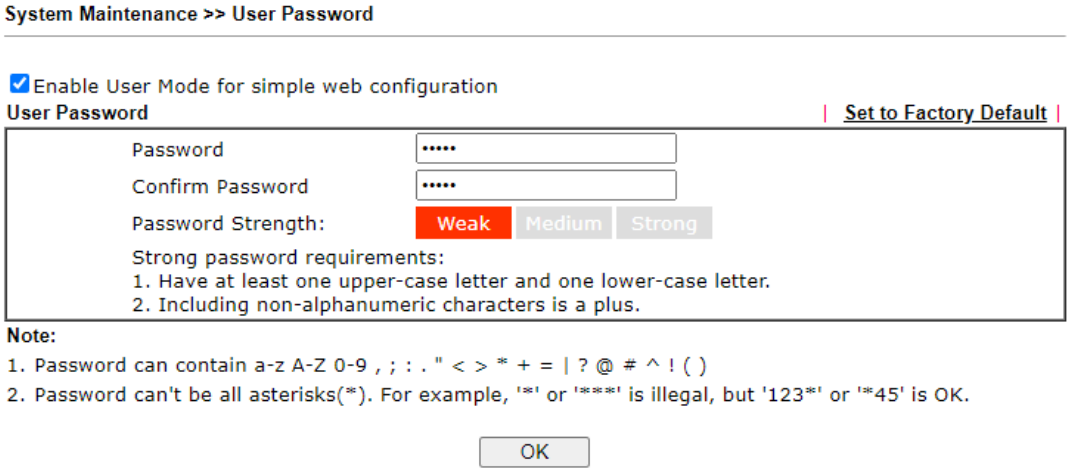
Available settings are explained as follows:

Item	Description
Administrator Password	**Old Password** - Enter the old password. The factory default setting for password is **"admin"**. **New Password** -Enter new password in this field. The length of the password is limited to 23 characters. **Confirm Password** -Enter the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

VI-1-4 User Password

This page allows you to set new password for user operation.



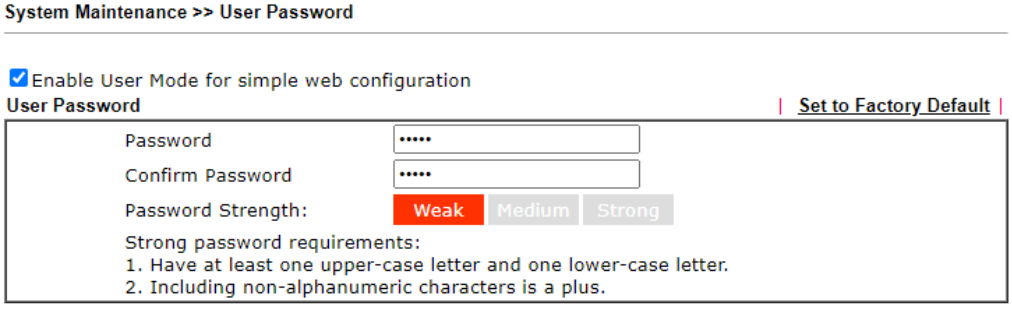
Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Enter new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Enter the new password again.
Password Strength	Display the security strength of the password specified above.
Set to Factory Default	Click to return to the factory default setting.

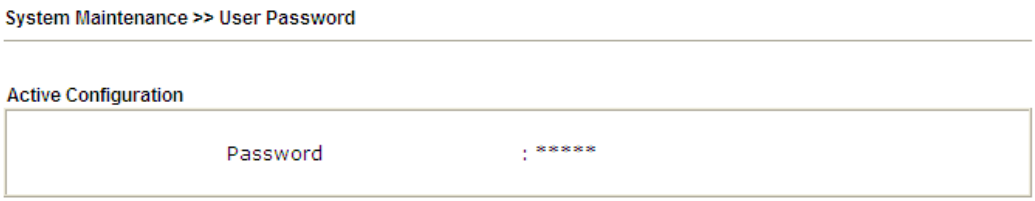
When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again. Below shows an example for accessing into User Operation with User Password.

1. Open **System Maintenance>>User Password**.

2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.



3. The following screen will appear. Simply click **OK**.



4. Log out Vigor router web user interface by clicking the Logout button.

5. The following window will be open to ask for username and password. Enter the new user password in the filed of **Password** and click **Login**.

6. The main screen with User Mode will be shown on the web page.

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

Info	Setting in User Mode can be configured as same as in Admin Mode.

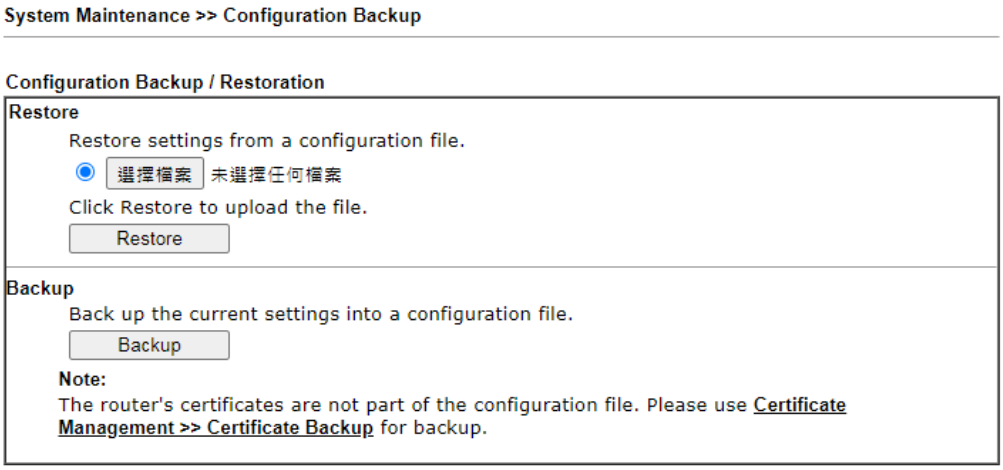
VI-1-5 Configuration Backup

Such function can be used to apply the router settings configured by other Vigor router to VigorLTE 200.

Backup the Configuration

Follow the steps below to backup your configuration.

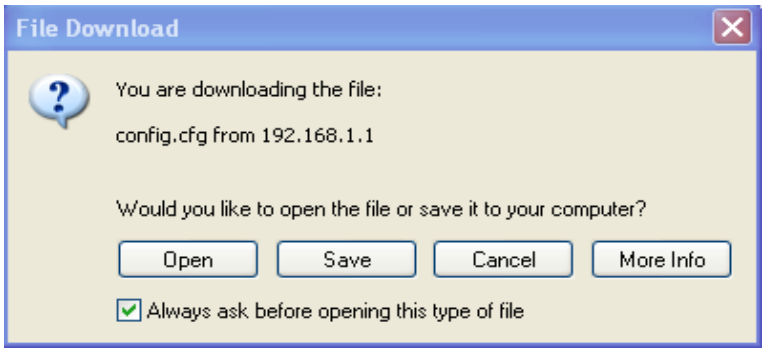
1. Go to **System Maintenance** >> **Configuration Backup**. The following page will be popped-up, as shown below.



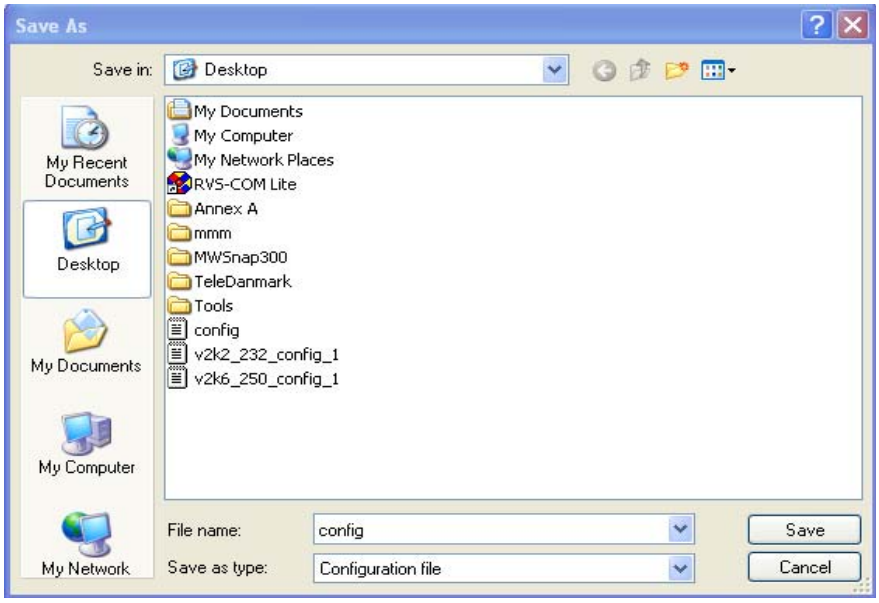
Available settings are explained as follows:

Item	Description
Restore	**Choose File** – Click it to specify a file to be restored. **Restore** - Restore the configuration. If the file is encrypted, the system will ask you to Enter the password to decrypt the configuration file.
Backup	Click it to perform the configuration backup of this router.

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



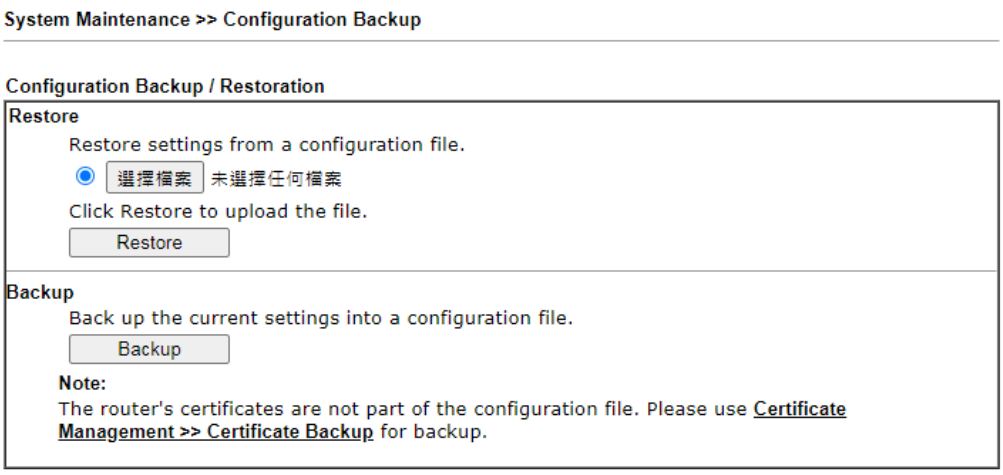
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Info	Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

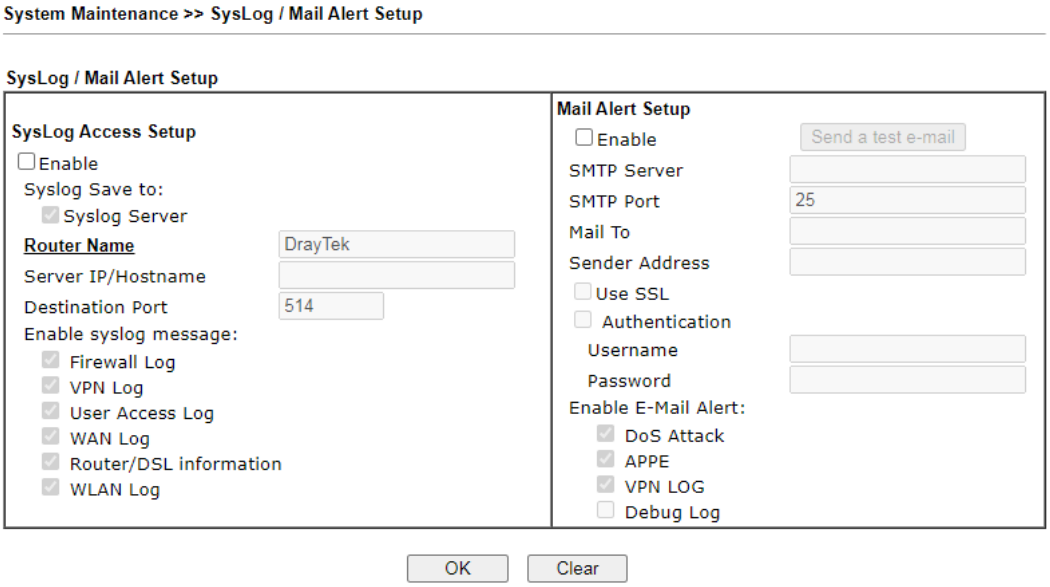
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Choose File** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

VI-1-6 Syslog/Mail Alert

SysLog function is provided for users to monitor router.



Available settings are explained as follows:

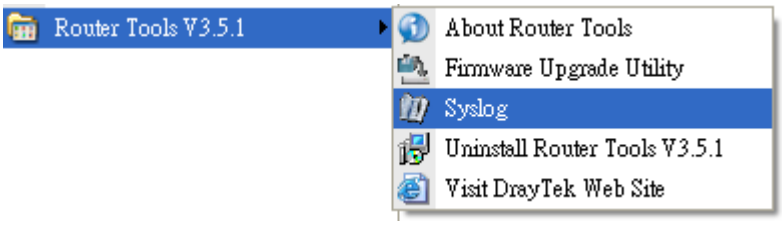
Item	Description
SysLog Access Setup	**Enable** - Check **Enable** to activate function of syslog. **Syslog Save to** – Check **Syslog Server** to save the log to Syslog server.
Router Name	Display the name for such router configured in **System Maintenance>>Management.** If there is no name here, simply lick the link to access into **System Maintenance>>Management** to set the router name. **Server IP /Hostname -**The IP address of the Syslog server. **Destination Port -** Assign a port for the Syslog protocol. **Enable syslog message -** Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, WAN, Router/DSL information and WLAN to Syslog.
Mail Alert Setup	Check **Enable** to activate function of mail alert. **Send a test e-mail -** Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not. **SMTP Server/SMTP Port -** The IP address/Port number of the SMTP server. **Mail To -** Assign a mail address for sending mails out. **Sender Address -** Assign a path for receiving the mail from outside. **Use SSL -** Check this box to use port 465 for SMTP server for

	some e-mail server uses https as the transmission method. **Authentication -** Check this box to activate this function while using e-mail application. **User Name -** Enter the user name for authentication. **Password -** Enter the password for authentication. **Enable E-mail Alert -** Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

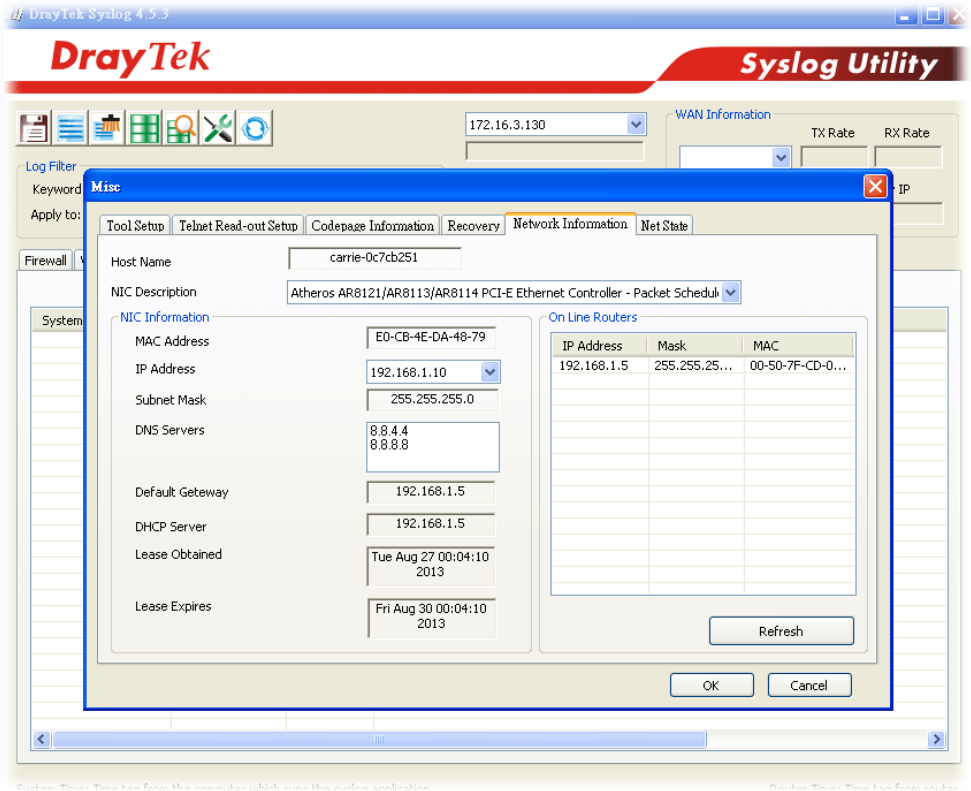
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.

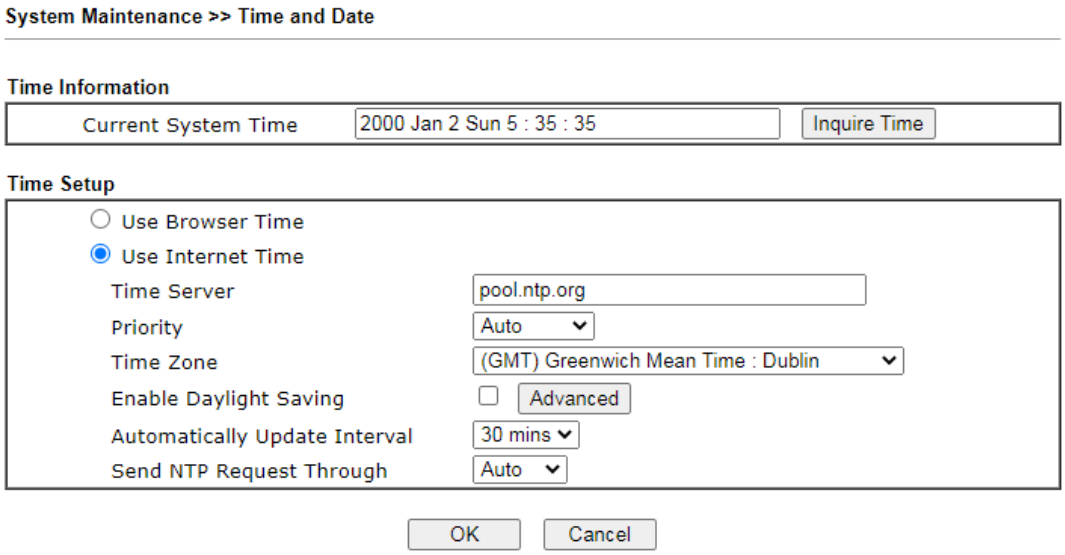


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

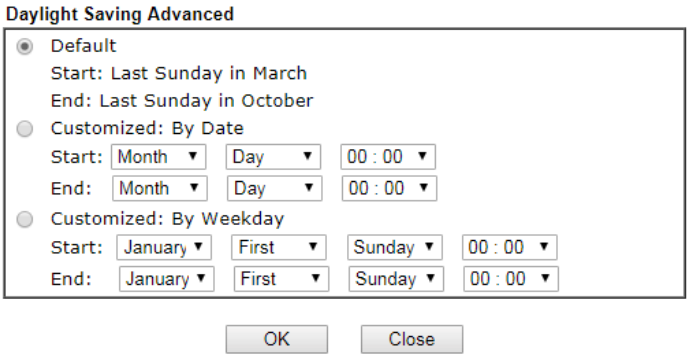


VI-1-7 Time and Date

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



Available settings are explained as follows:

Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Enter the web site of the time server.
Priority	Choose **Auto** or **IPv6 First** as the priority.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area. **Advanced** – Click it to open a pop up dialog.  Use the default time setting or set user defined time for your requirement.
Automatically Update Interval	Select a time interval for updating from the NTP server.

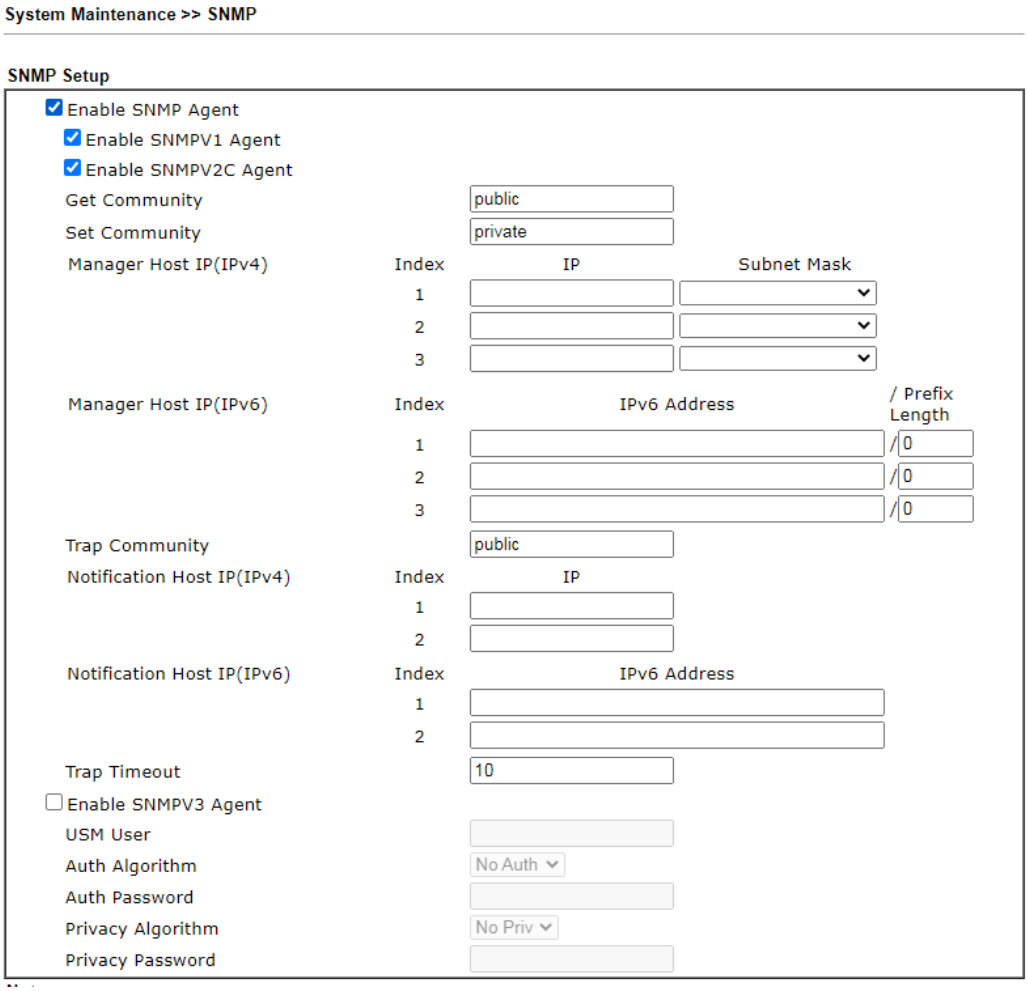
Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.

Click **OK** to save these settings.

VI-1-8 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.



Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check to enable SNMP function. Then, enable SNMPV1 Agent / SNMPV2C Agent/ SNMPV3 Agent.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.** The maximum length of the text is limited to 23 characters.
Set Community	Set community by typing a proper name. The default setting is **private.** The maximum length of the text is limited to 23 characters.
Manager Host IP (IPv4)	Set one host as the manager to execute SNMP function.

	Please Enter IPv4 address to specify certain host.
Manager Host IP (IPv6)	Set one host as the manager to execute SNMP function. Please Enter IPv6 address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is **public.** The maximum length of the text is limited to 23 characters.
Notification Host IP (IPv4)	Set the IPv4 address of the host that will receive the trap community.
Notification Host IP (IPv6)	Set the IPv6 address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.
Enable SNMPV3 Agent	Check to enable SNMPV3 function. **USM User -** USM means user-based security mode. Enter the username to be used for authentication. The maximum allowed length is 23 characters. **Auth Algorithm -** Choose one of the hashing methods to be used with the authentication algorithm. **Auth Password -** Enter a password for authentication. The maximum allowed length is 23 characters. **Privacy Algorithm -** Choose an encryption method as the privacy algorithm. **Privacy Password -** Enter a password for privacy. The maximum allowed length is 23 characters.

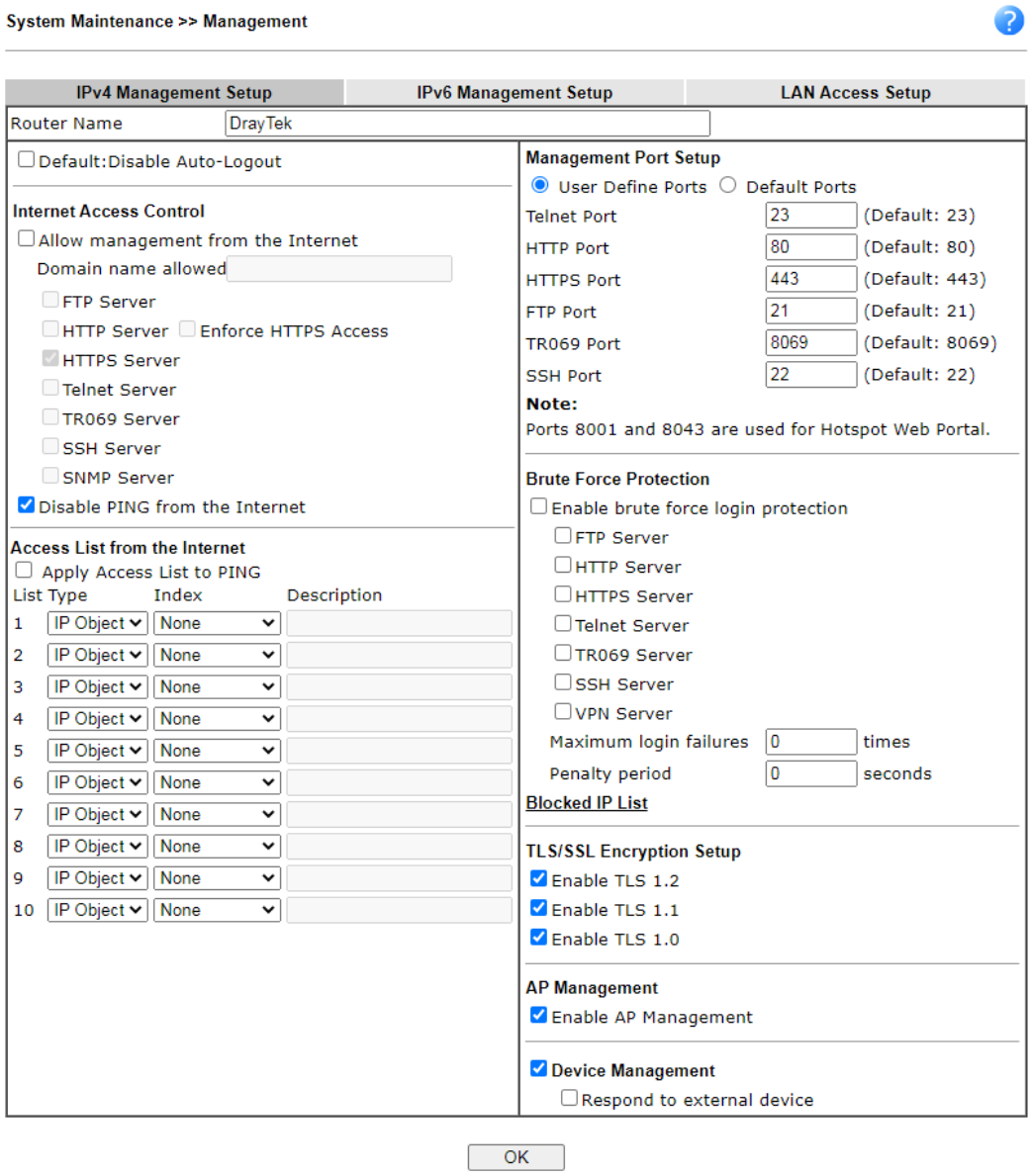
Click **OK** to save these settings.

VI-1-9 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.

The management pages for IPv4 and IPv6 protocols are different.

For IPv4



Available settings are explained as follows:

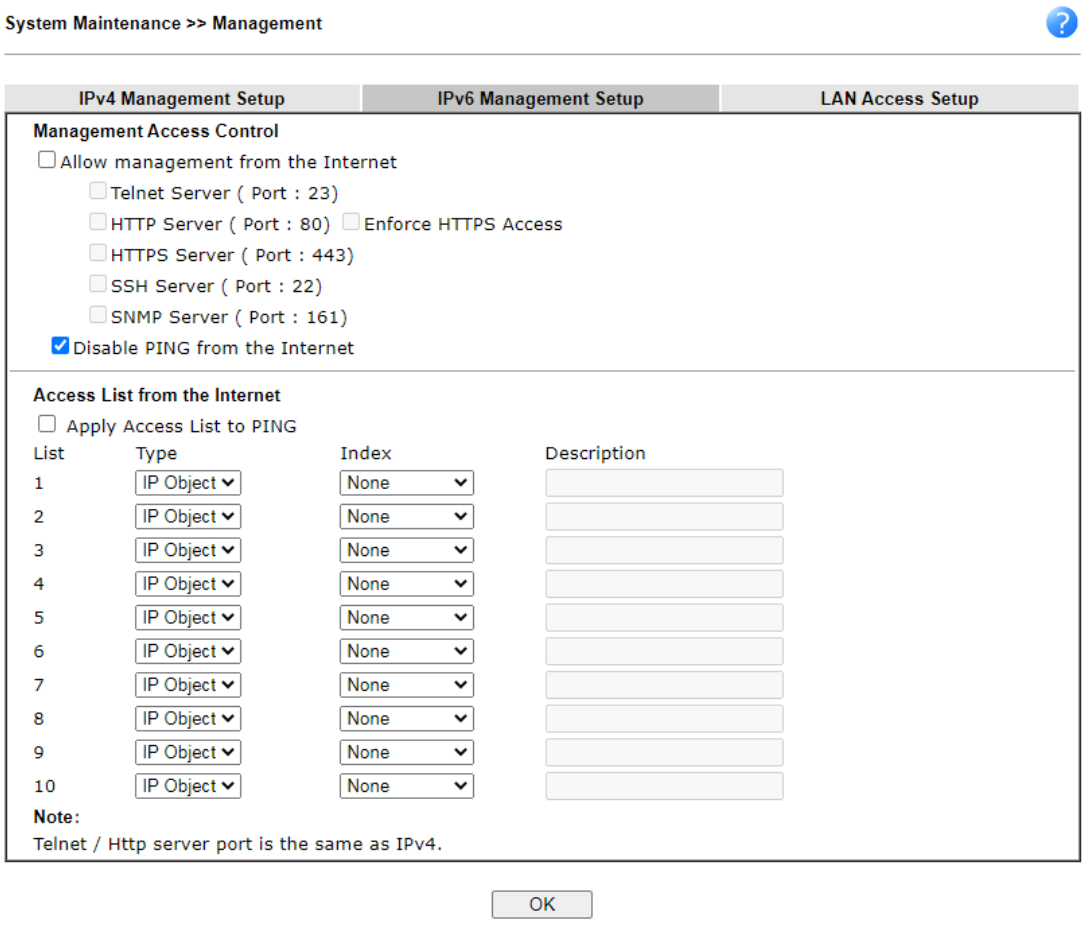
Item	Description
Router Name	Enter the router name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.

	 The web user interface will be open until you click the Logout icon manually. 
Internet Access Control	**Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify. **Disable PING from the Internet -** Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List from the Internet	The ability of system administrators to log into the router can be restricted to up to 10 specific hosts or networks. **Apply Access List to PING** – When this option is checked and **Disable PING from the Internet** is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if **Disable PING from the Internet** is checked, which blocks all pings from the Internet. **Type** - Select **IP Object**, **Hostname** or **IP Group**. **Index** - Select the index number of a configured IP object, keyword object or IP group object. **Description** - Shows a brief comment for the selected IP object (with subnet mask).
Management Port Setup	**User Define Ports -** Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers. **Default Ports -** Check to use standard port numbers for the Telnet and HTTP servers.
Brute Force Protection	Any client trying to access into Internet via Vigor router will be asked for passing through user authentication. Such feature can prevent Vigor router from attacks when a hacker tries every possible combination of letters, numbers and symbols until find out the correct combination of password. **Enable brute force login protection –** Enable the protection mechanism. **Maximum login failure –** Specify the maximum number of wrong password that client can try for logging to Vigor router. **Penalty period –** Set a period of time to block the IP address which is used (by user or hacker) for passing through the user authentication again and again but failed always. When the time is up, Vigor system will unblock that IP and allow it to

	access into Vigor router again. **Blocked IP List** – Open another web page which displays current blocked IPs.
TLS/SSL Encryption Setup	**Enable TLS 1.0/1.1/1.2** – Check the box to enable the function of TLS 1.0/1.1/1.2 if required. Due to security consideration, the built-in HTTPS and SSL VPN server of the router had upgraded to TLS1.x protocol. If you are using old browser(eg. IE6.0) or old SmartVPN Client, you may still need to enable SSL 3.0 to make sure you can connect, however, it's not recommended.
AP Management	**Enable AP Management** – Check it to enable the function of **Central Management>>AP**. If unchecked, menu items related to **Central Management>>AP** will be hidden.
Device Management	Check the box to enable the device management function for VigorLTE 200. **Respond to external device** – If it is enabled, VigorLTE 200 will be regarded as slave device. When the external device (master device) sends request packet to VigorLTE 200, VigorLTE 200 would send back information to respond the request coming from the external device which is able to manage VigorLTE 200.

After finished the above settings, click **OK** to save the configuration.

For IPv6

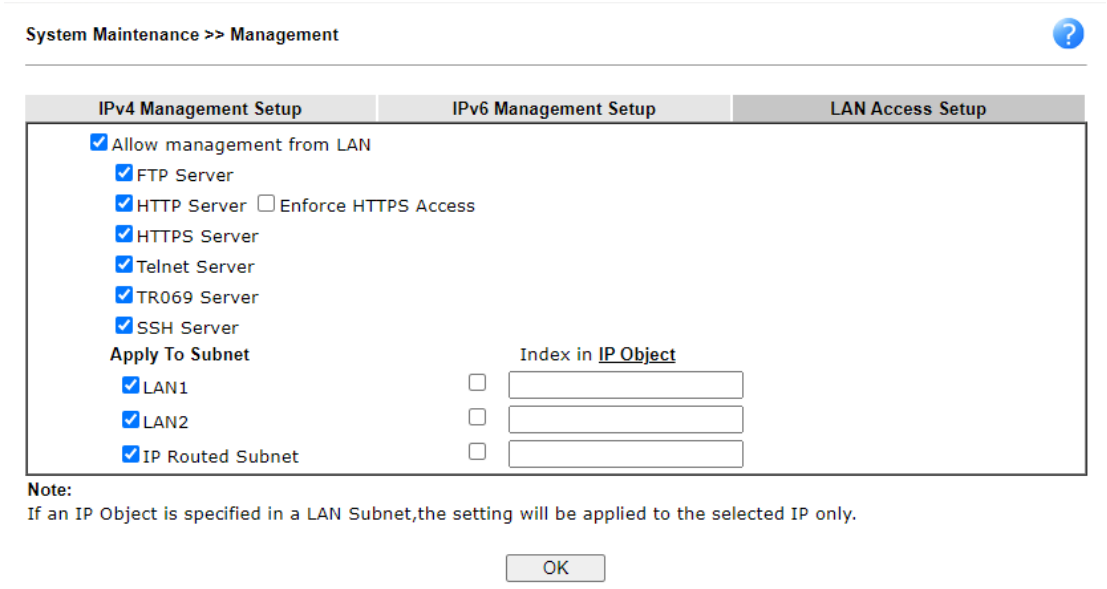


Available settings are explained as follows:

Item	Description
Management Access Control	**Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify. **Disable PING from the Internet** - Check the checkbox to disable all PING packets from the Internet. For security issue, this function is enabled by default.
Access List from the Inernet	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **Apply Access List to PING** – When this option is checked and **Disable PING from the Internet** is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if **Disable PING from the Internet** is checked, which blocks all pings from the Internet. **Type** - Select **IP Object/Group** or **Hostname**. **Index** - Select the index number of a configured IPv6 object.

After finished the above settings, click **OK** to save the configuration.

LAN Access Setup



Available settings are explained as follows:

Item	Description
Allow management from LAN	Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.
Apply To Subnet	Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router. **Index in IP Object**- Enter the index number of the IP object

	profile. Related IP address will appear automatically.

Select **OK** to save changes on the page.

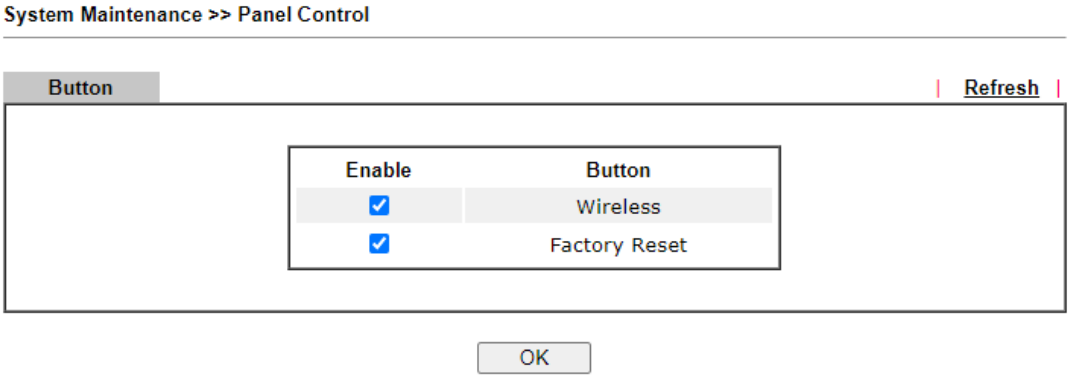
VI-1-10 Panel Control

The behavior of the buttons on the front panel of the Vigor router can be customized as desired.

For Button

The **Factory Reset** and **Wireless ON/OFF/WPS** buttons on the front panel are enabled by default and can be enabled or disabled if required. Disabling the Factory Reset button will prevent tampering by unauthorized parties, or to avoid accidental triggering of a router reset when being used wake up LEDs. Disabling the wireless button will prevent changing the wireless setting when LED Sleep Mode is enabled, and the buttons are primarily used to turn the LEDs on and off.

Click the **Button** tab to get the following page.



Available settings are explained as follows:

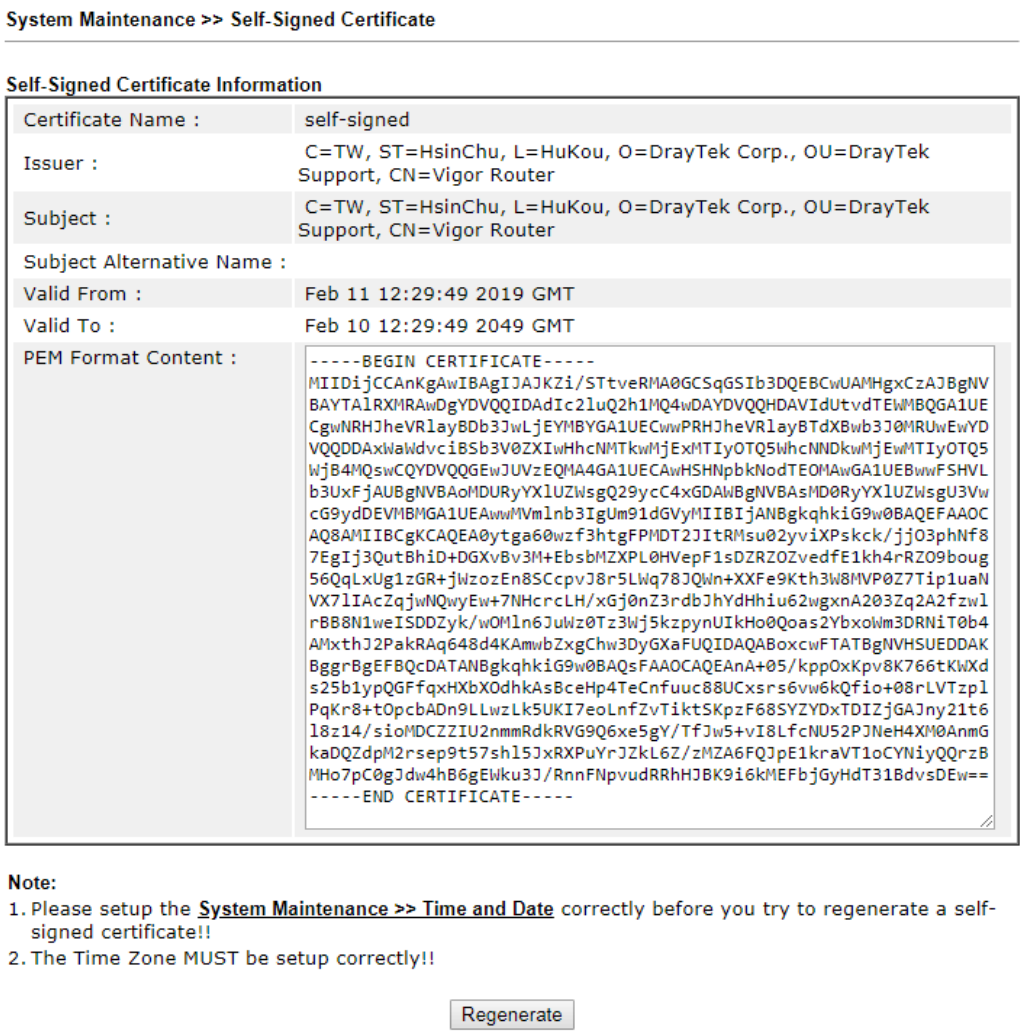
Item	Description
Refresh	Click to refresh the page to display the latest information**.**
Enable Wireless Button	The default value is **Enabled**. Deselect to disable the ability of the Wireless button to control WLAN and WPS functions. Disabling the wireless button only prevents it from being used to control WLAN functions. It can still be used to wake up the LEDs when LED sleep mode is enabled.
Enable Factory Reset Button	The default value is **Enabled**. Deselect to disable the reset function of the factory reset button. Disabling the Factory Reset button only prevents it from being used to reboot Vigor router with default settings. It can still be used to wake up the LEDs when LED sleep mode is enabled.

After finished the above settings, click **OK** to save the configuration.

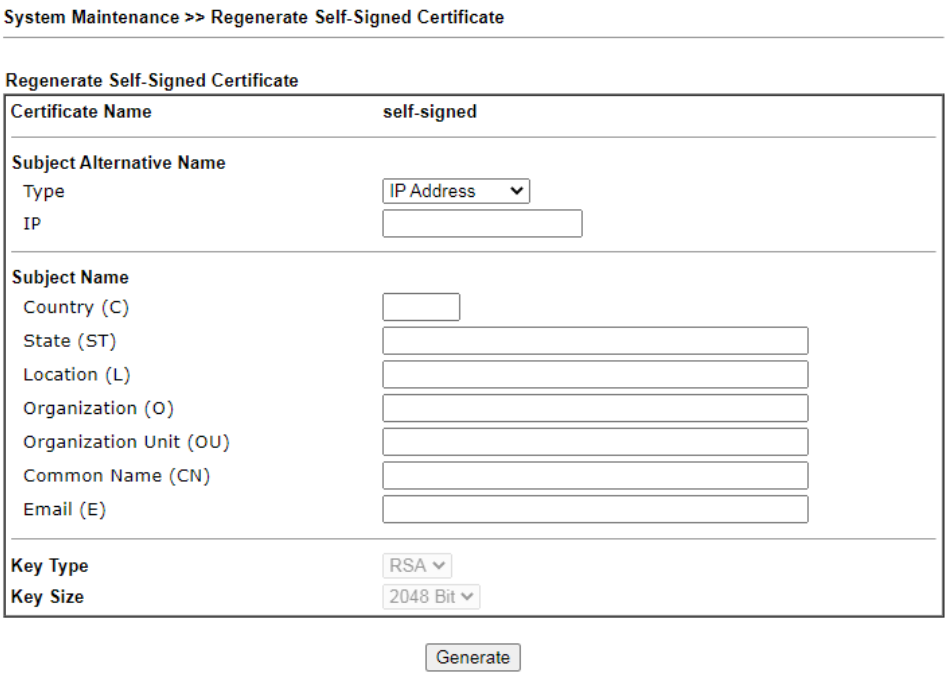
VI-1-11 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

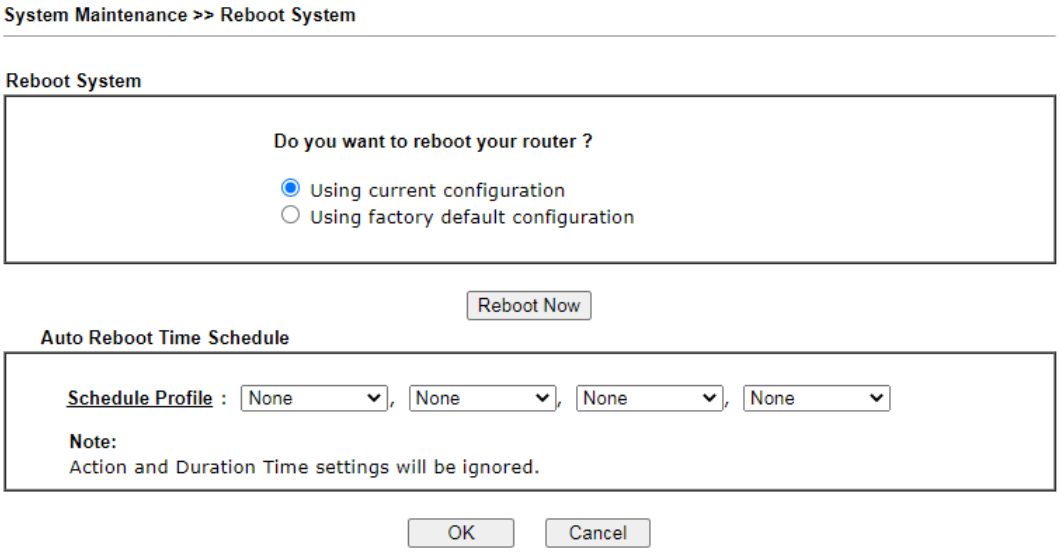


Click **Regeneration** to open **Regenerate Self-Signed Certificate** window. Enter all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE**.



VI-1-12 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.



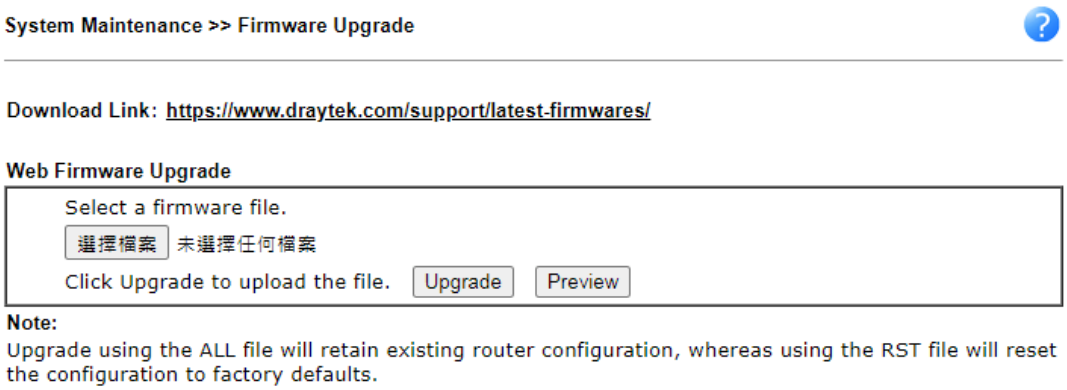
Schedule Profile - You can Enter four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

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

Info	When the system pops up Reboot System web page after you configure web settings, please click Reboot Now to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

VI-1-13 Firmware Upgrade

Click **System Maintenance>> Firmware Upgrade** to proceed to firmware upgrade.



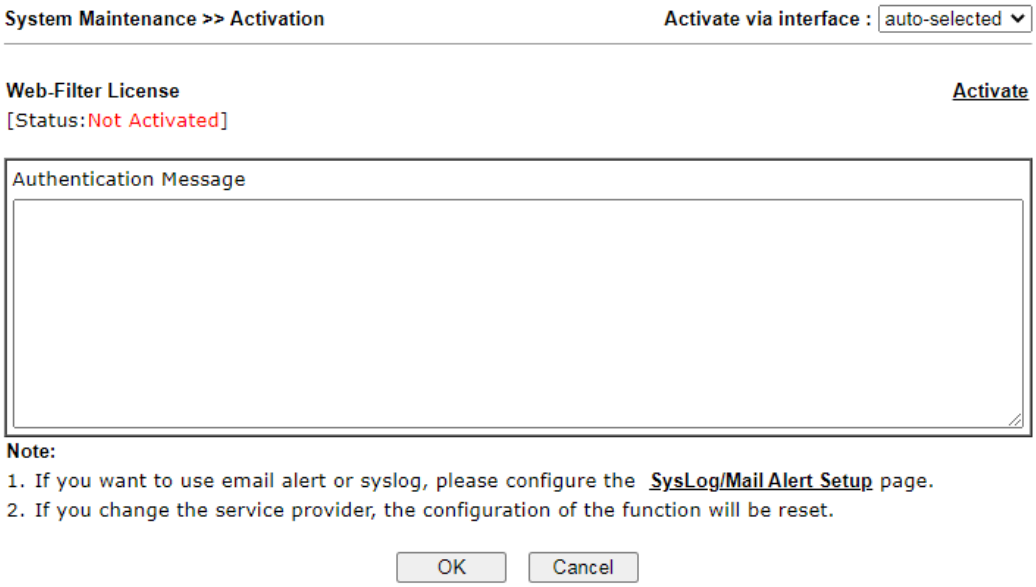
Click **Select** to specify the one you just download. After choosing the file you want, click **Upgrade**. The system will upgrade the firmware of the router automatically.

VI-1-14 Activation

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

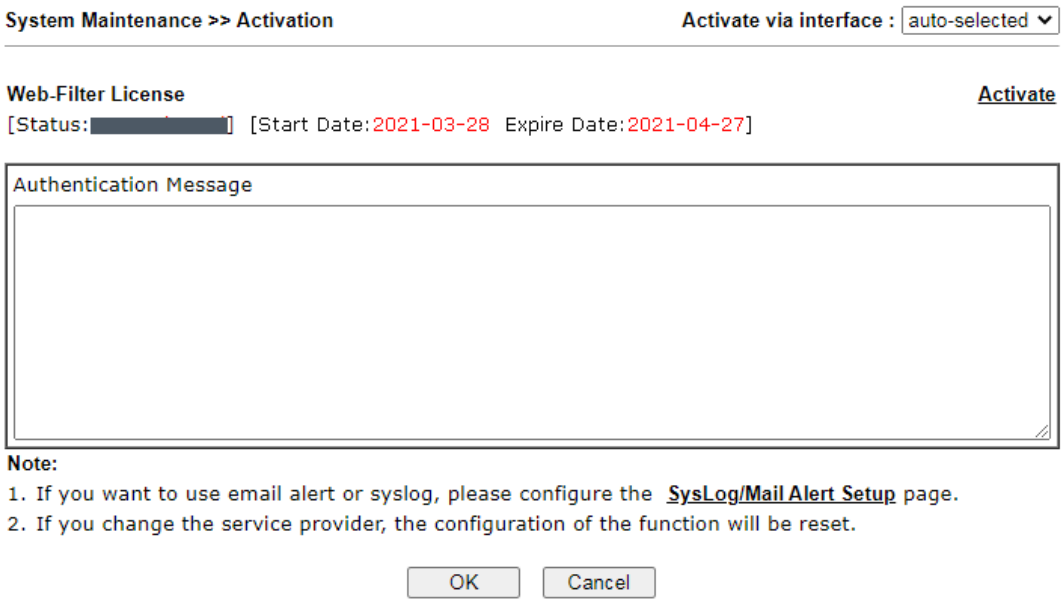
Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.



Available settings are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.
Activate	The **Activate** link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of **web filter**, the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of Web Content Filter:



VI-2 Bandwidth Management

Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

Bandwidth Limit

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

Quality of Service (QoS)

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

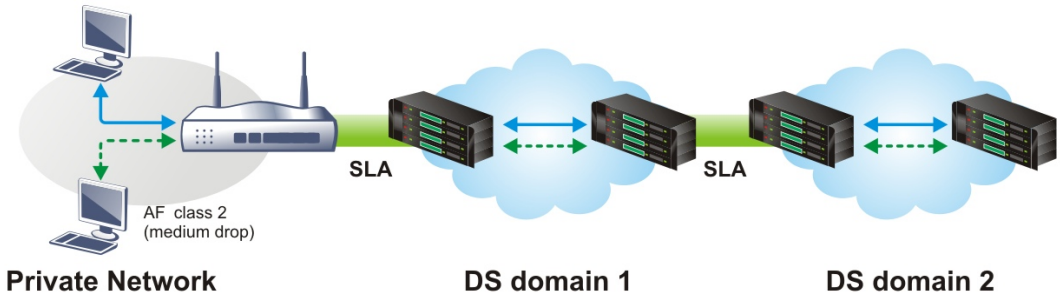
There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service Enterformation in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

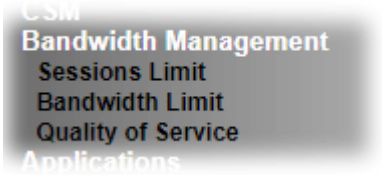
Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

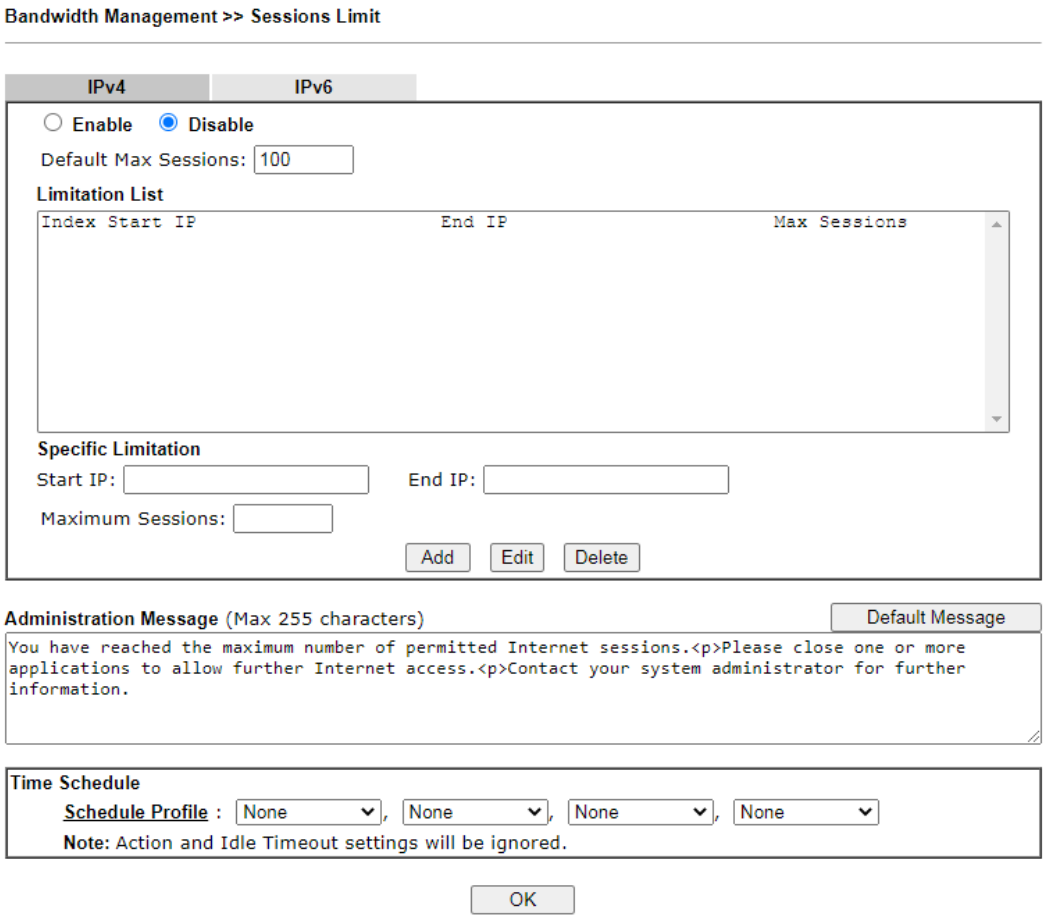
Web User Interface

Below shows the menu items for Bandwidth Management.



VI-2-1 Sessions Limit

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.



To activate the function of limit session for IPv4 and/or IPv6, simply click **Enable** and set the default session limit.

Available settings are explained as follows:

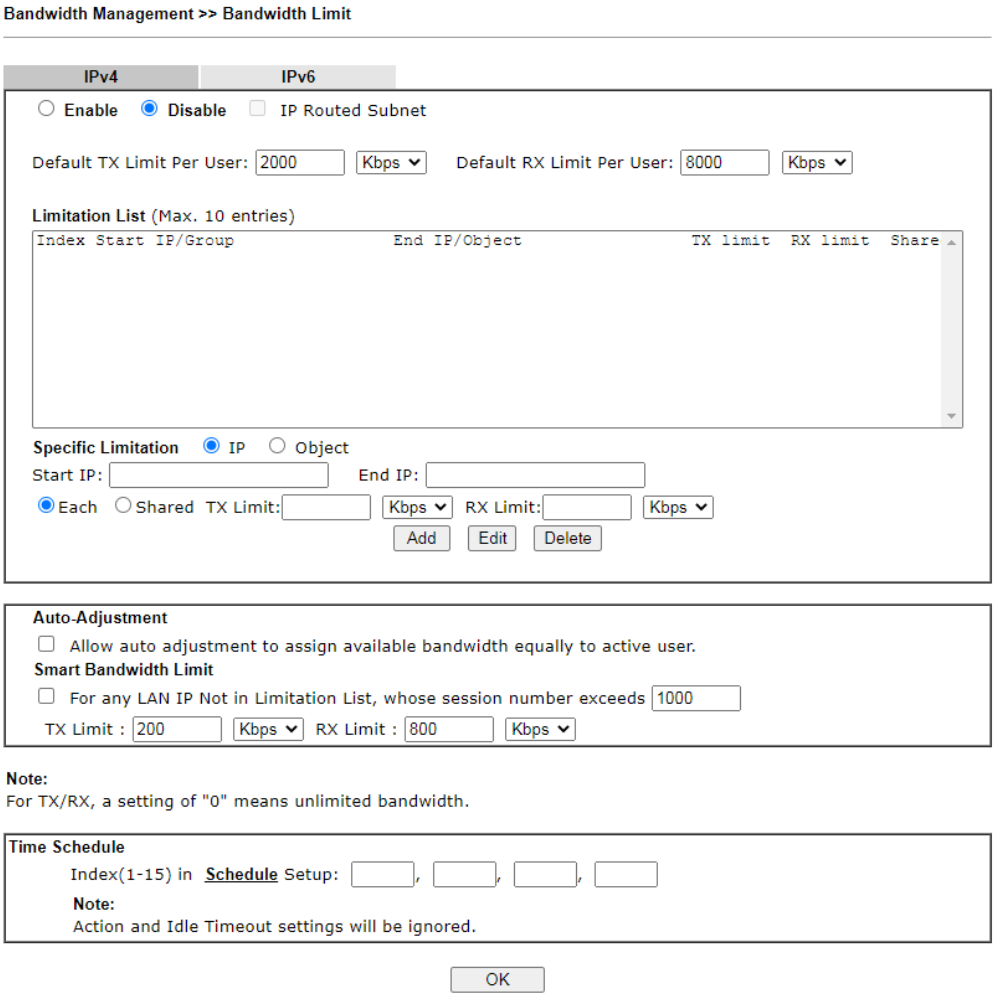
Item	Description
Session Limit	**Enable -** Click this button to activate the function of limit session. **Disable** - Click this button to close the function of limit session. **Default Max Sessions -** Defines the default session number

	used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	**Start IP-** Defines the start IP address for limit session. **End IP -** Defines the end IP address for limit session. **Maximum Sessions -** Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index. **Add -** Adds the specific session limitation onto the list above. **Edit -** Allows you to edit the settings for the selected limitation. **Delete -** Remove the selected settings existing on the limitation list.
Administration Message	Enter the words which will be displayed when reaches the maximum number of Internet sessions permitted. **Default Message -** Click this button to apply the default message offered by the router.
Time Schedule	**Schedule Profile** - You can Enter four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.

After finishing all the settings, please click **OK** to save the configuration.

VI-2-2 Bandwidth Limit

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.



To activate the function of limit bandwidth for IPv4 and /or IPv6, simply click **Enable** and set the default upstream and downstream limit.

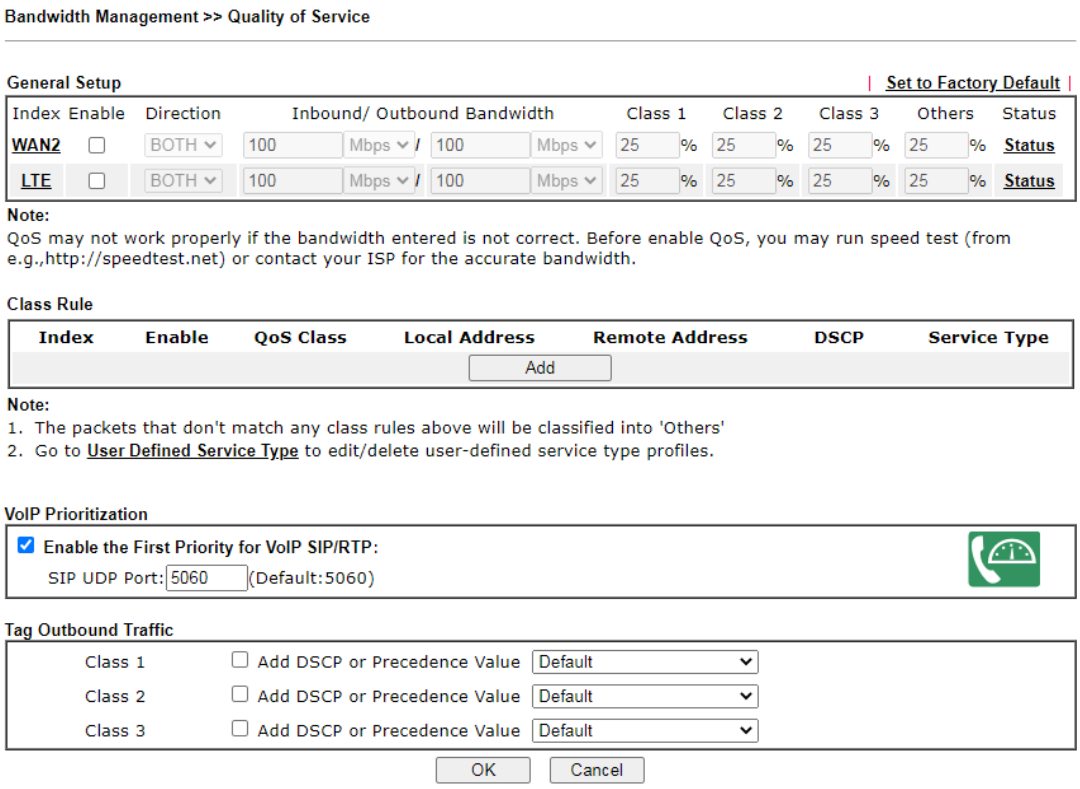
Available settings are explained as follows:

Item	Description
Bandwidth Limit	**Enable** - Click this button to activate the function of limit bandwidth. **IP Routed Subnet** – Check this box to apply the bandwidth limit to the second subnet specified in **LAN>>General Setup**. It is available for IPv4 settings only. **Disable -** Click this button to close the function of limit bandwidth. **Default TX limit Per User-** Define the default speed of the upstream for each computer in LAN. **Default RX limit Per User-** Define the default speed of the downstream for each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
Specific Limitation	**Start IP -** Define the start IP address for limit bandwidth.

	End IP - Define the end IP address for limit bandwidth. **Each /Shared -** Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields. **TX limit -** Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. **RX limit -** Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. **Add -** Add the specific speed limitation onto the list above. **Edit -** Allow you to edit the settings for the selected limitation. **Delete -** Remove the selected settings existing on the limitation list.
Allow auto adjustment…	Check this box to make the best utilization of available bandwidth.
Smart Bandwidth Limit	Check this box to have the bandwidth limit determined by the system automatically. **TX limit -** Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. **RX limit -** Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Time Schedule	**Schedule Profile -** You can Enter four sets of time schedule for your request. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

VI-2-3 Quality of Service

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page.



Available settings are explained as follows:

Item	Description
General Setup	**Index** – Display the WAN interface number link that you can edit. **Enable** – Check the box to enable the QoS function for WAN interface. If it is enabled, you can configure general QoS setting for each WAN interface. ● **Direction** – Define which traffic the QoS Control settings will apply to. ■ **IN-** apply to incoming traffic only. ■ **OUT-**apply to outgoing traffic only. ■ **BOTH-** apply to both incoming and outgoing traffic. ● **Inbound/Outbound Bandwidth** – Set the connecting rate of data input/output for other WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps. ● **Class 1 ~ 3 / Others** – Define the ratio of bandwidth to upstream speed and bandwidth to downstream speed. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. In which, the "Others" field is used for the packets which are not suitable for the three class rules.

Item	Description
	Status – Display the online statistics of WAN interface.
Class Rule	Define and list the Class rules. **Index** – Displays the class number that you can edit. **Enable** - Displays the status of this class rule. **QoS Class** - Displays the QoS class level. **Local Address** - Displays the local IP address for the rule. **Remote Address** - Displays the remote IP address for the rule. **DSCP** - Displays the levels of the data for processing with QoS control. **Service Type** – Displays detailed settings for the service type. **Add** - Click it to create a class rule for QoS.
VoIP Prioritization	**Enable the First Priority for VoIP SIP/RTP** - Select to allow VoIP traffic to receive the highest priority. **SIP UDP Port –** Port number to be monitored for SIP traffic.  - Click this icon to display the VoIP QoS Status.
Tag Outbound Traffic	Tag the outgoing traffic with the DSCP or Precedence value. **Add DSCP or Precedence Value for Class 1 to Class 3** - Check to apply the DSCP or precedence value for each class.

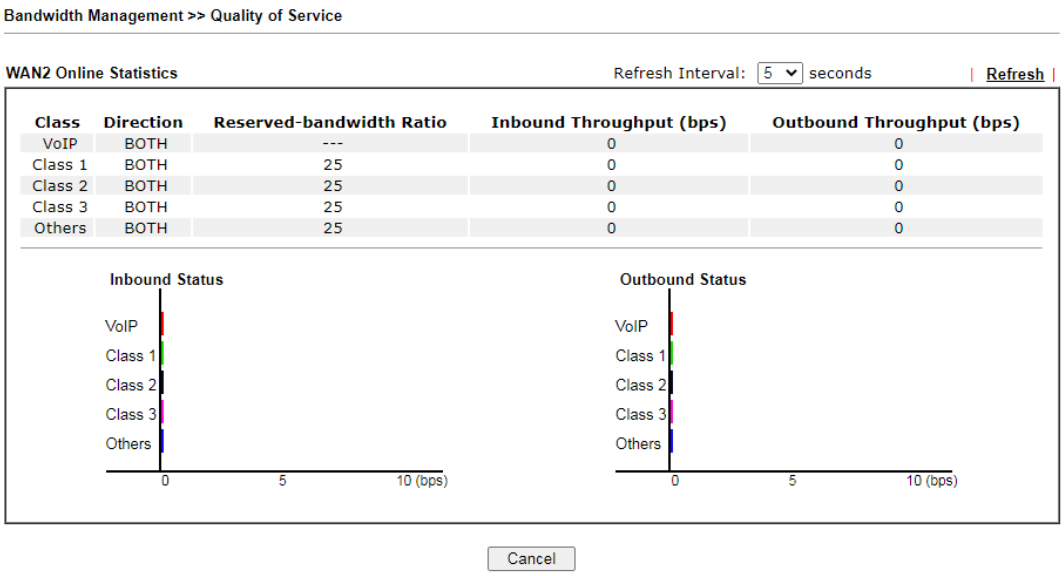
To save changes, click **OK**; to discard changes, click **Cancel**.

Click the **WAN2/LTE** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

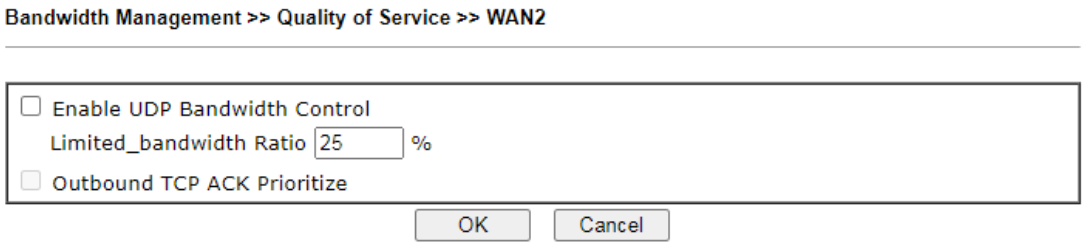
Online Statistics

Click the **WAN2/LTE** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.



General Setup for WAN Interface

Click WAN interface number link to configure the limited bandwidth ratio for QoS of the WAN interface.



Available settings are explained as follows:

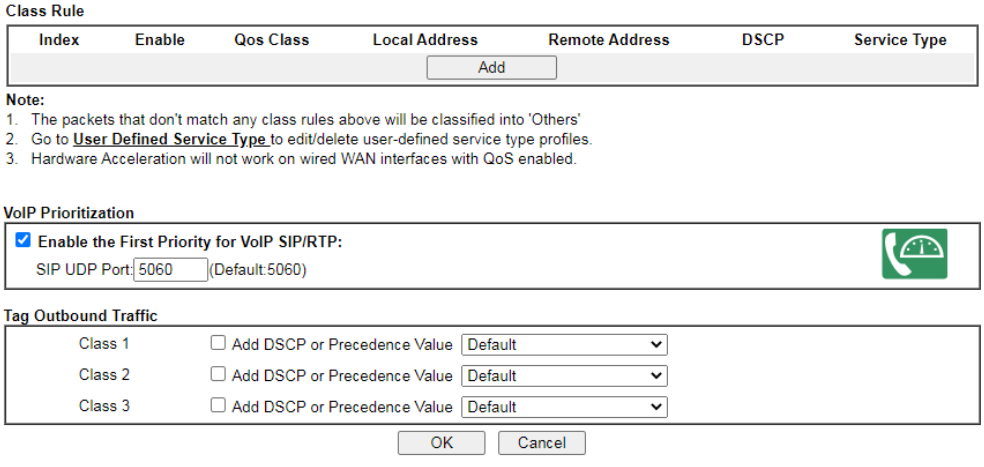
Item	Description
Enable UDP Bandwidth Control	Set the limited bandwidth ratio. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth. **Limited_bandwidth Ratio -** The ratio typed here is reserved for limited bandwidth of UDP application.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

Info

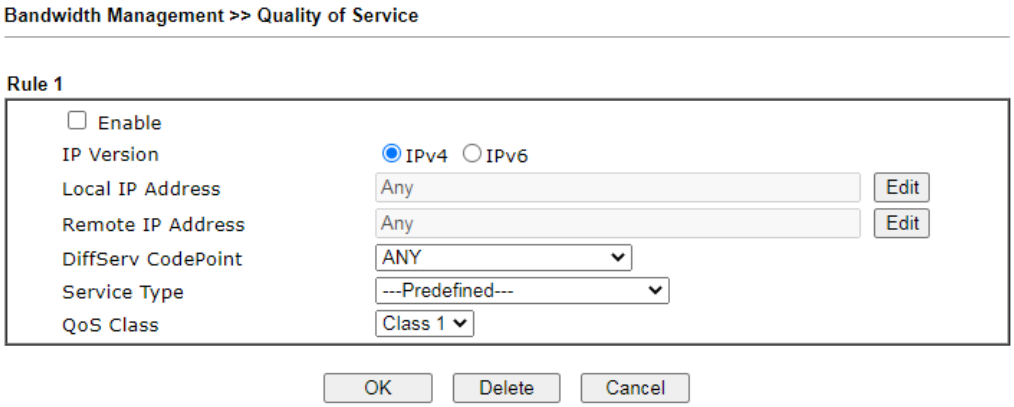
The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

Edit the Class Rule for QoS

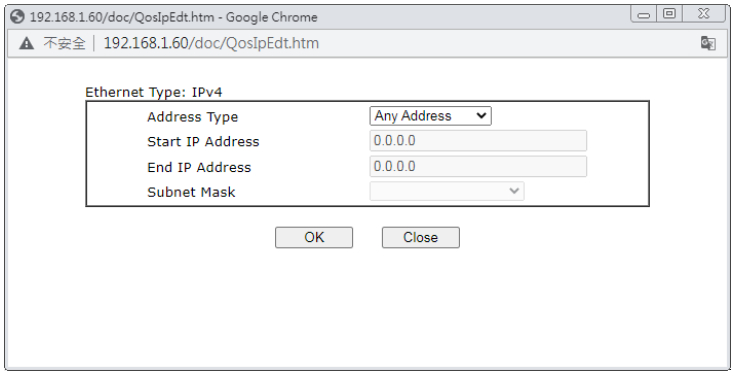
1. To add a rule, click **Add** to bring up the configuration page. To edit an existing rule, select the rule by clicking the radio button in front of the rule, and then click **Edit** to bring up the configuration page.



2. For adding a new rule, click **Add** to open the following page.

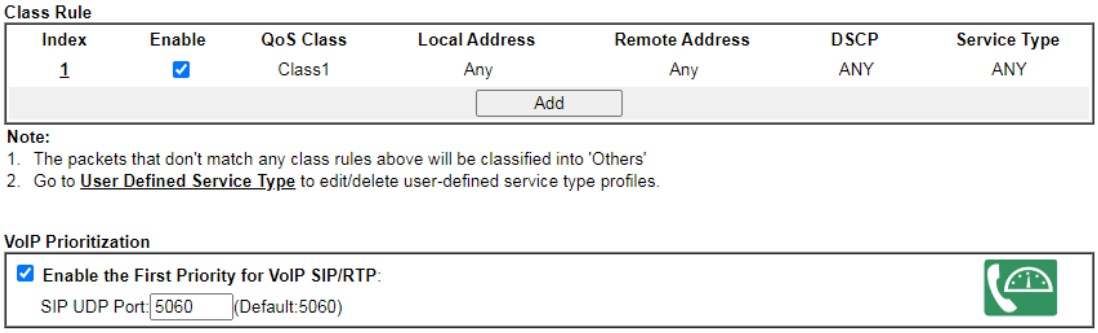


Available settings are explained as follows:

Item	Description
Enable	Check this box to invoke these settings.
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
Local Address	Click the **Edit** button to set the local IP address (on LAN) for the rule.
Remote Address	Click the **Edit** button to set the remote IP address (on LAN/WAN) for the rule.  **Address Type –** Determine the address type for the source address. For **Single Address**, you have to fill in Start IP address. For **Range Address**, you have to fill in Start IP address and End IP address. For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

3. After finishing all the settings here, please click **OK** to save the configuration.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.



VI-3 Central Management (AP)

VigorLTE 200 can manage the access points supporting AP management via Central AP Management.

AP Map

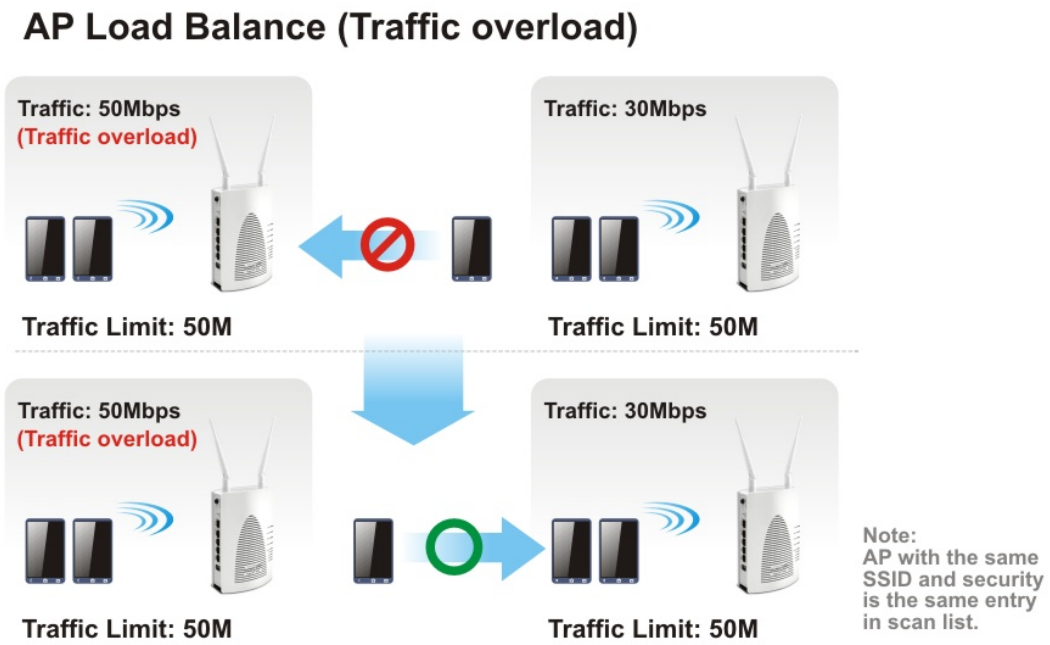
AP Map is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength

AP Maintenance

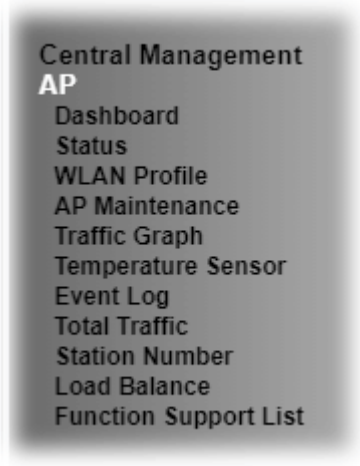
Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

Load Balance for AP

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

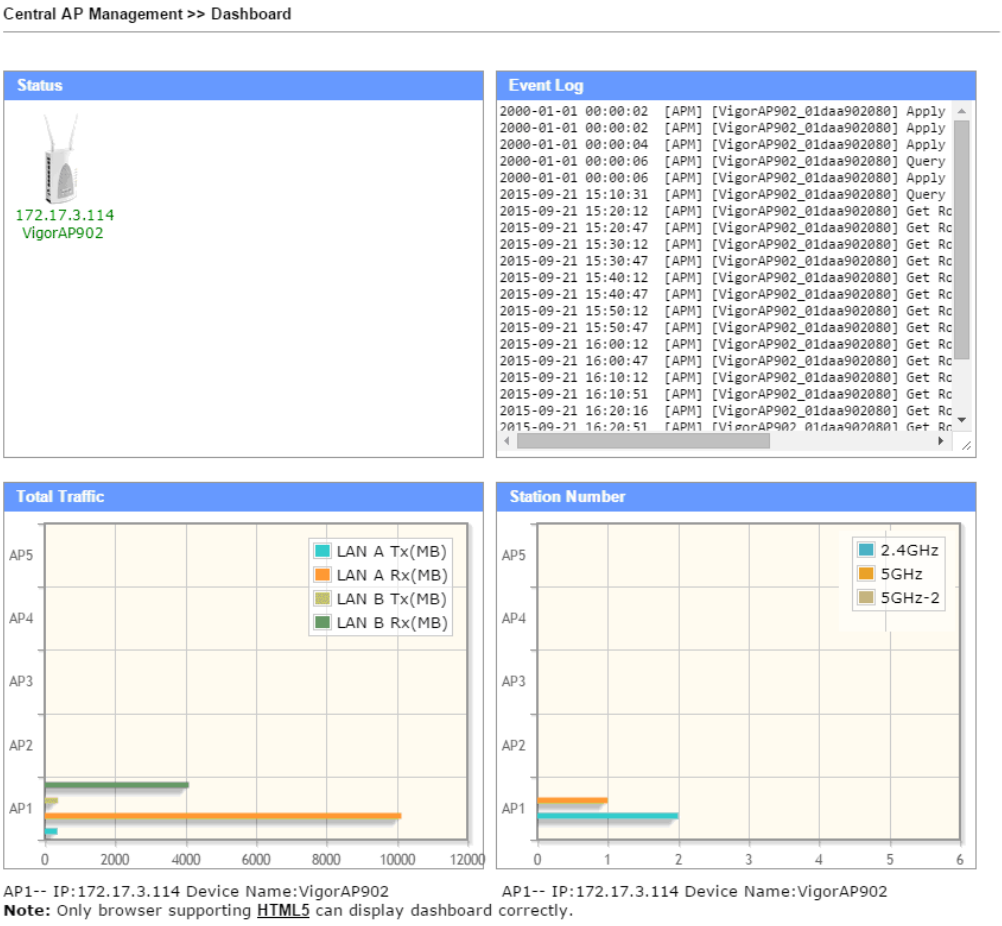


Web User Interface



VI-3-1 Dashboard

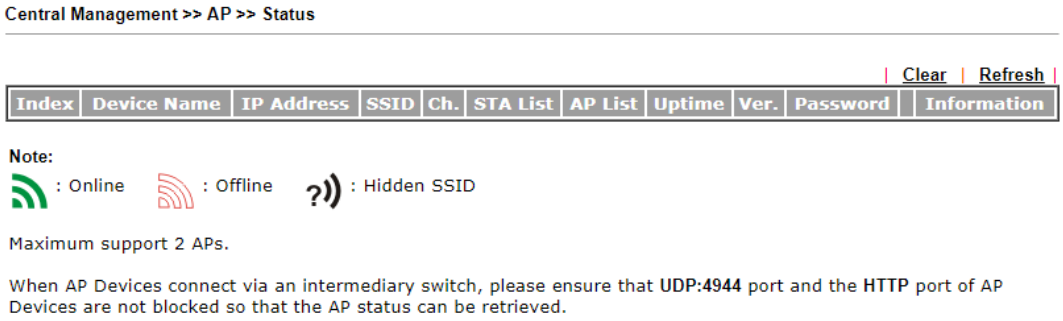
This page shows VigorAP's information about **Status, Event Log, Total Traffic** or **Station Number** by displaying VigorAP icon, text and histogram. Just move and click your mouse cursor on **Status, Event Log, Total Traffic** or **Station Number.** Corresponding web pages will be open immediately.



To access into the web user interface of VigorAP, simply move your mouse cursor on the VigorAP icon and click it. The system will guide you to access into the web user interface of VigorAP.

VI-3-2 Status

This page displays current status (online, offline or SSID hidden, IP address, encryption, channel, version, password and etc.) of the access points managed by Vigor router. Please open **Central AP Management>>Function Support List** to check what AP Models are supported.

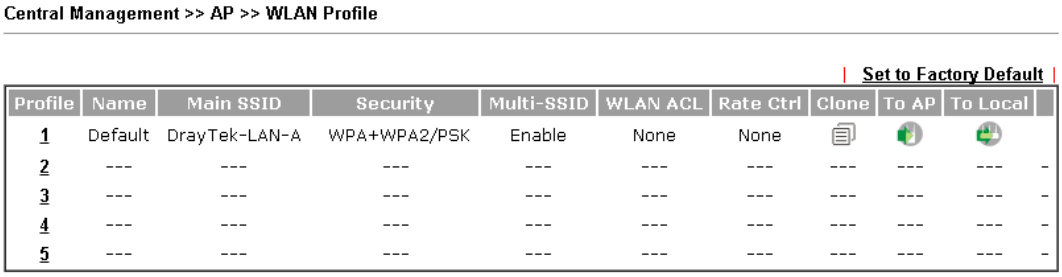


Available settings are explained as follows:

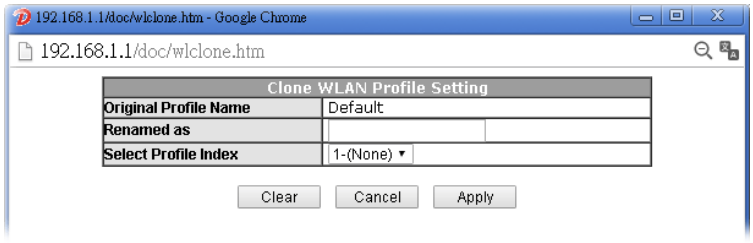
Item	Description
Index	Click the index number link for viewing the settings summary of the access point.
Device Name	The name of the AP managed by Vigor router will be displayed here.
IP Address	Display the true IP address of the access point.
SSID	Display the SSID configured for the access point(s) connected to VigorLTE 200.
Ch.	Display the channel used by the access point.
STA List	Display the number of wireless clients (stations) connecting to the access point. In which, 0/64 means that up to 64 clients are allowed to connect to the access point. But, now no one connects to the access point. The number displayed on the left side means 2.4GHz; and the number displayed on the right side means 5GHz.
AP List	Display the number of the AP around the device.
Uptime	Display the duration of the AP powered up.
Version	Display the firmware version used by the access point.
Password	VigorLTE 200 can get related information of the access point by accessing into the web user interface of the access point. This button is used to modify the logging password of the connected access point.
Information	Click Details to open a window of detailed information related to the selected VigorAP.

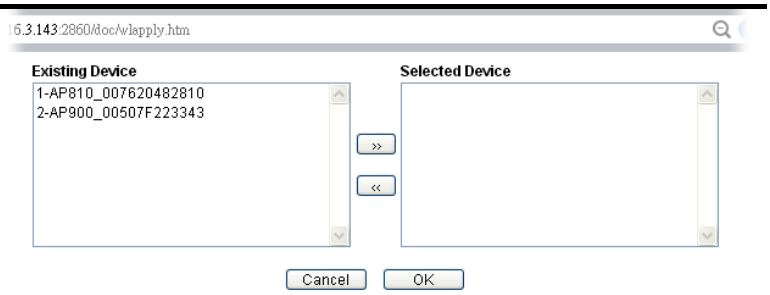
VI-3-3 WLAN Profile

WLAN profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.



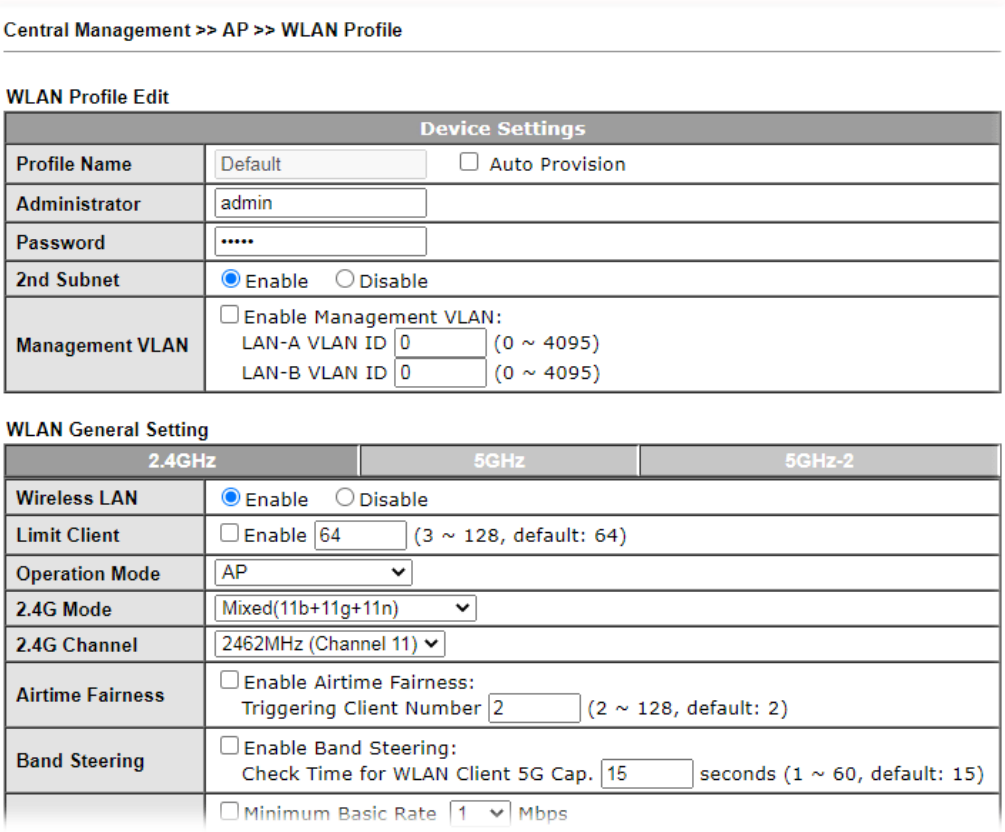
Click the number link of the selected profile to modify the content of the profile. Available settings are explained as follows:

Item	Description
Profile	There are five WLAN profiles offered to be configured. Simply click the index number link to open the modification page.
Name	Display the name of the profile. The default profile cannot be renamed.
Main SSID	Display the SSID configured by such wireless profile.
Security	Display the security mode selected by such wireless profile.
Multi-SSID	Enable means multiple SSIDs (more than one) are active. Disable means only SSID1 is active.
WLAN ACL	Display the name of the access control list.
Rate Ctrl	Display the upload and/or download transmission rate.
Clone	It can copy settings from an existing WLAN profile to another WLAN profile. First, you have to check the box of the existing profile as the original profile. Second, click **Clone**. The following dialog will appear.  Third, choose the profile index to accept the settings from the original profile. Forth, type a new name in the field of **Renamed as**. Last, click **Apply** to save the settings on this dialog. The new profile has been created with the settings coming from the original profile.
To AP	Click it to apply the selected wireless profile to the specified Access Point.

	 Simply choose the device you want from **Existing Device** field. Click **>>** to move the device to **Selected Device** field. Then, click **OK**. The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot.
To Local	WLAN Profile configured in this page is specified for VigorAP connected to Vigor router. If required, these settings also can be applied to Vigor router. Select and check one of wireless profiles and click this button to apply the settings onto the WI-Fi wireless settings configured for such Vigor router.

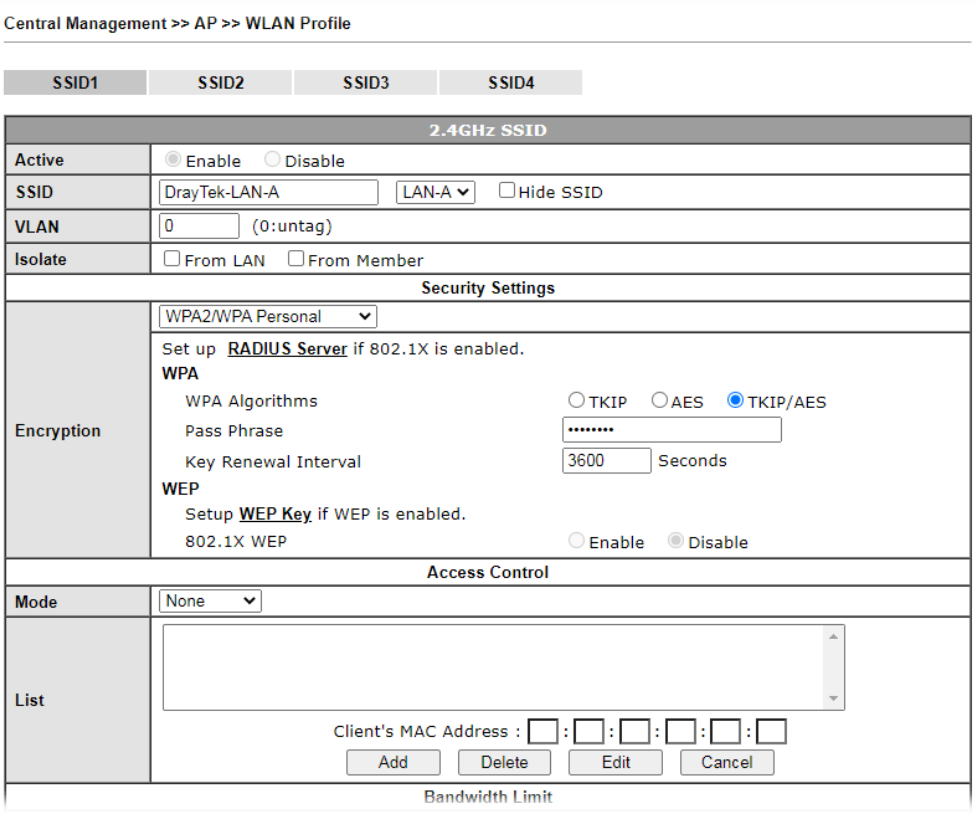
How to edit the wireless LAN profile?

1. Select the WLAN profile (index number 1 to 5) you want to edit.
2. Click the index number link to display the following page.

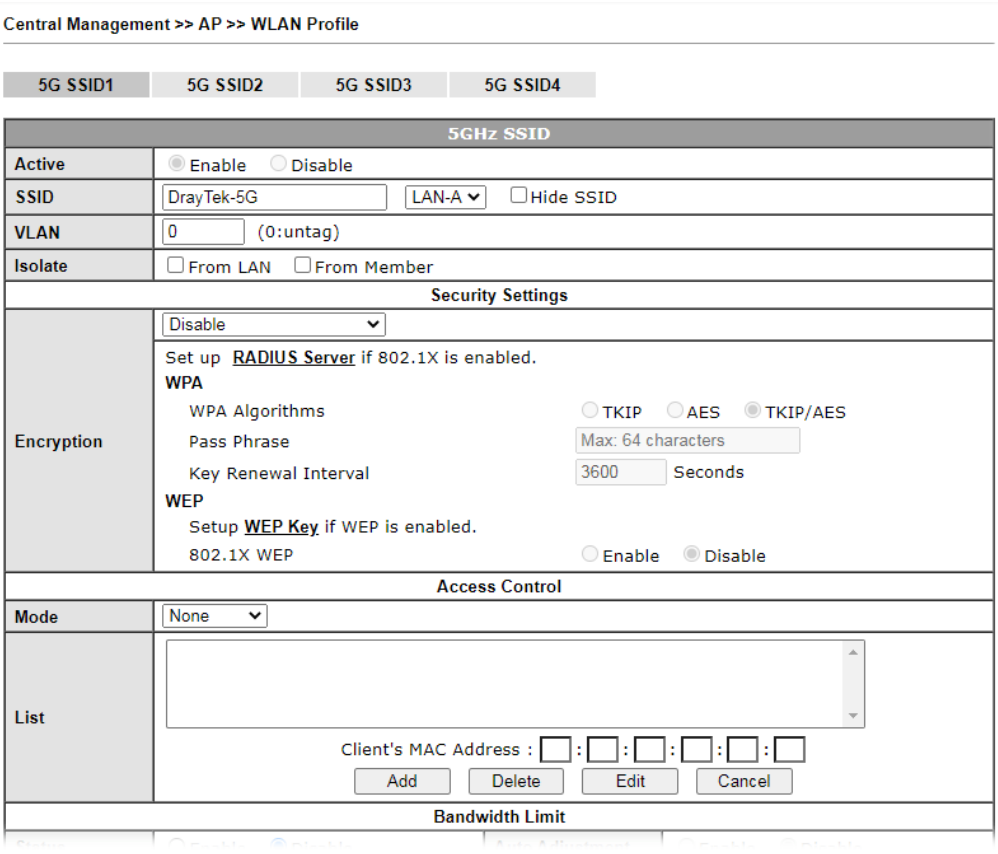


Info The function of Auto Provision is available for the default WLAN profile.

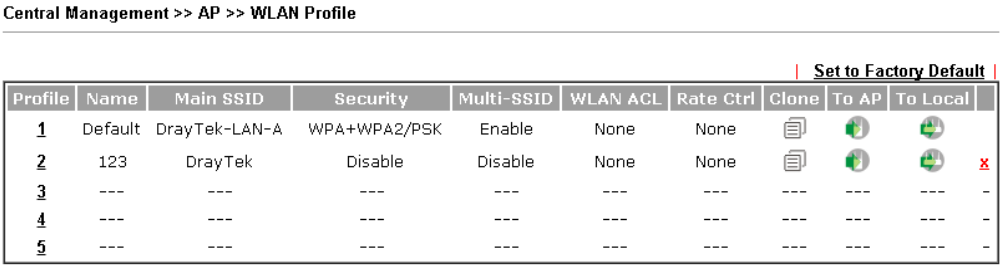
3. After finished the general settings configuration, click **Next** to open the following page for 2.4G wireless security settings.



4. After finished the above web page configuration, click **Next** to open the following page for 5G wireless security settings.



5. When you finished the above web page configuration, click **Finish** to exit and return to the first page. The modified WLAN profile will be shown on the web page.



Central Management >> AP >> WLAN Profile

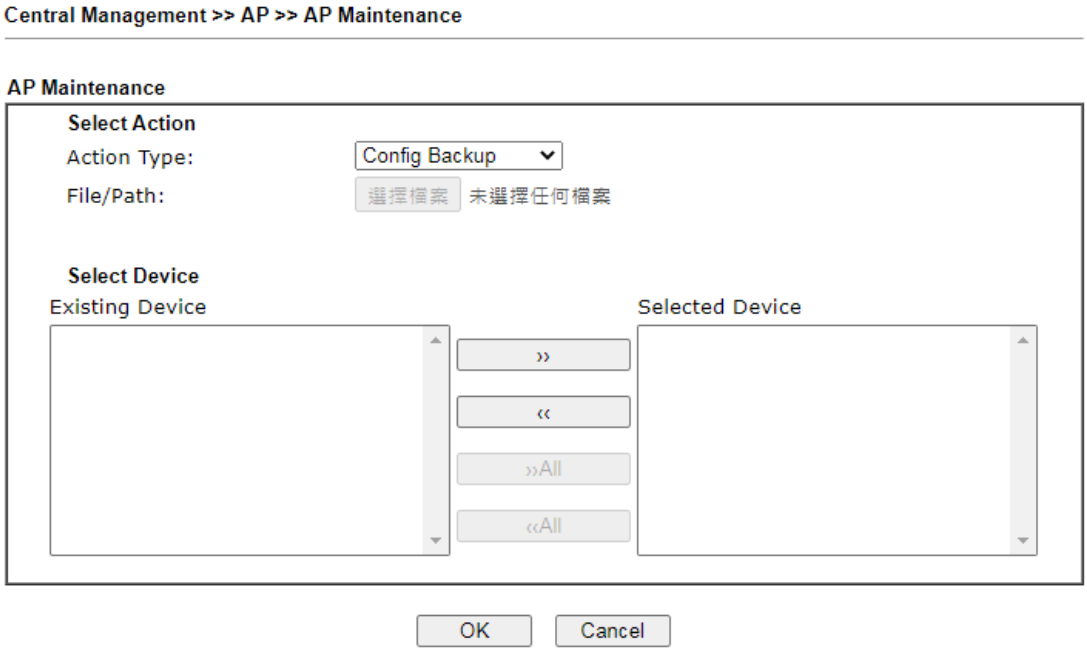
| Set to Factory Default |

Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local	
1	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None				
2	123	DrayTek	Disable	Disable	None	None				x
3	---	---	---	---	---	---	---	---	---	-
4	---	---	---	---	---	---	---	---	---	-
5	---	---	---	---	---	---	---	---	---	-

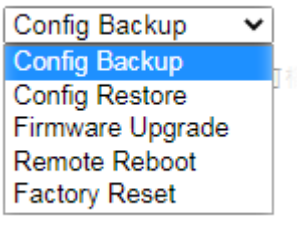
VI-3-4 AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

Info	Config Backup can be performed to one AP at one time. Others functions (e.g., Config Restore, Firmware Upgrade, Remote Reboot can be performed to more than one AP at one time by using VigorLTE 200.



Available settings are explained as follows:

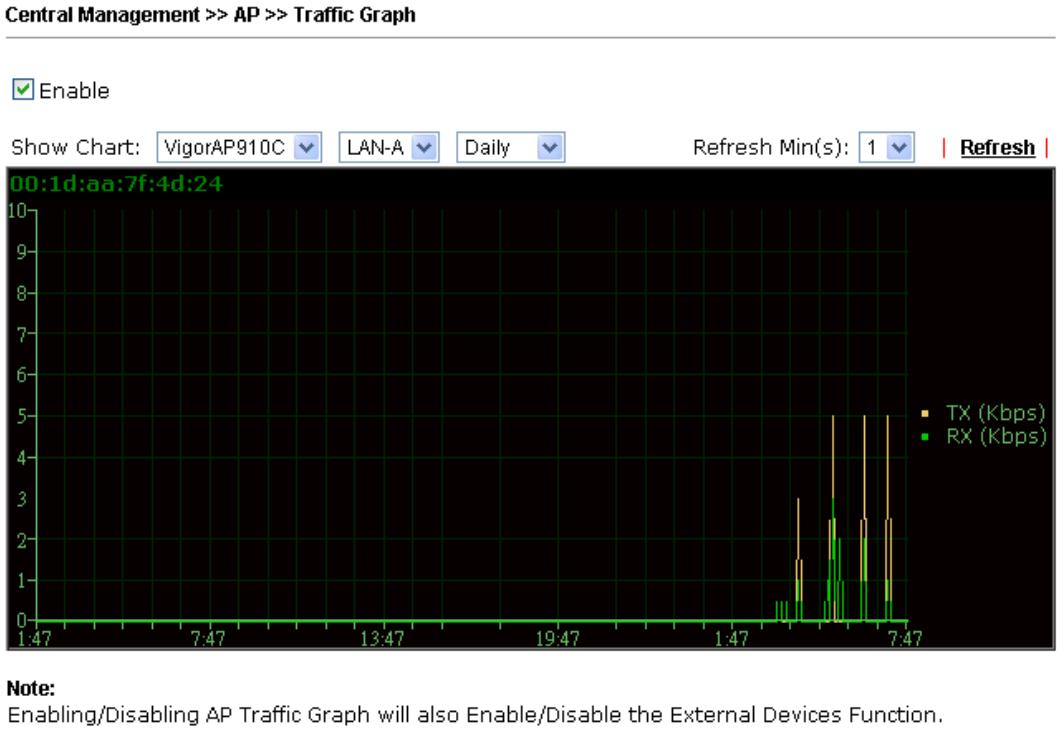
Item	Description
Action	There are four actions provided by Vigor router to manage the access points.  Vigor router can **backup** the configuration of the selected AP, **restore** the configuration for the selected AP, perform the **firmware upgrade** of the selected AP, **reboot** the selected AP remotely and perform the **factory reset** for the selected AP.
File/Path	Specify the file and the path which will be used to perform **Config Restore** or **Firmware Upgrade**.
Select Device	Display all the available access points managed by Vigor

	router. Simply click << or >> to move the device(s) between **Select Device** and **Selected Device** areas.
Selected Device	Display the access points that will be applied by such function after clicking OK.

After finishing all the settings here, please click **OK** to perform the action.

VI-3-5 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.



Note:
Enabling/Disabling AP Traffic Graph will also Enable/Disable the External Devices Function.

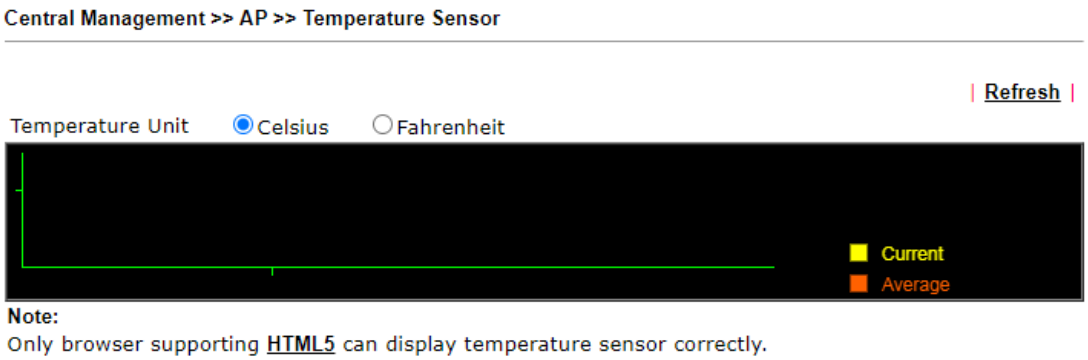
The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).

Info	Enabling/Disabling such function will also enable/disable the External Devices function.

VI-3-6 Temperature Sensor

Many VigorAPs and Vigor routers can be installed with temperature sensor. If VigorAP (e.g., VigorAP 910C) is managed under Vigor router, then Vigor router can obtain the temperature change graph of the USB temperature sensor installed onto VigorAP.

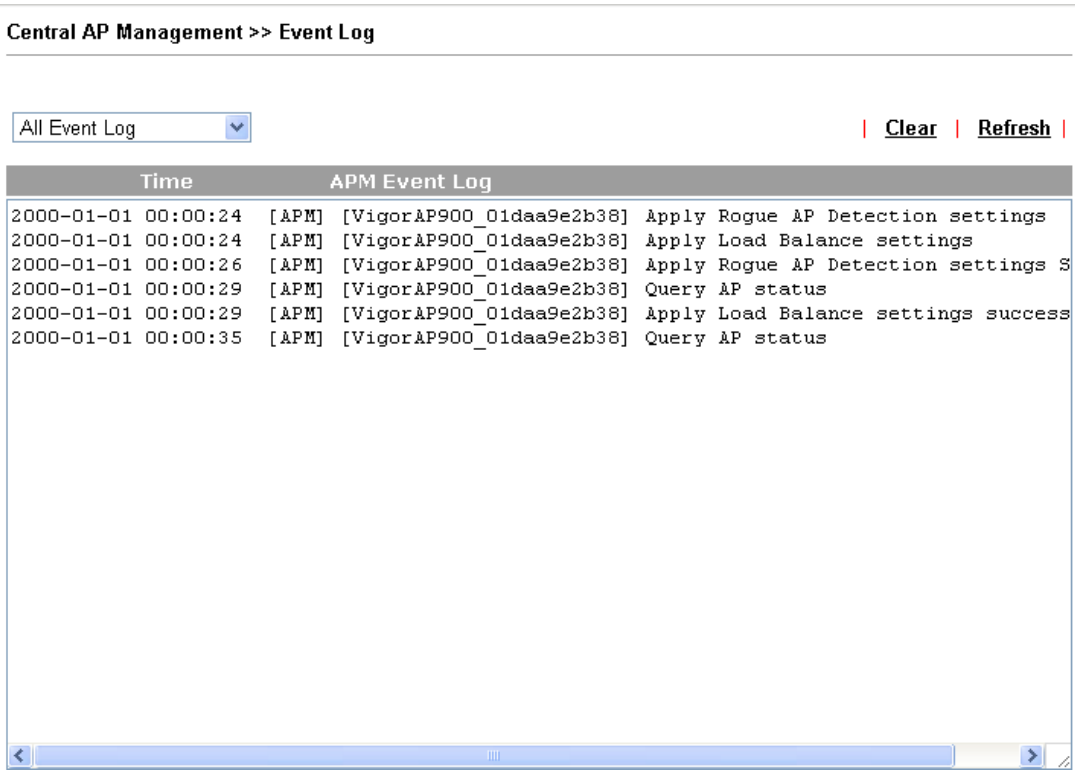
This page displays data including current temperature, maximum temperature, minimum temperature and average temperature.



Note:
Only browser supporting HTML5 can display temperature sensor correctly.

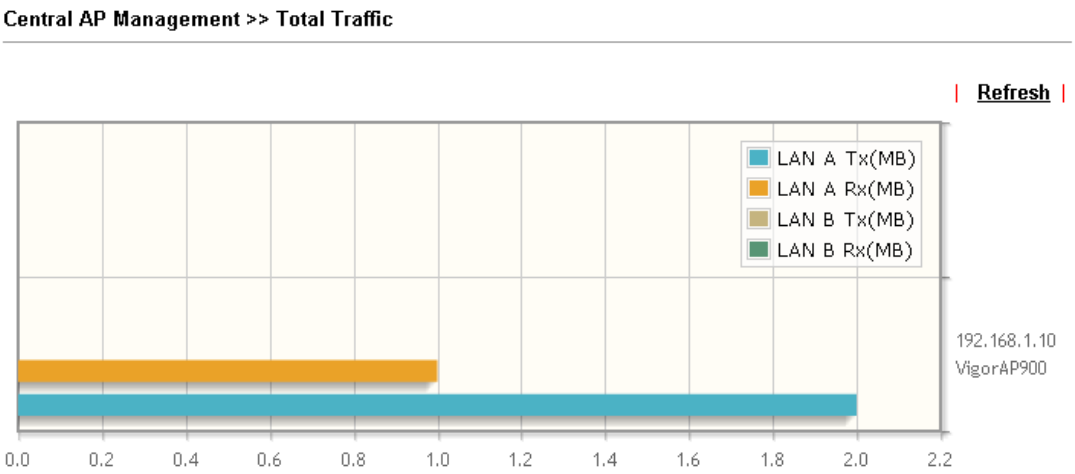
VI-3-7 Event Log

Time and event log for all of the APs managed by Vigor router will be shown on this page. It is useful for troubleshooting if required.



VI-3-8 Total Traffic

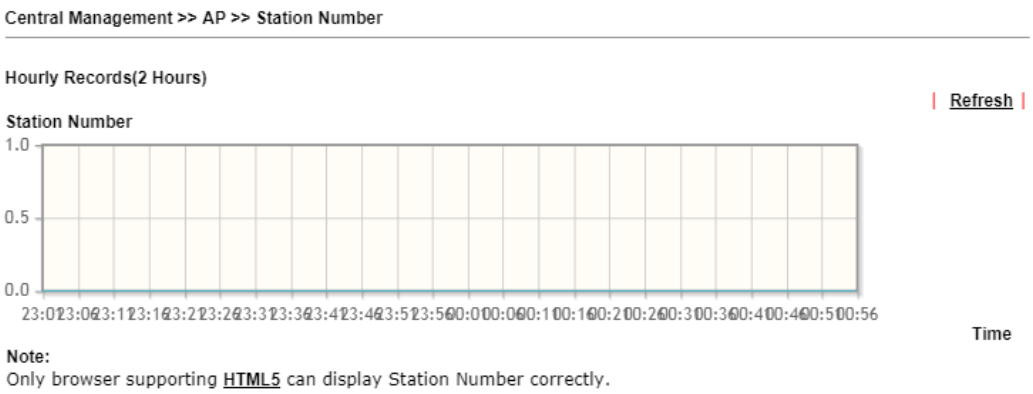
Such page will display the total traffic of data receiving and data transmitting for VigorAPs managed by Vigor router.



Note: Only browser supporting **HTML5** can display Total Traffic correctly.

VI-3-9 Station Number

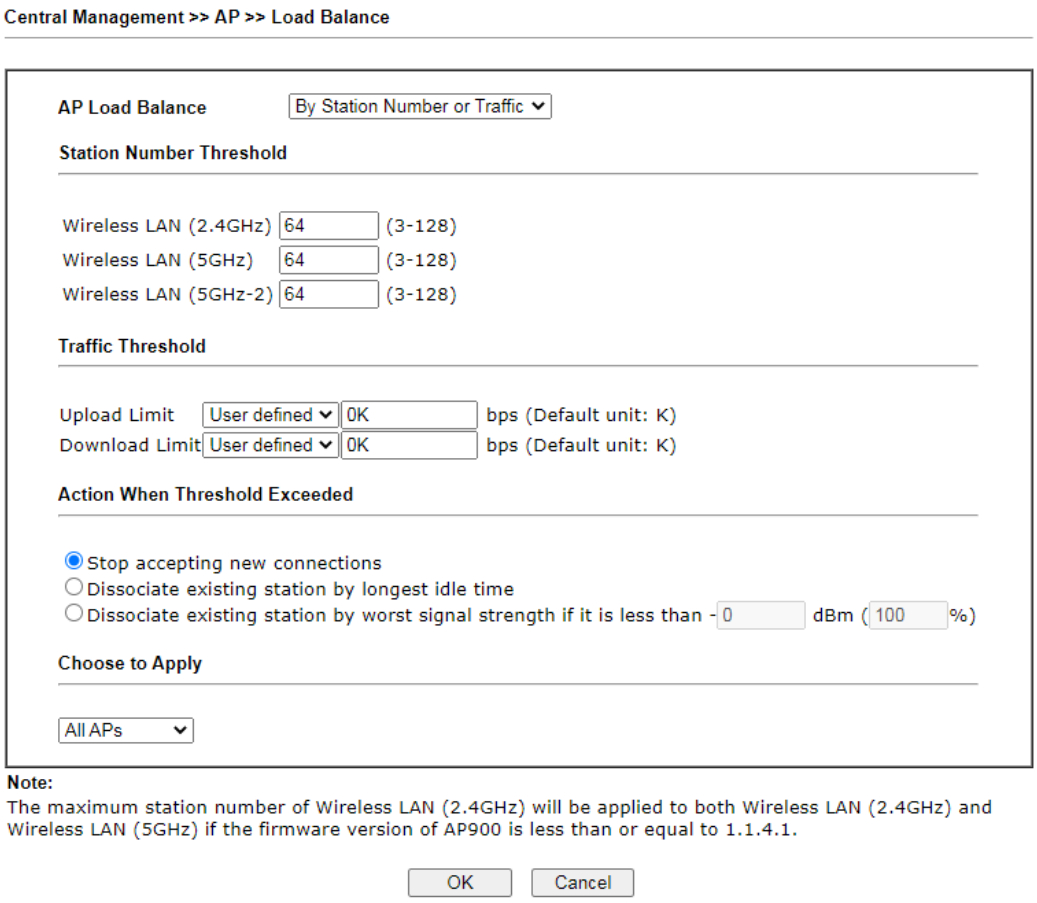
The total number of the wireless clients will be shown on this page.



Note:
Only browser supporting HTML5 can display Station Number correctly.

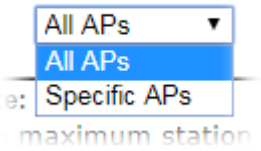
VI-3-10 Load Balance

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.



Available settings are explained as follows:

Item	Description
AP Load Balance	It is used to determine the operation mode when the system detects overload between access points. **Disable** – Disable the function of AP load balance. **By Station Number** –The operation of load balance will be executed based on the station number configured in this page. It is used to limit the allowed number for the station connecting to the access point. The purpose is to prevent lots of stations connecting to access point at the same time and causing traffic unbalanced. Please define the required station number for WLAN (2.4GHz) and WLAN (5GHz) separately. **By Traffic** – The operation of load balance will executed according to the traffic configuration in this page. **By Station Number or Traffic** - The operation of load balance will be executed based on the station number or the traffic configuration.
Station Number Threshold	Set the number of stations as a threshold to activate AP load balance.
Traffic Threshold	**Upload Limit** –Use the drop down list to specify the traffic

	limit for uploading. **Download Limit** – Use the drop down list to specify the traffic limit for downloading.
Action When Threshold Exceeded	**Stop accepting new connections –** When the number of stations or the traffic reaches the threshold defined in this web page, Vigor router will stop any new connection asked by other access point. **Dissociate existing station by longest idel time** - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station which is idle for a longest time. **Dissociate existing station by worst signal strength if it is less than** - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station with the weakest signal.
Choose to Apply	The settings configured for Load Balance can be applied to all of AP devices or selected AP devices. 

After finishing all the settings here, please click **OK** to save the configuration.

VI-3-11 Function Support List

Central AP Management >> Function Support List

Model Name	AP710	AP800	AP810	AP900	AP902	AP910C
FW Version	**1.2.0**	**1.1.6**	**1.1.6.1**	**1.1.7**	**1.1.7**	**1.1.6**
Register						
DHCP	•	•	•	•	•	•
Static IP	•	•	•	•	•	•
Profile						
2.4GHz	•	•	•	•	•	•
5GHz		• (with N65)		•	•	•
AP Mode	•	•	•	•	•	•
Auto Provision	•	•	•	•	•	•
WLAN Enable/Disable	•	•	•	•	•	•
Limit Client	•		•	•	•	•
Airtime Fairness	•		•	•	•	•
Band Steering				•	•	•
Fast Roaming	•		•	•	•	•
Access Control List	•	•	•	•	•	•
Bandwidth Limit	•	•	•	•	•	•
Centralized AP Management						
AP Maintenance	•		•	•	•	•
Traffic Graph	•	•	•	•	•	•
Event Log	•		•	•	•	•
Total Traffic	•		•	•	•	•
Station Number	•		•	•	•	•
Load Balance	•		•	•	•	•

This page is left blank.

Part VII Others

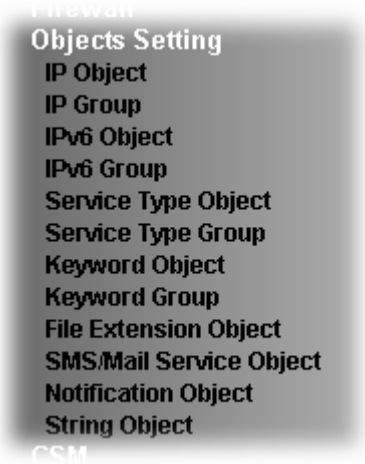
Objects Settings

Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.

VII-1 Objects Settings

Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.

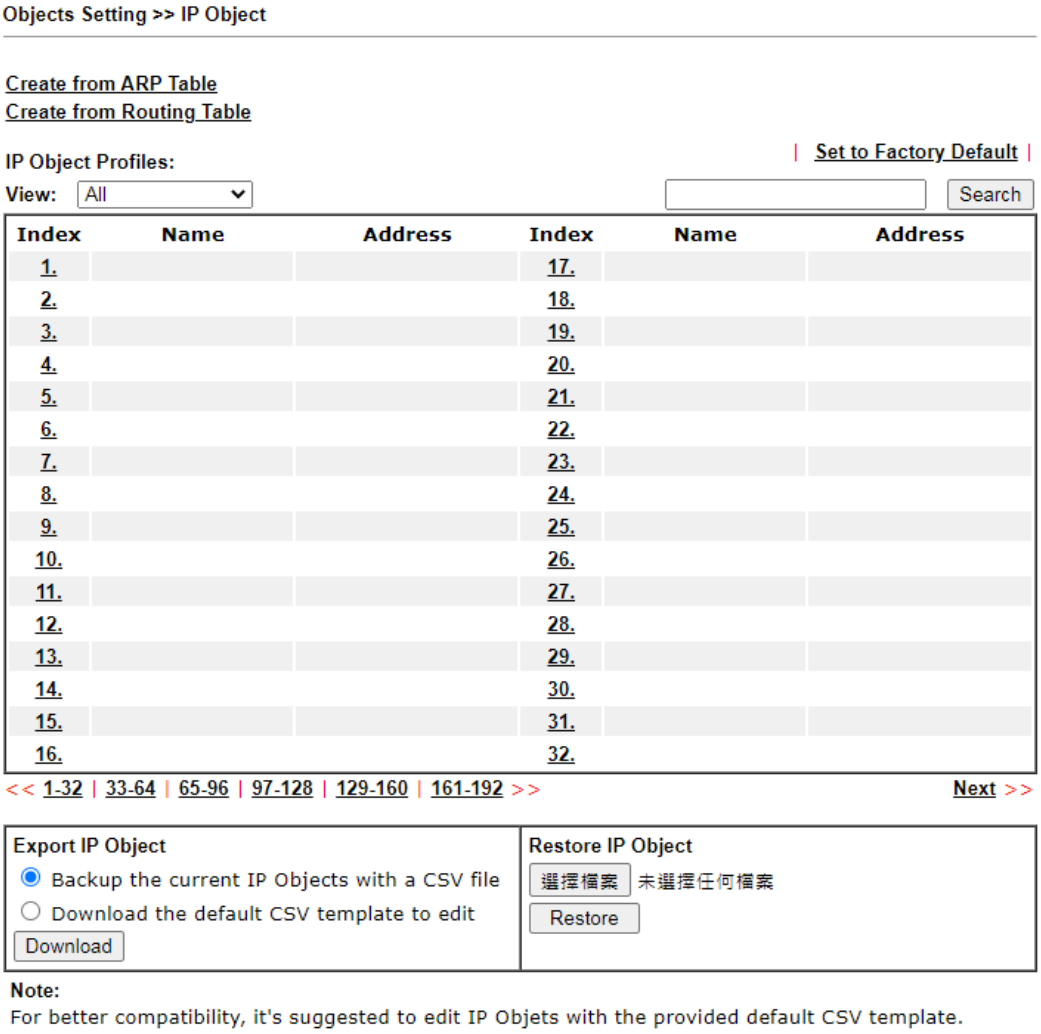
Web User Interface



VII-1-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

You can set up to 192 sets of IP Objects with different conditions.



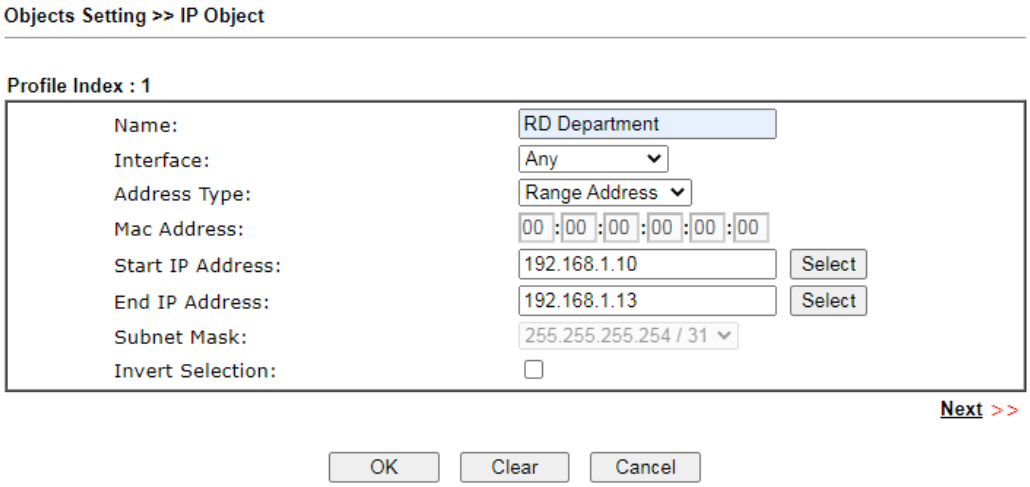
Available settings are explained as follows:

Item	Description
View	Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page.
Set to Factory Default	Clear all profiles.
Search	Type a string of the IP object that you want to search.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Address	Display the IP address configured for the object profile.
Export IP Object	Usually, the IP objects can be created one by one through the web page of **Objects>>IP Object**. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file. All of the IP objects (or the template) can be exported as a file by clicking Download. Then the user can open the CSV file through Microsoft Excel and modify all the IP objects at the same time. **Backup the current IP Objects with a CSV file** – Click it to backup current IP objecsts as a CSV file. Such file can be

	restored for future use. **Download the default CSV template to edit** – After clicking it, press Download to store the default CSM template (a table without any input data) to your hard disk. **Download** – Download the CSV file from Vigor router and store in your hard disk.
Restore IP Object	**Select –** Click it to specify a predefined CSV file. **Restore –** Import the selected CSV file onto Vigor router.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

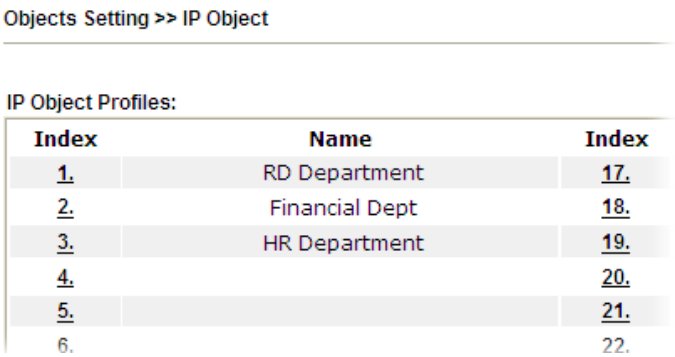


Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface. For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN/RT/VPN or any IP address. If you choose LAN/ RT/VPN as the **Interface** here, and choose LAN/RT/VPN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN/ RT/VPN interface will be opened for you to choose in **Edit Filter Rule** page.
Address Type	Determine the address type for the IP address. Select **Single Address** if this object contains one IP address only. Select **Range Address** if this object contains several IPs within a range. Select **Subnet Address** if this object contains one subnet for IP address. Select **Any Address** if this object contains any IP address. Select **Mac Address** if this object contains Mac address.
MAC Address	Enter the MAC address of the network card which will be controlled.
Start IP Address	Enter the start IP address for Single Address type.

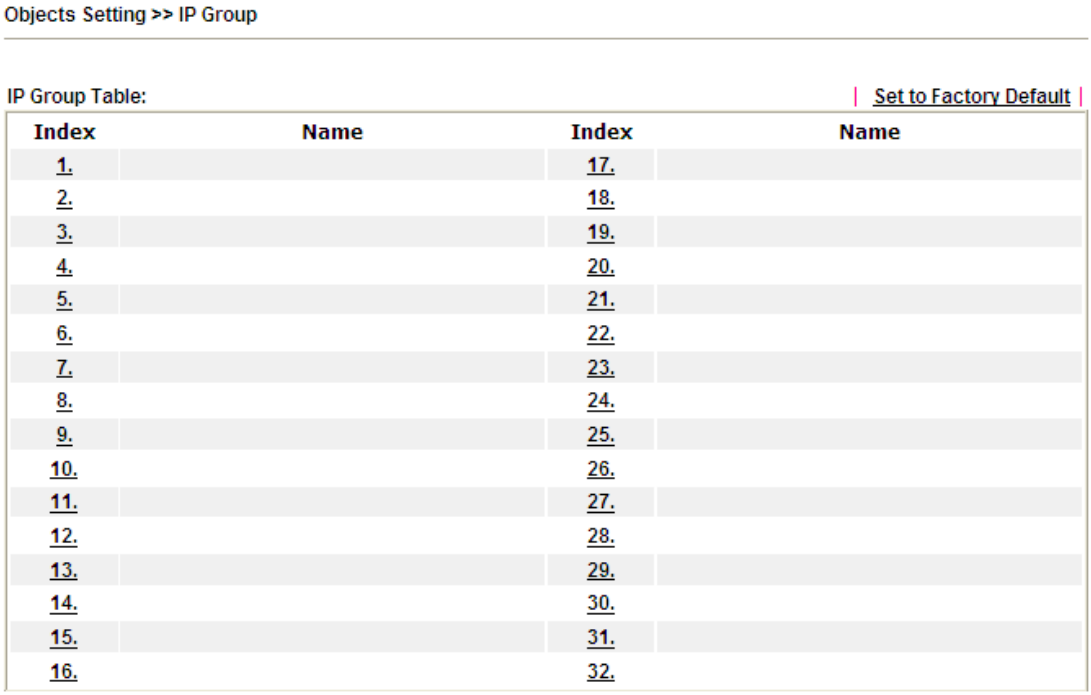
End IP Address	Enter the end IP address if the Range Address type is selected.
Subnet Mask	Enter the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

4. After finishing all the settings here, please click **OK** to save the configuration. Below is an example of IP objects settings.



VII-1-2 IP Group

This page allows you to bind several IP objects into one IP group.

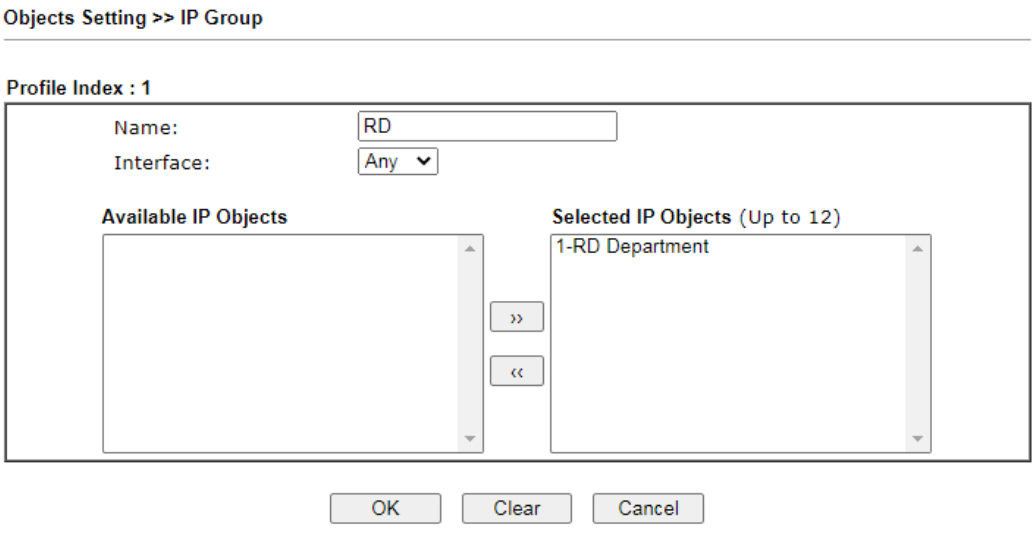


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



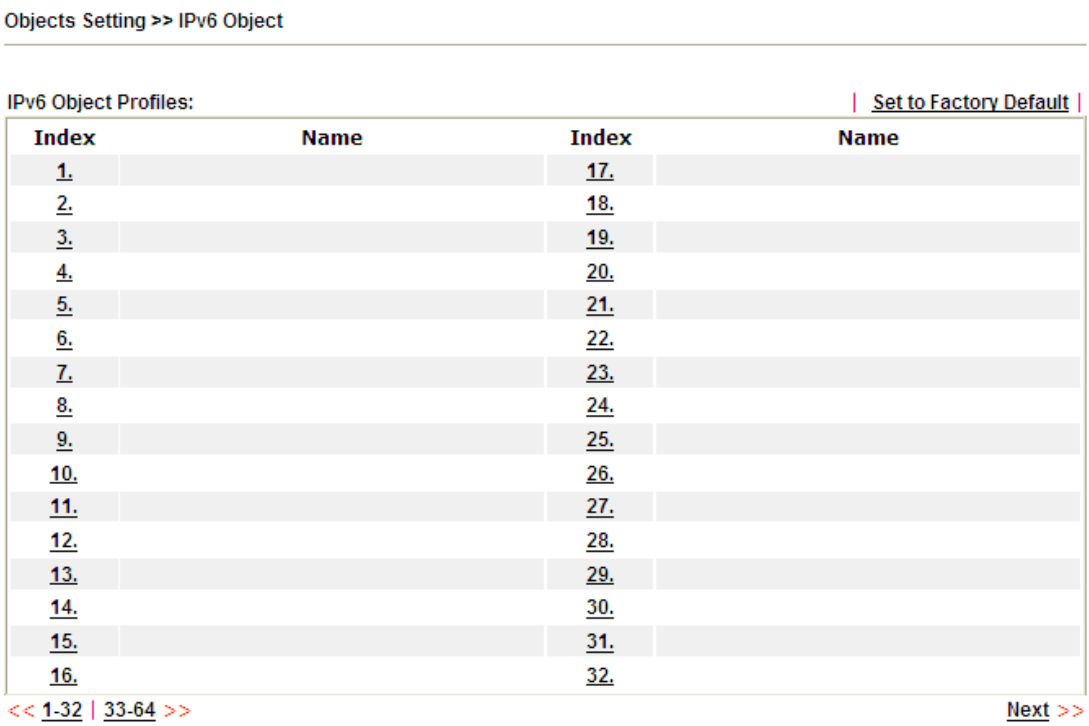
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click **>>** button to add the selected IP objects in this box.

3. After finishing all the settings here, please click **OK** to save the configuration.

VII-1-3 IPv6 Object

You can set up to 64 sets of IPv6 Objects with different conditions.

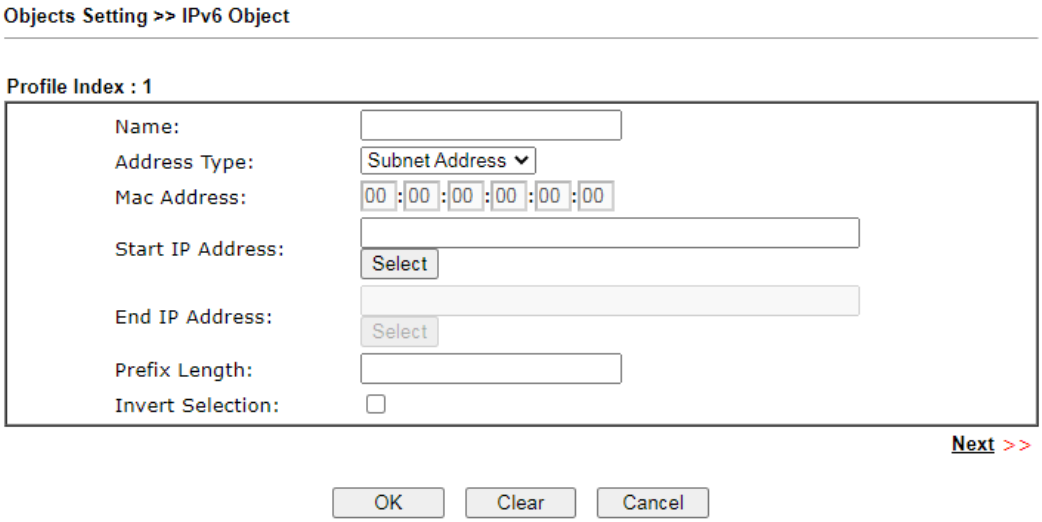


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



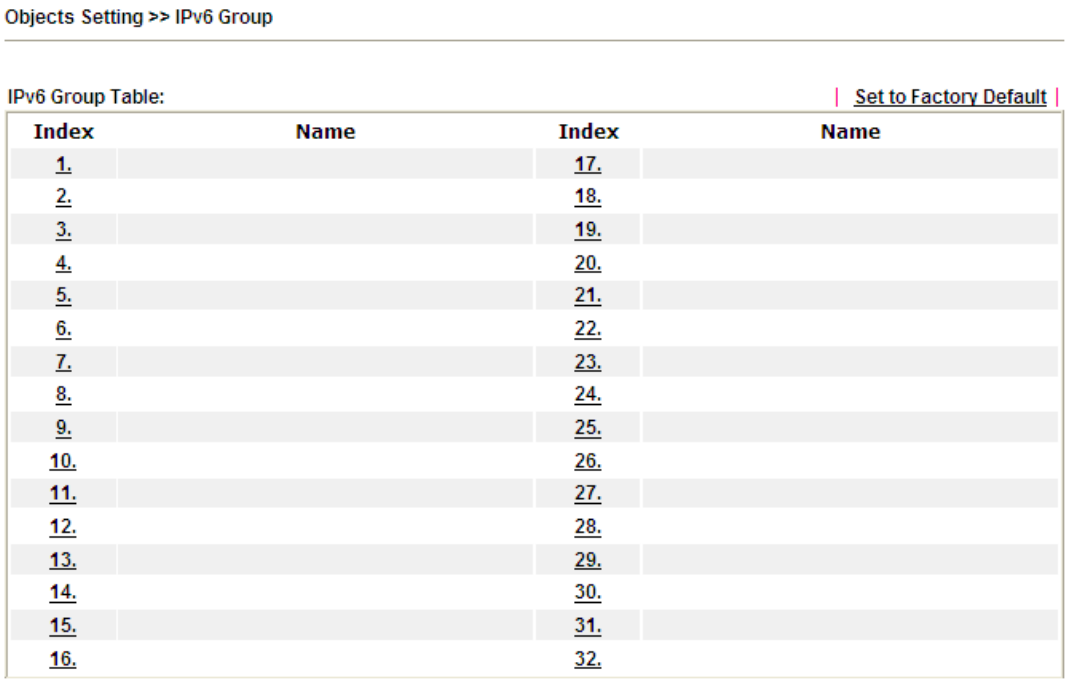
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	Determine the address type for the IPv6 address. Select **Single Address** if this object contains one IPv6 address only. Select **Range Address** if this object contains several IPv6s within a range. Select **Subnet Address** if this object contains one subnet for IPv6 address. Select **Any Address** if this object contains any IPv6 address. Select **Mac Address** if this object contains Mac address.
Mac Address	Enter the MAC address of the network card which will be controlled.
Start IP Address	Enter the start IP address for Single Address type.
End IP Address	Enter the end IP address if the Range Address type is selected.
Prefix Length	Enter the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

3. After finishing all the settings, please click **OK** to save the configuration.

VII-1-4 IPv6 Group

This page allows you to bind several IPv6 objects into one IPv6 group.

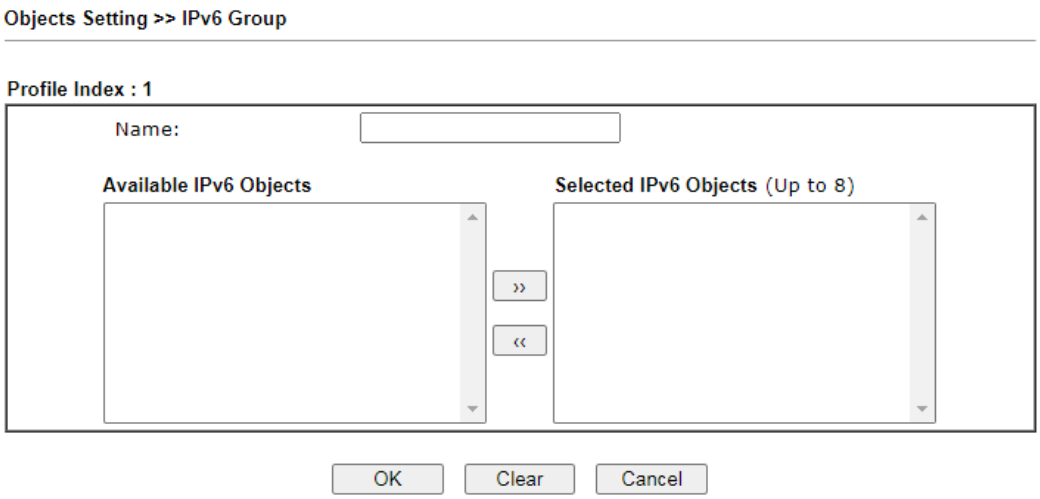


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



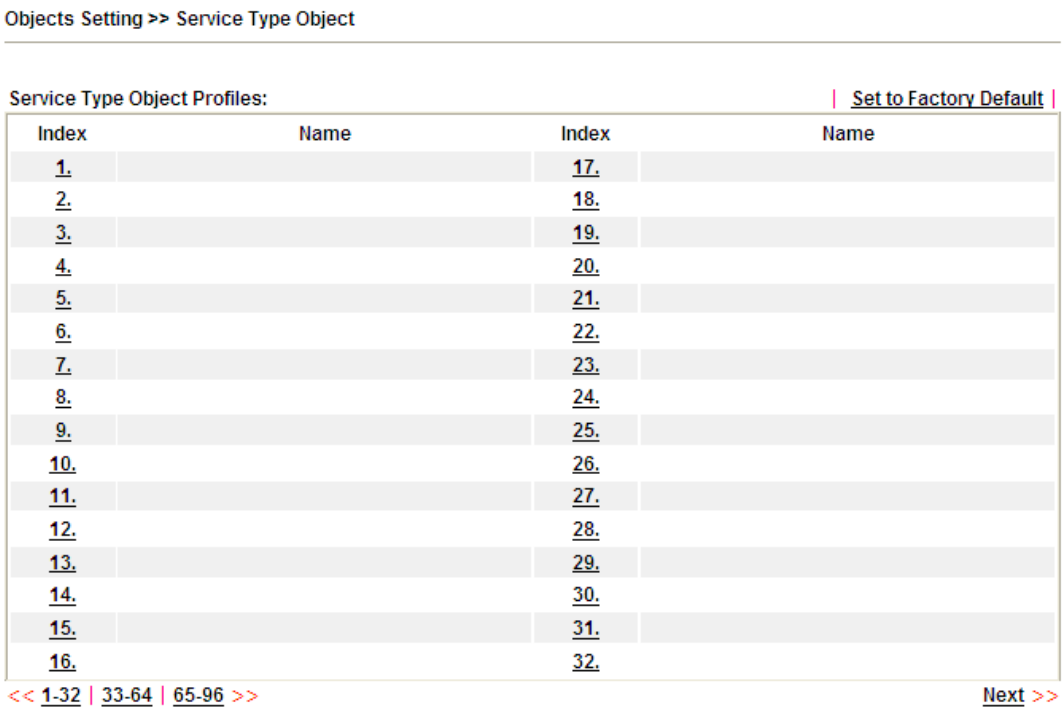
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click **>>** button to add the selected IPv6 objects in this box.

3. After finishing all the settings, please click **OK** to save the configuration.

VII-1-5 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.

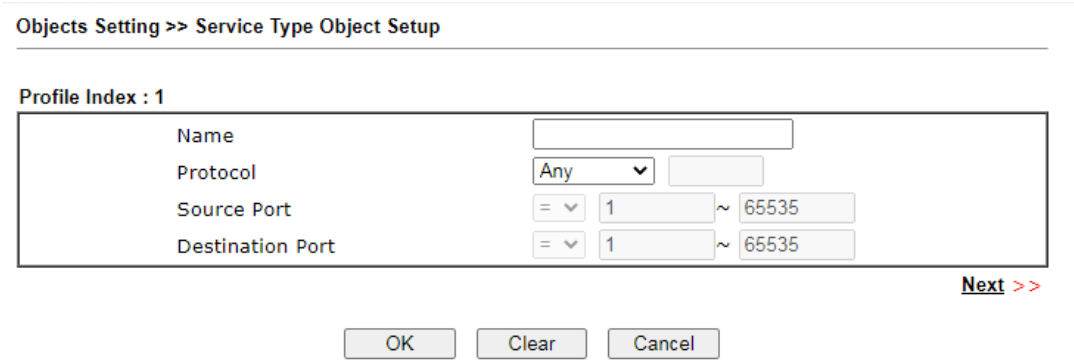


Available settings are explained as follows:

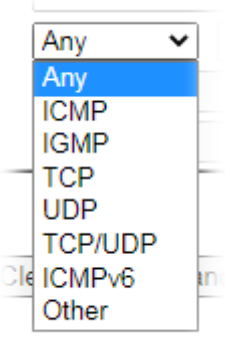
Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

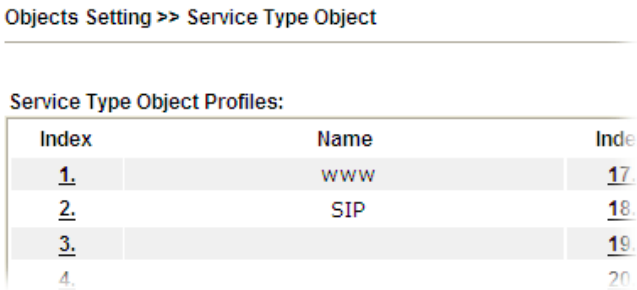
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

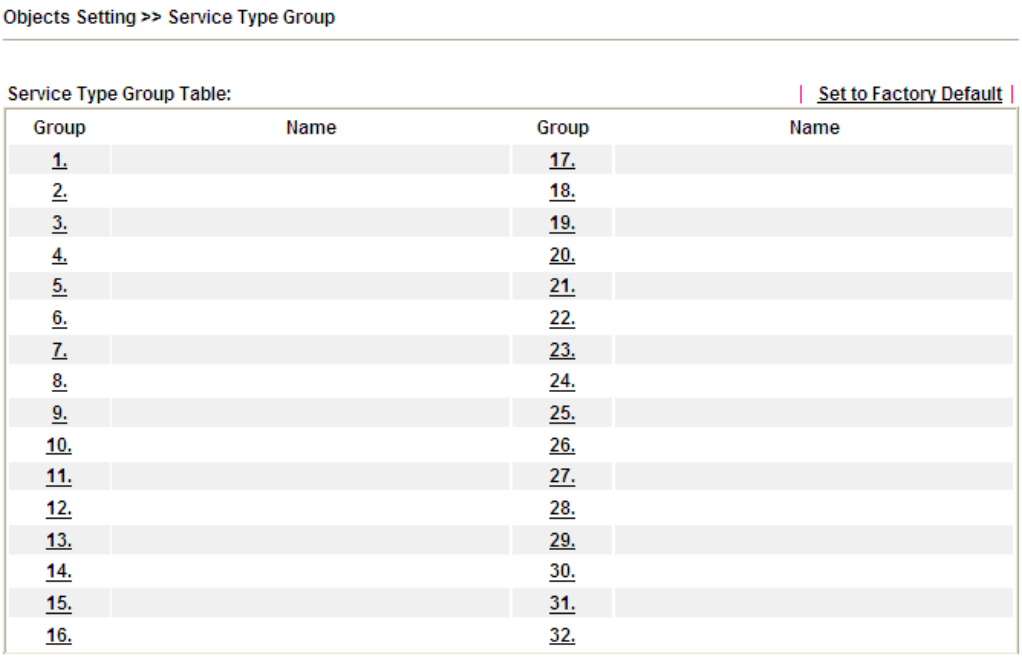
Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source/Destination Port	**Source Port** and the **Destination Port** columns are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. *(=)* – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. *(!=)* – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. *(>)* – the port number greater than this value is available. *(<)* – the port number less than this value is available for this profile.

3. After finishing all the settings, please click **OK** to save the configuration.



VII-1-6 Service Type Group

This page allows you to bind several service types into one group.

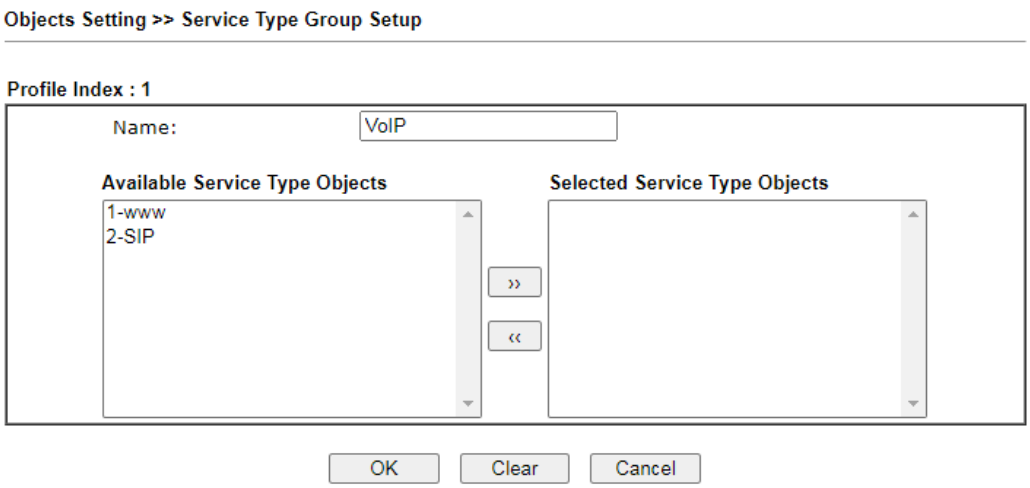


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Group column for configuration in details.
2. The configuration page will be shown as follows:



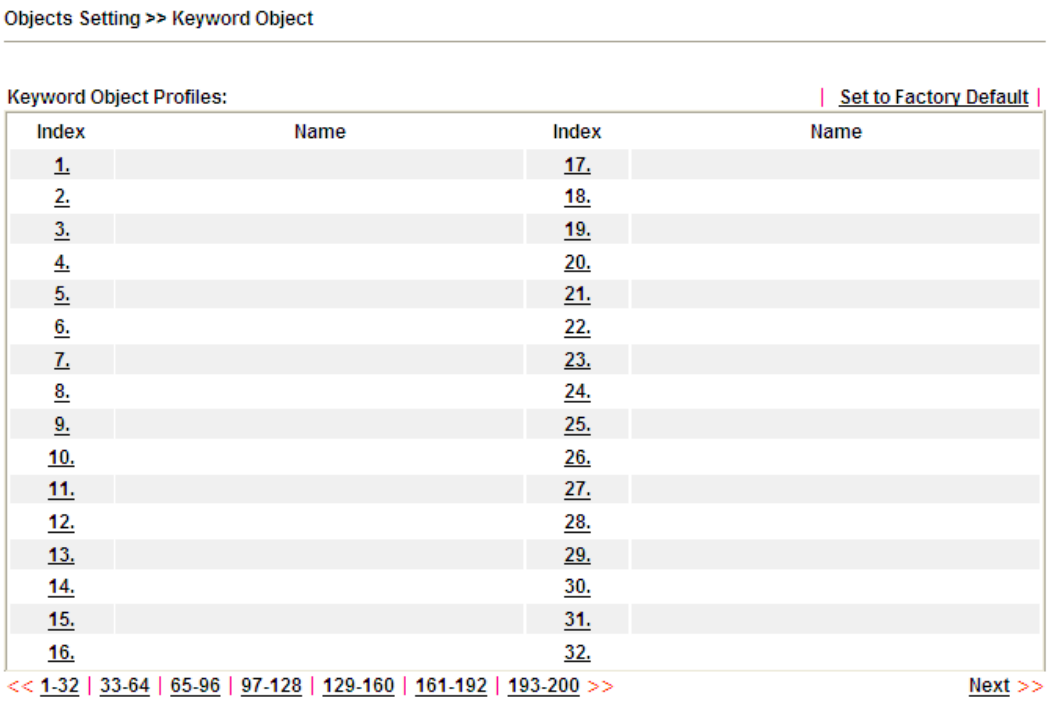
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available Service Type Objects	All the available service objects that you have added on **Objects Setting>>Service Type Object** will be shown in this box.
Selected Service Type Objects	Click **>>** button to add the selected IP objects in this box.

3. After finishing all the settings, please click **OK** to save the configuration.

VII-1-7 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in **CSM >>URL Web Content Filter Profile.**

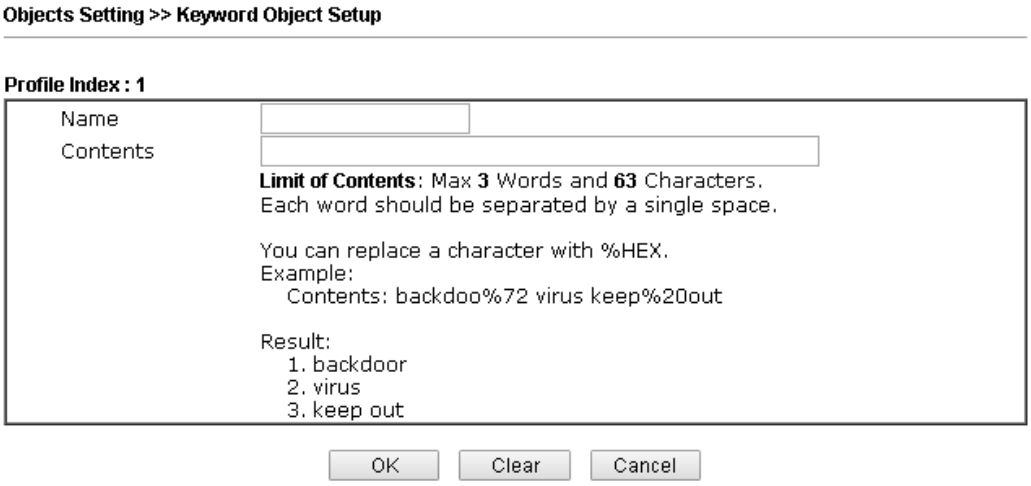


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



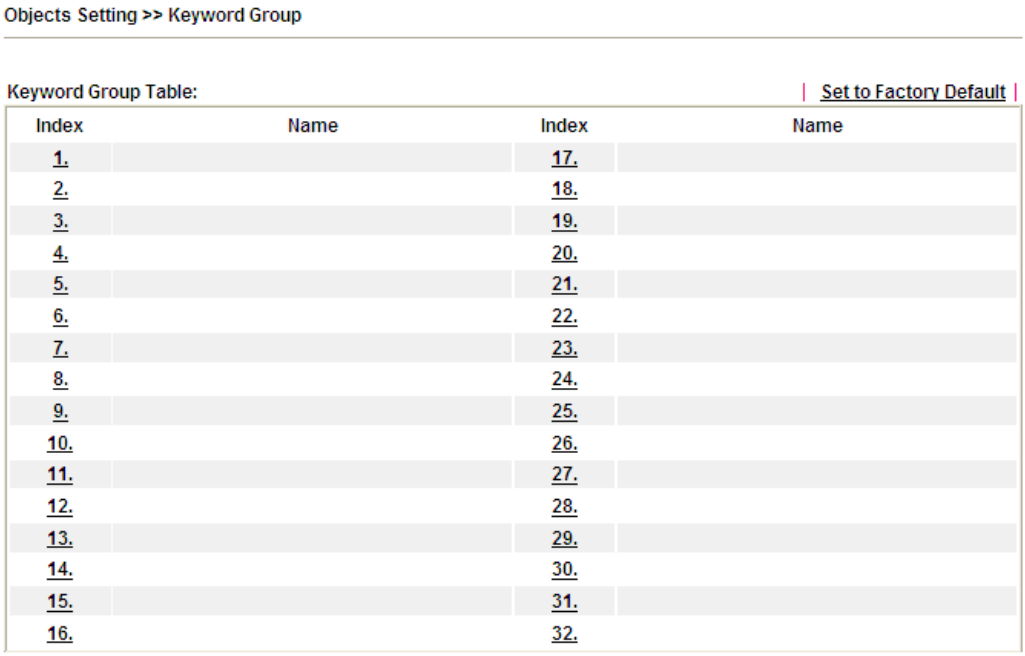
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Enter the content for such profile. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

3. After finishing all the settings, please click **OK** to save the configuration.

VII-1-8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **CSM >>URL /Web Content Filter Profile**.

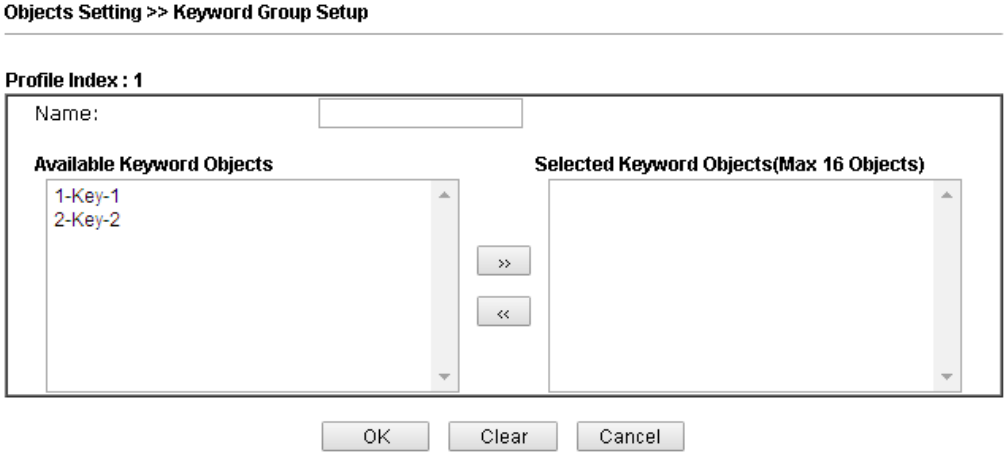


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



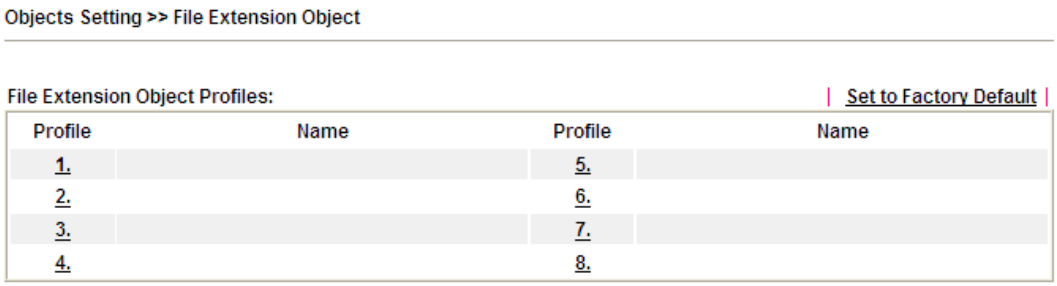
Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
Available Keyword Objects	You can gather keyword objects from **Keyword Object** page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click » button to add the selected Keyword objects in this box.

3. After finishing all the settings, please click **OK** to save the configuration.

VII-1-9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

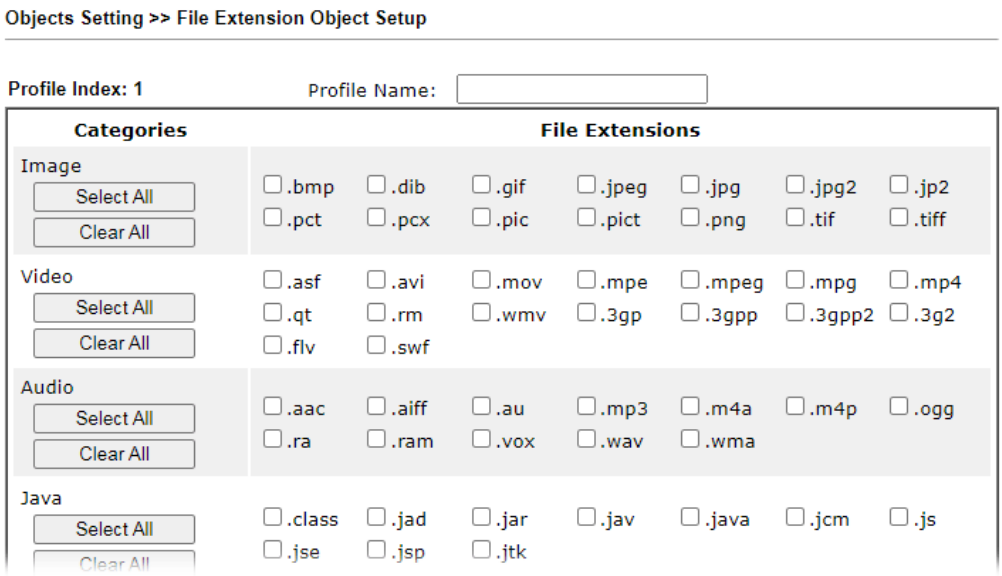


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Profile column for configuration in details.
2. The configuration page will be shown as follows:



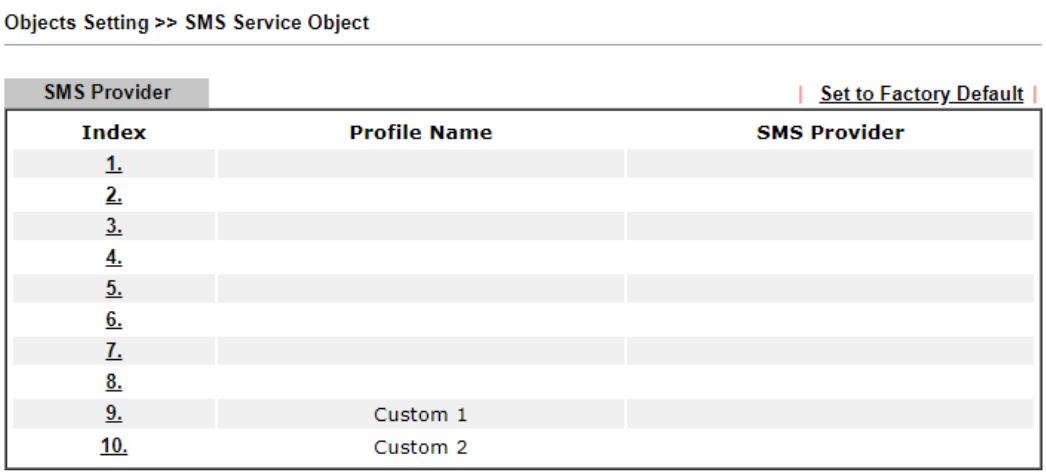
Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

VII-1-10 SMS Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS Service Object**.

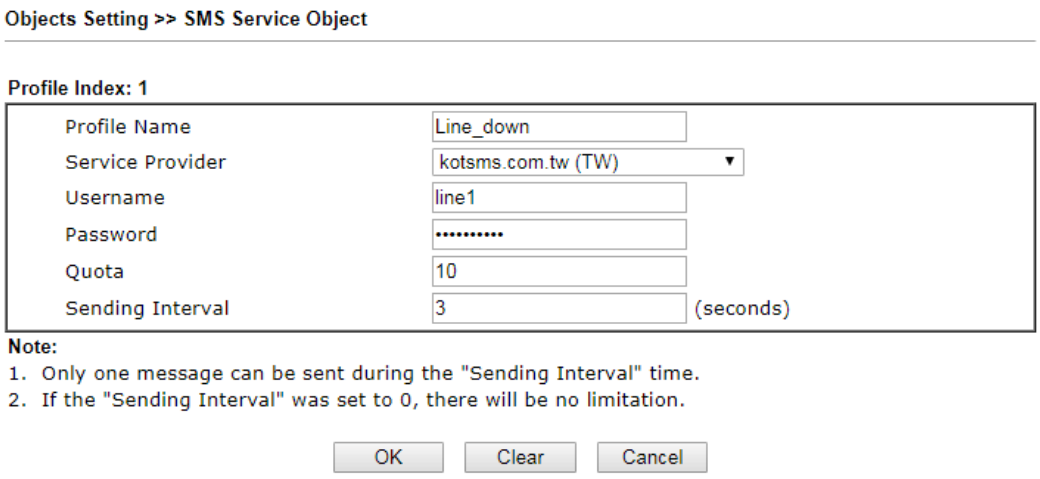


Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile Name	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.

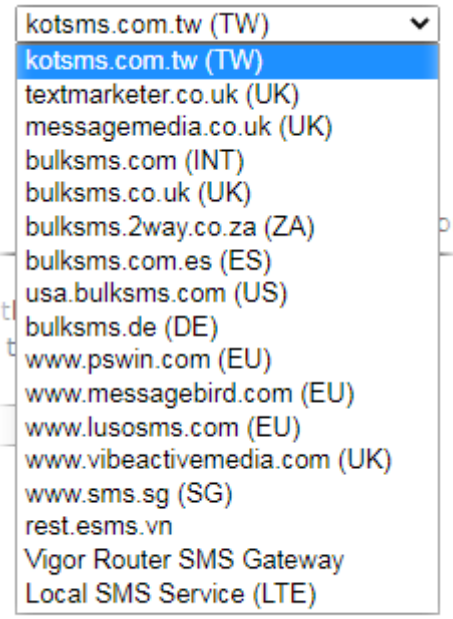
To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

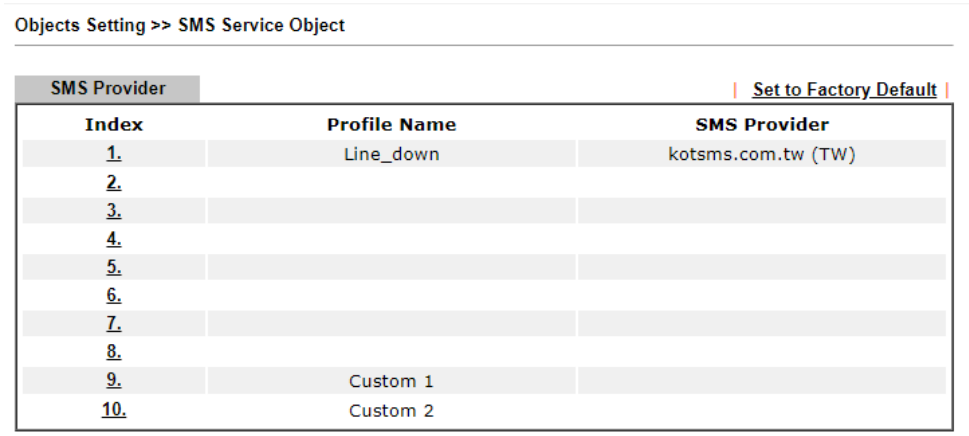


Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such SMS profile. The maximum length of the name you can set is 31 characters.

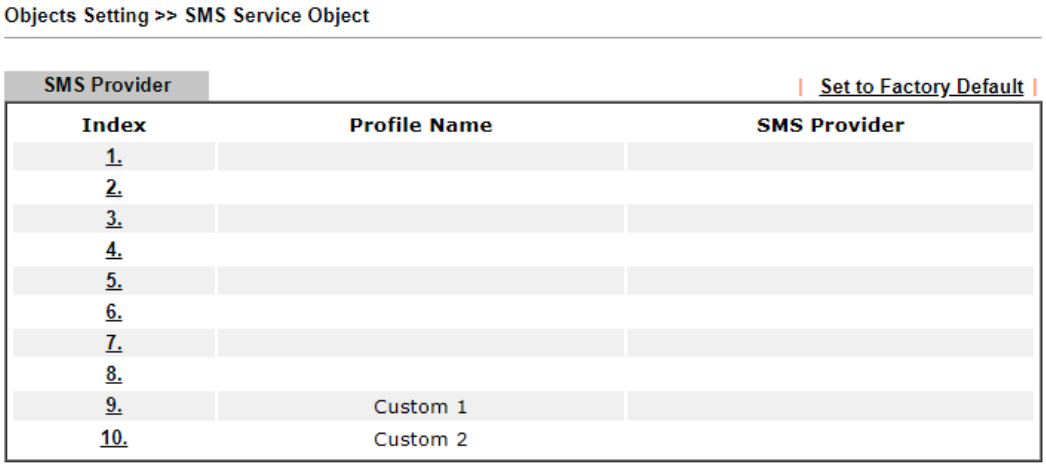
Service Provider	Use the drop down list to specify the service provider which offers SMS service. 
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Enter the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Sending Interval	To avoid quota being exhausted soon, type time interval for sending the SMS.

3. After finishing all the settings here, please click **OK** to save the configuration.

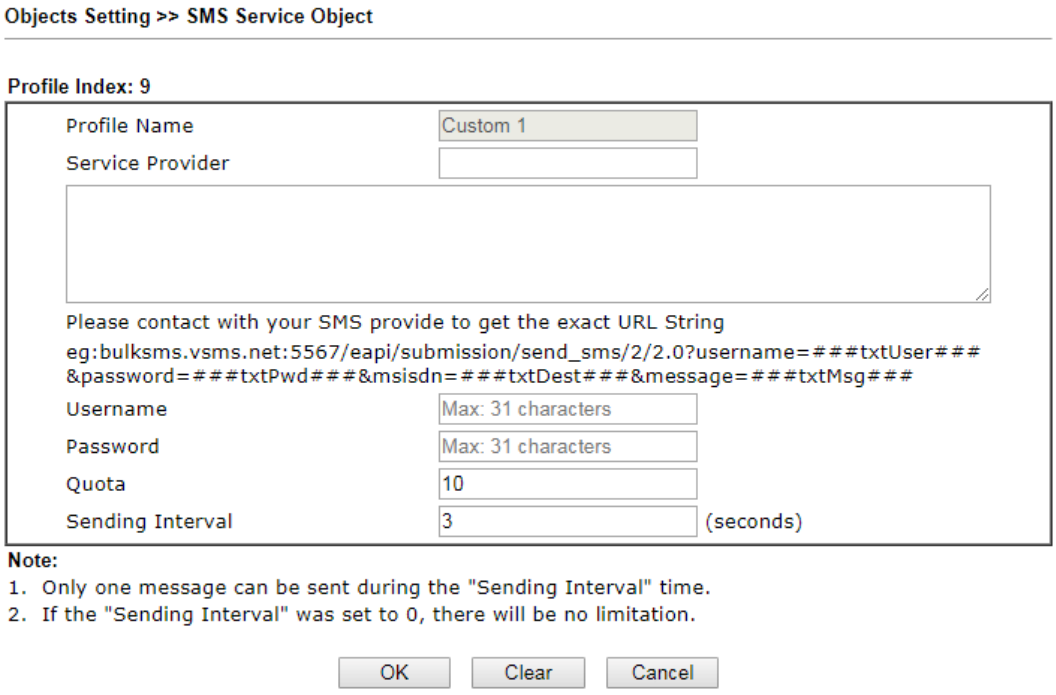


Customized SMS Service

Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.



You can click the number (e.g., #9) under Index column for configuration in details.



Available settings are explained as follows:

Item	Description
Profile Name	Display the name of this profile. It cannot be modified.
Service Provider	Enter the website of the service provider. Enter the URL string in the box under the filed of Service Provider. You have to contact your SMS provider to obtain the exact URL string.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31

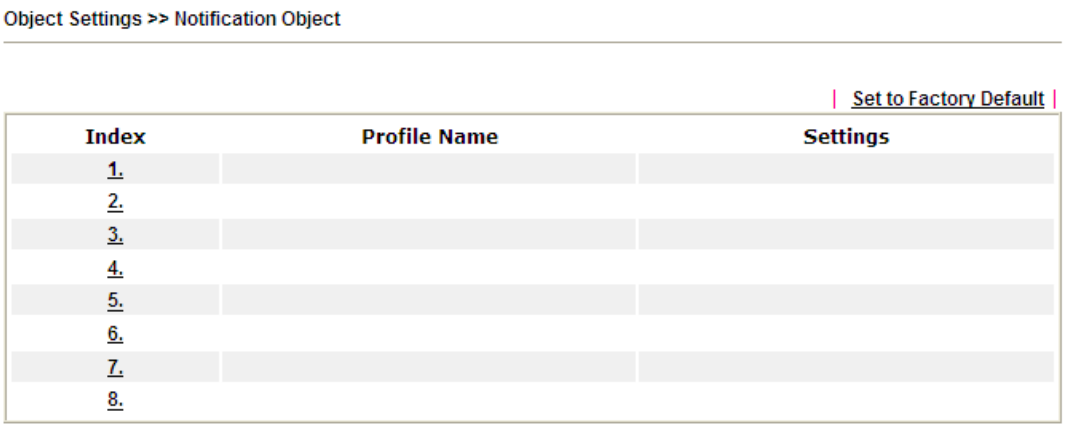
	characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Enter the total number of the messages that the router will send out.
Sending Interval	Enter the shortest time interval for the system to send SMS.

After finishing all the settings here, please click **OK** to save the configuration.

VII-1-11 Notification Object

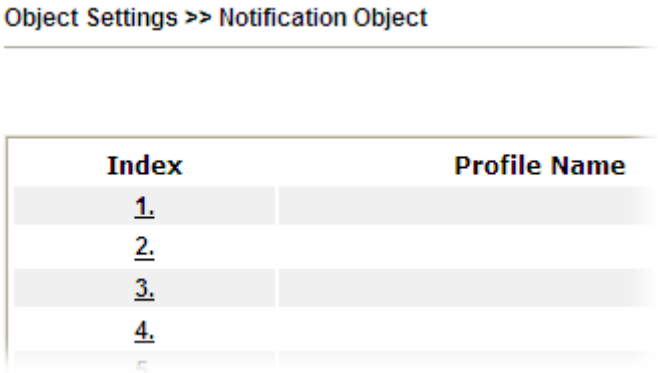
This page allows you to set ten profiles which will be applied in **Application>>SMS Alert Service**.

You can set an object with different monitoring situation.

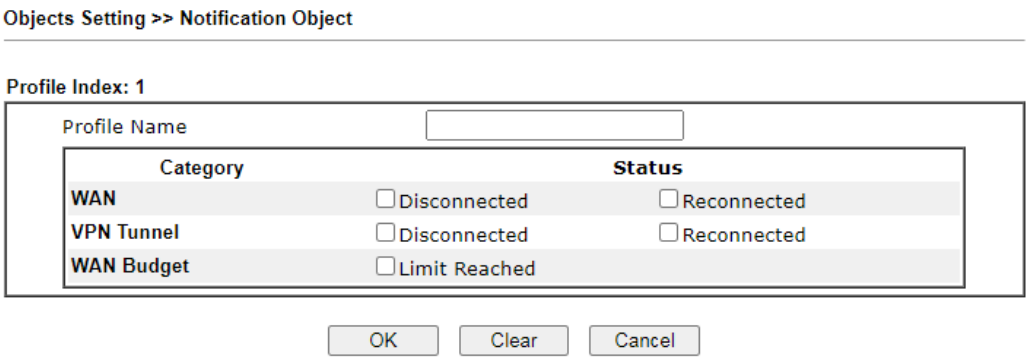


To set a new profile, please do the steps listed below:

1. Open **Object Setting>>Notification Object**, and click the number (e.g., #1) under Index column for configuration in details.



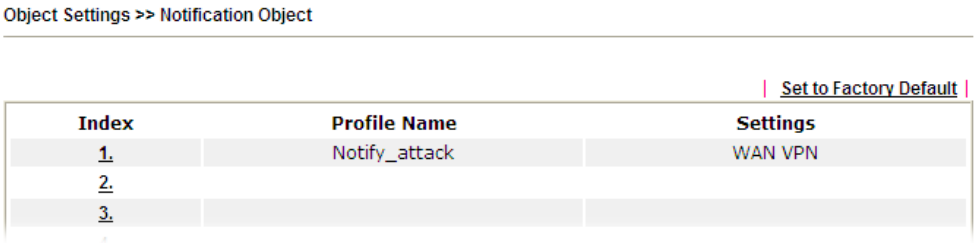
2. The configuration page will be shown as follows:



Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box to be monitored.

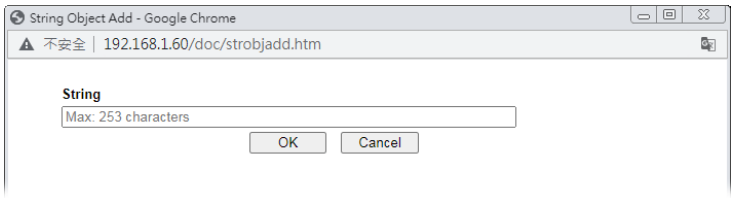
3. After finishing all the settings here, please click **OK** to save the configuration.



VII-1-12 String Object

This page allows you to set string profiles which will be applied in route policy (domain name selection for destination) and etc.

Available settings are explained as follows:

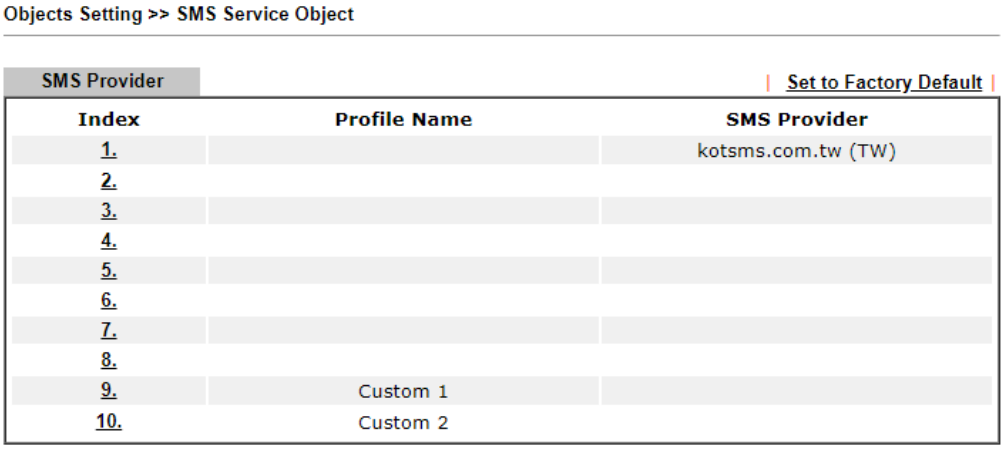
Item	Description
Add	Click it to open the following page for adding a new string object. 
Set to Factory Default	Click it to clear all of the settings in this page.
Index	Display the number link of the string profile.
String	Display the string defined.
Clear	Choose the string that you want to remove. Then click this check box to delete the selected string.

Application Notes

A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

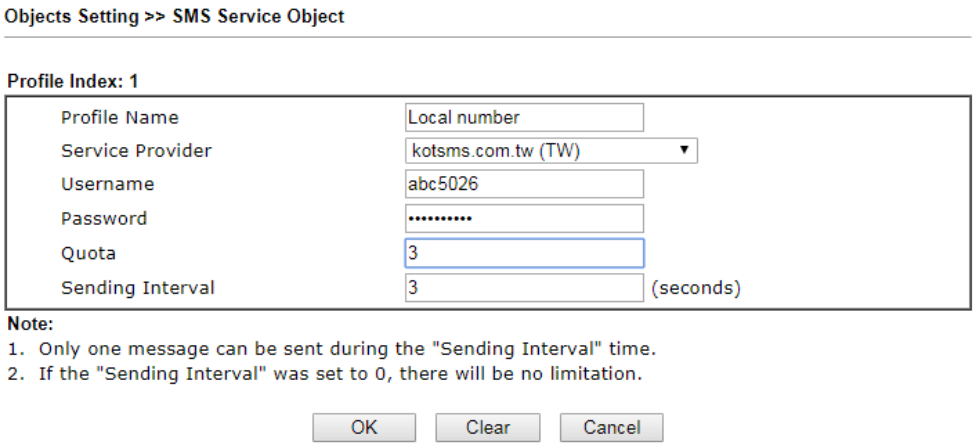
Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open **Object Settings>>SMS Server Object** to get the following page.

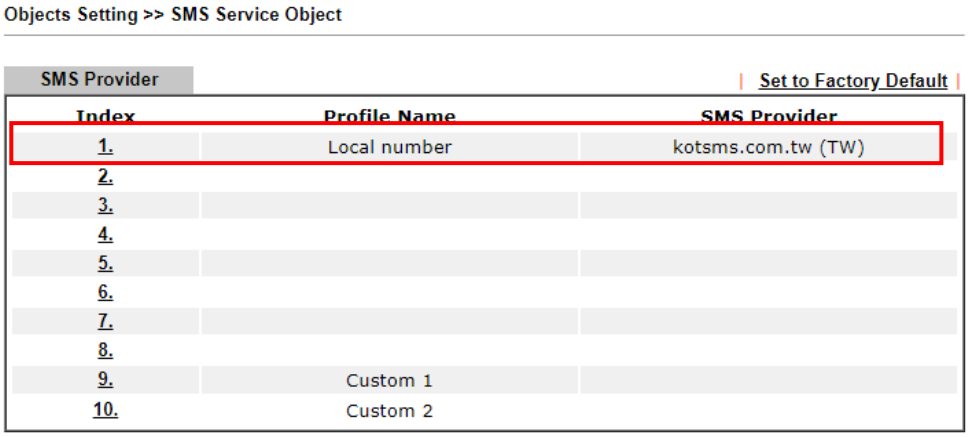


Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

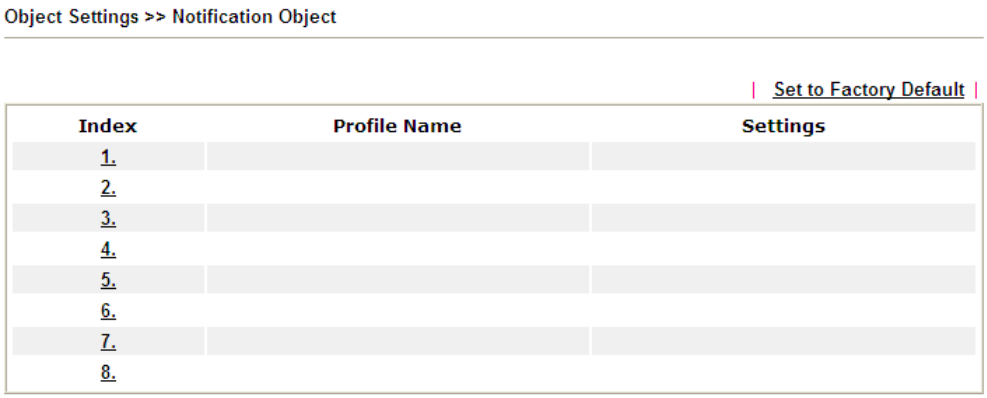
3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, Enter the username and password and set the quota that the router can send the message out.



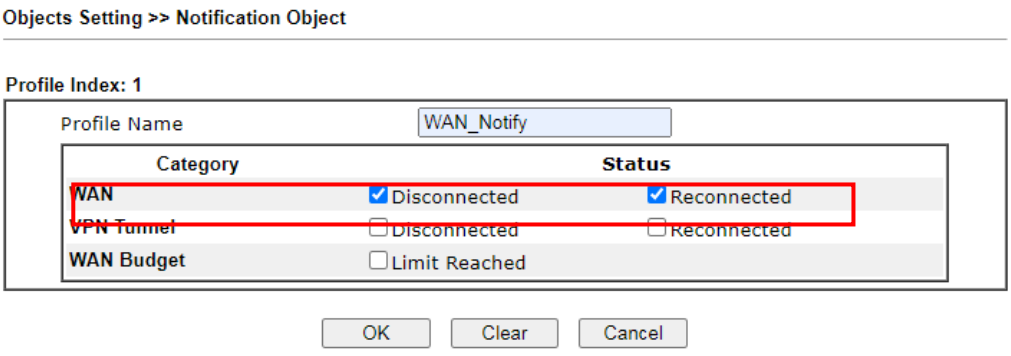
4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.



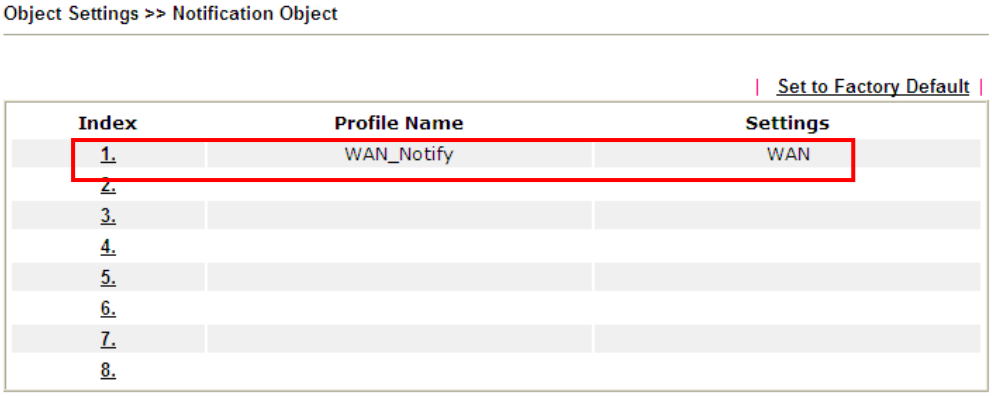
5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.



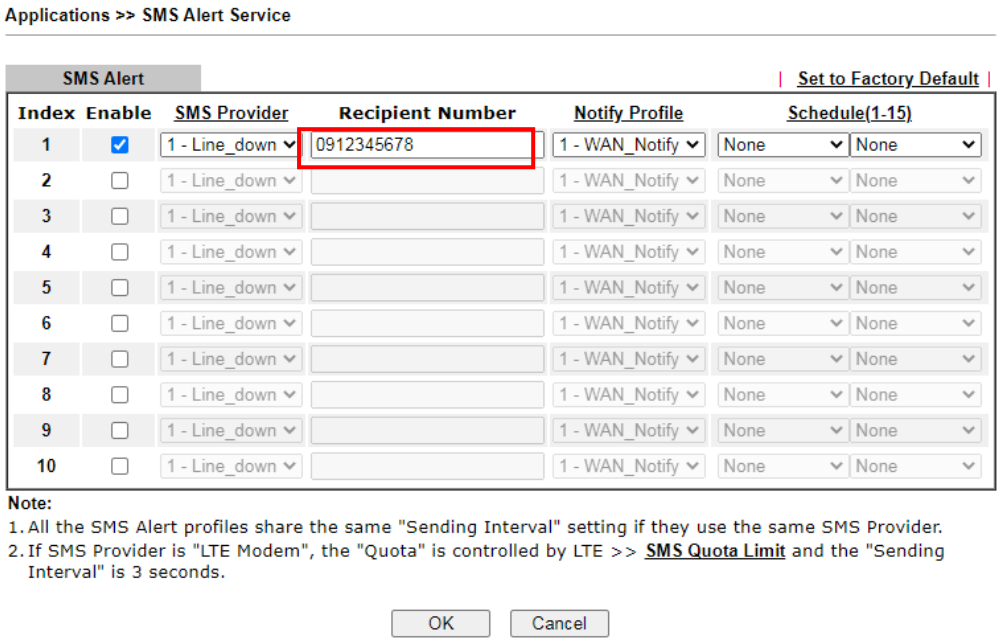
6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, Enter the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.



7. After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.



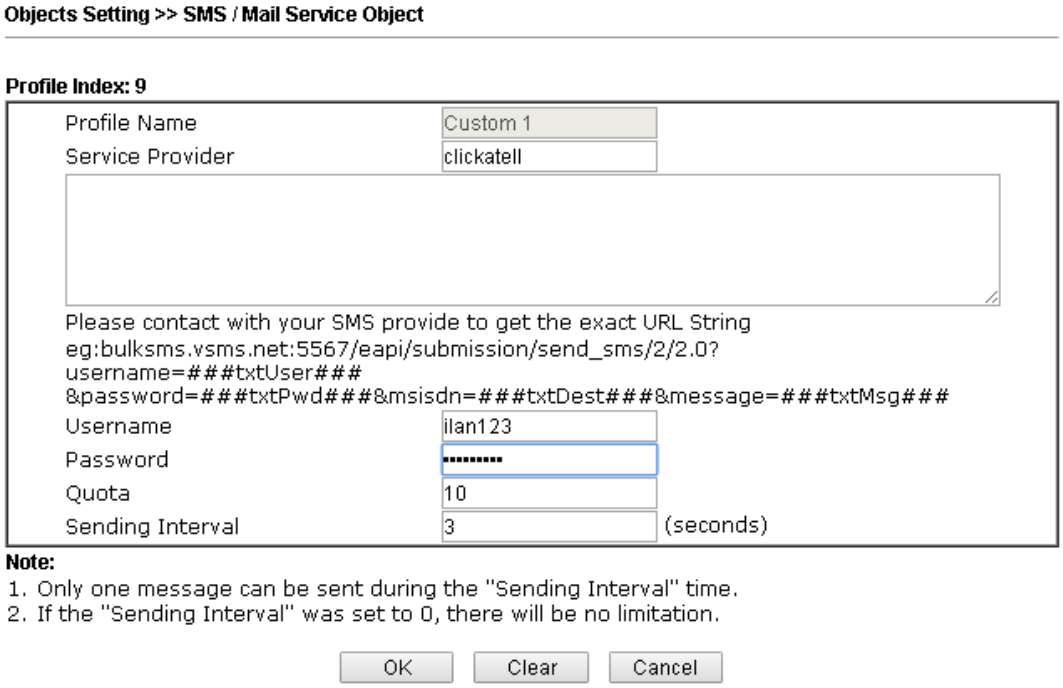
8. Now, open **Applications >> SMS Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, Enter the phone number in the field of Recipient Number (the one who will receive the SMS).



9. Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, Enter the URL string of the SMS provider and Enter the username and password. After clicking OK, the new added SMS provider will be added and will be available for you to specify for sending SMS out.



This page is left blank.

Part VIII Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration.

VIII-1 Diagnostics

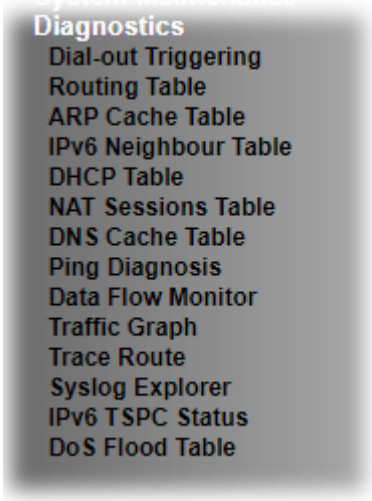
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

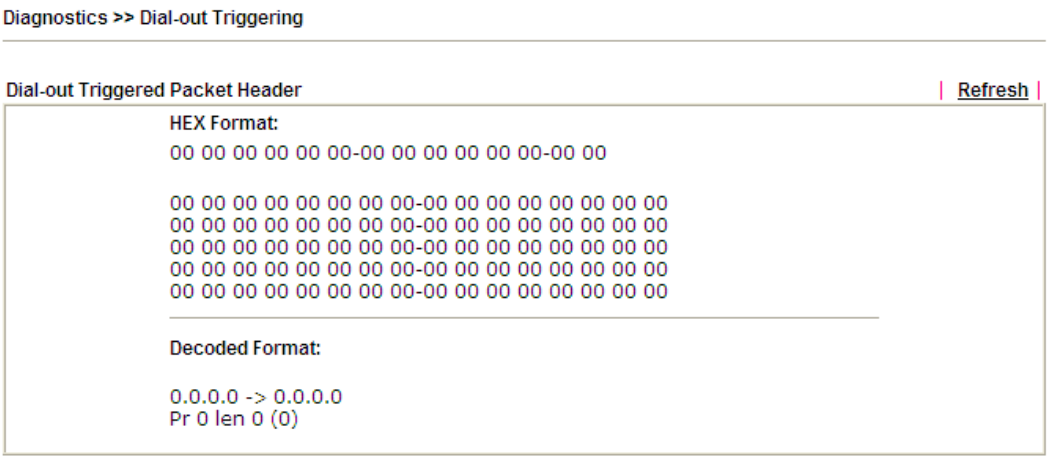
Web User Interface

Fisrt, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.



VIII-1-1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

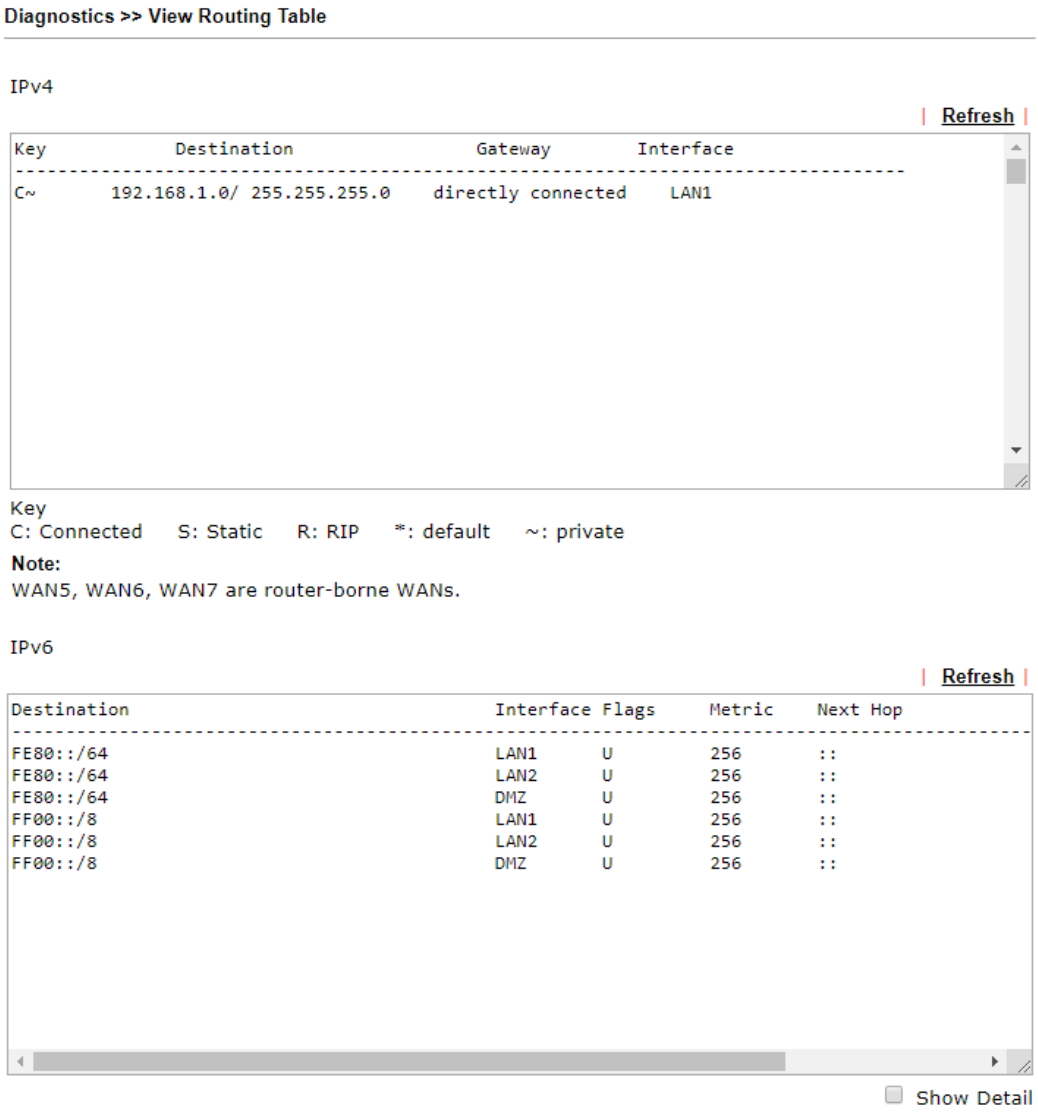


Available settings are explained as follows:

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

VIII-1-2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

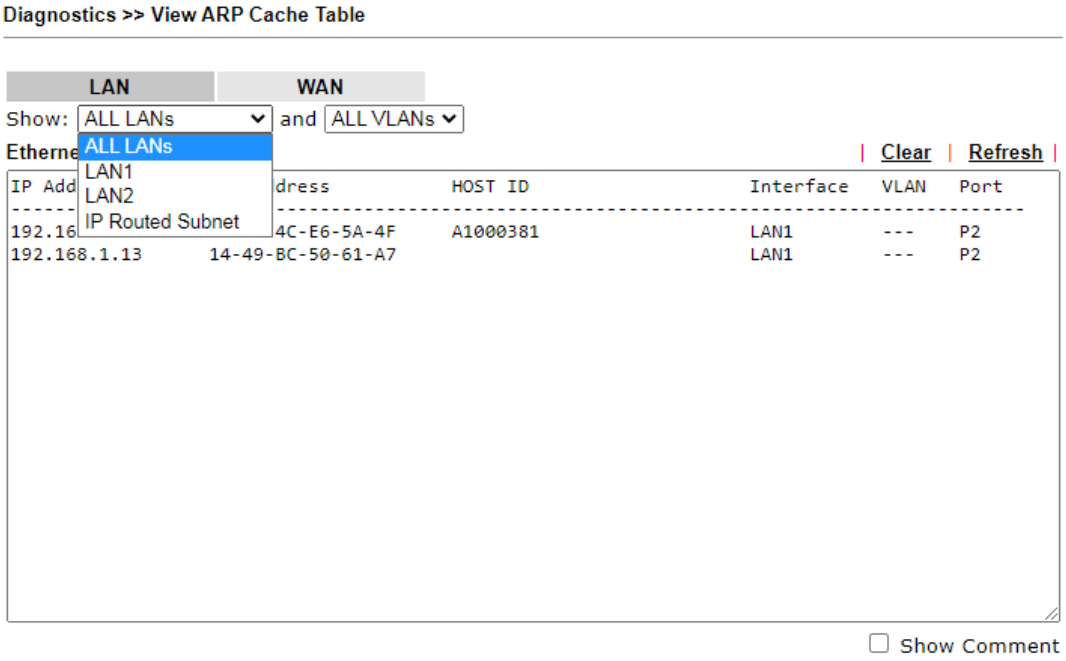


Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



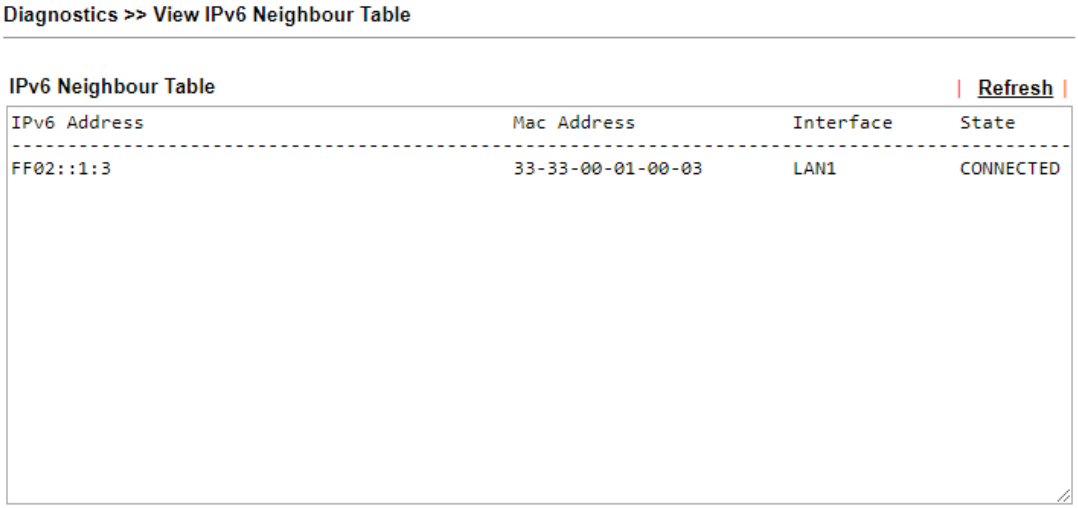
Available settings are explained as follows:

Item	Description
Show	Specify LAN and VLAN to display related information. In default, this page will display all of the information about LAN and VLAN.
Refresh	Click it to reload the page.

VIII-1-4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.



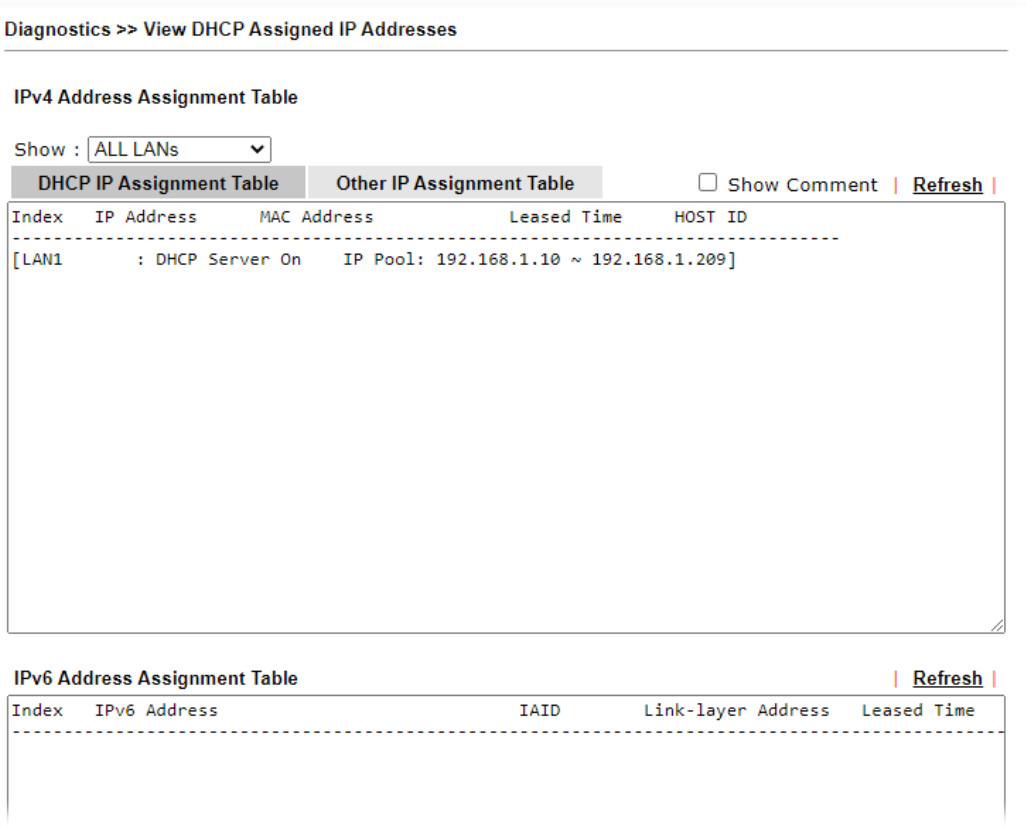
Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-5 DHCP Table

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

Click **Diagnostics** and click **DHCP Table** to open the web page.

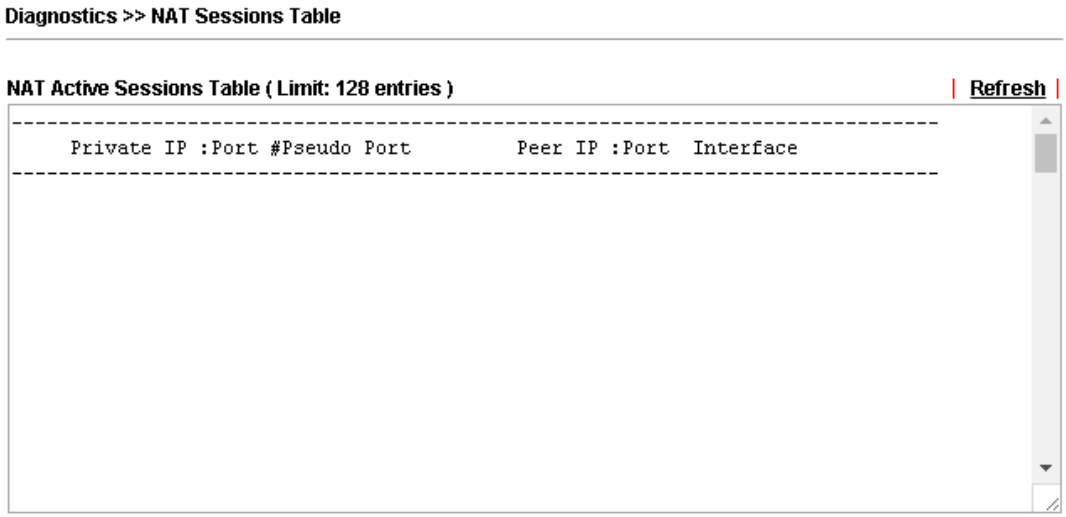


Available settings are explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

VIII-1-6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.



Available settings are explained as follows:

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

VIII-1-7 DNS Cache Table

Click **Diagnostics** and click **DNS Cache Table** to open the web page.

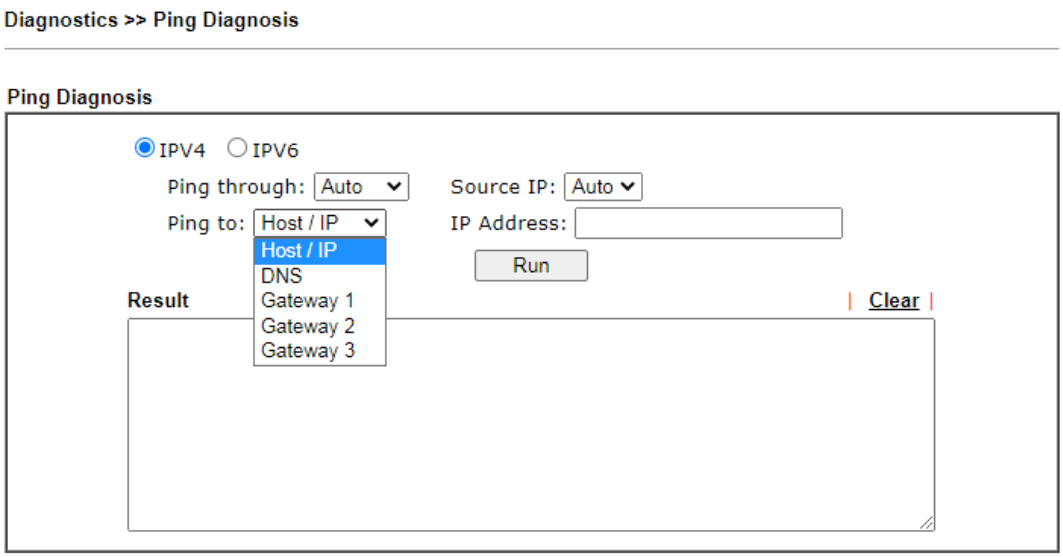
The record of domain Name and the mapping IP address for answering the DNS query from LAN will be stored on Vigor router's Cache temporarily and displayed on **Diagnostics >> DNS Cache Table**.

Available settings are explained as follows:

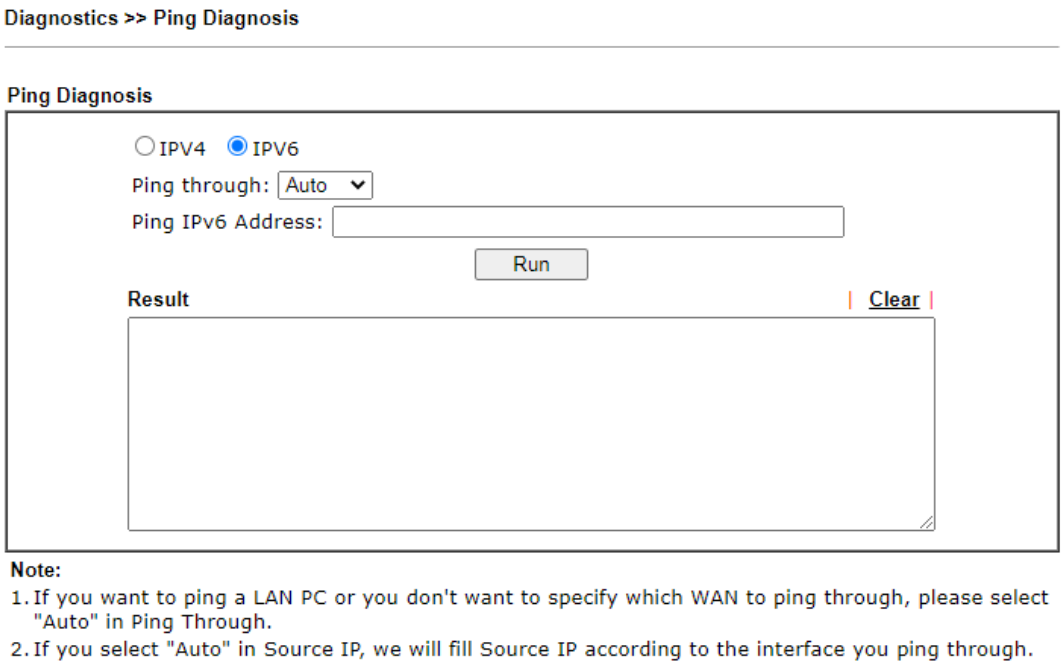
Item	Description
Clear	Click this link to remove the result on the window.
Refresh	Click it to reload the page.
When an entry's TTL is larger than….	Check the box the Enter the value of TTL (time to live) for each entry. Click **OK** to enable such function. It means when the TTL value of each DNS query reaches the threshold of the value specified here, the corresponding record will be deleted from router's Cache automatically.

VIII-1-8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to open the web page.



or



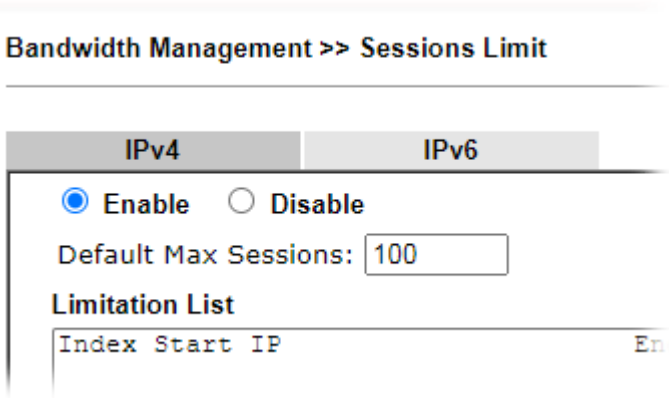
Available settings are explained as follows:

Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose **Auto** to be determined by the router automatically.

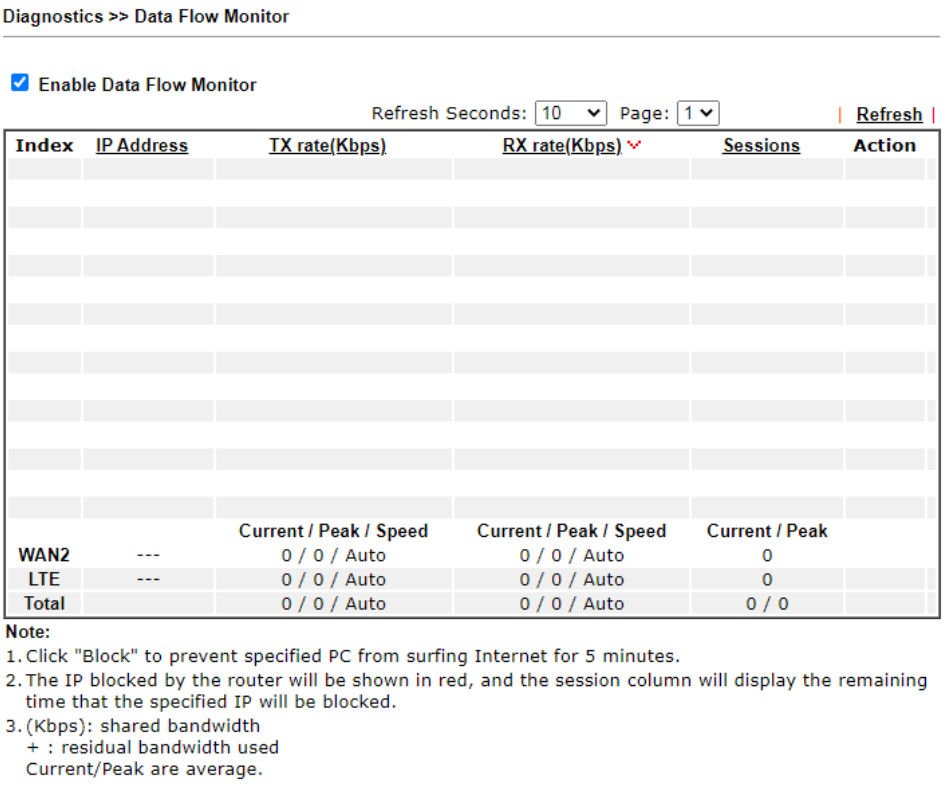
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Enter the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

VIII-1-9 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoking Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.



Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.

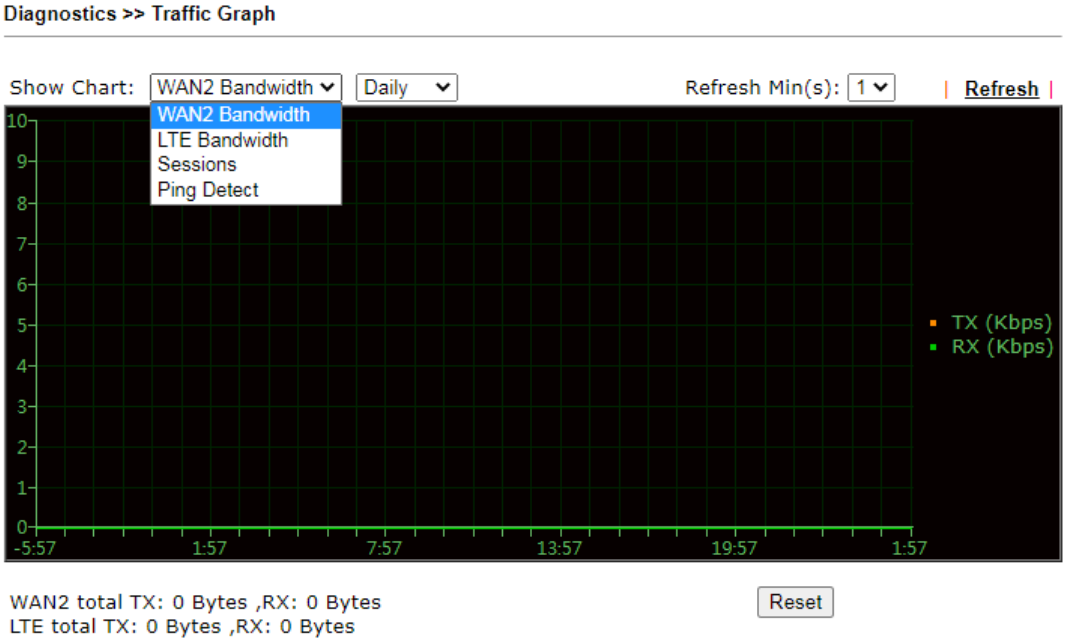


Available settings are explained as follows:

Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	**Block** - can prevent specified PC accessing into Internet within 5 minutes. **Unblock** –The device with the IP address will be blocked for five minutes. The remaining time will be shown on the session column. Click it to cancel the IP address blocking.
Current /Peak/Speed	**Current** means current transmission rate and receiving rate for WAN interface. **Peak** means the highest peak value detected by the router in data transmission. **Speed** means line speed specified in **WAN>>General Setup**. If you do not specify any rate at that page, here will display **Auto** for instead.

VIII-1-10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN2/LTE Bandwidth, Sessions, Ping Detect, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.

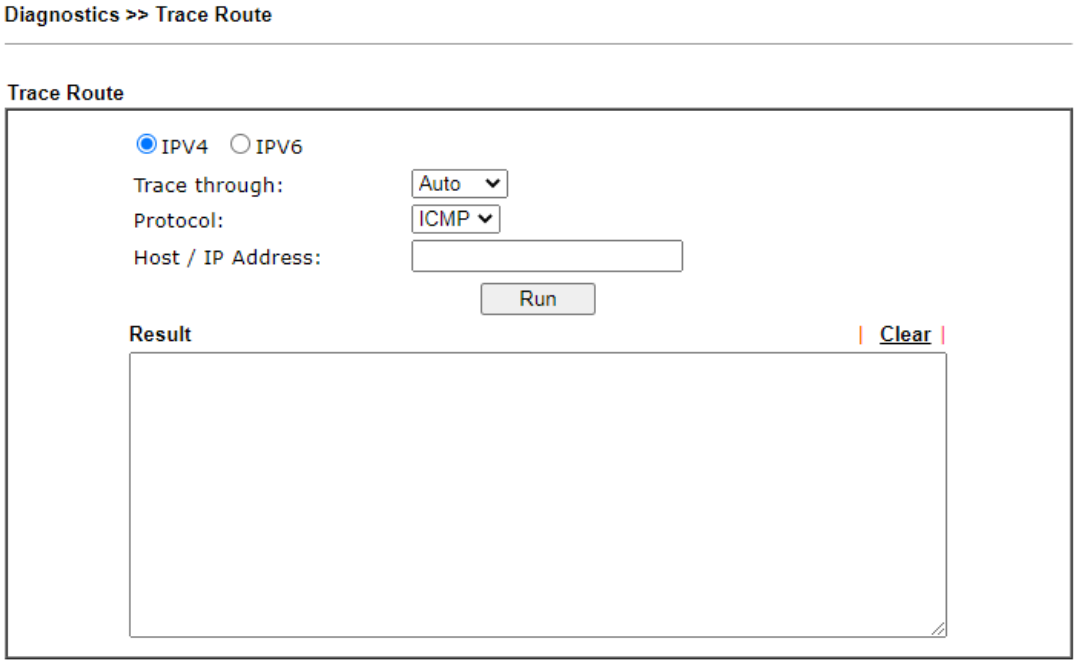


The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN2/LTE Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

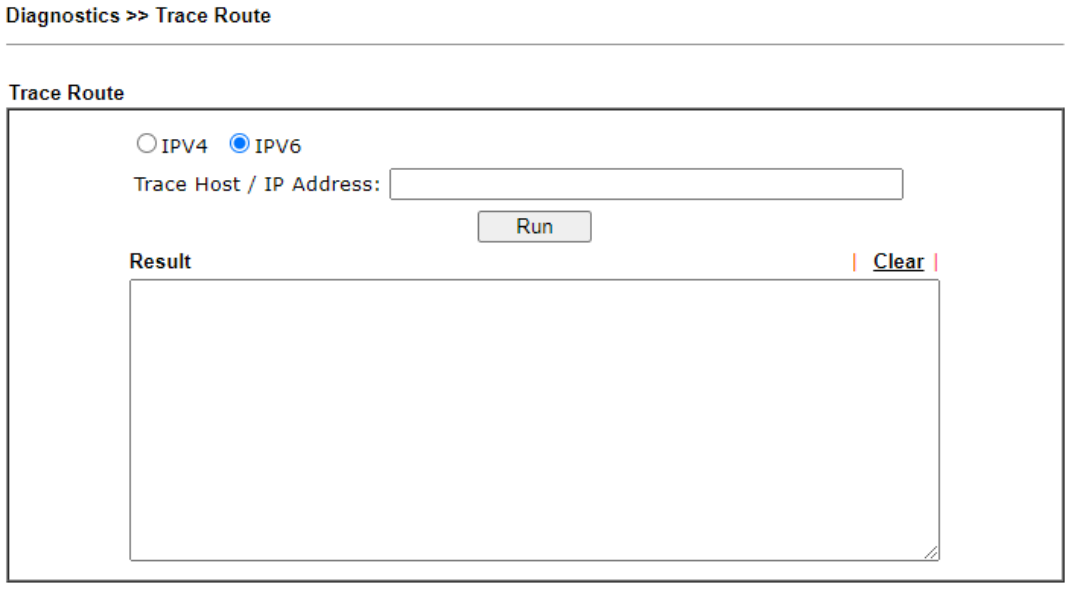
For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

VIII-1-11 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply Enter the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.



or



Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Trace through	Use the drop down list to choose the interface that you want to ping through.

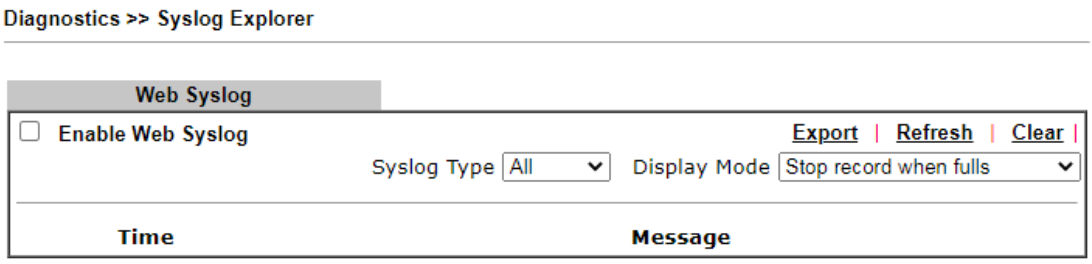
Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

VIII-1-12 Syslog Explorer

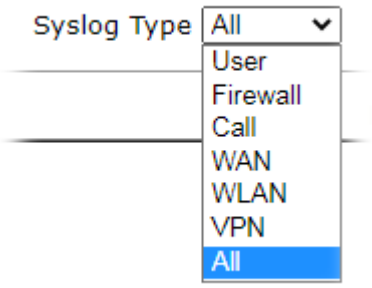
Such page provides real-time syslog and displays the information on the screen.

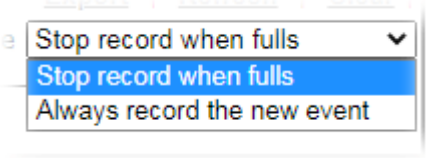
For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog,** specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.



Available settings are explained as follows:

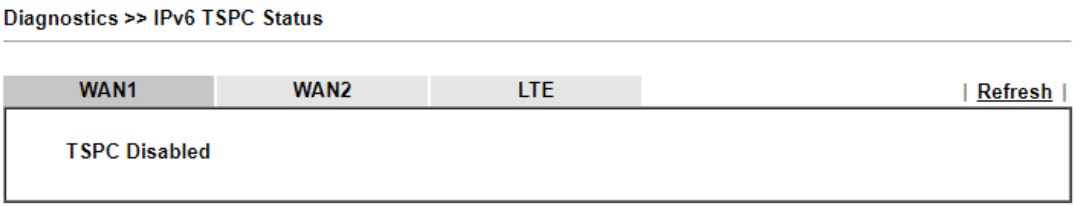
Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. 
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose.

	 **Stop record when fulls -** When the capacity of syslog is full, the system will stop recording. **Always record the new event -** only the newest events will be recorded by the system.
Time	Display the time of the event occurred.
Message	Display the information for each event.

VIII-1-13 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.



Available settings are explained as follows:

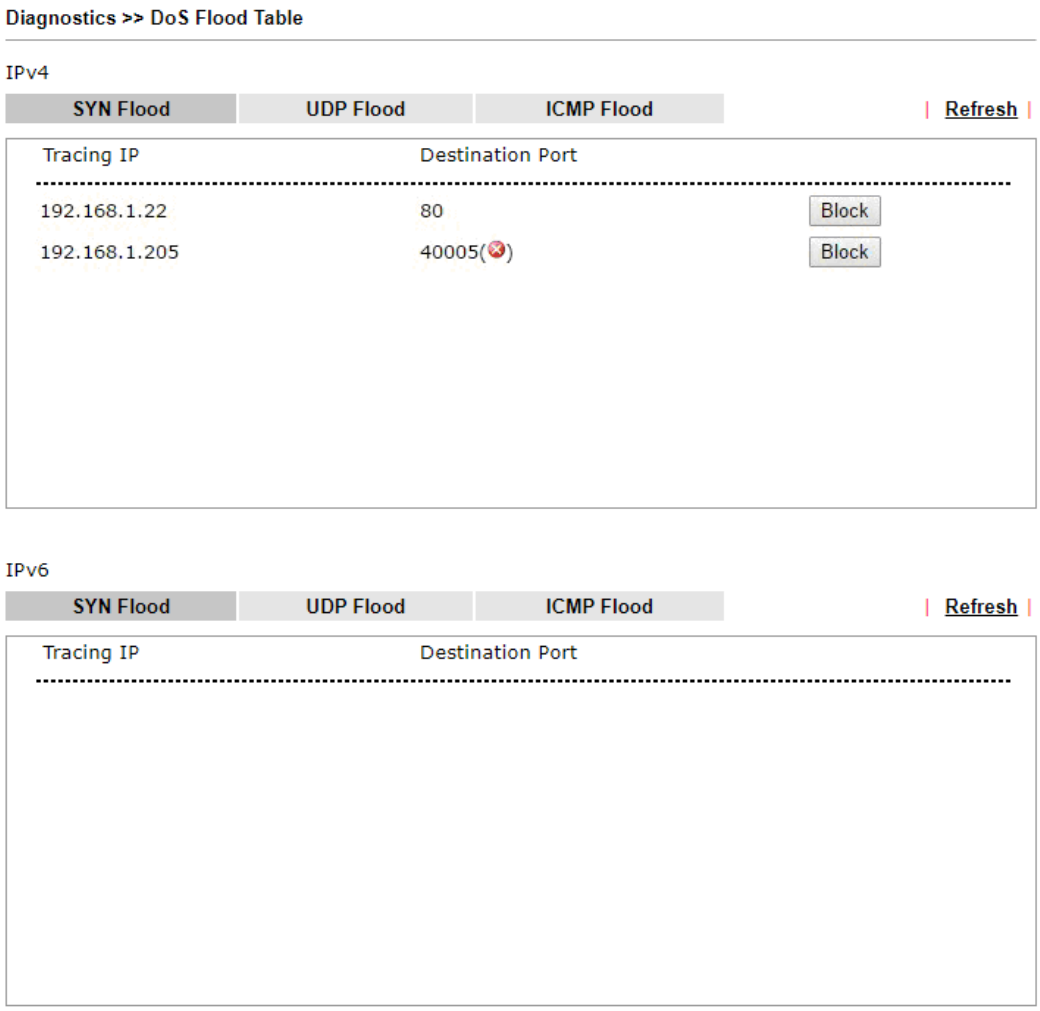
Item	Description
Refresh	Click this link to refresh this page manually.

VIII-1-14 DoS Flood Table

This page can display content of IP connection detected by DoS Flooding Defense mechanism. It is useful and convenient for network engineers (e.g., MIS engineer) to inspect the network environment to find out if there is any abnormal connection.

Information of IP traced and destination port used for SYN Flood, UDP Flood and ICMP Flood attacks will be detected and shown respectively on different pages.

Moreover, IP address detected and suspected to attack the network system can be blocked shortly by clicking the **Block** button shown on pages of SYN Flood, UDP Flood and ICMP Flood.



Info

The icon - ( ) - means there is something wrong (e.g., attacking the system) with that IP address.

VIII-2 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**I-2 Hardware Installation"** for details.
2. Turn on the router. Make sure the **Activity LED** blink once per second and the correspondent **LAN LED** is 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.

VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not

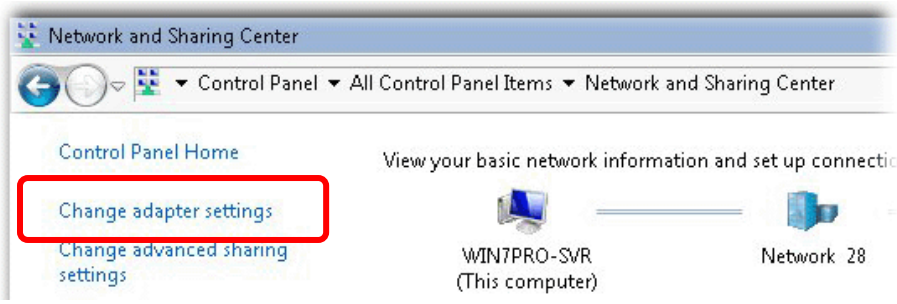
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

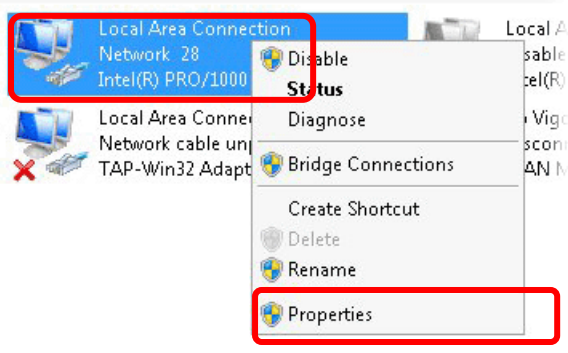
Info	The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

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

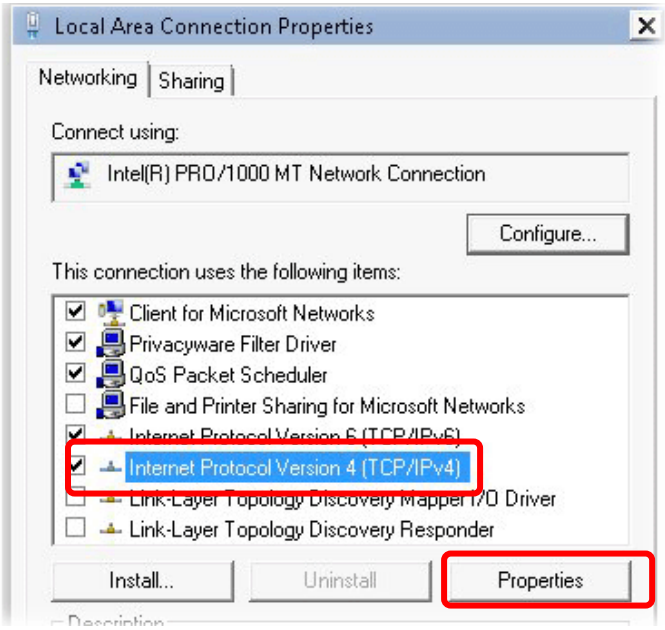
2. In the following window, click **Change adapter settings**.



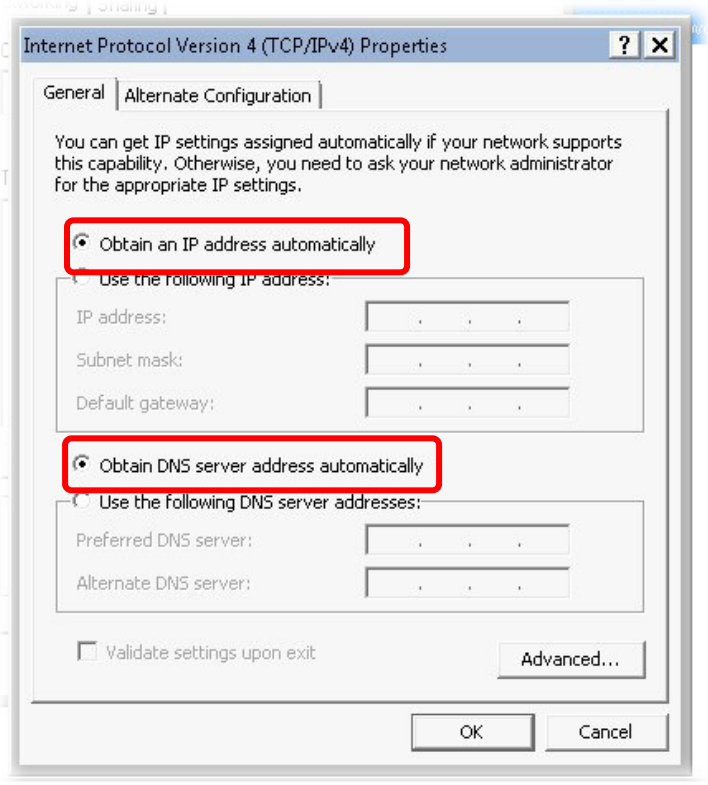
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

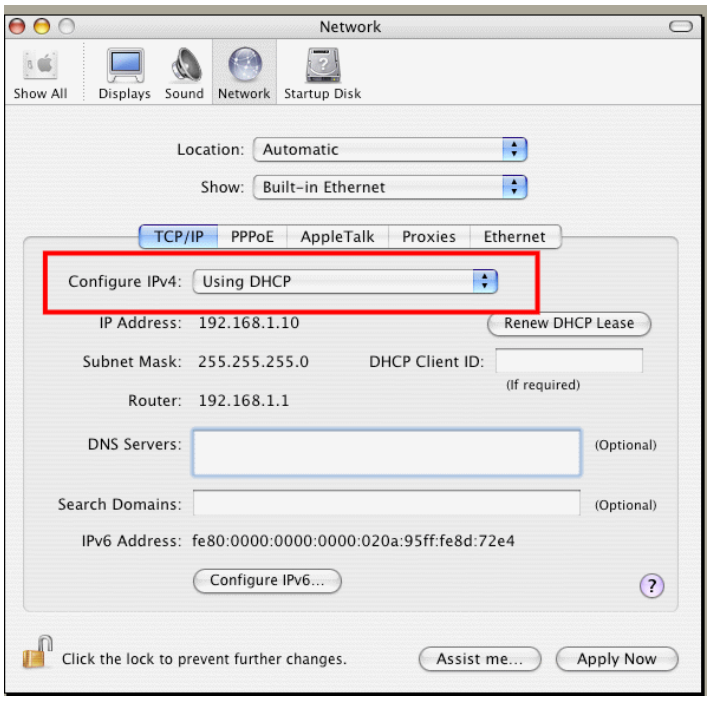


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



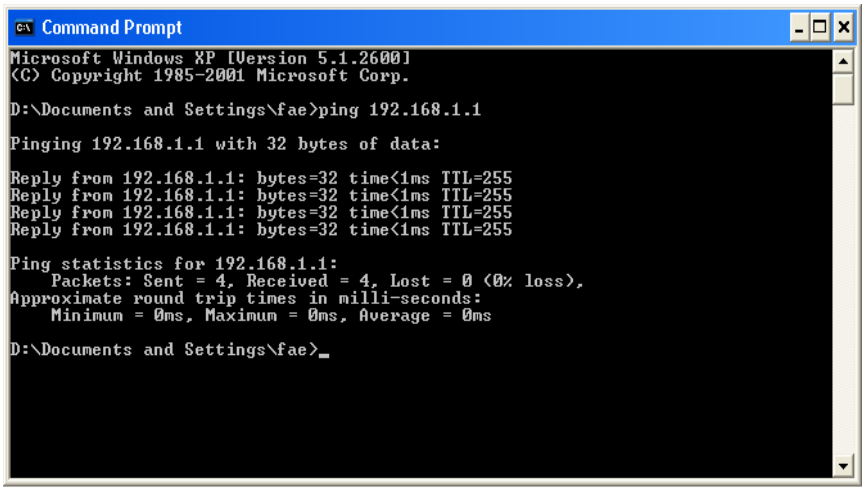
VIII-4 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **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 follow the steps below to ping the router correctly.

For Windows

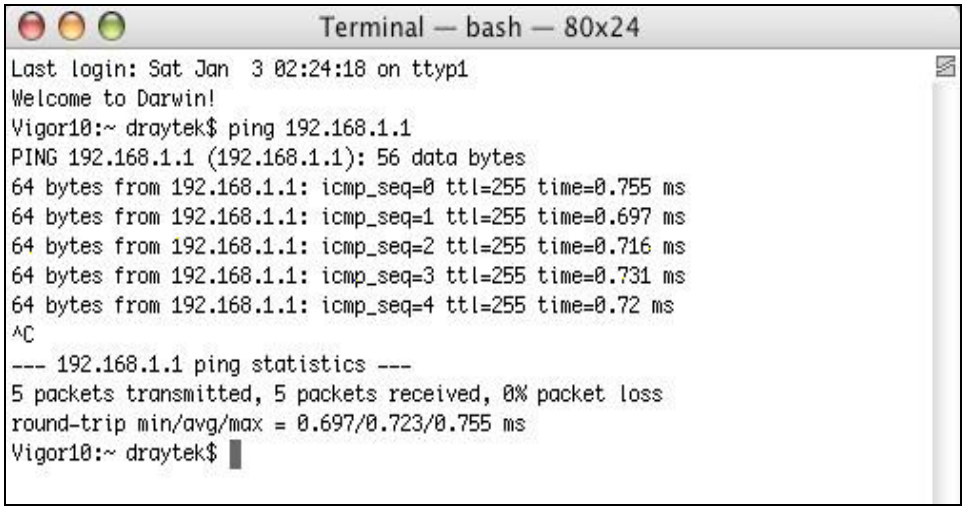
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd**. The DOS command dialog will appear.



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.

For Mac OS (Terminal)

1. Double click on the current used MacOs 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$

VIII-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section 1-2) are correct or not. If the LEDs are off, please:

- Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).
- Next, check if the LEDs on Vigor router are on or not.
- If not, please install an additional switch for connecting both Vigor router and the modem offered by ISP. Then, check if the LEDs on Vigor router are on or not.
- If the problem of LEDs cannot be solved by the above measures, please contact with the nearest reseller, or send an e-mail to DrayTek FAE for technical support.
- Check if the settings offered by ISP are configured well or not.

When the LEDs are on and correct, yet the WAN connection still cannot be up, please:

- Open **WAN >> Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1 to review the settings that you configured previously.

VIII-6 Backing to Factory Default Setting If Necessary

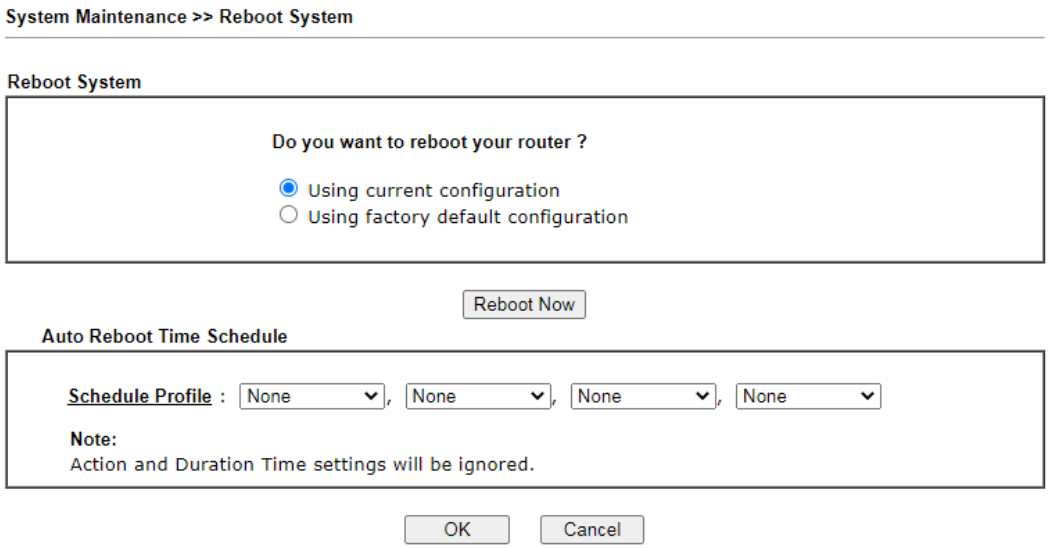
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

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

Software Reset

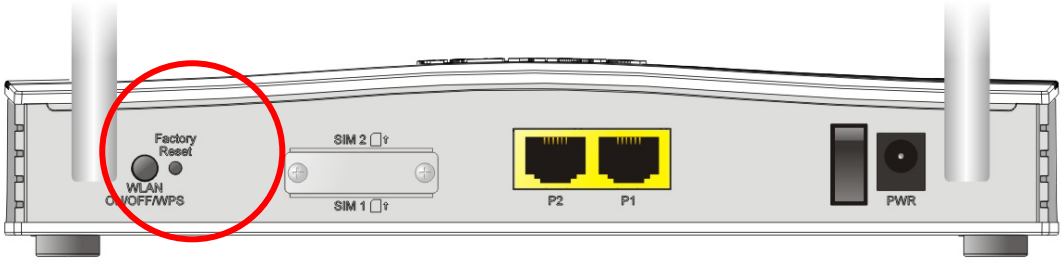
You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.



Hardware Reset

While the router is running (ACT LED blinking), 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 router will restart with the default configuration.



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

VIII-7 Contacting DrayTek

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

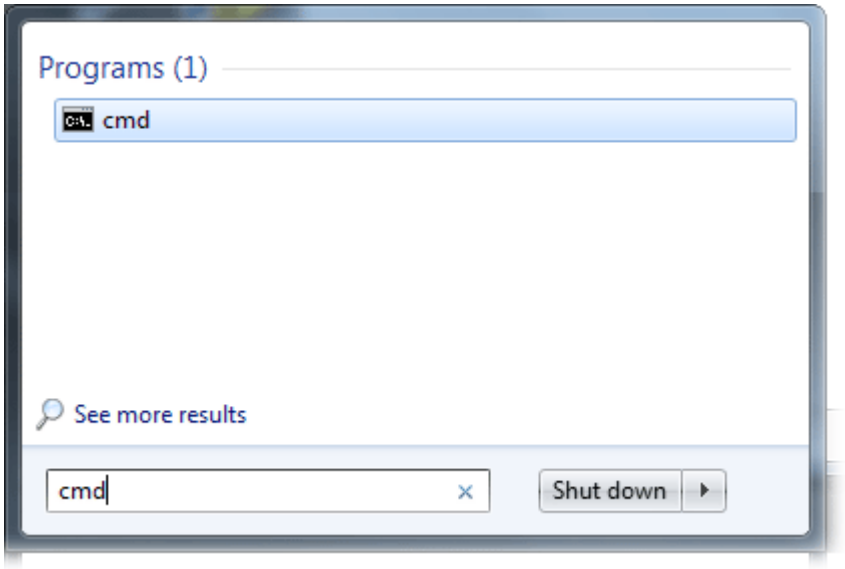
Part IX Telnet Commands

Accessing Telnet of VigorLTE 200

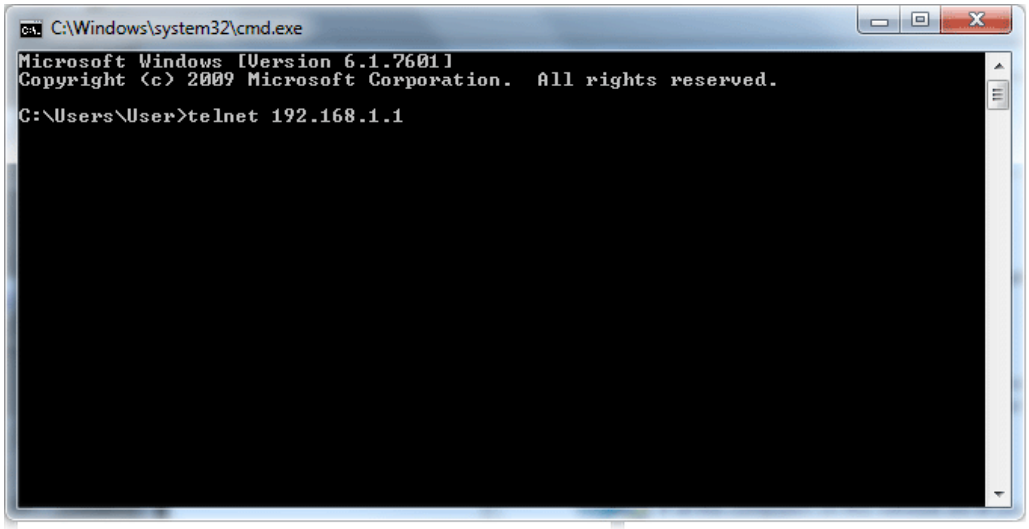
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.

Info	For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under **Control Panel>>Programs**.

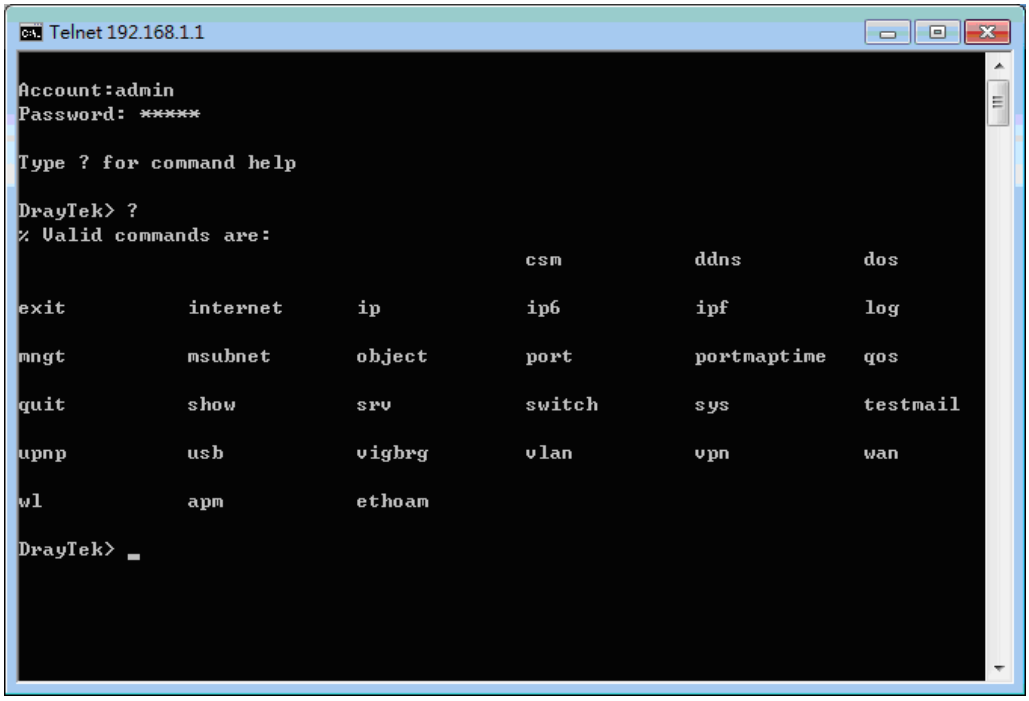
Type **cmd** and press Enter. The Telnet terminal will be open later.



In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, type admin/admin for Account/Password. Then, type **?**. You will see a list of valid/common commands depending on the router that your use.



Telnet Command: csm appe prof

Commands under CSM allow you to set CSM profile to define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application.

"csm appe prof " is used to configure the APP Enforcement Profile name. Such profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.

Syntax

csm appe prof -i <*INDEX***>** <*-v*>

csm appe prof -i <*INDEX***>** *-n <NAME>*

csm appe prof -i <*INDEX***>** <*setdefault*>

Syntax Description

Parameter	Description
<*INDEX*>	It means to specify the index number of CSM profile. INDEX= 1~32.
- v	It means to view the configuration of the CSM profile.
- n <NAME>	It means to set a name for the CSM profile. <NAME>: Specify a name for the CSM profile, less then 15 characters.
setdefault	Reset to default settings.

Example

```
> csm appe prof -i 1 -n game
The name of APPE Profile 1 was setted.

> csm appe prof -i 1 setdefault
APPE Profile 1 was reseted.
```

Telnet Command: csm appe set

It is used to configure group settings for IM/P2P/Protocol and Others in APP Enforcement Profile.

csm appe set *-i INDEX -v <GROUP>*

csm appe set *-i INDEX -e <AP_IDX>*

csm appe set *-i INDEX -d <AP_IDX>*

Syntax Description

Parameter	Description
<*INDEX*>	It means to specify the index number of CSM profile. INDEX= 1~32.
- v <GROUP>	View the IM/P2P/Protocol or Others configuration of the CSM profile. <GROUP>= IM, P2P, Protocol,or Others.
-e	Enable to block specific application.
-d	Disable to block specific application.

<AP_IDX>	Specify the index number of the application here. AP_IDX=1~119

Example

```
> csm appe set -i 1 -e 1
Profile 1 - : AIM is enabled.
> csm appe set -i 32 -e 90
Profile 32 - : PPTV is enabled.
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.

csm appe show <*-a/-i/-p/-t/-m*>

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show -t

         Type    Index                Name        Version   Advance
 Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
-------------------------------------------------------------
      PROTOCOL       52                 DB2
      PROTOCOL       53                 DNS
      PROTOCOL       54                 FTP
      PROTOCOL       55                HTTP            1.1
      PROTOCOL       56                IMAP            4.1
      PROTOCOL       57         IMAP STARTTLS            4.1
      PROTOCOL       58                 IRC          2.4.0            ……
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/P2P/Protocol/Other applications.

csm appe config -v <*INDEX*><*-i/-p/-t/-m*>

Syntax Description

Parameter	Description
<INDEX>	It means to specify the index number of CSM profile. INDEX= 1~32.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.

-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
> csm appe config -v 1 -m

    Group         Type    Index               Name        Enable     A
vance Enable
 Advance abbreviation: Message, File Transfer, Game, Conference, and Other
 Advance abbreviation: : M, F, G, C, and O
-----------------------------------------------------------------------
   OTHERS       TUNNEL       75            DNSCrypt           Disable
   OTHERS       TUNNEL       76            DynaPass           Disable
   OTHERS       TUNNEL       77               FreeU           Disable
   OTHERS       TUNNEL       78          HTTP Proxy           Disable
   OTHERS       TUNNEL       79         HTTP Tunnel           Disable
   OTHERS       TUNNEL       80            Hamachi           Disable
   OTHERS       TUNNEL       81       Hotspot Shield           Disable
   OTHERS       TUNNEL       82           MS Teredo           Disable
   OTHERS       TUNNEL       83              PGPNet           Disable
   OTHERS       TUNNEL       84         Ping Tunnel           Disable
.
.
.
-----------------------------------------------------------------------
Total 66 APPs
>
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

Syntax

csm ucf show
csm ucf setdefault
csm ucf msg *MSG*
csm ucf obj *<INDEX> -n <PROFILE_NAME> -l <P/B/A> <uac>< wf>*
csm ucf obj *<INDEX> -n <PROFILE_NAME>*
csm ucf obj <*INDEX> -p <VALUE>*
csm ucf obj *<INDEX> <-l P/B/A>*
csm ucf obj <*INDEX> uac*
csm ucf obj <*INDEX> wf*

Syntax Description

Parameter	Description
show	It means to display all of the profiles.
setdefault	It means to return to default settings for all of the profile.
msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	It means to specify the object for the profile.
<INDEX>	It means to specify the index number of CSM profile. INDEX= 1~8.
-n <PROFILE_NAME>	It means to set the profile name. PROFILE_NAME: Enter the name of the profile (less than 16

	characters).
-p <VALUE>	Set the priority (defined by the number specified in VALUE) for the profile. Number 0 to 3 represent different conditions. VALUE=0: It means Bundle: Pass. VALUE=1: It means Bundle: Block. VALUE=2: It means Either: URL Access Control First. VALUE=3: It means Either: Web Feature First.
-l <P/B/A>	It means the log type of the profile. They are: P: Pass, B: Block, A: All
uac	It means to set URL Access Control part.
wf	It means to set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1   Profile Name:[game]
```

Telnet Command: csm ucf obj INDEX uac

It means to configure the settings regarding to URL Access Control (uac).

Syntax

csm ucf obj *<INDEX> uac -v*
csm ucf obj *<INDEX> uac -e*
csm ucf obj *<INDEX> uac -d*
csm ucf obj *<INDEX> uac -a <P/B>*
csm ucf obj *<INDEX> uac -i <E/D>*
csm ucf obj *<INDEX> uac -o <KEY_WORD_Object_Index>*
csm ucf obj *<INDEX> uac -g <KEY_WORD_Group_Index>*

Syntax Description

Parameter	Description
<INDEX>	It means to specify the index number of CSM profile. INDEX= 1~8.
-v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the function of URL Access Control.
-d	It means to disable the function of URL Access Control.
-a <P/B>	Set the action of specific application, P or B. B: Block. The web access meets the URL Access Control will be blocked. P: Pass. The web access meets the URL Access Control will be passed.
-i <E/D>	Prevent the web access from any IP address. E: Enable the function. The Internet access from any IP address will be blocked.

	D: Disable the function.
-o <KEY_WORD_Object_Index>	Set the keyword object. KEY_WORD_Object_Index: Specify the index number of the object profile.
-g <KEY_WORD_Group_Index>	Set the keyword group. KEY_WORD_Group_Index: Specify the index number of the group profile.

Example

```
> csm ucf obj 1 uac -i E
Log:[none]
Priority Select : [Bundle : Pass]
------------------------------------------------
URL Access Control
[ ]Enable URL Access Control   Action:[pass]
[v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------
> csm ucf obj 1 uac -a B
Log:[none]
Priority Select : [Bundle : Pass]
------------------------------------------------
URL Access Control
[ ]Enable URL Access Control   Action:[block]
[v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------
```

Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

Syntax

csm ucf obj <*INDEX*> *wf -v*
csm ucf obj <*INDEX*> *wf -e*
csm ucf obj <*INDEX*> *wf -d*
csm ucf obj <*INDEX*> *wf -a <P/B>*
csm ucf obj <*INDEX*> *wf -s <WEB_FEATURE>*
csm ucf obj <*INDEX*> *wf -u <WEB_FEATURE>*
csm ucf obj <*INDEX*> *wf -f <File_Extension_Object_index>*

Syntax Description

Parameter	Description
<*INDEX*>	It means to specify the index number of CSM profile. INDEX= 1~8.
-v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the restriction of web feature.
-d	It means to disable the restriction of web feature.
-a <P/B>	Set the action of web feature, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
-s <WEB_FEATURE>	It means to enable the the Web Feature configuration. Features available for configuration are: <WEB_FEATURE>=c: Cookie <WEB_FEATURE>=p: Proxy <WEB_FEATURE>=u: Upload
-u <WEB_FEATURE>	It means to cancel the web feature configuration.
-f <File_Extension_Object_index>	It means to set the file extension object index number. File_Extension_Object_index=1 to 8

Example

```
> csm ucf obj 1 wf -s c
-----------------------------------------------
Web Feature
[ ]Enable Restrict Web Feature   Action:[pass]

File Extension Object Index : [0] Profile Name : []

[V] Cookie [ ] Proxy [ ] Upload
```

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

Syntax

csm wcf show
csm wcf look
csm wcf cache
csm wcf server WCF_SERVER
csm wcf msg MSG
csm wcf setdefault
csm wcf obj *<INDEX> -v*
csm wcf obj *<INDEX> -a <P/B>*
csm wcf obj *<INDEX> -n <PROFILE_NAME>*
csm wcf obj *<INDEX> -l <N/P/B/A>*
csm wcf obj *<INDEX> -o <KEY_WORD Object Index>*
csm wcf obj *<INDEX> -g <KEY_WORD Group Index>*
csm wcf obj *<INDEX> -w <E/D/P/B>*
csm wcf obj *<INDEX> -s <CATEGORY/WEB_GROUP>*
csm wcf obj *<INDEX> -u <CATEGORY/WEB_GROUP>*

Syntax Description

Parameter	Description
show	It means to display the web content filter profiles.
Look	It means to display the license information of WCF.
cache	It means to set the cache level for the profile.
server WCF_SERVER	It means to set web content filter server.
msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
setdefault	It means to return to default settings for all of the profile.
obj	It means to specify the object profile.
<INDEX>	It means to specify the index number of CSM profile. INDEX= 1~8.
-v	It means to view the web content filter profile.
-a <P/B>	Set the action of web content filter profile, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
-n <PROFILE_NAME>	It means to set the profile name. PROFILE_NAME: Enter the name of the profile (less than 16 characters)
-l <N/P/B/A>	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
-o <KEY_WORD Object Index>	Set the keyword object. *<KEY_WORD Object Index>*= Specify the index number of the object profile.
-g <KEY_WORD Group Index>	Set the keyword group. <KEY_WORD Group Index>= Specify the index number of the group profile.
-w <E/D/P/B>	It means to set the action for the black and white list. E:Enable, D:Disable, P:Pass, B:Block

-s <CATEGORY/WEB_GROUP>	It means to select the items under CATEGORY or WEB_GROUP. <WEB_GROUP>: Includes "Child Protection Group", "Leisure Group", "Business Group", "Chating Group", "Computer Internet Group", "Other Group" <CATEGORY>: Includes "Advertisement & Pop-Ups", "Alcohol & Tobacco", "Anonymizers", "Arts", "Business", "Transportation", "Chat", "Forums & Newsgroups", "Compromised", "Computers & Technology", "Criminal & Activity", "Dating & Personals", "Down sites", "Education", "Entertainment", "Finance", "Gambling", "Games", "Government", "Hate & Intolerance", "Health & Medicine", "Illegal Drug", "Job Search", "Streaming Media & Downloads", "News", "Non-profits & NGOs", "Nudity", "Persional Sites", "Phishing & Fraud", "Politics", "Pornography & Sexually explicit", "Real Estate", "Religion", "Restaurants & Dining", "Search engines & Portals", "Shopping", "Social Networking", "Spam sites", "Sports", "Malware", "Translators", "Travel", "Violence", "Weapons", "Web-Based Email", "General", "Leisure & Recreation", "Botnets", "Cults", "Fashion & Beauty", "Greeting Cards", "Hacking", "Illegal Softwares", "Image Sharing", "Information Security", "Instant Messaging", "Network Errors", "Parked Domains", "Peer-to-Peer", "Private IP Address", "School Cheating", "Sex Education", "Tasteless", "Child Abuse Images", "Uncategorised Sites"
-u <CATEGORY/WEB_GROUP>	It means to discard items under CATEGORY or WEB_GROUP. <WEB_GROUP>: Includes "Child Protection Group", "Leisure Group", "Business Group", "Chating Group", "Computer Internet Group", "Other Group" <CATEGORY>: Includes "Advertisement & Pop-Ups", "Alcohol & Tobacco", "Anonymizers", "Arts", "Business", "Transportation", "Chat", "Forums & Newsgroups", "Compromised", "Computers & Technology", "Criminal & Activity", "Dating & Personals", "Down sites", "Education", "Entertainment", "Finance", "Gambling", "Games", "Government", "Hate & Intolerance", "Health & Medicine", "Illegal Drug", "Job Search", "Streaming Media & Downloads", "News", "Non-profits & NGOs", "Nudity", "Persional Sites", "Phishing & Fraud", "Politics", "Pornography & Sexually explicit", "Real Estate", "Religion", "Restaurants & Dining", "Search engines & Portals", "Shopping", "Social Networking", "Spam sites", "Sports", "Malware", "Translators", "Travel", "Violence", "Weapons", "Web-Based Email", "General", "Leisure & Recreation", "Botnets", "Cults", "Fashion & Beauty", "Greeting Cards", "Hacking", "Illegal Softwares", "Image Sharing", "Information Security", "Instant Messaging", "Network Errors", "Parked Domains", "Peer-to-Peer", "Private IP Address", "School Cheating", "Sex Education", "Tasteless", "Child Abuse Images", "Uncategorised Sites"

Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[]White/Black list
Action:[block]
  No  Obj NO.    Object Name
 --- -------- ----------------------------------
  No  Grp NO.    Group Name
 --- -------- ----------------------------------
Action:[block]
 Log:[block]
--------------------------------------------------------------------------------
child Protection Group:
  [v]Alcohol & Tobacco     [v]Criminal & Activity     [v]Gambling
  [v]Hate & Intolerance    [v]Illegal Drug            [v]Nudity
  [v]Pornography & Sexually explicit  [v]Violence     [v]Weapons
  [v]School Cheating       [v]Sex Education           [v]Tasteless
  [v]Child Abuse Images
--------------------------------------------------------------------------------
leisure Group:
  [ ]Entertainment     [ ]Games                   [ ]Sports
  [ ]Travel            [ ]Leisure & Recreation    [ ]Fashion & Beauty
.
.
>
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns enable

Enables or disables the DDNS function.

Syntax

ddns enable *<0/1>*

Syntax Description

Parameter	Description
<0/1>	0 - Disable the DDNS function. 1 - Enable the DDNS function.

Example

```
> ddns enable 1
> Enable Dynamic DNS Setup
```

Telnet Command: ddns set

This command allows users to set Dynamica DNS account.

Syntax

ddns set *option <value>*

Syntax Description

Parameter	Description
-i <value>	It means index number of Dynamic DNS Account. <value>=1~6
-E <value>	It means to enable /disable Dynamic DNS Account. <value>=0~1 0: Disable 1: Enable
-W <value>	It means to specify WAN Interface. <value>=1~4 1: WAN1 First 2: WAN1 Only 3: WAN2 First 4: WAN2 Only example: To set WAN Interface: WAN1 First
-L <value>	It means to type Login Name. [value]: limit up to 64 characters
-P <value>	It means to type Password. [value]: limit up to 24 characters
-C <value>	It means to enable /disable Wildcards. <value>=0~1 0: Disable 1: Enable
-B <value>	It means to enable / disable Backup MX. <value>=0~1 0: Disable 1: Enable
-M <value>	It means to type Mail Extender. [value]: limit up to 60 characters
-R <value>	It means to type Determine Real WAN IP. <value>=0~1 0: WAN IP, 1: Internet IP
-S <value>	It means to specify Servive Provider. If user want to set User-Defined page, value must select 1. <value>= 1~19 1: User-Defined 2:3322 DDNS (www.3322.org) 3: ChangeIP.com (www.changeip.com) 4:ddns.com.cn (www.ddns.com.cn) 5: DtDNS (www.dtdns.com) 6: dyn.com (www.dyn.com) 7: DynAccess (www.dynaccess.com) 8: dynami.co.za (www.dynami.co.za) 9: freedns.afraid.org (freedns.afraid.org) 10: NO-IP.COM Free (www.no-ip.com) 11: opendns.com (www.opendns.com) 12: OVH (www.ovh.com) 13: Strato (www.strato.eu) 14: TwoDNS (www.twodns.de) 15: TZO (www.tzo.com) 16: ubddns.org (ubddns.org)

	17: Viettel DDNS (vddns.vn) 18: vigorddns.com (www.vigorddns.com) 19: ZoneEdit DDNS (dynamic.zoneedit.com)
T <value>	It means to type Servive Type. <value>= 1~3 1: Dynamic 2: Custom 3: Static
-D <Host Name> <sub Domain Name>	It means to type Domain Name. i.e: Account index 1 setting Domain Name for Dynamic Service Type >> ddns set -i 1 -T 1 -D "host ddns.com.cn" i.e: Account index 2 setting Domain Name for Custom Service Type >> ddns set -i 2 -T 2 -D "domain name" i.e: Account index 3 setting Domain Name for Static Service Type >> ddns set -i 3 -T 3 -D "domain name"
-H <value>	It means to type User-Defined Provider Host. <value>= limit up to 64 characters
-A <value>	It means to type User-Defined Service API. <value>= limit up to 256 characters
-a <value>	It means to type User-Defined Auth Type. <value>=0~1 0: basic 1: URL
-N <value>	It means to type User-Defined Connection Type. <value>=0~1 0: Http 1: Https
-O <value>	It means to type User-Defined Server Response. <value>: limit up to 32 characters

Example

```
> ddns set -i 1 -S 6 -T 1 -D "hostname dnsalias.net" -L user1 -P pwd1
> Save OK
```

Telnet Command: ddns time

Sets and displays the DDNS time.

Syntax

ddns time <*update in minutes*>

Syntax Description

Parameter	Description
update in minutes	Enter the value as DDNS time. <update in minutes>=1 ~ 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1440
```

```
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1000
```

Telnet Command: ddns forceupdate

This command will update DDNS automatically.

Example

```
> ddns forceupdate
 Now updating DDNS ...
 Please check result by using command "ddns log"
```

Telnet Command: ddns setdefault

This command will return DDS with factory default settings.

Example

```
>ddns setdefault
>Set to Factory Default.
```

Telnet Command: ddns show

This command allows users to check the content of selected DDNS account.

Syntax

ddns show -i <*value*>

Syntax Description

Parameter	Description
-i <*value*>	Display the content of selected DDNS account by entering the index number of the account. <value>=1~6

Example

```
> ddns show -i 1
-------------------------------------------------
 Index: 1
 [ ] Enable Dynamic DNS Account
 WAN Interface: WAN1 First
 Service Provider: dyn.com (www.dyn.com)
 Service Type: Dynamic
 Domain Name: [].[]
 Login Name:
 [ ] Wildcards
 [ ] Backup MX
 Mail Extender:
 Determine Real WAN IP: WAN IP

DrayTek>
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

Syntax

dos *<-V / D / A>*

dos *-s <ATTACK_F> <THRESHOLD> <TIMEOUT>*

dos *<-a /-e> <ATTACK_F><ATTACK_0>*

dos *-d <ATTACK_F><ATTACK_0>*

dos *-o <LOG_TYPE> -p<LOG_TYPE> -l <LOG_TYPE>*

dos *<-P/-B> add4 <ipv4_addr>*

dos *<-P/-B> remove4 <ipv4_addr/all>*

dos *<-P/-B> add6 <ipv6_addr>*

dos *<-P/-B> remove6 <ipv6_addr/all>*

dos *<-P/-B> show*

Syntax Description

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-A	It means to activate the DoS defense system.
-s <ATTACK_F> <THRESHOLD> <TIMEOUT>	It means to enable the defense function for a specific attack and set its parameter(s). <ATTACK_F>: Specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan. <THRESHOLD>*:* It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20. <TIMEOUT>: It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
-a <ATTACK_F> <ATTACK_0>	It means to enable the defense function for all attacks listed in ATTACK_0. <ATTACK_F>: Specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan. < *ATTACK_0*>: Specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-e <ATTACK_F> <ATTACK_0>	It means to enable defense function for a specific attack(s). <ATTACK_F>: Specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan. < *ATTACK_0*>: Specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d <ATTACK_F> <ATTACK_0>	It means to disable the defense function for a specific attack(s). <ATTACK_F>: Specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan. < *ATTACK_0*>: Specify a name of the following attacks:

	ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-o <LOG_TYPE>	It means to enable/disable DOS defense log. <LOG_TYPE>= 0~1 0:Disable 1:Enable
-p <LOG_TYPE>	It means to enable/disable spoofing defense log. <LOG_TYPE>= 0~1 0:Disable 1:Enable
-l <LOG_TYPE>	It means to enable/disable black and white list log. <LOG_TYPE>= 0~3 0:None 1:WhiteList 2:BlackList 3:All
<-P/-B> add4 <ipv4_addr>	It means to set Passing List or Blocking List. <ipv4_addr>= Enter an IPv4 address.
<-P/-B> remove4 <ipv4_addr/all>	It means to remove IPv4 address in Passing List or Blocking List. <ipv6_addr/all>= Enter an IPv4 address or enter all.
<-P/-B> add6 <ipv6_addr>	It means to add an IPv6 address to Passing List or Blocking List. <ipv6_addr>= Enter an IPv6 address.
<-P/-B> remove6 <ipv6_addr/all>	It means to remove IPv6 address in Passing List or Blocking List. <ipv6_addr/all>= Enter an IPv6 address or enter all.
<-P/-B> show	It means to show the Passing List or Blocking List.

Example

```
>dos –A
The Dos Defense system is Activated
>dos –s synflood 50 10
Synflood is enabled! Threshold=50 <pke/sec> timeout=10 <pke/sec>
DrayTek> dos -P add4 192.168.1.59
Add IP in Passing IP List success.
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet *-<command> <parameter> | ...*

Syntax Description

Parameter	Description
<*command*><*parameter*>|*...]*	The available commands with parameters are listed below. *[...]* means that you can Enter several commands in one line.
-M <n>	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 3) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP n=A: 3G/4G USB Modem(PPP mode) n=B: 3G/4G USB Modem(DHCP mode
-S <isp name>	It means to set ISP Name (max. 23 characters).
-P <on/off>	It means to enable PPPoE Service.
-u <username>	It means to set username (max. 49 characters) for Internet accessing.
-p <password>	It means to set password (max. 49 characters) for Internet accessing.
-a <n>	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-t <n>	It means to set connection duration and n means different conditions. n=1~999: Idle time for offline (default 180 seconds) n=-1: Always-on
-i <ip address>	It means that *PPPoE server* will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the router will use that one as a fixed IP.
-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	It means to assign gateway IP for such WAN connection.
-A <idx>	Set to Always On mode, and <idx> as backup WAN#.
-B <mode>	Set to Backup mode; <mode> 0: When any WAN disconnect; 1: When all WAN disconnect.
-V	It means to view Internet Access profile.
-C <sim pin code>	Set SIM PIN code (max. 15 characters) for USB PPP mode.
-O <init string>	Set Modem Initial String (max. 47 characters) for USB PPP mode.
-T <init string2>	Set Modem Initial String2 (max. 47 characters) for USB PPP mode.

-D <dial string>	Set Modem Dial String (max. 31 characters) for USB PPP mode.
-v <service name>	Set Service Name (max. 23 characters) for USB PPP mode.
-m <ppp username>	Set PPP Username (max. 63 characters) for USB PPP mode.
-o <ppp password>	Set PPP Password (max. 62 characters) for USB PPP mode.
-e <n>	Set PPP Authentication Type for USB PPP mode. n= 0: PAP/CHAP (default) 1: PAP Only
-q <n>	Set the first schedule for USB PPP mode. n=1~15
-x <n>	Set the second schedule for USB PPP mode. n=1~15
-y <n>	Set the third schedule for USB PPP mode. n=1~15
-z <n>	Set the fourth schedule for USB PPP mode. n=1~15
-Q <mode>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect
-I <ping ip>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP for USB DHCP or PPP mode. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP
-L <n>	Set WAN Connection Detection TTL (1-255) value for USB PPP mode. N=1~255
-E <sim pin code>	Set SIM PIN code (max. 19 characters) for USB DHCP mode.
-G <mode>	Set Network Mode for USB DHCP mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
-N <apn name>	Set APN Name (max. 47 characters) for USB DHCP mode.
-U <n>	Set MTU(1000-1440) for USB DHCP mode. n=1000~1440
-f <n>	Set DSL Mode. n= 0: Auto, n=1: ADSL Only, n=2: VDSL Only
-j <on/off>	Separate Account for ADSL. on: enable. off: disable.

-k <username>	Set ADSL account Username (max. 49 characters) when Separate Account is enabled.
-l <password>	Set ADSL account Password (max. 49 characters) when Separate Account is enabled.

Example

```
>internet -M 1 -S tcom -u username -p password -a 0 -t -1  -i 0.0.0.0
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 ISP Name set to tcom
 WAN1 Username set to username
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
 WAN1 Idle timeout set to always-on
 WAN1 Gateway IP set to 0.0.0.0
> internet -V
WAN1 Internet Mode:PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP
> internet -M 1 -u link1 -p link1 -a 0
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 Username set to link1
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the public subnet for your router.

Syntax

ip pubsubnet <*Enable/Disable*>

Syntax Description

Parameter	Description
<*Enable/Disable*>	Enable or disable the function.

Example

```
> ip pubsubnet enable
public subnet enabled!
```

Telnet Command: ip pubaddr

This command allows to set the **IP routed subnet** for the router.

Syntax

ip pubaddr *?*

ip pubaddr <*public subnet IP address*>

Syntax Description

Parameter	Description
?	Display current IP address which allows users set as the public subnet IP address.
<public subnet IP address>	Specify an IP address. The system will set the one that you specified as the public subnet IP address.

Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

ip pubmask *?*

ip pubmask *<public subnet mask>*

Syntax Description

Parameter	Description
?	Display current IP address which allows users set as the public subnet mask.
<public subnet IP address>	Specify a subnet mask. The system will set the one that you specified as the public subnet mask.

Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

Syntax

ip aux add *<IP> <Join to NAT Pool>*

ip aux remove *<index>*

Syntax Description

Parameter	Description
add <IP> <Join to NAT Pool>	It means to create a new WAN IP address. <IP>=Enter an IP address as the auxiliary WAN IP address.

	<*Join to NAT Pool*>=0~1, 0 (disable) or 1 (enable).
remove < *index* >	It means to delete an existed WAN IP address. <index>= Enter the index number of the table displayed on your screen.

Example

```
> ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 2.

DrayTek> ip aux ?
%% ip aux add [IP] [Join to NAT Pool]
%% ip aux remove [Index]

%%    Where IP = Auxiliary WAN IP Address.
%%         Join to NAT Pool = 0 or 1.
%%         Index = The Index number of table.

Now auxiliary WAN1 IP Address table:
Index no.      Status  IP address     NAT IP pool
-----------------------------------------------------
  1          Disable 0.0.0.0 Yes
  2          Enable  192.168.1.65   Yes
```

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

ip addr <*IP address*>

Syntax Description

Parameter	Description
<*IP address*>	It means the LAN IP address. <IP address>=Enter an IPv4 address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```

Info

When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

ip nmask <*IP netmask*>

Syntax Description

Parameter	Description
<*IP netmask*>	It means the netmask of LAN IP. <IP netmask>=Enter the netmask.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

ip arp add <*IP address*> <*MAC address*> <*LAN / WAN*>

ip arp del <*IP address*> <*LAN / WAN*>

ip arp flush

ip arp status

ip arp accept <*0/1/2/3/4/5/status***>**

ip arp setCacheLife <*time*>

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source /destination MAC address; arp **setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
add <IP address> <MAC address> <LAN / WAN>	It means to add one LAN IP address with subnet mask on selected interface. <IP address>: Enter an IP address. <MAC address>: Enter the MAC address of your router. <LAN / WAN>:It indicates the direction for the arp function.
del <IP address> <LAN / WAN>	It means to delete one LAN IP address on selected interface. <IP address>: Enter an IP address. <LAN / WAN>:It indicates the direction for the arp function
accept <0/1/2/3/4/5/status>	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
setCacheLife <time>	Available settings will be 10, 20, 30,....2550 seconds.

Example

```
> ip arp accept status
Accept illegal source mac arp: disable

Accept illegal dest mac arp: disable

Accept VRRP mac into arp table: disable
> ip arp status
[ARP Table]
 Index IP Address       MAC Address       Netbios Name
   1   192.168.1.113    00-05-5D-E4-D8-EE   A1000351
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc *option*

ip dhcpc *option -l*
ip dhcpc *option -d <idx>*
ip dhcpc *option -e <1 or 0> -w <wan unmber> -c<option number> -v <option value>*
ip dhcpc *option -e <1 or 0> -w <wan unmber> -c <option number> –x <option value>*
ip dhcpc *option -e <1 or 0> -w <wan unmber> -c<option number> –a <option value>*
ip dhcpc *option -u <idx unmber>*
ip dhcpc *release <wan number>*
ip dhcpc *renew <wan number>*
ip dhcpc *status*

Syntax Description

Parameter	Description
option	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number -e: enable/disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0~255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
release	It means to release current WAN IP address.
renew	It means to renew the WAN IP address and obtain another new one.
status	It displays current status of DHCP client.

Example

```
> ip dhcpc option -e 1 -w 1/2 -c 18 -v /path1
>
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2/PVC3/PVC4/PVC5 for verifying if the WAN connection is OK or not.

Syntax

ip ping <*IP address> <AUTO/WAN1/WAN2/PVC3/PVC4/PVC5> <Source IP address>*

Syntax Description

Parameter	Description
<IP address>	It means the WAN IP address.
<AUTO/WAN1/PVC3/PVC4/PVC5>	It means the WAN port /PVC that the above IP address passes through.
<Source IP address>	Enter the IP address.

Example

```
> ip ping 192.168.1.1 AUTO
```

```
Pinging 192.168.1.1 with 64 bytes of Data through LAN

Receive reply from 192.168.1.1, time<1ms
Receive reply from 192.168.1.1, time<1ms
Receive reply from 192.168.1.1, time<1ms
Receive reply from 192.168.1.1, time<1msReceive reply from 192.168.1.1,
time<1ms

Packets: Sent = 5, Received = 5, Lost = 0 (0% loss)
```

Telnet Command: ip tracert

This command allows users to trace the routes from the router to the host.

Syntax

ip tracert *<IP address> <WAN1/WAN2/WAN3> <Udp/Icmp>*

Syntax Description

Parameter	Description
< IP address>	It means the target IP address.
<WAN1/WAN2/WAN3>	It means the WAN port that the above IP address passes through.
<Udp/Icmp>	It means the UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
1    172.16.3.7    10ms
2    172.16.1.2    10ms
3    Request Time out.
4    168.95.90.66  50ms
5    211.22.38.134 50ms
6    220.128.2.62  50ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

ip telnet <*IP address><Port>*

Syntax Description

Parameter	Description
<IP address>	Enter the WAN or LAN IP address of the remote device.
<Port>	Type a port number (e.g., 23). Available settings: 0 ~65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

ip rip *<0/1/2>*

Syntax Description

Parameter	Description
<0/1/2>	0 means disable; 1 means first subnet and 2 means second subnet.

Example

```
> ip rip 1
%% Set RIP LAN1.
```

Telnet Command: ip wanrip

This command allows users to set the RIP (routing information protocol) of WAN IP.

Syntax

ip wanrip <*ifno*> *-e <0/1>*

Syntax Description

Parameter	Description
<*ifno*>	It means the connection interface. 1: WAN1, 2:WAN2, 3: PVC3,4: PVC4,5: PVC5 **Note**: PVC3 ~PVC5 are virtual WANs.
-e <0/1>	It means to disable or enable RIP setting for specified WAN interface. 1: Enable the function of setting RIP of WAN IP. 0: Disable the function.

Example

```
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1, 2:WAN2
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol disable
 WAN[6] Rip Protocol enable
 WAN[7] Rip Protocol enable
> ip wanrip 5 -e 1
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol enable
 WAN[6] Rip Protocol enable
 WAN[7] Rip Protocol enable
```

Telnet Command: ip route

This command allows users to set static route.

Syntax

ip route *add <dst> <netmask> <gateway> <ifno> <rtype>*

ip route *del <dst> <netmask> <rtype>*

ip route *status*

ip route *cnc*

ip route *default off*

ip route *clean <1/0>*

Syntax Description

Parameter	Description
add <dst> <netmask> <gateway> <ifno> <rtype>	It means to add an IP address as static route. <dst>: Enter the IP address of the destination. <*netmask*>:Enter the netmask of the specified IP address. <gateway>: Enter the gateway of the connected router. <ifno>: Speicfy the connection interface. 3=WAN1 4=WAN2 7=WAN5,8=WAN6,9=WAN7 <rtype>: Enter the type (default or static) of the route.
del <dst> <netmask> <rtype>	It means to delete specified IP address. <dst>:Enter the IP address of the destination. <*netmask*>: Enter the netmask of the specified IP address. <rtype>: Enter the type (default or static) of the route.
status	It means current status of static route.
cnc	It means current IP range for CNC Network.
default off	It is available for NAT subnet only. Set the default route as off.
clean <1/0>	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~       192.168.1.0/   255.255.255.0 is directly connected, LAN1
S         172.16.2.0/   255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

ip igmp_proxy *set*

ip igmp_proxy *reset*

ip igmp_proxy *wan <1~4>*

ip igmp_proxy *query*

ip igmp_proxy *ppp <0/1>*

ip igmp_proxy *status*

ip igmp_proxy *version <v2/v3/auto/show>*

Syntax Description

Parameter	Description
set	It means to enable proxy server.
reset	It means to disable proxy server.
wan <1~4>	It means to specify WAN interface for IGMP service.
t_home	It means to specify t_home proxy server for using.
on/off/show/help	It means to turn on/off/display or get more information of the T_home service.
query <value>	It means to set IGMP general query interval. <value>: Enter a number. The default value is 125000 ms.
ppp <0/1>	It means to enable or disable the function. 0: No need to set IGMP with PPP header. 1: Set IGMP with PPP header.
status	It means to display current status for proxy server.
version <v2/v3/auto/show>	It means to change or display current version of IGMP proxy server. v2: version v2 v3: version v3 auto: version used will be detected automatically show: Disply current version used.

Example

```
> ip igmp_proxy query 130000
 This command is for setting IGMP General Query Interval
 The default value is 125000 ms
 Current Setting is:130000 ms
> DrayTek> ip igmp_proxy version show
 igmp version rule: auto
 wan ver: v2
 lan ver: v3
```

Telnet Command: ip igmp_snoop

This command allows users to enable or disable IGMP snoop function.

Syntax

ip igmp_snoop enable

ip igmp_snoop disable

ip igmp_snoop status

ip igmp_snoop txquery *<on/off> <v2/v3>*

ip igmp_snoop chkleave

ip igmp_snoop separate *<on/off>*

Syntax Description

Parameter	Description
enable	It means to enable igmp snoop function
disable	It means to disable igmp snoop function.
status	It means to display current igmp configuration.
txquery <on/off> <v2/v3>	It means to send out IGMP QUERY to LAN periodically. On: enable Off: disable v2: version v2 v3: version v3
chkleave <on/off>	It means to check the leave status. On: enable the IGMP snoop leave checking function. Off: it will drop LEAVE if still clients on the same group.
separate <on/off>	It means to set IGMP packets being separated by NAT/Bridge. On: The packets will be separated. Off: The packets will not be separated by NAT/Bridge.

Example

```
> ip igmp_snoop enable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
> ip igmp_snoop disable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Disabled.
> ip igmp_snoop separate ?
% ip igmp separate [on/off]
 igmp snoop seprate is ON now.
igmp packets will be separated by  NAT/Bridge.
```

Telnet Command: ip igmp_fl

This command allows users to enable or disable IGMP Fast Leave function.

Syntax

ip igmp_fl enable

ip igmp_fl disable

ip igmp_fl status

Syntax Description

Parameter	Description
enable	It means to enable IGMP Fast Leave function
disable	It means to disable IGMP Fast Leave function.
status	It means to display current IGMP Fast Leave configuration.

Example

```
> ip igmp_fl enable ?
  If you want to use IGMP fast leave , you "MUST" enable IGMP snooping.
> ip igmp_snoop enable
% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
> ip igmp_fl enable
%% ip igmp_fl [enable|disable|status], IGMP Fast Leave is Enabled.
```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

ip dmz <*mac*>

Syntax Description

Parameter	Description
<*mac*>	It means the MAC address of the device that you want to specify

Example

```
>ip dmz ?
% ip dmz <mac>,  now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>,  now : 11-22-33-44-55-66
>
```

Telnet Command: ip dmzswitch

This command allows users to set DMZ mode.

ip dmzswitch *off*

ip dmzswitch *private*

ip dmzswitch *active_trueip*

Syntax Description

Parameter	Description
off	It means to turn off DMZ function.
private	It means to set DMZ with private IP.
active_trueip	It means to set the DMZ with active true IP.

Example

```
>ip dmzswitch off
>
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

Syntax

ip session *on*

ip session *off*

ip session *default <num>*

ip session *defaultp2p <num>*

ip session *status*

ip session *show*

ip session *timer <num>*

ip session *<block/unblock><IP>*

ip session *<add/del><IP1-IP2><num><p2pnum>*

Syntax Description

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default <num>	It means to set the default number of session num limit.
defaultp2p <num>	It means to set the default number of session num limit for p2p.
status	It means to display the current settings.
show	It means to display all session limit settings in the IP range.
timer <num>	It means to set when the IP session block works. The unit is second.
<block/unblock><IP>	It means to block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
<add/del><IP1-IP2><num><p2pnum>	It means to add / delete the session limits in an IP range. <IP1-IP2>: It means the range of IP address specified for this

	command. <num>: It means the number of the session limits, e.g., 100. <p2pnum>: It means the number of the session limits, e.g., 50 for P2P.

Example

```
> ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

  IP range:
    192.168.1.5 - 192.168.1.100 : 100

  Current ip session limit is turn on

  Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

Syntax

ip bandwidth *on*

ip bandwidth *off*

ip bandwidth *default <tx_rate><rx_rate>*

ip bandwidth *status*

ip bandwidth *show*

ip bandwidth <*add/del***>** *<IP1-IP2><tx><rx><shared>*

Syntax Description

Parameter	Description
on	It means to turn on the IP bandwidth limit.
off	It means to turn off the IP bandwidth limit.
default <tx_rate><rx_rate>	<tx_rate><rx_rate>: It means to set default tx and rx rate of bandwidth limit. The range is from 0 – 65535 Kpbs.
status	It means to display the current settings.
show	It means to display all the bandwidth limits settings within the IP range.
<*add/del***>** *<IP1-IP2><tx><rx><shared>*	It means to add / delete the bandwidth within the IP range. <IP1-IP2>: It means the range of IP address specified for this command. <tx>: It means to set transmission rate for bandwidth limit. <rx>: It means to set receiving rate for bandwidth limit. <shared>: It means that the bandwidth will be shared for the IP range.

Example

```
> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

  IP range:
    192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

  Current ip Bandwidth limit is turn off
  Auto adjustment is off
>
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

Syntax

ip bindmac *on*

ip bindmac *off*

ip bindmac *<strict_on/strict_off>*

ip bindmac *add <IP><MAC><Comment>*

ip bindmac *del <IP>/<all>*

ip bindmac *subnet <all/set LAN_Index/unset LAN_Index/clear/show>*

ip bindmac *show*

Syntax Description

Parameter	Description
on	It means to turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
off	It means to turn off all the bindmac policy.
<strict_on / strict_off>	It means that only those IP address in IP bindmac policy table can / can not access into network.
add <IP><MAC><Comment>	It means to add one ip bindmac. <IP>: It means to enter the IP address for binding with specified MAC address. <MAC>: It means to Enter the MAC address for binding with the IP address specified. <Comment>: It means to type words as a brief description.
del <IP>/<all>	It means to delete one ip bindmac. <IP>: It means to enter the IP address for binding with specified MAC address. <all>: It means to delete all the IP bindmac settings.
subnet <all/set LAN_Index/unset LAN_Index/clear/show>	It means to set LAN subnet to bind strict mode. <all>: It means to set all the LAN subnet to bind the strict mode. <set LAN_Index>: It means to specify the index number (1~4) of LAN subnet to enable the subnet setting. <unset LAN_Index>: It means to specify the index number (1~4) of LAN subnet to disable the subnet setting.

	<clear>: Remove the subnet settings. <show>: Display the subnet settings.
show	It means to display the IP address and MAC address of the pair of binded one.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned OFF
ip bind mac function is STRICT OFF
Show all IP Bind MAC entries.
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 HOST ID : (null)
  Comment : just
> ip bindmac subnet set 2
Set LAN 1 is OK.
> ip bindmac subnet show
 LAN 2

>
```

Telnet Command: ip maxnatuser

This command is used to set the maximum number of NAT users.

Syntax

ip maxnatuser <*user no***>**

Syntax Description

Parameter	Description
<*user no*>	A number specified here means the total NAT users that Vigor router supports. 0 – It means no limitation.

Example

```
> ip maxnatuser 100
% Max NAT user = 100
```

Telnet Command: ip spoofdef

This command is used to enable/disable the IP Spoofing Defense.

Syntax

ip spoofdef <*WAN/LAN*><*0/1*>

Syntax Description

Parameter	Description
<*WAN/LAN*>	It means to block IP packet from WAN/LAN with inconsistent source IP address.
<*0/1*>	0: Disable the function. 1: Enable the funciton.

Example

```
> ip spoofdef WAN 1
Setting saved:
>
```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

ip6 addr -s <*prefix*> <*prefix-length*> <*LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32*>

ip6 addr -d <*prefix*> <*prefix-length*> <*LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32*>

ip6 addr -a <*LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32*> *-u*

ip6 addr -v <*LAN1/LAN2/WAN1/WAN2/USB1/USB2*>

ip6 addr -t <*old-prefix*><*old-prefix-length*><*new-prefix*> <*new-prefix-length*> <*LAN1/LAN2/WAN1/WAN2/USB1/USB2*>

ip6 addr -o <*1/2*>

ip6 addr -o 3 <*prefix*> <*prefix-length*> <*WAN1/WAN2/USB1/USB2*>

ip6 addr -l *<prefix> <prefix-length> <LAN1/LAN2>*

ip6 addr <-*p/-b***>** *<prefix> <prefix-length> <WAN1/WAN2/USB1/USB2>*

ip6 addr -x *<LAN1|LAN2>*

ip6 addr -c *<LAN1|LAN2>*

ip6 addr -e *<type> <LAN1|LAN2>*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32>	It means to add a static ipv6 address. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32>: It means to specify LAN/WAN/USB/VPN interface for such address.
-d <prefix> <prefix-length> <LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32>	It means to delete an ipv6 address. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32>: It means to specify LAN/WAN/USB/VPN interface for such address.
-a <LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32> -u	It means to show current address(es) status. <LAN1/LAN2/WAN1/WAN2/USB1/USB2/VPN1/..VPN32>: It means to specify LAN/WAN/USB/VPN interface. <-u>: It means to show unicast address only.
-v <LAN1/LAN2/WAN1/WAN2/USB1/USB2>	It means to show prefix list status.
-t <old-prefix><old-prefix-length><new-prefix> <new-prefix-length> <LAN1/LAN2/WAN1/WAN2/USB1/USB2>	It means to update WAN static IPv6 address table. <old-prefix>: It means to enter the prefix number of IPv6 address. <old prefix-length>: It means to enter a fixed value as the length of the prefix. <new-prefix>: It means to enter the prefix number of IPv6 address. <new-prefix-length>: It means to enter a fixed value as the length of the prefix. <LAN1/LAN2/WAN1/WAN2/USB1/USB2 >: It means to specify LAN/WAN/USB interface for such address.
-o <1/2>	<1>: It means to show old prefix list. <2>: It means to send old prefix option by RA.
-o <3> <prefix> <prefix-length> <WAN1/WAN2/USB1/USB2>	<3>: It means to set old prefix. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <WAN1/WAN2/USB1/USB2 >: It means to specify a WAN/USB interface for such address.

-l <prefix> <prefix-length> <LAN1/LAN2>	It means to add a ULA. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <LAN1/LAN2 >: It means to specify a LAN interface for such address.
-p/-b <prefix> <prefix-length> <WAN1/WAN2/USB1/USB2>	It means to add/delete an prefix to/from prefix list. p: Add a prefix to a prefix list. b: Delete a prefix from a prefix list. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <WAN1/WAN2/USB1/USB2 >: It means to specify a WAN/USB interface for such address.
-x <LAN1/LAN2>	It means to generate a ULA automatically. <LAN1/LAN2 >: It means to specify a LAN interface.
-c <LAN1/LAN2>	It means to delete a ULA . <LAN1/LAN2 >: It means to specify a LAN interface.
-e <type> <LAN1/LAN2>	It means to set ULA type. <type>: 0, disable; 1, static; 2, auto <LAN1/LAN2 >: It means to specify a LAN interface.

Example

```
> ip6 addr -a
LAN
Unicast Address:
 FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
 FF02::2
 FF02::1:FF00:0
 FF02::1
> ip6 addr -o 3 2001:: 64 WAN2
% set WAN2 2001::/64 ok
```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

Syntax

ip6 dhcp *req_opt <LAN1/LAN2/WAN1/WAN2/USB1/USB2> [-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
req_opt	It means option-request.
<LAN1/LAN2/WAN1/WAN2/USB1/USB2>	It means to specify LAN or WAN or USB interface for such address.

[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-a	It means to show current DHCPv6 status.
-s	It means to ask the SIP.
-S	It means to ask the SIP name.
-d	It means to ask the DNS setting.
-D	It means to ask the DNS name.
-n	It means to ask NTP.
-i	It means to ask NIS.
-I	It means to ask NIS name.
-p	It means to ask NISP.
-P	It means to ask NISP name.
-b	It means to ask BCMCS.
-B	It means to ask BCMCS name.
-r	It means to ask refresh time.
Parameter	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%    sip name
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

Syntax

ip6 dhcp *client <WAN1/WAN2/USB1/USB2><-<command> <parameter>/ ... >*

Syntax Description

Parameter	Description
client	It means the dhcp client settings.
<<command> <parameter>|…>	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-r	It means to send a RELEASE message.
-a	It means to show current DHCPv6 status.
-p <IAID>	It means to request identity association ID for Prefix Delegation.
-n <IAID>	It means to request identity association ID for

	Non-temporary Address.
-t <time>	It means to set solicit interval. <time>: 0 ~ 7 seconds (default value is 0).
-c <parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-i <parameter>	It means to send information request to server. 1: Enable 0: Disable
-e <parameter>	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable
-m <parameter>	It means to enable/disable server DUID set by Link layer and time. 1: Enable 0: Disable
-d	It means to display the client DUID.
-A <parameter>	It means to set authentication protocol. 0: Undefine 2: delayed protocol
-R <parameter>	It means to set realm value (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-S <parameter>	It means to set shared secret (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-K <parameter>	It means to set key ID (1~65535) in delayed protocol. <parameter>: Enter a number.

Example

```
> ip6 dhcp client WAN2 –p 2008::1
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
      DHCPv6 client enabled
      request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 –n 1023456
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
      DHCPv6 client enabled
      request IA_NA whose IAID equals to 2008
> system reboot
```

Telnet Command : ip6 dhcp server

This command allows you to configure DHCPv6 server.

Syntax

ip6 dhcp *server -<<command> <parameter>/ ...>*

Syntax Description

Parameter	Description
server	It means the dhcp server settings.
<<command> <parameter>/…>	The available commands with parameters are listed below. <…> means that you can Enter several commands in one line.
-a	It means to show current DHCPv6 status.
-b	It means to show current DHCPv6 IP Assignment Table.
-n <name>	It means to set a profile name. <name>: Enter a string as profile name.
-c <parameter>	It means to send rapid commit to server. <parameter>: Enter 1 or 0. 1: Enable 0: Disable
-e <parameter>	It means to enable or disable the DHCPv6 server. <parameter>: Enter 1 or 0. 1: Enable 0: Disable
-t <time>	It means to set prefer lifetime. <time>: Enter a value.
-y <time>	It means to set valid lifetime. <time>: Enter a value.
-u <time>	It means to set T1 time. <time>: Enter a value.
-o <time>	It means to set T2 time. <time>: Enter a value.
-i <pool_min_addr>	It means to set the start IPv6 address of the address pool. <pool_min_addr>: Enter an IPv6 address.
-x <pool_max_addr>	It means to set the end IPv6 address of the address pool. <pool_max_addr>: Enter an IPv6 address.
-R	It means to send reconfigure packet to a client.
-r <1/0>	It means to enable (1) or disable (0) auto_range.
-N <1/0>	It means to enable (1) or disable (0) random address allocation.
-d <addr>	It means to set the first DNS IPv6 address. <addr> : Enter an IPv6 address.
-D <addr>	It means to set the second DNS IPv6 address. <addr> : Enter an IPv6 address.
-m <1/0>	It means to enable(1) or disable (0) the server DUID set by Link Layter and Time.
-q <name>	It means to set DNS domain search list. <name>: Enter a name.
-z<1/0>	It means enable (1) or disable (0) the DHCP PD.
pdadd	It means to add PD node.

<suffix><prefix_len><client linklocal><client DUID>	
pddel <PD index>	It means to delete PD node. <PD index>: Enter a number.
-A <parameter>	It means to set authentication protocol. <parameter>: Enter 0, 2 or 3. 0: Undefine 2: delayed protocol 3: Reconfigure key
- M <parameter>	It means to set realm value (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-S <parameter>	It means to set shared secret (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-K <parameter>	It means to set key ID (1~65535) in delayed protocol. <parameter>: Enter a number.

Example

```
> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%    DHCPv6 server disabled
%    maximum address of the pool: FF02::3
%    minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet <-<*command*> <*parameter*> | *...* >

Syntax Description

Parameter	Description
<*command*> <*parameter*>/*...*	The available commands with parameters are listed below. <*...*> means that you can Enter several commands in one line.
-W <n>	**W** means to set WAN interface and **n** means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
-M <n>	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 5) n=0: Offline, n=1: PPP, n=2: TSPC,

	n=3: AICCU, n=4: DHCPv6, n=5: Static n=6: 6in4-Static n=7: 6rd
-m n	It means to set IPv6 MTU. n = any value (0 means “unspecified”).
6rd	
-C <n>	It means to set 6rd connection mode. n=0: Auto n=1: Static
-s <server>	It means to set 6rd IPv4 Border Relay. <server>: Enter a string.
-m <n>	It means to set 6rd IPv4 address mask length. <n>: Enter a number.
-p <prefix>	It means to set IPv6 prefix for 6rd connection. <prefix>: Enter a prefix number of IPv6 address.
-l <n>	It means to set the prefix length for 6rd connection. <n>: It means to enter a fixed value as the length of the prefix.
6in4	
-s <server>	It means to set 6in4 remote endpoint IPv4 address.
-l <IPv6 Addr>	It means to set the IPv6 address for 6in4 connection.
-P <n>	It means to set IPv6 WAN prefix length for 6in4 connection.
-p <prefix>	It means to set 6in4 LAN Routed Prefix.
-l <n>	It means to set 6in4 LAN Routed Prefix length.
-T <n>	It means to set 6in4 Tunnel TTL.
TSPC/AICCU	
-u <username>	It means to set username (max. 63 characters). <username>: Enter a string.
-P <password>	It means to set Password (max. 63 characters). <password>: Enter a password.
-s <server>	It means to set Tunnel Server IP. <server>: Enter an IPv4 Address or URL (max. 63 characters)
AICCU	
-p <prefix>	It means to set Subnet Prefix (AICCU). <prefix>: Enter a prefix number of IPv6 address.
-l <n>	It means to set Subnet Prefix length (AICCU). <n>: Enter a number.
-o <1/0>	It means to set AICCU always on. 1: on 0: off
-f	It means to set AICCU tunnel ID.
Static	
-w <addr>	It means to set Default Gateway. <addr>: Enter an IPv6 address.
Others	
-d <server>	It means to set 1st DNS Server IP. <server>: Enter an IPv6 address.
-D <server>	It means to set 2nd DNS Server IP. <server>: Enter an IPv6 address.
-t <dhcp/ra/none>	It means to set ipv6 PPP WAN test mode for DHCP or RA. <dhcp/ra/none> : Enter dhcp, ra or none.
-V	It means to view IPv6 Internet Access Profile.
-k	It means to dial the Tunnel on the WAN.
-j	It means to drop the Tunnel on the WAN.
-r n	It means to set Prefix State Machine RA timeout.
-c n	It means to set Prefix State Machine DHCPv6 Client timeout.
-q <0/1/2>	It means to set WAN detection mode.

	0:NS Detect 1:Ping Detect 2:Always On
-z <value>	It means to set Ping Detect TTL (0-255). <value>: Enter 0~255.
-x <hostname/ IPv6 addr>	It means to set Ping Detect Host (hostname or IPv6 address). <hostname/ipv6 addr> : Enter a hostname or an IPv6 address.
-i <value>	It means to set ipv6 connection interval. <value>: Enter a number (1500-60000 (unit:10ms)).
-b <0/1>	It means to enable DNSv6 based on DHCPv6. 1 = on 0 = off
-R <0/1>	It means to Enable RIPng. 1 = on 0 = off

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 –s amsterdam.freenet6.net
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to set a IPv6 neighbour table.

Syntax

ip6 neigh *-s <inet6_addr> <eth_addr> <LAN1/LAN2/WAN1/WAN2/USB1/USB2>*

ip6 neigh *-d <inet6_addr> <LAN1/LAN2/WAN1/WAN2/USB1/USB2>*

ip6 neigh *-a <inet6_addr> <-N LAN1/LAN2/WAN1/WAN2/USB1/USB2>*

Syntax Description

Parameter	Description
-s <inet6_addr> <eth_addr> <LAN1/LAN2/WAN1/WAN2/USB1/USB2>	It means to add a neighbour. <inet6_addr>: Enter an IPv6 address. <eth_addr>: Enter a submask address. <LAN1/LAN2/WAN1/WAN2/USB1/USB2>: Specify an interface for the neighbor.
-d <inet6_addr> <LAN1/LAN2/WAN1/WAN2/USB1/USB2>	It means to delete a neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/LAN2/WAN1/WAN2/USB1/USB2>: Specify an interface for the neighbor.
-a <inet6_addr> -N <LAN1/LAN2/WAN1/WAN2/USB1/USB2>	It means to show neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1/LAN2/WAN1/WAN2/USB1/USB2>: Specify an interface for the neighbor.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN1
        Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a

I/F  ADDR                                MAC             STATE
-----------------------------------------------------------------------------
 LAN1 2001:2222:3333::1111                                IN_TIMER
 LAN4 ::                                                  NONE
 LAN3 ::                                                  NONE
 LAN1 ::                                                  NONE
 LAN2 ::                                                  NONE
 DMZ  ::                                                 NONE
>
```

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

Syntax

ip6 pneigh *-s <inet6_addr> <LAN1/LAN2/WAN1/WAN2/USB1/USB2>*

ip6 pneigh *-d <inet6_addr><LAN1/LAN2/WAN1/WAN2/USB1/USB2>*

ip6 pneigh *-a <inet6_addr> <-N LAN1/LAN2/WAN1/WAN2/USB1/USB2>*

Syntax Description

Parameter	Description
-s <inet6_addr> <eth_addr> <LAN1/LAN2/WAN1/WAN 2/USB1/USB2>	It means to add a proxy neighbour. <inet6_addr>: Enter an IPv6 address. <eth_addr>: Enter a submask address. <LAN1/LAN2/WAN1/WAN2/USB1/USB2>: Specify an interface for the proxy neighbor.
-d <inet6_addr> <LAN1/LAN2/WAN1/WAN 2/USB1/USB2>	It means to delete a proxy neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/LAN2/WAN1/WAN2/USB1/USB2>: Specify an interface for the proxy neighbor.
-a <inet6_addr> -N <LAN1/LAN2/WAN1/WAN 2/USB1/USB2>	It means to show proxy neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1/LAN2/WAN1/WAN2/USB1/USB2>: Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 LAN1
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to set route for IPv6 connection.

Syntax

ip6 route *-s <prefix> <prefix-length> <gateway> <LAN1/LAN2/WAN1/WAN2/ USB1/USB2/VPN1~VPN32> <-D>*

ip6 route -*d <prefix> <prefix-length>*

ip6 route -*a <LAN1/LAN2/WAN1/WAN2/ USB1/USB2/VPN1~VPN32>*

ip6 route -*l*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <gateway> <LAN1/LAN2/WAN1/WAN2/ USB1/USB2/VPN1~VPN32> <-D>	It means to add a route. <prefix>: It means to enter the prefix number of IPv6 address. <prefix length>: It means to enter a fixed value as the length of the prefix. <gateway>: It means to enter the gateway of the router. <LAN1/LAN2/WAN1/WAN2/ USB1/USB2/VPN1~VPN32>**:** It means to specify LAN or WAN or VPN interface for such address. <-D>: It means that such route will be treated as the

	default route.
-d <prefix> <prefix-length>	It means to delete a route. <prefix>: It means to enter the prefix number of IPv6 address. <prefix length>: It means to enter a fixed value as the length of the prefix.
-a <LAN1/LAN2/WAN1/WAN2/ USB1/USB2/VPN1~VPN32>	It means to show the route status. <LAN1/LAN2/WAN1/WAN2/ USB1/USB2/VPN1~VPN32>**:** It means to specify LAN or WAN or VPN interface for such address.
-l	It means to clear the routing table.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN1
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN1

 PREFIX/PREFIX-LEN                          I/F METRIC FLAG NEXT-HOP
-------------------------------------------------------------------------
 ::0.0.0.1/128                              LAN1    0 U ::
 FE80::/128                                 LAN1    0 U ::
 FE80::21D:AAFF:FE00:0/128                  LAN1    0 U ::
 FE80::/64                                  LAN1  256 U ::
 FE80::/16                                  LAN1 1024 UGS
                                            FE80::250:7FFF:FE12:100
 FF00::/8                                   LAN1  256 U ::
```

Telnet Command: ip6 ping

This command allows you to pin an IPv6 address or a host.

Syntax

ip6 ping *<IPv6 address/Host> <LAN1/LAN2/WAN1/WAN2/USB1/USB2> <send count> <data_size>*

Syntax Description

Parameter	Description
<IPV6 address/Host>	It means to specify the IPv6 address or host for ping.
<LAN1/LAN2/WAN1/WAN 2/USB1/USB2>	It means to specify LAN or WAN interface for such address.
<send count>	It means to set the request number of ping. Default number is 5.
<data_size>	It means to set the data size (1 to 1452). <data_size>: Enter a value.

Example

```
> ip6 ping 2001:4860:4860::8888 WAN1

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
```

```
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
>
```

Telnet Command: ip6 tracert

This command allows you to trace the routes from the router to the host.

Syntax

ip6 tracert <*IPV6 address/Host><LAN1/LAN2/WAN1/WAN2/USB1/USB2***>**

Syntax Description

Parameter	Description
<IPV6 address/Host>	It means to specify the IPv6 address or host for ping.
<LAN1/LAN2/WAN1/WAN2/USB1/USB2>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 tracert 2001:4860:4860::8888
traceroute to 2001:4860:4860::8888, 30 hops max through protocol ICMP
  1 2001:5C0:1400:B::10B8    340 ms
  2 2001:4DE0:1000:A22::1    330 ms
  3 2001:4DE0:A::1           330 ms
  4 2001:4DE0:1000:34::1     340 ms
  5 2001:7F8:1: :A501:5169:1 330 ms
  6 2001:4860::1:0:4B3       350 ms
  7 2001:4860::8:0:2DAF      330 ms
  8 2001:4860::2:0:66E       340 ms
  9 Request timed out.          *
 10 2001:4860:4860::8888     350 ms
Trace complete.
>
```

Telnet Command: ip6 tspc

This command allows you to display TSPC status.

Syntax

ip6 tspc <*ifno***>**

Syntax Description

Parameter	Description
<Ifno>	It means the connection interface. Ifno=1 (means WAN1) Ifno=2 (means WAN2)

Example

```
> ip6 tspc 1
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
```

```
Router DNS name : 8886666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net

Status: Connected

>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

Ip6 radvd <*LAN1/LAN2*> <-<*command*> <*parameter*>/ … >

Syntax Description

Parameter	Description
<<*command*> <*parameter*>/…>	The available commands with parameters are listed below. <…> means that you can Enter several commands in one line.
-s <0/1>	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
-D <0/1/2>	It means to set RDNSS Disable/Enable/Deploy (0/1/2) when WAN is up.
-d <lifetme>	It means to set RA default lifetime.
-i <lifetme>	It means to set RA min interval time(sec).
-I <lifetme>	It means to set RA MAX interval time(sec).
-h <hoplimit>	It means to set RA hop limit.
-m <mtu/auto>	It means to set RA MTU, 1280-1500. mtu: auto - auto select MTU from WAN,
-e <time>	It means to set reachable time.
-a <time/infinity>	It means to set retransmit timer /infinity.
-p <0/1/2>	It means to set radvd default preference Low/Medium/High. 0-low 1-medium 2-high
-v	It means to view radvd configuration.
-V	It means to view setting in RA.
-L <time/infinity>	It means to set prefix valid lifetime.
-P <time/infinity>	It means to set prefix preferred lifetime.
-r <num>	It means to to set RA test for item. <num>: 0, 121, 124 0: default, 121: logo 121, 124: logo 124..
-R	It means to reload Config and send RA for subnets.
-u	It means to view MTU on all interfaces.

Example

```
> ip6 radvd LAN1 -V
% [LAN1] setting !
%  Default Lifetime  : 0 seconds
%  min interval time : 200 seconds
%  MAX interval time : 600 seconds
```

```
%   Hop limit          : 64
%   MTU                : 0
%   Reachable time     : 0
%   Retransmit time    : 0
%   Preference         : Medium
```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

Syntax

ip6 mngt *list*

ip6 mngt *list add <Index> <prefix><prefix-length>*

ip6 mngt *list remove <Index>*

ip6 mngt *list flush*

ip6 mngt *status*

ip6 mngt *<internet/ http/telnet/ping/https/ssh/enforce_https> <on/off>*

Syntax Description

Parameter	Description
list	It means to show the setting information of the access list.
status	It means to show the status of IPv6 management.
add <Index> <prefix><prefix-length>	It means to add an IPv6 address which can be used to execute management through Internet. <index>: It means the number (1, 2 and 3) allowed to be configured for IPv6 management. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix.
remove <Index>	It means to remove (delete) the specified index number with IPv6 settings. <index>: It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
flush	It means to clear the IPv6 access table.
status	It means to dispaly current status of IPv6 access list.
<internet/ http/telnet/ping/https/ssh/enforce_https>	These protocols are used for accessing Internet.
<on/off>	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```
> ip6 mngt list add 1 2607:f0d0:1002:51::4 64
> ip6 mngt status
% IPv6 Remote Management :
internet access : off,  telnet : off,   http : off,    https : off,   ssh :
off,     ping : off,    enforce_https : off
> ip6 mngt list
% IPv6 Access List :
Index   IPv6 Prefix    Prefix Length
========================================
1      2607:F0D0:1002:51::4    64
```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 WAN/USB.

Syntax

ip6 *online* <*WAN1/WAN2/USB1/USB2*>

Syntax Description

Parameter	Description
<*WAN1/WAN2/USB1/USB2*>	It means the connection interface.

Example

```
> ip6 online WAN1
% WAN1 online status :
% IPv6 WAN1 Disabled
% Default Gateway : ::
% Interface : DOWN
% UpTime : 0:00:00
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
% MTU Onlink: 1280 , Config MTU : 0
```

Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

Syntax

ip6 aiccu -i <*ifno*> **-r**

ip6 aiccu -i <*ifno*> **-s**

Syntax Description

Parameter	Description
<*Ifno*>	It means the connection interface. 1=WAN1 2=WAN2
-r	It means to remove (delete) the specified index number with IPv6 settings.
-s	It means to display the AICCU status.

Example

```
> ip6 aiccu -i 1 -s
Status: Idle
```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

Syntax

ip6 ntp –h

ip6 ntp –v

ip6 ntp –p <0/1>

Syntax Description

Parameter	Description
–h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 – Auto 1 – First Query IPv6 NTP Server.

Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ip6 lan

This command allows you to set IPv6 settings for LAN interface.

Syntax

ip6 lan -l n <-<*l:w:d:D:m:o:s*> <*parameter*> / … >

Syntax Description

Parameter	Description
–h	It is used to display the usage of such command.
-l <n>	It means to selete LAN interface to be set. n= 1: LAN1 n= 2: LAN2, … x: LANx. Default is LAN1
-w <n>	It means to selete WAN interface to be primary interface. n= 0: None, n=1: WAN1 , n=2: WAN2, … x: WANx.
-d <server>	It means to set 1st DNS Server IP. <server>: Enter the IPv6 Address.
-D <server>	It means to set 2nd DNS Server IP. <server>: Enter the IPv6 Address.
-m <n>	It means to set ipv6 LAN management. n=0:OFF n=1:SLAAC. Default is SLAAC n=2:DHCPv6
-o <n>	It means to enable Other option(O-bit) flag. (O-bit is redundant when management is DHCPv6) n=0: Disable n=1: Enable.
-e <n>	It means to add an extension WAN. n: 1: WAN1, 2: WAN2, … x: WANx.
-E <n>	It means to delete an extension WAN. n: 1: WAN1 ,2: WAN2, … x: WANx.
-b <map>	It means to set bit map(decimal) for extension WAN. <map>: 0: WAN1; 1: WAN2, … n: WAN(n+1).
-f <n>	It means to disable IPv6. n=1: Disable IPv6, n=0: Enable IPv6.
-R <n>	It means to enable /disable RIPng. n=1: Enable RIPng, n=0: Disable RIPng.
-s <n>	It means to show IPv6 LAN setting. n=0:show all. Default is show all.

	n=1: LAN1 n=2: LAN2, n=3: DMZ.

Example

```
> ip6 lan -l 1 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
%   Set primary WAN1!

%  Set 1st DNS server 2001:4860:4860::8888

%   Set Other Option Enable!

%   [LAN1] support ipv6!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

% [LAN2] setting:
%  Primary WAN    : WAN1
%  Management     : SLAAC
%  Other Option   : Disable
%  WAN Exten      : None
%  Subnet ID      : 2
%  Static IP(0)   : ::/0
%                 [ifno: 0, enable: 0]
%  Static IP(1)   : ::/0
%                 [ifno: 0, enable: 0]
%  Static IP(2)   : ::/0
%                 [ifno: 0, enable: 0]
%  Static IP(3)   : ::/0
%                 [ifno: 0, enable: 0]
%  DNS1           : 2001:4860:4860::8888
%  DNS2           : 2001:4860:4860::8844
%  ULA Type       : OFF
%  RIPng          : Enable
```

Telnet Command: ip6 session

This command allows you to set sessions limit for IPv6 address.

Syntax

ip6 session *on*

ip6 session *off*

ip6 session *default <num>*

ip6 session *status*

ip6 session *show*

ip6 session *add <P1-IP2><num>*

ip6 session *del <P1>/<all>*

Syntax Description

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default <num>	It means to set the default number of session num limit. <num>: Enter a number.
status	It means to display the current settings.
show	It means to display all IP range session limit settings.
add <P1-IP2><num>	<add/del>*:* It means to add the session limit for an IPv6

	range. <IP1-IP2> : Specify a range for IPv6 addresses. <num>: Enter a number.
del<IP1> /all	<del>*:* It means to delete the session limit for an IPv6 range. <IP1> : Specify the first IPv6 address within the IPv6 range. all: Delete all the session limits.

Example

```
> ip6 session on
> ip6 session add 2100:ABCD::2-2100:ABCD::10 100
> ip6 session status

  IPv6 range:
    2100:ABCD::2 - 2100:ABCD::10 : 100

  Current ip6 session limit is turn on

  Current default session number is 100
```

Telnet Command: ip6 bandwidth

This command allows you to set IPv6 settings

Syntax

ip6 bandwidth *on*

ip6 bandwidth *off*

ip6 bandwidth *default <tx_rate> <rx_rate>*

ip6 bandwidth *status*

ip6 bandwidth *show*

ip6 bandwidth *add <IP1-IP2> <tx><rx><shared>*

ip6 bandwidth *del <IP1> /all*

Syntax Description

Parameter	Description
on	It means to turn on bandwidth limit for each IP.
off	It means to turn off bandwidth limit for each IP.
default <tx_rate> <rx_rate>	It means to set the default transmission (tx), receiving (rx) rate of bandwidth limit (0-30000 Kbps/Mbps). <tx_rate>: Enter a number. <rx_rate>: Enter a number.
status	It means to display the current settings.
show	It means to display all IP range bandwidth limit settings.
add <IP1-IP2> <tx><rx><shared>	<add>: It means to add the bandwidth limit for an IPv6 range. <del>: It means to delete the bandwidth limit for an IPv6 range by first IP (IP1) or 'del all'. <IP1-IP2> - Specify a range for IPv6 addresses. <tx><rx>: It means the bandwidth limit for transmission and receivign rate. <shared>: It means the bandwidth will be shared for the IPv6 range.
del <IP1> /all	It means to delete the bandwidth limit for an IPv6 range by first IP (IP1) or 'del all'.

	<IP1> - Specify a range for IPv6 addresses. all: Delete all the bandwidth limits.

Example

```
> ip6 bandwidth on
> ip6 bandwidth add 2001:ABCD::2-2001:ABCD::10 512 5M shared
> ip6 bandwidth status

  IPv6 range:
    2001:ABCD::2 - 2001:ABCD::10 : Tx:512K Rx:5M shared

  Current ip6 Bandwidth limit is turn on


  Current default ip6 Bandwidth rate is Tx:2000K Rx:8000K bps
> ip6 bandwidth del 2001:ABCD::2
>
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

Syntax

ipf view <*-command/…*>

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-c	It means to show the running call filter rules.
-d	It means to show the running data filter rules.
-h	It means to show the hit-number of the filter rules.
-r	It means to show the running call and data filter rules.
-t	It means to display all the information at one time.
-z	It means to clear a filter rule's statistics.
-Z	It means to clear IP filter's gross statistics.

Example

```
> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available
```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

Syntax

ipf flowtrack set *-r*

ipf flowtrack set *-e*

ipf flowtrack view *-f*

ipf flowtrack view *-b*

ipf flowtrack view *-i <IP address> -p<value> -t<value> -f*

Syntax Description

Parameter	Description
-r	It means to refresh the flowtrack.
-e	It means to enable or disable the flowtrack.
-f	It means to show the sessions state of flowtrack. If you do not specify any IP address, then all the session state of flowtrack will be displayed.
-b	It means to show all of IP sessions state.
view -i <IP address> -p<port> -t <protocol> -f	It means to show sessions state of flowtrack by specifying IP address (e.g,, -i 192.168.2.55). <IP address>: Enter an IP address. <port>: Enter a number (0 ~ 65535). <protocol>: Enter tcp, udp or icmp.

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>>  192.168.1.11:59939 ->       8.8.8.8:   53 ,ifno=0
REPLY >>      8.8.8.8:   53 ->   192.168.1.11:59939 ,ifno=3
      proto=17, age=93023180(3920), flag=203
ORIGIN>>  192.168.1.11:15073 ->       8.8.8.8:   53 ,ifno=0
REPLY >>      8.8.8.8:   53 ->   192.168.1.11:15073 ,ifno=3
      proto=17, age=93025100(2000), flag=203
ORIGIN>>  192.168.1.11: 7247 ->       8.8.8.8:   53 ,ifno=0
REPLY >>      8.8.8.8:   53 ->   192.168.1.11: 7247 ,ifno=3
      proto=17, age=93020100(7000), flag=203
End to show the flowtrack sessions state
> ipf flowtrack set -e
Current flow_enable=0
> ipf flowtrack set -e
Curretn flow_enable=1
```

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

Syntax

log *-<c/f/h/i/p/t/w/x> -F <a/c/f/w>*

Syntax Description

Parameter	Description

-c	It means to show the latest call log.
-f	It means to show the IP filter log.
-h	It means to show this usage help.
-p	It means to show PPP/MP log.
-t	It means to show all logs saved in the log buffer.
-w	It means to show WAN log.
-x	It means to show packet body hex dump.
-F <a/c/f/w>	It means to show the flush log buffer. a: flush all logs c: flush the call log f: flush the IP filter log w: flush the WAN log

Example

```
> log -w
0:00:05    DSL: DSL Channel = 0
0:00:05    DSL: VPI/VCI = 0/33
0:00:05    DSL: Mode = 1[PPPoE]
0:00:05    DSL: Encapsulation type = 1[LLC]
0:00:05    DSL: Modulation type = 4[MULTI]
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

Syntax

mngt ftpport <*FTP port***>**

Syntax Description

Parameter	Description
<FTP port>	<FTP port>: Enter the number of FTP port. The default setting is 21.

Example

```
> mngt ftpport 21
% Set FTP server port to 21 done.
```

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

Syntax

mngt httpport *<http port>*

Syntax Description

Parameter	Description
<http port>	<http port>: Enter the number of HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

Syntax

mngt httpsport *<https port>*

Syntax Description

Parameter	Description
<https port>	<https port>: Enter the number for HTTPS port. The default setting is 443.

Example

```
> mngt httpsport 443
% Set web server port to 443 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

Syntax

mngt telnetport <*telnet port***>**

Syntax Description

Parameter	Description
<telnet port>	**<**telnet port>: Enter the number for telnet port. The default setting is 23.

Example

```
> mngt telnetport 23
% Set Telnet server port to 23 done.
```

Telnet Command: mngt sshport

This command allows users to set SSH port for management.

Syntax

mngt sshport <*ssh port***>**

Syntax Description

Parameter	Description
<ssh port>	<ssh port>: Enter the number for SSH port. The default setting is 22.

Example

```
> mngt sshport 23
% Set ssh port to 23 done.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

Syntax

mngt noping *on*

mngt noping *off*

mngt noping *viewlog*

mngt noping *clearlog*

Syntax Description

Parameter	Description
on	All PING packets will be forwarded from LAN PC to Internet.
off	All PING packets will be blocked from LAN PC to Internet.
viewlog	It means to display a log of ping action, including source MAC and source IP.
clearlog	It means to clear the log of ping action.

Example

```
> mngt noping off
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

Syntax

mngt defenseworm *on*

mngt defenseworm *off*

mngt defenseworm *add <port>*

mngt defenseworm *del <port>*

mngt defenseworm *viewlog*

mngt defenseworm *clearlog*

Syntax Description

Parameter	Description
on	It means to activate the function of defense worm packet out.
off	It means to inactivate the function of defense worm packet out.
add <port>	It means to add a new TCP port for block. <port>: Enter a port number.
del <port>	It means to delete a TCP port for block.

	<port>: Enter a port number.
viewlog	It means to display a log of defense worm packet, including source MAC and source IP.
clearlog	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Delete TCP port 21
Block TCP port list: 135, 137, 138, 139, 445
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

Syntax

mngt rmtcfg *status*

mngt rmtcfg *enable*

mngt rmtcfg *disable*

mngt rmtcfg <*http/https/ftp/telnet/ssh/tr069/enforce_https*> <*on/off*>

Syntax Description

Parameter	Description
status	It means to display current setting for your reference.
enable	It means to allow the system administrators to login from the Internet.
disable	It means to deny the system administrators to login from the Internet.
<*http/https/ftp/telnet/ssh/tr069/enforce_https*> <*on/off*>	It means to specify one of the servers/protocols for enabling or disabling. <on> – enable the function. <off> – disable the function.

Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

Syntax

mngt lanaccess *-e <0/1> –s <value>–i <value>*

mngt lanaccess *–f*

mngt lanaccess *–d*

mngt lanaccess *–v*

mngt lanaccess *–h*

Syntax Description

Parameter	Description
-e <0/1> –s <value> –i <value>	-e: It means to enable/disable the function. <0/1>: Enter 0 or 1. 0,disable the function; 1, enable the function. –s <value>: It means to specify service offered. Enter FTP, HTTP, HTTPS, TELNET, SSH, None, or All. –i <value>: It means the interface which is allowed to access. Enter LAN2~LAN4, IP Routed Subnet, None, or All **Note**: LAN1 is always allowed for accessing into the router.
-f	It means to flush all of the settings.
-d	It means to restore the factory default settings.
-v	It means to view current settings.
-h	It means to get the usage of such command.

Example

```
> mngt lanaccess -e 1
> mngt lanaccess -s FTP,TELNET
> mngt lanaccess -i LAN3
> mngt lanaccess -v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
   - FTP:Yes
   - HTTP:No
   - HTTPS:No
   - TELNET:Yes
   - SSH:No
   - TR069:No
   - Enforce HTTPS:No
* Subnet:
   - LAN 1: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 2: enabled
     - Specific IP(IP object:0) is disabled
   - IP Routed Subnet: enabled
     - Specific IP(IP object:0) is disabled
```

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

Syntax

mngt echoicmp *enable*

mngt echoicmp *disable*

Syntax Description

Parameter	Description
enable	It means to accept the echo ICMP packet.
disable	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

Syntax

mngt accesslist *list*

mngt accesslist *add <index><IP addr><mask>*

mngt accesslist *remove <index>*

mngt accesslist *flush*

Syntax Description

Parameter	Description
list	It can display current setting for your reference.
add <index><IP addr><mask>	It means adding a new entry. <index>: Enter an index number of the entry. <IP addr>: Enter an IP address. <mask>: Enter the mask address.
remove <index>	It means to delete the selected item. <index>: Enter an index number of the entry.
flush	It means to remove all the settings in the access list.

Example

```
DrayTek> mngt accesslist add 2 192.168.2.76 255.255.255.0
%% Set OK.
> mngt accesslist list
DrayTek> mngt accesslist list
%% Access list :
  Index IP address     Subnet mask
========================================
  2    192.168.2.76    255.255.255.0
>
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

Syntax

mngt snmp -<*command*> <*parameter*> / ...

Syntax Description

Parameter	Description
<*command*> <*parameter*>/...	The available commands with parameters are listed below. *[...]* means that you can Enter several commands in one line.
-e <1/2>	1: Enable the SNMP function. 2: Disable the SNMP function.
-g <Community name>	It means to set the name for getting community by typing a proper character. (max. 23 characters) <Community name>: Enter a string.
-s <Community name>	It means to set community by typing a proper name. (max. 23 characters) <Community name>: Enter a string.
-m <IP address>	It means to set one host as the manager to execute SNMP function. Please Enter IPv4 address to specify certain host. <IP address>: Enter an IP address, or IP address with subnet, or manager host IP. Three IP addresses can be entered and separated by ','.
-t <Community name>	It means to set trap community by typing a proper name. (max. 23 characters) <Community name>: Enter a string.
-n <IP address>	It means to set the IPv4 address of the host that will receive the trap community. <IP address>: Enter an IP address, or IP address with subnet, or manager host IP. Two IP addresses can be entered and separated by ','.
-T <seconds>	It means to set the trap timeout. <seconds>: Enter a value (0~999)
-V	It means to list SNMP setting.

Example

```
> mngt snmp -e 1 -g draytek -s DK -m
192.168.1.20,192.168.5.192/26,10.20.3.40/24 -t trapcom -n
192.168.1.20,10.20.3.40 -T 88
 SNMP Agent Turn on!!!
 Get Community set to draytek
 Set Community set to DK
 Manager Host IP set to 192.168.1.20,192.168.5.192/26,10.20.3.40/24
 Trap Community set to trapcom
 Notification Host IP set to 192.168.1.20,10.20.3.40
 Trap Timeout set to 88 seconds
>
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

Syntax

msubnet switch *<2> <On/Off>*

Syntax Description

Parameter	Description
<2>	It means LAN interface. 2=LAN2
<On/Off>	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msubnet switch 2 On
% LAN2       Subnet On!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet addr

This command is used to configure IP address for the specified LAN interface.

Syntax

msubnet addr *<2><IP address>*

Syntax Description

Parameter	Description
<2>	It means LAN interface.
<IP address>	Enter the private IP address for the specified LAN interface.

Example

```
> msubnet addr 2 192.168.5.1
% Set LAN2 subnet IP address done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nmask

This command is used to configure net mask address for the specified LAN interface.

Syntax

msubnet nmask *<2><IP address>*

Syntax Description

Parameter	Description

<2>	It means LAN interface.
<IP address>	Enter the subnet mask address for the specified LAN interface.

Example

```
> msubnet nmask 2 255.255.0.0
% Set LAN2 subnet mask done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet status

This command is used to display current status of subnet.

Syntax

msubnet status *<2>*

Syntax Description

Parameter	Description
<2>	It means LAN interface.

Example

```
> msubnet status 2
% LAN2       Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

Syntax

msubnet dhcps *<2>* *<On/Off>*

Syntax Description

Parameter	Description
<2>	It means LAN interface.
<On/Off>	On means enabling the DHCP server for the specified LAN interface. Off means disabling the DHCP server.

Example

```
> msubnet dhcps 3 off
% LAN3       Subnet DHCP Server disabled!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

Syntax

msubnet nat *<2> <On/Off>*

Syntax Description

Parameter	Description
<2>	It means LAN interface.
<On/Off>	On – It means the subnet will be configured for NAT usage. Off **-** It means the subnet will be configured for Routing usage.

Example

```
> > msubnet nat 2 off
% LAN2 Subnet is for Routing usage!
%Note: If you have multiple WAN connections, please be reminded to setup a
Load-Balance policy so that packets from this subnet will be forwarded to the
right WAN interface!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet gateway

This command is used to configure an IP address as the gateway used for subnet.

Syntax

msubnet gateway *<2><Gateway IP>*

Syntax Description

Parameter	Description
<2>	It means LAN interface.
<Gateway IP>	Specify an IP address as the gateway IP.

Example

```
> msubnet gateway 2 192.168.1.13
% Set LAN2 Dhcp Gateway IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet ipcnt

This command is used to defined the total number allowed for each LAN interface.

Syntax

msubnet ipcnt *<2><IP counts>*

Syntax Description

Parameter	Description
<2>	It means LAN interface.
<IP counts>	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

Syntax

msubnet talk *<1/2> <1/2> <On/Off>*

Syntax Description

Parameter	Description
<1/2><1/2>	It means LAN interface. 1: LAN1 2: LAN2
<On/Off>	On: It means to establish a route. Off**:** It means Not to establish a route.

Example

```
> msubnet talk 1 2 on
> msubnet talk 1 2 on
% Enable routing between LAN1 and LAN2!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> msubnet talk
% msubnet talk <1/2> <1/2> <On/Off>
% where 1:LAN1, 2:LAN2
% Now:
%            LAN1   LAN2
% LAN1         V
% LAN2         V     V
DrayTek>
>
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

msubnet startip *<2><Gateway IP>*

Syntax Description

Parameter	Description
<2>	It means LAN interface. 2: LAN2
<Gateway IP>	Type an IP address as the starting IP address for a subnet.

Example

```
> msubnet startip 2 192.168.2.90
%Set LAN2 Dhcp Start IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> msubnet startip ?
% msubnet startip <2/3/4> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10; LAN5
192.168.5.1
0; LAN6 192.168.6.10
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

msubnet pppip *<2><Start IP>*

Syntax Description

Parameter	Description
<2>	It means LAN interface. 2: LAN2
<Start IP>	Type an IP address as the starting IP address for PPP connection.

Example

```
> msubnet pppip 2 192.168.2.250
% Set LAN2 PPP(IPCP) Start IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router

> msubnet pppip
% msubnet pppip <2> <Start IP>
% Now: LAN2 192.168.2.250

>
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

msubnet nodetype *<2><count>*

Syntax Description

Parameter	Description
<*2*>	It means LAN interface. 2=LAN2
<*count*>	Choose the following number for specifying different node type. 1: B-node 2: P-node 4: M-node 8: H-node 0: Not specify any type for node.

Example

```
> msubnet nodetype 2 1
% Set LAN2 Dhcp Node Type done !!!

> msubnet nodetype
% msubnet nodetype <2> <count>
% Now: LAN2 1

% count: 1. B-node 2. P-node 4. M-node 8. H-node
```

Telnet Command: msubnet primWINS

This command is used to configure primary WINS server.

Syntax

msubnet primWINS <*2*><*WINS IP*>

Syntax Description

Parameter	Description
<*2*>	It means LAN interface. 2:LAN2
<*WINS IP*>	Enter the IP address as the WINS IP.

Example

```
> msubnet primWINS ?
% msubnet primWINS <2> <WINS IP>
% Now: LAN2 0.0.0.0
> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS
% msubnet primWINS <2> <WINS IP>
% Now: LAN2 192.168.3.5
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

Syntax

msubnet secWINS *<2><WINS IP>*

Syntax Description

Parameter	Description
<2>	It means LAN interface. 2:LAN2
<WINS IP>	Enter the IP address as the WINS IP.

Example

```
> msubnet secWINS 2 192.168.3.89
% Set LAN2 Dhcp Secondary WINS IP done !!!

> msubnet secWINS
% msubnet secWINS <2> <WINS IP>
% Now: LAN2 192.168.3.89
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

Syntax

msubnet tftp *<2><TFTP server name>*

Syntax Description

Parameter	Description
<2>	It means LAN interface. 2:LAN2
<TFTP server name>	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp ?
% msubnet tftp <2> <TFTP server name>
% Now: LAN2

> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

>  msubnet tftp
% msubnet tftp <2> <TFTP server name>
% Now: LAN2 publish
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/DMZ/IP Routed Subnet.

Syntax

msubnet mtu <*interface*> <*value*>

Syntax Description

Parameter	Description
<*interface*>	Available settings include LAN1~LAN2, IP_Routed_Subnet.
<*value*>	<value>: Enter a number (1000 ~ 1500(Bytes)). Default value is 1500.

Example

```
> msubnet mtu LAN1 1492
 Set LAN1 subnet mtu as 1492
> msubnet mtu
Usage:

  >msubnet mtu <interface> <value>

  <interface>: LAN1~LAN2,IP_Routed_Subnet,  <value>:    1000 ~ 1500 (Bytes),
de
fault: 1500 (Bytes)

  e.x: >msubnet mtu LAN1 1492

Current Settings:

   LAN1 MTU:               1492 (Bytes)
   LAN2 MTU:               1500 (Bytes)
   IP Routed Subnet MTU:   1500 (Bytes)
```

Telnet Command: msubnet leasetime

This command allows you to configure lease time for LAN interface.

Syntax

msubnet leasetime <*1/2*> <*Lease Time <sec.>*>

Syntax Description

Parameter	Description
<*1/2*>	Available settings include 1: LAN1 2: LAN2
<*Lease Time <sec.>*>	<lease time>: Enter a number (10 ~ 2592000). Default value is 86400.

Example

```
> msubnet leasetime 1 3000000
% Invalid lease time input (Valid:  10 to 2592000 ) !!!
% Now: 86400

> msubnet leasetime 1 92000
% Set LAN1 lease time: 92000
```

```
>
```

Telnet Command: object ip obj

This command is used to create an IP object profile.

Syntax

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

object ip obj I*NDEX -a TYPE <START_IP><END/MASK_IP>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified object profile. INDEX: Enter the index number of the specified group profile. Example: *object ip obj 1 -v*
INDEX -n NAME	It means to define a name for the IP object. INDEX: Enter the index number of the specified group profile. NAME: Enter a name with less than 15 characters. Example: *object ip obj 9 -n bruce*
INDEX -i INTERFACE	It means to define an interface for the IP object. INDEX: Enter the index number of the specified group profile. INTERFACE: Enter 0, 1, 3 0, means any 1, means LAN 3, means WAN Example: *object ip obj 8 -i 0*
INDEX -s INVERT	It means to set invert seletion for the object profile. INDEX: Enter the index number of the specified group profile. INVERT: Enter 0, 1 0, means disableing the function. 1, means enabling the function. Example: *object ip obj 3 -s 1*
INDEX -a TYPE <START_IP> <END/MASK_IP>	It means to set the address type and IP for the IP object profile. INDEX: Enter the index number of the specified group profile. TYPE: Enter 0, 1, 2, 3 or 4 0, means Mask 1, means Single 2, means Any 3, means Rang 4, means Mac Example: *object ip obj 3 -a 2* <START_IP>: When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as

	end point. <END/MASK_IP>: Enter an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
OK.

> object ip obj 1 -a 1 192.168.1.45
OK.

> object ip obj 1 -v
 IP Object Profile 1
 Name   :[marketing]
 Interface:[Any]
 Address type:[single]
 Start ip address:[192.168.1.45]
 End/Mask ip address:[0.0.0.0]
 MAC Address:[00:00:00:00:00:00]
 Invert Selection:[0]
```

Telnet Command: object ip grp

This command is used to integrate several IP objects under an IP group profile.

Syntax

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified group profile. INDEX: Enter the index number of the specified group profile. Example: *object ip grp 1 -v*
INDEX -n NAME	It means to define a name for the IP group. INDEX: Enter the index number of the specified group profile. NAME: Type a name with less than 15 characters. Example: *object ip grp 8 -n bruce*
INDEX -i INTERFACE	It means to define an interface for the IP group. INDEX: Enter the index number of the specified group profile. INTERFACE: Enter 0, 1 or 3 0, means any 1, means LAN 3, means WAN Example: *object ip grp 3 -i 0*
INDEX -a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile. INDEX: Enter the index number of the specified group

	profile. IP_OBJ_INDEX: Enter the index number of object profiles. Example: :*object ip grp 3 -a 1 2 3 4 5* The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
> object ip grp 2 -n First
 IP Group Profile 2
 Name   :[First]
 Interface:[Any]
 Included ip object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
 [8:][0]
 [9:][0]
 [10:][0]
 [11:][0]
> object ip grp 2 -a 1 2
 IP Group Profile 2
 Name   :[First]
 Interface:[Lan]
 Included ip object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
 [8:][0]
 [9:][0]
 [10:][0]
 [11:][0]

Set ok!
```

Telnet Command: object ipv6 obj

This comman is used to create an IPv6 object profile.

Syntax

object ipv6 obj *setdefault*

object ipv6 obj *INDEX -v*

object ipv6 obj *INDEX -n NAME*

object ipv6 obj *INDEX -s INVERT*

object ipv6 obj *INDEX -e MATCH_TYPE*

object ipv6 obj *INDEX -a TYPE <START_IP> <END_IP>/<Prefix Length>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified object profile. INDEX: Enter the index number of the specified object profile. Example: *object ipv6 obj 1 -v*
INDEX -n NAME	It means to define a name for the IPv6 object. NAME: Type a name with less than 15 characters. Example: *object ipv6 obj 9 -n bruce*
INDEX -s INVERT	It means to set invert seletion for the object profile. INVERT: Enter 0 or 1. 0, means disableing the function. 1, means enabling the function. Example: *object ipv6 obj 3 -s 1*
INDEX -e MATCH_TYPE	It means to set the match type of ipv6 object profile. MATCH_TYPE: Enter 0 or 1. 0:128 Bits, 1:Suffix 64 Bits Interface ID
INDEX -a TYPE <START_IP> <END_IP>/<Prefix Length>	It means to set the address type for the IPv6 object profile. TYPE: Enter 0, 1, 2, 3, or 4 0, means Mask 1, means Single 2, means Any 3, means Rang 4, means Mac Example: *object ipv6 obj 3 -a 2* <*START_IP*>: When the TYPE is set with 2, you have to type an IPv6 address as a starting point and another IP address as end point. Enter an IPv6 address as the starting point. <*END_IP*>/ <*Prefix Length*>*:* Enter an IPv6 address (different with START_IP) as the end IPv6 address or the prefix length of the IPv6 address.

Example

```
> object ipv6 obj 9 -n bruce
Setting saved.

> object ipv6 obj 3 -s 1
Setting saved.
```

```
> object ipv6 obj 3 -e 1
You can not set 64 bits Interface ID for Subnet type.

Setting saved.

> object ipv6 obj 3 -a 3 2607:f0d0:1002:51::4 2607:f0d0:1002:51::4
Setting saved.

> object ipv6 obj 3 -v
 IPv6 Object Profile 3
 Name   :[]
 Address Type:[range]
 Start IPv6 Address:[2607:F0D0:1002:51::4]
 End IPv6 Address:[2607:F0D0:1002:51::4]
 Prefix Length:[0]
 MAC Address:[00:00:00:00:00:00]
 Invert Selection:[0]
 Match Type:[0]
```

Telnet Command: object ipv6 grp

This command is used to integrate several IPv6 objects under an IPv6 group profile.

Syntax

object ipv6 grp *setdefault*

object ipv6 grp *INDEX -v*

object ipv6 grp *INDEX -n NAME*

object ipv6 grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified group profile. INDEX*:* Enter the index number of the specified group profile. Example: *object ipv6 grp 1 -v*
INDEX -n NAME	It means to define a name for the IPv6 group. INDEX*:* Enter the index number of the specified group profile. NAME: Type a name with less than 15 characters. Example: *object ipv6 grp 8 -n bruce*
INDEX -a IP_OBJ_INDEX	It means to specify IPv6 object profiles for the group profile. INDEX: Enter the index number of the specified group profile. IP_OBJ_INDEX: Enter the index number of object profiles. Example: :*object ipv6 grp 3 -a 1 2 3 4 5* The IPv6 object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
> object ipv6 grp 8 -n bruce
IPv6 Group Profile 8
 Name   :[bruce]
 Included ip object index:
```

```
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
> object ipv6 grp 8 -a 1 2 3 4 5
IPv6 Group Profile 8
 Name   :[bruce]
 Included ip object index:
 [0:][1]
 [1:][2]
 [2:][3]
 [3:][4]
 [4:][5]
 [5:][0]
 [6:][0]
 [7:][0]
```

Telnet Command: object service obj

This command is used to create service object profile.

Syntax

object service obj *setdefault*

object service obj *INDEX -v*

object service obj *INDEX -n NAME*

object service obj *INDEX -p PROTOCOL*

object service obj *INDEX -s CHK <START_P><END_P>*

object service obj *INDEX -d CHK <START_P><END_P>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified service object profile. INDEX: Enter the index number of the specified service object profile. Example: *object service obj 1 -v*
INDEX -n NAME	It means to define a name for the IP object. INDEX: Enter the index number of the specified service object profile. NAME: Type a name with less than 15 characters. Example: *object service obj 9 -n bruce*
INDEX -p PROTOCOL	It means to define a PROTOCOL for the service object profile. INDEX: Enter the index number of the specified service object profile. PROTOCOL: Enter 0, 1, 2, 6, 17, 58, 255, others 0, means any 1, means ICMP 2, means IGMP 6, means TCP 17, means UDP

	58, means ICMPv6 255, means TCP/UDP Other values mean other protocols. Example: *object service obj 8 -p 1*
INDEX -s CHK <START_P><END_P>	It means to set source port check and configure port range (1~65565) for TCP/UDP. INDEX: Enter the index number of the specified service object profile. CHK: Enter 0, 1, 2, or 3 0, means equal**(=)**, when the starting port and ending port values are the same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type. 1, means not equal**(!=)**, when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type. 2, means larger**(>)**, the port number greater than this value is available. 3, means less**(<)**, the port number less than this value is available for this profile. <START_P>: Enter a number as starting port number. <END_P>: Enter a port number as the eding port number. Example: *object service obj 3 -s 0 100 200*
INDEX -d CHK <START_P><END_P>	It means to set destination port check and configure port range (1~65565) for TCP/UDP. INDEX: Enter the index number of the specified service object profile. CHK: Enter 0, 1, 2, or 3 0, means equal**(=)**, when the starting port and ending port values are the same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type. 1, means not equal**(!=)**, when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type. 2, means larger**(>)**, the port number greater than this value is available. 3, means less**(<)**, the port number less than this value is available for this profile. <START_P>: Enter a number as starting port number. <END_P>: Enter a port number as the eding port number. Example: *object service obj 3 -d 1 100 200*

Example

```
> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
Service Object Profile 1
 Name   :[limit]
```

```
 Protocol:[TCP/UDP]
 Source port check action:[!=]
 Source port range:[120~240]
 Destination port check action:[!=]
 Destination port range:[200~220]
>
```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

object service grp setdefault

object service grp *INDEX –v*

object service grp *INDEX –n NAME*

object service grp *INDEX –a SER_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified service group profile. INDEX: Enter the index number of the specified group profile. Example: *object service grp 1 –v*
INDEX -n NAME	It means to define a name for the service group. INDEX: Enter the index number of the specified service group profile. NAME: Type a name with less than 15 characters. Example: *object service grp 8 –n bruce*
INDEX -a SER_OBJ_INDEX	It means to specify service object profiles for the group profile. INDEX: Enter the index number of the specified service group profile. SER_OBJ_INDEX: Enter the index number of the service object profile. Example: *:object service grp 3 –a 1 2 3 4 5* The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
> object service grp 1 -n group_1
 Service Group Profile 1
 Name   :[group_1]
 Included service object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
>object service grp 1 –a 1 2
 Service Group Profile 1
```

```
Name   :[Grope_1]
Included service object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

Syntax

object kw obj setdefault

object kw obj show

object kw obj show PAGE

object kw obj *INDEX –v*

object kw obj *INDEX –n NAME*

object kw obj *INDEX –a CONTENTS*

object kw obj *INDEX -c*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
show	It means to show the contents for all of the profiles.
show PAGE	It means to show the contents of the specified profile. PAGE: Enter the page number.
INDEX -v	It means to view the information of the specified keyword profile. INDEX: Enter the index number of the specified keyword profile.
INDEX -n NAME	It means to define a name for the keyword profile. INDEX: Enter the index number of the specified keyword profile. NAME: Enter a name with less than 15 characters as the keyword profile.
INDEX -a CONTENTS	It means to set the contents for the keyword profile. INDEX: Enter the index number of the specified keyword profile. CONTENTS: Enter a string as the content of the keyword profile. Example: *object kw obj 40 –a test*
INDEX -c	It means to clear the contents of keyword object profile. INDEX: Enter the index number of the specified keyword profile.

Example

```
> object kw obj 1 -n children
 Profile 1
 Name   :[children]
 Content:[]
```

```
> object kw obj 1 -a gambling
 Profile 1
 Name   :[children]
 Content:[gambling]

> object kw obj 1 -v
 Profile 1
 Name   :[children]
 Content:[gambling]
```

Telnet Command: object fe

This command is used to create File Extension Object profile.

Syntax

object fe show

object fe setdefault

object fe obj *INDEX -v*

object fe obj *INDEX -n NAME*

object fe obj *INDEX -e CATEGORY|FILE_EXTENSION*

object fe obj *INDEX -d CATEGORY|FILE_EXTENSION*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified file extension object profile. INDEX: Enter the index number (from 1 to 8) of the specified file extension object profile.
INDEX -n NAME	It means to define a name for the file extension object profile. INDEX: Enter the index number (from 1 to 8) of the specified file extension object profile. NAME: Type a name with less than 15 characters.
INDEX -e CATEGORY|FILE_EXTENSION	It means to enable the specific CATEGORY or FILE_EXTENSION. INDEX: Enter the index number (from 1 to 8) of the specified file extension object profile. CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Executation Example: *object fe obj 1 -e Image* FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".flv", ".swf", ".aac", ".aiff" ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole", ".tlb", ".viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr", ".torrent" Example: *object fe obj 1 -e .bmp*
INDEX -d	It means to disable the specific CATEGORY or

CATEGORY|FILE_EXTENSION	FILE_EXTENSION. INDEX: Enter the index number (from 1 to 8) of the specified file extension object profile. CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Executation Example: *object fe obj 1 -e Image* FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".flv", ".swf", ".aac", ".aiff" ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole", ".tlb", ".viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr", ".torrent" Example: *object fe obj 1 -e .bmp*

Example

```
> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]

-------------------------------------------------------------------------
Image category:
 [ ].bmp   [ ].dib   [ ].gif   [ ].jpeg  [ ].jpg   [ ].jpg2  [ ].jp2   [ ].pct
 [ ].pcx   [ ].pic   [ ].pict  [ ].png   [ ].tif   [ ].tiff
-------------------------------------------------------------------------
Video category:
 [ ].asf   [ ].avi   [ ].mov   [ ].mpe   [ ].mpeg  [ ].mpg   [v].mp4   [ ].qt
 [ ].rm    [v].wmv   [ ].3gp   [ ].3gpp  [ ].3gpp2 [ ].3g2
-------------------------------------------------------------------------
Audio category:
 [v].aac   [v].aiff  [v].au    [v].mp3   [v].m4a   [v].m4p   [v].ogg   [v].ra
 [v].ram   [v].vox   [v].wav   [v].wma
-------------------------------------------------------------------------
Java category:
 [ ].class [ ].jad   [ ].jar   [ ].jav   [ ].java  [ ].jcm   [ ].js    [ ].jse
 [ ].jsp   [ ].jtk
-------------------------------------------------------------------------
ActiveX category:
 [ ].alx   [ ].apb   [ ].axs   [ ].ocx   [ ].olb   [ ].ole   [ ].tlb   [ ].viv
 [ ].vrm
-------------------------------------------------------------------------
Compression category:
 [ ].ace   [ ].arj   [ ].bzip2 [ ].bz2   [ ].cab   [ ].gz    [ ].gzip  [ ].rar
 [ ].sit   [ ].zip
-------------------------------------------------------------------------
Executation category:
 [ ].bas   [ ].bat   [ ].com   [ ].exe   [ ].inf   [ ].pif   [ ].reg   [ ].scr
```

Telnet Command: object sms

This command is used to create short message object profile.

Syntax

object sms show

object sms setdefault

object sms obj *INDEX -v*

object sms obj *INDEX -n NAME*

object sms obj *INDEX -s Service Provider*

object sms obj *INDEX -u Username*

object sms obj *INDEX -p Password*

object sms obj *INDEX -q Quota*

object sms obj *INDEX -i Interval*

object sms obj *INDEX -l URL*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified SMS object profile. INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile.
INDEX -n NAME	It means to define a name for the SMS object profile. INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile. NAME: Enter a name with less than 15 characters as SMS object profile name.
INDEX -s Service Provider	It means to specify the number of the service provider which offers the service of SMS. Different numbers represent different service provider. INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile. Service Provider: Enter 0, 2, 4, 5, 6, 7, 8, 9,10, 11, 12, 13 or 14 0 : kotsms.com.tw (TW) 2 : textmarketer.co.uk (UK) 4 : messagemedia.co.uk (UK) 5 : bulksms.com (INT) 6 : bulksms.co.uk (UK) 7 : bulksms.2way.co.za (ZA) 8 : bulksms.com.es (ES) 9 : usa.bulksms.com (US) 10 : bulksms.de (DE) 11 : www.pswin.com (EU) 12 : www.messagebird.com (EU) 13 : www.lusosms.com (EU) 14 : www.vibeactivemedia.com (UK)
INDEX -u Username	It means to define a user name for the SMS object profile. INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile. Username: Enter a user name that the sender can use to register to selected SMS provider.
INDEX -p Password	It means to define a password for the SMS object profile.

	INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile. Password: Enter a password that the sender can use to register to selected SMS provider.
INDEX -q Quota	Enter the number of the credit that you purchase from the service provider. INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile. Quota: Enter a number. Note that one credit equals to one SMS text message on the standard route.
INDEX -I Interval	It means to set the sending interval for the SMS to be delivered. INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile. Interval: Enter the shortest time interval for the system to send SMS.
INDEX -I URL	It means to set the URL of SMS object profile 9 and 10. INDEX: Enter the index number (from 1 to 10) of the specified SMS object profile. URL: Enter the URL of SMS object.

Example

```
> object sms obj 1 –n CTC
> object sms obj 1 -n CTC
> object sms obj 1 -s 0
> object sms obj 1 -u carrie
> object sms obj 1 -p 19971125cm
> object sms obj 1 -q 2
> object sms obj 1 -i 50
> object sms obj 1 -v
Profile Index: 1
Profile Name:[CTC]
SMS Provider:[kotsms.com.tw (TW)]
Username:[carrie]
Password:[******]
Quota:[2]
Sending Interval:[50(seconds)]
```

Telnet Command: object mail

This command is used to create mail object profile.

Syntax

object mail show

object mail setdefault

object mail obj *INDEX -v*

object mail obj *INDEX -n Profile Name*

object mail obj *INDEX -s SMTP Server*

object mail obj *INDEX -I Use SSL*

object mail obj *INDEX -m SMTP Port*

object mail obj *INDEX -a Sender Address*

object mail obj *INDEX -t Authentication*

object mail obj *INDEX -u Username*

object mail obj *INDEX -p Password*

object mail obj *INDEX -i Sending Interval*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified mail object profile. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile.
INDEX -n Profile Name	It means to define a name for the mail object profile. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. Profile Name: Enter a name with less than 15 characters.
INDEX -s SMTP Server	It means to set the IP address of the mail server. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. SMTP Server: Enter the name or the IP address of the SMTP server.
INDEX -l Use SSL	It means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. Use SSL: Enter 0 or 1. 0 – disable 1 – enable to use the port number.
INDEX -m SMTP Port	It means to set the port number for SMTP server. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. SMTP Port: Enter a port number.
INDEX -a Sender Address	It means to set the e-mail address of the sender. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. Sender Address: Enter the e-mail address (e.g., johnwash@abc.com.tw).
INDEX -t Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. Authentication: Enter 0 or 1. 0 – disable 1 – enable to use the port number.
INDEX -u Username	Type a name for authentication. The maximum length of the name you can set is 31 characters. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. Username: Enter a string as a username.
INDEX -p Password	Type a password for authentication. The maximum length of the password you can set is 31 characters. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. Password: Enter a password.
INDEX -i Sending Interval	Define the interval for the system to send the SMS out. The unit is second. INDEX: Enter the index number (from 1 to 10) of the specified mail object profile. Sending Interval: Enter a value (seconds).

Example

```
> object mail obj 1 -n buyer
> object mail obj 1 -s 192.168.1.98
> object mail obj 1 -m 25
> object mail obj 1 -t 1
> object mail obj 1 -u john
> object mail obj 1 -p happy123456
> object mail obj 1 -i 25
> object mail obj 1 -v
Profile Index: 1
Profile Name:[buyer]
SMTP Server:[192.168.1.98]
SMTP Port:[25]
Sender Address:[]
Use SSL:[disable]
Authentication:[enable]
Username:[john]
Password:[******]
Sending Interval:[25(seconds)]
>
```

Telnet Command: object noti

This command is used to create notification object profile.

Syntax

object noti show

object noti setdefault

object noti obj *INDEX -v*

object noti obj *INDEX -n Profile Name*

object mail obj *INDEX –e Category Status*

object mail obj *INDEX –d Category Status*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX -v	It means to view the information of the specified notification object profile. INDEX: Enter the index number (from 1 to 8) of the specified notification object profile.
INDEX -n Profile Name	It means to define a name for the notification object profile. INDEX: Enter the index number (from 1 to 8) of the specified notification object profile. Profile Name: Type a name with less than 15 characters.
INDEX–e Category Status	It means to enable the status of specified category. INDEX: Enter the index number (from 1 to 8) of the specified notification object profile. Category: Enter 1, 2, 3, 4 or 5. 1: WAN; 2: VPN Tunnel; 3: Temperature Alert; 4: WAN Budget; 5: CVM Status: Enter 1, 2, 3, 4, or 5 For WAN – 1: Disconnected; 2: Reconnected. For VPN Tunnel - 1: Disconnected; 2: Reconnected. For Temperature Alert –

	1: Out of Range. For WAN Budget 1: Limit Reached. For CVM 1: CPE Offline; 2: Backup Fail; 3: Restore Fail; 4: FW Update Fail; 5: VPN Profile Setup Fail.
INDEX -d Category Status	It means to disable the status of specified category. INDEX: Enter the index number (from 1 to 8) of the specified notification object profile. Category: Enter 1, 2, 3, 4 or 5. 1: WAN; 2: VPN Tunnel; 3: Temperature Alert; Status: Enter 1, 2 For WAN – 1: Disconnected; 2: Reconnected. For VPN Tunnel - 1: Disconnected; 2: Reconnected. For Temperature Alert – 1: Out of Range.

Example

```
> object noti obj 1 –n marketing
> object noti obj 1 -e 1 1
> object noti obj 1 -e 2 1
> object noti obj 1 -e 5 3
> object noti obj 1 -v
DrayTek> object noti obj 1 -v
Profile Index: 1
Profile Name:[marketing]
    Category                  Status
  WAN              [v]Disconnected     [ ]Reconnected
  VPN Tunnel        [v]Disconnected     [ ]Reconnected
  Temperature Alert   [v]Out of Range
```

Telnet Command: object schedule

This command is used to create schedule object profile.

Syntax

object schedule set <*INDEX***>** *<option list>*

object schedule view *<INDEX>*

object schedule setdefault

Syntax Description

Parameter	Description
set	It means to set the schedule profile.
<INDEX>	It means the index number (from 1 to 15) of the specified object profile.
<option list>	Available options for schedule includes: -e , -c, -D, -T, -d, -a, -i, -h
<INDEX> -e <value>	It means to enable the schedule setup. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object. <value>: Enter 0 or 1. 0, disable 1, enable
<INDEX> -c <comment>	It means to set brief description for the specified profile. <INDEX>: Enter the index number (from 1 to 15) of the

	specified schedule object. <comment>: Enter a brief description (1 ~ 32 characters).
<INDEX> -D <year> <month> <day>	It means to set the starting date of the profile. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object. <year> – Must be between 2000-2049. <month>- Must be between 1-12. <day> - Must be between 1-31. For example: To set Start Date 2015/10/6, type *> object schedule set 1 -D "2015 10 6"*
<INDEX> -T <hour> <minute>	It means to set the starting time of the profile. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object. <hour>: Must be between 0-23. <minute>: Must be between 0-59. For example: To set Start Time 10:20, type *> object schedule set 1 -T "10 20"*
<INDEX> -d <hour> <minute>	It means to set the duration time of the profile. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object. <hour>: Must be between 0-23. <minute>: Must be between 0-59. For example: To set Duration Time 3:30, type *> object schedule set 1 -d "3 30"*
<INDEX> -a <value>	It means to set the action used for the profile. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object. <value>: Enter 0, 1, 2, or 3 0:Force On, 1:Force Down, 2:Enable Dial-On-Demand, 3:Disable Dial-On-Demand
<INDEX> -I <value>	It means to set idle time. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object. <value>: Must be between 0-255(minute). The default is 0.
<INDEX> -h <option> <day/date/cycle_days>	Set how often the schedule will be applied. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object. <option>: Enter 0, 1, 2 or 3 0: Once, 1: Weekdays, 2:Monthly, 3:Cycle days <day>: Enter Sun, Mon, Tue, Wed, Thu, Fri, Sat If the <option> set Weekdays, then must select which days of Week. example: To select Sunday, Monday, Thursday, type <date>: Enter 1-28. <cycle_days> : Enter 1-30. If the <option> set cycle days, then must select which days to do cycle schedule example: To select cycle 10 days: *> object schedule set 1 -h 3 10"*
view <INDEX>	It means to show the content of the profile. <INDEX>: Enter the index number (from 1 to 15) of the specified schedule object.
setdefault	It means to return to default settings for all profiles.

Example

```
> object schedule set 1 -e 1
> object schedule set 1 -c Working
> object schedule set 1 -D "2017 4 18"
> object schedule set 1 -T "8 1"
> object schedule set 1 -d "2 30"
```

```
> object schedule set 1 -a 0
> object schedule set 1 -h "1 Mon Wed"
> object schedule view 1
Index No.1

-------------------------------------------------
[v] Enable Schedule Setup
       Comment [ Working ]
       Start Date (yyyy-mm-dd) [ 2017 ]-[  4 ]-[ 18 ]
       Start Time (hh:mm)      [  8 ]:[  1 ]
       Duration Time (hh:mm)   [  2 ]:[ 30 ]
       Action                  [ Force On ]
       Idle Timeout            [  0 ] minute(s).(max. 255, 0 for default)

-------------------------------------------------------------------
       How Often
        [v] Weekdays
            [ ]Sun  [v]Mon  [ ]Tue  [v]Wed  [ ]Thu  [ ]Fri  [ ]Sat
>
```

Telnet Command: port

This command allows users to set the speed for specific port of the router.

Syntax

port *<1, 2, all> <AN, 100F, 100H, 10F, 10H, status>*

port *<wan2> <AN, 1000F, 100F, 100H, 10F, 10H, status>*

port status

port wanfc

Syntax Description

Parameter	Description
<1, 2, all> <AN, 100F, 100H, 10F, 10H, status>	<1, 2, all> : Enter 1, 2 or all to specify the number of LAN port. <AN, 100F, 100H, 10F, 10H, status>: It means the physical type for the specific port. AN: auto-negotiate. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.
<wan2> <AN, 1000F, 100F, 100H, 10F, 10H, status>	It means the WAN2 interface. <AN, 1000F, 100F, 100H, 10F, 10H, status>: It means the physical type for the specific port. AN: auto-negotiate. 1000F: 1000M Full Duplex. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.

status	It means to view the Ethernet port status.
wanfc	It means to set WAN flow control.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmaptime

This command allows you to set a time of keeping the session connection for specified protocol.

Syntax

portmaptime -<*command*> <*parameter*> / ...

Syntax Description

Parameter	Description
<*command*> <*parameter*>|...	The available commands with parameters are listed below. <...> means that you can Enter several commands in one line.
-t <sec>	It means "TCP" protocol. <sec>: Type a number to set the TCP session timeout.
-u <sec>	It means "UDP" protocol. <sec>: Type a number to set the UDP session timeout.
-i <sec>	It means "IGMP" protocol. <sec>: Type a number to set the IGMP session timeout.
-w <sec>	It means "TCP WWW" protocol. <sec>: Type a number to set the TCP WWW session timeout.
-s <sec>	It means "TCP SYN" protocol. <sec>: Type a number to set the TCP SYN session timeout.
-f	It means to flush all portmaps (useful for diagnostics).
-l <List>	List all settings.

Example

```
> portmaptime -t 86400 -u 300  -i 10
> portmaptime -l
------ Current setting ------
TCP Timeout   : 86400 sec.
UDP Timeout   : 300 sec.
IGMP Timeout  : 10 sec.
TCP WWW Timeout: 60 sec.
TCP SYN Timeout: 60 sec.
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup -<*command*> <*parameter*> / ...

Syntax Description

Parameter	Description
<*command*>	The available commands with parameters are listed below.

<parameter>/…	<…> means that you can Enter several commands in one line.
-h	Enter it to display the usage of this command.
-W <1~3>	It means to specify WAN interface. <1~3>: Enter 1, 2, 3. Default is 1 (WAN1).
-m <mode>	It means to define which traffic the QoS control settings will apply to and eable QoS control. <mode>: Enter 0, 1, 2, or 3. Default is 2. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic.
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only) <bandwidth>: Enter the value (1 to 100000).
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). <bandwidth>: Enter the value (1 to 100000).
-r <index:ratio>	It means to set ratio for class index, in %. <index:ratio>: Enter a value with ratio (e.g., -r 3:20).
-u <mode>	It means to enable bandwidth control for UDP. <mode>: Enter 0 or 1. Default is disable. 0: disable 1: enable
-p <ratio>	It means to enable bandwidth limit ratio for UDP. <ratio>: Enter the value.
-t <mode>	It means to enable/disable Outbound TCP ACK Prioritize. <mode>: Enter 0 or 1. Default is disable. 0: disable 1: enable
-V	Show all the settings.
-D	Set all to factory default (for all WANs).
[…]	It means that you can Enter several commands in one line.

Example

```
> qos setup -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

 WAN1 QOS mode is both
 Wan 1 is XDSL model ,don,t need to set up
 Wan 1 is XDSL model ,don,t need to set up
 WAN1 class 3 ratio set to 20
 WAN1 udp bandwidth control set to enable
 WAN1 udp bandwidth limit ratio set to 50
 WAN1 Outbound TCP ACK Prioritizel set to enable
QoS WAN1 set complete; restart QoS
>
```

Telnet Command: qos class

This command allows user to set QoS class.

Syntax

qos class -c *<no> -<a/e/d <no>><-<command> <parameter> / … >*

Syntax Description

Parameter	Description

<command> <parameter>/…	The available commands with parameters are listed below. <…> means that you can Enter several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. <no>: Enter 1, 2 or 3. The default setting is class 1.
-n <name>	It means to type a name for the class. <name>: Enter a name.
-a <no>	It means to add rule for specified class. <no>: Enter the index number for the rule.
-e <no>	It means to edit specified rule. <no>: Enter the index number for the rule.
-d <no>	It means to delete specified rule. <no>: Enter the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. <mode>: Enter 0 or 1. 0: disable, 1: enable
-I <addr>	Set the local address. <addr>: Enter <Addr1>, <addr1:addr2>, <addr1:subnet> or any. <Addr1> – It means Single address. Please specify the IP address directly, for example, "-I 172.16.3.9". <addr1:addr2> – It means Range address. Please specify the IP addresses, for example, "-I 172.16.3.9: 172.16.3.50." <addr1:subnet> – It means the subnet address with start IP address. Please Enter the subnet and the IP address, for example, "-I 172.16.3.9:255.255.0.0".0 <any> – It means Any address. Simple type "*-I*" to specify any address for this command.
-r <addr>	Set the remote address. <addr>: Enter <Addr1>, <addr1:addr2>, <addr1:subnet> or any. <Addr1> – It means Single address. Please specify the IP address directly, for example, "-I 172.16.3.9". <addr1:addr2> – It means Range address. Please specify the IP addresses, for example, "-I 172.16.3.9: 172.16.3.50." <addr1:subnet> – It means the subnet address with start IP address. Please Enter the subnet and the IP address, for example, "-I 172.16.3.9:255.255.0.0".0 <any> – It means Any address. Simple type "*-I*" to specify any address for this command.
-p <DSCP id>	Specify the ID. <DSCP id>: Enter the ID.
-s <Service type>	Specify the service type by typing the number. <Service type>: Enter 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29 or 30. 1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP
-S <d/s>	Show the content for specified DSCP ID/Service type. <d/s>: Enter d or s.
-V <1/2/3>	Show the rule in the specified class. <1/2/3>: Enter 1, 2 or 3.
[…]	It means that you can Enter several commands in one line.

Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80

 Following setting will set in the class2
 class 2 name set to draytek
 Add a rule in class2
 Class2 the 1 rule enabled
 Set local address type to Range, 192.168.1.50:192.168.1.80
```

Telnet Command: qos type

This command allows user to configure protocol type and port number for QoS.

Syntax

qos type *-a <service name> / -e <no> / -d <no> /-n <name> /-t <type>/-p <port>/-l*

Syntax Description

Parameter	Description
-a <service name>	It means to add rule. <name>: Enter a name for a rule.
-e <no>	It means to edit user defined service type. <no>: Enter 1 ~ 40 (index number of the service type).
-d <no>	It means to delete user defined service type. <no>: Enter 1 ~ 40 (index number of the service type).
-n <name>	It means the name of the service. <name>: Enter a name of the service.
-t <type>	<type>: It means protocol type. Enter 6, 17, 0 or other number. 6: tcp(default) 17: udp 0: tcp/udp <1~254>: other
-p <port>	It means service port. <port>: Enter the port number. The typing format must be [start:end] (ex., 510:330).
-l	List user defined types. “no” means the index number. Available numbers are 1~40.

Example

```
> qos type -a draytek -t 6 -p 510:1330

 service name set to draytek
 service type set to 6:TCP
 Port type set to Range
 Service Port set to 510 ~ 1330
>
```

Telnet Command: qos setdefault

This command allows user to recover the default settings for QoS.

Syntax

qos setdefault

Example

```
> qos setdefault
Setdefault!
>
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

Example

```
> show lan

The LAN settings:
Status   IP            Mask          DHCP Start IP       Pool Gateway
-------- --------------- --------------- ---- --------------- ----
[V]LAN1  192.168.1.1    255.255.255.0   V    192.168.1.10    200  192.168.1.1

[X]LAN2  192.168.5.1    255.255.255.0   V    192.168.2.10    100  192.168.2.1

[X]Route 192.168.0.1    255.255.255.0   V    0.0.0.0         0    192.168.0.1
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0

%     WAN2 DMZ mapping status:
 Index  Status  WAN2 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0

%     WAN3 DMZ mapping status:
 Index  Status  WAN3 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0
```

Telnet Command: show dns

This command displays current status of DNS setting.

Example

```
> show dns
%%     Domain name server settings:
%  LAN1  Primary DNS: [Not set]
%  LAN1  Secondary DNS: [Not set]

%  LAN2  Primary DNS: [Not set]
%  LAN2  Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
Index   Status  Comment        Local IP Address
*****************************************************
  1.    Enable  TEST           192.168.1.110
Total 1 items listed.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
 Port Redirection Running Table:

Index Protocol Public Port      Private IP    Private Port
 1        0              0    0.0.0.0           0
 2        0              0    0.0.0.0           0
 3        0              0    0.0.0.0           0
 4        0              0    0.0.0.0           0
 5        0              0    0.0.0.0           0
 6        0              0    0.0.0.0           0
 7        0              0    0.0.0.0           0
 8        0              0    0.0.0.0           0
 9        0              0    0.0.0.0           0
10        0              0    0.0.0.0           0
11        0              0    0.0.0.0           0
12        0              0    0.0.0.0           0
13        0              0    0.0.0.0           0
14        0              0    0.0.0.0           0
15        0              0    0.0.0.0           0
16        0              0    0.0.0.0           0
17        0              0    0.0.0.0           0
18        0              0    0.0.0.0           0
19        0              0    0.0.0.0           0
20        0              0    0.0.0.0           0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
```

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```
> show portmap
------------------------------------------------------------------------------
  Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Index/Protocol/Flag]
------------------------------------------------------------------------------

 Total Portmap Session:0
```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
  Level0 TCP=86400001 UDP=300001 ICMP=10001
  Level1 TCP=600000 UDP=90000 ICMP=7000
```

```
  Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 30000
% Maximum Session Usage: 0
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
% WAN2 Current Session Usage: 0
% WAN3 Current Session Usage: 0
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:25:40:53
LAN Status
Primary DNS:8.8.8.8         Secondary DNS:8.8.4.4
IP Address:192.168.1.1       Tx Rate:21417    Rx Rate:15413

WAN 1 Status: Disconnected
Enable:Yes      Line:Fiber      Name:
Mode:PPPoE      Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate(bps):0   RX Packets:0         RX Rate(bps):0


WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:
Mode:DHCP Client Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate(bps):0   RX Packets:0         RX Rate(bps):0
```

Telnet Command: show adsl

This command displays current status of ADSL.

Example

```
> show status
  ---------------- ATU-R Info (hw: annex A, f/w: annex A/B/C) -----------
   Running Mode            :            State                 : TRAINING
   DS Actual Rate          :    0 bps   US Actual Rate        :    0 bps
   DS Attainable Rate      :    0 bps   US Attainable Rate    :    0 bps
   DS Path Mode            :    Fast    US Path Mode          :    Fast
   DS Interleave Depth     :    0       US Interleave Depth   :    0
   NE Current Attenuation  :    0 dB    Cur SNR Margin        :    0  dB
   DS actual PSD           :    0.0 dB  US actual PSD         :    0. 0  dB
   NE CRC Count            :    0       FE CRC Count          :    0
   NE ES Count             :    0       FE  ES Count          :    0
   Xdsl Reset Times        :    0       Xdsl Link  Times      :    0
```

```
   ITU Version[0]          : b5004946   ITU Version[1]        : 544e0000
   VDSL Firmware Version   : 05-07-06-0D-01-07  [with Vectoring support]
   Power Management Mode   : DSL_G997_PMS_NA
   Test Mode               : DISABLE
  ---------------- ATU-C Info ---------------
   Far Current Attenuation :       0 dB   Far SNR Margin      :    0  dB
   CO ITU Version[0]       : 00000000      CO ITU Version[1]   : 00000000
   DSLAM CHIPSET VENDOR    : < ----- >
>
```

Telnet Command: show traffic

This comman can display traffic graph for WAN1, transmitted bytes, receivied bytes and sessions.

Syntax

show traffic *<wan1/wan2/wan3> <tx/rx> <weekly>*

show traffic session *<weekly>*

Example

```
> show traffic session weekly0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,2 ,1 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,1 ,3 ,0 ,0 ,0 ,0 ,0 ,2 ,15 ,5 ,4 ,1 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 0 ,0 ,0 ,0
> show traffic wan1 tx weekly0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
```

Telnet Command: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset *[interface]*

Syntax Description

Parameter	Description
reset	It means to reset the transmitted/received bytes to Zero.
interface	It means to specify WAN1 interface for displaying related statistics.

Example

```
> DrayTek> show statistic
 WAN1 total TX: 0 Bytes ,RX: 0 Bytes
 WAN2 total TX: 0 Bytes ,RX: 0 Bytes
 WAN3 total TX: 0 Bytes ,RX: 0 Bytes
 WAN4 total TX: 0 Bytes ,RX: 0 Bytes
 WAN5 total TX: 0 Bytes ,RX: 0 Bytes
 WAN6 total TX: 0 Bytes ,RX: 0 Bytes
 WAN7 total TX: 0 Bytes ,RX: 0 Bytes

 >
```

Telnet Command: srv dhcp dhcp2

This command is used to enable DCHP2 server.

Syntax

srv dhcp dhcp2 -<*command*> <*parameter*> / …

Syntax Description

Parameter	Description
<*command*> <*parameter*>/…	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-l <enable>	It menas to enable the LAN port to public DHCP. <enable>: Enter 0 or 1. 0: Disenable 1: Enable
-m<enable>	It menas to enable MAC address to public DHCP. <enable>: Enter 0 or 1. 0: Disenable 1: Enable
-e <id>	It menas to turn on the flag of LAN port 1/2. <id>: Enter 1 or 2.
-d <id>	It menas to turn off the flag of LAN port 1/2. <id>: Enter 1 or 2.
-v	It menas to view current status.

Example

```
> srv dhcp dhcp2 -l 1 -e 1
> srv dhcp dhcp2 -v
 2nd DHCP server flag status --
   Server works on specified MAC address: ON
   Server works on specified LAN port: ON
   Port 1 flag: ON
   Port 2 flag: ON
```

Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

Syntax

srv dhcp public *start <IP address>*

srv dhcp public *cnt* **<***IP counts>*

srv dhcp public *status*

srv dhcp public *add <MAC Addr XX-XX-XX-XX-XX-XX>*

srv dhcp public *del <MAC Addr XX-XX-XX-XX-XX-XX >*

srv dhcp public *del all/ALL*

Syntax Description

Parameter	Description
start <IP address>	It means the starting point of the IP address pool for the DHCP server. <IP address>: Enter an IP address as the starting point in the IP address pool.
cnt <IP counts>	It means the IP count number. <IP counts>: Specify the number of IP addresses in the pool.

	The maximum is 10.
status	It means the execution result of this command.
add <MAC Addr XX-XX-XX-XX-XX-XX>	It means creating a list of hosts to be assigned. <MAC Addr>: Enter the MAC Address of the host.
del <MAC Addr XX-XX-XX-XX-XX-XX>	It means removing the selected MAC address. <MAC Addr>: Enter the MAC Address of the host.
del all/ALL	It means removing all of the MAC addresses.

Example

```
> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
> srv dhcp public status
Index   MAC Address
```

Telnet Command: srv dhcp dns1

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns1 *<LAN1/LAN2> <DNS IP address>*

Syntax Description

Parameter	Description
<LAN1/LAN2>	It means to specify the LAN interface. <LAN1/LAN2>: Enter LAN1 or LAN2.
<DNS IP address>	It means the IP address that you want to use as DNS1. <DNS IP address>: Enter the IP address that you want to use as DNS1 (primary DNS). **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns1 lan1 168.95.1.1
% srv dhcp dns1 lan1 <DNS IP address>
% Now: 168.95.1.1
```

Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns2 <*LAN1/LAN2*> <*DNS IP address*>

Syntax Description

Parameter	Description
<*LAN1/LAN2*>	It means to specify the LAN interface.
<*DNS IP address*>	It means the IP address that you want to use as DNS2. <DNS IP address>: Enter the IP address that you want to use as DNS1 (seconday DNS). **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 lan1 168.95.1.1
% srv dhcp dns2 lan1 <DNS IP address>
% Now: 168.95.1.1
```

Telnet Command: srv dhcp frcdnsmanl

This command can force the router to invoke DNS Server IP address.

Syntax

srv dhcp frcdnsmanl <*on /off*>

Syntax Description

Parameter	Description
on	It means to use manual setting for DNS setting.
Off	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: srv dhcp gateway

This command allows users to specify gateway address for DHCP server.

Syntax

srv dhcp gateway <*Gateway IP*>

Syntax Description

Parameter	Description
<*Gateway IP*>	It means to specify a gateway address used for DHCP server. <gateway IP>: Enter an IP address.

Example

```
> srv dhcp gateway 192.168.2.1
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp ipcnt

This command allows users to specify IP counts for DHCP server.

Syntax

srv dhcp ipcnt <*IP counts*>

Syntax Description

Parameter	Description
<*IP counts*>	It means the number that you have to specify for the DHCP server. <IP counts>: Enter a value (0~256).

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 150
```

Telnet Command: srv dhcp off

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp on

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp relay

This command allows users to set DHCP relay setting.

Syntax

srv dhcp relay servip <*server ip*>

srv dhcp relay subnet <*index*>

Syntax Description

Parameter	Description
<server ip>	It means the IP address that you want to used as DHCP server. <server ip>: Enter an IP address.
<Index>	The router will invoke this function according to the subnet 1 or 2 specified here. <index>: Enter 1 or 2.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
> srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: srv dhcp startip

Syntax

srv dhcp startip *<IP address>*

Syntax Description

Parameter	Description
<IP address>	It means the IP address that you can specify for the DHCP server as the starting point. <IP address>: Enter an IP address.

Example

```
> srv dhcp startip 192.168.1.53
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp status

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
LAN1      : DHCP Server On    IP Pool: 192.168.1.10 ~ 192.168.1.209
            Default Gateway: 192.168.1.1
------------------------------------------------------------------------
Index   IP Address     MAC Address           Leased Time     HOST ID
------------------------------------------------------------------------
LAN1
```

Telnet Command: srv dhcp leasetime

This command can set the lease time for the DHCP server.

Syntax

srv dhcp leasetime <*Lease Time (sec)***>**

Syntax Description

Parameter	Description
<*Lease Time (sec)***>**	It means the lease time that DHCP server can use. The unit is second. **<**Lease Time (sec)>: Enter a value.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 92000
>
```

Telnet Command: srv dhcp nodetype

This command can set the node type for the DHCP server.

Syntax

srv dhcp nodetype *<count>*

Syntax Description

Parameter	Description
<count>	It means to specify a type for node. <count>: Enter 1, 2, 4 or 8. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: srv dhcp primWINS

This command can set the primary IP address for the DHCP server.

Syntax

srv dhcp primWINS <*WINS IP address*>

srv dhcp primWINS clear

Syntax Description

Parameter	Description
<*WINS IP address*>	It means the IP address of primary WINS server. <WINS IP address>: Enter an IP address.
clear	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: srv dhcp secWINS

This command can set the secondary IP address for the DHCP server.

Syntax

srv dhcp secWINS <*WINS IP address*>

srv dhcp secWINS clear

Syntax Description

Parameter	Description
<*WINS IP address*>	It means the IP address of secondary WINS server. <WINS IP address>: Enter an IP address.
clear	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: srv dhcp expRecycleIP

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

Syntax

srv dhcp expRecycleIP <*sec time*>

Syntax Description

Parameter	Description
<*sec time*>	It means to set the time (5~300 seconds) for checking if the IP can be assigned again or not. <sec time>: Enter a value.

Example

```
> srv dhcp expRecycleIP 250
% DHCP expRecycleIP = 250
```

Telnet Command: srv dhcp tftp

This command can set the TFTP server as the DHCP server.

Syntax

srv dhcp tftp <*TFTP server name*>

Syntax Description

Parameter	Description
<*TFTP server name*>	It means to Enter the name of TFTP server. <TFTP server name>: Enter a name.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: srv dhcp tftpdel

This command can remove the name defined for the TFTP server.

Syntax

srv dhcp tftpdel

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
> srv dhcp tftpdel
 % The TFTP Server Name had been deleted !!!
```

Telnet Command: srv nat dmz

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

Syntax

srv nat dmz *n m -e <1/0> -i <IP address>*

srv nat dmz *-r*

srv nat dmz *-v*

Syntax Description

Parameter	Description
n	It means to map selected WAN IP to certain host. 1: wan1
m	It means the index number of the DMZ host. m: Enter 1 ~ 8. Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
-e <1/0>	It means to enable/disable such feature. <1/0>: Enter 1 or 0. 1:enable 0:disable
-i <IP address>	It means to specify the private IP address of the DMZ host. <IP address>: Enter an IP address.
-r	It means to remove DMZ host setting.
-v	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96 -e 1
> srv nat dmz -v
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP    Private IP
-------------------------------------------------
   1    Enable  0.0.0.0 192.168.1.96

%     WAN2 DMZ mapping status:
 Index  Status  WAN2 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0

%     WAN3 DMZ mapping status:
 Index  Status  WAN3 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0
```

Telnet Command: srv nat ipsecpass

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

srv nat ipsecpass *on*

srv nat ipsecpass *off*

srv nat ipsecpass *status*

Syntax Description

Parameter	Description
[options]	The available commands with parameters are listed below.
on	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
off	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
status	It means to display current status for checking.

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is OFF.
```

Telnet Command: srv nat openport

This command allows users to set open port settings for NAT server.

Syntax

srv nat openport n m *-<command> <parameter> / …*

Syntax Description

Parameter	Description
n	It means the index number for the profiles. N: Enter 1 ~20.
m	It means to specify the sub-item number for this profile. m: Enter 1 ~10.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile. <enable>: Enter 1 or 0. 0: disable 1: enable
-c <comment>	It means to Enter the description (less than 23 characters) for the defined network service. <comment>: Enter a description.
-i <local ip>	It means to set the IP address for local computer. <local ip>: Enter an IP address.

-w <widx> <ipidx>	It means to specify the public IP. <*widx*> – Enter 1, 2, 255 (means the WAN interface) 1: WAN1 (Default) 2: WAN1 Alias 1 255: all WANs. <ipidx> – Enter 1 ~ 32 for Alias IPs.
-p <protocol>	Specify the transport layer protocol. <protocol>: Enter TCP, UDP, or ALL.
-s <start port>	It means to specify the starting port number of the service offered by the local host. <start port>: Enter a value (0 to 65535).
-e <end port>	It means to specify the ending port number of the service offered by the local host. <end port>: Enter a value (0 to 65535).
-v	It means to display current settings.
-r	It means to delete the specified open port setting.
-f	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.56 -w 1 1 -p TCP -s 23 -e
83
> Set WAN Port ok!!
> srv nat openport 1 1 -v
%% Status: Enable
%% Comment: games
%% WAN Interface: WAN1
%% Private IP address: 192.168.1.56
Index   Protocal       Start Port     End Port
************************************************************
  1.    TCP           23            83

> srv nat openport 1 1 -r
> srv nat openport 1 1 -f
>
```

Telnet Command: srv nat portmap

This command allows users to set port redirection table for NAT server.

Syntax

srv nat portmap add *<idx> <serv name> <proto> <pub port> <src ip idx> <pri ip> <pri port> <wan1 ~ wan4> <alias IP>*

srv nat portmap *del <idx>*

srv nat portmap *disable <idx>*

srv nat portmap *enable <idx> <proto>*

srv nat portmap *flush*

srv nat portmap *table*

Syntax Description

Parameter	Description
add <idx> <serv name> <proto> <pub port> <src ip idx> <pri ip> <pri port> <wan1 ~ wan4> <alias IP>	It means to add a new port redirection table with an index number. <idx>: Enter an index number (1 to 20). **<** serv name**>:** Enter a name as service name. <proto>: Specify TCP or UDP or All as the protocol. <pub port>: Enter a value (0~65535). <src ip idx>: Enter an index number of source IP object profile. <pri ip>: Specify the private IP address of the internal host providing the service. <pri port>: Enter a value (0~65535). <wan1 ~ wan4>: Specify WAN interface for the port redirection. <alias IP>: Enter the index number (1~32) of alias IP.
del <idx>	It means to remove the selected port redirection setting. <idx>: Enter an index number (1 to 20).
disable <idx>	It means to inactivate the selected port redirection setting. <idx>: Enter an index number (1 to 20).
enable <idx> <proto>	It means to activate the selected port redirection setting. <idx>: Enter an index number (1 to 20). <proto>: Specify TCP or UDP or All as the protocol.
flush	It means to clear all the port mapping settings.
table	It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 name tcp 100 0 192.168.1.10 200 wan1 1
> srv nat portmap table

NAT Port Redirection Configuration Table:

Index  Service Name Protocol  Public Port    Private IP     Private Port    ifno
 1        name       TCP      100            192.168.1.10   200            -1
 2                       Disabled        0   0     -2
 3                       Disabled        0   0     -2
 4                       Disabled        0   0     -2
 5                       Disabled        0   0     -2
 6                       Disabled        0   0     -2
...
```

Telnet Command: srv nat status

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
NAT Port Redirection Running Table:

Index  Protocol  Public Port    Private IP       Private Port
 1          6         100      192.168.1.11             200
 2          0          0       0.0.0.0                   0
 3          0          0       0.0.0.0                   0
```

```
 4          0          0       0.0.0.0                  0
 5          0          0       0.0.0.0                  0
 6          0          0       0.0.0.0                  0
 7          0          0       0.0.0.0                  0
 8          0          0       0.0.0.0                  0
 9          0          0       0.0.0.0                  0
10          0          0       0.0.0.0                  0
11          0          0       0.0.0.0                  0
12          0          0       0.0.0.0                  0
13          0          0       0.0.0.0                  0
14          0          0       0.0.0.0                  0
15          0          0       0.0.0.0                  0
16          0          0       0.0.0.0                  0
17          0          0       0.0.0.0                  0
18          0          0       0.0.0.0                  0
19          0          0       0.0.0.0                  0

20          0          0       0.0.0.0                  0

--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: srv nat showall

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
> srv nat showall
Index   Proto   WAN IP:Port              Private IP:Port           Act
**************************************************************************
****
R01     TCP     0.0.0.0:100              192.168.1.10:200          Y


D01     All     0.0.0.0                  192.168.1.96             Y
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys board

This command is used to disable/enable the function of default or wireless LAN button.

Syntax

sys board button <*def/wlan*><*on/off*>

Syntax Description

Parameter	Description
<*def/wlan*><*on/off*>	It means to set default usage of the button. <def>: Enter def (for factory default setting). <wlan>: Enter wlan (for wireless button). <on/off>: Enter on or off. It is used to disable/enable the function of the button.

	On – enable the button function. Off – disable the button function.

Example

```
> sys board button def on
> default button is on now.
```

Telnet Command: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

Syntax

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
default	It means to reset current settings with default values.
status	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0   Status: 1 (0x4845af2c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
   [1] ?
   [2] sys ?
   [3] sys adminuser ?
   [4] sys board ?
   [5] sys board button ?
   [6] sys board button def on
   [7] sys cfg ?
   [8] sys cfg status
   [9] sys /
   [10] sys cmdlog ?
   [11] sys cmdlog
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd <*on/off***>**

Syntax Description

Parameter	Description
<on/off>	<on>: Turn on the FTP server of the system. <off>: Turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

Syntax

sys domainname <*wan1/wan2*> <*Domain Name Suffix*>

sys domainname <*wan1/wan2*> *clear*

Syntax Description

Parameter	Description
<*wan1/wan2*> <*Domain Name Suffix*>	<wan1/wan2>: Specify WAN interface for assigning a name for it. <Domain Name Suffix>: Enter a name. It means the name for the domain of the system. The maximum number of characters that you can set is 39.
<*wan1/wan2*> *clear*	<wan1/wan2>: Specify WAN interface for assigning a name for it. <clear>: Remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 39 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intellegent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFF00 (Private)
IP Address: 0.0.0.0         Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
```

```
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
>
```

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

Syntax

sys name <*wan1/wan2*> <*ASCII string*>

sys name <*wan1/wan2*> *clear*

Syntax Description

Parameter	Description
<*wan1/wan2*> <*ASCII string*>	It means to specify WAN interface for assigning a name for it. <wan1/wan2>: Specify WAN interface for assigning a name for it. <ASCII string>: Enter a string. The maximum number of characters that you can set is 39.
<*wan1/wan2*> *clear*	It means the name for router. <wan1/wan2>: Specify WAN interface for assigning a name for it. <clear>: Remove the name of the system.

Example

```
> sys name wan1 drayrouter
> sys name ?
% sys name <wan1/wan2> <ASCII string (max. 39 characters)>
% sys name <wan1/wan2> clear
% Now: wan1 == drayrouter, wan2 ==
>
```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: sys passwd

This command allows users to set password for the administrator.

sys passwd *<old password> <new password: ASCII string>*

Syntax Description

Parameter	Description
<old password> <new password: ASCII string>	<old password>: Enter the old password for administrator. <new passoword: ASCII string>: Enter the the password for administrator. The maximum number of characters that you can set is 23.

Example

```
> sys passwd admin admin123
> Password change successful !!!
> sys passwd admin123 admin
```

Telnet Command: sys reboot

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

Syntax

sys autoreboot *[on/off/hour(s)]*

Syntax Description

Parameter	Description
on/off	On – It means to enable the function of auto-reboot. Off – It means to disable the function of auto-reboot.
hours	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an **interval** of two hours.

Example

```
> sys autoreboot on
 autoreboot is ON
> sys autoreboot 2
 autoreboot is ON
 autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
DrayTek> sys version
Router Model: VigorLTE200n   Version: 3.8.12_RC2 English
Profile version: 3.0.0   Status: 1 (0x4844488c)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Apr 17 2019 19:00:48
Router Name: DrayTek
Revision: 81388 V388_2620L
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff  ( 200B), used#: 1968, cached#:   21
Buf KMC5112  (5112B), used#:  257, cached#:   49
Buf KMC4088  (4088B), used#:    1, cached#:    7
Buf KMC2552  (2552B), used#: 1810, cached#:  434
Buf KMC1016  (1016B), used#:   17, cached#:    7
Buf KMC504   ( 504B), used#:   17, cached#:   31
Buf KMC248   ( 248B), used#:   87, cached#:   41
Buf KMC120   ( 120B), used#:  302, cached#:  402
Buf KMC56    (  56B), used#:  139, cached#:  117
Buf KMC24    (  24B), used#:    0, cached#:    0
Dynamic memory: 39321600B; 6458816B used; 1520192B/0B in level 1/2 cache.

FLOWTRACK Memory Status
# of free = 30000
# of maximum = 0
# of flowstate = 30000
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: sys pollbuf

This command can turn on or turn off polling buffer for the router.

Syntax

sys pollbuf *<on/off>*

Syntax Description

Parameter	Description
<on/off>	<on>: Turn on pulling buffer. <off>: Turn off pulling buffer.

Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!
```

Telnet Command: sys britask

This command can improve triple play quality.

Syntax

sys britask *<on/off>*

Syntax Description

Parameter	Description
<on/off>	<on>: Turn on the bridge task for improving the triple play quality. <off>: Turn off the bridge task.

Example

```
> sys britask on
% bridge task is ON, now
```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

Syntax

sys tr069 get int.

sys tr069 get *<parm> <nextlevel>*

sys tr069 set *<parm> <value>*

sys tr069 getnoti *<parm>*

sys tr069 setnoti *<parm> <value>*

sys tr069 log

sys tr069 debug *<on/off>*

sys tr069 save

sys tr069 clear

sys tr069 inform *<event code>*

sys tr069 port *<port num>*

sys tr069 cert_auth *<on/off>*

Syntax Description

Parameter	Description
get int.	It means to get all of the parameters for TR-069.
get <parm> <nextlevel>	It means to get configured value for the specified parameter. <parm>: Enter the abbriviation/full name of the parameter. For example, "Int." means Internet. "Man." means Management Server. Int.Man. = InternetGatewayDevice.ManagementServer. <nextlevel>: Get the information of the next level for specified parameter (e.g., sys tr069 get Int.Man. nextlevel).
set <parm> <value>	It means to configure TR-069 parameters settings. Available parameters can be seen by using "get Int.". <parm>: Enter the abbriviation of the parameter. <value>: Enter the number, address, string, or name for the selected parameter.
getnoti <parm>	It means to get notification value for the specified parameter. <parm>: Enter the abbriviation of the parameter.
setnoti <parm> <value>	It means to configure notification value for TR-069 paramters. <parm>: Enter the abbriviation of the parameter. <value>: Enter the value for the selected parameter.
log	It means to display the TR-069 log.
debug <on/off>	<on/off>: Enter on or off. on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.
save	It means to save the parameters to the flash memory of the router.

inform <event code>	It means to inform parameters for tr069 with different event codes. <event code>: Enter 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 0, BOOTSTRAP 1, 1 BOOT 2, PERIODIC 3, SCHEDULED 4, VALUE CHANGE 5, KICKED 6, CONNECTION REQUEST 7, TRANSFER COMPLETE 8, DIAGNOSTICS COMPLETE 9, M Reboot
port <port num>	It means to change tr069 listen port number. <port num>: Enter a port number (1~65535).
cert_auth <on/off>	<on/off>: Enter on or off. on: turn on certificate-based authentication. off: turn off certificate-based authentication.

Example

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: sys alg

This command can turn on/off ALG (Application Layer Gateway) for traversal.

Syntax

sys alg *<1/0>*

Syntax Description

Parameter	Description
<1/0>	<1/0>: Enter 1 or 0. 1, means to turn on ALG. 0, means to turn off ALG.

Example

```
> sys sip_alg ?
Usage: sys alg <command> <parameter>
 -e: enable ALG (0:disable, 1:enable)

Current ALG status
 -ALG Master Switch: Disabled
> sys alg -e 0
 Disable ALG
```

Telnet Command: sys sip_alg

This command can turn on/off ALG (Application Layer Gateway) for SIP.

Syntax

sys sip_alg *-e <1/0>*

sys sip_alg *-p <port number>*

sys sip_alg *-u <1/0>*

sys sip_alg *-t <1/0>*

Syntax Description

Parameter	Description
-e <1/0>	<1/0>: Enter 1 or 0. Enable (1) or disable (0) the SIP ALG function.
-p <port number>	Set the listening port for SIP ALG. <port number>: Enter a port number (1~65535).
-u <1/0>	<1/0>: Enter 1 or 0. Enable (1) or disable (0) the listening along UDP path.
-t <1/0>	<1/0>: Enter 1 or 0. Enable (1) or disable (0) the listening along TCP path.

Example

```
> sys sip_alg -p 65535
 Current listening port: 65535
```

Telnet Command: sys rtsp_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for RTSP

Syntax

sys rtsp_alg *-e <1/0>*

sys rtsp_alg *-p <port number>*

sys rtsp_alg *-u <1/0>*

sys rtsp_alg *-t <1/0>*

sys rtsp_alg *-v*

Syntax Description

Parameter	Description
-e <1/0>	Enable (1) or disable (0) the function of RTSP ALG.
-p <port number>	Set the listening port for RTSP ALG. <port number>: Enter a port number (1~65535).
-u <1/0>	<1/0>: Enter 1 or 0. Enable (1) or disable (0) the listening along UDP path.
-t <1/0>	<1/0>: Enter 1 or 0. Enable (1) or disable (0) the listening along TCP path.
-v	Display RTP and RTCP portmap information of RTSP ALG.

Example

```
> sys rtsp_alg -e 1
 Auto enable ALG Master Switch

 Enable RTSP ALG

> sys rtsp_alg -p 85
 Current listening RTSP Port: 85
> sys rtsp_alg ?
Usage: sys rtsp_alg <command> <parameter>
 -e: enable RTSP ALG (0:disable, 1:enable)
 -p: set your listening port for RTSP ALG
 -u: enable listen along UDP path (0:disable, 1:enable)
 -t: enable listen along TCP path (0:disable, 1:enable)
 -v: show rtp and rtcp portmap information of RTSP ALG

Current RTSP ALG status
 -ALG Master Switch: Enabled
 -RTSP ALG: Enabled
 -Listen along UDP path: Yes
 -Listen along TCP path: Yes
 -Listening Port: 85
 -Max RTSP session num: 256
 -Remain RTSP session num: 256
```

Telnet Command: sys license

This command can process the system license.

Note that DO NOT use the commands for system administrator only (for example, sys license licmsg, sys license licauth, and etc).

Syntax

sys license *reset_regser*

sys license *licifno <AUTO/WAN#1>*

sys license *lic_trigger <-e/-d/-s>*

Syntax Description

Parameter	Description
reset_regser	It means to reset the server as default setting, http://auth.draytek.com.
licera	It means to erase license setting.
licifno <AUTO/WAN#1>	It means license and signature download interface setting. <AUTO/WAN#1>: Enter AUTO or WAN1, WAN2, etc.
lic_trigger <-e/-d/-s>	It means to trigger the license automatically to update on boot time. -e : Enable the license trigger to update. -d : Disable the license trigger to update. -s : Display license status.

Example

```
> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Download interface is "auto-selected" now.

> sys license lic_trigger -e
Trigger the license to update, value=1

> sys license lic_trigger -d
Don't trigger the license to update, value=0

> sys license lic_trigger -s
License update state=0 (0:disable, 1:enable)
```

Telnet Command: sys daylightsave

This command is used to configure daylight save setting.

Syntax

sys daylightsave *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
<command><parameter>/ …	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-v	Display the daylight saving settings.
-r	Set to factory default setting.
-e <enable>	<enable>: Enter 1 or 0. Enable (1) / disable (0) daylight saving.
-t <type>	Specify the saving type for daylight setting. <type>: Enter 0, 1 or 2. 0 – Default 1 – Time range 2 - Yearly
-s <year> <month> <day> <hour>	Set the detailed settings of the starting day for time range type. <year>: Enter the year. <month>: Enter 1 ~ 12. <day>: Enter 1 ~ 31. <hour>: Enter 0 ~ 23. e.g., sys daylightsave -s 2014 3 10 12
-d <year> <month> <day> <hour>	Set the detailed settings of the ending day for time range type. <year>: Enter the year. <month>: Enter 1 ~ 12. <day>: Enter 1 ~ 31. <hour>: Enter 0 ~ 23. e.g., sys daylightsave -d 2014 9 10 12
-y <month> <th weekday> <day in week> <hour>	Set the detailed settings of the starting day for yearly type. <month>: Enter 1 ~ 12. <th weekday>: Enter 1 ~ 5, 9: last week <day in week>: Enter 0 ~6. 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat <hour>: Enter 0 ~ 23. e.g, sys daylightsave -y 9 1 0 14
-z <month> <th weekday> <day in week> <hour>	Set the detailed settings of the ending day for yearly type. <month>: Enter 1 ~ 12. <th weekday>: Enter 1 ~ 5, 9: last week <day in week>: Enter 0 ~6. 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat <hour>: Enter 0 ~ 23. e.g, sys daylightsave -z 3 1 6 14

Example

```
> sys daylightsave -y 9 1 0 14
% Start: Yearly on Sep 1th Sun 14:00
```

Telnet Command: sys dnsCacheTbl

This command is used to configure TTL settings which will be displayed in DNS Cache table.

Syntax

sys dnsCacheTbl *<command><parameter>/…*

Syntax Description

Parameter	Description
[<command><parameter> |…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-l	Display DNS IPv4 entry in the DNS cache table.
-s	Display DNS IPv6 entry in the DNS cache table.
-v	Display the TTL limit value in the DNS cache table.
-t <ttl>	Set the TTL limit value (seconds) in the DNS cache table. <ttl>: Enter 0 ~5. (0, no limit)
-c	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -l
%DNS Cache Table List
> sys dnsCacheTbl -t 65
% Set TTL limit: 65 seconds.
% When TTL larger than 65s , delete the DNS entry in the router's DNS cache
tabl
e.
>
```

Telnet Command: sys syslog

This command is used to enable / disable syslog.

Syntax

sys syslog *-a <enable> [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
<command><parameter>/ …	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-a <enable>	Enable (1) or disable (0) Syslog Access Setup. <enable>: Enter 1 or 0.
-s <enable>	Enable (1) or disable (0) Syslog Save to Syslog Server. <enable>: Enter 1 or 0.
-i <IP>	Define the IP address of the Syslog server. <IP>: Enter the IP address (e.g., 192.168.5.66)
-d <port>	Define the port number as the destination port. <port>: Enter a port value (1~65535).
-u <enable>	Enable (1) or disable (0) Syslog Save to USB Disk. <enable>: Enter 1 or 0.
-m <enable>	Enable (1) or disable (0) Mail Syslog. <enable>: Enter 1 or 0.
-f <enable>	Enable (1) or disable (0) Filewall Log.

	<enable>: Enter 1 or 0.
-v <enable>	Enable (1) or disable (0) VPN Log. <enable>: Enter 1 or 0.
-e <enable>	Enable (1) or disable (0) User Access Log. <enable>: Enter 1 or 0.
-c <enable>	Enable (1) or disable (0) Call Log. <enable>: Enter 1 or 0.
-w <enable>	Enable (1) or disable (0) WAN Log. <enable>: Enter 1 or 0.
-r <enable>	Enable (1) or disable (0) Router/DSL Information. <enable>: Enter 1 or 0.
-t <enable>	Enable (1) or disable (0) AlertLog Setup. <enable>: Enter 1 or 0.
-o <port>	Define the port number for AlertLog. <port>: Enter a port value (1~65535).
-p	Update the IP address of the server.
-W <mode>	Define the action (1 for overwritting the oldest logs or 0 for stopping the logs) of syslog. <mode>: Enter 1 or 0.
-U <unit>	Set the unit (1 for MB or 0 for GB) of Syslog storing on a USB disk. <unit>: Enter 1 or 0.
-S <capacity>	Define the folder capacity of a USB disk. <capacity>: Enter 1~16GB or 1~1024MB.

Example

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
> sys syslog –p
> Updating server IP address..
```

Telnet Command: sys mailalert

This command is used to configure settings for mail alert function.

Syntax

sys mailalert *<command><parameter>/…*

Syntax Description

Parameter	Description
<command><parameter>/ …	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-e <0/1>	Enable (1) or disable (0) the mail alert function. <0/1>: Enter 0 or 1.
-i <SMTP Server IP>	Set the SMTP sever IP address. <SMTP Server IP>: Enter an IP address.
-o <SMTP Server Port>	Set the port number for SMTP server. <SMTP Server Port>: Enter a number (1~65535).
-a <Mail Address>	Set Alert Mail Reciver E-maiil Address. <Mail Address>: Enter a mail address.
-r <Mail Address>	Set Mail Return E-mail Address. <Mail Address>: Enter a mail address.
-s <0/1>	Enable/Disable Use SSL. <0/1>: Enter 0 or 1.
-h <0/1>	Enable/Disable SMTP Authentication. <0/1>: Enter 0 or 1.
-u <Username>	Set Username for SMTP Authentication. <Username>: Enter a string as username.

-p <Password>	Set Password for SMTP Authentication. <Password>: Enter a password.
-l <type> <0 /1 >	<type>: Enter 0, 1, 2 6. 0, Mail Alert of the DoS Attack. 1, Mail Alert of the APPE. 2, Mail Alert of the VPN Log. 6, Mail Alert of the Reboot Debug Log. <0/1>: Enter 0 (disable) or 1 (enable).
-f	Reset Mail Alert Setting to factory default.
-v	Show Current Mail Alert Setting.
-R <0/1>	Set Mail Alert Reboot Debug Log Mode. <0/1>: Enter 0 or 1. 0, Limited Mode 1, Unlimited Mode

Example

```
> sys mailalert -e 1
Set Enable Mail Alert.
> sys mailalert -i 172.16.3.168
> sys mailalert -o 886
Set SMTP Server Port as 886
> sys mailalert -a john@draytek.com
Set Alert Mail Reciver E-maiil Address as john@draytek.com
> sys mailalert -v
------ Current setting for Mail Alert ------
Mail Alert: Enable
SMTP Server IP Address: 172.16.3.168
SMTP Server Port: 886
Alert Mail Reciver E-maiil Address: john@draytek.com
Mail Return E-mail Address:
Use SSL: Disable
SMTP Authentication: Disable
Username for SMTP Authentication:
Password for SMTP Authentication:
Mail Alert for DoS Attack: Enable.
Mail Alert for APPE: Enable.
Mail Alert for VPN Log: Enable.
Mail Alert for Reboot Debug Log: Disable, Mode: Limited.
-------------------------------------------
>
```

Telnet Command: sys time

This command is used to configure system time and date.

Syntax

sys time server <*domain*>

sys time inquire

sys time show

sys time wan <*option*>

sys time zone <*index*>

Syntax Description

Parameter	Description

server <domain>	Set the domain name of the time server. <domain>: Enter a string. The maximum length is 39 characters.
show	Display the time server setting.
wan <option>	Select WAN interface for applying the time server. <option>: Enter 0, 1, 2, 3 or 4. 0, Auto 1, WAN1 2, WAN2 3, WAN3 4, WAN4
zone <Index>	Different number means different time zone. 1 - GMT-12:00 Eniwetok, Kwajalein 2 - GMT-11:00 Midway Island, Samoa 3 - GMT-10:00 Hawaii 4 - GMT-09:00 Alaska 5 - GMT-08:00 Pacific Time (US & Canada) 6 - GMT-08:00 Tijuana 7 - GMT-07:00 Mountain Time (US & Canada) 8 - GMT-07:00 Arizona 9 - GMT-06:00 Central Time (US & Canada) 10 - GMT-06:00 Saskatchewan 11 - GMT-06:00 Mexico City, Tegucigalpa 12 - GMT-05:00 Eastern Time (US & Canada) 13 - GMT-05:00 Indiana (East) 14 - GMT-05:00 Bogota, Lima, Quito 15 - GMT-04:00 Atlantic Time (Canada) 16 - GMT-04:00 Caracas, La Paz 17 - GMT-04:00 Santiago 18 - GMT-03:30 Newfoundland 19 - GMT-03:00 Brasilia 20 - GMT-03:00 Buenos Aires, Georgetown 21 - GMT-02:00 Mid-Atlantic 22 - GMT-01:00 Azores, Cape Verde Is. 23 - GMT Greenwich Mean Time : Dublin 24 - GMT Edinburgh, Lisbon, London 25 - GMT Casablanca, Monrovia 26 - GMT+01:00 Belgrade, Bratislava 27 - GMT+01:00 Budapest, Ljubljana, Prague 28 - GMT+01:00 Sarajevo, Skopje, Sofija 29 - GMT+01:00 Warsaw, Zagreb 30 - GMT+01:00 Brussels, Copenhagen 31 - GMT+01:00 Madrid, Paris, Vilnius 32 - GMT+01:00 Amsterdam, Berlin, Bern 33 - GMT+01:00 Rome, Stockholm, Vienna 34 - GMT+02:00 Bucharest 35 - GMT+02:00 Cairo 36 - GMT+02:00 Helsinki, Riga, Tallinn 37 - GMT+02:00 Athens, Istanbul, Minsk 38 - GMT+02:00 Jerusalem 39 - GMT+02:00 Harare, Pretoria 40 - GMT+03:00 Volgograd 41 - GMT+03:00 Baghdad, Kuwait, Riyadh 42 - GMT+03:00 Nairobi 43 - GMT+03:00 Moscow, St. Petersburg 44 - GMT+03:30 Tehran 45 - GMT+04:00 Abu Dhabi, Muscat 46 - GMT+04:00 Baku, Tbilisi 47 - GMT+04:30 Kabul 48 - GMT+05:00 Ekaterinburg 49 - GMT+05:00 Islamabad, Karachi, Tashkent

	50 - GMT+05:30 Bombay, Calcutta 51 - GMT+05:30 Madras, New Delhi 52 - GMT+06:00 Astana, Almaty, Dhaka 53 - GMT+06:00 Colombo 54 - GMT+07:00 Bangkok, Hanoi, Jakarta 55 - GMT+08:00 Beijing, Chongqing 56 - GMT+08:00 Hong Kong, Urumqi 57 - GMT+08:00 Singapore 58 - GMT+08:00 Taipei 59 - GMT+08:00 Perth 60 - GMT+09:00 Seoul 61 - GMT+09:00 Osaka, Sapporo, Tokyo 62 - GMT+09:00 Yakutsk 63 - GMT+09:30 Darwin 64 - GMT+09:30 Adelaide 65 - GMT+10:00 Canberra, Melbourne, Sydney 66 - GMT+10:00 Brisbane 67 - GMT+10:00 Hobart 68 - GMT+10:00 Vladivostok 69 - GMT+10:00 Guam, Port Moresby 70 - GMT+11:00 Magadan, Solomon Is. 71 - GMT+11:00 New Caledonia 72 - GMT+12:00 Fiji, Kamchatka, Marshall Is. 73 - GMT+12:00 Auckland, Wellington

Example

```
> sys time zone 8
  Set Time Zone OK

> sys time show
  ***************  System Time  ***************
  Current System Time: [2000 Jan 03 Mon 06:11:12]
  Time Server: [pool.ntp.org]
  Time Zone Index: [8]. GMT-07:00
  Send NTP Request Through: Auto
  ******************************************
```

Telnet Command: sys dashboard

This command is used to display or hidden the information displayed on the dashboard.

Syntax

sys dashboard show

sys dashboard -<*command*> <*value*> …

Syntax Description

Parameter	Description
<*command*><*parameter*>/ …	The available commands with parameters are listed below. <…> means that you can Enter several commands in one line.
- <*command*> <*value*>	<command>: Enter 0, 1, 2, 3,4, 5, 6, 7, 8, 9 adn a 0, Front Panel 1, System Information 2, IPv4 LAN Information 3, IPv4 Internet Access

	4, IPv6 Internet Access 5, Interface 6, Security 7, System Resource 8, LTE Status 9, Quick Access a, VoIP <value>: Enter 1 or 0. 1, Enable 0, Disable

Example

```
> sys dashboard -1 1 -2 0
  System Information enabled
  IPv4 LAN Information disabled
```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
 Mail Alert:[Disable]
 SMTP_Server:[0.0.0.0]
 Mail to:[]
 Return-Path:[]
```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
*****************  IGD NAT Status  ****************
```

```
((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.

> upnp service
>>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL     /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN        uuid:774e9bbe-7386-4128-b627-001daa843464

>>>>> SERVICE TABLE2 <<<<<
  serviceType urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL     /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN        uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```
> upnp on
```

```
UPNP start.
> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

>>>> (3) serviceType urn:schemas-upnp-org:service:WANPOTSLinkConfig:1

>>>> (4) serviceType urn:schemas-upnp-org:service:WANPPPConnection:1

>>>> (5) serviceType urn:schemas-upnp-org:service:WANIPConnection:1
```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
Vigor> upnp tmpvs
******************  Temp virtual server status  ****************

((0))
real_addr  >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr  >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

Syntax

upnp wan <*n*>

Syntax Description

Parameter	Description
<*n*>	It means to specify WAN interface to apply UPnP. <n>: Enter 0 ~3. 0, auto-select WAN interface. 1, WAN1 2, WAN2 3, WAN3

Example

```
> upnp wan 1
```

```
use wan1 now.
```

Telnet Command: vigbrg set

This command is to configure specified WAN as bridge mode.

Syntax Description

vigbrg set *-v <IP version> -w <WAN_idx> -l <LAN_idx> -e <0/1> -f <0/1>*

Syntax Description

Parameter	Description
-v <IP version> -w <WAN_idx> -l <LAN_idx> -e <0/1> -f <0/1>	-v <IP version>: Enter 4 or 6. Indicate the IP version for the IP address. 4, IPv4. 6, IPv6. -w <WAN_idx>: Enter 1. Indicate the WAN interface. 1, WAN1 -l <LAN_idx>: Enter 1, or 2. Indicate the LAN interface. 1, LAN1 2, LAN2 -e <0/1>*:* Enter 0 or 1 to *e*nable/disable the Vigor Bridge for WAN or/and LAN. -f <0/1>: Enter 0 or 1 to *e*nable/disable the firewall functions. 0, disable 1, enable

Example

```
> vigbrg set -v 4 -w 1 -l 1 -e 1
[WAN1] IPv4 bridge is enable. Set subnet[LAN1]
```

Telnet Command: vigbrg closeall

This command can close Vigor Bridge Function.

Example

```
> vigbrg closeall ?
Close all bridge and bridge firewall

[WAN1] IPv4 firewall is disable.
```

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status
Show gConfig setting of bridge mode
[WAN1] IPv4 bridge is enable [LAN1].
```

Telnet Command: vigbrg cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

Syntax

vigbrg cfgip *<IP Address>*

Syntax Description

Parameter	Description
<IP Address>	It means to type an IP address for users to manage the router. <IP Address>: Enter an IP address.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vlan group

This command allows you to set VLAN group. You can set four VLAN groups. Please run *`vlan restart`* command after you change any settings.

Syntax

vlan group *id <set/set_ex> <p1/p2/p3/p4/s1/s2/s3/s4>*

Syntax Description

Parameter	Description
id <set/set_ex> <p1/p2/p3/p4/s1/s2/s3/s4>	Id: Enter 0 ~ 7. It means the group 0 to 7 for VLAN. <set/set_ex>: Enter set or set_ex to let the selected port number joining a VLAN group. In which, "set" indicates each port can join more than one VLAN group. "set_ex" indicates each port can join one VLAN group. <p1/p2/p3/p4/s1/s2/s3/s4>: Enter p1, p2, p3, p4, s1, s2, s3 or s4. In which, p1, p2, p3 and p4 mean LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please enter the port number(s) you want. S1, s2, s3 and s4 are configured for WLAN function.

Example

```
> vlan group 3 set p1 s3 s4
 VLAN   p1   p2   p3   p4   s1   s2   s3   s4
 ---------------------------------------------
   3    V                        V    V
>
```

Telnet Command: vlan off

This command allows you to disable VLAN function.

Syntax

vlan off

Example

```
> vlan off
 VLAN is Disable!
 Force subnet LAN2 to be disabled!!
```

Telnet Command: vlan on

This command allows you to enable VLAN function.

Syntax

vlan on

Example

```
> vlan on
 VLAN is Enable!
```

Telnet Command: vlan pri

This command is used to define the priority for each VLAN profile setting.

Syntax

vlan pri *n pri_no*

Syntax Description

Parameter	Description
n pri_no	n: Enter 0 ~ 7. It means VLAN ID number. pri_no: Enter 0 ~ 7 (from none to highest priority). It means the priority of VLAN profile.

Example

```
> vlan pri 1 2
 VLAN1: Priority=2
```

Telnet Command: vlan restart

This command can make VLAN settings restarted with newest configuration.

Syntax

vlan restart

Example

```
> vlan restart ?
 VLAN restarts!!!
```

Telnet Command: vlan status

This command display current status for VLAN.

Syntax

vlan status

Example

```
> vlan status
VLAN  is Enable :
-----------------------------------------------------
VLAN Enable VID  Pri   p1 p2 p3 p4 s1 s2 s3 s4  subnet
-----------------------------------------------------
 0    OFF    0   0                          1:LAN1
 1    OFF    0   2                          1:LAN1
 2    OFF    0   0                          1:LAN1
 3    OFF    0   0   V              V  V  1:LAN1
 4    OFF    0   0                          1:LAN1
 5    OFF    0   0                          1:LAN1
 6    OFF    0   0                          1:LAN1
 7    OFF    0   0                          1:LAN1
-----------------------------------------------------
 Note: they are only untag for s1/s2/s3/s4, but they can join tag vlan with
lan ports.
 Permit untagged device in P1 to access router: ON.
```

Telnet Command: vlan subnet

This command is used to configure the LAN interface used by the VLAN group.

Syntax

vlan subnet group_id *<1/2>*

Syntax Description

Parameter	Description
<1/2>	<1/2>: Enter 1 or 2. 1, LAN1 2, LAN2

Example

```
> vlan subnet group_id 2
% Vlan Group-0 using LAN2      !

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
drayrouter> vlan subnet
%% vlan subnet group_id <1/2>
% Now
% VLAN0: 2(LAN2      )
% VLAN1: 1(LAN1      )
% VLAN2: 1(LAN1      )
% VLAN3: 1(LAN1      )
% VLAN4: 1(LAN1      )
% VLAN5: 1(LAN1      )
% VLAN6: 1(LAN1      )
% VLAN7: 1(LAN1      )

>
```

Telnet Command: vlan submode

This command changes the VLAN encapsulation mechanisms in the LAN driver.

Syntax

vlan submode <*on/off/status*>

Syntax Description

Parameter	Description
<*on/off/status*>	<on/off/status>: Enter on, off or status to enable, disable or display the submode status. on, means to enable the promiscuous mode. off**,** means to disable the promiscuous mode. status, means to display if submode is normal mode or promiscuous mode.

Example

```
> vlan submode status
% vlan subnet mode : normal mode
> vlan submode on
% vlan subnet mode modified to promiscuous mode.
> vlan submode status
% vlan subnet mode : promiscuous mode
```

Telnet Command: vlan tagged

This command is used to enable or disable the incoming of untagged packets.

Syntax

vlan tagged <*n*> <*on/off*>

vlan tagged *unlimited* <*on/off*>

vlan tagged *p1_untag* <*on/off*>

Syntax Description

Parameter	Description
<*n*> <*on/off*>	<n>: Enter 0 to 7. It means VLAN channel. <on/off>: Enter on or off to enable/disable the tagged VLAN. on, enable off, disable
unlimited <*on/off*>	unlimited <on/off>: Allow/forbid the incoming of untagged packets even all VLAN are tagged. on, allow off, forbid
p1_untag <*on/off*>	p1_untag <on/off>: Allow/forbid the incoming of untagged packets form LAN port 1. on, allow off, forbid

Example

```
> vlan tagged unlimited on
 unlimited mode is ON
```

Telnet Command: vlan vid

This command is used to configure VID number for each VLAN channel.

Syntax

vlan vid *n vid_no*

Syntax Description

Parameter	Description
n vid_no	n: Enter 0 ~ 7. It means VLAN channel. Vid_no: Enter 0 ~ 4095. It means the value of VLAN ID. Enter the value as the VLAN ID number.

Example

```
> vlan vid 1 4095
 VLAN1, vid=4095
```

Telnet Command: vlan sysvid

This command is used to modify and show the scope (reserved 78) of the VLAN IDs used internally by the system.

Syntax

vlan sysvid *show/<n>*

Syntax Description

Parameter	Description
show	It means to show the scope of VLAN ID used internally.
<n>	<n>: Enter 0 ~ 4016. It means the value to be set as VLAN ID.

Example

```
> vlan sysvid 100
 You have set system VLAN ID to range: 100 ~ 177,
 We recommend that you reboot the system now.

> vlan sysvid 200
 You have set system VLAN ID to range: 200 ~ 263,
 We recommend that you reboot the system now.
> vlan sysvid show
 The system VLAN ID is in range: 200 ~ 263
```

Telnet Command: vpn l2lset

This command allows users to set advanced parameters for LAN to LAN function.

Syntax

vpn l2lset <*list index*> **peerid** <*peerid*>

vpn l2lset <*list index*> **localid** <*localid*>

vpn l2lset <*list index*> **main** <*auto/proposal index*>

vpn l2lset <*list index*> **aggressive** <*desg1/desg2/aesg1/aesg2*>

vpn l2lset <*list index*> **pfs** <*on/off*>

vpn l2lset <*list index*> **phase***1* <*lifetime*>

vpn l2lset <*list index*> **phase2** <*lifetime*>

vpn l2lset <*list index*> **x509localid** <*0/1*>

Syntax Description

Parameter	Description
<*list index*> *peerid* <*peerid*>	<list index>: Enter the index number of L2L (LAN to LAN) profile. <peerid>: Enter the peer identity for aggressive mode.
<*list index*> *localid* <*localid*>	<list index>: Enter the index number of L2L (LAN to LAN) profile. <localid>: Enter the local identity for aggressive mode.
<*list index*> *main* <*auto/proposal index*>	It means to choose proposal for main mode. <list index>: Enter the index number of L2L (LAN to LAN) profile. <auto/proposal index>: Enter auto or proposal index number to choose the default proposal or specified proposal.
<*list index*> *aggressive* <*desg1/desg2/aesg1/aesg2*>	It means the chosen DH group for aggressive mode. <list index>: Enter the index number of L2L (LAN to LAN) profile. <desg1/desg2/aesg1/aesg2>: Enter desg1, desg2, aesg1 or aesg2.
<*list index*> *pfs* <*on/off*>	It means “perfect forward secrete”. <list index>: Enter the index number of L2L (LAN to LAN) profile. <on/off>: Enter or or off to turn on/off the PSF configuration.
<*list index*> *phase1* <*lifetime*>	It means to set the lifetime value for phase 1 of IKE. <list index>: Enter the index number of L2L (LAN to LAN) profile. <lifetime>: Enter a value.
<*list index*> *phase2* <*lifetime*>	It means to set the lifetime value for phase 2 of IKE. <list index>: Enter the index number of L2L (LAN to LAN) profile. <lifetime>: Enter a value.
<*list index*> *X509localid* <*0/1*>	It means the local identity for X509 server. <list index>: Enter the index number of L2L (LAN to LAN) profile. <0/1>: Enter 1 or 0 to enable or disable the local identity configuration of X509 server.

Example

```
> vpn l2lset 1 peerid test
```

Telnet Command: vpn dinset

This command allows users to configure setting for remote dial-in VPN profile.

Syntax

vpn dinset <*list index*>
vpn dinset <*list index*> <*on/off*>
vpn dinset <*list index*> **username** <*USERNAME*>
vpn dinset <*list index*> **password** <*PASSWORD*>
vpn dinset <*list index*> **motp** <*on/off*>
vpn dinset <*list index*> **pin_secret** <*pin*> <*secret*>
vpn dinset <*list index*> **timeout** <*0~9999*>
vpn dinset <*list index*> **dintype** <*Type*> <*on/off*>
vpn dinset <*list index*> **subnet** <*0~2*>
vpn dinset <*list index*> **assignip** <*on/off*>
vpn dinset <*list index*> **srnode** <*on/off*>
vpn dinset <*list index*> **remoteip** <*Remote_Client_IP_Address*>
vpn dinset <*list index*> **peer** <*Peer_ID*>
vpn dinset <*list index*> **naming** <*pass/block*>
vpn dinset <*list index*> **multicastvpn** <*pass/block*>
vpn dinset <*list index*> **prekey** <*on/off*>
vpn dinset <*list index*> **assignkey** <*Pre_Shared_Key*>
vpn dinset <*list index*> **digsig** <*on/off*>
vpn dinset <*list index*> **ipsec** <*Method*> <*on/off*>
vpn dinset <*list index*> **localid** <*Local_ID*>

Syntax Description

Parameter	Description
<*list index*>	<list index>: Enter the index number of L2L (LAN to LAN) profile.
<*list index*> <*on/off*>	It means to enable or disable the profile. <list index>: Enter the index number of L2L (LAN to LAN) profile. <on/off>: Enter on or off. On, Enable. Off, Disable.
<*list index*> *username* <*USERNAME*>	It means to set a username for **dial-in** VPN profile. <list index>: Enter the index number of L2L (LAN to LAN) profile. <USERNAME>: Enter a string.
<*list index*> *password* <*PASSWORD*>	It means to set a password for **dial-in** VPN profile. <list index>: Enter the index number of L2L (LAN to LAN) profile. <PASSWORD>: Enter a password.
<*list index*> *motp* <*on/off*>	It means to enable or disable the authentication with mOTP function. <list index>: Enter the index number of L2L (LAN to LAN) profile. <on/off>: Enter on or off. On, Enable. Off, Disable.
<*list index*>	It means to set PIN code with secret.

pin_secret<pin> <secret>	<list index>: Enter the index number of L2L (LAN to LAN) profile. <pin>: Enter the code for authentication (e.g, 1234). <secret>: Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)
<list index> timeout <0~9999>	It means to set the time out for dial-in VPN profile. <list index>: Enter the index number of L2L (LAN to LAN) profile. <0~9999>: Enter a number. The default is 300 seconds.
<list index> dintype <Type> <on/off>	It means to set dial-in type for creating VPN connection. <list index>: Enter the index number of L2L (LAN to LAN) profile. <Type>: 0:PPTP,1:IPsec Tunnel,2:L2TP with IPsec Policy,3:SSL Tunnel <on/off>: Enter on or off. On, Enable. Off, Disable.
<list index> subnet <0~2>	It means to set the LAN subnet for the VPN profile. <list index>: Enter the index number of L2L (LAN to LAN) profile. <0~2>: Enter 0, 1 or 2. 0:LAN1 1:LAN2 2:LAN3
<list index> assignip <on/off>	It means to enable the assignment for static IP address. <list index>: Enter the index number of L2L (LAN to LAN) profile. <on/off>: Enter on or off. On, Enable. Off, Disable.
<list index> srnode <on/off>	It means to enable the function of Specify Remote Node. <list index>: Enter the index number of L2L (LAN to LAN) profile. <on/off>: Enter on or off. On, Enable. Off, Disable.
<list index>remoteip <Remote_Client_IP_Address>	It means to assign the IP address for the remote client. <list index>: Enter the index number of L2L (LAN to LAN) profile. <Remote_Client_IP_Address>: Enter the IP address.
<list index> peer <Peer_ID>	It means to assign the peer ID for such profile. <list index>: Enter the index number of L2L (LAN to LAN) profile. <Peer_ID>: Enter the peer ID.
<list index>naming <pass/block>	<list index>: Enter the index number of L2L (LAN to LAN) profile. <pass/block>: Enter pass or block. Pass, have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

	Block, when there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, it can block data transmission of Netbios Naming Packet inside the tunnel.
<list index> multicastvpn <pass/block>	<list index>: Enter the index number of L2L (LAN to LAN) profile. <pass/block>: Enter pass or block. Pass –Let multicast packets pass through the router. Block – This is default setting. It can let multicast packets be blocked by the router.
<list index> prekey <on/off>	It means to enable/disable the pre-shared key for IKE authentication method. <list index>: Enter the index number of L2L (LAN to LAN) profile. <on/off>: Enter on or off. On, Enable. Off, Disable.
<list index> assignkey <Pre_Shared_Key>	Assign the pre-shared key. <list index>: Enter the index number of L2L (LAN to LAN) profile. <Pre_Shared_Key>: Enter a string.
<list index>digsig <on/off>	Enable /disable the function of Digital Signature (X.509) for IKE authentication method.
<list index> ipsec <Method> <on/off>	Set the IPsec security medthod for the specified VPN profile. <list index>: Enter the index number of L2L (LAN to LAN) profile. <Method>: Enter 0, 1, 2 or 3. 0, Medium(AH) High(ESP) 1, DES 2, 3DES 3, AES <on/off>: Enter on or off. On, Enable. Off, Disable..
<list index> localid <Local_ID>	Assign a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. <list index>: Enter the index number of L2L (LAN to LAN) profile. <Local_ID>: Enter a string.

Example

```
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Deactive

Mobile OTP: Disabled

Password:
```

```
Idle Timeout: 300 sec

> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec
```

Telnet Command: vpn subnet

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

Syntax

vpn subnet <*index*> <*1/2*>

Syntax Description

Parameter	Description
<*index*> <*1/2*>	It means the index number of the VPN profile. <index>: Enter the index number of L2L (LAN to LAN) profile. <1/2>: Enter 1 or 2. 1, LAN1 2, LAN2

Example

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

Syntax

Command of PPTP Dial-Out

vpn setup <*index*> <*name*> **pptp_out** <*ip*> <*usr*> <*pwd*> <*nip*> <*nmask*>

Command of IPSec Dial-Out

vpn setup <*index*> <*name*> **ipsec_out** <*ip*> <*key*> <*nip*> <*nmask*>

Command of L2Tp Dial-Out

vpn setup <*index*> <*name*> **l2tp_out** <*ip*> <*usr*> <*pwd*> <*nip*> <*nmask*>

Command of Dial-In

vpn setup <*index*> <*name*> **dialin** <*ip*> <*usr*> <*pwd*> <*key*> <*nip*> <*nmask*>

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<*index*> <*name*> *pptp_out* <*ip*> <*usr*> <*pwd*> <*nip*> <*nmask*>	<index>: Enter the index number of L2L (LAN to LAN) profile. <name>: Enter the name of the profile. <ip>: Enter the IP address to dial to. <usr>: Enter the user name for the PPTP connection. <pwd>: Enter the password required for the PPPT connection. <nip>: Enter the remote network IP address. <nmask>: Enter the mask for the remote network IP. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	
<*index*> <*name*> *ipsec_out* <*ip*> <*key*> <*nip*> <*nmask*>	<index>: Enter the index number of L2L (LAN to LAN) profile. <name>: Enter the name of the profile. <ip>: Enter the IP address to dial to. <key>: Enter the value of IPsec Pre-Shared Key. <nip>: Enter the remote network IP address. <nmask>: Enter the mask for the remote network IP. e.g., vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
For L2TP Dial-Out	
<*index*> <*name*> *l2tp_out* <*ip*> <*usr*> <*pwd*> <*nip*> <*nmask*>	<index>: Enter the index number of L2L (LAN to LAN) profile. <name>: Enter the name of the profile. <ip>: Enter the IP address to dial to. <usr>: Enter the user name for the PPTP connection. <pwd>: Enter the password required for the PPPT connection. <nip>: Enter the remote network IP address. <nmask>: Enter the mask for the remote network IP. e.g., vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For Dial-In	
<*index*> <*name*> *dialin* <*ip*> <*usr*> <*pwd*> <*key*> <*nip*> <*nmask*>	<index>: Enter the index number of L2L (LAN to LAN) profile. <name>: Enter the name of the profile. <ip>: Enter the IP address to dial to.

	<usr>: Enter the user name for the PPTP connection. <pwd>: Enter the password required for the PPPT connection. <key>: Enter the value of IPsec Pre-Shared Key. <nip>: Enter the remote network IP address. <nmask>: Enter the mask for the remote network IP. e.g., vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server :  ISDN PPTP IPSec L2TP
% Dial from : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
>
```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

Syntax

vpn option <*index*> <*cmd1*>=<*param1*> <*cmd2*>=<*para2*>/ …

Commands of Common Settings

vpn optoin <*index*> <*pname=*> <*ena=*> <*nnpkt=*> <*dir=*> <*idle=*> <*palive=*>

Commands of Dial-Out Settings

vpn optoin <*index*> <*ctype=*> <*dialto=*> <*ltype=*> <*oname=*> <*opwd=*> <*pauth=*> <*ovj=*> <*okey=*> <*ometh=*> <*sch=*> <*ikemode=*> <*ikeid=*>

Commands of Dial-In Settings

vpn optoin <*index*> <*itype=*> <*peer=*> <*peerid=*> <*iname=*> <*ipwd=*> <*ivj=*> <*ikey=*> <*imeth=*>

Commands of TCP/IP Network Settings

vpn optoin <*index*> <*mywip=*> <*rgip=*> <*rnip=*> <*rnmask=*> <*lnip=*> <*lnmask=*> <*rip=*> <*mode=*> <*droute=*>

Syntax Description

Parameter	Description
For Common Settings	
<*index*> <*pname=*> <*ena=*> <*nnpkt=*> <*dir=*>	<index>: Enter the index number of L2L (LAN to LAN) profile. <pname=>: Enter pname=the name of the profile (e.g.,

<idle=> <palive=>	pname=testname). <ena=>: Enter ena=on or ena=off. In which, on means Enable, off means disable. <nnpkt=>: Enter nnpkt=on or nnpkt=off to pass or block the NetBios Naming Packet. In which, on means pass, off means block. <dir=>: Enter dir=b, dir=o or dir=i to determine the call direction. In which, b means Both, o means Dial-Out and i means Dial-In. <idle=>: Enter idle=-1, idle=0 or idle=other value. In which, -1 means always on for dial-out, 0 means always on for dial-in. Other numbers (e.g., idle=200, idle=300, idle=500) mean the router will be idle after the interval (seconds) configured here. <palive=>: Enter palive=-1, or palive=IP address for PING to keep alive. In which, -1 means to disable the function. If an IP address is specified here, it means to enable PING to the IP address.
For Dial-Out Settings	
<index> <ctype=> *<dialto=> <ltype=>* *<oname=> <opwd=>* *<pauth=> <ovj=> <okey=>* *<ometh=> <sch=>* *<ikemode=> <ikeid=>*	<index>: Enter the index number of L2L (LAN to LAN) profile. <ctype=>: Enter ctype=t, ctype=s, ctype=l, ctype=l1 or ctype=l2 to set "Type of Server I am calling". t, PPTP s, IPSec. l, L2TP(IPSec Policy None). l1, L2TP(IPSec Policy Nice to Have). l2, L2TP(IPSec Policy Must). <dialto=>: Enter dialto=IP address or dialto=Host Name for VPN (such as dialto=draytek.com or dialto=123.45.67.89). <ltype=>: Enter ltype=0, ltype=1, ltype=2 or ltype=3 to specify Link Type. 0, disable 1, 64kbps 2, 128kbps 3, BOD <oname=>: Enter oname=dial-out username (e.g., oname=admin). <opwd=>: Enter opwd=dial-out password (e.g., opwd=1234). <pauth=>: Enter pauth=pc or pauth=p to set PPP authentication. In which, pc means PAP&CHAP, p means AP Only. <ovj=>: Enter ovj=on or ovj=off to enable/disable VJ Compression. <okey=>: Enter okey=IKE Pre-Shared Key to set the PSK (e.g., okey=abcd). <ometh=>: see below Enter ometh=ah a/m/s/S (means AH Auto, AH MD5, AH SHA1, or AH SHA2). Enter ometh=espd a/m/s/S or ometh=espda a/m/s/S (means ESP DES without or with Authentication Auto/ MD5/ SHA1/ SHA2). Enter ometh=esp3 or ometh=esp3a a/m/s/S (means ESP 3DES without or with Authentication Auto /

	MD5/ SHA1/ SHA2). Enter ometh=espa 1/9/2 or ometh=espaa a/m/s/S 1/9/2. (means ESP AES 128/192/256 without or with Authentication Auto/MD5/SHA1/SHA2 (AES128/192/256) <sch=>: Enter sch=1 ~ 15 to select schedule 1 ~ 15. (e.g., sch=1,3,5,7 Set schedule 1->3->5->7) <ikemode=>: Enter ikemode=m or ikemode=a to set IKE phase 1 mode as Main or Aggressive mode. <ikeid=>: Enter ikeid=local ID to set IKE local ID (e.g., ikeid=vigor).
For Dial-In Settings	
<index> <itype=> <peer=> <peerid=> <iname=> <ipwd=> <ivj=> <ikey=> <imeth=>	<index>: Enter the index number of L2L (LAN to LAN) profile. <itype=>: see below Enter itype=t (for PPTP) Enter itype=s (for IPsec) Enter itype=l (for L2TP(IPsec Policy None) Enter itype=l1 (for L2TP(IPsec Policy Nice to Have) Enter itype=l2 (for L2TP(IPsec Policy Must) Enter itype=c (for SSL Tunnel) <peer=>: Enter peer=off or peer=IP address. In which, “off” means any remote IP is allowed to dial in. "IP address" means to allow VPN dial-in with a specified IP address (e.g., 203.12.23.48). <peerid=>: Enter peerid=ID name as the peer ID for remote VPN gateway. For example, peerid=draytek means the word "draytek" is used as the local ID. <iname=>: Enter iname=name as the dial-in username. For example, iname=admin means the word "admin" is used as the username. <ipwd>: Enter ipwd=password as the dial-in password. For example, ipwd=1234 means the word "1234" is used as the password. <ivj>: Enter ivj=on or ivj=off to enable or diable the function of VJ Compression. <ikey>: Enter ikey=ikey as the IKE Pre-Shared Key. For example, ikey=abcd means the word "abcd" is used as the IKE PSK. <imeth=>: Enter imeth=h, d, 3, a to specify the IPsec security method. d, Allow AH d, Allow DES 3, Allow 3DES a, Allow AES
For TCP/IP Settings	
<index> <mywip=> <rgip=> <rnip=> <rnmask=> <lnip=> <lnmask=> <rip=> <mode=> <droute=>	<index>: Enter the index number of L2L (LAN to LAN) profile. <mywip=>: Enter mywip=IP address to set MY WAN IP. For example, mywip=1.2.3.4 means the IP address "1.2.3.4" is used as My WAN IP. <rgip=>: Enter rgip= IP address to set the Remote Gateway IP. For example, rgip=2.3.4.5 means the IP address "2.3.4.5" is used as the Remote Gateway IP. <rnip=>: Enter rnip= IP address to set the Remote Network IP.

	For example, rnip=4.5.6.7 means the IP address "4.5.6.7" is used as the Remote Network IP. <rnmask=>: Enter rnmask=mask address to set the Remote Network Mask. For example, rnmask=255.255.255.0 means the mask address "255.255.255.0" is used as the Remote Network Mask. <lnip=>: Enter lnip=IP address to set the Local Netowrk IP. For example, lnip=1.2.3.4 means the IP address "1.2.3.4" is used as the Local Netowrk IP. <lnmask=>: Enter lnmask=mask address to set the Local Network Mask. For example, lnmask=255.255.255.200 means the mask address "255.255.255.00" is used as the Local Network Mask. <rip=>: Enter rip=d, t, r or b to set RIP Direction. d, Disable t, TX r, RX b, Both <mode=>: Enter mode=r or mode=n. mode=r means to set Route mode for the option of “From first subnet to remote network, you have to do”. mode=n means to set NAT mode for the option of “From first subnet to remote network, you have to do”. <droute=>: Enter droute=off or droute=on for the option of "Change default route to this VPN tunnel (Only single WAN supports this)". droute=on means to enable the fuction. droute=off means to disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..
% Idle Timeout = 250
> vpn option 1 itype=t,s,l2 peer=192.168.1.54 peerid=mary iname=userca
rrie ipwd=12345678 ivj=on ikey=abcd imeth=h
% Change Log..

% Allowed Dial-In Type : PPTP IPsec L2TP(Must)
% Allow dial from (IP) : 192.168.1.54
% Allow dial from (peer id): mary
% Dial-in Username = usercarrie
% Password : 12345678
% VJ Compression (dial-in) = on
% Pre-share Key (dial-in): abcd
% Dial-in IPsec Security Method: AH
>
```

Telnet Command: vpn mroute

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

Syntax

vpn mroute <*index*> **list**

vpn mroute <*index*> **add** <*network ip*>/<*mask*>

vpn mroute <*index*> **del** <*network ip*>/<*mask*>

Syntax Description

Parameter	Description
<*index*> *list*	It means to display the route settings. <index>: Enter an index number (1 ~ 32) of the VPN profile.
<*index*> *add* <*network ip*>/<*mask*>	It means to add a new route. <index>: Enter an index number (1 ~ 32) of the VPN profile. <network ip>/<*mask*>: Enter the IP address with the network mask address (e.g., 192.168.3.5/24).
<*index*> *del* <*network ip*>/<*mask*>	It means to delete specified route. <index>: Enter an index number (1 ~ 32) of the VPN profile. <network ip>/<*mask*>: Enter the IP address with the network mask address (e.g., 192.168.3.5/24).

Example

```
> vpn mroute 1 add 192.168.5.0/24
% 192.168.5.0/24
% Add new route 192.168.5.0/24 to profile 1
```

Telnet Command: vpn list

This command allows users to view LAN to LAN VPN profiles.

Syntax

vpn list <*index*> **all**

vpn list <*index*> **com**

vpn list <*index*> **out**

vpn list <*index*> **in**

vpn list <*index*> **net**

Syntax Description

Parameter	Description
<*index*> *all*	It means to list configuration of the specified profile. <index>: Enter an index number (1 ~ 32) of the VPN profile.
<*index*> *com*	It means to list common settings of the specified profile. <index>: Enter an index number (1 ~ 32) of the VPN profile.
<*index*> *out*	It means to list dial-out settings of the specified profile. <index>: Enter an index number (1 ~ 32) of the VPN profile.
<*index*> *in*	It means to list dial-in settings of the specified profile. <index>: Enter an index number (1 ~ 32) of the VPN profile.
<*index*> *net*	It means to list Network Settings of the specified profile. <index>: Enter an index number (1 ~ 32) of the VPN profile.

Example

```
> rayrouter> vpn list 1 all
 Common Settings

 Profile Name         : name1
 Profile Status       : Enable
 VPN Connection Through   : WAN1 First
 Dialout WAN IP Alias Index  : None
 Netbios Naming Packet  : Pass
 Call Direction       : Dial-In
 Idle Timeout         : 300
 PING to keep alive    : off

 Dial-out Settings

 Type of Server       : ISDN
 Link Type:          : 64k bps
 Username            : ???
 Password            :
 PPP Authentication   : PAP/CHAP
 VJ Compression       : on
 Pre-Shared Key       :
 IPsec Security Method : AH
 Schedule            : 0,0,0,0
 Remote Callback      : off
 Provide ISDN Number   : off
 IKE phase 1 mode     : Main mode
 IKE Local ID        :

 Dial-In Settings
...
```

Telnet Command: vpn remote

This command allows users to enable or disable *PPTP/IPSec/L2TP* VPN service.

Syntax

vpn remote *<PPTP/IPsec/L2TP/SSLVPN> <on/off>*

Syntax Description

Parameter	Description
<PPTP/IPsec/L2TP/SSLVPN> <on/off>	<PPTP/IPsec/L2TP/SSLVPN>: There are four types to be selected. Enter PPTP, IPsec, L2TP or SSLVPN. <on/off>: Enter on or off. on – enable VPN remote setting. off – disable VPN remote setting.

Example

```
> vpn remote PPTP on
Set PPTP VPN Service : On

Please restart the router!!
```

Telnet Command: vpn 2ndsubnet

This command allows users to enable second subnet IP as VPN server IP.

Syntax

vpn 2ndsubnet <*on/off***>**

Syntax Description

Parameter	Description
<on/off>	<on/off>: Enter on or off. on: enable or disable second subnet. off: disable the second subnet.

Example

```
> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!
```

Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

Syntax

vpn NetBios set *<H2I/L2I> <index> <Block/Pass>*

Syntax Description

Parameter	Description
<H2I/L2I> <index> <Block/Pass>	<H2I/L2I>: Enter H2I or L2L. Specify which one will be applied by NetBios. H2I, means Remote Access User Accounts. L2I, means LAN-to-LAN Profile. <index>: Enter an index number of the profile. <Block/Pass>: Enter Pass or Block. Pass – Have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, set it block data transmission of Netbios Naming Packet inside the tunnel.

Example

```
> vpn NetBios set H2l 1 Pass
% Remote Dial In Profile Index [1] :
% NetBios Block/Pass: [PASS]
```

Telnet Command: vpn mss

This command allows users to configure the maximum segment size (MSS) for different TCP types.

Syntax

vpn mss show

vpn mss default

vpn mss set <*connection type*> <*TCP maximum segment size range*>

Syntax Description

Parameter	Description
show	It means to display current setting status.
default	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
set	Use it to specify the connection type and value of MSS.
<*connection type*> <*TCP maximum segment size range*>	<connection type>: Enter 1, 2, 3, 4 or 5. 1, PPTP 2, L2TP 3, IPSec 4, L2TP over IPSec 5, SSL Tunnel <TCP maximum segment size range>: Enter a value. Each type has different segment size range. PPTP, 1 ~ 1412 L2TP, 1 ~ 1408 IPSec, 1 ~ 1381 L2TP over IPSec, 1 ~ 1361 SSL Tunnel, 1 ~ 1360

Example

```
> vpn mss set 1 1400
% VPN TCP maximum segment size (MSS) :
  PPTP  = 1400
  L2TP  = 1360
  IPsec = 1360
  L2TP over IPsec  = 1360
  SSL Tunnel  = Not yet setting!
```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

Syntax

vpn ike -q

vpn ike -s

vpn ike v2

vpn ike v2 debug <*on/off*>

Syntax Description

Parameter	Description
-q	Display IKE memory status an dleakage list.
-s	Display IPsec state list.
V2 debug <on/off>	It is used for RD debug.

Example

```
> vpn ike -q
IKE Memory Status and Leakage List

# of free L-Buffer=95, minimum=94, leak=1
# of free M-Buffer=529, minimum=529 leak=3
# of free S-Buffer=1199, minimum=1198, leak=1
# of free Msgid-Buffer=1024, minimum=1024
```

Telnet Command: vpn Multicast

This command allows users to pass or block the multi-cast packet via VPN**.**

Syntax

vpn Multicast set <*H2L/L2L*> <*index*> <*Block/Pass*>

Syntax Description

Parameter	Description
<*H2L/L2L*> <*index*> <*Block/Pass*>	<H2L/L2L>: Enter H2L or L2L. Specify which one will be applied for multi-cast packets. H2L, means Host to LAN (Remote Access User Accounts). L2L, means LAN-to-LAN Profile. <index>: Enter an index number of the profile. <Block/Pass>: Enter Pass or Block the Multicast Packets..

Example

```
> vpn Multicast set L2L 1 Pass
% Lan to Lan Profile Index [1] :
% Status Block/Pass: [PASS]
```

Telnet Command: vpn pass2nd

This command allows users to determine if the packets coming from the second subnet passing through current used VPN tunnel.

Syntax

vpn pass2nd <*on/off***>**

Syntax Description

Parameter	Description
<*on/off***>**	**<**on/off>: Enter on or off.

	on – the second subnet is allowed to pass VPN tunnel. off –the second subnet is not allowed to pass VPN tunnel.

Example

```
> vpn pass2nd on
% 2nd subnet is allowed to pass VPN tunnel!
```

Telnet Command: vpn pass2nat

This command allows users to determine if the packets passing through by NAT or not when the VPN tunnel disconnects.

Syntax

vpn pass2nat <*on/off***>**

Syntax Description

Parameter	Description
<*on/off***>**	**<**on/off>: Enter on or off. on – the packets can pass through NAT. off – the packets cannot pass through NAT.

Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

Telnet Command: vpn sameSubnet

This command allows users to build VPN between clients via virtual subnet.

vpn sameSubnet *–I <value>*

vpn sameSubnet *–E <0/1>*

vpn sameSubnet *–e <value>*

vpn sameSubnet *–I <IP address>*

vpn sameSubnet *–o <add/del>*

vpn sameSubnet *–v*

Syntax Description

Parameter	Description
–I <value>	It means to specify the index number of VPN profile. <value>: Enter the index number of the VPN profile.
–E <0/1>	It means to enable / disable the IpsecWithSameSubnet. <0/1>: Enter 0 or 1. 0: Disable 1: Enable.
–e <value>	It means to translate LAN subnet to virtual subnet. <value>: Enter 1, 2 1: LAN1 2: LAN2
–I <IP address>	Set the IP address as the virtual subnet.
–o <add/del>	Specify the operation to be performed. <add/del>: Enter add or del.
-v	View the current settings. However, only the enabled profile will be viewed.

Example

```
> vpn sameS  -i 1 -e 1 -E 1 -e 1 -I 10.10.10.0 -o add
> vpn sameS -v
IPsec with the same subnet:
VPN profile 1 enable,
 % translated LAN1 to Virtual subnet: 10.10.10.0
```

Telnet Command: wan ppp_mru

This command allows users to adjust the size of PPP LCP MRU. It is used for specific network.

Syntax

wan ppp_mru *<WAN interface number> <MRU size >*

Syntax Description

Parameter	Description
<WAN interface number> *<MRU size>*	<WAN interface number>: Enter a number (1 ~5) to represent the physical interface. (1 means WAN1, 2 means WAN2, …)

	<MRU size>: Enter a value (1400 ~ 1600) to set the number of PPP LCP MRU.

Example

```
>wan ppp_mru 1 ?
% Now: 1492

> wan ppp_mru 1 1490
>
> wan ppp_mru 1 ?
% Now: 1490

> wan ppp_mru 1 1492
> wan ppp_mru 1 ?
% Now: 1492
```

Telnet Command: wan mtu

This command allows users to adjust the size of MTU for WAN1.

Syntax

wan mtu <*value*>

Syntax Description

Parameter	Description
<*value*>	It means the number of MTU for PPP. The available range is from 1000 to 1500. For Static IP/DHCP, the maximum number will be 1500. For PPPoE, the maximum number will be 1492. For PPTP/L2TP, the maximum number will be 1460.

Example

```
> wan mtu 1100
> wan mtu ?
Static IP/DHCP (Max MSS: 1500)
PPPoE(Max MSS: 1492)
PPTP/L2TP(Max MSS: 1460)
% wan ppp_mss <MSS size: 1000 ~ 1500>
% Now: 1100
```

Telnet Command: wan dns

This command allows you to configure the DNS server.

Syntax

wan dns <*wan_no*> <*dns_select*> <*ipv4_addr*>

Syntax Description

Parameter	Description
<*wan_no*> <*dns_select*> <*ipv4_addr*>	<wan_no>: Enter 1 or 2. It means to indicate the WAN interface. 1, WAN1 2, WAN2 <dns_select>: Enter pri or sec.

	pri, primary DNS sec, secondary DNS <ipv4_addr>: Enter the IPv4 address for the DNS server.

Example

```
> wan dns 1 pri 192.168.1.126
% Set WAN1 primary DNS done.
% Now: 192.168.1.126
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

wan DF_check <*on/off*>

Syntax Description

Parameter	Description
<*on/off*>	<on/off>: Enter on or off. on, enable DF. off, disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
> wan DF_check off
%DF bit check disable (reset DF bit)!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to disable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

Syntax

wan forward <*on/off*>

Syntax Description

Parameter	Description
<on/off>	<on/off>: Enter on or off. on, enable WAN forward. off, disable WAN forward.

Example

```
> wan forward ?
%WAN forwarding is Disable!

> wan forward on
%WAN forwarding is enable!
```

Telnet Command: wan status

This command allows you to display the status of WAN connection, including connection mode, TX/RX packets, DNS settings and IP address.

Example

```
> wan status
WAN1: Offline, stall=Y
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0
 Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0

WAN2: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0
 Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0

PVC_WAN3: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0
 Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0

PVC_WAN4: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0
 Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0

PVC_WAN5: Offline, stall=N

 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0

PVC_WAN6: Offline, stall=N

 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0

PVC_WAN7: Offline, stall=N

 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0
```

Telnet Command: wan detect

This command allows you to configure WAN connection detection. When Ping Detection is enabled (for Static IP or PPPoE mode), Router pings specified IP addresses to detect the WAN connection.

Syntax

wan detect <wan1> *<on/off/always_on>*

wan detect <wan1> *<off> -t <time>*

wan detect <wan1> *<off> -i <Interval>*

wan detect <wan1> *target <ip addr>*

wan detect <wan1> *ttl <1-255>*

wan detect <wan1> target2 *<ip addr>*

wan detect <wan1> target_gw *<1/0>*

wan detect <wan1> interval *<interval>*

wan detect <wan1> retry *<retry>*

wan detect status

Syntax Description

Parameter	Description
<wan1> <on/off/always_on>	<wan1>: Enter wan1 to specify WAN1. <on/off/always_on>: Enter on, off, or always_on. On, enable ping detection. Off, enable the ARP detection. Always_on, disable the link detection. The connnection is always on.
<wan1> <off> -t <time>	<wan1>: Enter wan1 to specify WAN1. <off>: Enter off. <time>: Enter a time value. The default value is “30” and the range shall be 1 to 255.
<wan1> <off> -i <Interval>	<wan1>: Enter wan1 to specify WAN1. <off>: Enter off. <interval>: Enter a value. It is the interval for the system to execute the PING operation. The default value is “5” and it shall be smaller than time setting.
<wan1> target <ip addr>	<wan1>: Enter wan1 to specify WAN1. <ip addr>: Enter an IP address as the ping target.
<wan1> ttl <1-255>	<wan1>: Enter wan1 to specify WAN1. <1-255>: It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
<wan1> target2 <ip addr>	<wan1>: Enter wan1 to specify WAN1. <ip addr>: Enter an IP address as the the secondary ping target.
<wan1> target_gw <1/0>	<wan1>: Enter wan1 to specify WAN1. <1/0>: Enter 1 or 0 to set whether to use gateway as ping

	target. (1, yes; 0, no) Note that USB WAN (PPP mode) cannot support PING gateway
<wan1> interval<Interval>	<wan1>: Enter wan1 to specify WAN1. <interval>: Enter a value to set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second.
<wan1> retry <retry>	<wan1>: Enter wan1 to specify WAN1. <retry>: Enter a number to set how many ping operations are retried before the Router judges that the WAN connection is disconnected. Available setting is between 1 and 255. The unit is times.
status	It means to show the current status.

Example

```
> wan detect status
 WAN1: off, send time=30, Interval = 5
 WAN2: off, send time=30, Interval = 5
 WAN3: off, send time=30, Interval = 5
 WAN4: off, send time=30, Interval = 5
 WAN5: off, send time=30, Interval = 5
 WAN6: off, send time=30, Interval = 5>
```

Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

Syntax

wan mvlan *<pvc_no/status/save/enable/disable> <on/off/clear/tag tag_no> <service type/vlan priority> <px ... >*

wan mvlan *keeptag <pvc_no><on/off>*

Syntax Description

Parameter	Description
<pvc_no/status/save/enable/disable> <on/off/clear/tag tag_no> <service type/vlan priority> <px ... >	<pvc_no/status/save/enable/disable>: see below, <pvc_no>: Enter the index number of PVC. It means index number of PVC. There are 8 PVC, 0(Channel-1) to 7(Channel-8) allowed to be configured. However, bridge mode can be set on PVC number 2 to 7. <status>: Enter status to display the whole Bridge status. <save>: Enter save to save the configuration into flash of Vigor router. <enable>: Enter enable for enabling the Multi-VLAN function. <disable>: Enter disable for disabling the Multi-VLAN function. <on/off/clear/tag tag_no>: see below. <on>: Enter on to turn on bridge mode for the specific channel. <off>: Enter off to turn off bridge mode for the specific

	channel. <clear>: Enter clear to clear the port setting. <tag tag_no>: Enter a tag number (-1, 1~4095) for VLAN (e.g, tag -1, tag 100, and etc.) <service type/vlan priority>: Enter 0 or 1 (for service type, 0 for Normal, 1 for IGMP), or enter a value (0~7) for VLAN priority. <px ... >: Enter 2, 3 or 4. It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
keeptag	It means Multi-VLAN packets will keep their VLAN headers to LAN.

Example

```
> wan mvlan 7 on p2
 PVC  Bridge   p1   p2   Service Type    Tag      Priority

-------------------------------------------------------------------------
   7    OFF    0    0       Normal      0(OFF)        0
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

wan multifno <*channel #*> <*WAN interface #*>

wan multifno *status*

Syntax Description

Parameter	Description
<*channel #*> <*WAN interface #*>	<channel #>: Enter channel 5, channel 6, channel 7 or channel 8. <WAN interface #>: Enter 1 or 2 to indicate the WAN interface. 1, WAN1 2, WAN2
status	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
>
```

Telnet Command: wan vlan

This command allows you to configure the VLAN tag of WAN1.

Syntax

wan vlan wan <*#*> *tag* <*value*>

wan vlan wan <#> <*enable/disable*>

wan vlan wan <#> *pri* <*value*>

wan vlan stat

Syntax Description

Parameter	Description
wan <#> *tag* <*value*>	Specify which WAN interface will be tagged. <#>: Enter 1 for WAN1. tag: Type a number for tagging on WAN interface. <value>: Enter a number.
wan <#> <*enable/disable*>	<#>: Enter 1 for WAN1. <enable/disable>: Enter enable or disable. Enable: Specified WAN interface will be tagged. Disable: Disable the function of tagging on WAN interface.
wan <#> *pri* <*value*>	It means the priority for such VLAN. <#>: Enter 1 for WAN1. <value>: Enter 0 ~ 7.
stat	Display current VLAN status.

Example

```
> wan vlan stat
 Interface    Pri     Tag    Enabled
 ======================================
 WAN1 (ADSL)   0      0
```

Telnet Command: wan detect_mtu

This command allows you to run a WAN MTU Discovery. The user can specify an IPv4 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu -i <*Host/IP address*> *-s* <*mtu_size*> *-d* <*decrease size*> *-w* <*1*> *-c* <*1-10*>

Syntax Description

Parameter	Description
-i <*Host/IP address*> *-s* <*mtu_size*> *-d* <*decrease size*> *-w* <*1*> *-c* <*1-10*>	-i <Host/IP address>: Enter the IP address/domain name of the target to detect. -s <mtu_size>: Enter a value (1000 ~ 1500) as the MTU size you want to start to decrease. -d <decrease size>: Enter a value (1 ~ 100) as the MTU size to decrease between detections. -w <1>: Enter 1 to specify WAN1. -c <1~10>: Enter a value (1~10) to set the times to send the ping packets out. Default value is 3.

Example

```
> wan detect_mtu -w 1 -i 8.8.8.8 -s 1500 -d 30 -c 10
 detecting  mtu size:1500!!!

 mtu size:1470!!!
```

Telnet Command: wan detect_mtu6

This command allows you to run a WAN MTU Discovery. The user can specify an IPv6 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu6 *-i <Host/IP address> -s <mtu_size> -w <1>*

Syntax Description

Parameter	Description
-i <Host/IP address> -s <mtu_size> -w <1>	-i <Host/IP address>: Enter the IPv6 address/domain name of the target to detect. -s <mtu_size>: Enter a value (1280 ~ 1500) as the MTU size you want to start to decrease. -w <1>: Enter 1 to specify WAN1.

Example

```
> wan detect_mtu6 -w 2 -i 2404:6800:4008:c06::5e -s 1500
>
```

Telnet Command: wl acl

This command allows the user to configure wireless access control settings.

Syntax

wl acl enable *<ssid1 ssid2 ssid3 ssid4>*

wl acl disable *<ssid1 ssid2 ssid3 ssid4>*

wl acl add *<MAC> <ssid1 ssid2 ssid3 ssid4> <comment> <isolate>*

wl acl del *<MAC>*

wl acl mode *<ssid1 ssid2 ssid3 ssid4> <white/black>*

wl acl show

wl acl showmode

wl acl clear

Syntax Description

Parameter	Description
enable <ssid1 ssid2 ssid3 ssid4>	<ssid1 ssid2 ssid3 ssid4>: Enter ssid1, ssid2, ssid3, or ssid4 to enable the settings for SSID1, SSID2, SSID3 or SSID4.
disable <ssid1 ssid2 ssid3 ssid4>	<ssid1 ssid2 ssid3 ssid4>: Enter ssid1, ssid2, ssid3, or ssid4 to disable the settings for SSID1, SSID2, SSID3 or SSID4.
add <MAC> <ssid1 ssid2 ssid3 ssid4> <comment> <isolate>	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx <MAC>: Enter a MAC address.

	<ssid1 ssid2 ssid3 ssid4>: Enter ssid1, ssid2, ssid3, or ssid4 to select SSID1, SSID2, SSID3 or SSID4. <comment>: Enter a brief decription. <isolate>: Enter isolate.
del <MAC>	It means to delete a MAC address entry defined in the access control list. <MAC>: Enter a MAC address.
mode <ssid1 ssid2 ssid3 ssid4> <white/black>	It means to set white/black list for each SSID. <ssid1 ssid2 ssid3 ssid4>: Enter ssid1, ssid2, ssid3, or ssid4 to select SSID1, SSID2, SSID3 or SSID4. <white/black>: Enter white or black.
wl acl show	It means to show access control status.
wl acl showmode	It means to show the mode for each SSID.
wl acl clean	It means to clean all access control setting.

Example

```
> wl acl add 00-1D-AA-93-9F-3C ssid1 test isolate
 Set Done !!
> wl acl show
 ----------Mac Address Filter Status---------
 SSID1: Disable
 SSID2: Disable
 SSID3: Disable
 SSID4: Disable

 ----------MAC Address List----------
 Index   Attribute      MAC Address        Associated SSIDs        Comment
   1       s          00:1d:aa:93:9f:3c   SSID1                 test

 s: Isolate the station from LAN
> wl acl showmode
 SSID1: None
 SSID2: None
 SSID3: None
 SSID4: None
>
```

Telnet Command: wl config

This command allows users to configure general settings and security settings for wireless connection.

Syntax

wl config *mode <value>*

wl config *mode show*

wl config *channel <number>*

wl config *preamble <enable>*

wl config *txburst <enable>*

wl config *ssid <ssid_num><enable> <ssid_name> <hidden_ssid>*

wl config *security <SSID_NUMBER> <mode>*

wl config *ratectl <ssid_num><enable> <upload download>*

wl config *isolate <ssid_num> <lan member>*

wl config *dtim <value>*

wl config *beaconperiod <value>*

wl config *radio <enable>*

wl config *frag <value>*

wl config *rts <value>*

wl config *rate_alg <value>*

wl config *country <value>*

Syntax Description

Parameter	Description
mode <value>	It means to select connection mode for wireless connection. <value>: Enter 11bg, 11gn, 11bgn, 11n, 11g or 11b to set connection mode for wireless connection.
mode show	It means to display what the current wireless mode is.
channel <number>	It means the channel of frequency of the wireless LAN. <number>: Enter 0,1,2,3,4,5,6,7,8,9,10,11,12 or 13. number=0, means Auto number=1, means Channel 1 …. number=13, means Channel 13.
preamble <enable>	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. <enable>: Enter 0 or 1. 0, disable to use long preamble. 1, enable to use long preamble.
txburst <enable>	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. <enable>: Enter 0 or 1. 0, disable the function. 1, enable the funciton.
ssid <ssid_num> <enable> <ssid_name> <hidden_ssid>	It means to set the name of the SSID, hide the SSID if required. <ssid_num>: Enter 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <enable>: Enter 1 or 0. 1, enable; 0, disable. <ssid_name>: Enter a name for the specified SSID. <hidden_ssid>: Enter 0 to hide the SSID or 1 to display the SSID
security <SSID_NUMBER>	It means to configure security settings for the wirelesss

<mode><key><index>	connection. <SSID_NUMBER>: Enter 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <mode>: Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP <key>: Enter a string. You have to add keys for *wpapsk, wpa2psk, wpamixpsk* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format. <index>: Enter an index number.
ratectl <ssid_num><enable> <upload download>	It means to set the rate control for the specified SSID. <ssid_num>: Enter 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <enable>: Enter 0 or 1. It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. <upload>: Enter a value. It means to configure the rate control for data upload. The unit is kbps. <download>: Enter a value. It means to configure the rate control for data download. The unit is kbps.
Isolate <ssid_num> <lan member>	It means to isolate the wireless connection for LAN and/or Member. <ssid_num>: Enter 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <lan> – It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. Enter 1 to enable, or 0 to disable. <member> – It can make the wireless clients (stations) with the same SSID not accessing for each other. Enter 1 to enable, or 0 to disable.
dtim <value>	<value>: Enter a number (1 ~255) to set DTIM.
beaconperiod <value>	<value>: Enter a number (20 ~1023, unit in milli-seonds) as beacon period.
radio <enable>	<enable>: Enter 1 or 0 to enable or disable the wireless radio.
frag <value>	<value>: Enter a number (256 ~2346) to set fragment threshold.
rts <value>	<value>: Enter a number (1 ~2347) to set RTS threshold.
rate_alg <value>	<value>: Enter 0, or 1 to set the version of rate algorithm. 0, old algorithm 1, new algorithm

country <value>	<value>: Enter two capital letters (e.g., TW) to specify the country.

Example

```
> wl config mode 11bgn
 Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
 Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
 Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
 SSID  Enable  Hide_SSID  Name
 1     1       0         dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
% SSID1
%%  Mode: wpa1x
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
> wl config isolate 1 1 1
```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

Syntax

wl set <*SSID***> <***CHAN***> <***En***>**

wl set *txburst <enable>*

Syntax Description

Parameter	Description
<*SSID***> <***CHAN***> <***En***>**	<SSID>: Enter a SSID for the router. The maximum character that you can use is 32. <CHAN>: Enter a number (1~13) for selecting a channel. <En>: Enter on or off. on, enable the function. off, disable the function.
txburst <enable>	It means to enhance the performance in data transmission about 40%* more (by enabling *Tx Burst).* It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. <enable>: Enter 0 or 1. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
```

```
% New Wlan Setting is:
% SSID=MKT
% Chan=2
% Wl is Enable
```

Telnet Command: wl act

This command allows users to activate wireless settings.

Syntax

wl act <*En***>**

Syntax Description

Parameter	Description
<*En*>	It means to enable or disable the function of VPN isolation. <enable>: Enter 0 or 1. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl iso_vpn

This command allows users to activate the function of VPN isolation.

Syntax

wl iso_vpn *<ssid> <En>*

Syntax Description

Parameter	Description
<ssid> <En>	<SSID>: Enter 1, 2, 3 or 4 to specify each SSID. 1, SSID1 2, SSID2 3, SSID3 4, SSID4 <En>: Enter 1 or 0 to enable or disable the function of VPN isolation. 0, disable 1, enable

Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

Syntax

wl wmm *ap QueIdx Aifsn Cwmin Cwmax Txop ACM*

wl wmm *bss QueIdx Aifsn Cwmin Cwmax Txop ACM*

wl wmm *ack Que0_Ack Que1_Ack Que2_Ack Que3_Ack*

wl wmm *enable SSID0 SSID1 SSID2 SSID3*

wl wmm *apsd value*

wl wmm *show*

Syntax Description

Parameter	Description
ap QueIdx Aifsn Cwmin Cwmax Txop ACM	It means to set WMM for access point. · QueIdx means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video. · Aifsn controls how long the client waits for each data transmission. · CWMin means contention Window-Min and CWMax means contention Window-Max. Specify the value ranging from 1 to 15. · Txop means transmission opportunity. Specify the value ranging from 0 to 65535.

	· ACM can restrict stations from using specific category class if it is enabled. Example: *wl wmm ap 0 3 4 6 0 0*
bss QueIdx Aifsn Cwmin Cwmax Txop ACM	It means to set WMM for wireless clients. · QueIdx means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video. · Aifsn controls how long the client waits for each data transmission. · CWMin means contention Window-Min and CWMax means contention Window-Max. Specify the value ranging from 1 to 15. · Txop means transmission opportunity. Specify the value ranging from 0 to 65535. · ACM can restrict stations from using specific category class if it is enabled. Example: *wl wmm bss 0 3 4 10 0 0*
ack Que0_Ack Que1_Ack Que2_Ack Que3_Ack	It means to map to the Ack policy settings of AP WMM. Example: *wl wmm ack 0 0 0 0*
enable SSID0 SSID1 SSID2 SSID3	It means to enable the WMM for each SSID. 0: disable 1: enable Example: *wl wmm enable 1 1 1 1*
Apsd [value]	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable Example: *wl wmm apsd 1*
show	It displays current status of WMM.

Example

```
> wl wmm ap 0 3 4 6 0 0
 QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm show
 Enable WMM: SSID0 =1, SSID1 =1,SSID2 =1,SSID3 =1
APSD=0
QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
QueIdx=1: APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0
QueIdx=2: APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0
QueIdx=3: APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0
QueIdx=0: BSSAifsn=3,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
QueIdx=1: BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
QueIdx=2: BSSAifsn=2,BSSCwmin=3,BSSCwmax=4, BSSTxop=94,BSSACM=0
QueIdx=3: BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0
AckPolicy[0]=0: AckPolicy[1]=0,AckPolicy[2]=0,AckPolicy[3]=0
```

```
>
```

Telnet Command: wl ht

This command allows you to configure wireless settings.

Syntax

wl ht *bw value*

wl ht *gi value*

wl ht *badecline value*

wl ht *autoba value*

wl ht *rdg value*

wl ht *msdu value*

wl ht *txpower value*

wl ht *antenna value*

wl ht *greenfield value*

Syntax Description

Parameter	Description
bw value	<value>: Enter 0 or 1. 0 (for BW_20) and 1 (for BW_40).
gi value	<value>: Enter 0 or 1. 0 (for GI_800) and 1 (for GI_4001)
badecline value	<value>: Enter 0 or 1. 0 (for disabling) and 1 (for enabling).
autoba value	<value>: Enter 0 or 1. 0 (for disabling) and 1 (for enabling).
rdg value	<value>: Enter 0 or 1. 0 (for disabling) and 1 (for enabling).
msdu value	<value>: Enter 0 or 1. 0 (for disabling) and 1 (for enabling).
txpower value	<value>: Enter 1 ~ 6 (level).
antenna value	<value>: Enter 0,1,2 or3. 0, 2T3R 1, 2T2R 2, 1T2R 3, 1T1R
greenfield value	<value>: Enter 0 or 1. 0 (for mixed mode) and 1 (for green field).

Example

```
> wl ht bw value 1
 BW=0
 <Note> Please restart wireless after you set new parameters.
```

```
> wl restart
 Wireless restart.............
```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart
 Wireless restart.............
```

Telnet Command: wl wds

This command allows you to configure WDS settings.

Syntax

wl wds *mode <value>*

wl wds *security <value>*

wl wds *ap <value>*

wl wds *hello <value>*

wl wds *status*

wl wds *show*

wl wds *mac add <index addr>*

wl wds *mac <clear/disable/enable> <index/all>*

wl wds *flush*

Syntax Description

Parameter	Description
mode <value>	It means to specify connection mode for WDS. <value>: Enter d, b or or. d, Disable b, Bridge r, Repeapter
security <value>	It means to configure security mode with encrypted keys for WDS. <value>: Available settings are: disable: No security. wep: WEP wpapsk <key>: WPA/PSK wpa2psk <key>: WPA2/PSK key: Moreover, you have to add keys for *wpapsk, wpa2psk,* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format. e.g., *wl dual wds security disable* *wl dual wds security wep 12345* *wl dual wds security wpa2psk 12345678*

ap <*value*>	It means to enable or disable the AP function. <value>: Enter 1 or 0. 1,– enable the function. 0, disable the function.
hello <*value*>	It means to send hello message to remote end (peer). <value>: Enter 1 or 0. 1, enable the function. 0, disable the function.
status	It means to display WDS link status for 2.4GHz connection.
show	It means to display current WDS settings.
mac add <*index addr*>	add <index addr> –Enter the index number and the MAC address. Add the peer MAC entry in Repeater/Bridge WDS MAC table. e.g., *wl wds mac add 1 00:1D:AA:93:9F:3C*
mac <*clear/disable/enable*> <*index/all*>	clear/disable/enable **<***index/all*> - Clear, disable, enable the specifed or all MAC entries in Repeater/Bridge WDS MAC table. e.g, *wl dual wds mac enable 1*
flush	It means to reset all WDS setting.

Example

```
> wl wds status
Please enable WDS hello function first.

> wl wds hello 1
% <Note> Please restart router after you set the parameters.

> wl wds status
```

Telnet Command: wl btnctl

This command allows you to enable or disable wireless button control.

Syntax

wl btnctl <*value*>

Syntax Description

Parameter	Description
<*value*>	<value>: Enter 0 or 1. 0, disable 1, enable

Example

```
> wl btnctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

Telnet Command: wl iwpriv and wl ce_cert

These commands are reserved for RD debug. Do not use them.

Telnet Command: wl efuse

This command is used to configure parameters related to wireless RF hardware. At present, it is not allowed for end user to operate.

Telnet Command: wl stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

wl stalist *show*

wl statlist *num*

Syntax Description

Parameter	Description
show	Display the station list.
num	Display the number of wireless station.

Example

```
> wl stalist show
2.4G Wireless Station List :

Index  Status  IP Address      MAC Address       Associated with


Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.
```

Telnet Command: apm enable / disable / show /clear/discover/query

The apm command(s) is use to display, remove, discover or query the information of VigorAP registered to VigorLTE 200.

Syntax

apm enable

amp disable

apm show

apm clear

apm discover

apm query

Syntax Description

Parameter	Description
enable	Enable the APM function.
disable	Disable the APM function.
show	It displays current information of APM profile.
clear	It is used to remove all of the APM profile.
discover	It is used to search VigorAP on LAN.
query	It is used to query any VigorAP which has been registered to APM (Central AP Management) in VigorLTE 200. Information related to the registered AP will be send back to VigorLTE 200 for updating the web page of Central AP Management.

Example

```
> apm clear ?
Clear all clients ... done
```

Telnet Command: apm profile

This command allows to configure wireless profiles to be used in Central AP Management.

Syntax

apm profile *clone <from index><to index><new name>*

apm profile *del <index>*

apm profile *reset*

apm profile *summary*

apm profile *show <profile index>*

apm profile *apply <profile index> <client index1<index2 .. index5>>*

Syntax Description

Parameter	Description
clone <from index><to index><new name>	It is used to copy the same parameters settings from one profile to another APM profile.

	<from index>: Enter the index number of the profile. It is the original APM profile to be cloned to other APM profile. <to index>: Enter an index number. It is the target profile which will clone the parameters settings from an existed APM profile. <new name>: Enter a name for a new APM profile.
del <index>	It is used to delete a specified APM profile. The default (index #1) should not be deleted. <index>: Enter the index number of existed profile.
reset	It is used to reset to factory settings for WLAN profile.
summary	It is used to list all of the APM profiles with required information.
show <profile index>	It is used to display specified APM profile. <profile index>: Enter the index number of existed profile.
apply <profile index> <client index1<index2 .. index5>>	It is used to apply the selected APM profile onto specified VigorAP. <profile index>: Enter the index number of existed profile. <client index1… index5>: Enter the index number of the selected APM profiel to the specified VigorAP.

Example

```
> apm profile clone 1 2 forcarrie
(Done)

> apm profile summary
# Name           SSID           Security    ACL    RateCtrl(U/D)
- ---------------- ---------------- ------------ ------- ------
0 Default       DrayTek-LAN-A    WPA+WPA2/PSK x          - /     -
                DrayTek-LAN-B    WPA+WPA2/PSK x          - /     -

1 -              -              -           -                 -
2 forcarrie       DrayTek         Disable     x          - /     -

3 -              -              -           -                 -
4 -              -              -           -                 -
```

Telnet Command: apm cache

This command is used to display or remove the information of registered VigorAP, including MAC address, name, and authentication. Up to 30 entries of registered information can be stored and displayed.

Syntax

apm cache *show*

apm cache *clear*

Syntax Description

Parameter	Description
show	It means to display the information related to VigorAP registered VigorLTE 200.

clear	It means to remove the information related to VigorAP registered VigorLTE 200.

Example

```
> apm cache show
MAC         Name               Auth
------------ -------------------- --------------------

>
```

Telnet Command: apm lbcfg

This command allows to set parameters related to AP management control.

Syntax

apm lbcfg <*set***> <***value***>**

apm lbcfg <*show*>

Syntax Description

Parameter	Description
<*set***> <***value***>**	It means to set the load balance configuration file for APM. <set>: Enter 1 ~ 11. <value>: Enter 1 (enable) or 0 (disable). Each number represents different setting value. [1] – The first number means the load balance function. 1 – enable load balance, 0 – disable load balance. [2] – The second number means the station limit function. 1 –enable station limit, 0 – disable station limit. [3] – The third number means the traffic limit function. 1 – enable traffic limit, 0 – disable traffic limit. [4] – The forth number means the limit num of station. Available range is 3~64. [5] – The fifth number means the upload limit function. 1 – enable upload limit, 0 – disable upload limit. [6] – The sixth number means the download limit function. 1 – enable download limit, 0 – disable download limit. [7] – The seventh number means disassociation by idle time. 1 – enable disassociation, 0 – disable disassociation. [8] – The eighth number means to enable or disable disassociation by signal strength. 1 – enable disassociation, 0 – disable disassociation. [9] – The ninth number means to determine the unit of traffic

	limit (for upload) 1 – Mbps 0 – kbps [10] – The tenth number means to determine the unit of traffic limit (for download) 1 – Mbps 0 – kbps [11] - Define the RSSI threshold (-200 ~ -50 dbm)
show	It shows the configuration value.

Example

```
> apm lbcfg set 1 1 1 32 100 200 1 1 1 0 -200
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 1
2. Enable station limit : 1
3. Enable traffic limit : 1
4. Limit Number : 32
5. Upload limit : 100
6. Download limit : 200
7. Enable disassociation by idle time : 1
8. Enable disassociation by Signal strength : 1
9. Traffic limit unit (upload)   : 1
10.Traffic limit unit (download) : 0
11.RSSI threshold : -200
flag : 31
```

Telnet Command: apm apsyslog

This command is used to display the AP syslog data coming form VigorAP.

Syntax

apm apsyslog <*AP_Index*>

Syntax Description

Parameter	Description
<*AP_Index*>	Specify the index number which represents VigorAP.

Example

```
> apm apsyslog 1
8d 02:46:09  syslog: [APM] Send Rogue AP Detection data.
8d 02:53:04  syslog: [APM] Run AP Detection / Discovery.
8d 02:56:09  syslog: [APM] Send Rogue AP Detection data.
8d 03:00:42  kernel: 60:fa:cd:55:f5:ea had disassociated.
8d 03:03:12  syslog: [APM] Run AP Detection / Discovery.
8d 03:06:09  syslog: [APM] Send Rogue AP Detection data.
8d 03:13:21  syslog: [APM] Run AP Detection / Discovery.
8d 03:16:10  syslog: [APM] Send Rogue AP Detection data.
8d 03:16:41  kernel: 60:fa:cd:55:f5:ea had associated successfully
8d 03:16:55  kernel: 60:fa:cd:55:f5:ea had disassociated.
```

Telnet Command: apm syslog

This command is used to display related syslog data from central AP management.

Syntax

apm syslog

Example

```
> apm syslog
"2015-11-04 12:24:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"
2015-11-04 12:24:56", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
2015-11-04 12:34:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"
2015-11-04 12:34:57", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
```

Telnet Command: apm stanum

This command is used to display the total number of the wireless clients, no matter what mode of wireless connection (2.4G WLAN or 5G WLAN) used by wireless clients to access into Internet through VigorAP.

Syntax

apm stanum <*AP_Index*>

Syntax Description

Parameter	Description
<*AP_Index*>	Specify the index number which represents VigorAP.

Example

```
> apm stanum

% Show the APM AP Station Number data.
% apm stanum AP_Index.
%     ex : apm stanum 1
%          Idx Nearby(2.4/5G) Conn(2.4/5G)
%           1   2   5          0   0
%           2   2   5          1   0
%           3   2   5          1   0
```

Telnet Command: service

This command is used to display information about Myvigor service. In addition, it allows to transfer MyVigor service from the original account to other account.

Syntax

service -s

service -r

service -l <*account*><*password*>

service -i <*new_owner*><*new_owner_email*>

service -t <*yes*>/<*no*>

service -c

Syntax Description

Parameter	Description
-s	Display the service status.
-r	Refresh the service status
-l <account><password>	Login to MyVigor server. Enter the account and password registered to MyVigor server account - Enter the name of the account. Password - Enter the password of the account.
-i <new_owner> <new_owner_email>	Enter the name and the e-mail address of the new owner for service transfer. New_owner - Enter the account name of the new owner. New_owner_email - Enter the e-mail address of the new owner.
-t <yes>/<no>	Transfer this Vigor device to a new owner.
-c	Clear current owner's account information.

Example

```
> service -l carrieni ttt0016ttt5
Login Account:carrieni, Pw:ttt0016ttt5
Login Success! Please check Service Status again!
> service -s
Show service status.
Now state is [SS_STATE_REG_ACC_VALID]
Service Status:
Model Name   : VigorLTE 200
Serial Number: 2019053108580701
MAC Address  : 00:1D:AA:73:4A:78
Owner Account: carrieni
E-mail       : ca******i@draytek.com

Device service support status:
Service WCF, ID = [1]
   Service Provider [Cyren]
   Licese Start_date [2019-09-26]
   Licese Exp_date [2019-10-26]

Service APPE, ID=[4]
   Service Provider [Not Activated]
   Licese Start_date []
   Licese Exp_date []

Service DDNS, ID=[6]
   Service Provider [Not Activated]
   Licese Start_date []
   Licese Exp_date []
```