DrayTek

Vigor2135 Series

Gigabit Broadband Router

USER'S GUIDE

V1.0

Vigor2135 Series
Gigabit Broadband Router

User's Guide

Version: 1.0

Firmware Version: V4.2.1.2

(For future update, please visit DrayTek web site)

Date: December 16, 2020

Copyrights

© All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

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

Safety Instructions

- 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 http://www.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.

  http://www.DrayTek.com

Table of Contents

Part I Installation i

I-1 Introduction 1

I-1-1 Indicators and Connectors 2

I-1-1-1 Vigor2135 2

I-1-1-2 Vigor2135ac / Vigor2135Vac / Vigor2135FVac 3

I-2 Hardware Installation 6

I-2-1 Installing Vigor Router 6

I-2-2 Wall-Mounted Installation 7

I-3 Accessing Web Page 8

I-4 Changing Password 10

I-5 Dashboard 11

I-5-1 Virtual Panel 12

I-5-2 Name with a Link 13

I-5-3 Quick Access for Common Used Menu 14

I-5-4 GUI Map 16

I-5-5 Web Console 17

I-5-6 Config Backup 18

I-5-7 Logout 18

I-5-8 Online Status 19

I-5-8-1 Physical Connection 19

I-5-8-2 Virtual WAN 21

I-6 Quick Start Wizard 23

I-6-1 Ethernet Connection on WAN1 24

I-6-3 USB Connection on WAN3 33

I-7 Service Activation Wizard 35

I-8 Registering Vigor Router 37

Part II Connectivity 39

II-1 WAN 40

Web User Interface 42

II-1-1 General Setup 42

II-1-1-1 WAN1 (Ethernet) 43

II-1-1-2 WAN3 (USB) 44

II-1-2 Internet Access 45

II-1-2-1 WAN1 Details Page (PPPoE, Physical Mode: Ethernet) 47

II-1-2-2 WAN2 Details Page (Static or Dynamic IP, Physical Mode: Ethernet) 50

II-1-2-3 WAN2 Details Page (PPTP/L2TP, Physical Mode: Ethernet) 54

II-1-2-4 WAN3 Details Page (PPP mode, Physical Mode: USB) 57

II-1-2-5 WAN3 Details Page (DHCP mode, Physical Mode: USB) 59

II-1-2-6 WAN1/WAN3 Details Page for IPv6 – Offline 62

II-1-2-7 WAN1 Details Page for IPv6 – PPP 62

II-1-2-8 WAN1/WAN3 Details Page for IPv6 – TSPC 63

II-1-2-9 WAN1/WAN3 Details Page for IPv6 – AICCU 65

II-1-2-10 WAN1 Details Page for IPv6 – DHCPv6 Client 66

II-1-2-11 WAN1 Details Page for IPv6 – Static IPv6 ..... *68*
II-1-2-12 WAN1 Details Page for IPv6 – 6in4 Static Tunnel *69*
II-1-2-13 WAN1 Details Page for IPv6 – 6rd in *72*
II-1-3 Multi- VLAN 74
II-1-4 WAN Budget 79
II-1-4-1 General Setup *79*
II-1-4-2 Status *82*
II-2 LAN 83
Web User Interface 85
II-2-1 General Setup 85
II-2-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup *87*
II-2-1-2 Details Page for LAN2 ~ LAN4 ..... *89*
II-2-1-3 Details Page for IP Routed Subnet *91*
II-2-1-4 Details Page for LAN IPv6 Setup *93*
II-2-1-5 DHCP Server Options *96*
II-2-2 VLAN 98
II-2-3 Bind IP to MAC 102
II-2-4 LAN Port Mirror 105
II-2-5 Wired 802.1x 106
II-3 NAT 107
Web User Interface 108
II-3-1 Port Redirection 108
II-3-2 DMZ Host 112
II-3-3 Open Ports 115
II-3-4 Port Triggering 117
II-3-5 ALG 120
II-4 Applications 121
Web User Interface 123
II-4-1 Dynamic DNS 123
II-4-2 LAN DNS / DNS Forwarding 129
II-4-3 DNS Security 133
II-4-3-1 General Setup *133*
II-4-3-2 Domain Diagnose *134*
II-4-4 Schedule 135
II-4-5 RADIUS 138
II-4-6 UPnP 140
II-4-7 IGMP 141
II-4-7-1 General Setting *141*
II-4-7-2 Working Group *142*
II-4-8 Wake on LAN 143
II-4-9 SMS / Mail Alert Service 144
II-4-9-1 SMS Alert *144*
II-4-9-2 Mail Alert *145*
II-4-10 Bonjour 146
Application Notes 149

A-1 How to use DrayDDNS? *149*
A-2 How to Configure Customized DDNS? *154*
II-5 Routing 158
Web User Interface 159
II-5-1 Static Route 159
II-5-2 Route Policy 165
Application Notes 174
A-1 How to set up Address Mapping with Route Policy? *174*
A-2 How to use destination domain name in a route policy? *176*
A-3 Introduction to Route Policy *178*

Part III Wireless LAN 181

III-1 Wireless LAN (2.4GHz/5GHz) 182
Web User Interface 185
III-1-1 Wireless Wizard 185
III-1-2 General Setup 189
III-1-3 Security 191
III-1-4 Access Control 193
III-1-5 WPS 195
III-1-6 WDS (for 5GHz) 198
III-1-7 Advanced Setting 200
III-1-8 Station Control 204
III-1-9 Bandwidth Management 205
III-1-10 AP Discovery 206
III-1-11 Airtime Fairness 207
III-1-12 Band Steering (2.4 GHz) 209
III-1-13 Roaming 214
III-1-14 Station List 215

Part IV VPN 217

IV-1 VPN and Remote Access 218
Web User Interface 219
IV-1-1 VPN Client Wizard 219
IV-1-2 VPN Server Wizard 225
IV-1-3 Remote Access Control 234
IV-1-4 PPP General Setup 235
IV-1-5 SSL General Setup 237
IV-1-6 IPsec General Setup 238
IV-1-7 IPsec Peer Identity 240
IV-1-8 OpenVPN 242
IV-1-8-1 OpenVPN Server Setup *242*
IV-1-8-2 Client Config *245*
IV-1-8-3 Import Certificate *246*

IV-1-9 Remote Dial-in User 247
IV-1-10 LAN to LAN 251
IV-1-11 Connection Management 259
IV-2 Certificate Management 260
Web User Interface 261
IV-2-1 Local Certificate 261
IV-2-2 Trusted CA Certificate 266
IV-2-3 Certificate Backup 269
IV-2-4 Self-Signed Certificate 270

Part V Security 271

V-1 Firewall 272
Web User Interface 274
V-1-1 General Setup 274
V-1-2 Filter Setup 279
V-1-3 Defense Setup 289
V-1-3-1 DoS Defense 289
V-1-3-2 Spoofing Defense 292
V-1-4 Diagnose 293
Application Notes 296
A-1 How to Configure Certain Computers Accessing to Internet 296
V-2 Central Security Management (CSM) 299
Web User Interface 300
V-2-1 APP Enforcement Profile 300
V-2-2 APPE Signature Upgrade 302
V-2-3 URL Content Filter Profile 304
V-2-4 Web Content Filter Profile 308
V-2-5 DNS Filter Profile 311
Application Notes 313
A-1 How to Create an Account for MyVigor 313
A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter 318

Part VI Management 323

VI-1 System Maintenance 324
Web User Interface 325
VI-1-1 System Status 325
VI-1-2 TR-069 327
VI-1-2-1 ACS and CPE Settings 327
VI-1-2-2 Reporting Configuration 329
VI-1-2-3 Export Parameters 330
VI-1-3 Administrator Password 331
VI-1-4 User Password 334
VI-1-5 Login Page Greeting 337

VI-1-6 Configuration Backup 339
VI-1-7 Syslog/Mail Alert 342
VI-1-8 Time and Date 345
VI-1-9 SNMP 346
VI-1-10 Management 348
VI-1-11 Panel Control 353
VI-1-12 Self-Signed Certificate 357
VI-1-13 Reboot System 359
VI-1-14 Firmware Upgrade 360
VI-1-15 Firmware Backup 361
VI-1-16 Dashboard Control 362
VI-2 Bandwidth Management 363
Web User Interface 364
VI-2-1 Sessions Limit 364
VI-2-2 Bandwidth Limit 366
VI-2-3 Quality of Service 368
VI-2-4 APP QoS 374
VI-3 User Management 375
Web User Interface 376
VI-3-1 General Setup 376
VI-3-2 User Profile 378
VI-3-3 User Group 382
VI-3-4 User Online Status 383
Application Notes 385
A-1 How to authenticate clients via User Management 385
A-2 How to use Landing Page Feature 394
VI-4 Hotspot Web Portal 398
Web User Interface 398
VI-4-1 Profile Setup 398
VI-4-1-1 Login Method 399
VI-4-1-2 Steps for Configuring a Web Portal Profile 399
VI-4-2 Quota Management 415
Application Notes 418
A-1 How to create Facebook APP for Web Portal Authentication? 418
A-2 How to create Google APP for Web Portal Authentication? 424
VI-5 Central Management (AP) 426
Web User Interface 427
VI-6-1 Status 427
VI-6-2 WLAN Profile 429
VI-6-3 AP Maintenance 434
VI-6-4 Traffic Graph 435
VI-6-5 Load Balance 436

VI-7 Central Management (External Devices) 438

Part VII Others 439

VII-1 Objects Settings 440
Web User Interface 441
VII-1-1 IP Object 441
VII-1-2 IP Group 444
VII-1-3 IPv6 Object 446
VII-1-4 IPv6 Group 448
VII-1-5 Service Type Object 450
VII-1-6 Service Type Group 452
VII-1-7 Keyword Object 454
VII-1-8 Keyword Group 456
VII-1-9 File Extension Object 457
VII-1-10 SMS/Mail Service Object 459
VII-1-11 Notification Object 465
VII-1-12 String Object 466
VII-1-13 Country Object 468
VII-1-14 Objects Backup/Restore 470
Application Notes 471
A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection 471
VII-2 USB Application 475
Web User Interface 476
VII-2-1 USB General Settings 476
VII-2-2 USB User Management 477
VII-2-3 File Explorer 479
VII-2-4 USB Device Status 480
VII-2-5 Temperature Sensor 481
VII-2-6 Modem Support List 483
VII-2-7 SMB Client Support List 484
Application Notes 485
A-1 How can I get the files from USB storage device connecting to Vigor router? ... 485

Part VIII Troubleshooting 489

VIII-1 Diagnostics 490
Web User Interface 491
VIII-1-1 Dial-out Triggering 491
VIII-1-2 Routing Table 492
VIII-1-3 ARP Cache Table 493
VIII-1-4 IPv6 Neighbour Table 494
VIII-1-5 DHCP Table 495

VIII-1-6 NAT Sessions Table 496
VIII-1-7 DNS Cache Table 497
VIII-1-8 Ping Diagnosis 498
VIII-1-9 Data Flow Monitor 499
VIII-1-10 Traffic Graph 501
VIII-1-11 Trace Route 502
VIII-1-12 Syslog Explorer 503
VIII-1-13 IPv6 TSPC Status 504
VIII-1-14 DoS Flood Table 505
VIII-1-15 Route Policy Diagnosis 506
VIII-2 Checking If the Hardware Status Is OK or Not 508
VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not 509
VIII-4 Pinging the Router from Your Computer 512
VIII-5 Checking If the ISP Settings are OK or Not 514
VIII-6 Problems for 3G/4G Network Connection 515
VIII-7 Backing to Factory Default Setting If Necessary 516
VIII-8 Contacting DrayTek 517

Part IX Telnet Commands 519

Accessing Telnet of Vigor2135 520

Index 782

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.

Vigor2135 Series integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

The entertainment applications running over the home network infrastructure and home-based productivity for SOHO are growing while the broadband bandwidth is increasingly available within affordable budget along with deployment of FTTx. The fiber WAN port of Vigor2135FVn optimizes the throughput performance and flexibility for time-critical console gaming, multi-media streaming and P2P downloading as well as IP telephony. The four Gigabit Ethernet (10/100/1000 LAN ports) auto-sensing ports facilitate home networking with width-intensive applications! Through the combination of Fiber WAN and Gigabit LAN ports to optimize the bandwidth usage, the downstream data and voice packets for Triple play can be flawlessly displayed in endpoint devices, such as HDTV, desktop/laptop or analog/IP phone.

The Vigor2135FVn/Vac/ac series router gives you not only the 802.11n/ac standards for coverage, but also the time scheduling function to save your energy bill plus reducing the carbon footprint. For wireless security, it is also efficient for wireless network management. For instance, its "Wireless LAN isolation" can easily isolate wireless network for friends or guests. Then, the access rights of various wireless clients can be managed by "MAC address control" and deployed "WEP/WPA/WPA2" authentication. No need to remember passwords, you simply press "WPS" button on router and then enable users to securely connect laptop or computers to the router!

The fiber deployment (for Vigor2135FVn) lets businesses and common people have fatter pipe of accessing global network. DrayTek Vigor2135FVn Fiber Router is developed in compliance with the Super-fast broadband architecture and customized for users which already have Fiber to the building (FTTB) or Fiber to the home (FTTH). The bandwidth-consumed multimedia streaming and crystal-clear VoIP functionalities are realized through the Vigor2135FVn's upto-1000Mpbs (1 Gigabit) WAN throughput and advanced bandwidth management. You can apply the rules of Session Limit, Bandwidth Limit, Port Rate Control, QoS control list, Ports Priority to different traffic type for better efficiency.

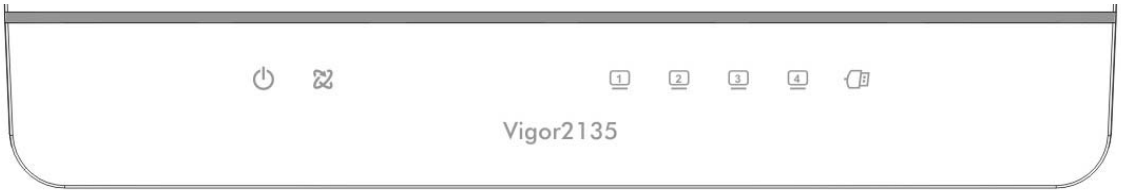
By making the most of your broadband line, the VoIP call will be carried to the destination via Internet. So you can save on the telephone bill. Combining the Internet Telephony service from the Internet Telephony Service Provider (ITSP), the Vigor2135FVn charter VoIP calls to be made to any legacy phone numbers, even including mobile and long distance numbers!

In addition, it supports the worldwide standard TR-069 management and customized triple play while most fiber routers could not have the above distinguished features.

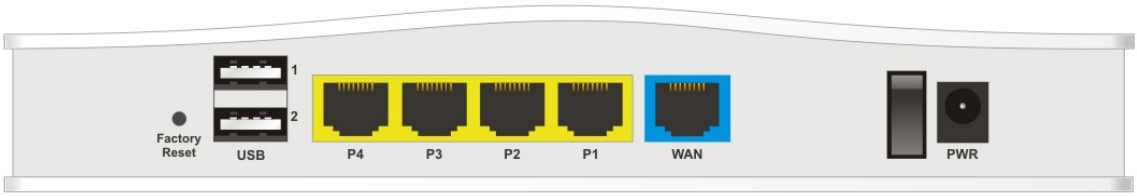
I-1-1 Indicators and Connectors

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

I-1-1-1 Vigor2135



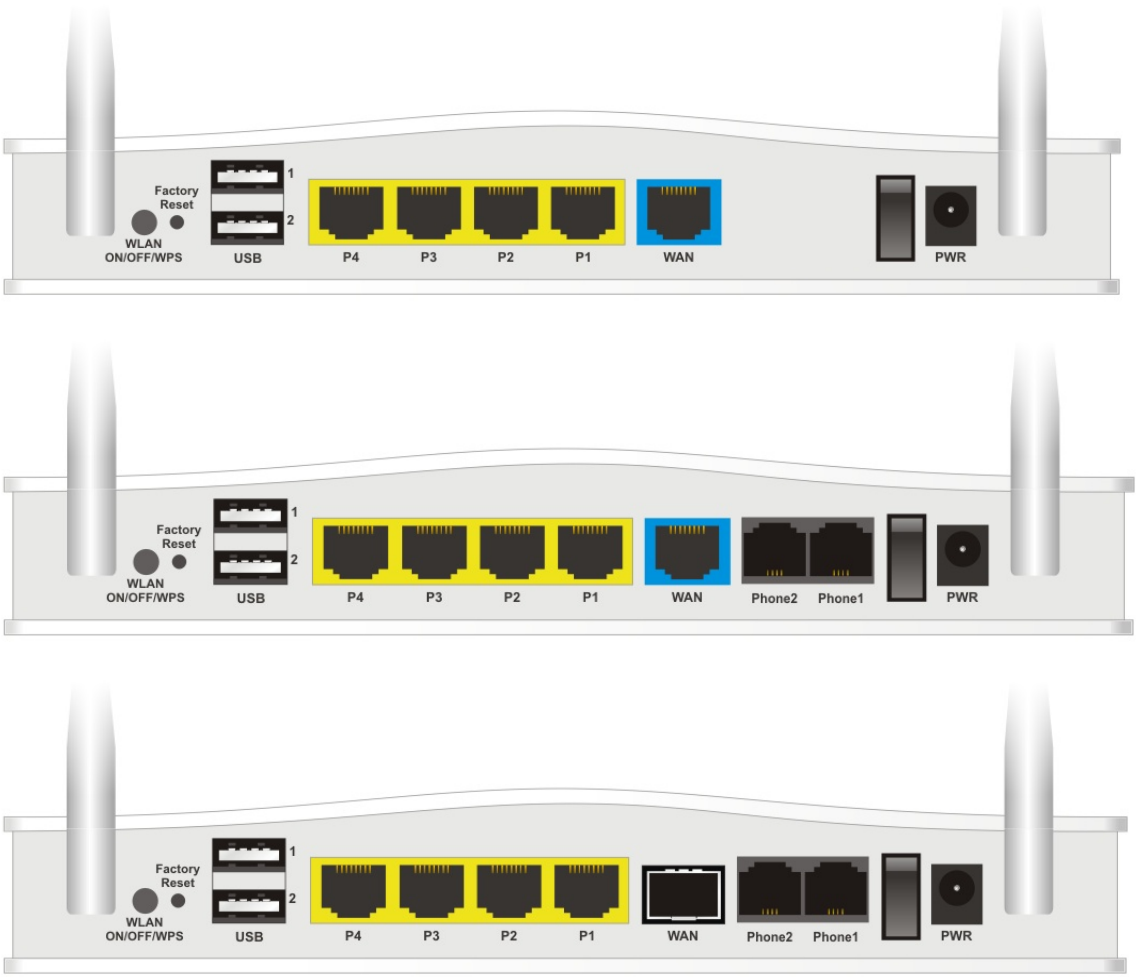
LED	Status	Explanation
(Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
WAN	On	Internet connection is ready.
	Blinking	The data is transmitting.
	Off	Internet connection is not ready.
~ LAN1/2/3/4	On	The LAN port is connected.
	Blinking	The data is transmitting.
	Off	The LAN port is disconnected.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.



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.
USB1~USB2	Connector for a USB device (for USB Modem or printer).
P4~P1	Connectors for local networked devices.
WAN	Connector for remote networked devices (by Ethernet cable).
ON/OFF	Power switch.
PWR	Connector for a power adapter.

I-1-1-2 Vigor2135ac / Vigor2135Vac / Vigor2135FVac

LED	Status	Explanation
(Activity)	Blinking	The router is powered on and running normally.
	Blinking (quickly)	When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection.
	Off	The router is powered off.
WAN	On	Internet connection is ready.
	Blinking	The data is transmitting.
	Off	Internet connection is not ready.
1, 2 (for "V" model)	Off	Internet connection is not ready.
	On	The phone connected to this port is off-hook.
	Off	The phone connected to this port is on-hook.
2.4 ~ 5 WLAN	Blinking	A phone call comes.
	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Blinking (quickly)	When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection.
	Off	The WLAN function is inactive.
1 ~ 4 LAN1/2/3/4	On	The LAN port is connected.
	Blinking	The data is transmitting.
	Off	The LAN port is disconnected.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.



Interface	Description
Wireless LAN ON/OFF/WPS	WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on. WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off. WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS.
Factory Reset	Restore the default settings. Usage: Turn on the router (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.
USB1~USB2	Connector for a USB device (for 3G/4G USB Modem or printer).
P4~P1	Connectors for local networked devices.
WAN	Connector for remote networked devices (by Ethernet cable).
WAN (FVac)	Connector for fiber connection for accessing the Internet.

Phone2/Phone1 (for “V” model)	Connector of analog phone for VoIP communication.
ON/OFF	Power switch.
PWR	Connector for a power adapter.

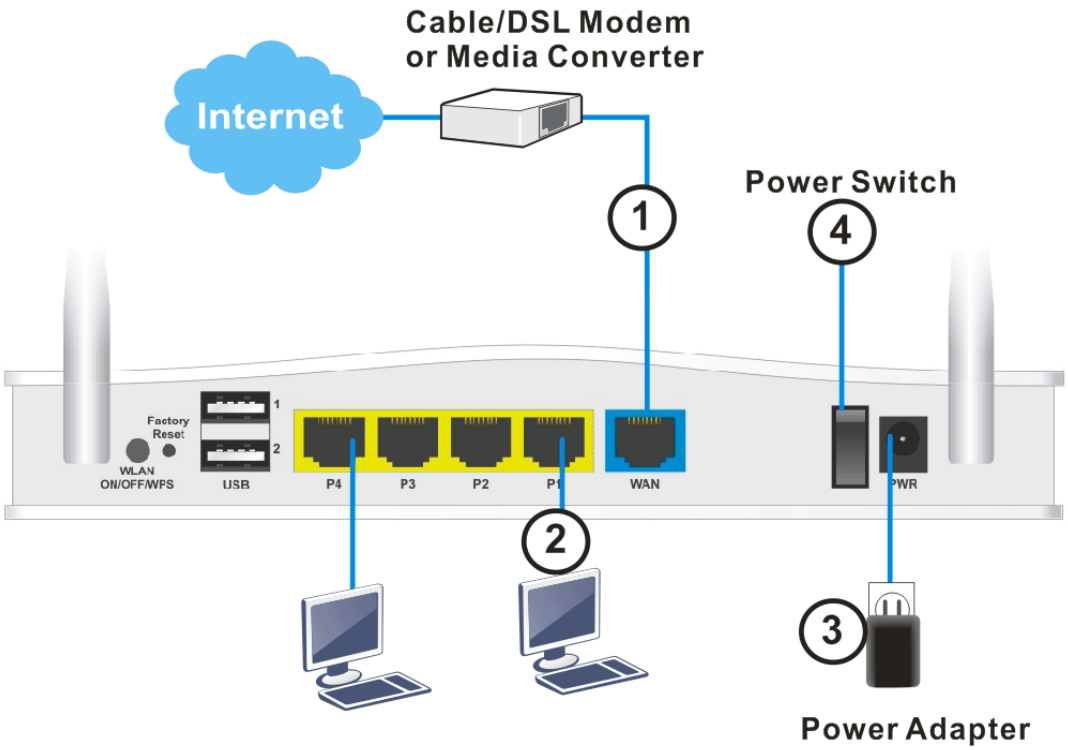
I-2 Hardware Installation

I-2-1 Installing Vigor Router

Before starting to configure the router, you have to connect your devices correctly. Here we take Vigor2135ac as an example.

1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect detachable antennas to the router.
4. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
5. Power on the router.
6. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connection.

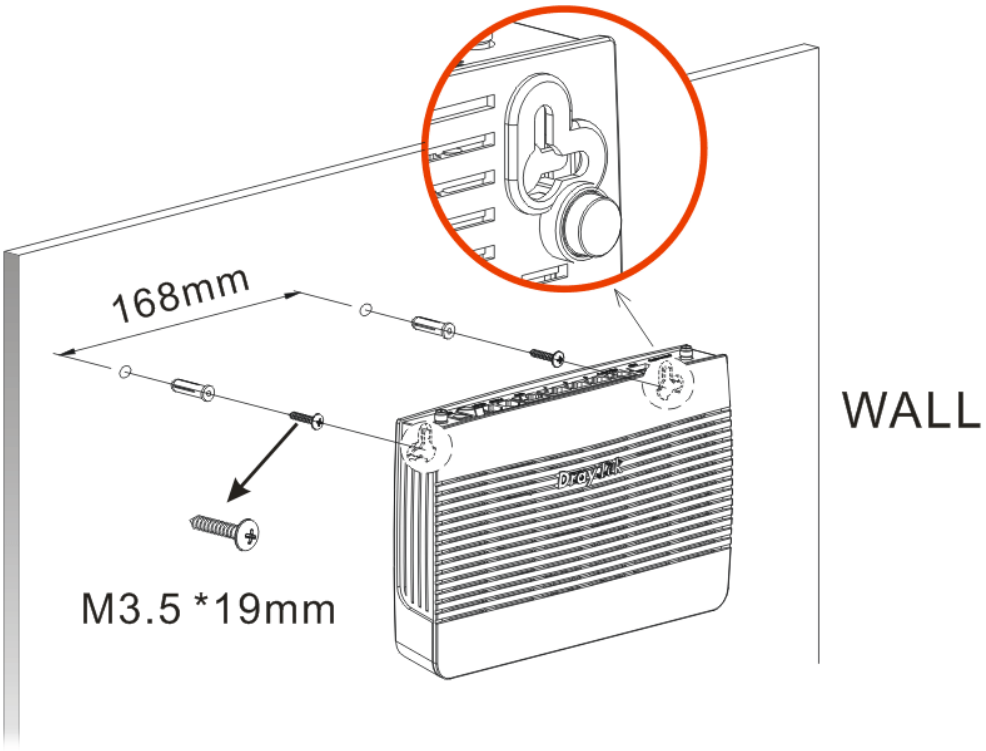
   (For the hardware connection, we take *"ac"* model as an example.)



I-2-2 Wall-Mounted Installation

Vigor router has keyhole type mounting slots on the underside.

1. A template is provided on the Vigor router 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.



Info	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.

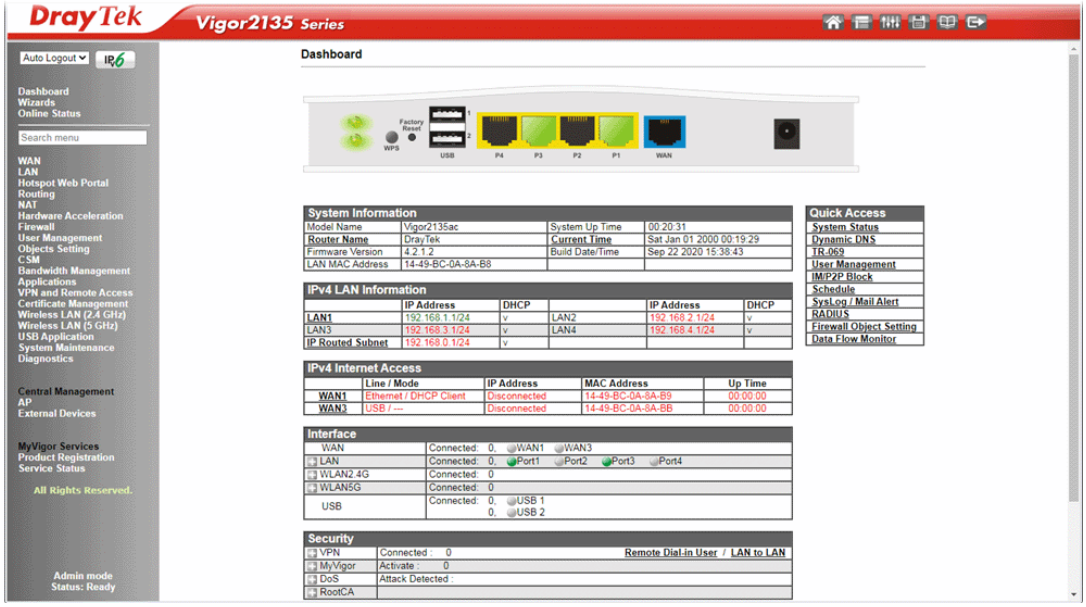
   You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

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**.

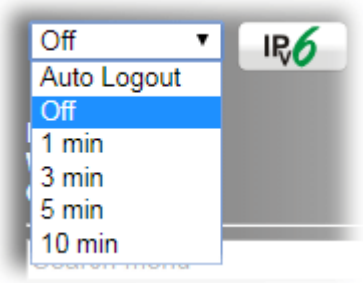
Info	If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

4. Now, the **Main Screen** will appear. Take Vigor2135ac as an example.



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

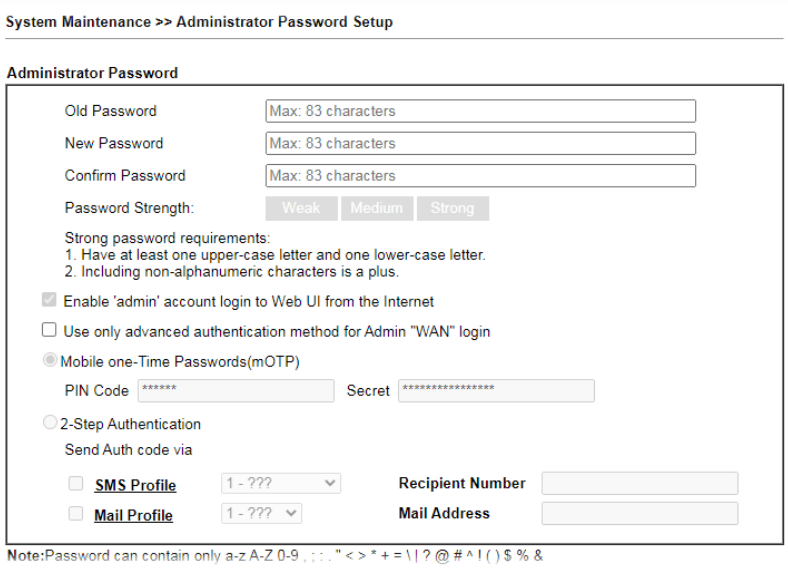
5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



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.

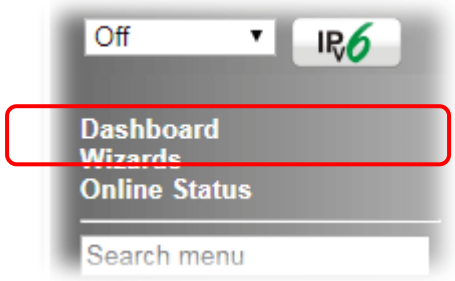
Info	The maximum length of the password you can set is 23 characters.

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".

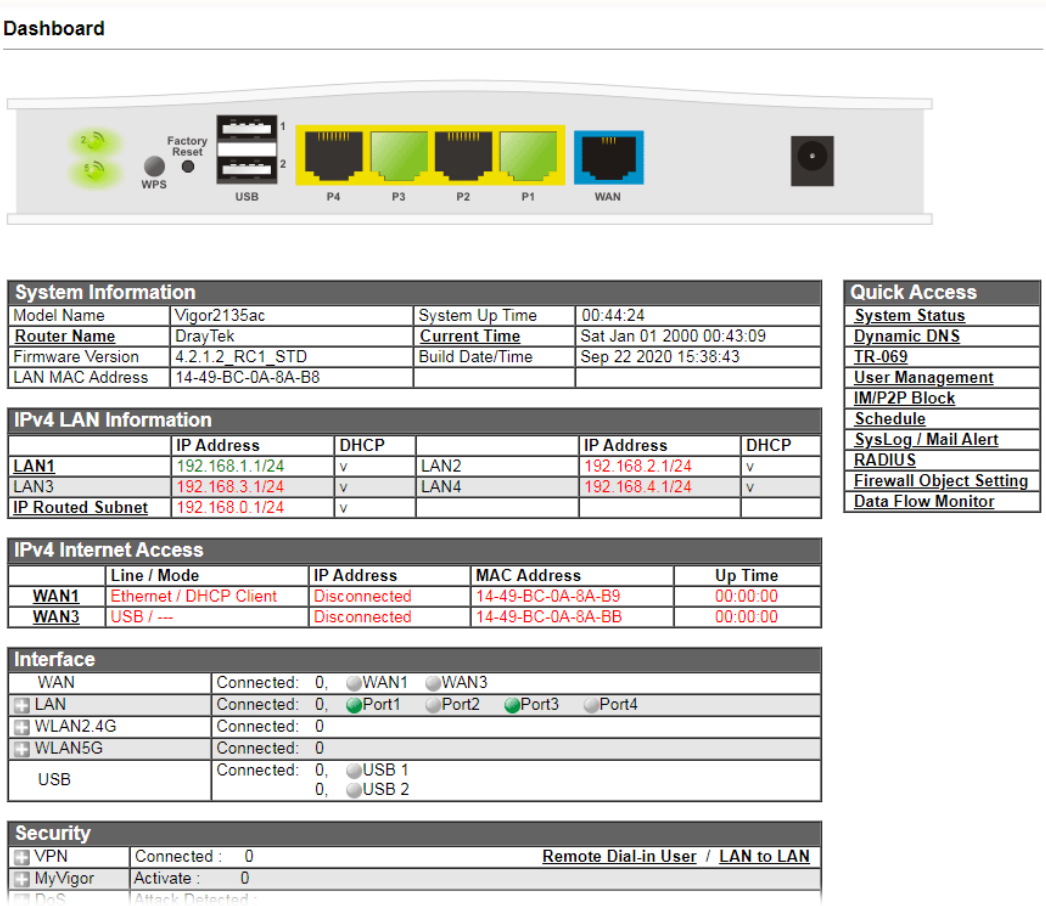
I-5 Dashboard

The Dashboard provides a convenient way to monitor the current status of the router, including firmware version, system resource usage, LAN and WAN connection uptimes, and interface usage. It is refreshed every 5 seconds with the latest information.



For the Dashboard is the landing page after logging into the web configuration utility, you can also bring up the Dashboard by clicking on the Dashboard on the menu bar.

The Dashboards of other Vigor2135 models are may vary slightly due to differences in features. The figure below shows the Dashboard of the Vigor2135ac.



The System Information section displays general information about the router, such as system uptime, system time, and firmware version.

The IPv4 Internet Access section shows the IPv4 connection status of the WAN ports, including their access modes, IP addresses, MAC addresses and uptimes.

The IPv6 Internet Access section shows the IPv6 connection status of the WAN port that has IPv6 enabled. Unlike IPv4, IPv6 support is limited to one WAN port at a time, so there is always at most one IPv6 WAN connection shown.

The Interface section shows the physical connection status of the WAN, Ethernet, Wi-Fi and USB interfaces.

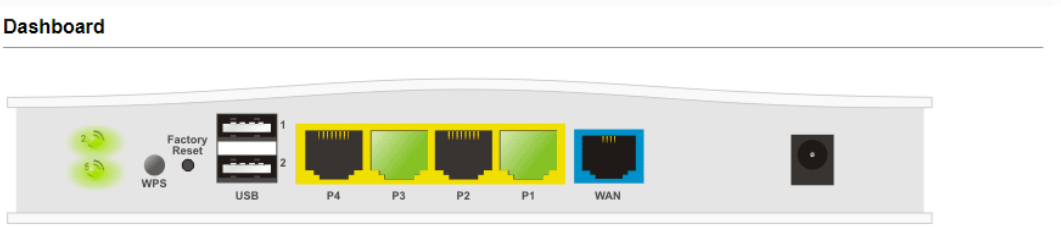
The Security section shows the states of the security-related features, including VPN, Web Content Filter and App Enforcement.

The System Resource section shows the current CPU and memory usage of the router.

I-5-1 Virtual Panel

At the top of the Dashboard page is the Virtual Panel, a graphical simulation of the front panel of the router.

The WAN and LAN connectors are shaded with various colours to indicate their status at any given point in time.

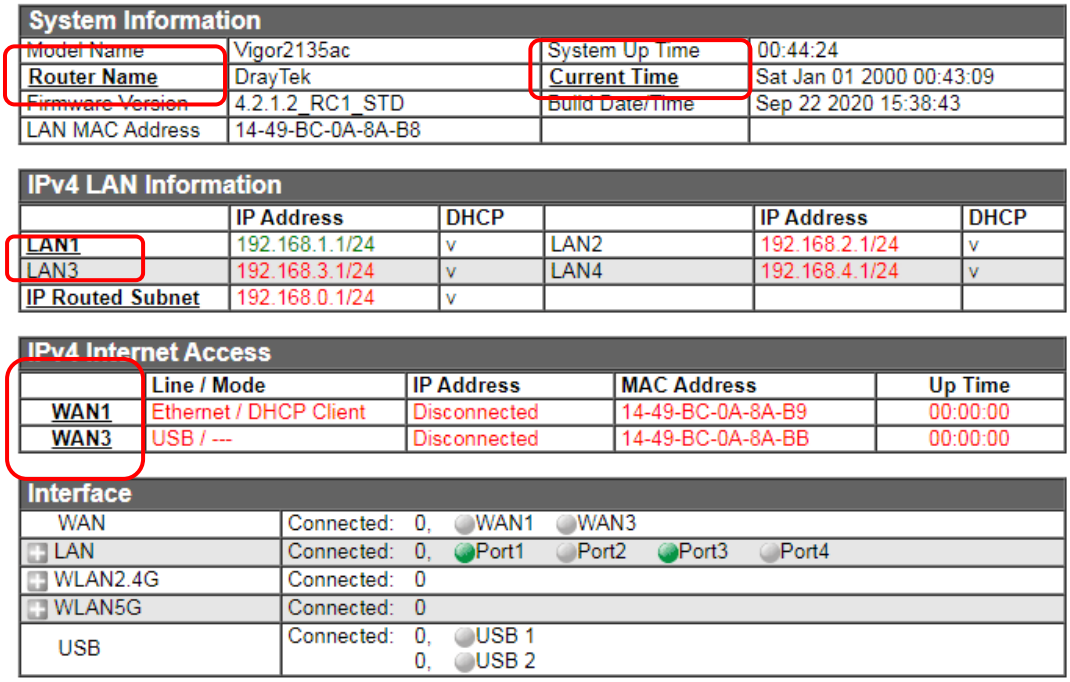


Port	Color	Description
USB	Black	No USB device is connected.
	Green	A USB device is connected.
LAN P4 ~ P1	Black	LAN port is disconnected.
	Green	LAN port is connected at 1 Gbps.
	Orange	LAN port is connected at 10/100 Mbps.
WAN	Black	WAN2 port is disconnected.
	Green	WAN2 port is connected at 1 Gbps.
	Orange	WAN2 port is connected at 10/100 Mbps.

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, WAN# and etc.) below means you can click it to open the configuration page for modification.



System Information

Model Name	Vigor2135ac	System Up Time	00:44:24
Router Name	DrayTek	**Current Time**	Sat Jan 01 2000 00:43:09
Firmware Version	4.2.1.2_RC1_STD	Build Date/Time	Sep 22 2020 15:38:43
LAN MAC Address	14-49-BC-0A-8A-B8		

IPv4 LAN Information

	IP Address	DHCP		IP Address	DHCP
LAN1	192.168.1.1/24	v	LAN2	192.168.2.1/24	v
LAN3	192.168.3.1/24	v	LAN4	192.168.4.1/24	v
IP Routed Subnet	192.168.0.1/24	v			

IPv4 Internet Access

	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Ethernet / DHCP Client	Disconnected	14-49-BC-0A-8A-B9	00:00:00
WAN3	USB / ---	Disconnected	14-49-BC-0A-8A-BB	00:00:00

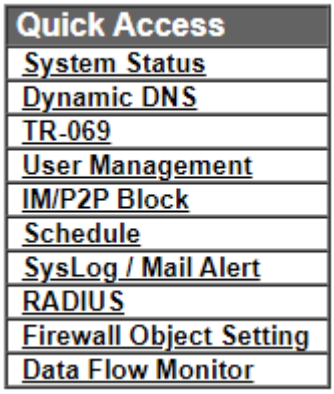
Interface

WAN	Connected: 0, WAN1 WAN3
LAN	Connected: 0, Port1 Port2 Port3 Port4
WLAN2.4G	Connected: 0
WLAN5G	Connected: 0
USB	Connected: 0, USB 1 0, USB 2

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. For your convenience, some of the most-frequently-used items in the Web Configuration Utility are listed under the Quick Access section on the Dashboard.

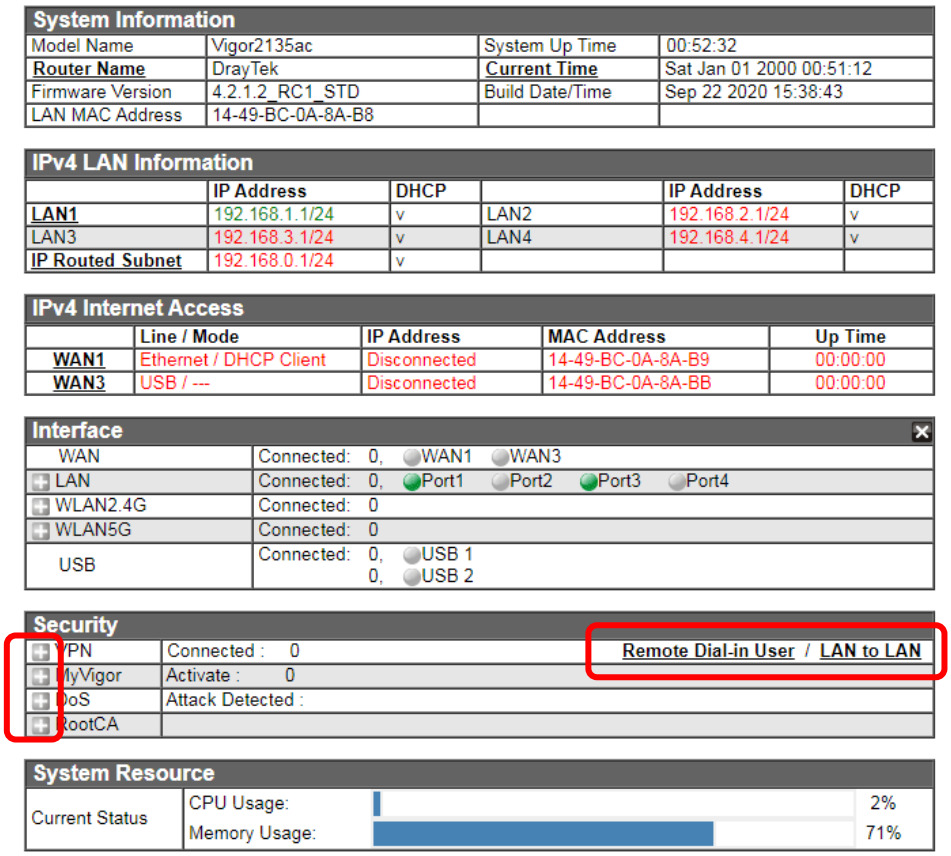
Look at the right side of the Dashboard. You will find a group of common used functions grouped under **Quick Access**.



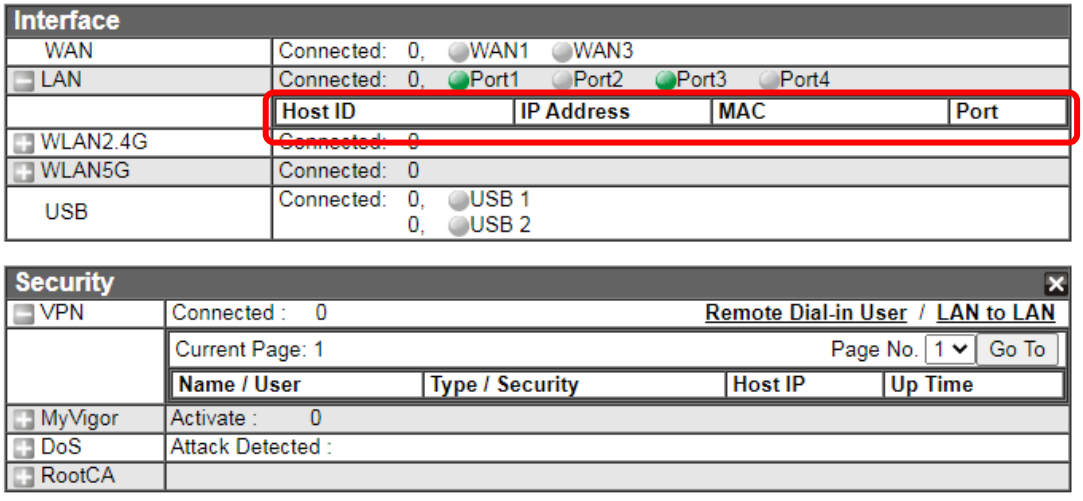
Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be open immediately.

Hyperlink	Destination
System Status	System Maintenance >> System Status
Dynamic DNS	Applications >> Dynamic DNS Setup
TR-069	System Maintenance >> TR-069 Setting
User Management	User Management >> User Profile
IM/P2P Block	CSM >> APP Enforcement Profile
Schedule	Applications >> Schedule
SysLog / Mail Alert	System Maintenance >> SysLog / Mail Alert Setup
LDAP	Applications >> Active Directory /LDAP
RADIUS	Applications >> RADIUS/TACACS+
Firewall Object Setting	Objects Setting >> IP Object
Data Flow Monitor	Diagnostics >> Data Flow Monitor

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 appearing on Interface/Security. Click it to review the 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.

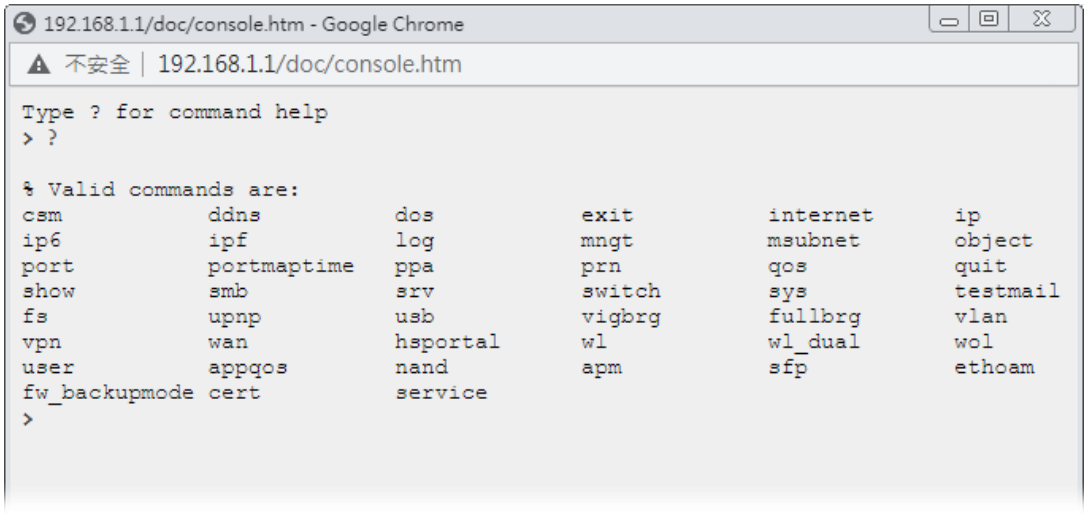
GUI Map

Dashboard		**VPN and Remote Access**	
Wizards			Remote Access Control
	Quick Start Wizard		PPP General Setup
	Service Activation Wizard		SSL General Setup
	VPN Client Wizard		IPsec General Setup
	VPN Server Wizard		IPsec Peer Identity
	Wireless Wizard		OpenVPN
Online Status			Remote Dial-in User
	Physical Connection		LAN to LAN
	Virtual WAN		Connection Management
WAN		**Certificate Management**	
	General Setup		Local Certificate
	Internet Access		Trusted CA Certificate
	Multi-VLAN		Certificate Backup
	WAN Budget		Self-Signed Certificate
LAN		**Wireless LAN (2.4 GHz)**	
	General Setup		General Setup
	VLAN		Security
	Bind IP to MAC		Access Control
	LAN Port Mirror		WPS
	Wired 802.1X		Advanced Setting
Hotspot Web Portal			Station Control
	Profile Setup		AP Discovery
	Quota Management		Band Steering
Routing			Roaming
	Static Route		Station List

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**.

I-5-7 Logout

Click this icon to exit the web user interface.

I-5-8 Online Status

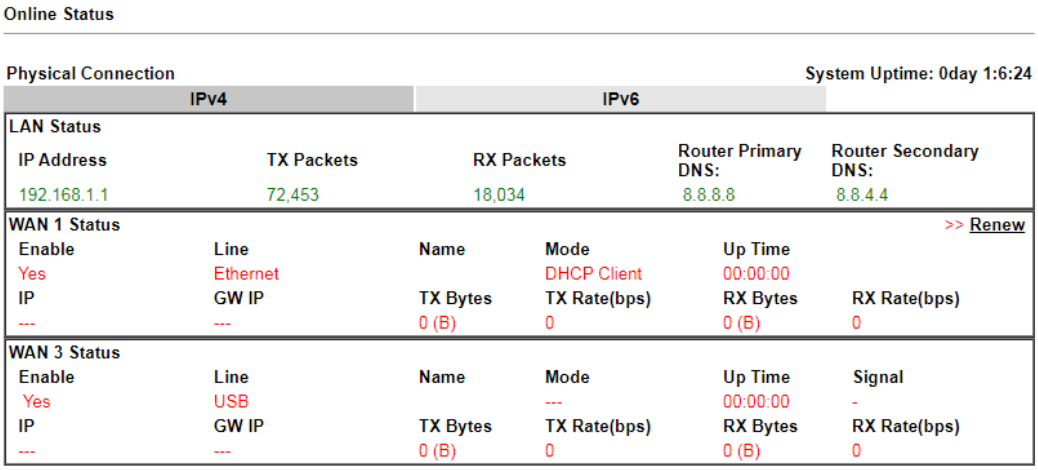
I-5-8-1 Physical Connection

The Physical Connection page displays the status of all the physical network interfaces, including LAN, WAN and DSL.

The information shown for every interface can be in green, indicating the interface is enabled and online; or red, indicating the interface is either disabled or offline.

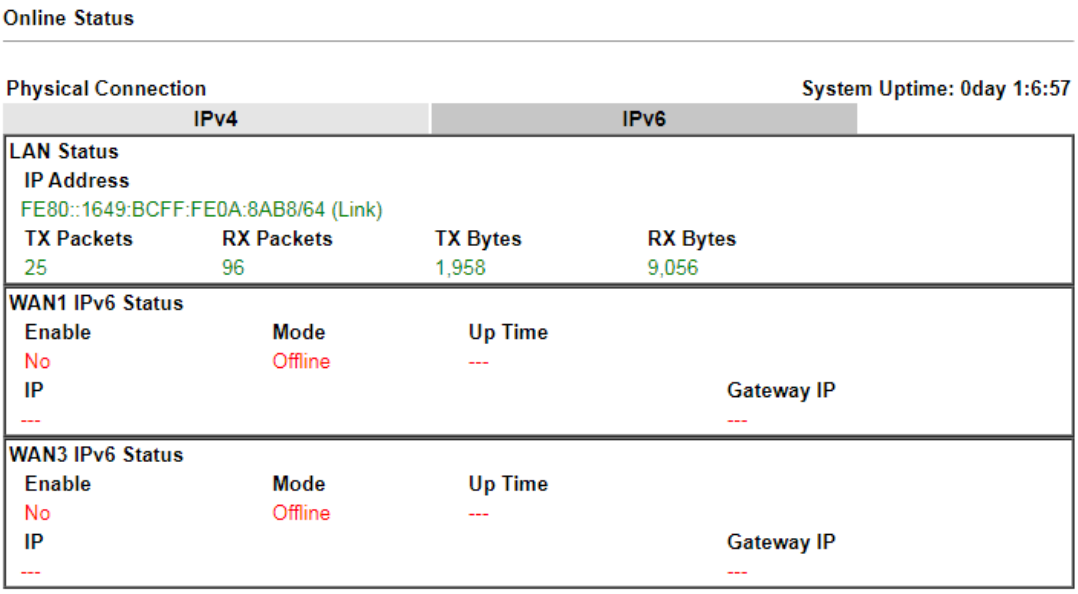
Physical Connection for IPv4 Protocol

This IPv4 tab displays IPv4 related information of all the LAN and WAN interfaces, plus the DSL connection status.



Physical Connection for IPv6 Protocol

This IPv6 tab displays IPv6 related information of all the LAN and WAN interfaces.



Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	**Primary DNS-**Displays the primary DNS server address for WAN interface. **Secondary DNS -**Displays the secondary DNS server address for WAN interface. **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.
WAN# Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. **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

Item	Description
LAN Status	**IP Address**- Displays the IPv6 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. **TX Bytes** - Displays the speed of transmitted octets at the LAN interface. **RX Bytes** - Displays the speed of received octets at the LAN interface.
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.

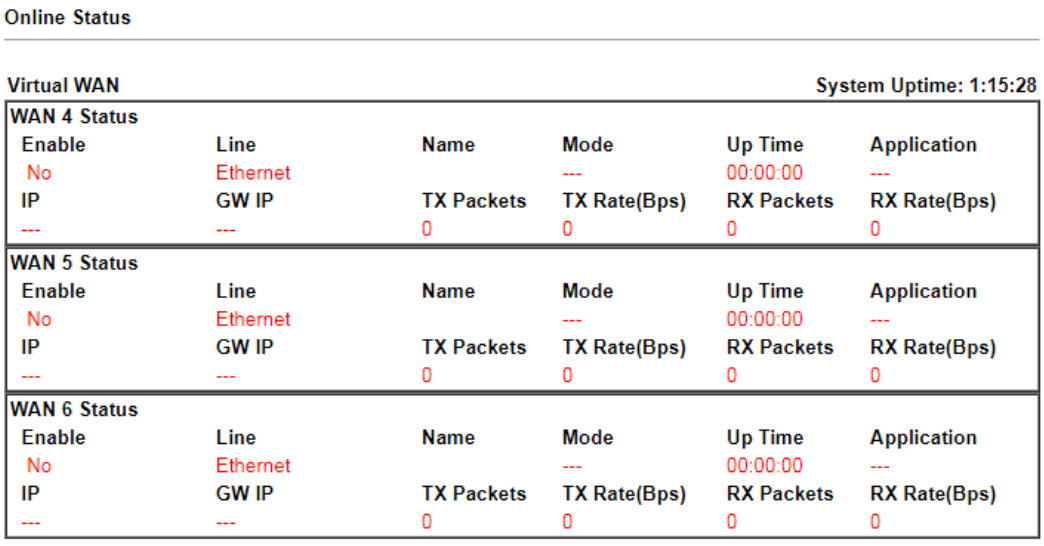
Info	The words in green mean that the WAN connection of that interface is ready for accessing Internet; the words in red mean that the WAN connection of that interface is not ready for accessing Internet.

I-5-8-2 Virtual WAN

The Virtual WAN screen displays the status of the 3 virtual WAN interfaces.

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

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



Detailed explanation is shown below:

Item	Description
Enable	Yes- Virtual WAN interface is enabled. No- Virtual WAN interface is disabled.

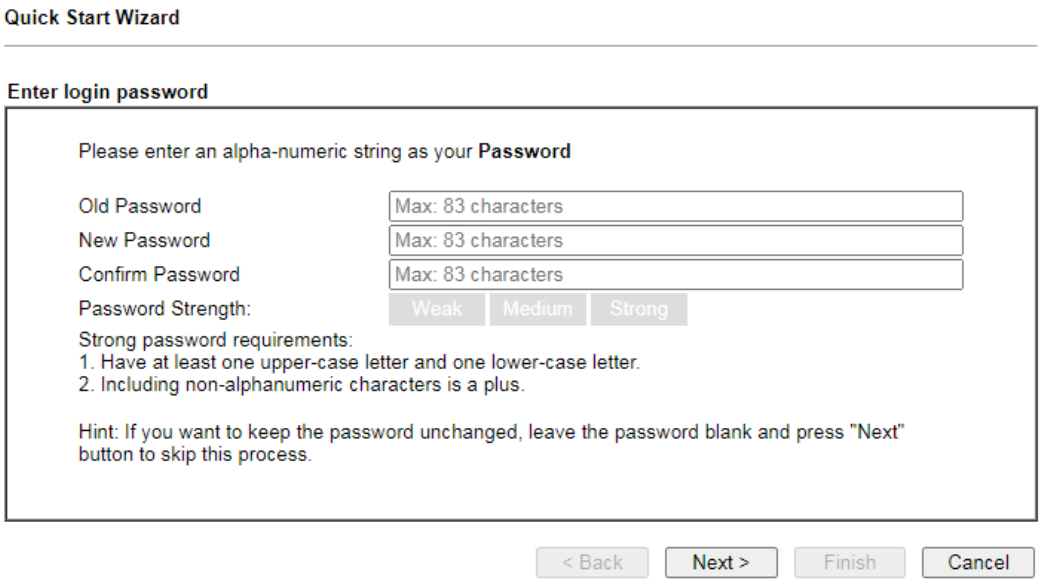
Item	Description
Line	Ethernet- The Ethernet port is used for this virtual WAN.
Name	The IPv6 addresses of the WAN interface. The global address is routable whereas the link local address is for LAN use only.
Mode	Gateway address of the IPv6 WAN connection.
Up Time	Yes: IPv6 support on the WAN interface is enabled. No: IPv6 support on the WAN interface is disabled.
Application	The IPv6 access mode, which can be one of Offline, PPP, TSPC, AICCU, DHCPv6 Client, Static IPv6, 6in4 Static Tunnel, and 6rd.
IP	The IPv6 addresses of the WAN interface. The global address is routable whereas the link local address is for LAN use only.
GW IP	Gateway address of the IPv6 WAN connection.
TX Packets	Total number of IPv6 packets leaving the WAN interface.
TX Rate(Bps)	The speed of transmitted octets.
RX Packets	Total number of IPv6 packets received by the WAN interface.
RX Rate(Bps)	The speed of received octets.

I-6 Quick Start Wizard

The **Quick Start Wizard** allows you to quickly and easily set the router up for Internet access.

Note that only one specific WAN interface can be configured each time the wizard is run. If you have additional WAN interfaces to configure, rerun the wizard and select the appropriate WAN interface. As an alternative, you may use the WAN menu item.

Go to **Wizards>>Quick Start Wizard**. The first screen of **Quick Start Wizard** is entering login password. After entering the password, please click **Next** to proceed.



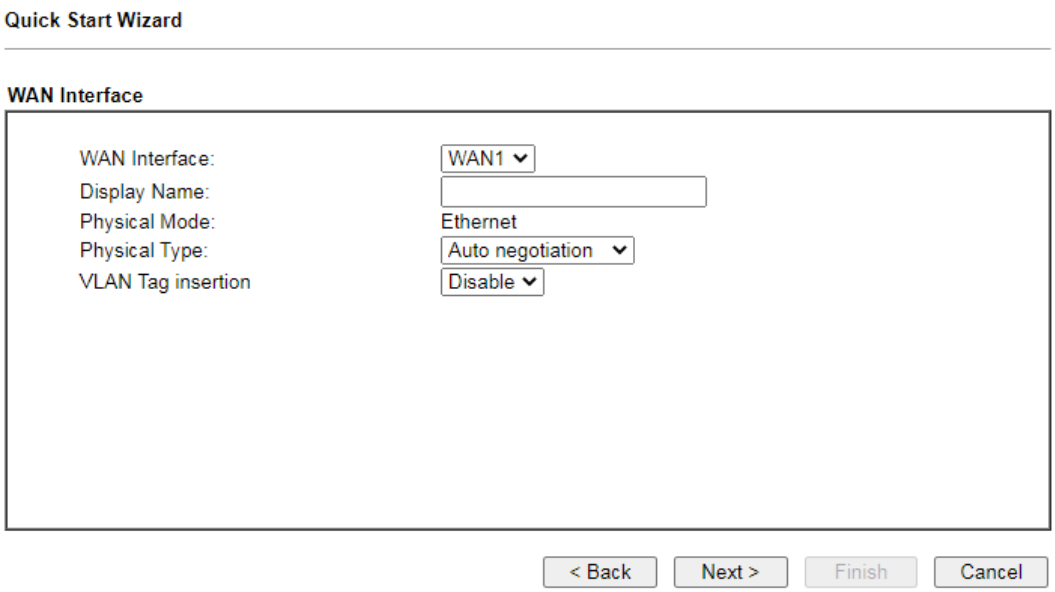
On the next screen, you can select a WAN interface to configure. The configuration steps that follow vary slightly depending on the type of Internet connection you have.

If Ethernet interface is used, please choose WAN1; if USB modem is used, please choose WAN3. Then click **Next** for next step.

Each WAN interface will bring up different configuration page. Refer to the following for detailed information.

I-6-1 Ethernet Connection on WAN1

WAN2 can be configured for physical mode of Ethernet.



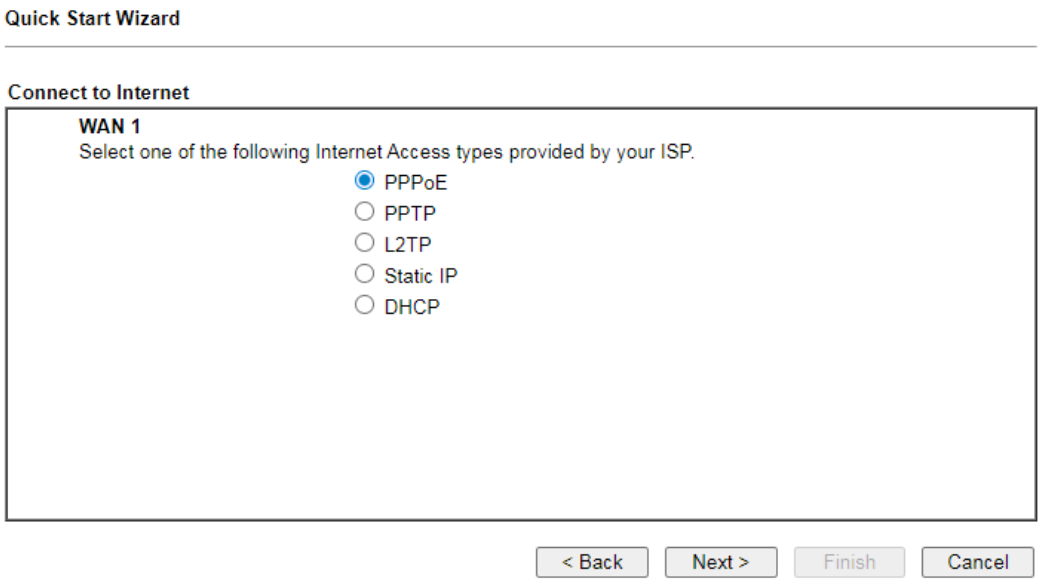
Available settings are explained as follows:

Item	Description
Display Name	Optional name that identifies the connection.
Physical Type	Ethernet link parameters. **Auto negotiation** – Speed and duplex mode are automatically configured by negotiating with the connected device. **10M half duplex** – 10 Mbit/s Ethernet half duplex. **10M full duplex** – 10 Mbit/s Ethernet full duplex. **100M half duplex** – 100 Mbit/s Fast Ethernet full duplex. **100M full duplex** – 100 Mbit/s Fast Ethernet half duplex. **1000M full duplex** – 1 Gbit/s Gigabit Ethernet full duplex.
VLAN Tag insertion	Enables or disables 802.1q VLAN tagging of WAN traffic. Some Internet connections require the use of VLAN tags. For more information, please contact your Internet Service Provider. **Enable** – Enables VLAN tagging of all frames leaving the WAN interface. ● **Tag value** – VLAN identifier, used to tag outbound WAN traffic. Valid tag values range from 0 to 4095. ● **Priority** – 802.1p Class of Service, used to assign the traffic priority. Valid priority values range from 0 (highest) to 7 (lowest). **Disable** – Disables VLAN tagging.

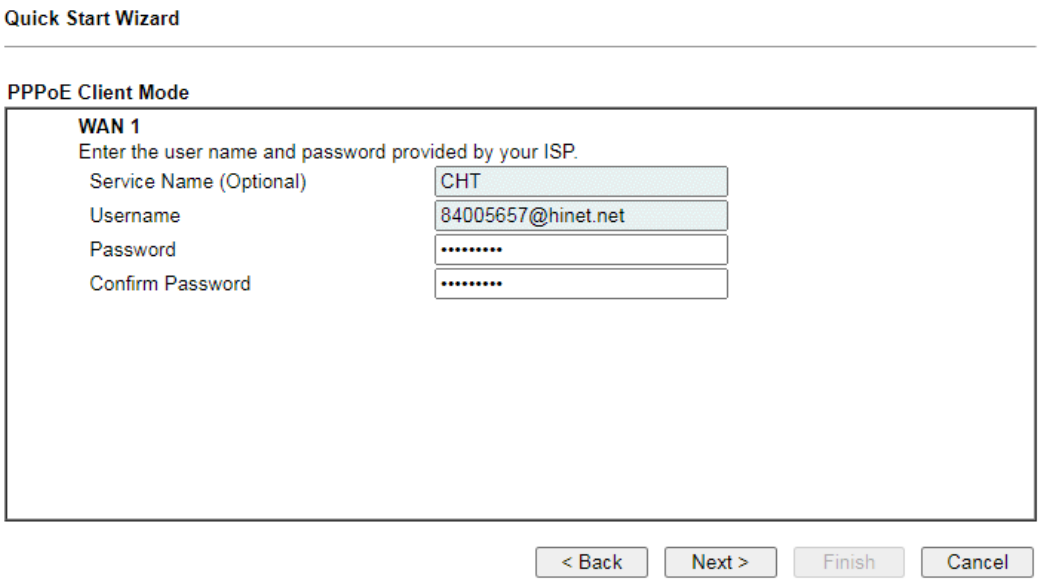
On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

Ethernet WAN1 - PPPoE

1. Choose **WAN1** 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 (Point-to-Point Protocol over Ethernet)** as the Internet Access Type. Then click **Next** to continue.

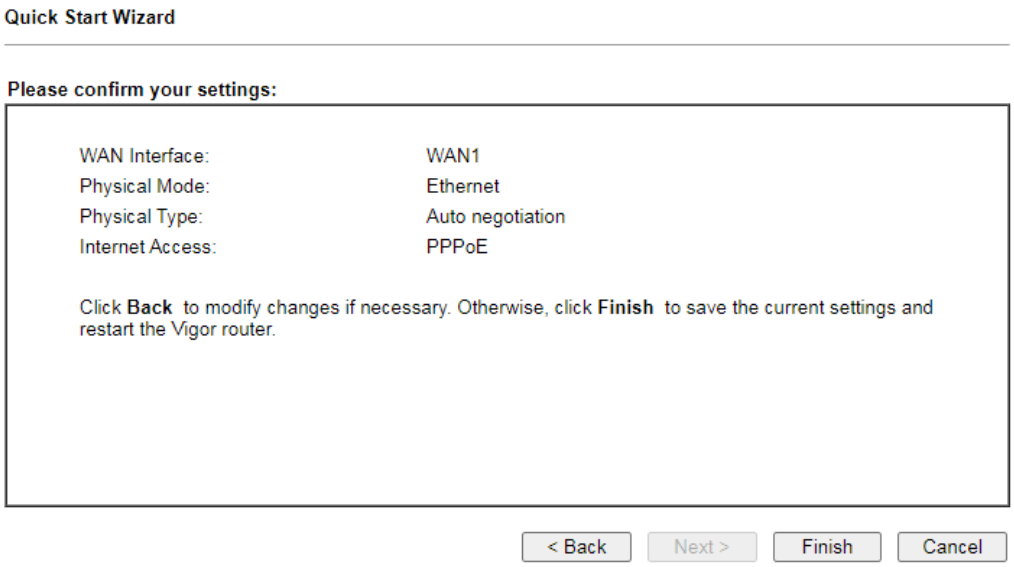


Available settings are explained as follows:

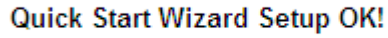
Item	Description
Service Name (Optional)	PPP service name tag. Required by some ISPs. Leave blank unless instructed otherwise by your ISP.
Username	Username provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 63 characters.
Password	Password provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters.
Confirm Password	Re-enter the password for confirmation.
Back	Click it to return to previous setting page.

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

3. Fill in the fields on the page using information provided by your ISP. Then click **Next** for viewing the summary of all the settings you have entered.



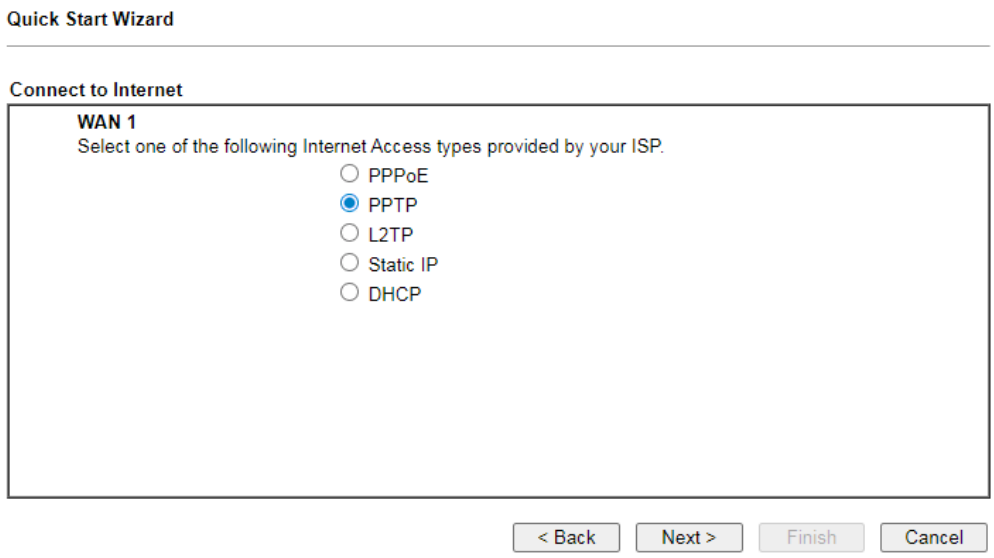
4. If you are satisfied with what you see, click **Finish** to save your changes. The following message appears indicating that the changes have been successfully saved.



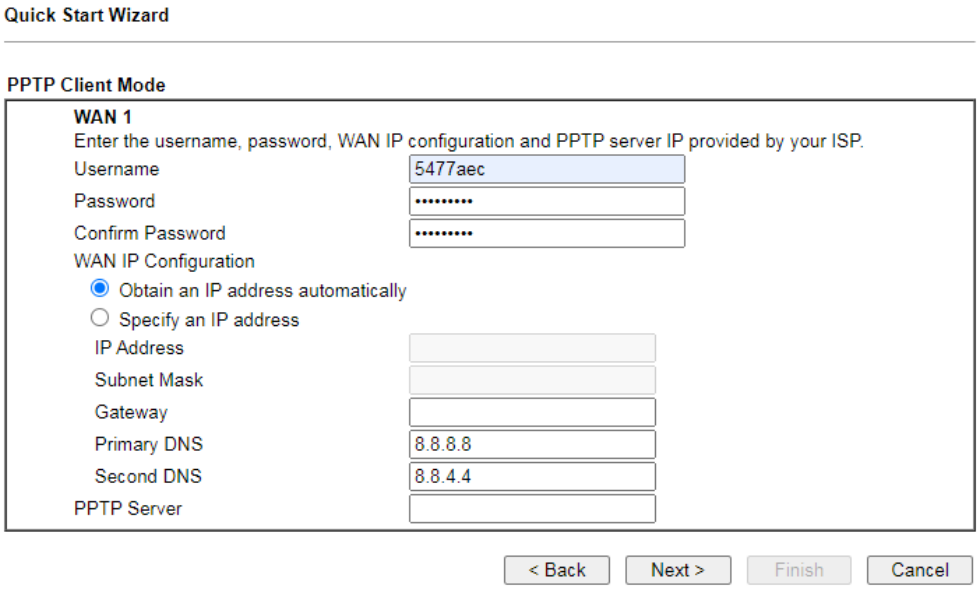
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN1 - PPTP/L2TP

1. Choose **WAN1** 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 **PPTP/L2TP (Point-to-Point Tunneling Protocol/ Layer 2 Tunneling Protocol)** as the Internet Access Type. Then click **Next** to continue.

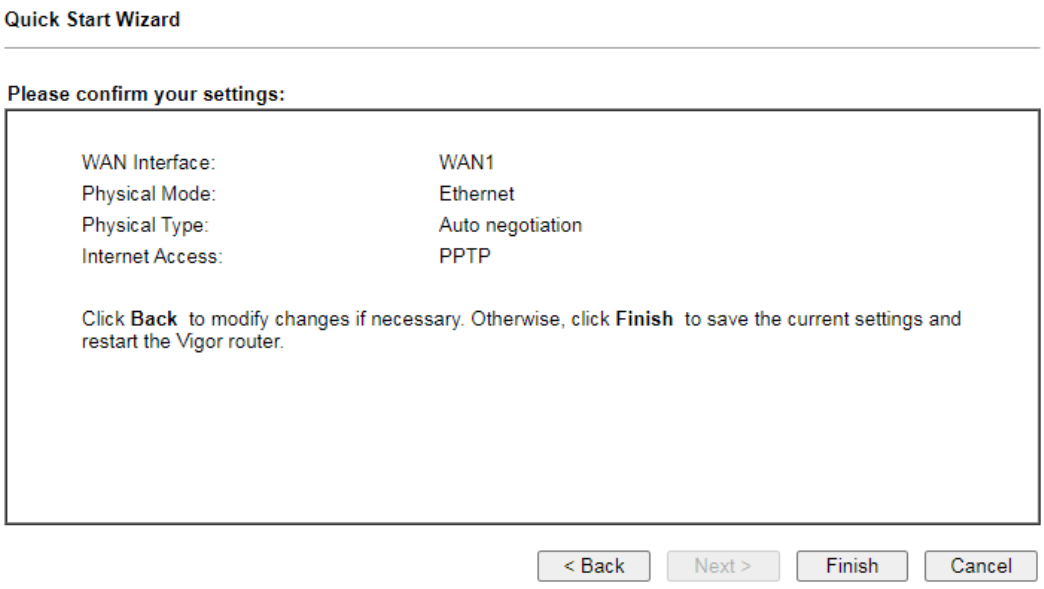


Available settings are explained as follows:

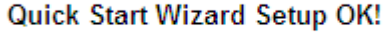
Item	Description
Username	User name provided by the ISP. The maximum length of the user name you can set is 63 characters.
Password	Password provided by the ISP. The maximum length of the password you can set is 62 characters.
Confirm Password	Re-enter the password for confirmation.

WAN IP Configuration	**Obtain an IP address automatically** – The router receives IP configuration information from a DHCP server. **Specify an IP address** – Use the IP address, Subnet Mask and Gateway values specified below. ● **IP Address** - Static WAN IP address of the router. ● **Subnet Mask** –Subnet mask of the Internet connection. ● **Gateway** – IP address of the remote gateway. ● **Primary DNS** – IP address of the Primary DNS server. ● **Second DNS** – IP address of the Secondary DNS server.
PPTP Server / L2TP Server	IP address of the PPTP or L2TP 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. Fill in the fields on the page using information provided by your ISP. Then click **Next** for viewing the summary of all the settings you have entered.



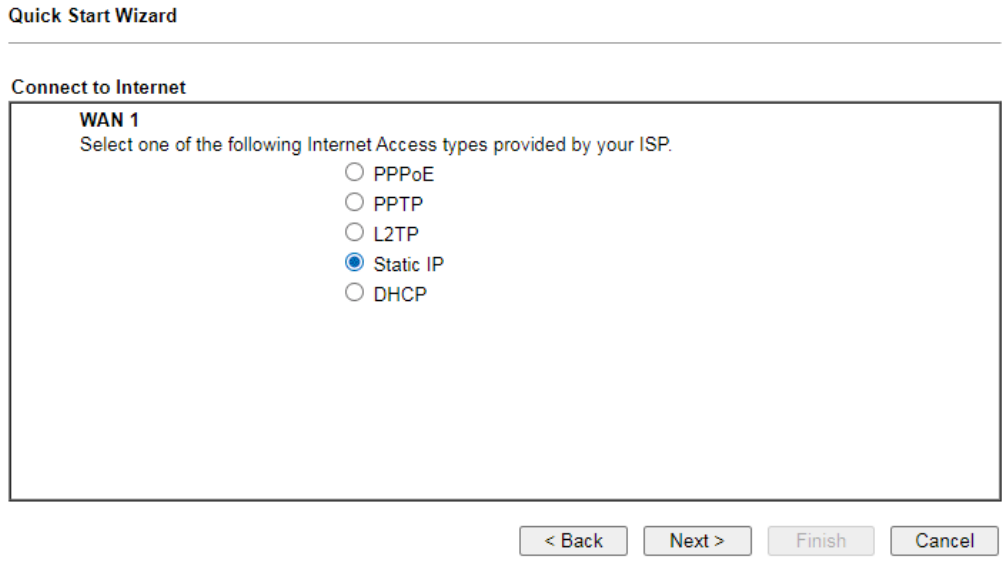
4. If you are satisfied with what you see, click **Finish** to save your changes. The following message appears indicating that the changes have been successfully saved.



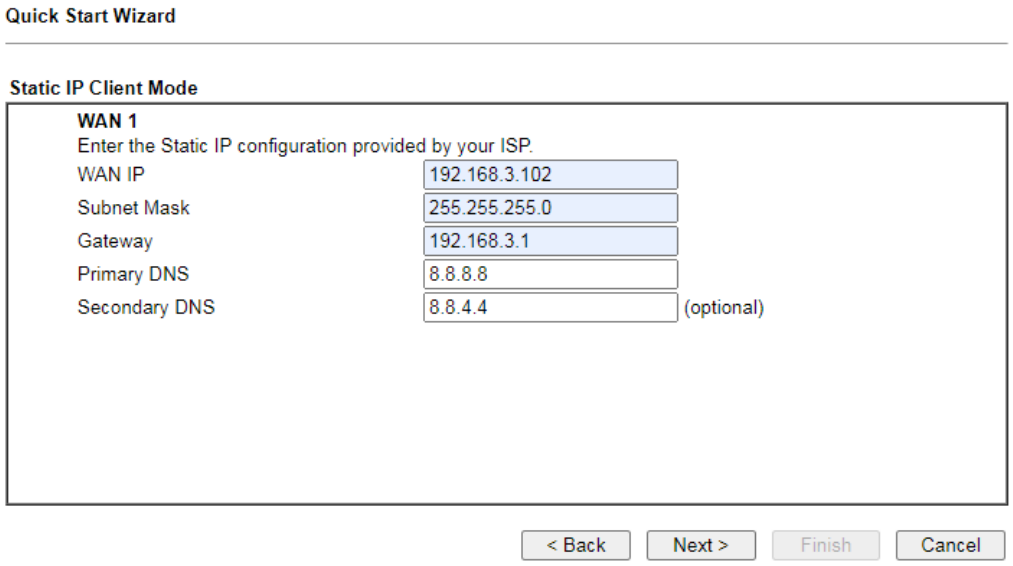
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN1 - Static IP

1. Choose **WAN1** 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 **Static IP (Statically assigned IP address)** as the Internet Access type. Simply click **Next** to continue.

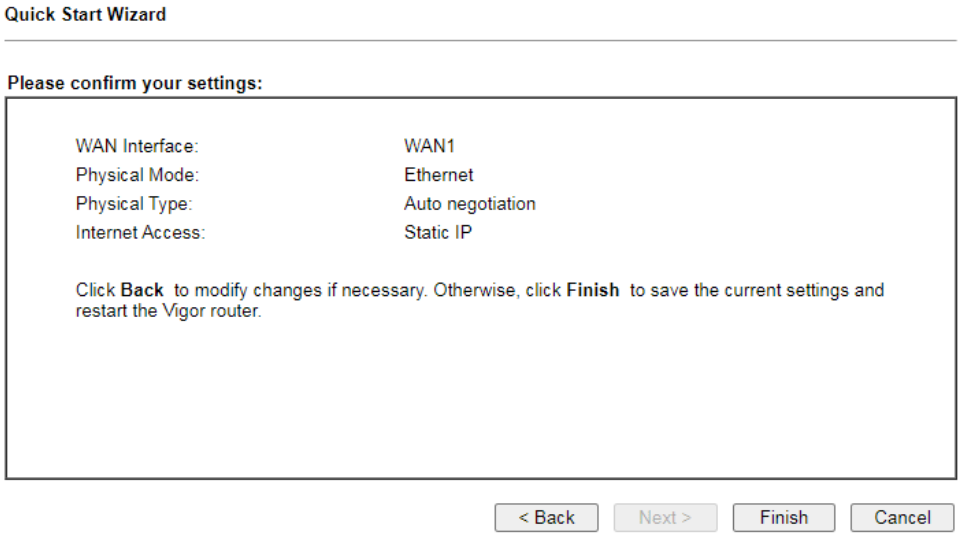


Available settings are explained as follows:

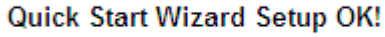
Item	Description
WAN IP	Static WAN IP address of the router.
Subnet Mask	Subnet mask of the Internet connection.
Gateway	IP address of the remote gateway.
Primary DNS	IP address of the Primary DNS server.
Secondary DNS	IP address of the Secondary DNS server.
Back	Click it to return to previous setting page.

Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Fill in the fields on the page using information provided by your ISP. Then click **Next** for viewing the summary of all the settings you have entered.



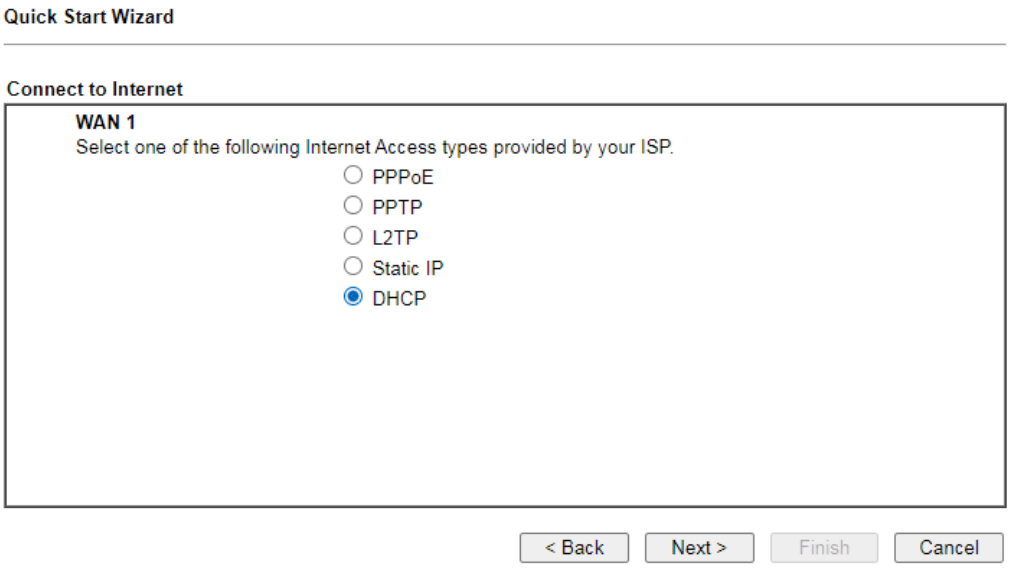
4. If you are satisfied with what you see, click **Finish** to save your changes. The following message appears indicating that the changes have been successfully saved.



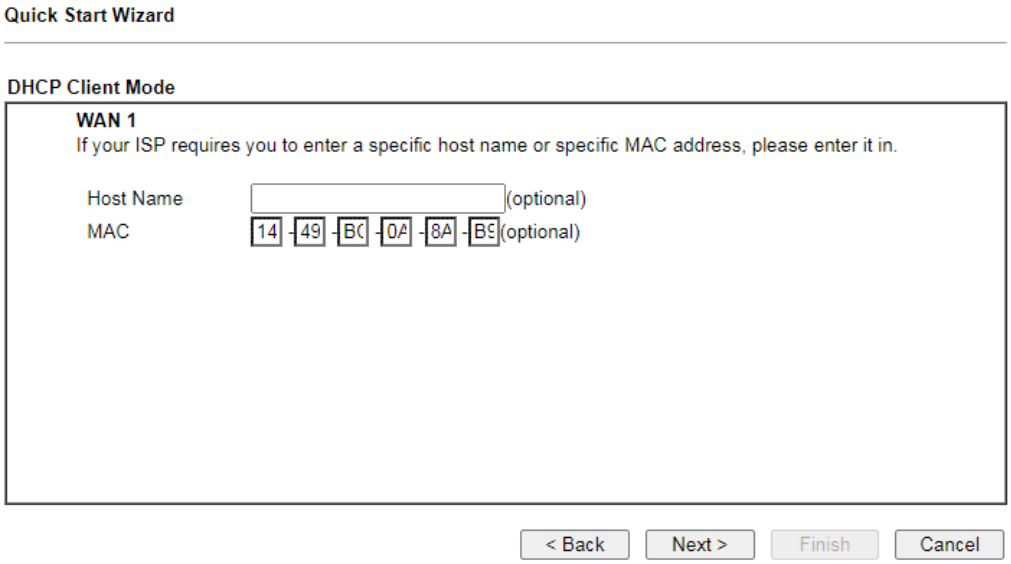
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN1 - DHCP

1. Choose **WAN1** 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.



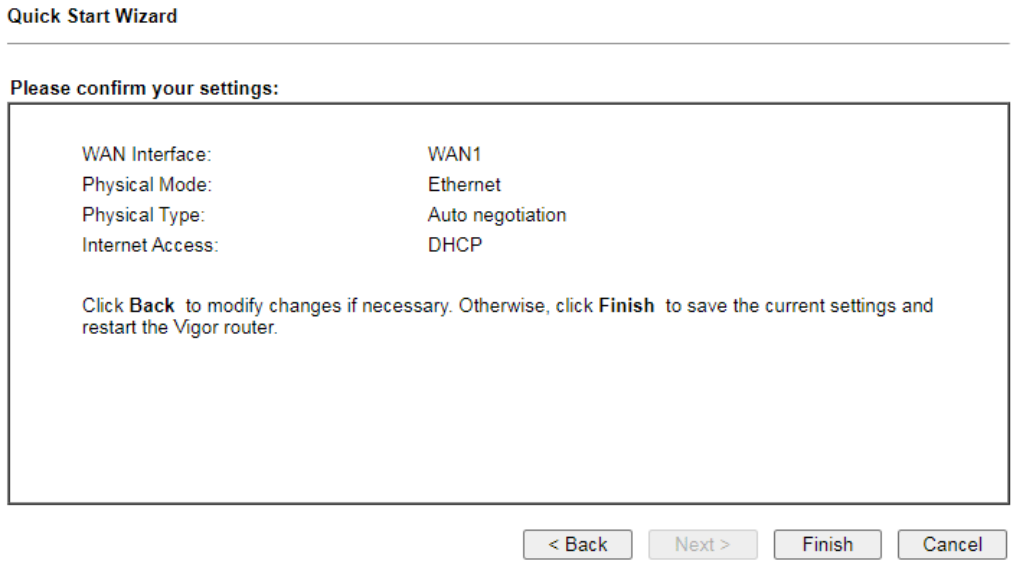
2. Click **DHCP (Dynamic Host Configuration Protocol)** as the Internet Access type. Simply click **Next** to continue.



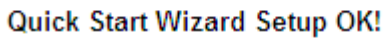
Available settings are explained as follows:

Item	Description
Host Name	Hostname required by some ISPs. Maximum length of the host name is 39 characters.
MAC	MAC address of the WAN interface. Required by some ISPs that authenticate by MAC addresses.
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. Fill in the fields on the page using information provided by your ISP. Then click **Next** for viewing the summary of all the settings you have entered.



4. If you are satisfied with what you see, click **Finish** to save your changes. The following message appears indicating that the changes have been successfully saved.



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

I-6-3 USB Connection on WAN3

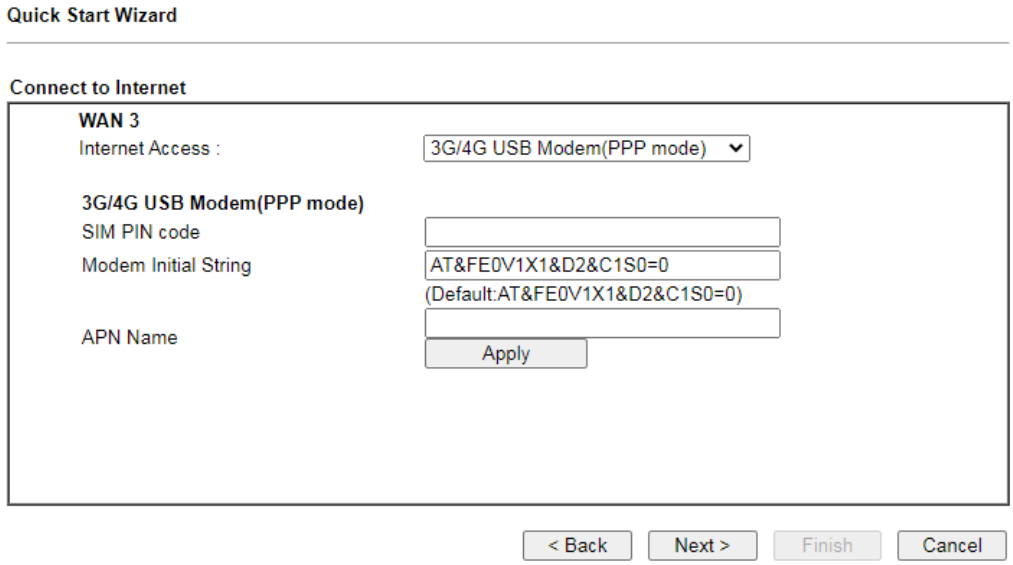
If you will be using a USB modem to connect to the Internet, you will first need to connect the modem to one of the USB ports before proceeding with the following steps.

1. Choose **WAN3** as WAN Interface.

Available settings are explained as follows:

Item	Description
Display Name	Optional name that identifies the connection.

2. Then, click **Next** for getting the following page.

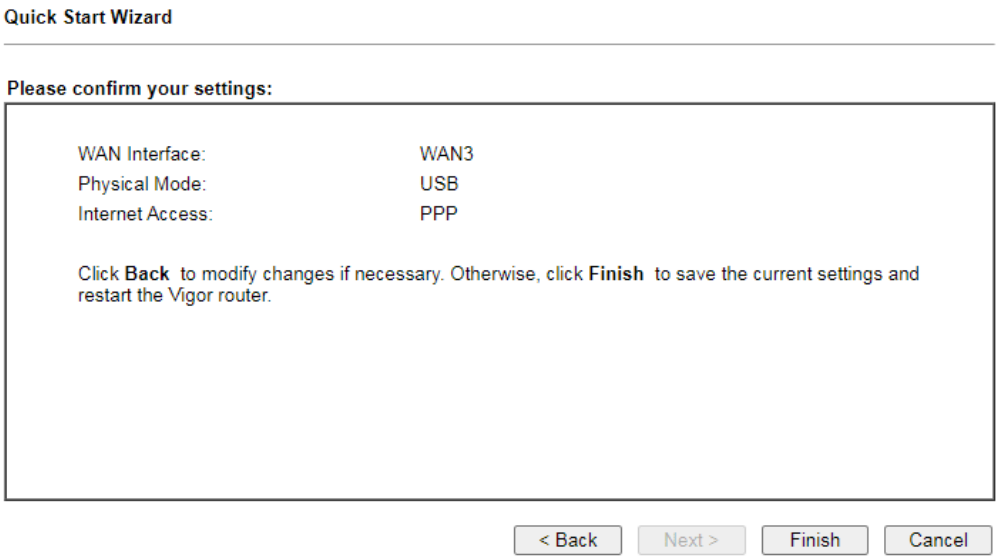


Available settings are explained as follows:

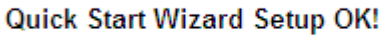
Item	Description
Internet Access	**3G/4G USB Modem(PPP mode)** – Point-to-Point Protocol is used to establish a connection. **4G USB Modem(DHCP mode)** – Dynamic Host Configuration

	Protocol is used to establish a connection.
3G/4G USB Modem (PPP mode)	**SIM Pin code** – PIN code of the SIM card in the modem. The maximum length of the PIN is 15 characters. **Modem Initial String** – String to be sent to the modem during initialization. The default value should suffice in most cases. If you need assistance with setting this value, please contact your ISP or carrier. The maximum length of the string is 47 characters. **APN Name** – Access Point Name to be used for the connection. Please contact your ISP or carrier for the appropriate value. Enter the name and click **Apply**.
3G/4G USB Modem (DHCP mode)	**SIM Pin code** – PIN code of the SIM card in the modem. The maximum length of the PIN is 15 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** – Access Point Name to be used for the connection. Please contact your ISP or carrier for the appropriate value. Enter the name and click **Apply**.
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. Fill in the fields on the page using information provided by your ISP. Then click **Next** for viewing the summary of all the settings you have entered.



4. If you are satisfied with what you see, click **Finish** to save your changes. The following message appears indicating that the changes have been successfully saved.



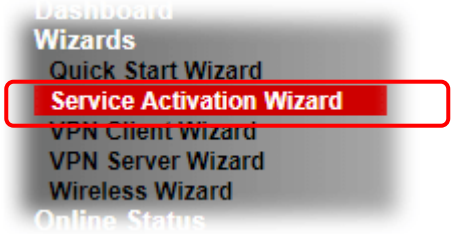
5. Now, you can enjoy surfing on the Internet.

I-7 Service Activation Wizard

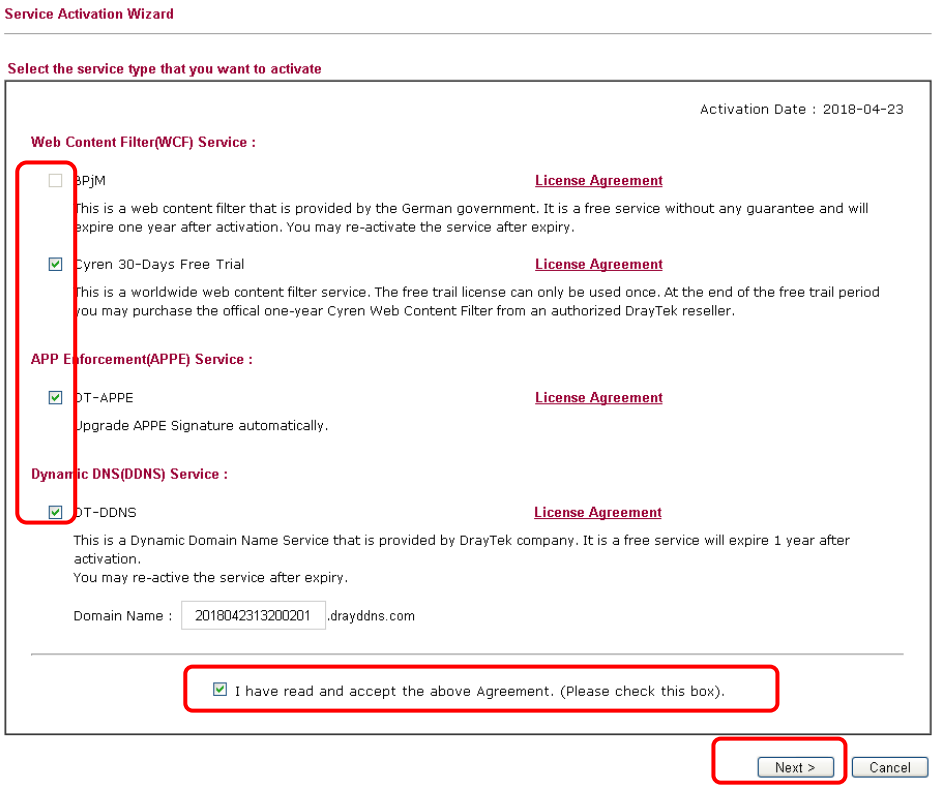
The Service Activation Wizard guides you through the activation of the Web Content Filter (WCF) and Application Enforcement (APPE) free trial subscriptions. For detailed information on the WCF and APPE services, please see the sections Web Content Filter Profile and APP Enforcement Profile.

Note: You must log in as the administrator (admin mode) to use the Service Activation Wizard.

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



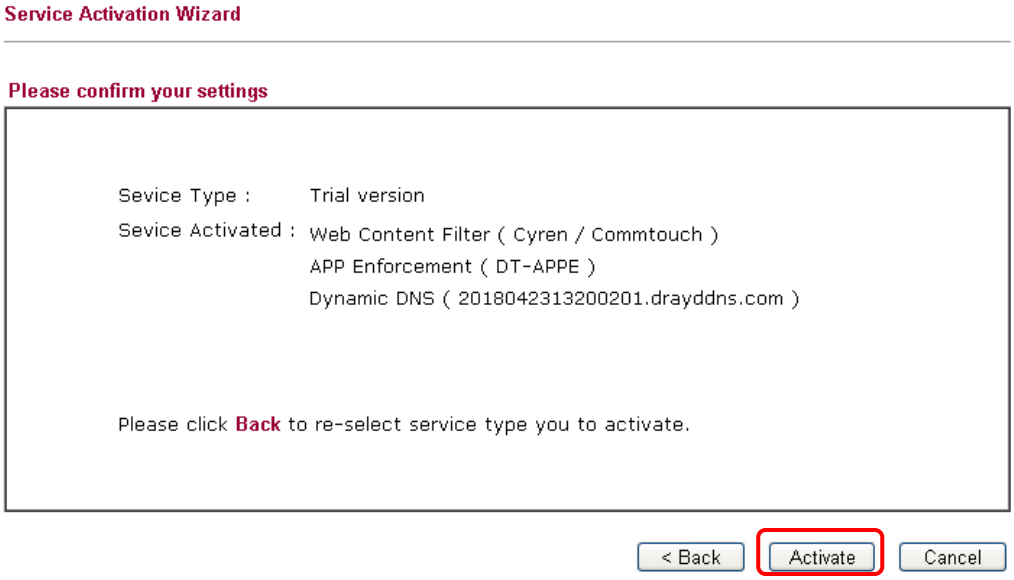
2. The screen of **Service Activation Wizard** will be shown as follows. You can activate the Web content filter services and/or APPE enforcement service and / or DDNS service at the same time or individually. When you finish the selection, please click **Next**.



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.

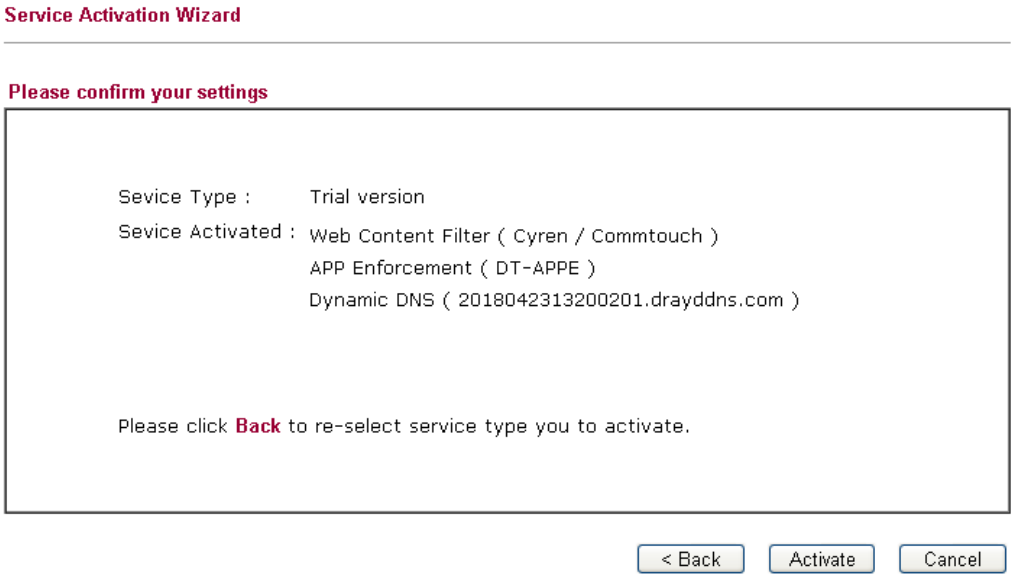
- DT-APPE, developed by DrayTek, offers a mechanism to upgrade APPE signature automatically.
- DT-DDNS, developed by DrayTek, offers one year free charge service of dynamic DNS service for internal use.

3. A confirmation page detailing your selection will be displayed. Please click **Activate**.



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

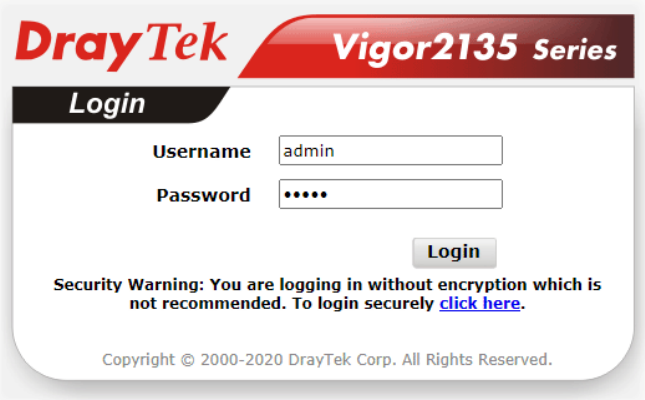
4. Now, the web page will display the service that you have activated according to your selection(s).



I-8 Registering Vigor Router

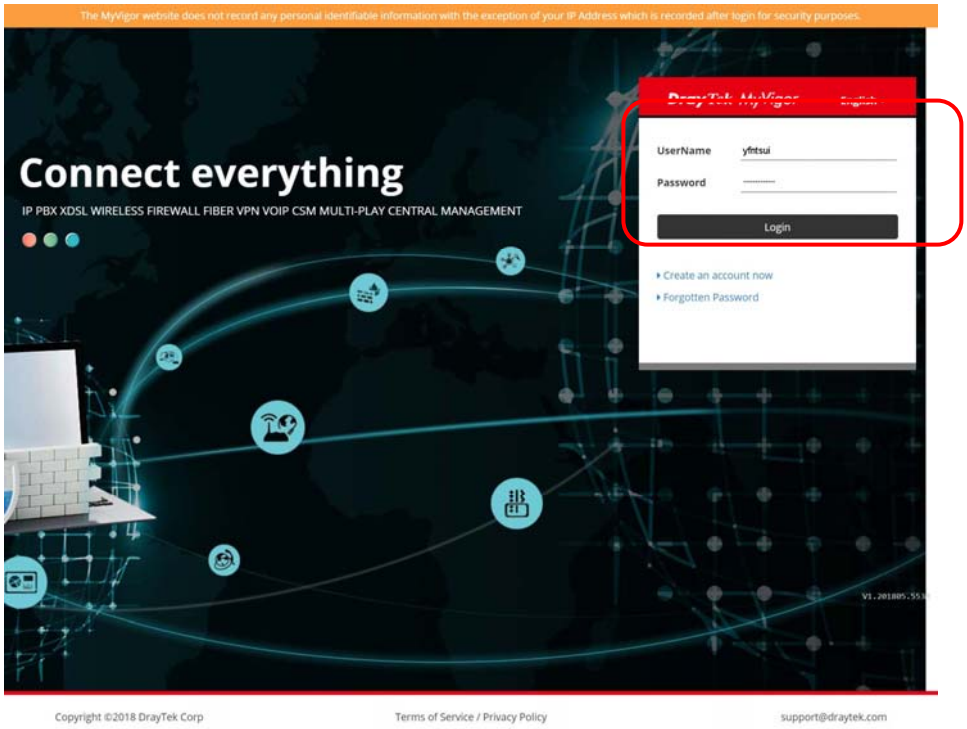
You have finished the configuration of Quick Start Wizard and you can surf the Internet at any time. Now it is the time to register your Vigor router to MyVigor website for getting more service. Please follow the steps below to finish the router registration.

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



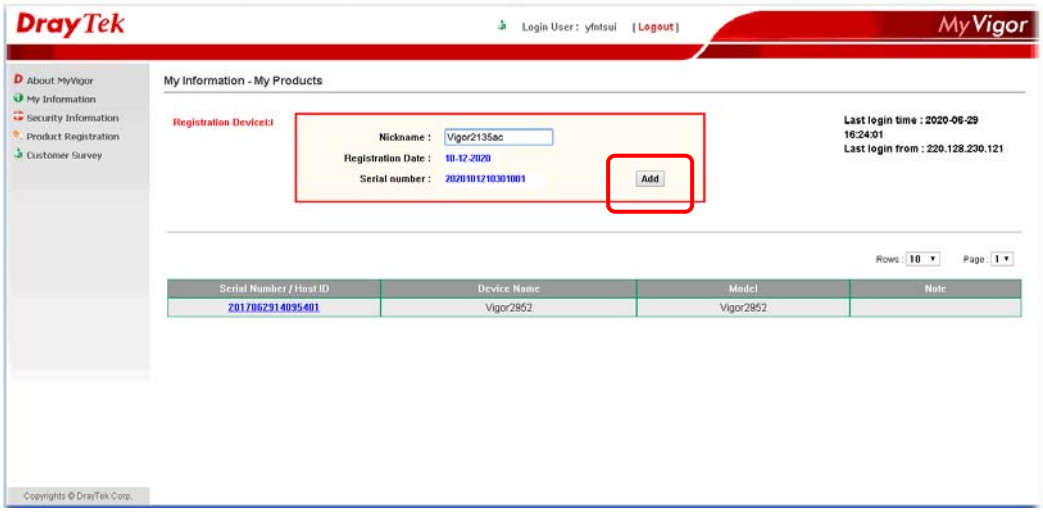
2 Click **Support Area>>Production Registration** from the home page.

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

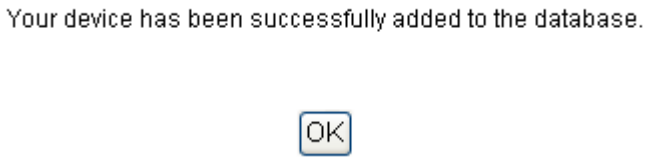


Info	If you haven't an accessing account, please refer to section Creating an Account for MyVigor to create your own one. Please read the articles on the Agreement regarding user rights carefully while creating a user account.

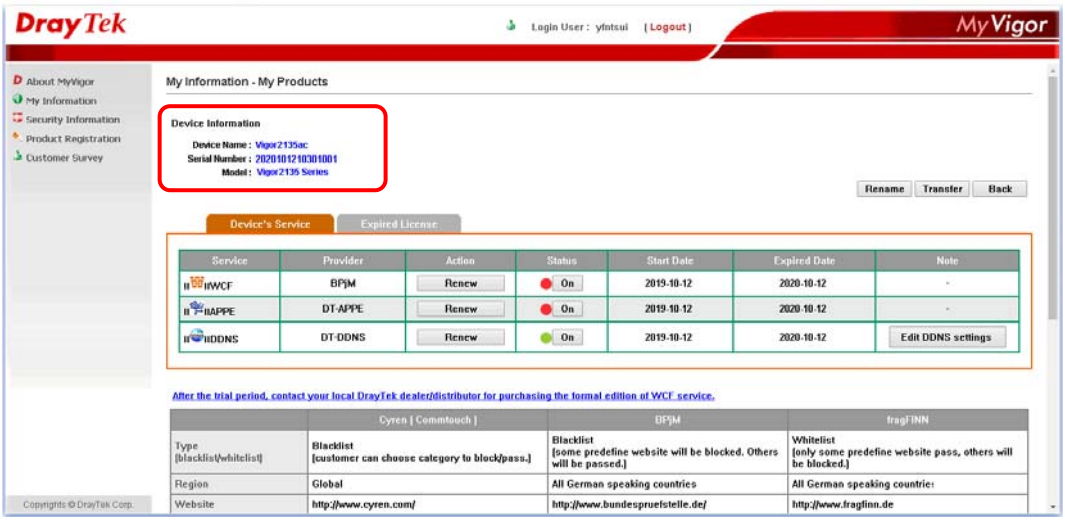
4 The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click **Add**.



5 When the following page appears, your router information has been added to the database.



6 After clicking **OK**, you will see the following page. Your router has been registered to *myvigor* website successfully.



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, LDAP, UpnP, IGMP, WOL, RADIUS, SMS, Bonjour

Static Route, Load-Balance/Route Policy

II-1 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.

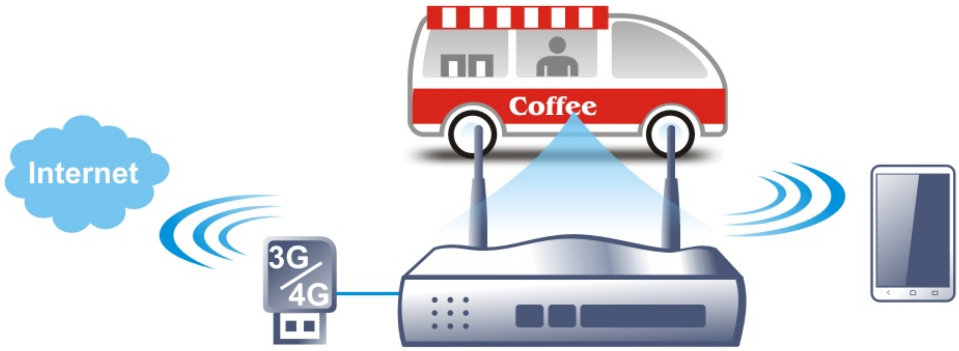
Get Your Public IP Address from ISP

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.

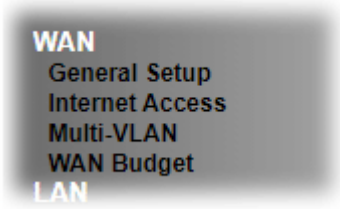
Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor2135 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2135, it can support LTE/HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor2135n with 3G/4G USB Modem allows you to receive 3G/4G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use LAN ports on the router to access Internet. Also, they can access Internet via 802.11(a/b/g/n/ac) wireless standard, and enjoy the powerful firewall, bandwidth management, and VPN features of Vigor2135n series.



After connecting into the router, 3G/4G USB Modem will be regarded as the WAN3/WAN4 port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G/4G USB Modem in WAN3/WAN4 also can be used as backup device. Therefore, when WAN1 and WAN2 are not available, the router will use 3.5G for supporting automatically. The supported 3G/4G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Web User Interface

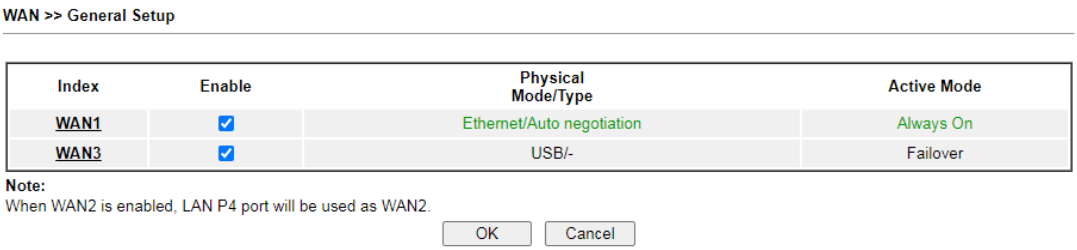


II-1-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 and WAN3 in details.

This router supports multiple-WAN function. It allows users to access Internet and combine the bandwidth of the multiple WANs to speed up the transmission through the network. Each WAN port can connect to different ISPs, even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN3 settings.

This webpage allows you to set general setup for WAN1 and WAN3 respectively.



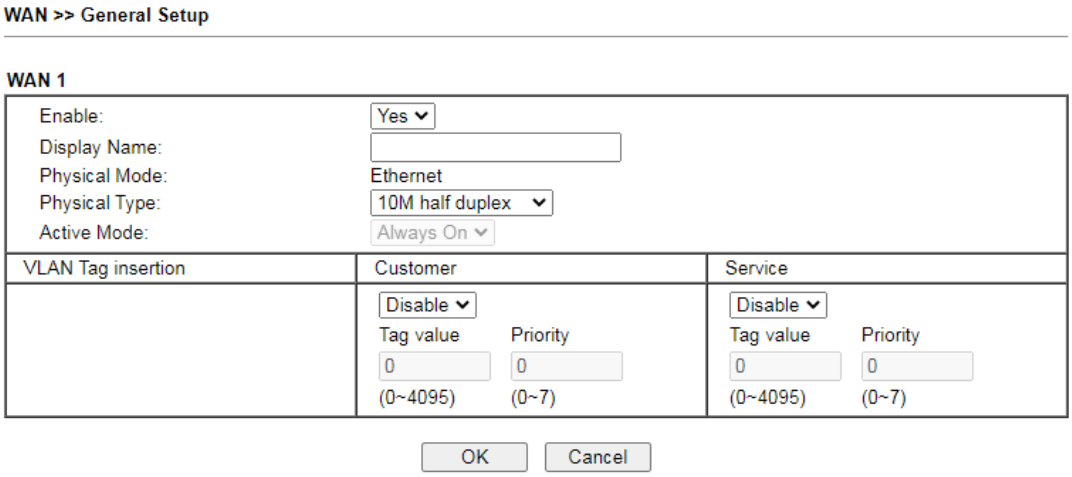
Available settings are explained as follows:

Item	Description
Index	Click on the WAN# link to bring up its settings page. WAN1: Ethernet WAN interface. WAN3: USB modem connected.
Enable	Select to enable WAN interface.
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. **Always On** - WAN is always enabled. **Failover -** Display the backup WAN interface for this WAN when it is disabled.

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

II-1-1-1 WAN1 (Ethernet)

WAN1 can be configured for physical mode of Ethernet.



Available settings are explained as follows:

Item	Description
Enable	**Yes** - WAN is enabled. **No** - WAN is disabled.
Display Name	Optional name to identify the WAN. Enter the description for the interface.
Physical Mode	Physical connection used for this WAN. **Ethernet** - WAN connection to be established through the WAN1 Ethernet port.
Physical Type	(Available only when Physical Mode is set to Ethernet) **Auto negotiation**- Ethernet connection speed is automatically negotiation between the router and the ISP's equipment. **10M half duplex**-Ethernet speed is manually set to 10 Mbit/s, half duplex. **10M full duplex**- Ethernet speed is manually set to 10 Mbit/s, full duplex. **100M half duplex**- Ethernet speed is manually set to 100 Mbit/s, half duplex. **100M full duplex**- Ethernet speed is manually set to 100 Mbit/s, full duplex. **1000M full duplex**- Ethernet speed is manually set to 1 Gbit/s, full duplex.
VLAN Tag insertion	Determines whether 802.1ad VLAN tags will be added to outbound WAN traffic in ADSL/VDSL 2 mode. Check with your ISP to determine if this is required, and if so, the proper tag and priority values to be used. **Enabled** - Tagging enabled. **Disabled** - Tagging disabled. **Tag value** – Value must be between 1 and 4095. **Priority** – Priority code point (PCP). Value must be between 0 and 7.

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

II-1-1-2 WAN3 (USB)

To use 3G/4G network connection through 3G/4G USB Modem, please configure **WAN3** interface.

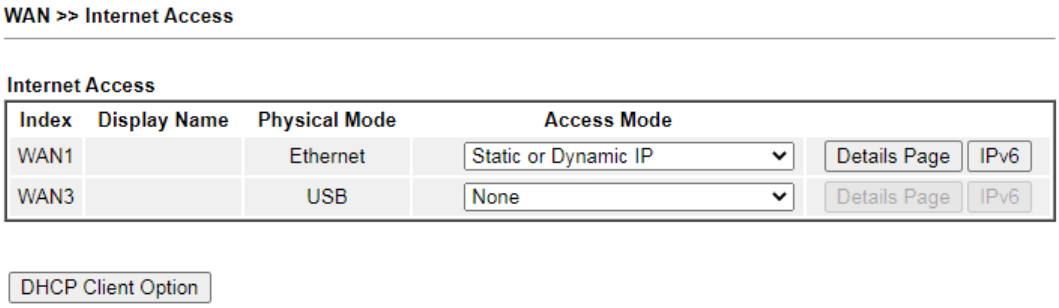
Available settings are explained as follows:

Item	Description
Enable	**Yes** - WAN is enabled. **No** - WAN is disabled.
Display Name	Optional name to identify the WAN. Enter the description for the interface.
Physical Mode	Physical connection used for this WAN. **USB -** WAN connection to be established through USB.
Active Mode	**Always On** - WAN is always enabled. **Failover** – WAN is enabled only when other WAN ports specified in Backup have lost connection.

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

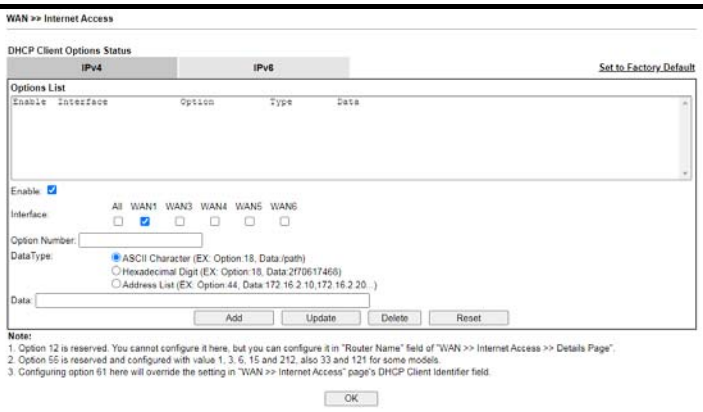
II-1-2 Internet Access

For the router supports multi-WAN function, the users can set different WAN settings (for WAN1, WAN3) for Internet Access. Due to different Physical Mode for WAN interface, the Access Mode for these connections also varies. Refer to the following figures for examples.



Available settings are explained as follows:

Item	Description
Index	The WAN interface.
Display Name	Reflects the Display Name configured for the WAN in the General Setup section.
Physical Mode	Reflects the Physical Mode configured for the WAN in the **General Setup** section.
Access Mode	Internet access mode of the WAN. 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	Click this button to bring up the Internet Access settings page.
IPv6	Click this button to bring up the IPv6 settings page. When IPv6 is enabled, the button label is shown in green: - IPv6 is enabled. - IPv6 is disabled.
DHCP Client Option	Click this button to configure additional DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.



Options List - Shows all the DHCP options that have been configured in the system**.**

Enable/Disable – If selected, DHCP option entry is enabled. If unselected, DHCP option entry is disabled. Each DHCP option is composed by an option number with data. For example,

Option number:100

Data: abcd

When it is enabled, the specified values for DHCP option will be seen in DHCP reply packets.

Interface – WAN interface(s) to which this entry is applicable. WAN1 through WAN4 are physical WANs that can be set up in the WAN>>General Setup and WAN>>Internet Access sections. WAN7 through WAN9 are virtual WANs that can be set up in the WAN>>Multi-PVC/VLAN section.

Option Number – Enter a number for this function.

DataType – Choose the type (ASCII or Hex or Address List) for the data to be stored. Type of data in the Data field:

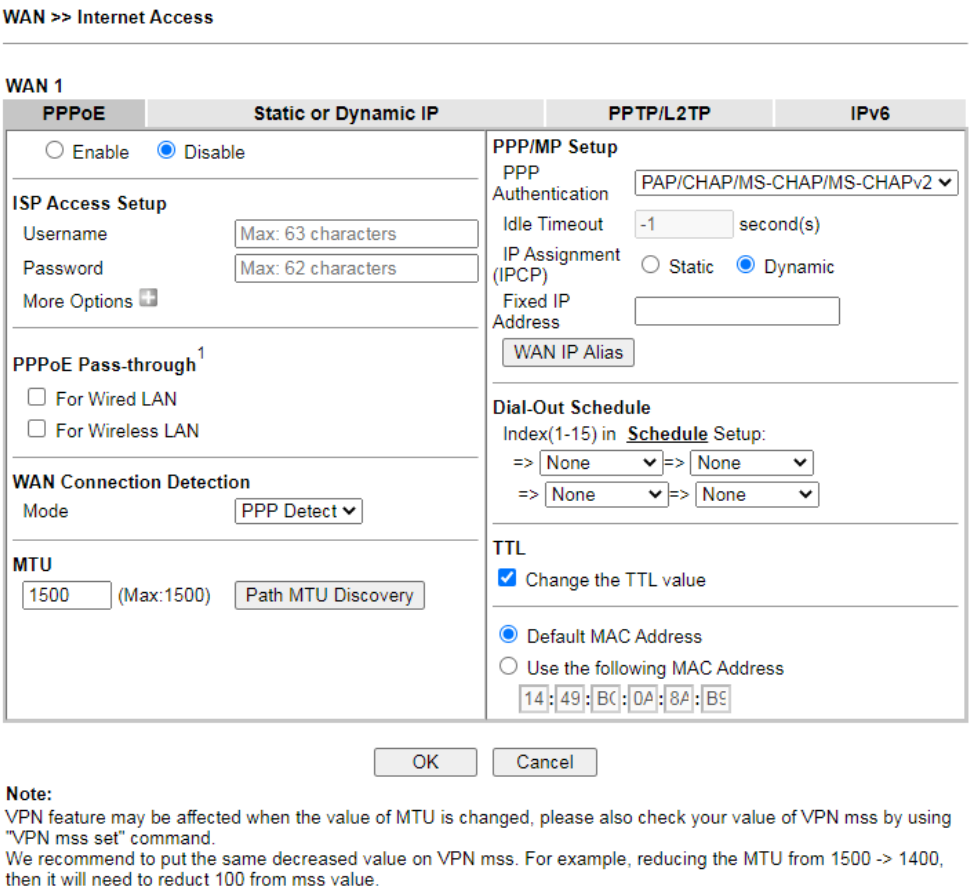
- ASCII Character: A text string. Example: /path.
- Hexadecimal Digit: A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.
- Address List: One or more IPv4 addresses, delimited by commas.

Data – Data of this DHCP option. Enter the content of the data to be processed by the function of DHCP option.

Info	If you choose to configure option 61 here, the detailed settings in WAN>>Interface Access will be overwritten.

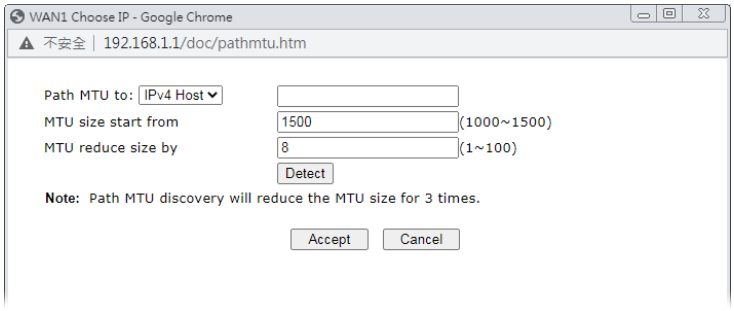
II-1-2-1 WAN1 Details Page (PPPoE, Physical Mode: Ethernet)

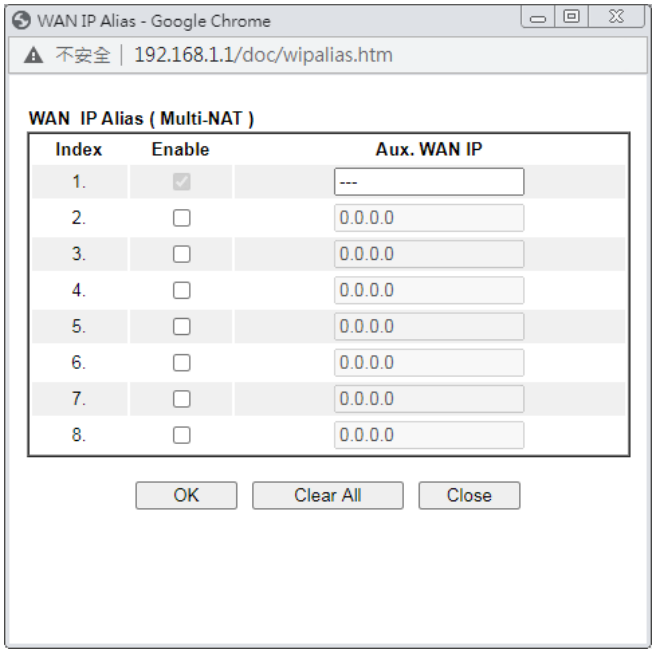
To choose PPPoE as the accessing protocol of the Internet, please select **PPPoE** from the **WAN>>Internet Access >>WAN1** page. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Enable/Disable	Enable or disable **PPPoE** access mode.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. **Username** – Username provided by the ISP for PPPoE authentication. **Password** – Password provided by the ISP for PPPoE authentication. **More Options** - Click to display more options. • **Service Name (Optional) -** Sets the PPP service name tag. Required by some ISPs. Leave blank unless instructed otherwise by your ISP**.**
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. **For Wired LAN** – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. **For Wireless LAN** – It is available for *n* model. If you check

	this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.
WAN Connection Detection	Configures how the WAN connection is monitored. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. ● **ARP Detect** - The router broadcasts an ARP request every 5 seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Primary/Secondary Ping IP** – Enter Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – 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)** – Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255. ● **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	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492. **Path MTU Discovery** – Use this feature to determine the optimal MTU size for the WAN. Click **Detect** to open the following dialog.  ● **Path MTU to** – Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, and then enter the IP address in the textbox. ● **MTU size start from** – Determine the starting point value of the packet. ● **MTU reduce size by** – Number of octets by which to

	decrease the 1500-byte MTU. Start with a 0 value for the reduce size and click the Detect button. If the message Fail is returned, increase the MTU reduce size and try again. Repeat until you see the message Success, indicating that the optimal MTU size has been reached. ● **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/MP Setup	**PPP Authentication** – The protocol used for PPP authentication. ● **PAP only** - Only PAP (Password Authentication Protocol) is used. ● **PAP/CHAP/MS-CHAP/MS-VHAPv2** - 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. **Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action. **IP Assignment (IPCP)** - Configure the router according to how your ISP allocates WAN IP address(es) to you. **Fixed IP Address –** WAN IP address assigned by the ISP. **WAN IP Alias** - Click to enter multiple WAN IP addresses assigned by your ISP. 
Dial-Out Schedule Setup	Specify up to 4 time schedule entries to enable or disable the WAN. 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.
TTL	**Change the TTL value –** Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router. ● **If enabled** - 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”.

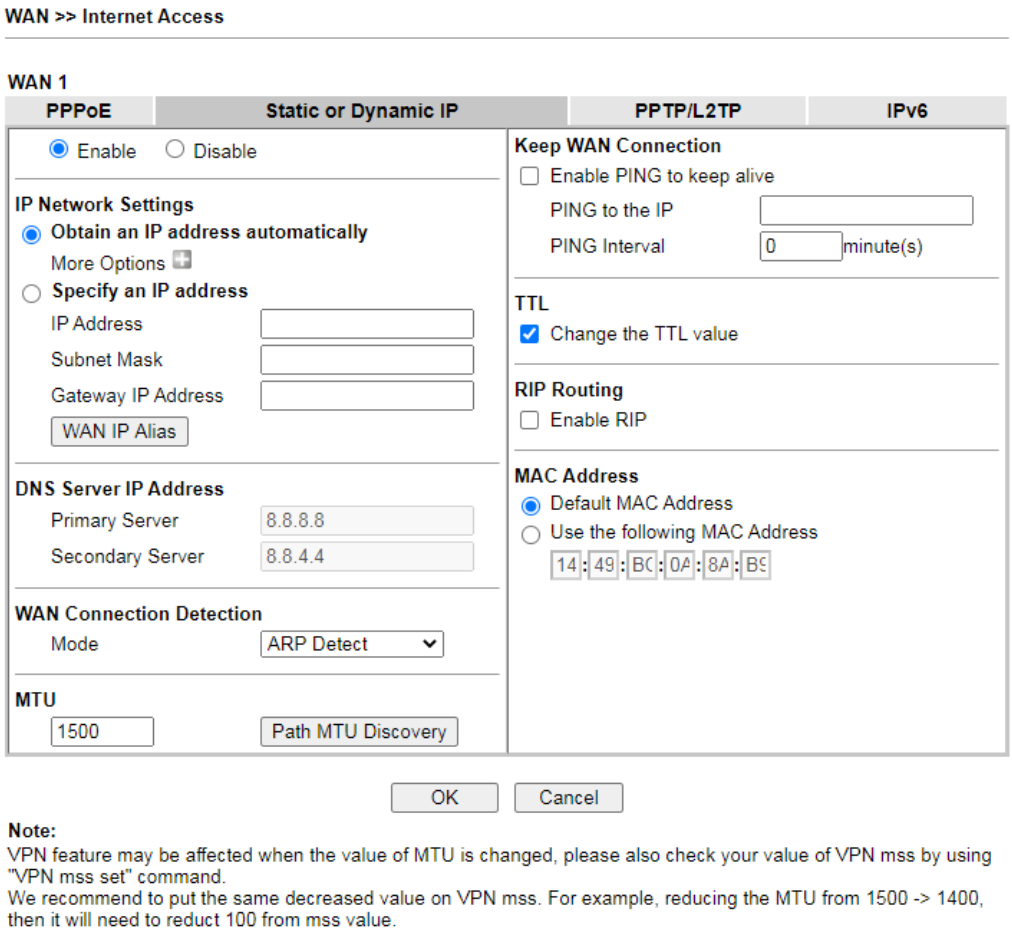
	● **If disabled** – TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP. **Default MAC Address** – Use the default MAC address for the WAN Ethernet port. **Specify a MAC Address** – Specify a MAC address for the WAN Ethernet port. Select this option if your ISP authenticates by MAC addresses.

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

II-1-2-2 WAN2 Details Page (Static or Dynamic IP, Physical Mode: Ethernet)

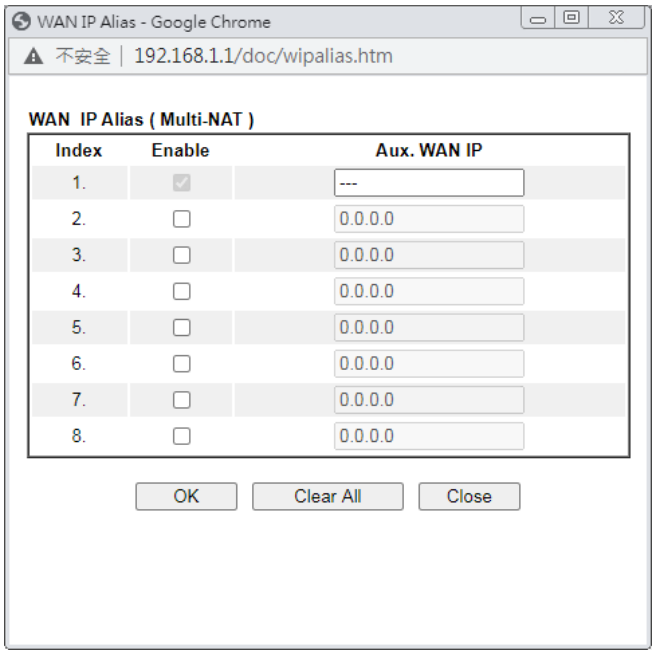
For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you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

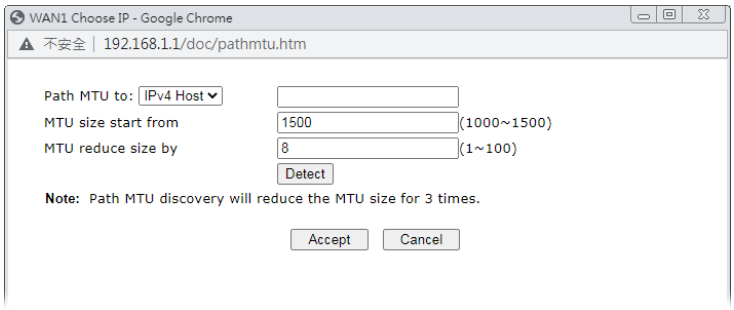
To use **Static or Dynamic IP** as the accessing protocol of the internet, please click the **Static or Dynamic IP** tab. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Enable/Disable	Enable or disable **Static or Dynamic IP** access mode.
IP Network Settings	**Obtain an IP address automatically** – The router receives IP

	configuration information from a DHCP server. **More Options** - Click to display more options. ● **Router Name** – Used by some ISPs. Contact your ISP for the appropriate values. ● **Domain Name** –Used by some ISPs. Contact your ISP for the appropriate values. ● **DHCP Client Identifier* -** Used by some ISPs that authenticates using DHCP Client Identifier (Option 61). To enable, tick this box and fill out the Username and Password fields below. **Specify an IP address** –Use the IP address, Subnet Mask and Gateway values specified below. ● **IP Address** –WAN IP address assigned by the ISP. ● **Subnet Mask** –WAN subnet mask. ● **Gateway IP Address** – IP address of the WAN Gateway. **WAN IP Alias** - Click to enter multiple WAN IP addresses assigned by your ISP. 
DNS Server IP Address	**Primary IP Address** - IP address of primary DNS server. **Secondary IP Address** - IP address of secondary DNS server.
WAN Connection Detection	Configures how the WAN connection is monitored. **Mode** – Choose **ARP Detect, Ping Detect, Always On** or **Strict ARP Detect** for the system to execute for WAN detection. ● **ARP Detect** - The router broadcasts an ARP request every 5 seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. ● **Always On**- The router assumes the WAN connection is always active. If you choose **Ping Detect** as the detection mode, you have

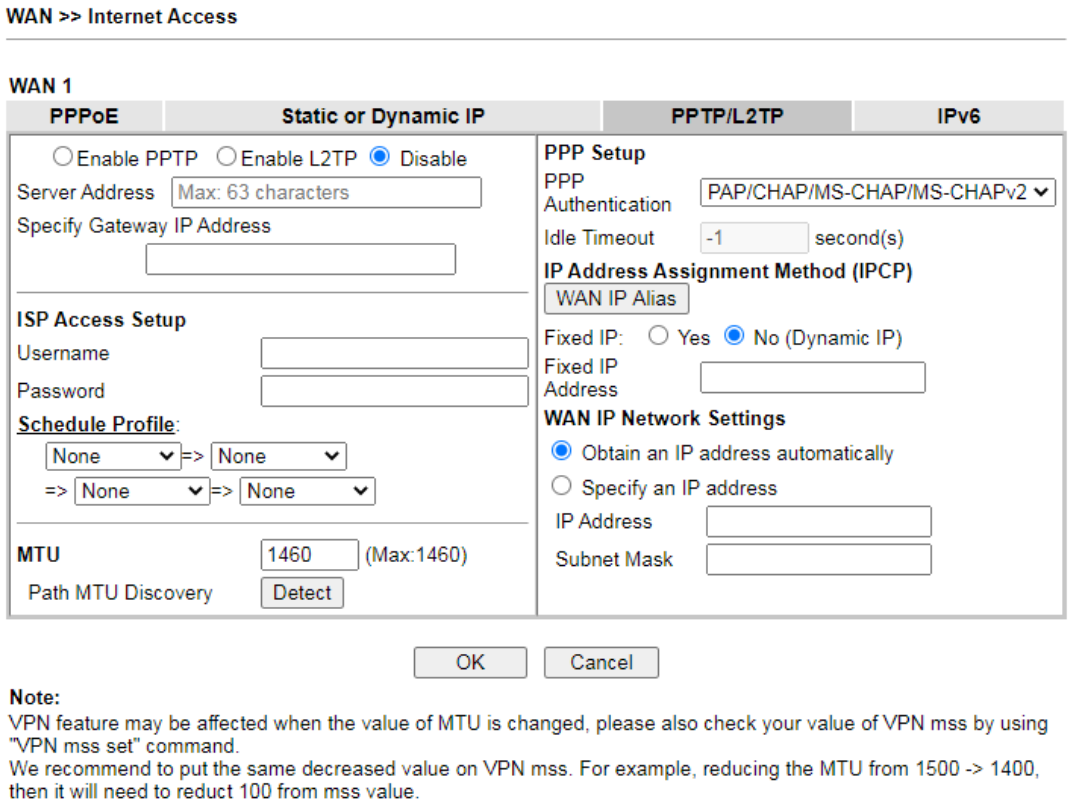
	to enter required settings for the following items. ● **Primary/Secondary Ping IP** – Enter Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – Enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● **TTL (Time to Live)** – Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255. ● **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	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492. **Path MTU Discovery** – Use this feature to determine the optimal MTU size for the WAN. Click **Detect** to open the following dialog.  ● **Path MTU to** – Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, and then enter the IP address in the textbox. ● **MTU size start from** – Determine the starting point value of the packet. ● **MTU reduce size by** – Number of octets by which to decrease the 1500-byte MTU. Start with a 0 value for the reduce size and click the Detect button. If the message Fail is returned, increase the MTU reduce size and try again. Repeat until you see the message Success, indicating that the optimal MTU size has been reached. ● **Detect** – Click it to detect a suitable MTU value. ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
Keep WAN Connection	**Enable PING to keep alive** - If selected, ping a WAN host to maintain the connection. If unselected, ping to keep WAN alive is disabled. **PING to the IP** - IP address of host to be pinged. **PING Interval** - Number of minutes to wait before sending a ping request to the WAN host.
TTL	**Change the TTL value –** Enable or disable the TTL (Time to

	Live) for a packet transmitted through Vigor router. ● **If enabled** - 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". ● **If disabled** – 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.
RIP Protocol	Routing Information Protocol is abbreviated as RIP(RFC1058). If selected, the router can exchange routing information with other routers.
MAC Address	**Default MAC Address** – Use the default MAC address for the WAN Ethernet port. **Specify a MAC Address** – Specify a MAC address for the WAN Ethernet port. Select this option if your ISP authenticates by MAC addresses.

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

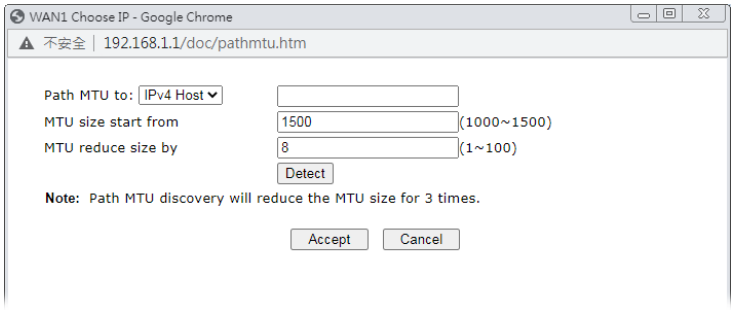
II-1-2-3 WAN2 Details Page (PPTP/L2TP, Physical Mode: Ethernet)

To use **PPTP/L2TP** as the accessing protocol of the internet, please click the **PPTP/L2TP** tab. The following web page will be shown.



Available settings are explained as follows:

Item	Description
PPTP/L2TP	**Enable PPTP**- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface. **Enable L2TP** - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface. **Disable** – Click this radio button to close the connection through PPTP or L2TP. **Server Address** - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode. **Specify Gateway IP Address** – Specify the gateway IP address for the WAN interface.
ISP Access Setup	**Username** – Username provided by the ISP for PPTP/L2TP authentication. **Password** – Password provided by the ISP for PPTP/L2TP authentication. **Schedule Profile** - Specify up to 4 time schedule entries to enable or disable the WAN. 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.
MTU	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE

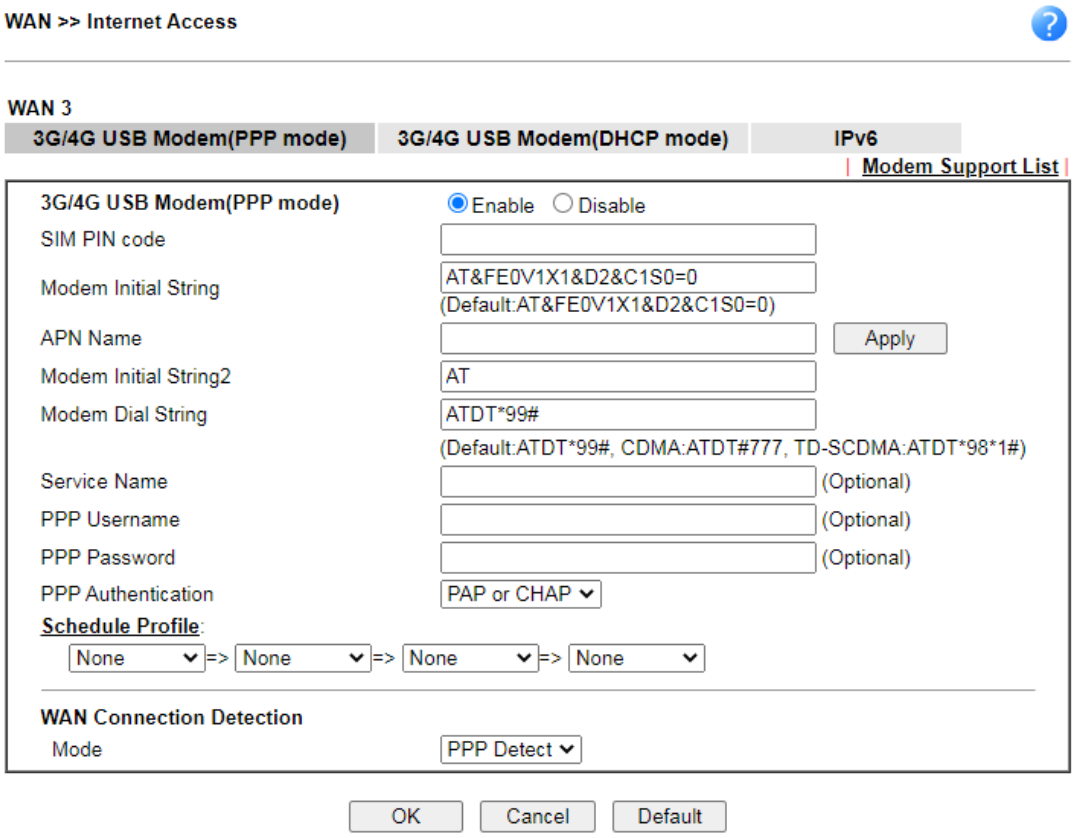
	is 1492. **Path MTU Discovery** – Use this feature to determine the optimal MTU size for the WAN. Click **Detect** to open the following dialog.  ● **Path MTU to** – Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, and then enter the IP address in the textbox. ● **MTU size start from** – Determine the starting point value of the packet. ● **MTU reduce size by** – Number of octets by which to decrease the 1500-byte MTU. Start with a 0 value for the reduce size and click the Detect button. If the message Fail is returned, increase the MTU reduce size and try again. Repeat until you see the message Success, indicating that the optimal MTU size has been reached. ● **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** – The protocol used for PPP authentication. ● **PAP only** - Only PAP (Password Authentication Protocol) is used. ● **PAP/CHAP/MS-CHAP/MS-VHAPv2**- 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. ● **Idle Timeout -** Maximum length of time, in seconds, of idling allowed (no traffic) before the connection is dropped.
IP Address Assignment Method(IPCP)	Configure the router according to how your ISP allocates WAN IP address(es) to you. **WAN IP Alias** - Configure the router according to how your ISP allocates WAN IP address(es) to you. **Fixed IP** – Enter a fixed IP address. ● **Yes**- ISP has assigned a fixed WAN IP address, which is to be entered below in Fixed IP Address. ● **No**-WAN IP address is dynamically allocated. **Fixed IP Address –** WAN IP address assigned by the ISP.
WAN IP Network Settings	**Obtain an IP address automatically** – The router receives IP configuration information from a DHCP server. **Specify an IP address** –Use the IP address, Subnet Mask and

	Gateway values specified below. ● **IP Address** –WAN IP address assigned by the ISP. ● **Subnet Mask** –WAN subnet mask.

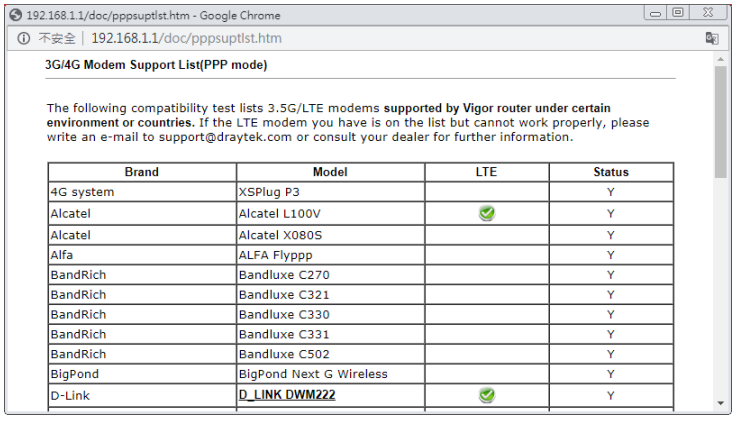
After finishing all the settings here, please click **OK** to activate them.

II-1-2-4 WAN3 Details Page (PPP mode, Physical Mode: USB)

To use **3G/4G USB Modem (PPP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (PPP mode)** for WAN3. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Modem Support List	It lists all of the modems supported by such router. 
3G /4G USB Modem (PPP mode)	Enable or disable **3G /4G USB Modem (PPP mode)** access mode.
SIM PIN code	Enter PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 15 characters.

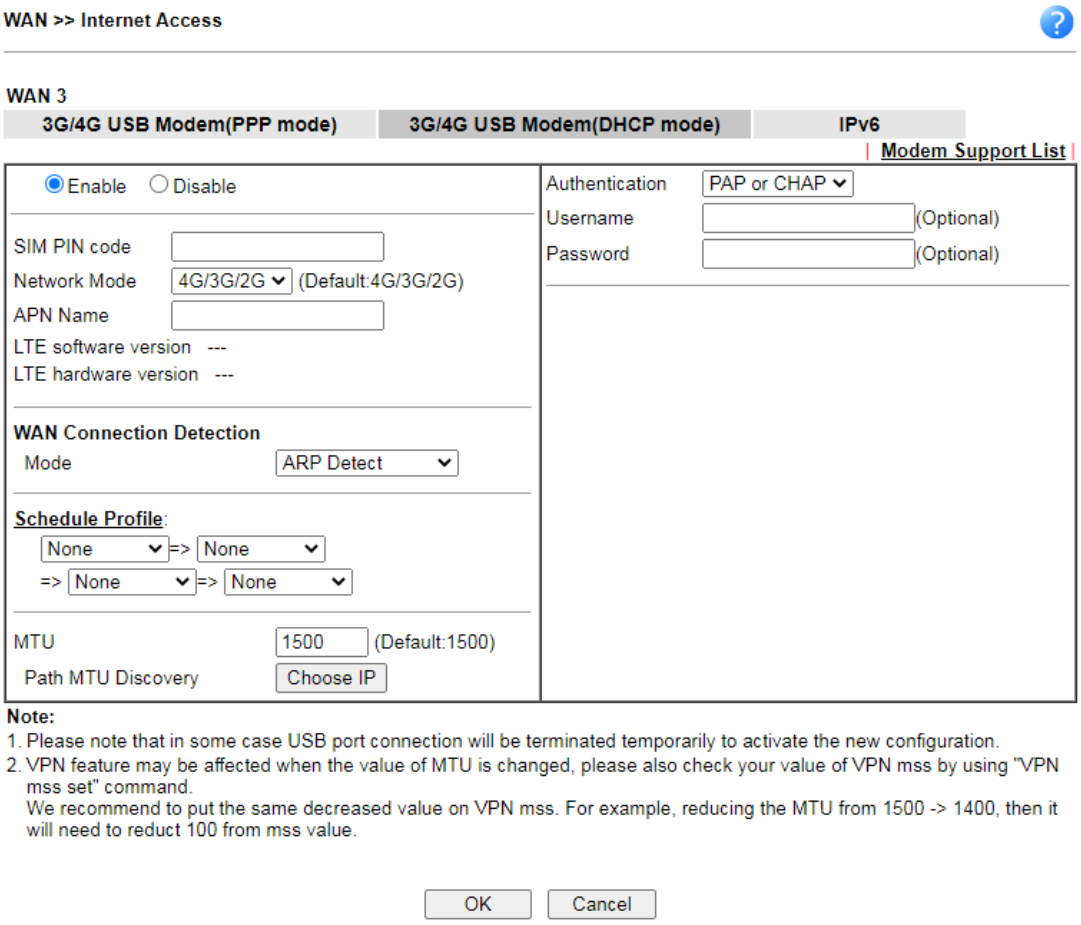
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Enter the name and click **Apply**. The maximum length of the name you can set is 43 characters.
Modem Initial String2	The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings. The maximum length of the string you can set is 47 characters.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 31 characters.
Service Name	Enter the description of the specific network service.
PPP Username	Enter the PPP username (optional). The maximum length of the name you can set is 63 characters.
PPP Password	Enter the PPP password (optional). The maximum length of the password you can set 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.
Schedule Profile	Specify up to 4 time schedule entries to enable or disable the WAN. 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	Configures how the WAN connection is monitored. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. ● **ARP Detect** - The router broadcasts an ARP request every 5 seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Primary/Secondary Ping IP** – Enter Primary or Secondary IP address in this field for pinging. ● **TTL (Time to Live)** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values

	range from 1 to 255. ● **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.

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

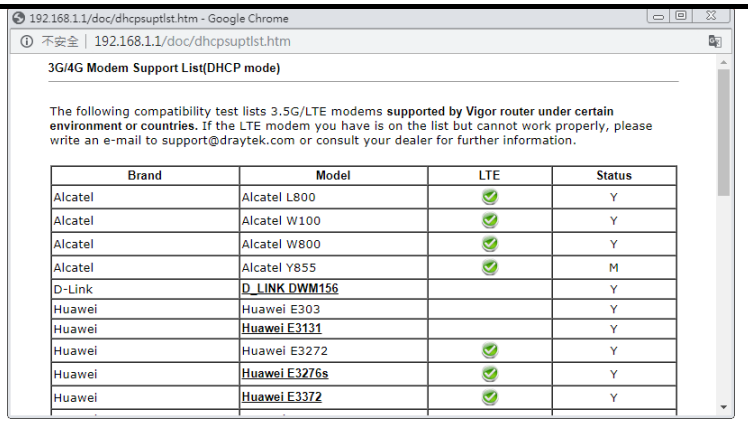
II-1-2-5 WAN3 Details Page (DHCP mode, Physical Mode: USB)

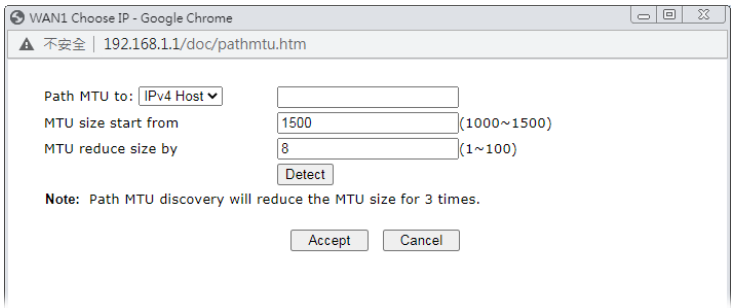
To use **3G/4G USB Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (DHCP mode)** for WAN3. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Modem Support List	It lists all of the modems supported by such router.

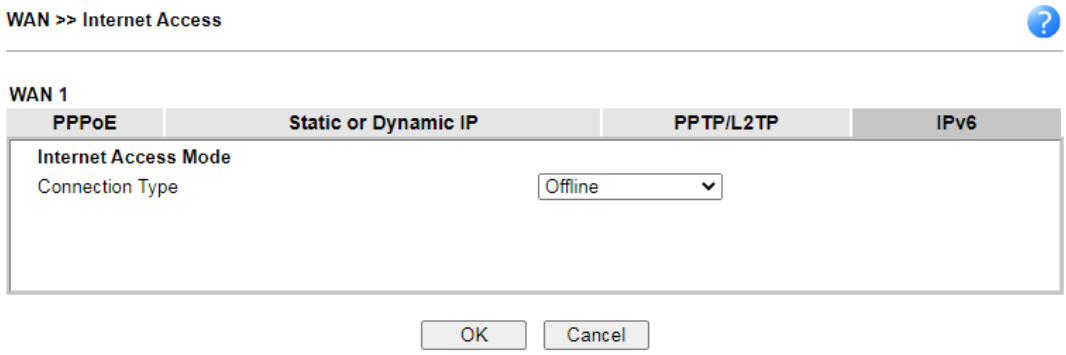
	
Enable / Disable	Enable or disable **3G /4G USB Modem (DHCP mode)** access mode.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 19 characters.
Network Mode	Force Vigor router to connect Internet with the mode specified 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. Enter the name and click **Apply.** The maximum length of the name you can set is 47 characters.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect, Strict ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect, Strict 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. ● **ARP Detect** - The router broadcasts an ARP request every 5 seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. ● **Strict ARP Detect** If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Primary/Secondary Ping IP** – Enter Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – 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)** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255. ● **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.
Schedule Profile	Specify up to 4 time schedule entries to enable or disable the WAN. 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.
MTU	Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. **Path MTU Discovery** – Use this feature to determine the optimal MTU size for the WAN. Click **Choose IP** to open the following dialog.  ● **Path MTU to** – Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, and then enter the IP address in the textbox. ● **MTU size start from** – Determine the starting point value of the packet. ● **MTU reduce size by** – Number of octets by which to decrease the 1500-byte MTU. Start with a 0 value for the reduce size and click the Detect button. If the message Fail is returned, increase the MTU reduce size and try again. Repeat until you see the message Success, indicating that the optimal MTU size has been reached. ● **Detect** – Click it to detect a suitable MTU value ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
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. **Username** –Username provided by the ISP for authentication (optional). **Password** –Password provided by the ISP for authentication (optional).

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

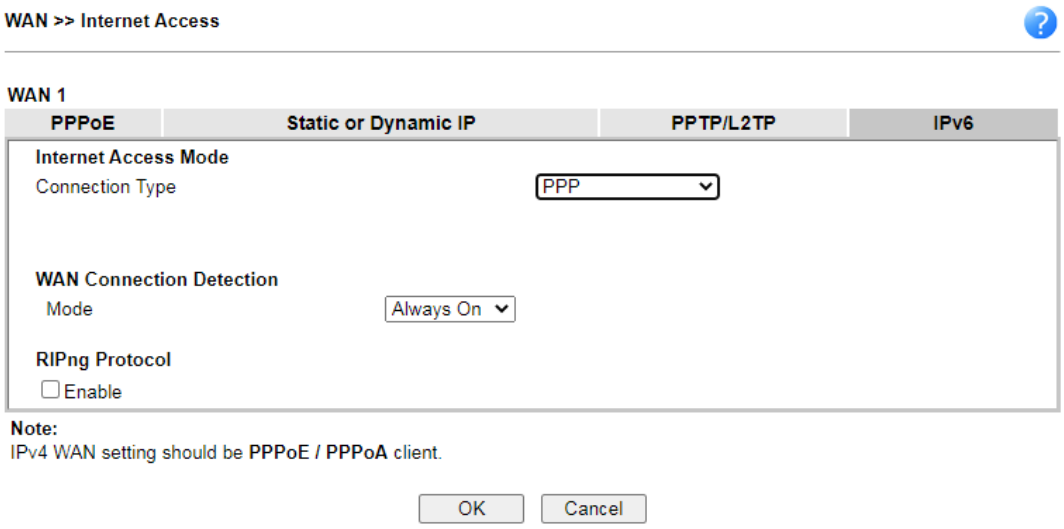
II-1-2-6 WAN1/WAN3 Details Page for IPv6 – Offline

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



II-1-2-7 WAN1 Details Page for IPv6 – PPP

IPv6 WAN address is assigned along with the IPv4 WAN address during PPPoE negotiation. This IPv6 access mode requires that the IPv4 uses PPPoE.

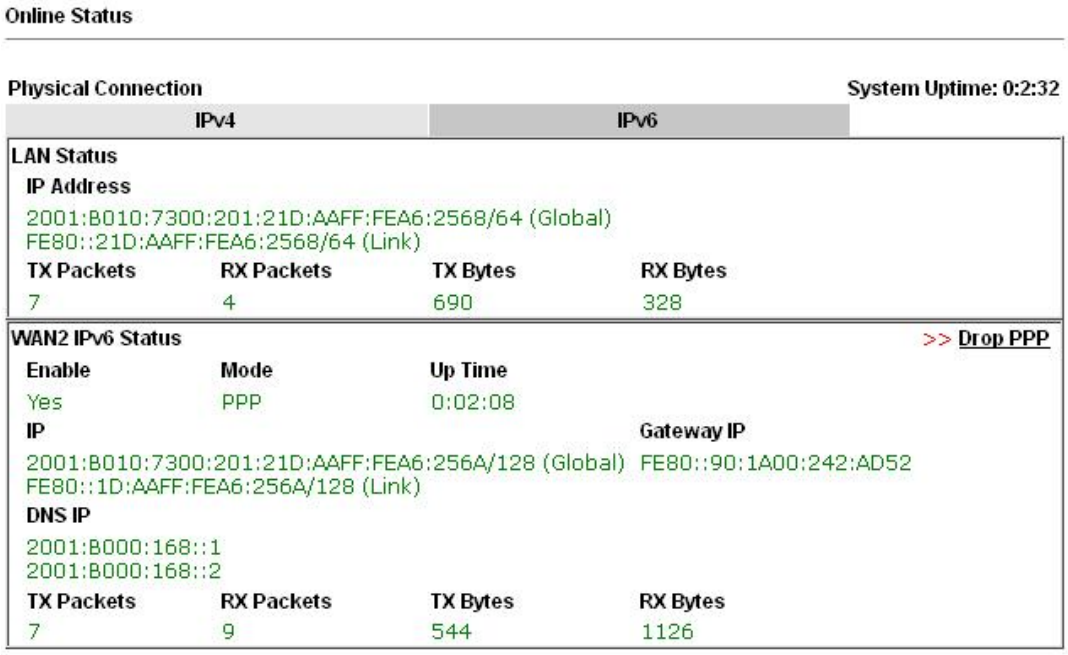


Available settings are explained as follows:

Item	Description
WAN Connection Detection	Configures how the WAN connection is monitored. **Mode** – Choose **Ping Detect** or **Always On** for the system to execute for the WAN detection. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. ● **Always On** - The router assumes the WAN connection is always active. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Ping IP/Hostname** – Enter IP address in this field for pinging.

	• **TTL (Time to Live)** – Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
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.



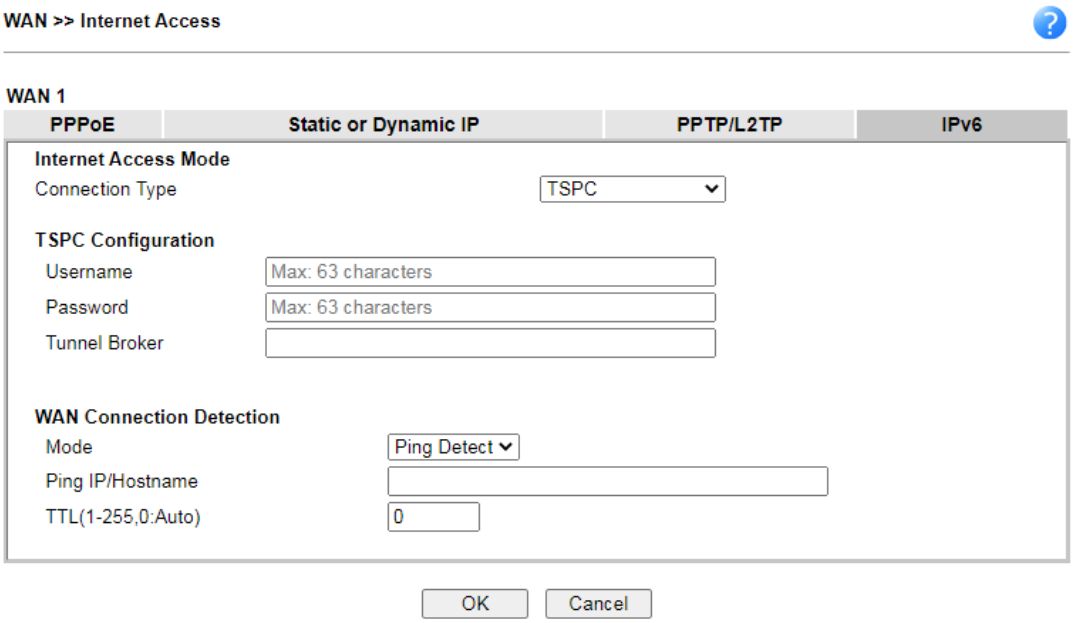
Info	At present, the IPv6 prefix can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

II-1-2-8 WAN1/WAN3 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.

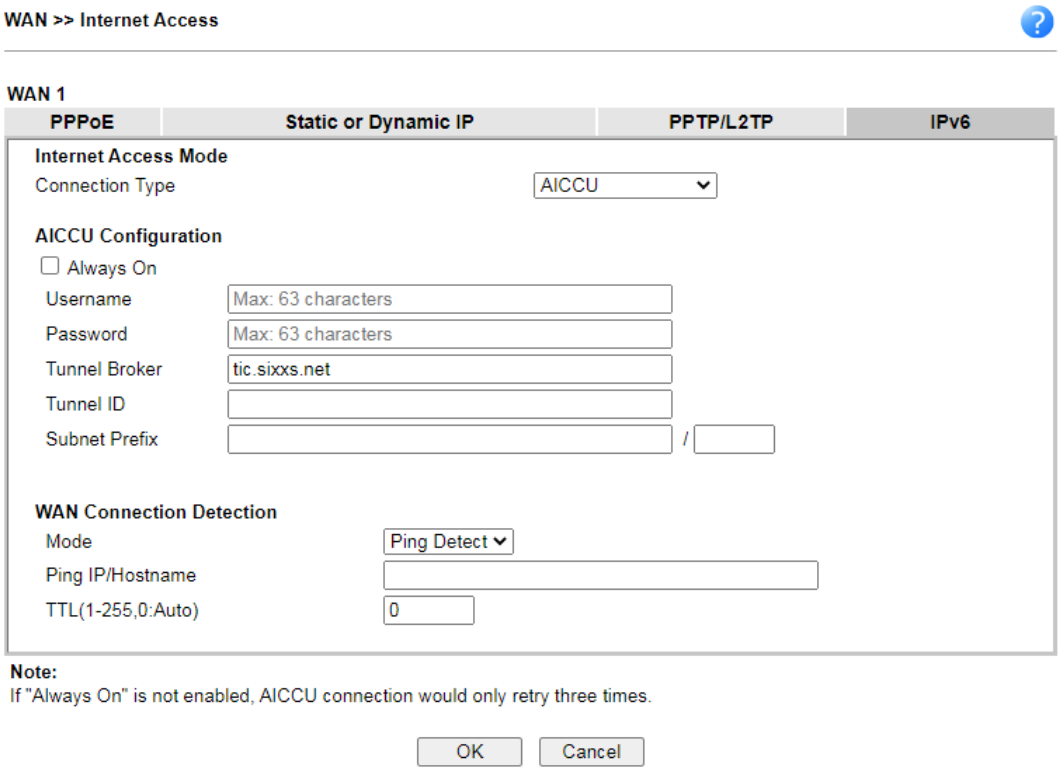


Available settings are explained as follows:

Item	Description
Username	It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account.
Password	Enter the password assigned with the user name.
Tunnel Broker	Enter the address for the tunnel broker IP, FQDN or an optional port number.
WAN Connection Detection	Configures how the WAN connection is monitored. **Mode** – Choose **Ping Detect** or **Always On** for the system to execute for the WAN detection. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. ● **Always On** - The router assumes the WAN connection is always active. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Ping IP/Hostname** – Enter IP address in this field for pinging. ● **TTL (Time to Live)** – Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.

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

II-1-2-9 WAN1/WAN3 Details Page for IPv6 – AICCU



Available settings are explained as follows:

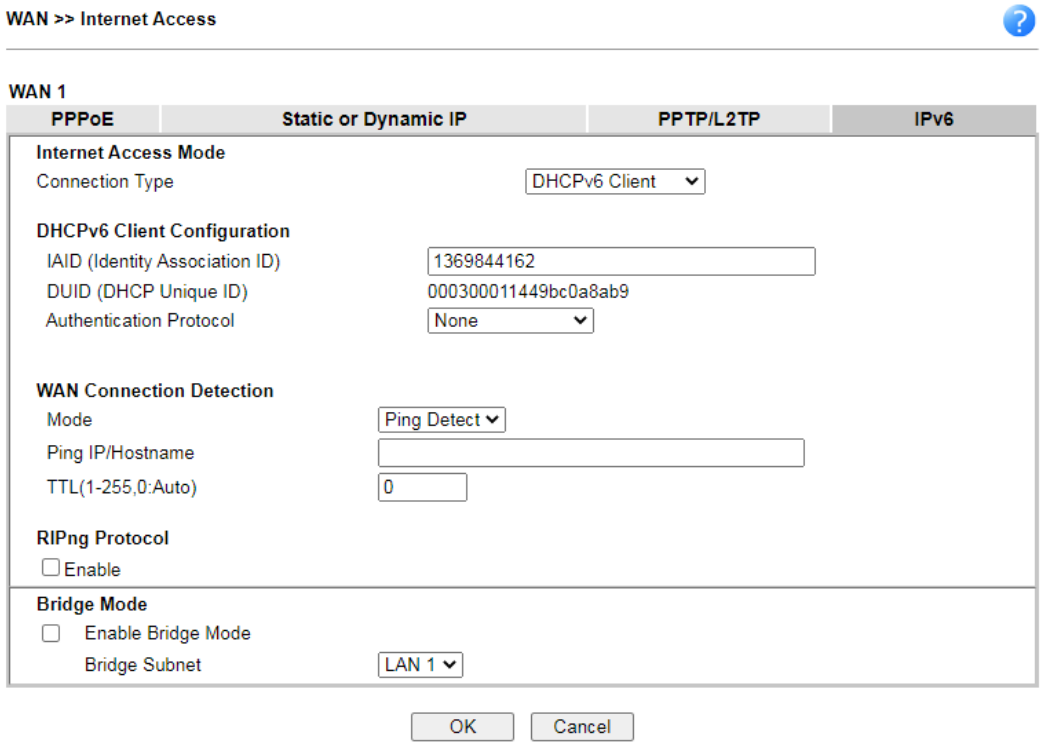
Item	Description
Always On	If selected, always attempt to reconnect if connection is lost. If unselected, reconnect up to 3 times if connection is lost.
Username	Login Username. Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password.
Password	Login Password. Enter the password.
Tunnel Broker	Address of the tunnel broker. 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	Configures how the WAN connection is monitored. **Mode** – Choose **Ping Detect** or **Always On** for the system to execute for the WAN detection.

	• **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. • **Always On** - The router assumes the WAN connection is always active. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. • **Ping IP/Hostname** – Enter an IP address in this field for pinging. • **TTL (Time to Live)** – Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.

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

II-1-2-10 WAN1 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:

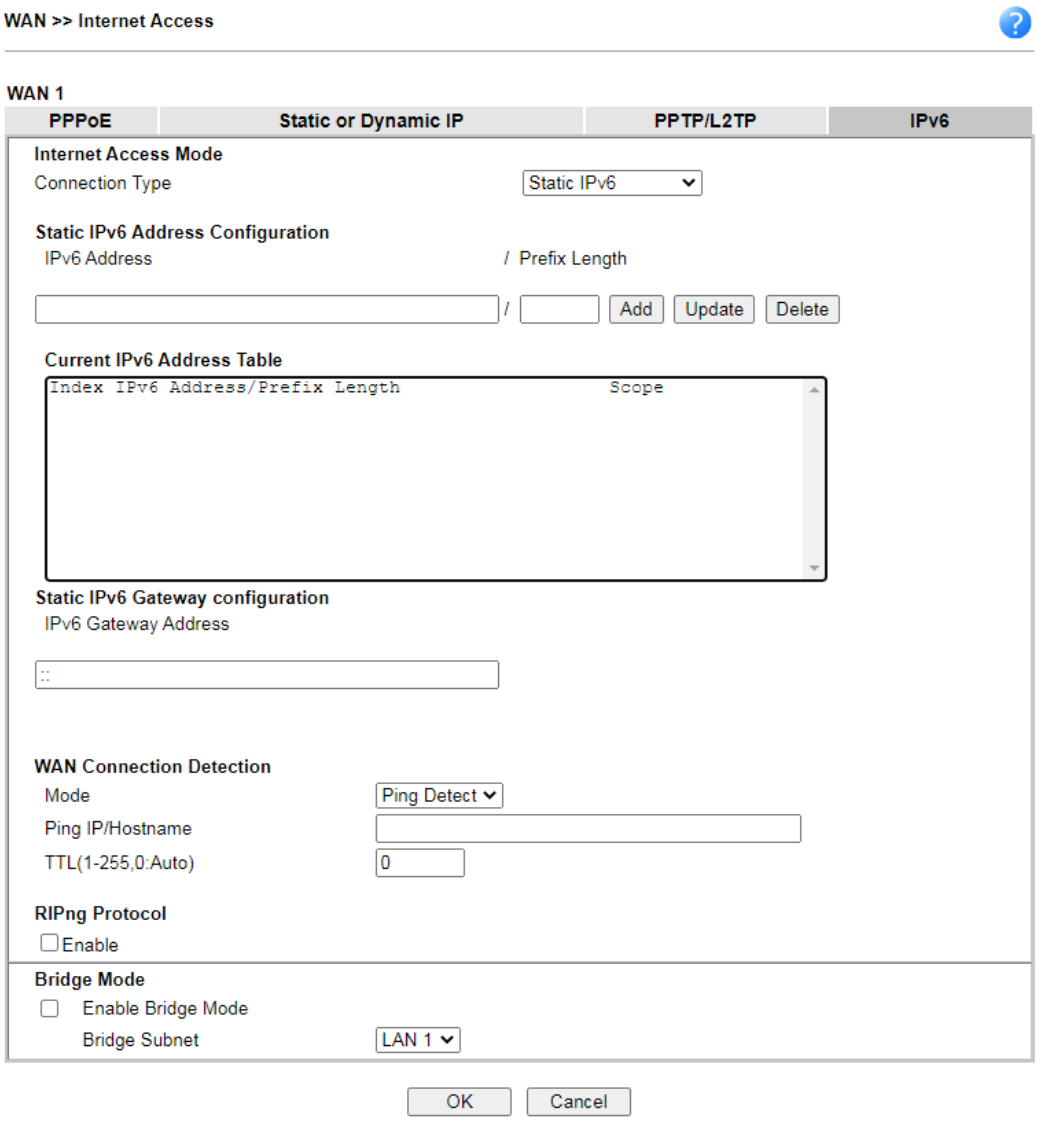
Item	Description
DHCPv6 Client Configuration	**IAID** - Unique integer that identifies this WAN interface. **DUID** – Display the DHCP unique ID used by this WAN interface. **Authentication Protocol** – This protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, **Reconfigure Key**, **Delayed** and **None**. In general,

	the default setting is None. • **Reconfigure Key** – During the connection process, DHCPv6 server will authenticate the client automatically. • **Delayed** - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields. - **Key ID** – Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value. - **Realm** – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value. - **Secret** – Type a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.
WAN Connection Detection	Configures how the WAN connection is monitored. **Mode** – Choose **Always On**, **Ping Detect** or **NS Detect** for the system to execute for WAN detection. • **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. • **Always On** - The router assumes the WAN connection is always active. • **NS Detect** - The router verifies connectivity by issuing Neighbor Solicitation packets. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. • **Ping IP/Hostname** – Enter an IP address in this field for pinging. • **TTL (Time to Live)** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	**Enable Bridge Mode** - If selected, the router will bridge the WAN connection to a LAN group. **Enable Firewall** – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated. **Bridge Subnet** – LAN subnet to be bridged.

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

II-1-2-11 WAN1 Details Page for IPv6 – Static IPv6

This page allows you to configure an ISP-assigned static IPv6 setup.



Available settings are explained as follows:

Item	Description
Static IPv6 Address Configuration	**IPv6 Address** – WAN IPv6 address assigned by the ISP. **Prefix Length** – Length of the IPv6 prefix. **Add** – Click this button to add the values in the IPv6 Address and Prefix Length fields to the IPv6 address table. **Update** - Click it to modify an existed entry. **Delete** – To remove an IPv6 address, select it by clicking on the entry in the Current IPv6 Address Table, then click the Delete button.
Current IPv6 Address Table	Display current interface IPv6 address.
Static IPv6 Gateway Configuration	**IPv6 Gateway Address -** IPv6 address of the ISP gateway.
WAN Connection	Configures how the WAN connection is monitored.

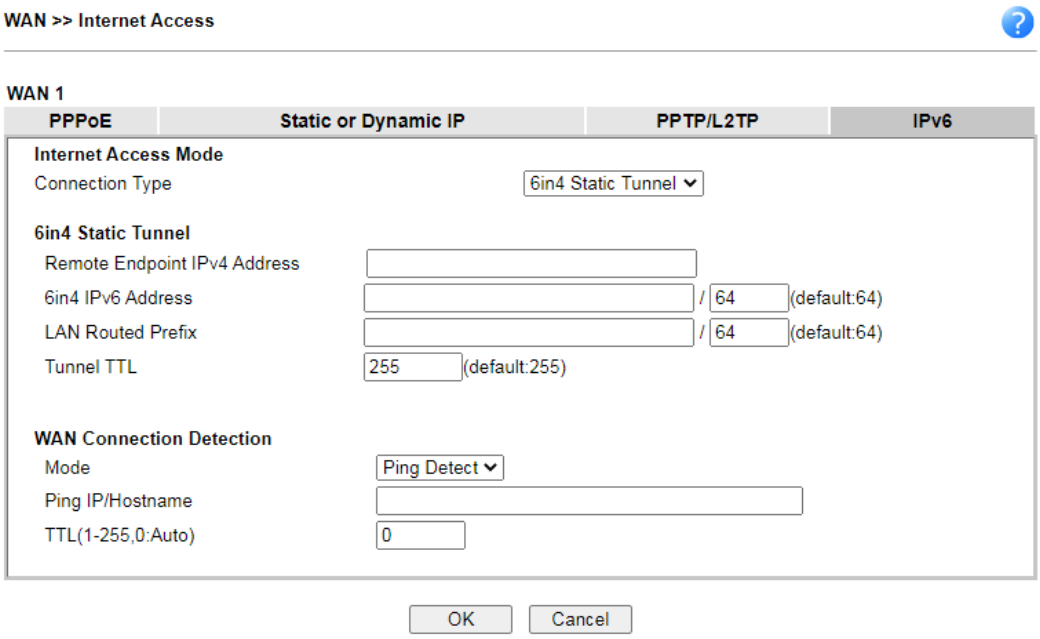
Detection	**Mode** – Choose **Always On**, **Ping Detect** or **NS Detect** for the system to execute for WAN detection. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. ● **Always On** - The router assumes the WAN connection is always active. ● **NS Detect** - The router verifies connectivity by issuing Neighbor Solicitation packets. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Ping IP/Hostname** – Enter an IP address in this field for pinging. ● **TTL (Time to Live)** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	**Enable Bridge Mode** - If selected, the router will bridge the WAN connection to a LAN group. **Enable Firewall** – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated. **Bridge Subnet** – LAN subnet to be bridged.

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

II-1-2-12 WAN1 Details Page for IPv6 – 6in4 Static Tunnel

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

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



Available settings are explained as follows:

Item	Description
6in4 Static Tunnel	**Remote Endpoint IPv4 Address -** WAN IPv6 address assigned by the tunnel provider. **6in4 IPv6 Address** - WAN IPv6 address and prefix length assigned by the tunnel provider. **LAN Routed Prefix** - LAN IPv6 address prefix and prefix length. **Tunnel TTL** - Time to live value, which is the maximum number of hops allowed to the endpoint.
WAN Connection Detection	Configures how the WAN connection is monitored. **Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. ● **Always On** - The router assumes the WAN connection is always active. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Ping IP/Hostname** – Enter an IP address in this field for pinging. ● **TTL (Time to Live)** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.

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)

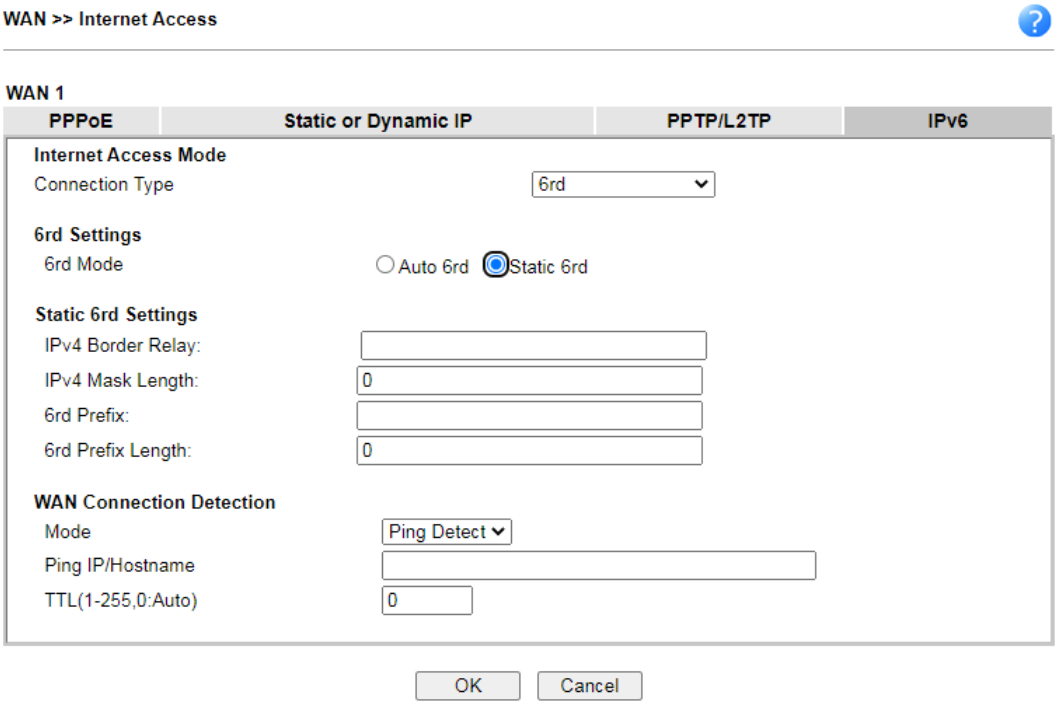
TX Packets	RX Packets	TX Bytes	RX Bytes
14	80	1244	6815

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-1-2-13 WAN1 Details Page for IPv6 – 6rd in

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



Available settings are explained as follows:

Item	Description
6rd Mode	**Auto 6rd** - Used in conjunction with DHCPv4, the router automatically provisions IPv6 using option 212. **Static 6rd** - IPv6 configuration information is manually entered.
IPv4 Border Relay	Enter the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Number of high-order bits that are identical in the IPv4 addresses within the 6rd domain. These bits are excluded when constructing the 6rd delegated prefix. 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	Configures how the WAN connection is monitored. **Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. ● **Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed. ● **Always On** - The router assumes the WAN connection is always active. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. ● **Ping IP/Hostname** – Enter an IP address in this field for pinging. ● **TTL (Time to Live)** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.

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

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

Online Status

Physical Connection **System Uptime: 0day 0:9:15**

IPv4	IPv6

LAN Status

IP Address

2001:E41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)
FE80::21D:AAFF:FE83:11B4/64 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1354	18040

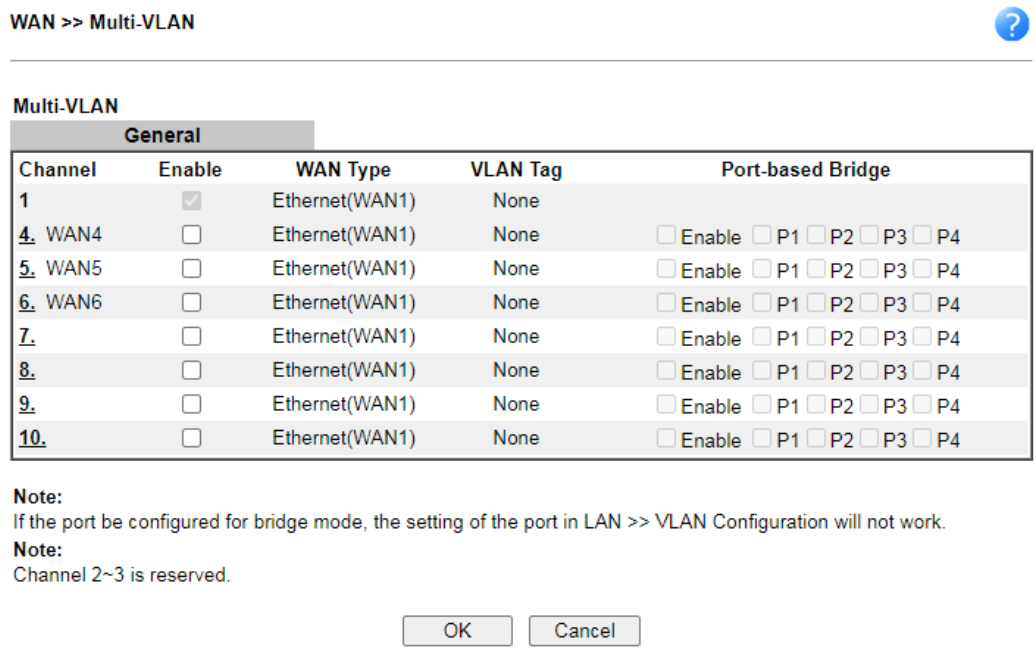
WAN1 IPv6 Status

Enable	Mode	Up Time	
Yes	6rd	0:09:06	
IP			**Gateway IP**
2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 (Global) FE80::C0A8:651D/128 (Link)			---
TX Packets	**RX Packets**	**TX Bytes**	**RX Bytes**
13	29	967	2620

II-1-3 Multi- VLAN

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

This page shows the basic configurations used by every channel.

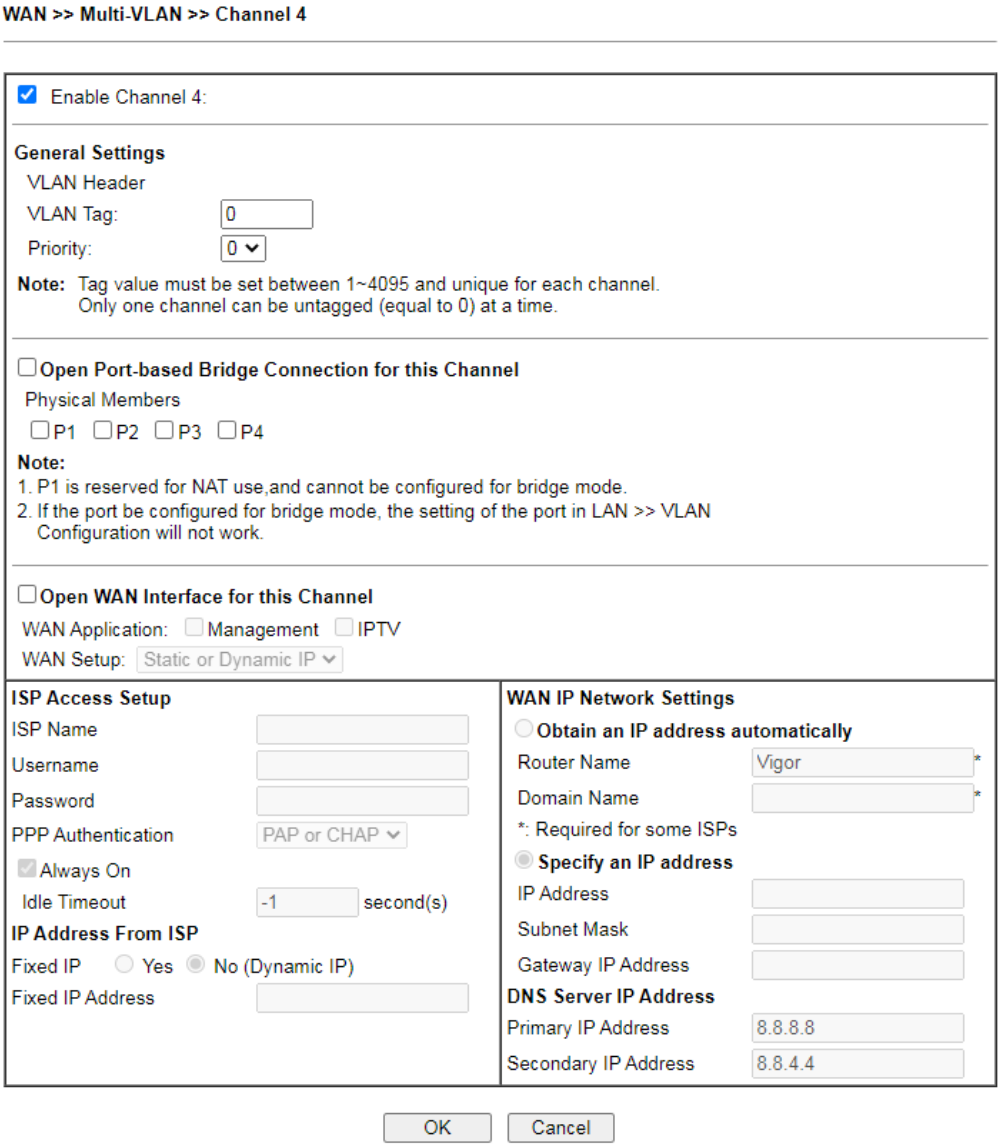


Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1 is used by the Internet Access web user interface and can not be configured here. Channels 4 ~ 10 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 ~ P4** – Check the box(es) to build bridge connection on LAN.

To configure a channel, click its channel number.

WAN links for Channel 4~6 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 4~6 to configure your router.



Available settings are explained as follows:

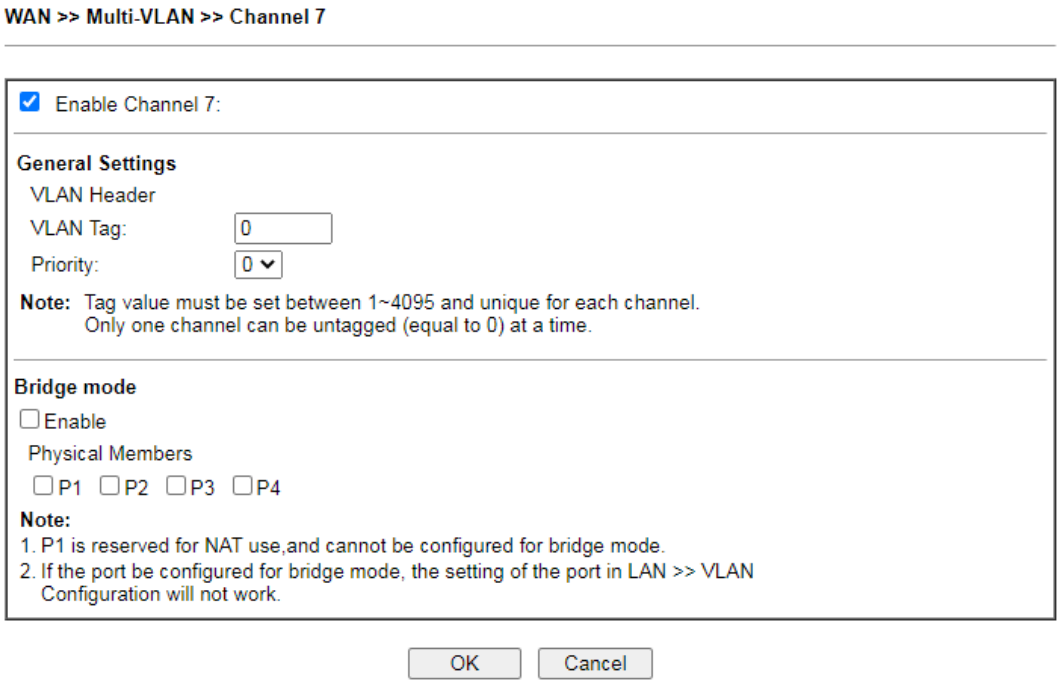
Item	Description
Enable Channel 4~6	**Enable** - Select to enable this channel. **Disable** - Select to disable this channel.
General Settings	**VLAN Tag** – Enter the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified 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 Connection for this Channel	If selected, bridge this channel to one or more LAN ports. **Physical Members** – If selected, a channel is bridged to this LAN port. **Note:** LAN port P1 is reserved for NAT use and cannot be selected for bridging.

Open WAN Interface for this Channel	If selected, NAT (Network Address Translation) will be applied to this channel to create a virtual WAN. The virtual WAN carries the same number as the channel itself. **WAN Application** – The intended usage of this channel. ● **Management** – The router can be managed using the web-based configuration, telnet and TR-069 via this channel. ● **IPTV** - IGMP packets can be sent to IPTV servers on this channel. **WAN Setup -** The WAN access method of this channel. Available options are PPPoE/PPPoA and Static or Dynamic IP. ● **PPPoE/PPPoA** - When PPPoE/PPPoA is selected, the ISP Access Setup and IP Address From ISP settings are available for configuration, and will be used to establish the WAN connection. ● **Static or Dynamic IP** - When Static or Dynamic IP is selected, the WAN IP Network Settings and DNS Server IP Address settings are available for configuration, and will be used to establish the WAN connection**.**
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 or MPoA	**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** – Enter the IP address. • **Subnet Mask** – Enter the subnet mask. • **Gateway IP Address** – Enter gateway IP address. **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 finished the above settings, click **OK** to save the settings and return to previous page.

Click any index (7~10) to get the following web page:



Available settings are explained as follows:

Item	Description
Enable Channel 7~10	**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.
Bridge mode	If selected, bridge this channel to one or more LAN ports. **Physical Members**– If selected, a channel is bridged to this LAN port. **Note:** LAN port P1 is reserved for NAT use and cannot be selected for bridging.

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

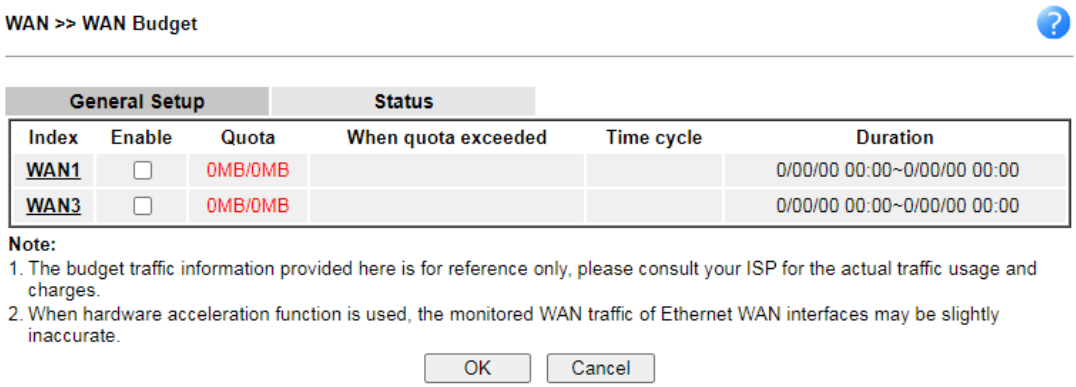
II-1-4 WAN Budget

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:

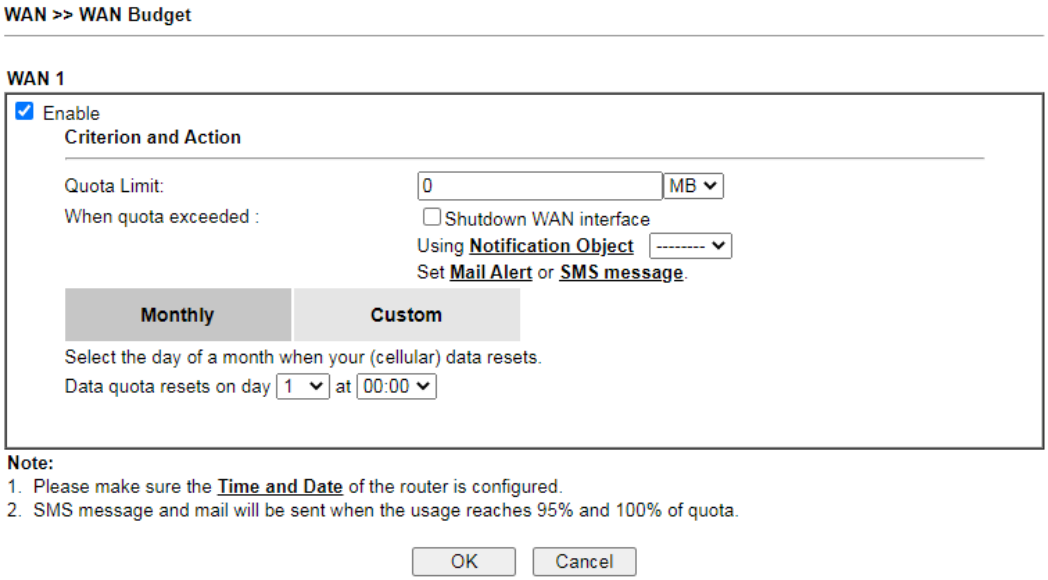
- set up calendar cycles to monitor;
- limit your Internet usage according to your ISP's quota;
- set up action(s) to take when the quota is exceeded.

II-1-4-1 General Setup

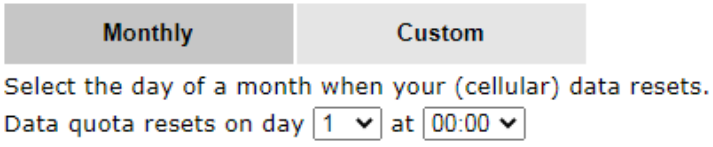


Item	Description
Index	The WAN port. Click to configure WAN Budget for a particular WAN.
Enable	**v -** WAN Budget is enabled on this WAN. **x -** WAN Budget is disabled on this WAN.
Quota	The current cycle's Internet usage is expressed as *x/y* where *x* is the cumulative usage and *y* is the upper 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 WAN# link to open the following web page.

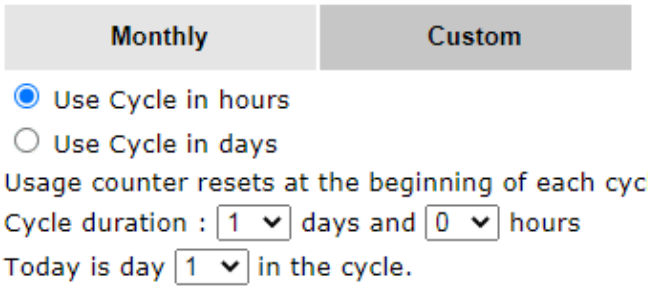


Available settings are explained as follows:

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.  **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

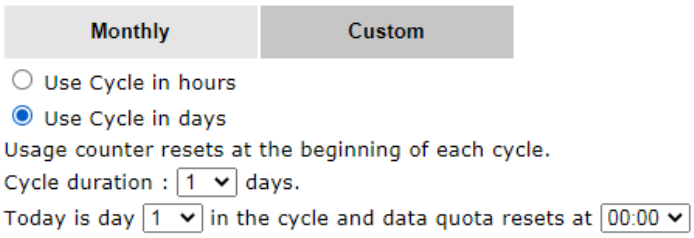
duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.

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 -

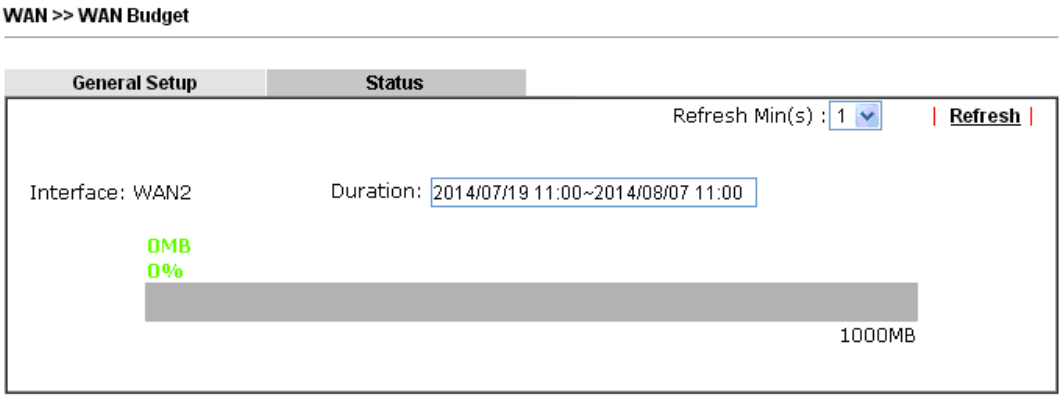


- **Cycle duration**: Specify the days to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically.
- **Today is day** – Specify the day and time for data quota rest in the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

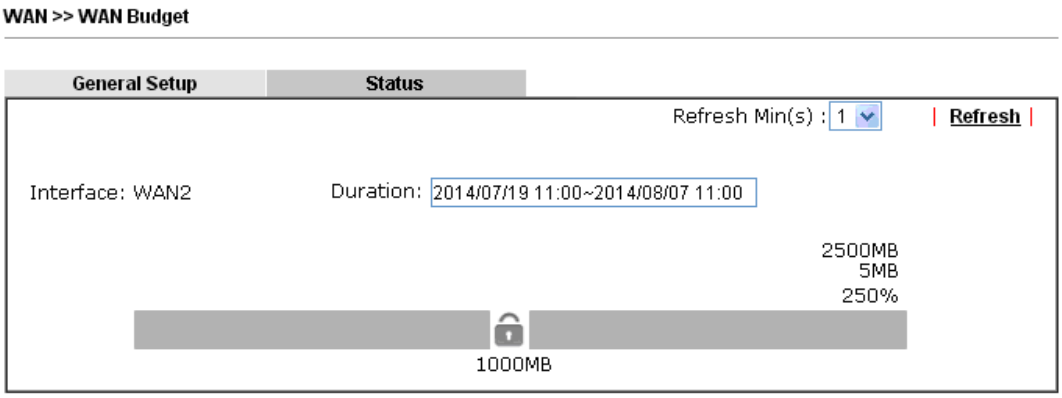
After finished the above settings, click **OK** to save the settings.

II-1-4-2 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.



II-2 LAN

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

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

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

IP Address

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

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

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

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

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

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

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

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

Alternatively, static IP addresses can be manually configured on LAN clients as part of their network settings. No matter how IP addresses are configured, it is important that no two devices get the same IP address. If both DHCP and static assignment are used on a network, it is important to exclude the static IP addresses from the DHCP IP pool. For example, if your LAN uses the 192.168.1.x subnet and you have 20 DHCP clients and 20 static IP clients, you could configure 192.168.1.10 as the Start IP Address, 50 as the IP Pool Counts (enough for the current number of DHCP clients, plus room for future expansion), and use addresses greater than 192.168.1.100 for static assignment.

Web User Interface

To begin configuring the LAN settings, select LAN>>General Settings from the menu bar of the Web UI.

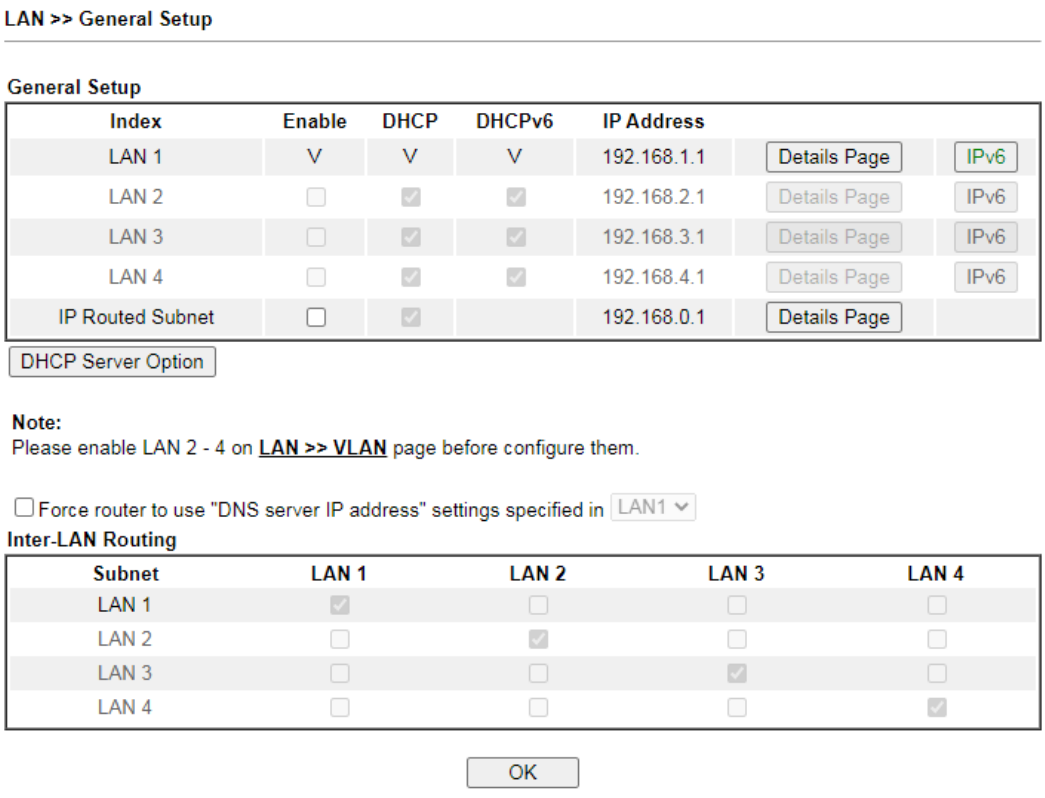
II-2-1 General Setup

This page provides you the general settings for LAN.

There are eight subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN4). 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.

LAN 1 is always enabled and is used as the default subnet. LANs 2 to 4 are subnets to be used in conjunction with Virtual LANs (VLANs). Each VLAN can be configured to allow or disallow communication with other VLANs using the Inter-LAN Routing matrix.

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



Available settings are explained as follows:

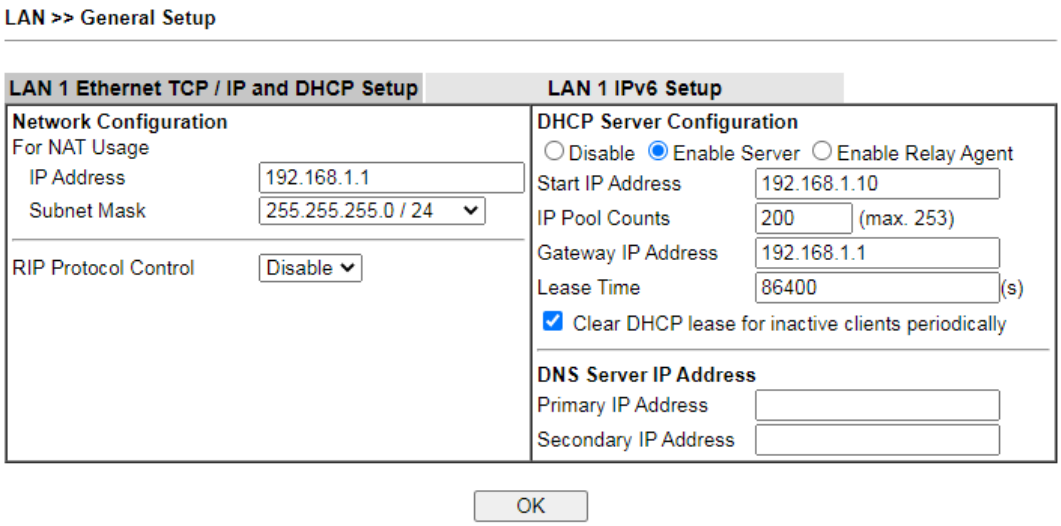
Item	Description
General Setup	Allow to configure settings for each subnet respectively. **Index -** Display all of the LAN items. **Enable-** Basically, LAN1 status is enabled in default. LAN2 –LAN4 and IP Routed Subnet can be observed by checking the box of **Status**. **DHCP/DHCPv6-** LAN1 is configured with DHCP/DHCPv6 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/LAN3/LAN4 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP 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.

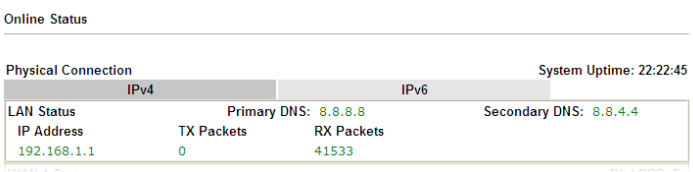
II-2-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

This page has two tabs, LAN Ethernet TCP/IP and DHCP Setup, which sets up the IPv4 LAN environment, and LAN IPv6 Setup, which sets up the IPv6 environment.



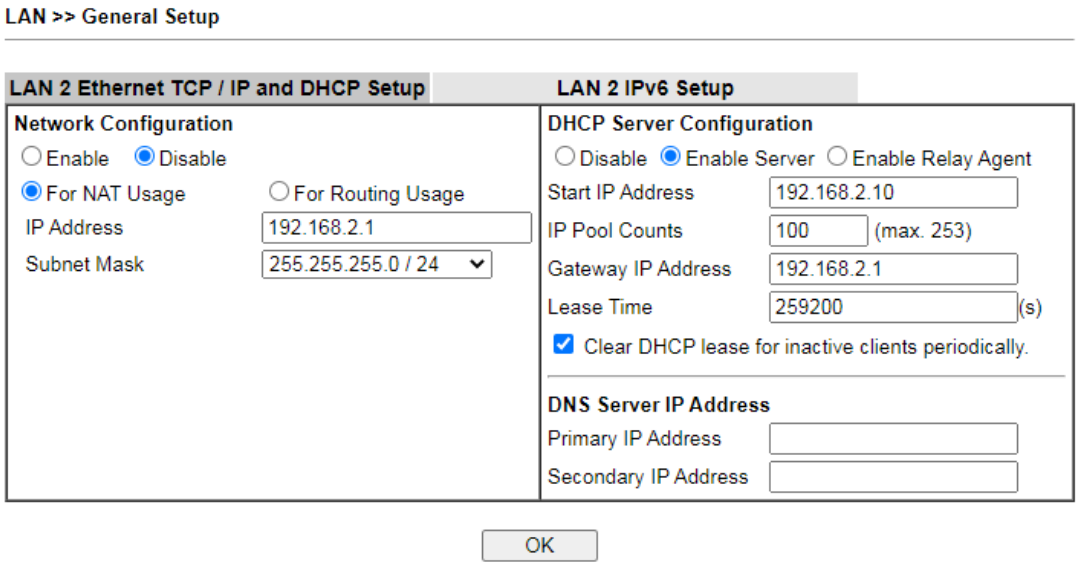
Available settings are explained as follows:

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 -** 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** – Disables the built-in DHCP server on the router. **Enable Server** - Enables the built-in DHCP server on the router. ● **Start IP Address -** The beginning LAN IP address that is given out to LAN DHCP clients. ● **IP Pool Counts -** The maximum number of IP addresses to be handed out by DHCP. The default value is 200. Valid range is between 1 and 1021. The actual number of IP addresses available for assignment is the IP Pool Counts, or 1021 minus the last octet of the Start IP Address, whichever is smaller. ● **Gateway IP Address -** The IP address of the gateway, which is the host on the LAN that relays all traffic

	coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **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 –** IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded.
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. When these fields are populated, they will be used as the IP addresses of the DNS server information in DHCPv6 responses, overriding the ISP-supplied DNS server addresses. **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 DNS servers obtained from WAN interface to local users as a DNS proxy server and maintain a DNS cache. If there is no DNS servers available, router will use its own IP address instead. 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.

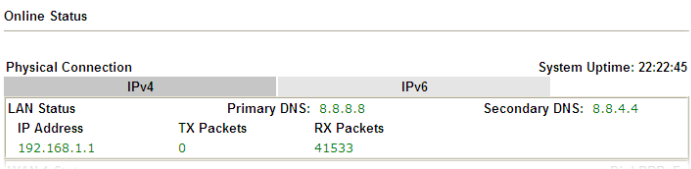
When you finish the configuration, please click **OK** to save and exit this page.

II-2-1-2 Details Page for LAN2 ~ LAN4



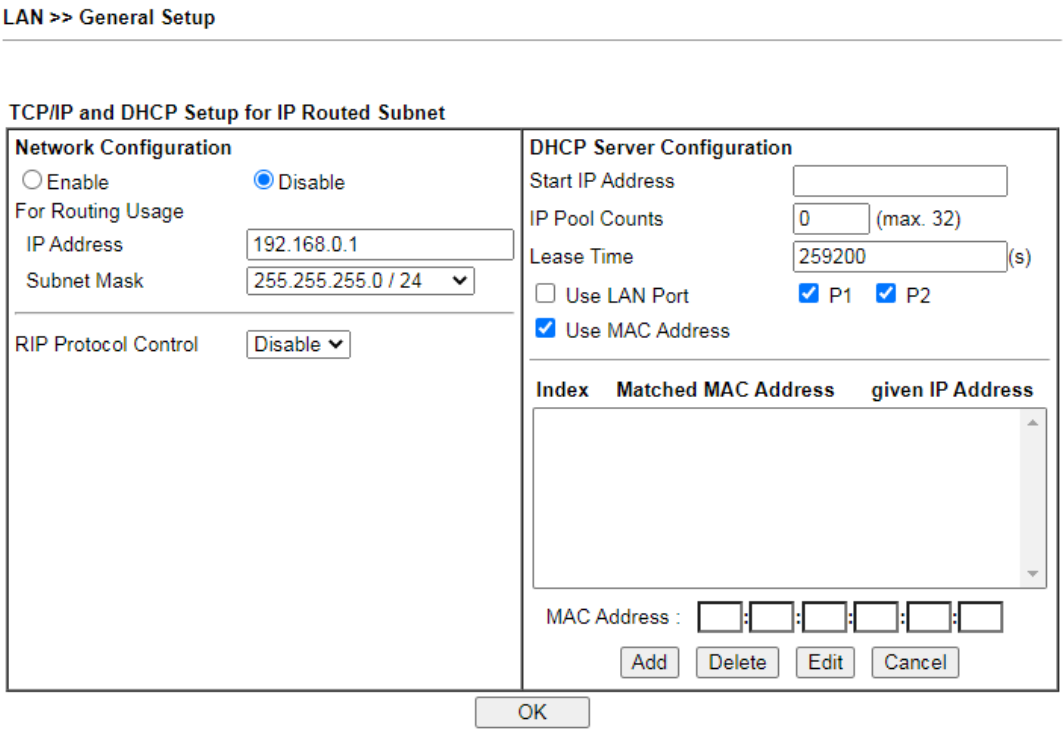
Available settings are explained as follows:

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	**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 100. Valid range is between 1 and 1021. The actual number of IP addresses available for assignment is the IP Pool Counts, or 1021 minus the last octet of the Start IP Address, whichever is smaller. ● **Gateway IP Address -** The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **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-2-1-3 Details Page for IP Routed Subnet



Available settings are explained as follows:

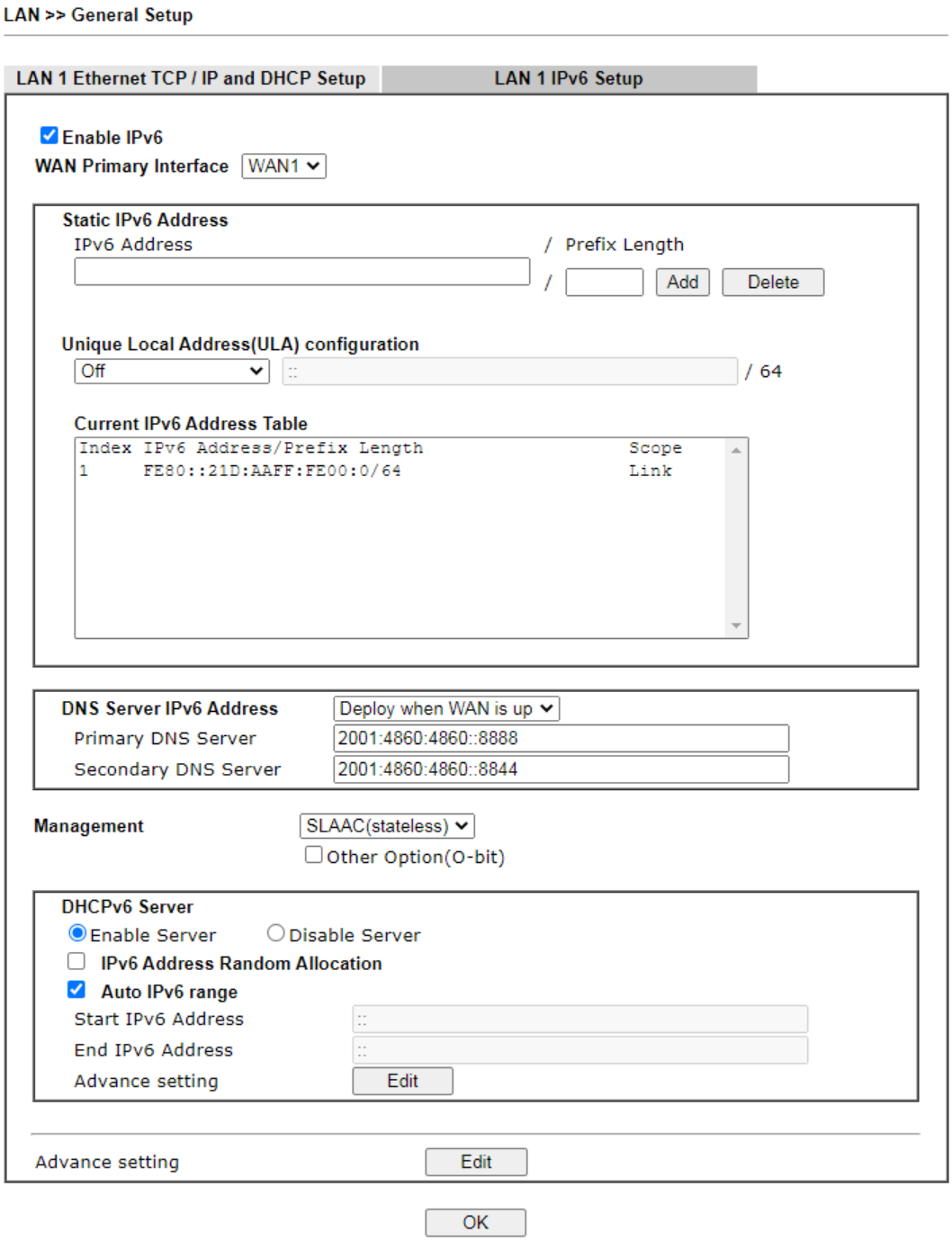
Item	Description
Network Configuration	**Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration. **For Routing Usage,** **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together 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. **Start IP Address -** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. **IP Pool Counts -** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. **Lease Time** - Enter the time to determine how long the IP

	address assigned by DHCP server can be used. **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-2-1-4 Details Page for LAN IPv6 Setup

There are two configuration pages for LAN1/LAN2/LAN3/LAN4 Port, 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. Below shows the settings page for IPv6.

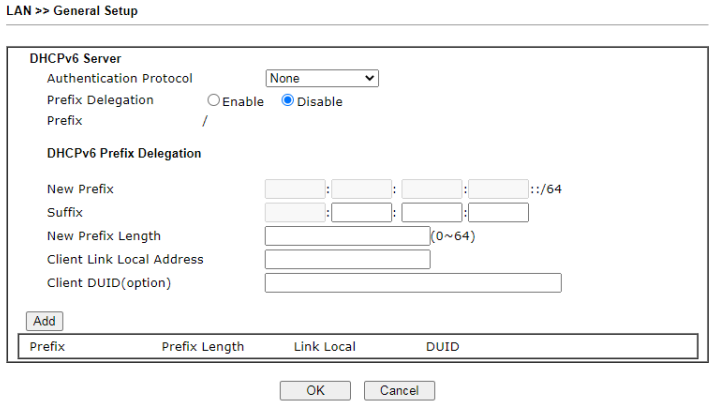
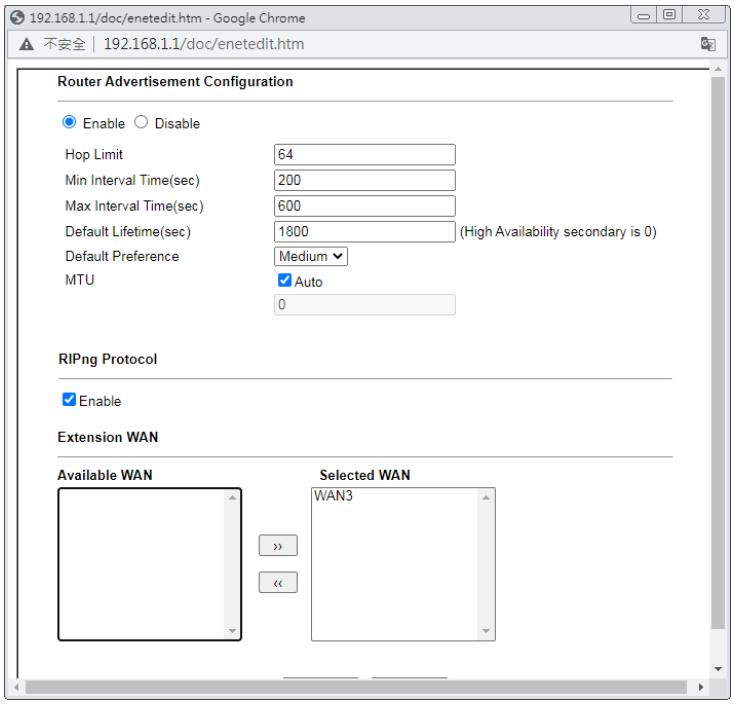


It provides 2 daemons for LAN side IPv6 address configuration. One is **SLAAC**(stateless) and the other is **DHCPv6** (Stateful) server.

Available settings are explained as follows:

Item	Description
Enable IPv6	Enables or disables IPv6 on the LAN.

WAN Primary Interface	Select the WAN to be used for IPv6 traffic.
Static IPv6 Address	Enter IPv6 Address and Prefix length to be added, or click an existing IPv6 address to be deleted in the Current IPv6 Address Table below and the values will be automatically copied over. **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.

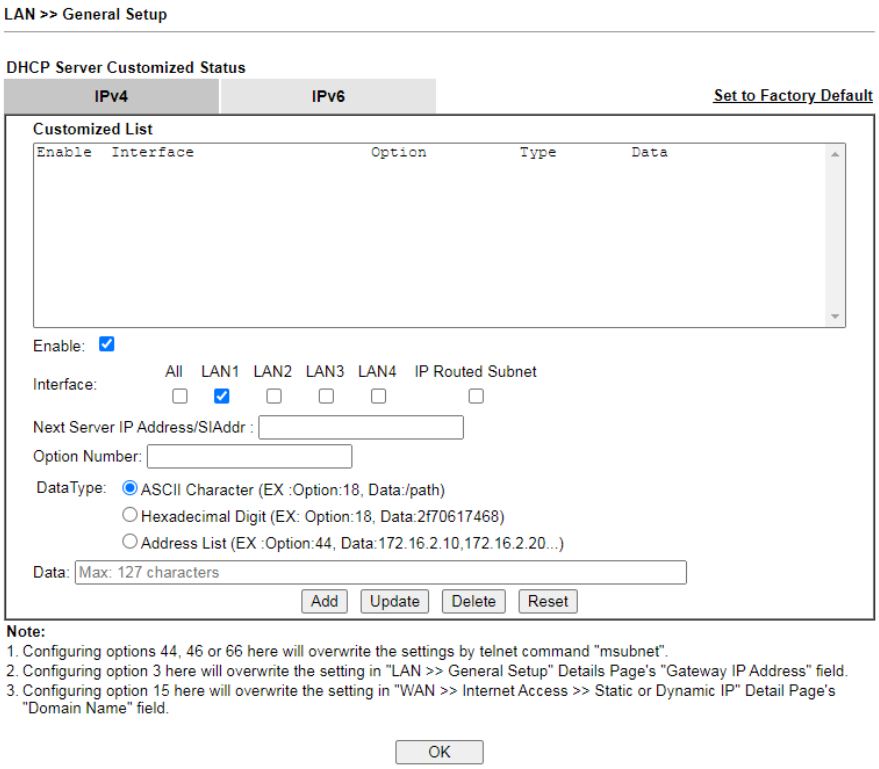
	IPv6 Address Random Allocation - Check it to assign the DHCPv6 IP address randomly to prevent the attacks from the IPv6 reconnaissance techniques. **Auto IPv6 range** – When selected, the router's built-in DHCPv6 server decides the LAN IPv6 address range to be used. When deselected, LAN IPv6 addresses given out will be within the range as specified in the **Start IPv6 Address** and **End IPv6 Address**. ● **Start IPv6 Address** / **End IPv6 Address** –Enter the start and end address for IPv6 server. **Advance setting** – Click the **Edit** button to bring up the IPv6 Advanced Settings page. 
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. Default value of hop limit field in Route Advertisement messages. **Min/Max Interval Time (sec)** – Minimum/ Maximum time, in seconds, between unsolicited multicast route advertisement messages sent by the RA server. **Default Lifetime (sec)** – Time, in seconds, that the router is to be used as the default router. **Default Preference** – Default preference value (Low, Medium, High) of the router sent in route advertisement messages. **MTU** – It means Max Transmit Unit for packet. If **Auto** is selected, the router determines the MTU value to send in route advertisement messages. **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-2-1-5 DHCP Server Options

DHCP Options can be configured by clicking the **DHCP Server Option** 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-2-2 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

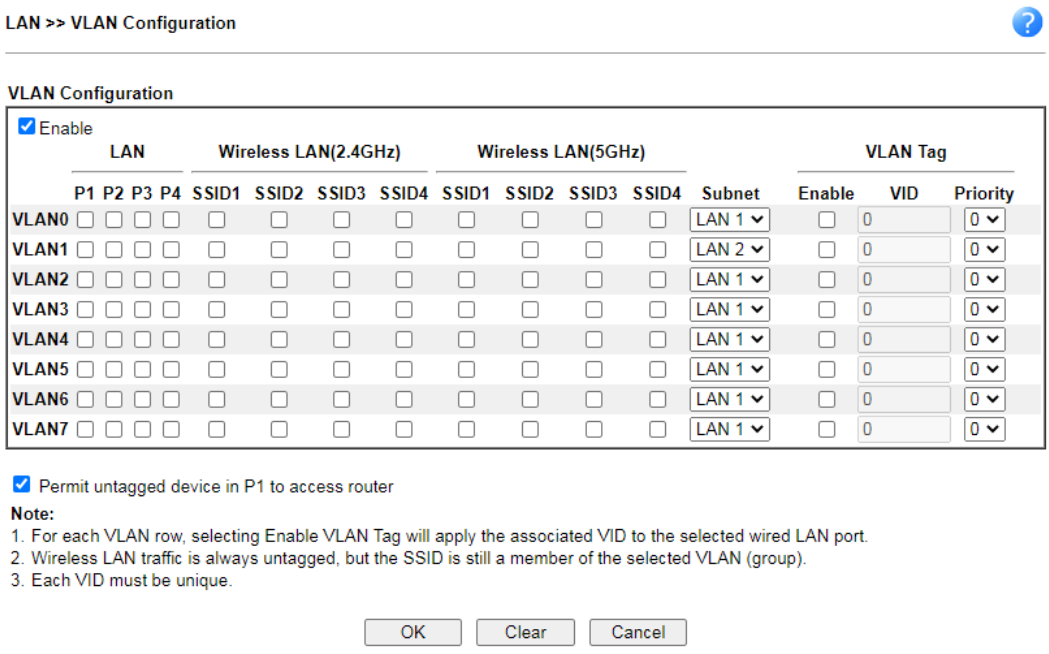
The tagged VLANs (802.1q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each 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 ~ P4) 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 Vigor2135ac:



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

Available settings are explained as follows:

Item	Description
Enable	Enables or disables VLAN functionality.
VLAN0 to VLAN7	Virtual LANs.

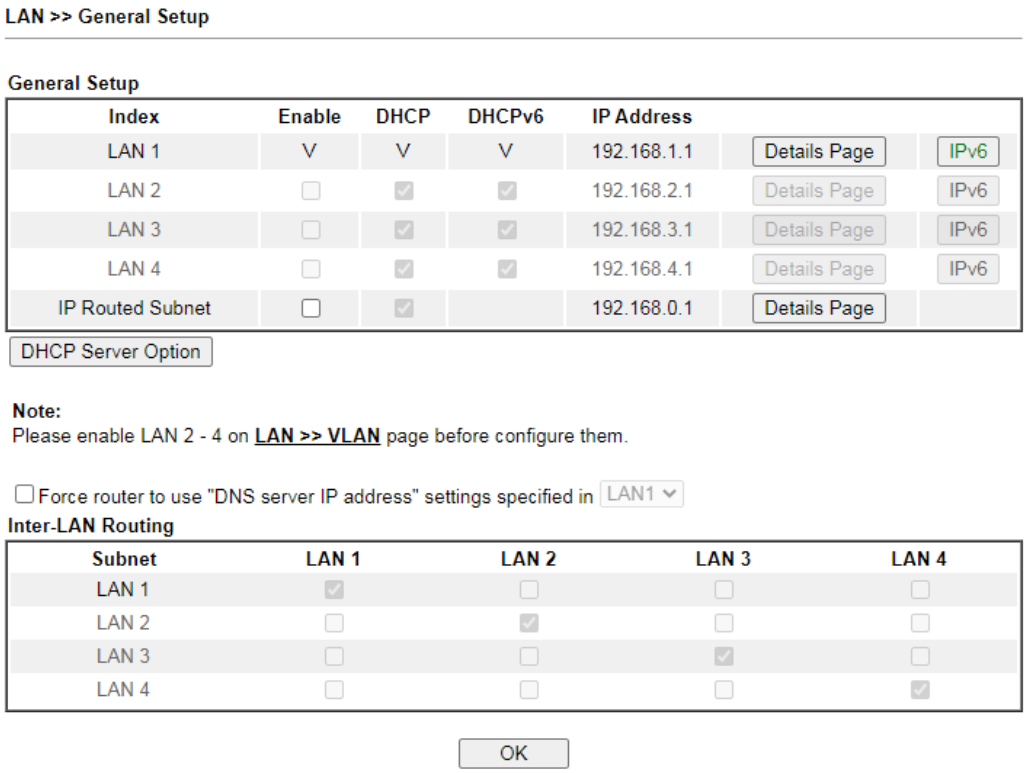
LAN	**P1 – P5** – Physical Ethernet ports on the router. Select the LAN port(s) to group them under the selected VLAN.
Wireless LAN (2.4GHz)	**SSID1 – SSID4 –** Select the SSID boxes to group them under the selected VLAN.
Wireless LAN (5GHz)	**SSID1 – SSID4 –** Select the SSID boxes to group them under the selected VLAN.
Subnet	Select a LAN subnet from LAN 1 to LAN 4 to make the selected VLAN mapping to the specified subnet only.
VLAN Tag	**Enable** – Select to enable 802.1Q tagging on this VLAN. 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** – VLAN Identifier. Valid values are 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.
Permit untagged device in P1 to access router	Select to allow untagged hosts connected to LAN port P1 to access the router. In case you have incorrectly configured VLAN functionality, you will still be able to access the router via the Web UI, and telnet and SSH shells to adjust the configuration.

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

Inter-LAN Routing

The Vigor router supports up to 7 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).

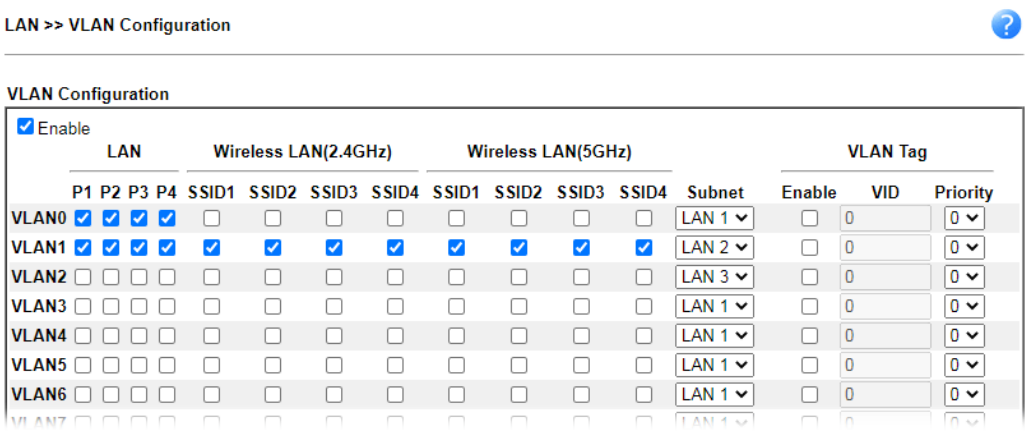


Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

Vigor2135 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.

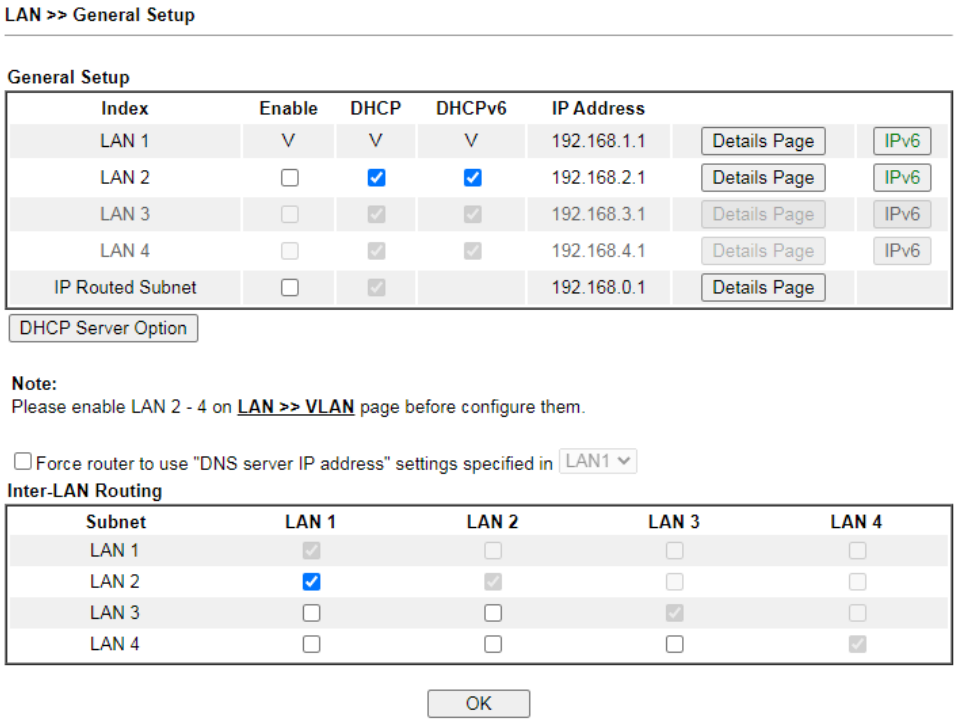
Configuring port-based VLAN for wireless and non-wireless clients

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 Configuration**. 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.**



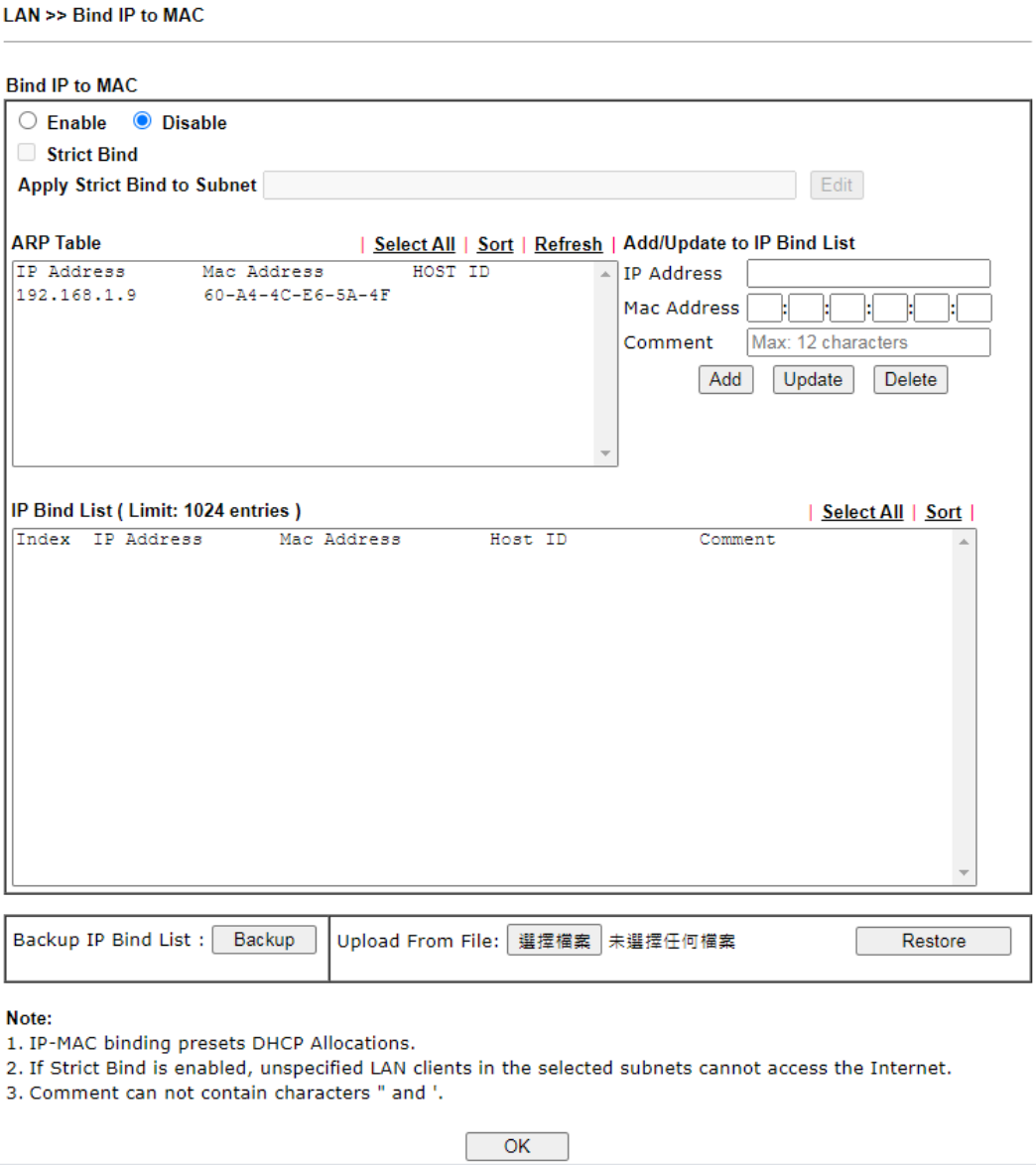
Vigor router supports up to six private IP subnets on LAN. Each can be independent (isolated) or common (able to communicate with each other). This is ideal for departmental or multi-occupancy applications.

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

II-2-3 Bind IP to MAC

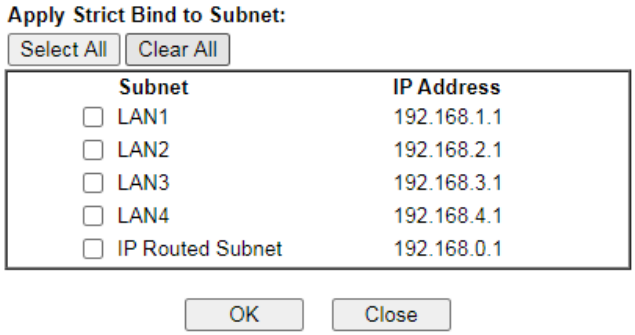
This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

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



Available settings are explained as follows:

Item	Description
Enable	MAC addresses that have an IP address assigned on this page will receive that IP address through DHCP.
Disable	MAC address-to-IP address bindings configured on this page are ignored by the DHCP server when assigning IP addresses through DHCP.
Strict Bind	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** – Select 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	Sort the entries in the ARP Table by IP address.
Refresh	Refresh the screen to reflect the current state of the ARP table.
Add or 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** – Optional comment field to identify this IP Address – MAC Address pair.
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.

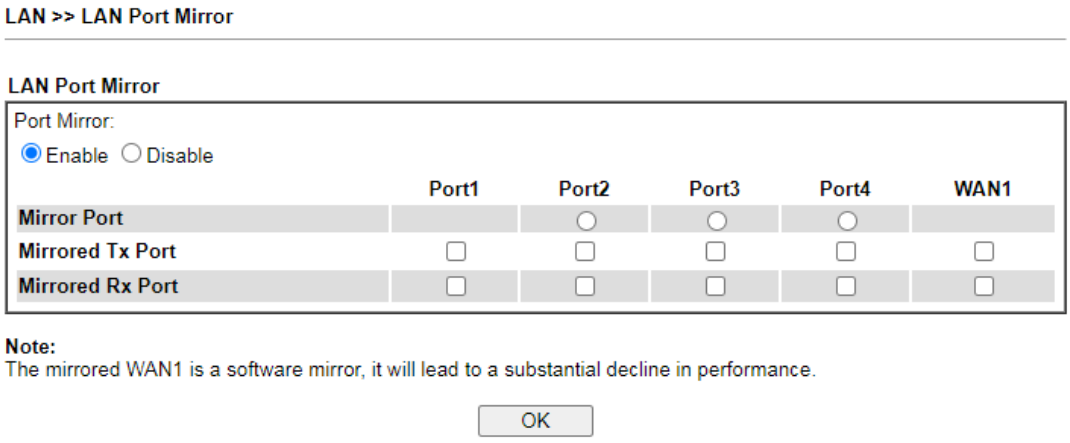
Info	Before you select Strict Bind, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web user interface of the router might not be accessed.

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

II-2-4 LAN Port Mirror

The **LAN Port Mirror** function allows network traffic of select LAN ports to be forwarded to another LAN port for analysis. This is useful for enforcing policies, detecting unauthorized access, monitoring network performance, etc.

Select **LAN>>LAN Port Mirror** from the menu bar of the Web UI to bring up the **LAN Port Mirror** configuration page.



Available settings are explained as follows:

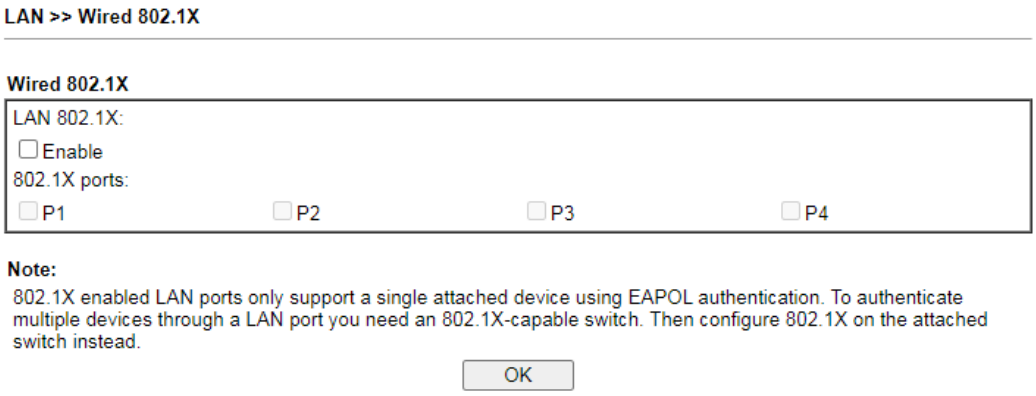
Item	Description
Port Mirror	Enables or disables LAN Port Mirroring.
Mirror Port	One and only one port is selected as the mirror port, to which traffic is to be forwarded.
Mirrored Tx Port	Port(s) whose outbound traffic will be forwarded to the mirror port.
Mirrored Rx Port	Port(s) whose inbound traffic will be forwarded to the mirror port.

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

II-2-5 Wired 802.1x

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

Select **LAN>>Wired 802.1X** from the menu bar of the Web UI to bring up the **Wired 802.1X** configuration page.



Available settings are explained as follows:

Item	Description
Enable	Check the box to enable LAN 802.1x function.
802.1X ports	802.1X authentication will be available for the selected LAN ports.

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

II-3 NAT

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

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

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

The benefit of the NAT includes:

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

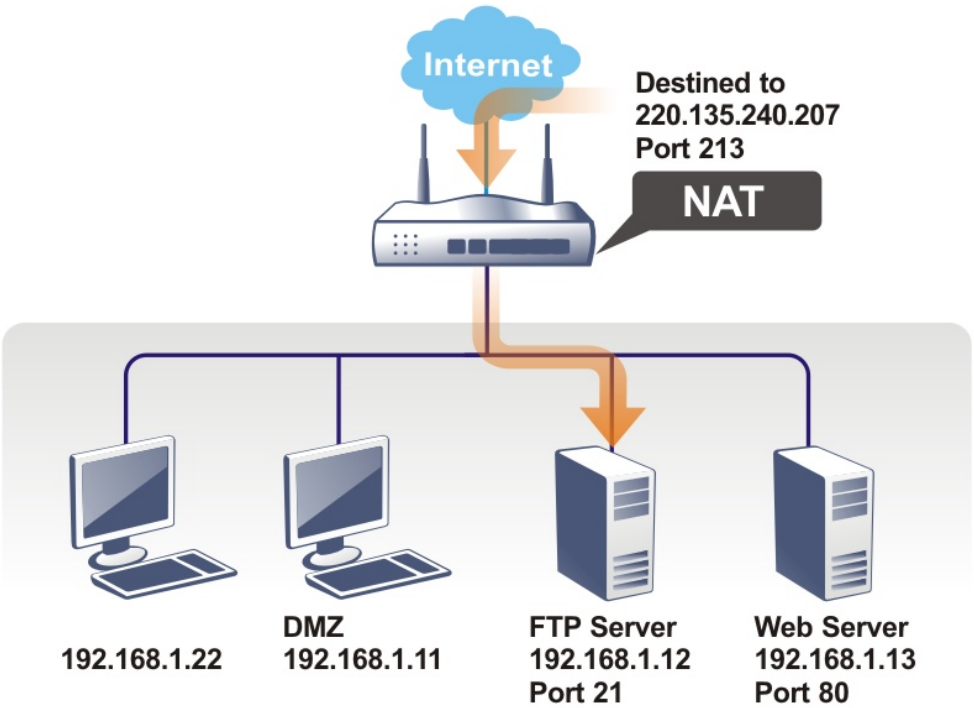
Info	On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved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

Web User Interface

II-3-1 Port Redirection

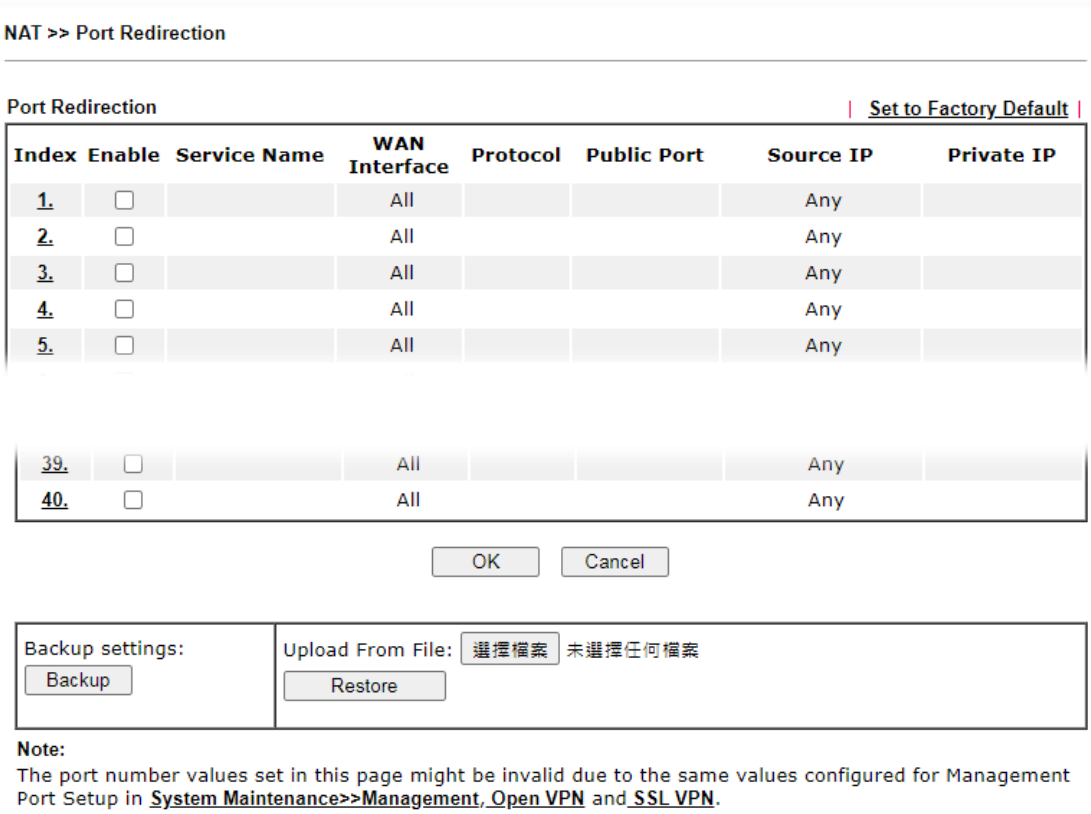
Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers, etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually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

That is, it allows a range of ports to be mapped to a port across a range of local IP addresses. For example, ports 80 through 89 (a total of 10 ports) can be mapped to port 80 LAN clients 192.168.1.20 through 192.168.1.29 (a total of 10 IP addresses). Henceforth all WAN-to-LAN traffic from ports 80 to 89 will be sent to the respective LAN clients.



The port redirection can only apply to incoming traffic.

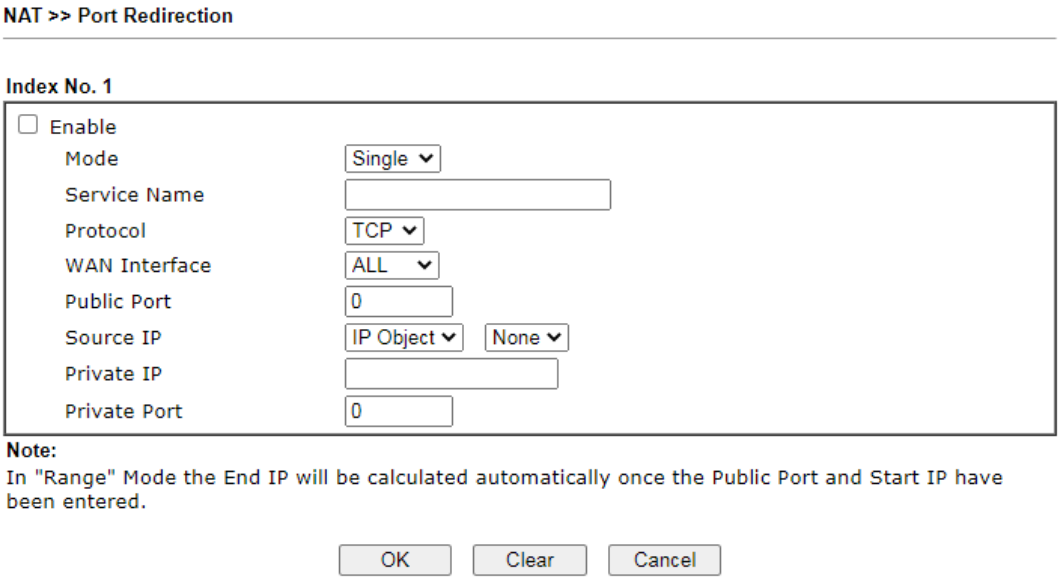
To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 40 port-mapping entries for the internal hosts.



Each item is explained as follows:

Item	Description
Index	Click to view and edit details of the rule.
Enable	Select to enable the port redirection rule.
Service Name	User-entered name that identifies the rule.
WAN Interface	WAN interface(s) to which this rule applies. A particular WAN interface or ALL interfaces.
Protocol	The protocol to which this rule applies, TCP or UDP.
Public Port	The port or range of WAN ports that is redirected by this rule.
Source IP	The IP object of the source IP.
Private IP	The LAN IP address(es) to which the traffic is redirected.
Backup	Click it to backup the configuration of port redirection settings.
Restore	Click it to restore the configuration of port redirection settings. Before clicking, make sure upload the configuration file onto Vigor router.

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



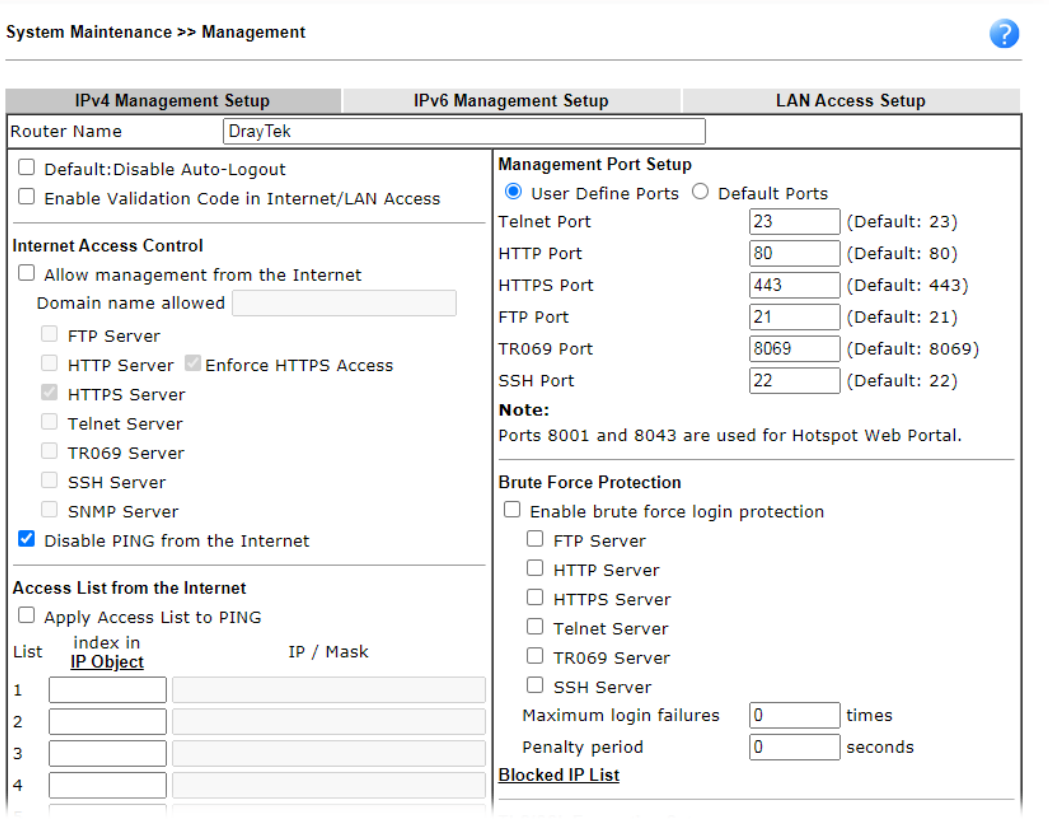
Available settings are explained as follows:

Item	Description
Enable	Select to enable the port redirection setting.
Mode	Allows a single port or a range of ports to be redirected. **Single -** redirects one single port. **Range -** redirects a contiguous range of ports.
Service Name	Enter the description of the specific network service.
Protocol	The protocol to which this rule applies, TCP or UDP.
WAN Interface	WAN interface(s) to which this rule applies. **WAN #** - Traffic from the selected WAN interface will be redirected. **ALL** - Traffic from all WAN interfaces will be redirected.
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	**IP Object** - Use the drop down list to specify an IP object profile. **IP Group** - Use the drop down list to specify an IP group profile.
Private IP	The LAN IP address or range of IP addresses to which the traffic is redirected. In the case of a range, only the beginning IP address needs to be entered. The ending IP address will automatically be derived from the number of public ports.
Private Port	The port on each LAN client to which the traffic will be directed to.

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

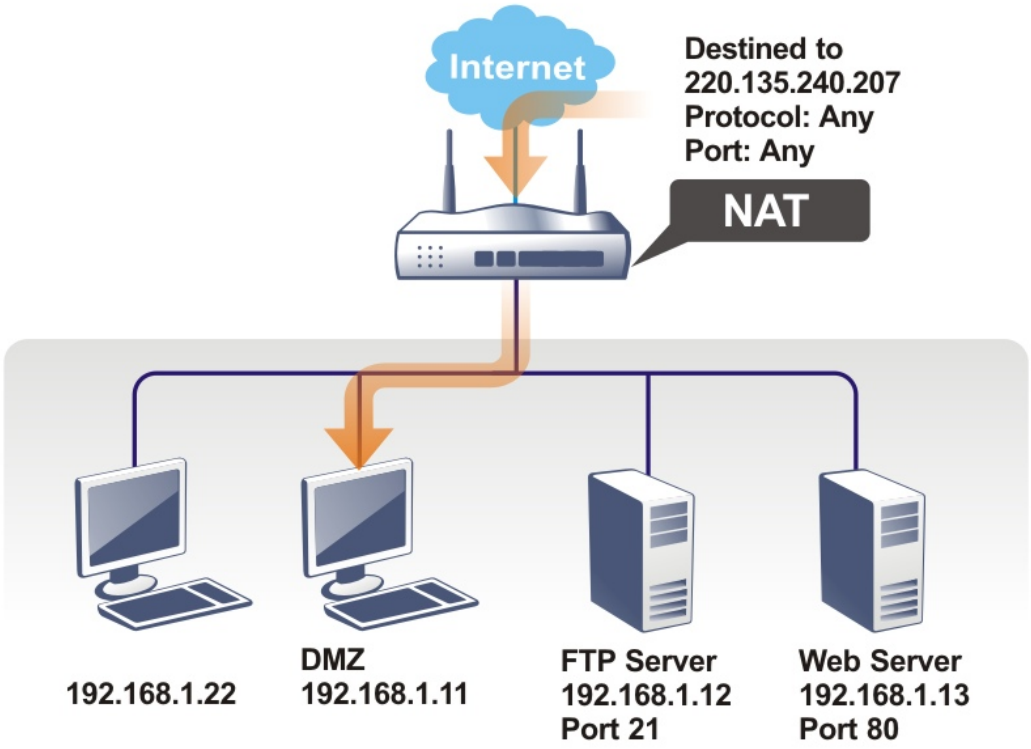
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

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.



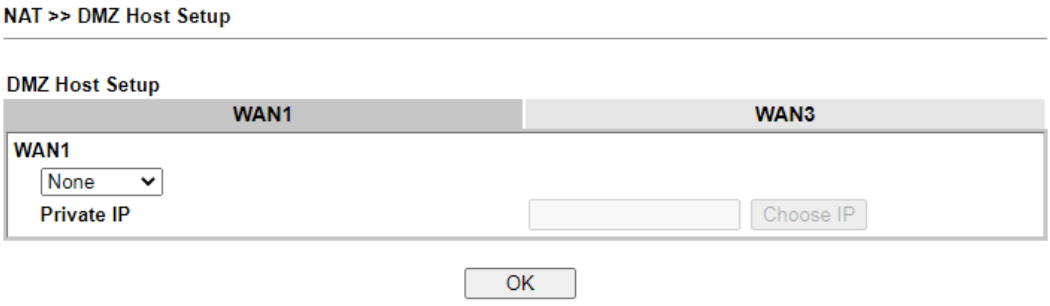
II-3-2 DMZ Host

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.

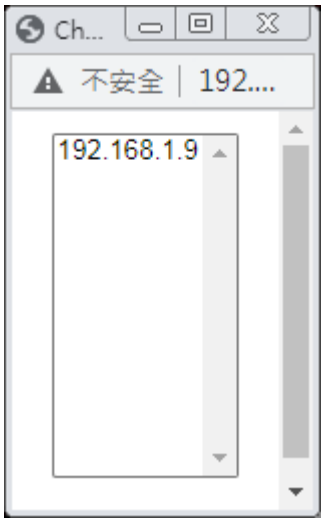
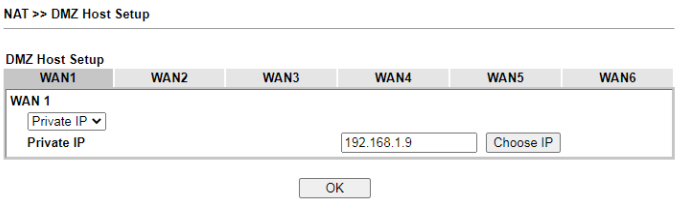


The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

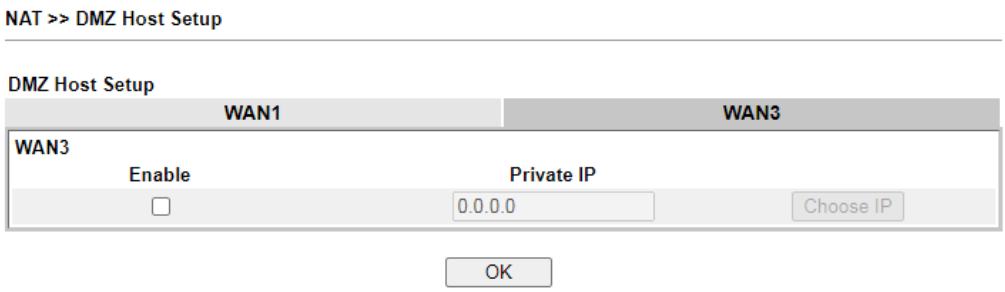
Click **DMZ Host** to open the following page. You can set different DMZ host for each WAN interface. Click the WAN tab to switch into the configuration page for that WAN.



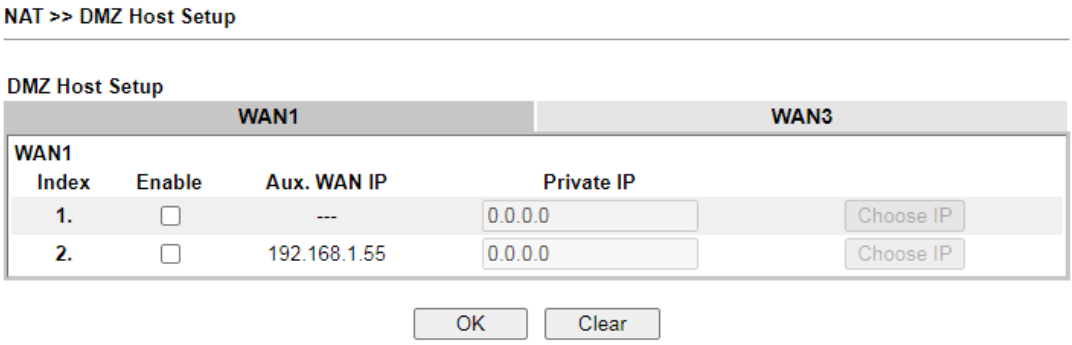
Available settings are explained as follows:

Item	Description
WAN 1	Enables or disables DMZ host.. **None** - Disables DMZ host function. **Private IP** - Allows WAN traffic to be sent to a specific LAN IP address.
Private IP	If Private IP mode has been selected, click the **Choose IP** button to select a LAN IP address.
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 following screen. Click **OK** to save the setting. 

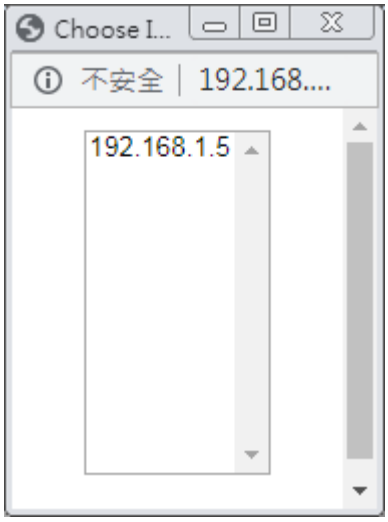
DMZ Host for WAN3 is slightly different with WAN1. See the following figure.



If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2 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 PC 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.

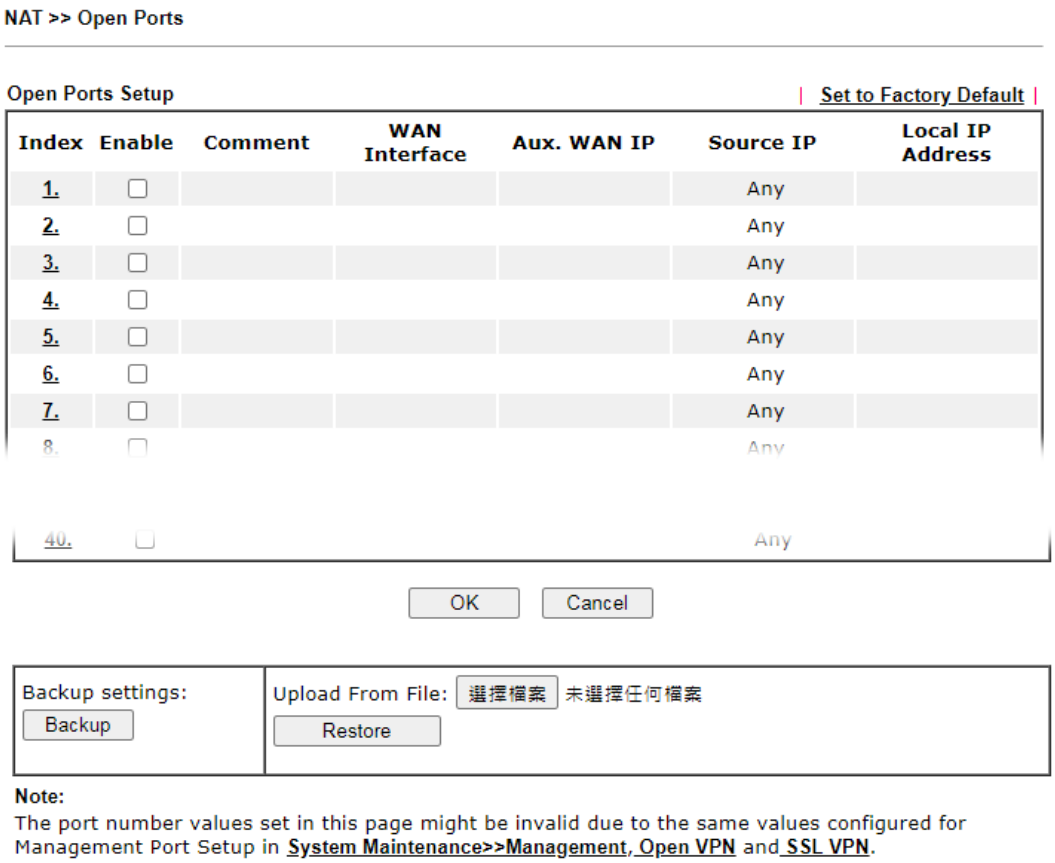
After finishing all the settings here, please click **OK** to save the configuration.

II-3-3 Open Ports

The Open Ports function allows inbound traffic from specific ports on WAN interfaces to be forwarded to LAN clients. Unlike Port Redirection, LAN client ports cannot be remapped and must remain identical to the opened ports on the WAN interface.

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

The 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.

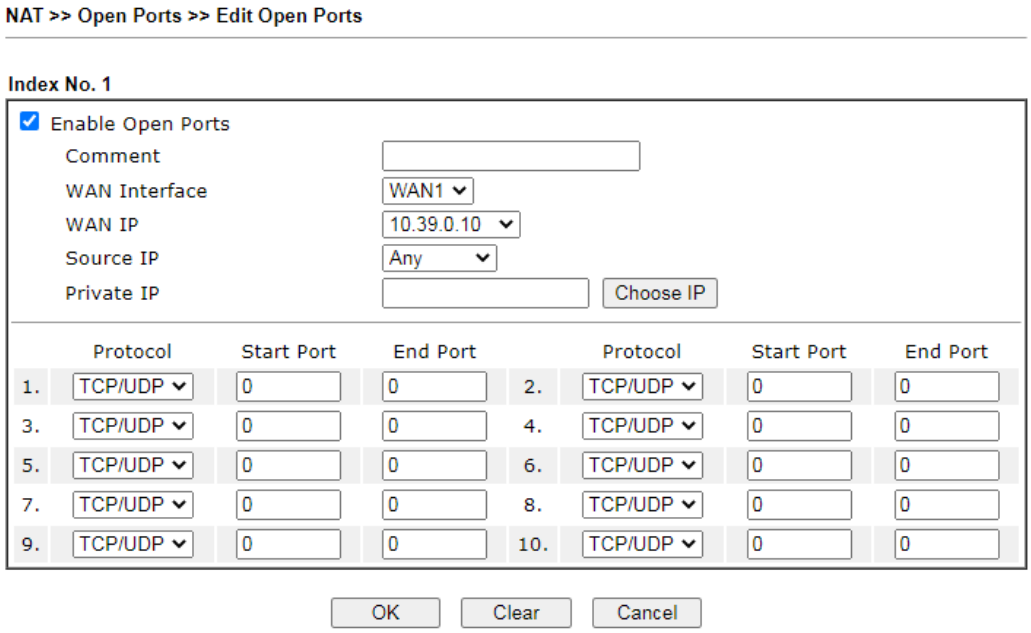


Available settings are explained as follows:

Item	Description
Index	Rule number. Click to view and edit the rule.
Enable	Select the box to enable the open port rule.
Comment	User-entered label that identifies the rule.
WAN Interface	The WAN port(s) whose incoming traffic will be forwarded to a LAN client.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, this field will not appear.
Source IP	The IP object of the source IP.
Local IP Address	LAN client to receive the forwarded WAN traffic.
Backup	Click it to backup the configuration of open ports settings.

Restore	Click it to restore the configuration of open ports settings. Before clicking, make sure upload the configuration file onto Vigor router.

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.

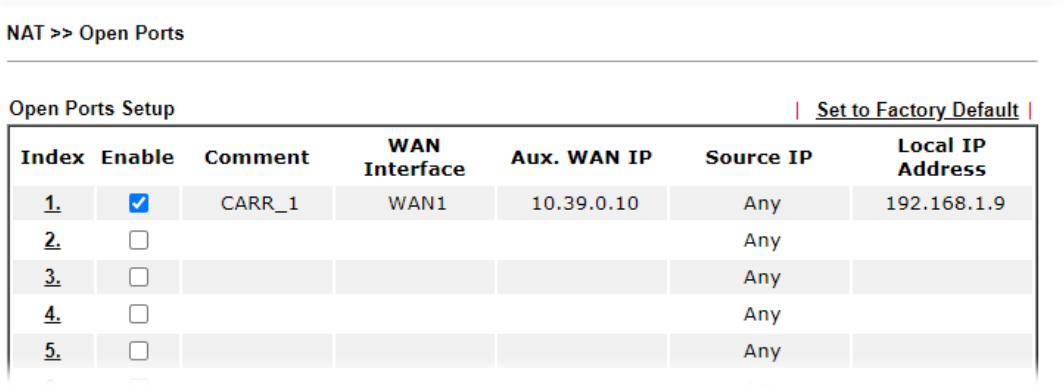


Available settings are explained as follows:

Item	Description
Enable Open Ports	Select to enable this rule.
Comment	User-entered label that identifies the rule.
WAN Interface	The WAN port(s) whose incoming traffic will be forwarded to a LAN client. Select from a specific WAN interface WAN1 to WAN6, or choose ALL to apply the rule to all WAN interfaces.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Source IP	**Any -** Any IP can be used as the source IP. **IP Object** - Use the drop down list to specify an IP object proifle. **IP Group** - Use the drop down list to specify an IP group profile.
Private IP	IP address of LAN client to receive the forwarded WAN traffic. Click **Choose IP** to select. **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	The protocol(s) to which this rule applies. **TCP** - forward only TCP traffic. **UDP** - forward only UDP traffic. **TCP/UDP** - forward both TCP and UDP traffic.
Start Port	The port number of the starting port to be forwarded.

End Port	The port number of the ending port to be forwarded. If only one port is to be forwarded, enter the same port number as the Start Port.

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



II-3-4 Port Triggering

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

Port Triggering is a variation of open ports function.

The key difference between "open port" and "port triggering" is:

- Once the OK button is clicked and the configuration has taken effect, "open port" keeps the ports opened forever.
- Once the OK button is clicked and the configuration has taken effect, "port triggering" will only attempt to open the ports once the triggering conditions are met.
- The duration that these ports are opened depends on the type of protocol used. The "default" durations are shown below and these duration values can be modified via telnet commands.

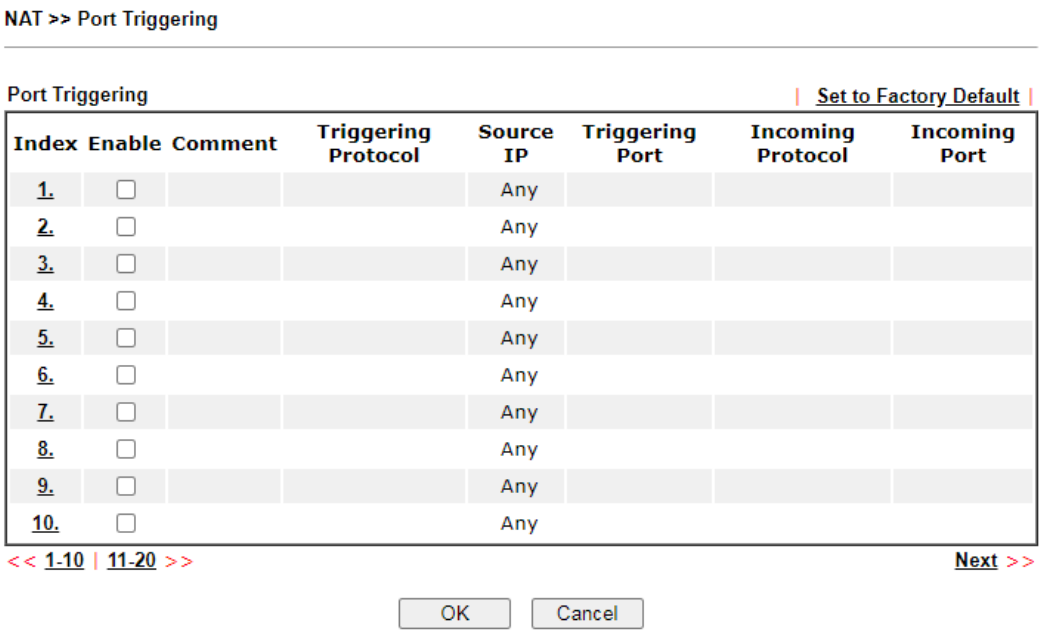
  TCP: 86400 sec.

  UDP: 180 sec.

  IGMP: 10 sec.

  TCP WWW: 60 sec.

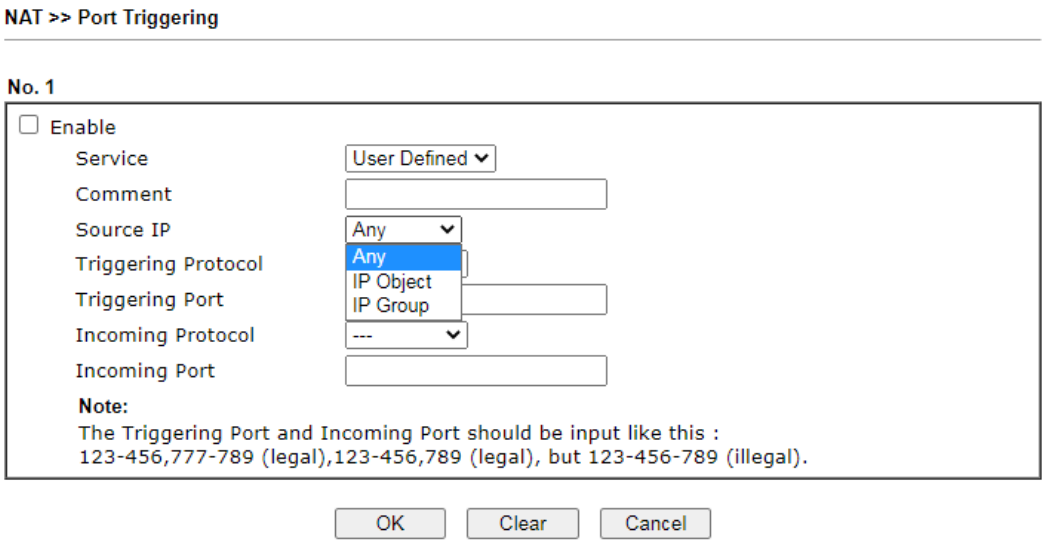
  TCP SYN: 60 sec.



Available settings are explained as follows:

Item	Description
Index	Rule number. Click to view or modify rule settings.
Enable	Select to enable the Port Triggering rule.
Comment	User-entered label that identifies the rule.
Triggering Protocol	The protocol(s) of the outgoing traffic that this rule monitors. **TCP**- monitor only TCP traffic. **UDP**- monitor only UDP traffic. **TCP/UDP**- monitor both TCP and UDP traffic.
Source IP	The IP object of the source IP.
Triggering Port	Display the port of the triggering packets. Outgoing traffic destined for these port numbers will trigger the opening WAN ports to incoming traffic.
Incoming Protocol	Display the protocol for the incoming data of such triggering profile. The protocol(s) of the incoming traffic. **TCP**-open port(s) to TCP traffic. **UDP**- open port(s) to UDP traffic. **TCP/UDP**- open port(s) to both TCP and UDP traffic.
Incoming Port	Display the port for the incoming data. Incoming traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule.

Click the index number link to open the configuration page.



Available settings are explained as follows:

Item	Description
Enable	Select to enable rule.
Service	Select from list of predefined service, or User Defined to manually configure triggering and incoming protocols and ports.
Comment	Enter the text to memorize the application of this rule.
Source IP	**Any -** Any IP can be used as the source IP. **IP Object** - Use the drop down list to specify an IP object proifle. **IP Group** - Use the drop down list to specify an IP group profile.
Triggering Protocol	The protocol(s) of the outgoing traffic that this rule monitors. **TCP** - monitor only TCP traffic. **UDP** - monitor only UDP traffic. **TCP/UDP** - monitor both TCP and UDP traffic.
Triggering Port	Outgoing traffic destined for these port numbers will trigger the opening WAN ports to incoming traffic. Enter the port or port range for such triggering profile.
Incoming Protocol	The protocol(s) of the incoming traffic. **TCP**-open port(s) to TCP traffic. **UDP**- open port(s) to UDP traffic. **TCP/UDP**- open port(s) to both TCP and UDP traffic. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.
Incoming Port	Incoming traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule. Enter the port or port range for the incoming packets.

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

Open Port and Port Triggering Compared

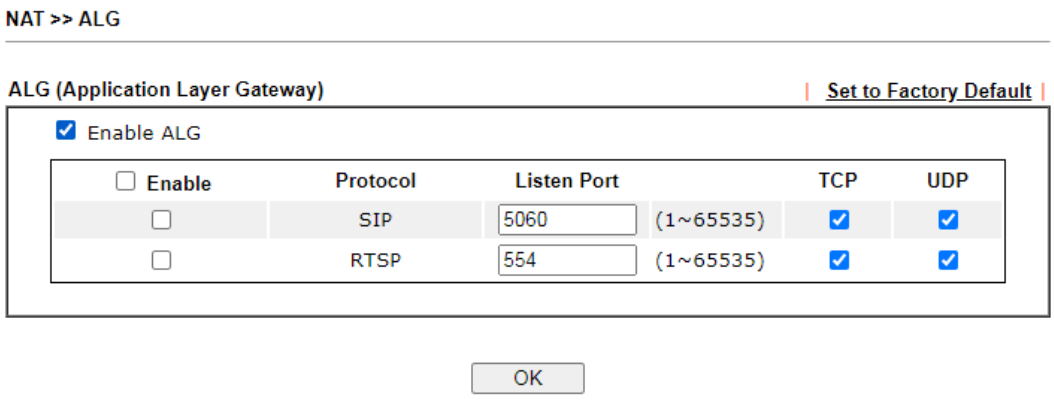
Port Triggering	Open Port
Ports are opened when the triggering condition is met.	Ports are always open on the WAN interface.
	Opened ports will be closed after predefined durations have elapsed. Default duration values vary depending on the protocol and traffic content: ● TCP (all TCP ports, except those that pass HTTP and HTTPS traffic): 86400 seconds ● UDP: 180 seconds ● TCP WWW (TCP ports that engage in HTTP and HTTPS communication): 60 seconds ● TCP SYN: 60 seconds (SYN packets expire after 60 seconds) These values can be changed by using the command line interface (telnet or SSH).

II-3-5 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-4 Applications

Dynamic DNS

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

The Vigor router supports a wide range of DDNS providers, such as DynDNS, No-IP.com, DtDNS, and ChangeIP. Please contact the DDNS provider of your choice to set up service before configuring DDNS on the router.

LAN DNS / DNS Forwarding

LAN DNS allows the network administrator to override standard DNS resolutions for selecting domain addresses. The router will respond to queries on matched domain addresses with custom IP addresses.

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

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

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/TACACS+

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

The 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.

LDAP /Active Directory Setup

Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team of Internet Engineering Task Force (IETF).

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory

securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.

UPnP

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

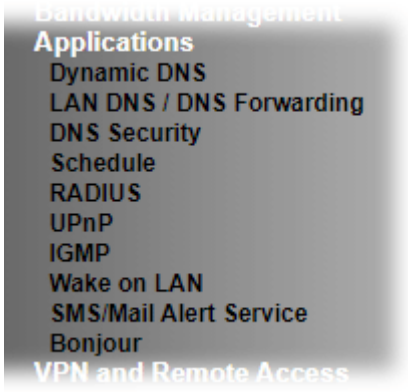
Examples of applications and devices that support UPnP include file-sharing applications such as uTorrent, Vuze and eMule, gaming consoles such as the Sony PlayStations 3 and 4 Xbox 360 and Xbox One, media streaming applications such as Plex and XBMC, and messaging and calling applications such as Skype.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

Wake on LAN

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

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

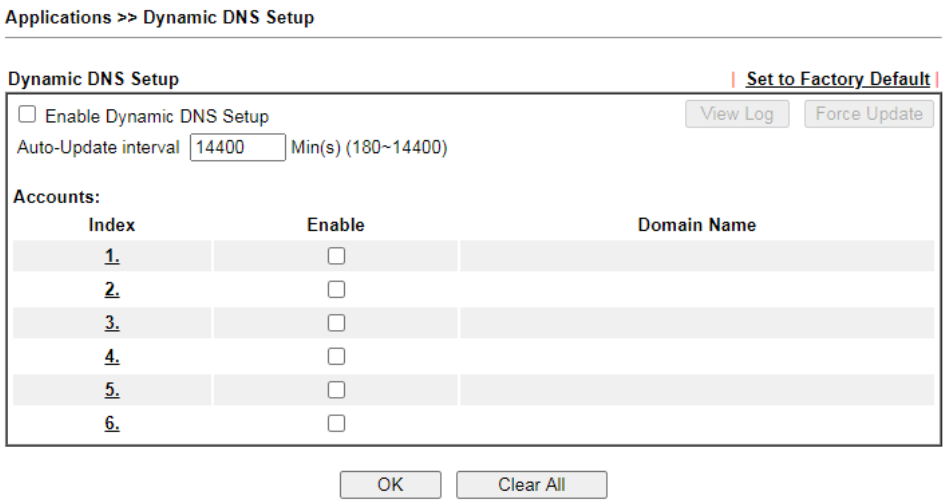
Web User Interface



II-4-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

To begin configuring Dynamic DNS, from the main menu, navigate to **Applications**, and select **Dynamic DNS**. The Dynamic DNS main configuration screen appears:

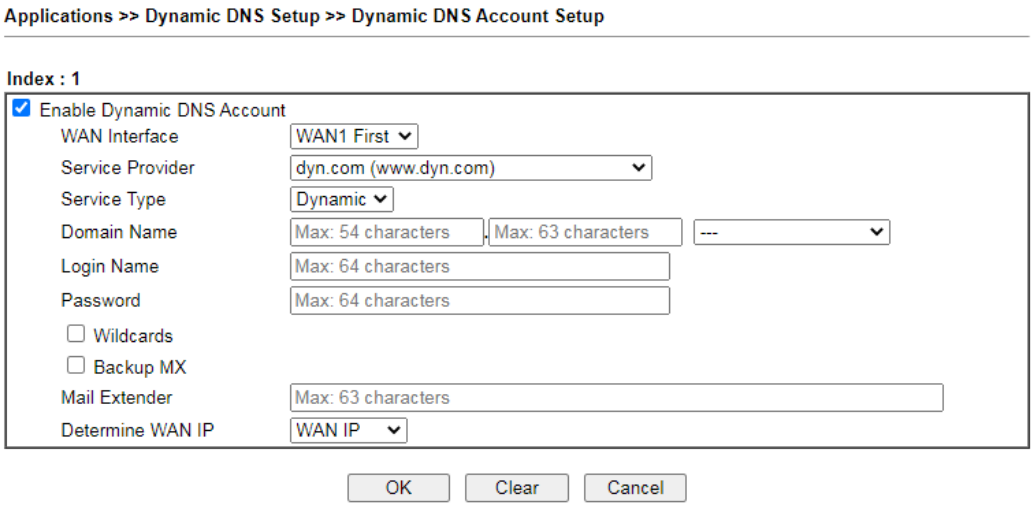


Available settings are explained as follows:

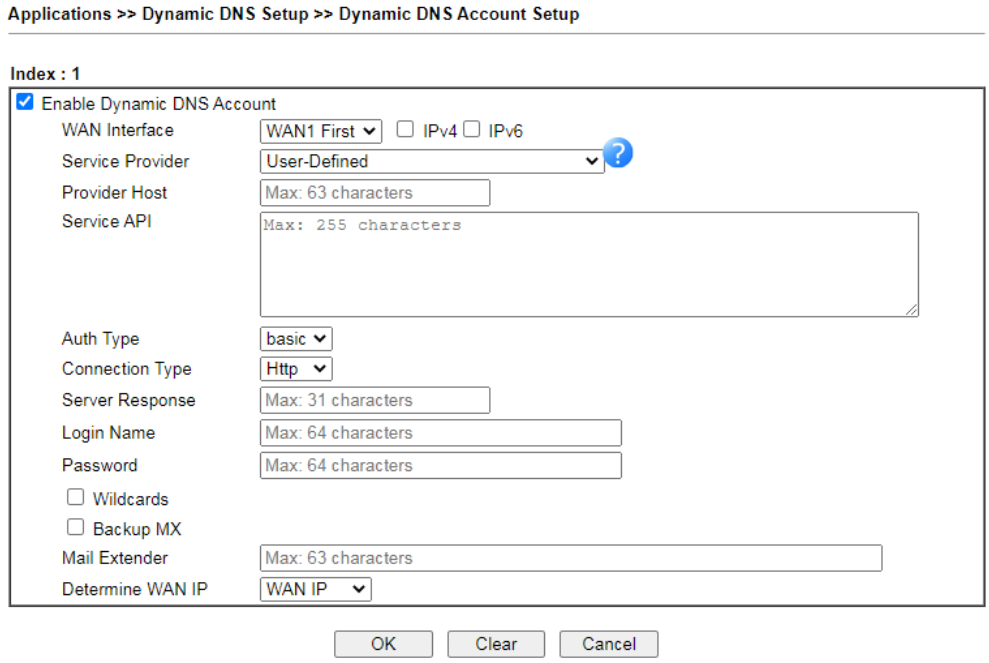
Item	Description
Enable Dynamic DNS Setup	Select to enable DDNS function.
Set to Factory Default	Click to clear all profiles to factory settings.
View Log	Select to display the most recent DDNS update messages.
Force Update	Click to connect immediately to DDNS servers to update IP address information.
Auto-Update interval	The frequency, in minutes, at which the router connects to DDNS servers to update IP address information.
Index	Click to bring up the configuration page of the DDNS profile.
Enable	Check the box to enable such account.

Domain Name	Shows the domain name with which the profile is associated.

After clicking on the index number, the detail configuration screen for the DDNS profile appears:

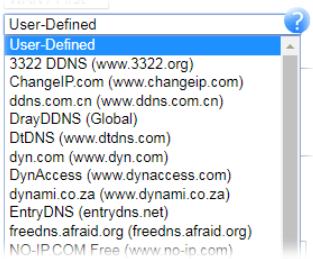


If **User-Defined** is specified as the service provider, the web page will be changed slightly as follows:



Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Select to enable this DDNS profile.
WAN Interface	Select the WAN interface to monitor for IP address changes. **WANx First** – The specified WAN interface will be examined first. If it is online, its IP address will be used in the DDNS update. **WANx Only** – Only the specified WAN interface will be examined. If the WAN interface is online, its IP address will be used in the DDNS update. Otherwise no update will be

	performed for this DDNS profile.
Service Provider	Select the DDNS provider. If your DDNS provider is not listed, select **User-Defined** and manually configure the profile.  ● **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. If other service provider is selected, you have to configure Service Type, Domain Name, Login Name and Password. ● **Service Type** - Select the service type that matches that of your DynDNS account. If you are unsure which service type to select, try Dynamic first. This options is applicable to DynDNS only. ● **Domain Name** - The domain and subdomain to be updated.
Login Name	The login name of the DDNS account.
Password	The password of the DDNS account.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

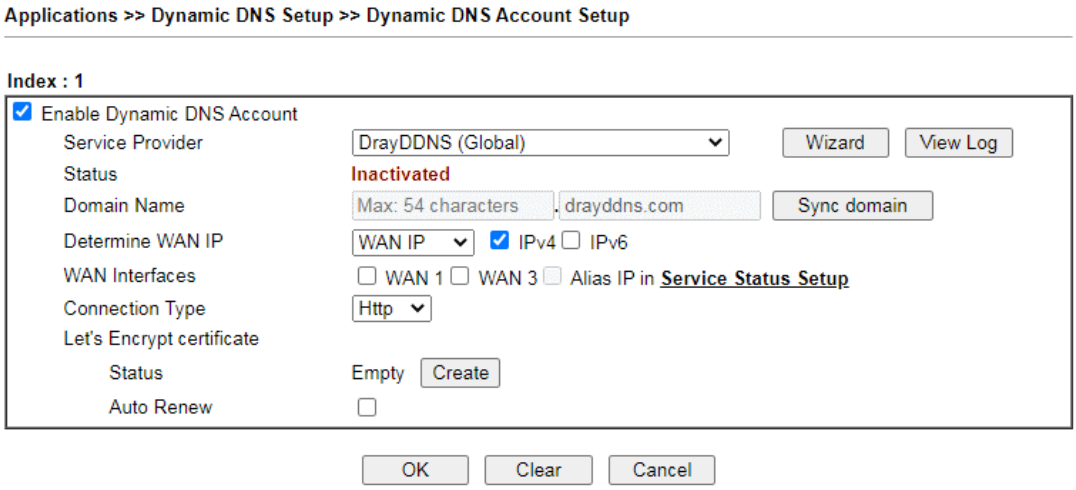
Mail Extender	If the mail server is defined with another name, please enter the name in this area. Such mail server will be used as backup mail exchange.
Determine WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used 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** - The IP address of the router's WAN interface will be used. ● **Internet IP** – The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address.

Click **OK** to save changes, **Clear** to clear all settings, or **Cancel** to discard changes and return to the main DDNS screen.

DrayDDNS Settings

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

Choose **DrayTek Global** as the service provider, the web page will be displayed 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	Choose **DrayTek Global** as the service provider. **Wizard** – This button is available when DrayTek Global is selected as Service Provider. To activate the DrayTek's DDNS service, click it to enable license issued by DrayTek through **Wizards>>Service Activation Wizard**. Refer to secion **A-1 How to use DrayDDNS?** for detailed information.
Status	Display if the license is actvtaed or not.
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.
WAN Interfaces	**WANx** - While connecting, the router will use WANx as the channel for such account.
Let's Encrypt certificate	**Create –** Click it to generate a certificate issued by Let's Encrypt for applying to such DDNS account. **Auto Update** – Check the box to make the system update the certificate automatically.

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.

Delete a Dynamic DNS Account

Click the **Index** number you want to delete and then click **Clear All** button to delete the account.

DDNS updates take place when:

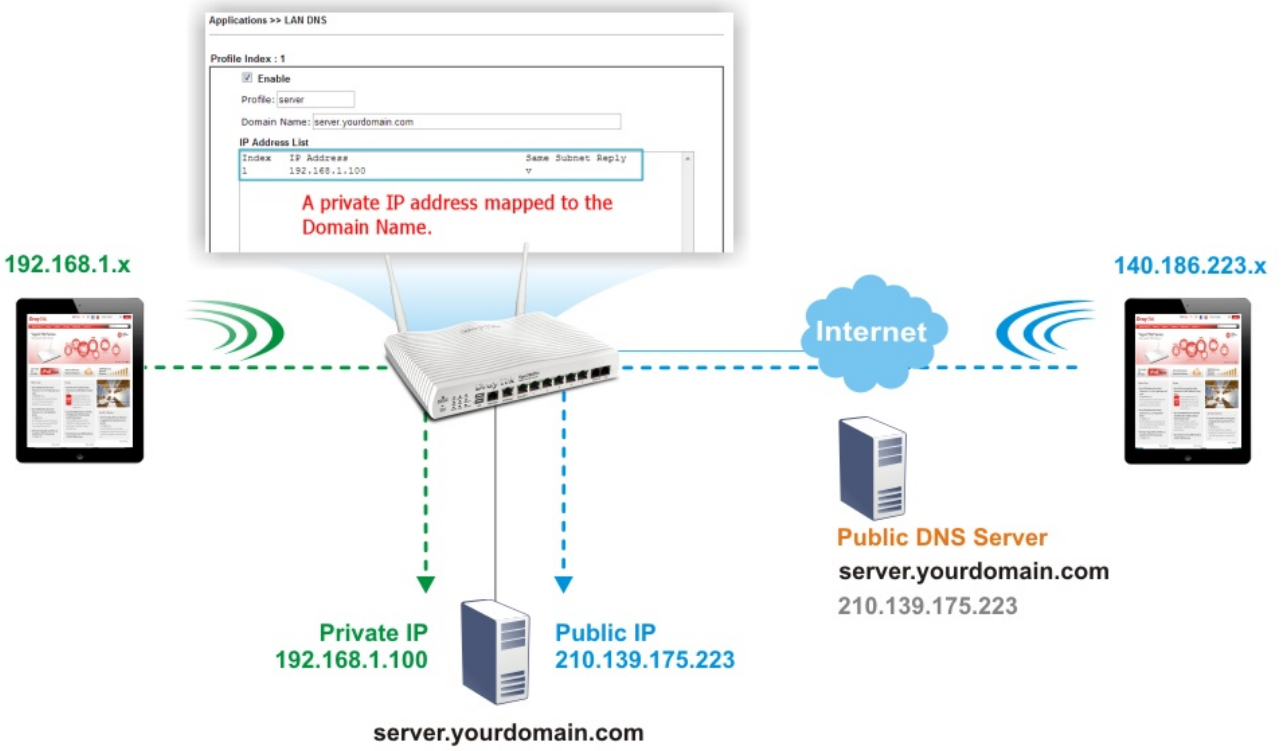
- The router is powered on or rebooted.
- The public IP address of any WAN interface changes.
- The online status of a WAN interface changes (going from online to offline or vice versa).
- The DDNS function is changed from disabled to enabled.
- A DDNS entry is modified and enabled.
- The Auto-Update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

Procedures for Setting up a Dynamic DNS Entry

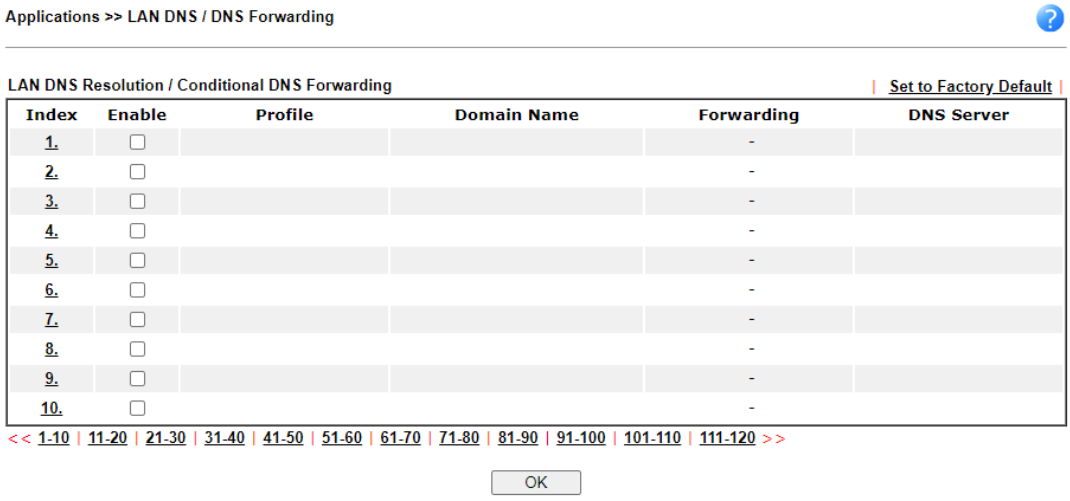
1. Contact the dynamic DNS provider of your choice and have service set up. Most DDNS providers accept signups on their websites. Service could be provided free of charge or for a fee.
2. Create a DDNS entry on the router by selecting the appropriate DDNS provider and enter the account information.
3. Make sure that both the DDNS entry and the DDNS feature are enabled on the router.
4. Click the View Log button on the DDNS main page to bring up the update log.
5. Examine the update log to make sure the update was successful.
6. If the update was not successful, verify the DDNS entry to make sure the settings are entered correctly.

II-4-2 LAN DNS / DNS Forwarding

LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2135 series will respond the specified private IP address.



To start configuring LAN DNS or DNS Forwarding, from the main menu, click **Applications**, followed by **LAN DNS / DNS Forwarding**.

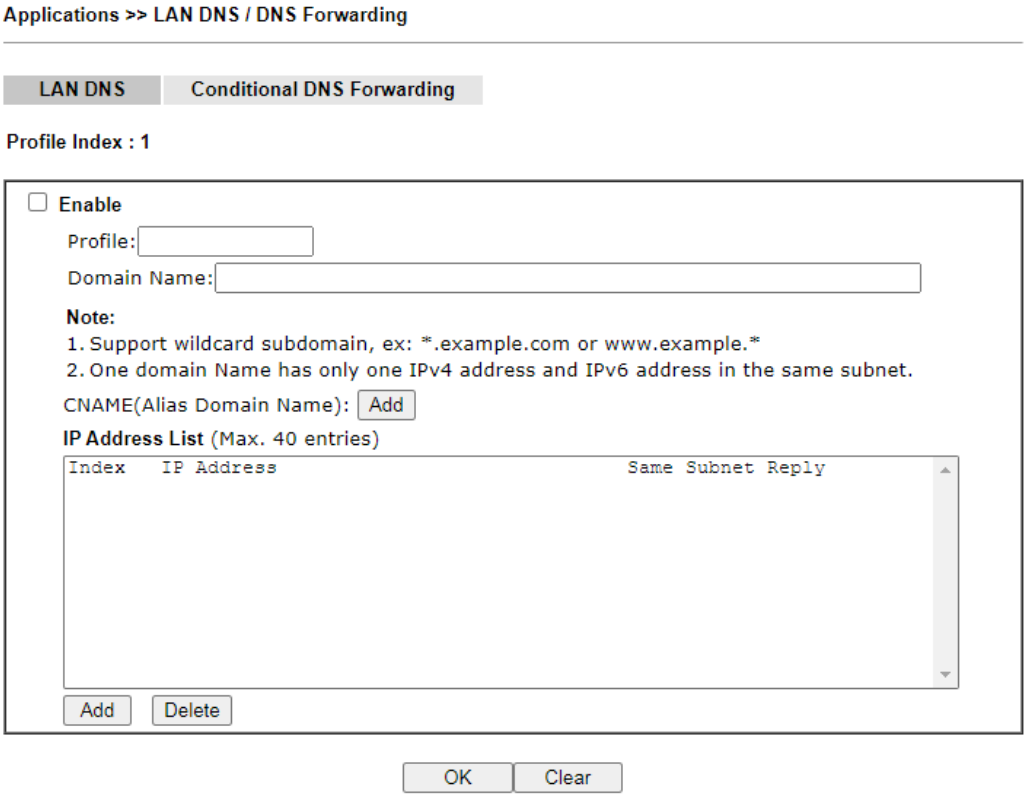


Each item is explained as follows:

Item	Description
Set to Factory Default	Click to clear all profiles to factory settings.

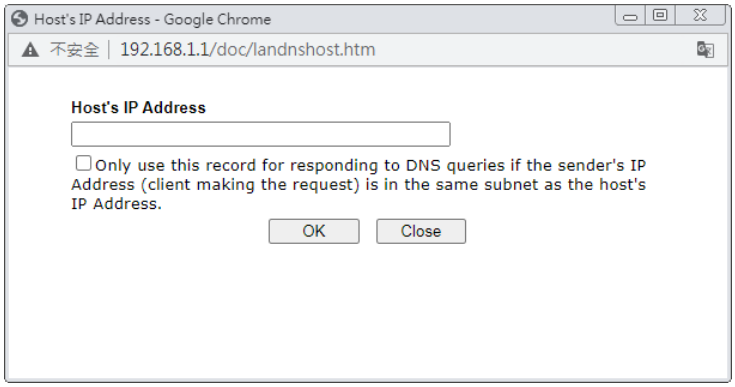
Index	Click to bring up the configuration page for the profile.
Enable	Select to enable this profile.
Profile	Shows the name of the profile.
Domain Name	Shows the domain name configured for the profile.
Forwarding	V – DNS queries for the specified domain name will be forwarded to the specified server. - DNS queries for the specified domain name will not be forwarded.
DNS Server	DNS server to which DNS queries for the specified domain name will be forwarded.

To configure a LAN DNS profile, click on its index to bring up the configuration page.



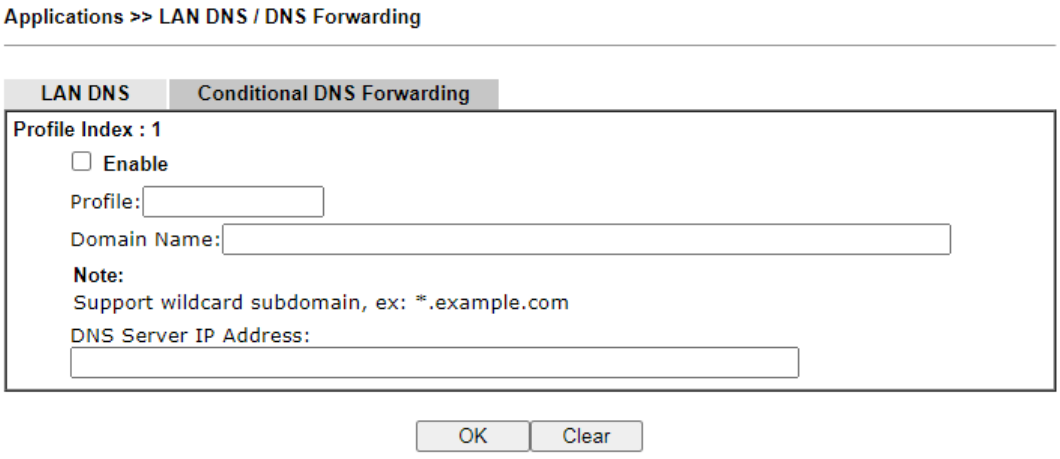
Available settings are explained as follows:

Item	Description
Enable	Select to enable this profile.
Profile	Enter a name to identify this profile. **Note:** If you type a name here for LAN DNS and click **OK** to save the configuration, the name also will be applied to conditional DNS forwarding automatically.
Domain Name	Enter the domain name for the router to look for in DNS queries to intercept and reply to. Wildcards in the form of asterisks (*) can be used to match a domain level. For example, *.draytek.com will match domain names such as www.draytek.com and ftp.draytek.com, whereas www.draytek.* will match domain names such as www.draytek.com and www.draytek.co.uk.

CNAME	Click **Add** to add an domain name alias for the domain name. Click Delete next to an alias entry to delete it.
IP Address List	The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name. **Add** – Click **Add** to bring up the Add IP Address dialog box:  ● **Host's IP Address –** Enter the IP address to be returned in response to a DNS query for the configured domain names and aliases. ● **Only use this record….** – Select to use this IP address only if the IP address of the source of the DNS query belongs to the same subnet as the host IP address entered above. After changes have been made, click **OK** to save and dismiss the dialog box, or **Close** to discard the changes and dismiss the dialog box. **Delete** –To delete an IP address, click on it and then click Delete.

To save changes made to the LAN DNS profile, click **OK**. To clear the profile and restore the factory default blank values, click **Clear**.

If you need to configure LAN DNS settings, click index 1 to edit the LAN DNS profile just created. Or, you can click index 2 to use this profile as conditional DNS forwarding.



Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile. **Note:** If you type a name here for conditional DNS forwarding and click **OK** to save the configuration, the name also will be applied to LAN DNS automatically.
Domain Name	Enter the domain name for such profile.
DNS Server IP Address	Enter the IP address of the DNS server you want to use for DNS forwarding.

To save changes made to the LAN DNS profile, click **OK**. To clear the profile and restore the factory default blank values, click **Clear**.

II-4-3 DNS Security

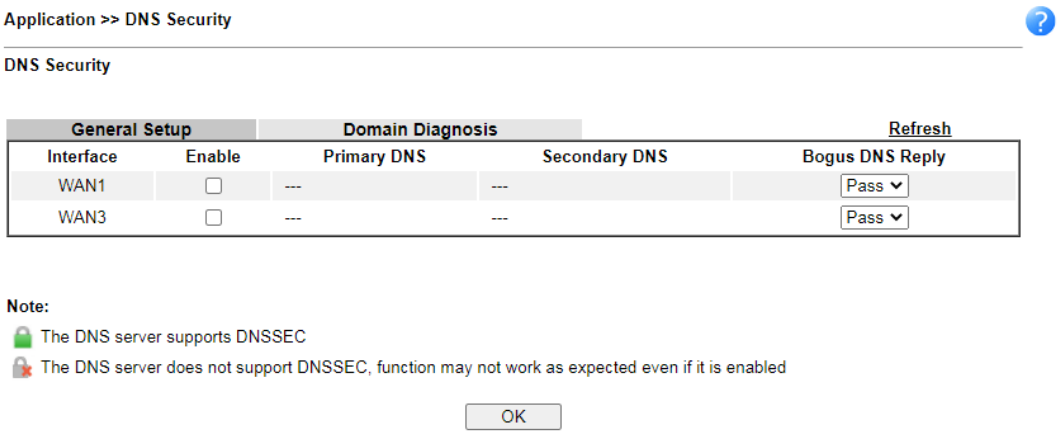
Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.

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

To configure DNS security, from the main menu, click **Applications**, followed by **DNS Security**.

II-4-3-1 General Setup

All of WAN interfaces of Vigor router can be configured with DNS Security enabled respectively.



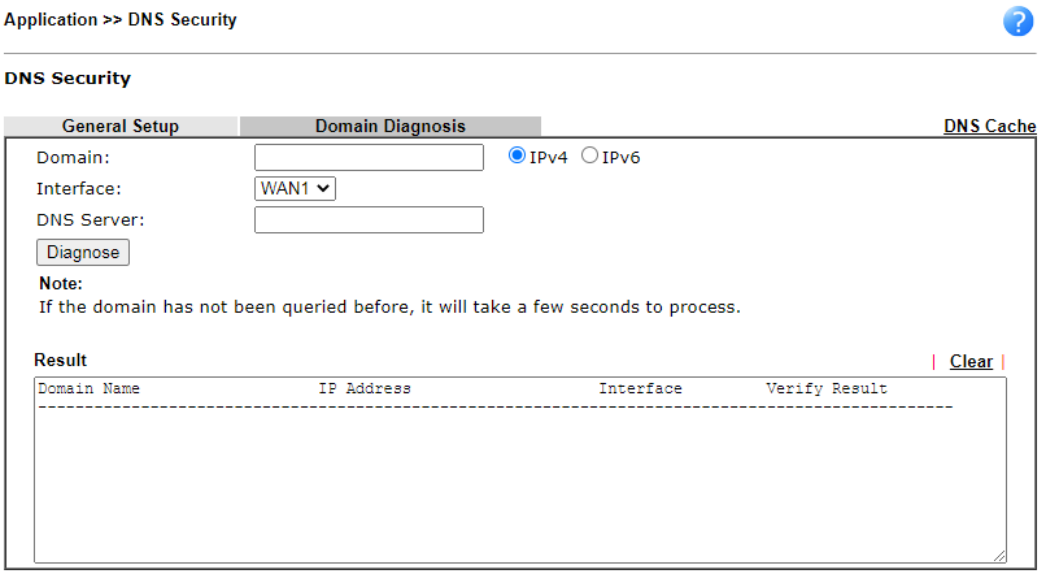
Available settings are explained as follows:

Item	Description
Interface	The WAN interface name for which DNS security is to be configured.
Enable	Select to enable DNS security for this WAN Interface.
Primary DNS	Shows the primary DNS server IP address in effect for this WAN.
Secondary DNS	Shows the secondary DNS server IP address in effect for this WAN.
Bogus DNS Reply	Show action to be taken for DNS responses that fail authentication. Choose Pass or Drop. **Pass** – Pass DNS result. **Drop** – Do not pass DNS result.

Press **OK** to save changes.

II-4-3-2 Domain Diagnose

While using the Domain Diagnose feature, you can check to see if the router's DNS security function is working properly, or whether a given domain is secured by DNS security. Note that DNS Security has to be first enabled or the test results would not be meaningful.

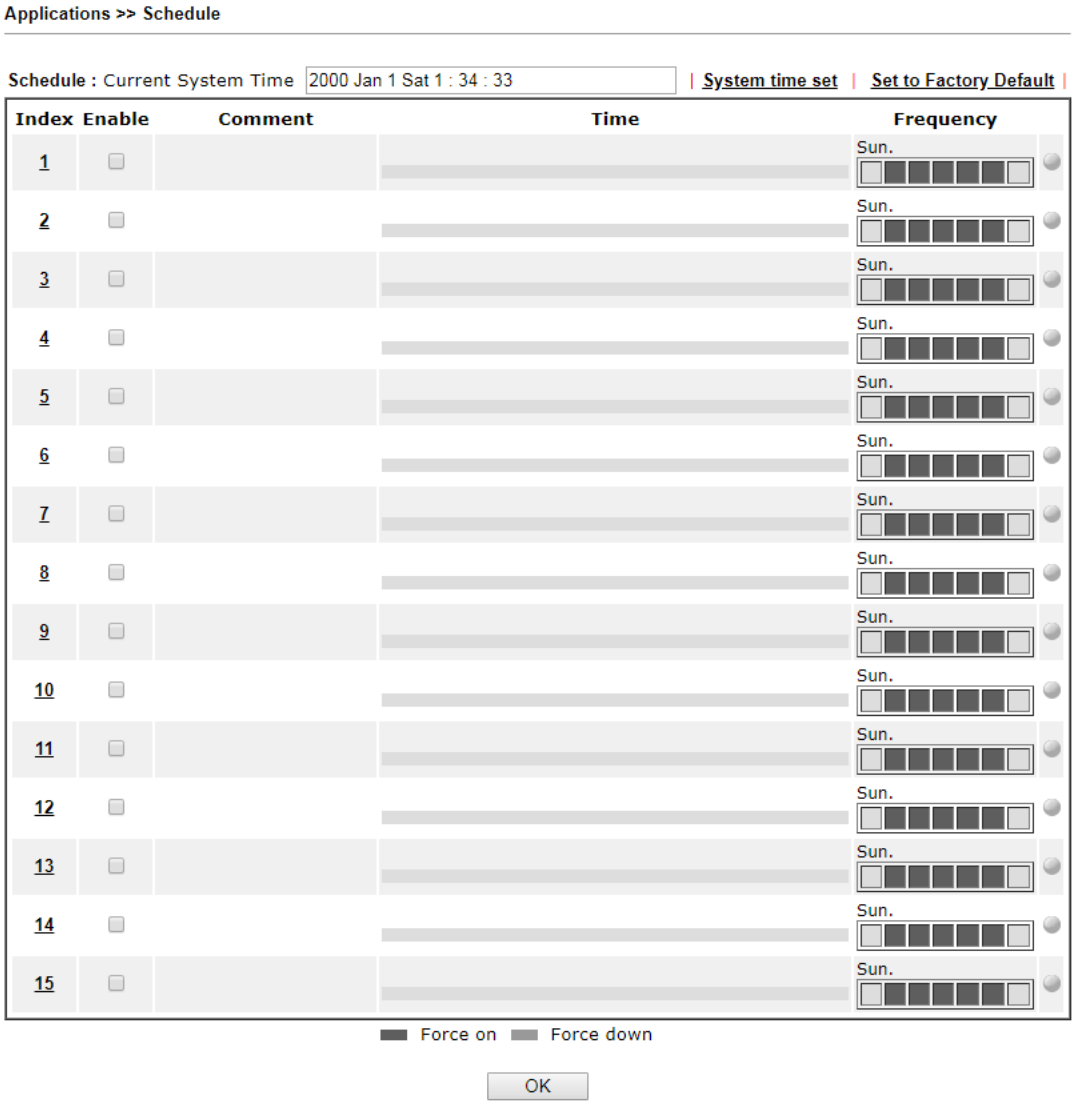


Available settings are explained as follows:

Item	Description
Domain	Enter domain address to be diagnosed. Select the type of IP address to be looked up. IPv4 – looks up A records. IPv6 – looks up AAAA records.
Interface	Select the WAN port to be used for the lookup.
DNS Server	Enter the IPv4 address of the DNS server to be used for the lookup.
Diagnose	Click to begin DNS lookup.
Result	The history of domain diagnosis is shown in the Result panel.

II-4-4 Schedule

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

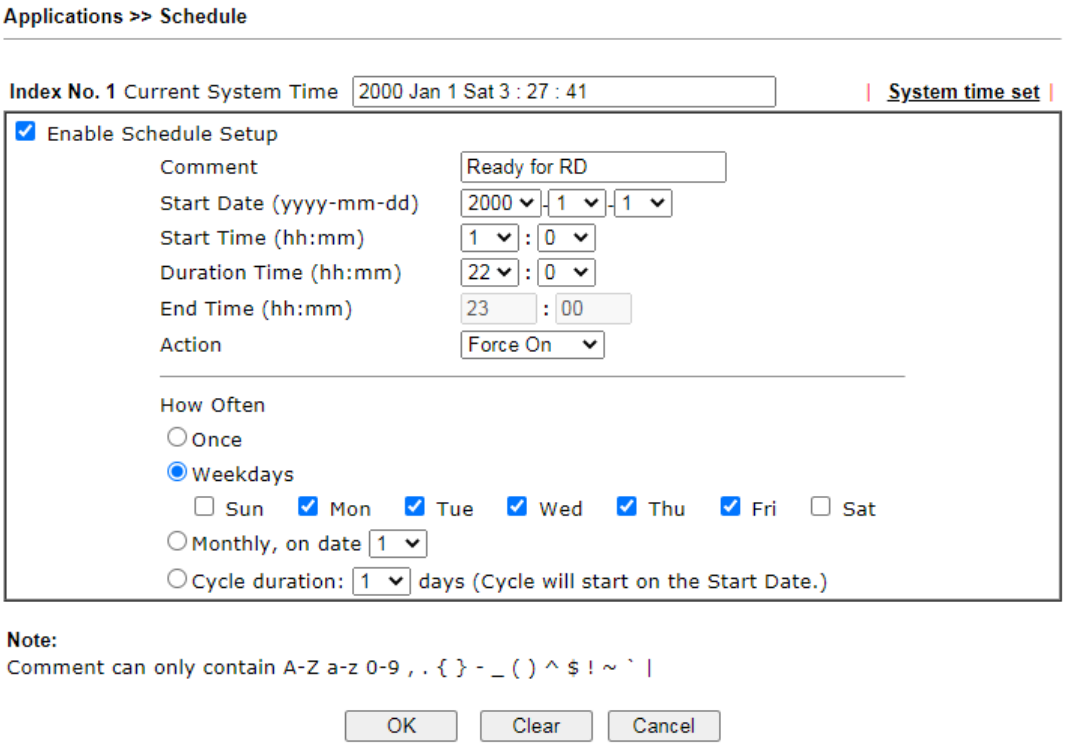


Available settings are explained as follows:

Item	Description
Current System Time	Shows the current time of the router.
System time set	Click to navigate to **System Maintenance >> Time and Date** to set the system time and date.
Set to Factory Default	Reset all schedules to factory default values.
Index	Shows the index number of the schedule entry.
Enable	Select to enable the schedule; clear to disable it.
Comment	Shows the name given to the schedule.
Time	Shows the start and end times of the schedule. The time interval of the schedule is indicated in dark grey.

Frequency	Shows the days of the week configured for the schedule. Selected days are shown in dark grey. - If it lights in green, it means such schedule is active.

To configure a schedule, click on its index to bring up the settings page.



Available settings are explained as follows:

Item	Description
Enable Schedule Setup	Select to enable the schedule; clear to disable it.
Comment	Name to identify this schedule entry.
Start Date (yyyy-mm-dd)	The date when the entry comes into effect.
Start Time (hh:mm)	The time when the schedule is triggered. See the **How Often** setting below for details.
Duration Time (hh:mm)	How long the action lasts when the scheduled is triggered.
End Time (hh:mm)	It will be calculated automatically when Start Time and Duration Time are configured well.
Action	Action to take when the schedule is triggered. **Force On** – The feature with which this schedule is associated will be turned on. **Force Down** – The feature with which this schedule is associated will be turned off.
How Often	How frequently the schedule is triggered. ● **Once** - The schedule is triggered once, on the **Start Date** at the **Start Time**, for the **Duration Time**. ● **Weekdays** - The schedule will be triggered repeatedly, starting on the **Start Date** at the **Start Time**, on the selected days of the week, at the **Start Time**, for the **Duration Time**.

	• **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.

To save changes made to the Schedule, click **OK**. To clear the schedule and restore the factory default blank values, click **Clear**. To cancel the changes and return to the main Schedule page, click **Cancel**.

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**

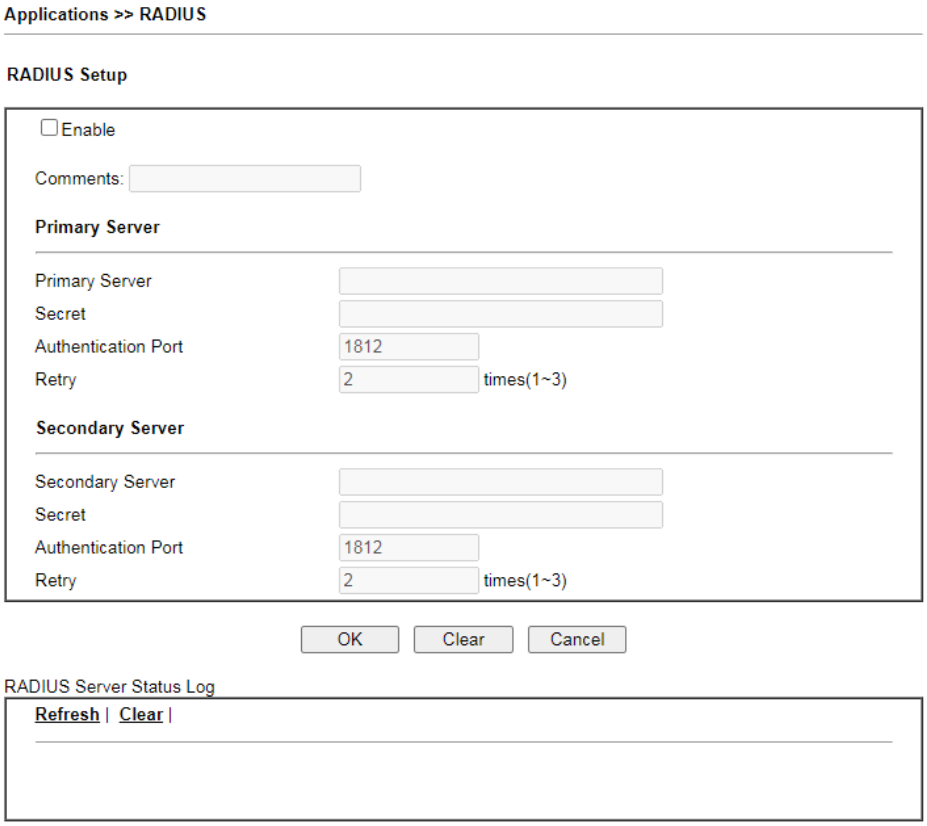
1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet 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-4-5 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. This web page is used to configure settings for external RADIUS server. Then LAN users of Vigor router will be authenticated and accounted by such server for network application.



Available settings are explained as follows:

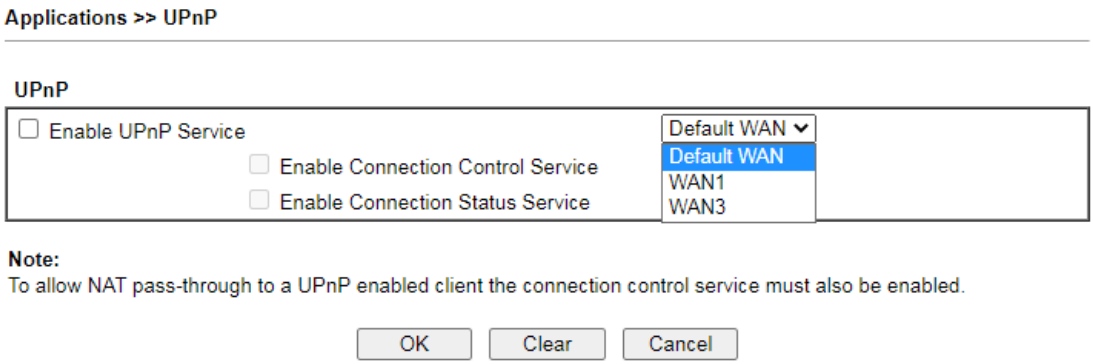
Item	Description
Enable	Check to enable RADIUS client profile. **Comments** - Enter a brief description for this profile.
Primary Server	**Primary Server** - Enter the IP address of RADIUS server. **Secret** - The RADIUS server and client share a secret that is used to authenticate the messages sent 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 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".
RADIUS Server Status Log	Display the record of current status of RADIUS server.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To reset all settings to blank, click **Clear**.

II-4-6 UPnP

To configure UPnP settings, from the Main Menu select **Applications >> UPnP**.



Available settings are explained as follows:

Item	Description
Enable UPnP Service	Select to enable UPnP.
Default WAN	Select the WAN port on which ports will be opened in response to UPnP commands.
Enable Connection Control Service	Select to enable the connection control service.
Enable Connection Status Service	Select to enable the connection status service.

To save changes on the page, select **OK**; to discard changes, select **Cancel**; to revert all settings to the factory default, select **Clear**.

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 UPnP allows any application or network devices to open ports on the WAN side to allow connections to the LAN, which could compromise network security. Also if UPnP applications or network devices malfunction or terminate abnormally, the opened ports may remain open indefinitely, and thus increasing the chance of it getting exploited by malicious parties.

If you do not have applications or network devices which requires UPnP, you are advised to disable UPnP.

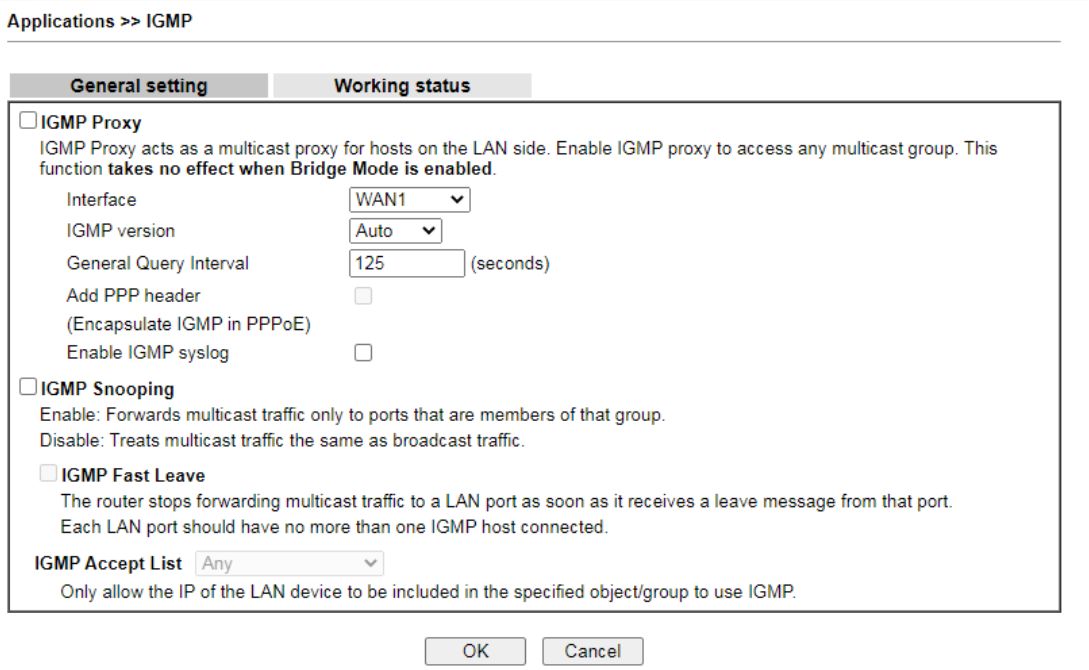
Info	UPnP is required for some applications such as PPS, Skype, eMule...and etc. If you are not familiar with UPnP, it is suggested to turn off this function for security.

II-4-7 IGMP

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

To configure IGMP settings, from the Main Menu select **Applications >> IGMP**.

II-4-7-1 General Setting



Available settings are explained as follows:

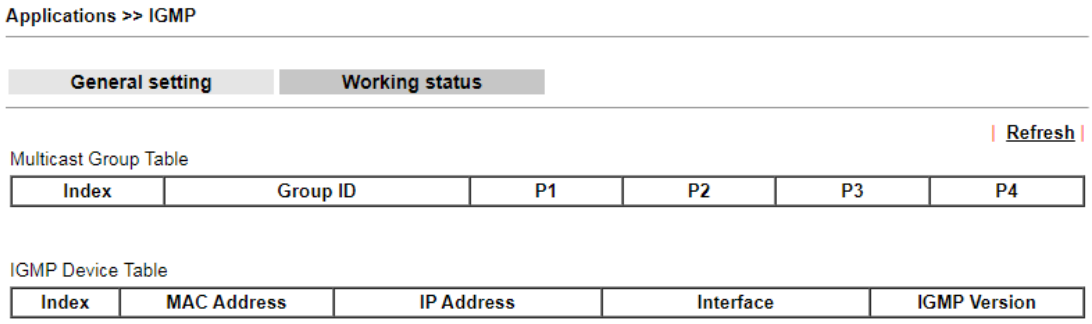
Item	Description
IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode. **Interface** – Specify an interface for packets passing through. **IGMP version** – At present, two versions (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.

To save changes on the page, select **OK**; to discard changes, select **Cancel**.

II-4-7-2 Working Group

Displays a list of active multicast groups.



Available settings are explained as follows:

Item	Description
Refresh	Click to reload the Multicast Group Table with the latest information.
Index	Index number of the multicast group.
Group ID	ID port of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254.
P1 to P4	LAN ports that have IGMP hosts joined to this multicast group.

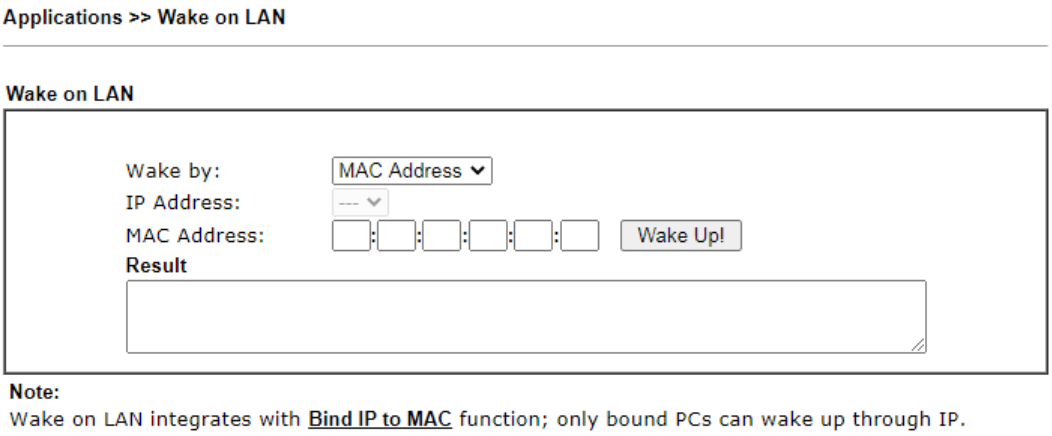
II-4-8 Wake on LAN

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

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

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

To configure Wake on LAN settings, from the Main Menu select **Applications >> Wake on LAN**.



Available settings are explained as follows:

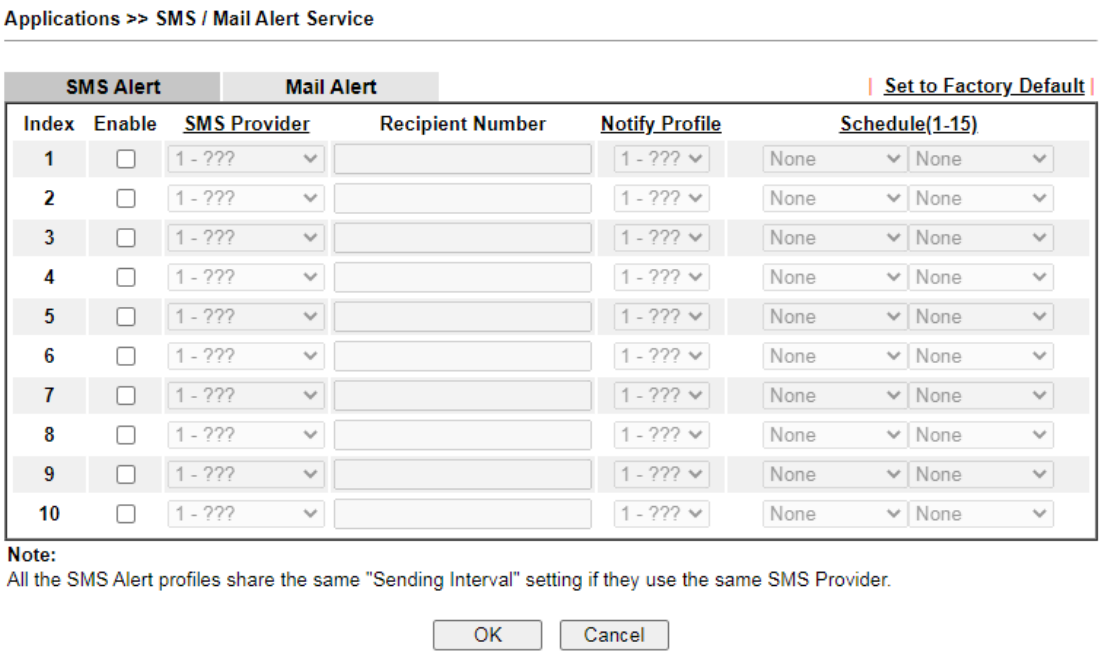
Item	Description
Wake by	The type of address of the LAN client to be woken up. ● If you choose Wake by **MAC Address**, you have to Enter the correct MAC address of the host in MAC Address boxes. ● If you choose Wake by **IP Address**, you have to choose the correct IP address.
IP Address	The IP addresses that have been configured in **Firewall>>Bind IP to MAC** will be shown in this drop down list. Select the IP address of the LAN client.
MAC Address	Enter the MAC address of the LAN client.
Wake Up	Click to send Wake-on-LAN message to the specified LAN client.
Result	Result of the transmission of the Wake-on-LAN message.

II-4-9 SMS / Mail Alert Service

You can set up SMS or mail profiles for the router to send events or alerts to designated recipients. Up to 10 SMS profiles and 10 mail profiles can be configured.

II-4-9-1 SMS Alert

To configure SMS alert profiles, select the SMS Alert tab.



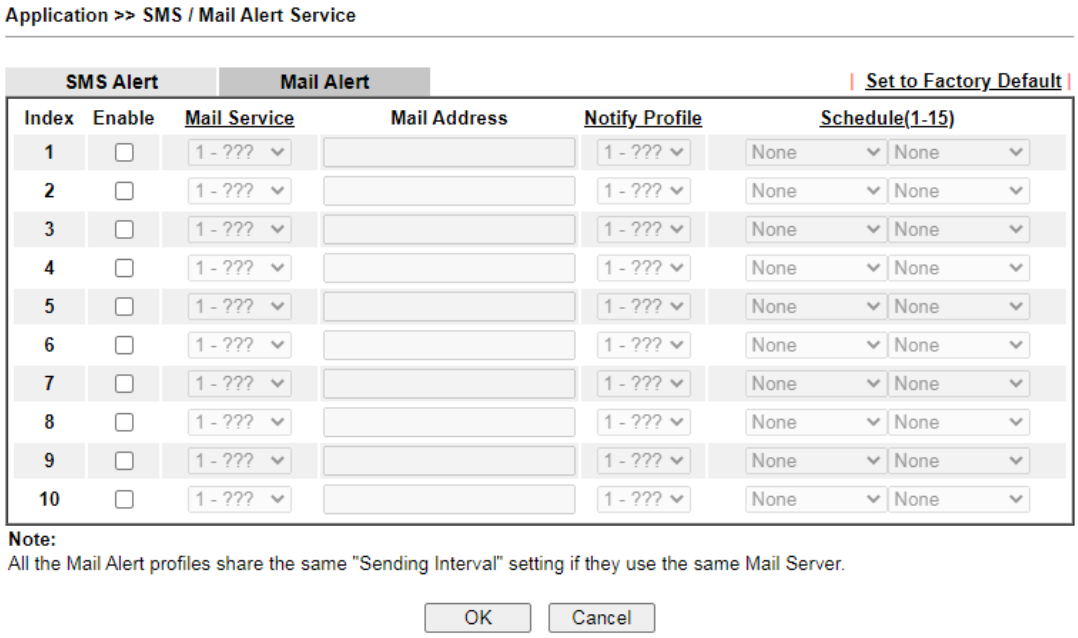
Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all SMS alert profiles.
Enable	Select the checkbox to enable the profile.
SMS Provider	Select the profile of the SMS provider to be used. To set up or modify SMS provider profiles, click the hyperlink **SMS Provider** to go to Objects Setting >> SMS/Mail Service Object.
Recipient Number	Enter the recipient's SMS number.
Notify Profile	Select the notification profile to be used. To set up or modify notification object profiles, click the hyperlink **Notify Profile** to go to Objects Setting >> Notification Object.
Schedule (1-15)	Enter up to 2 schedule profile indexes. To set up or modify schedule profiles, click the hyperlink **Schedule(1-15)** to go to Applications >> Schedule.

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

II-4-9-2 Mail Alert

To configure mail alert profiles, select the SMS Alert tab.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all mail alert profiles.
Enable	Select the checkbox to enable the profile.
Mail Service	Select the profile of the mail provider to be used. To set up or modify a mail provider profile, click the hyperlink **Mail Service** to go to Objects Setting >> SMS/Mail Service Object.
Mail Address	Enter the recipient's email address.
Notify Profile	Select the notification profile to be used. To set up or modify a notification object profile, click the hyperlink **Notify Profile** to go to Objects Setting >> Notification Object.
Schedule (1-15)	Enter up to 2 schedule profile indexes. To set up or modify schedule profiles, click the hyperlink **Schedule(1-15)** to go to Applications >> Schedule.

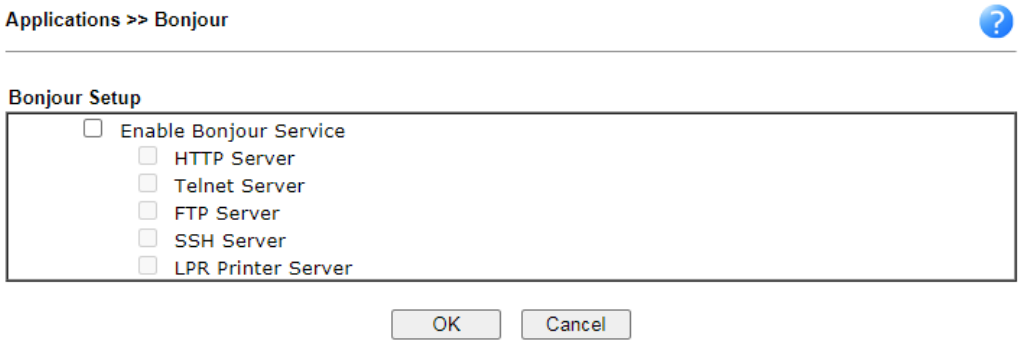
After finishing all the settings here, please click **OK** to save the configuration.

II-4-10 Bonjour

Bonjour is Apple's implementation of zero-configuration networking (Zeroconf), a technology that allows automatic discovery and configuration of network devices and services. Bonjour is built into OS X, and versions for Windows PCs can be downloaded without charge from Apple's website.

Without Bonjour, routers, computers, and other network peripherals would require manual configuration of network settings such as IP addresses and port numbers, which could be complex and cumbersome. By enabling Bonjour on the Vigor router, users only need to know the name of the router in order to set up connectivity between LAN devices, and the router and the peripherals that are connected to it.

To enable the Bonjour service, click **Application>>Bonjour** to open the following page. Check the box(es) of the server service(s) that you want to share to the LAN clients.

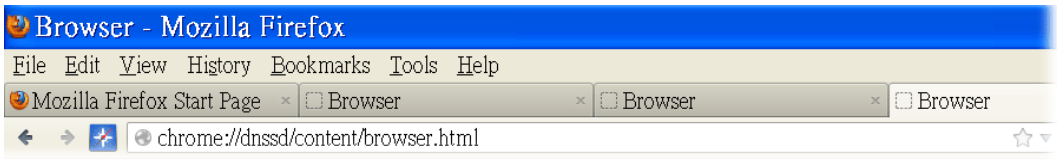


Available settings are explained as follows:

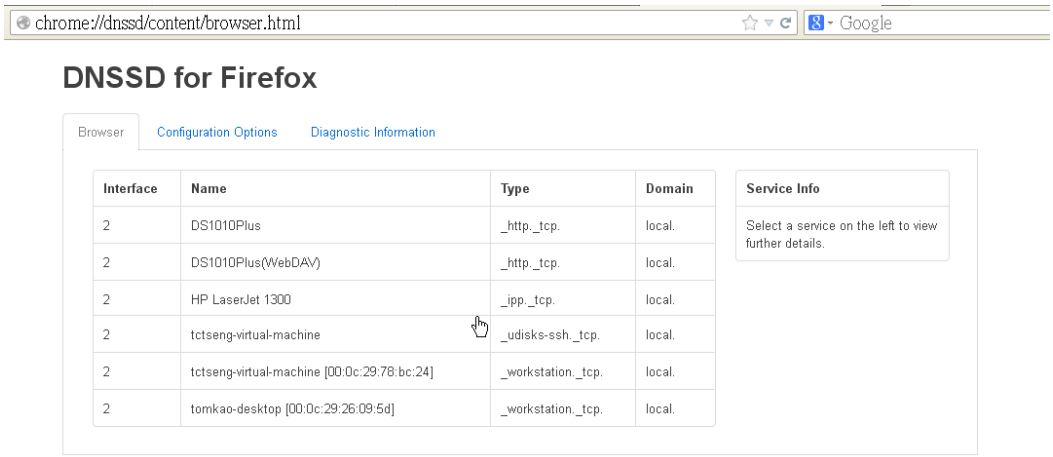
Item	Description
Enable Bonjour Service	Select to enable the Bonjour service on the router. The rest of the checkboxes will be enabled for selection when this checkbox has been selected.
HTTP Server	Select to allow the router's HTTP server to be discovered via Bonjour.
Telnet Server	Select to allow the router's telnet server to be discovered via Bonjour.
FTP Server	Select to allow the router's FTP server to be discovered via Bonjour.
SSH Server	Select to allow the router's SSH server to be discovered via Bonjour.
LPR Print Server	Select to allow the router's LPR server to be discovered via Bonjour. This allows printers attached to the router's USB ports to be discovered.

Below shows an example for applying the bonjour feature that Vigor router can be used as the FTP server.

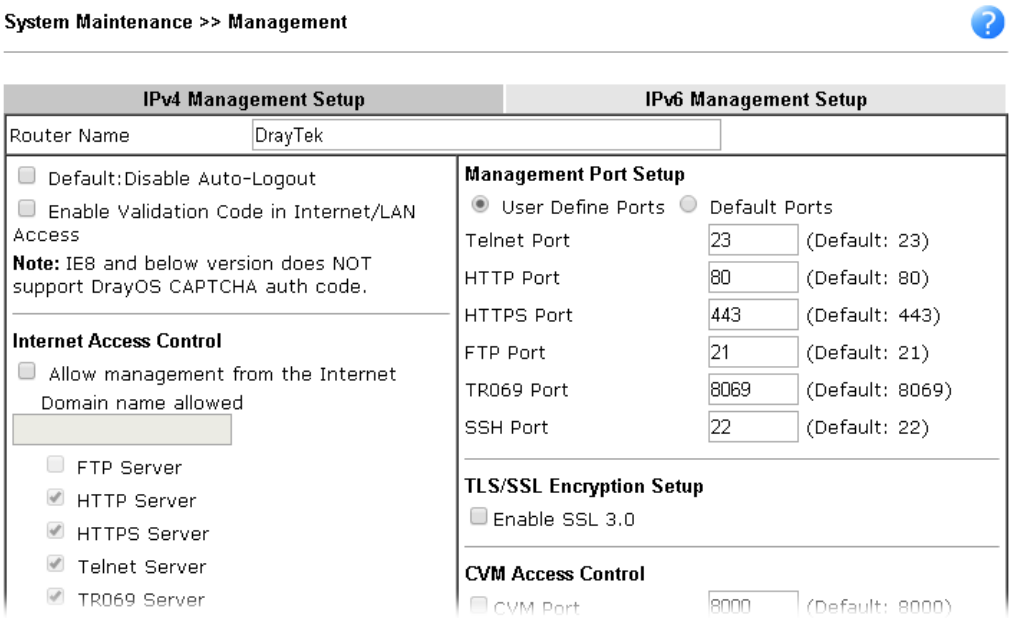
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



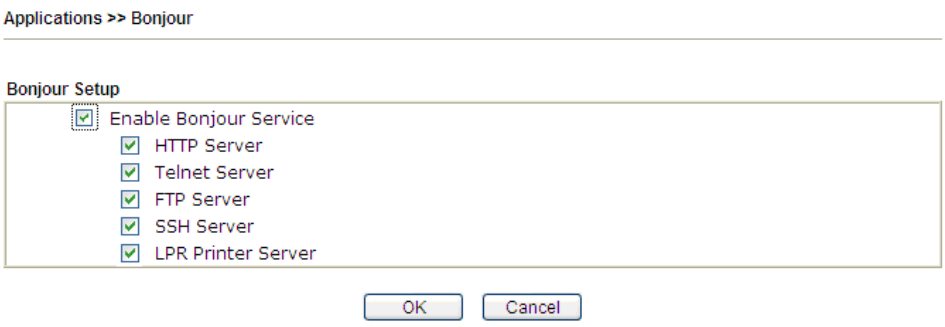
2. Open the web browse, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.



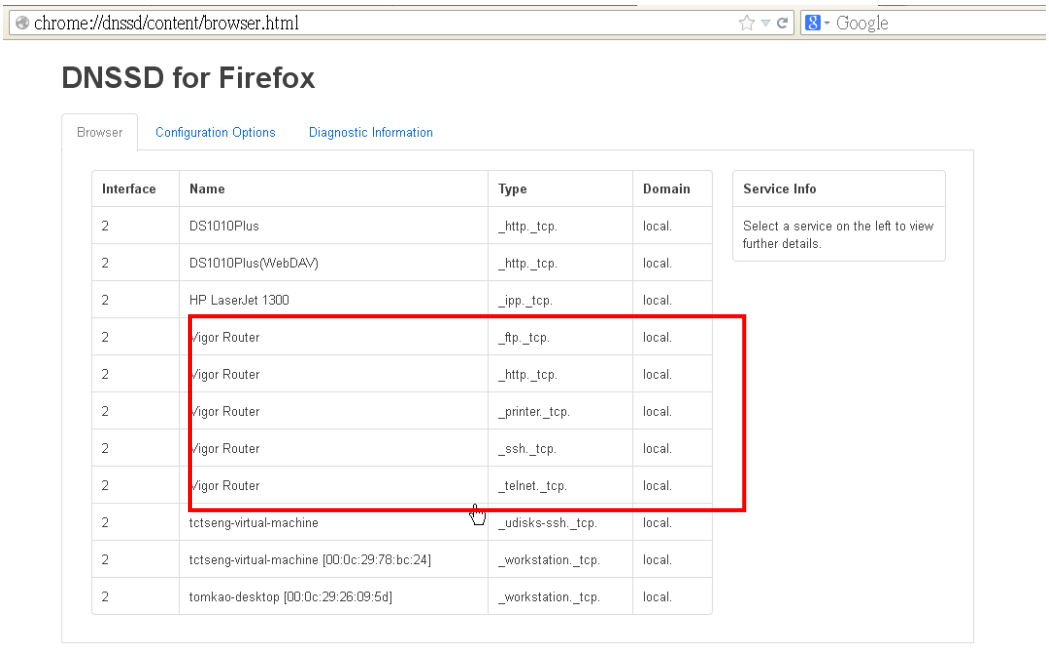
3. Open **System Maintenance>>Management**. Type a name as the Router Name and click **OK**.



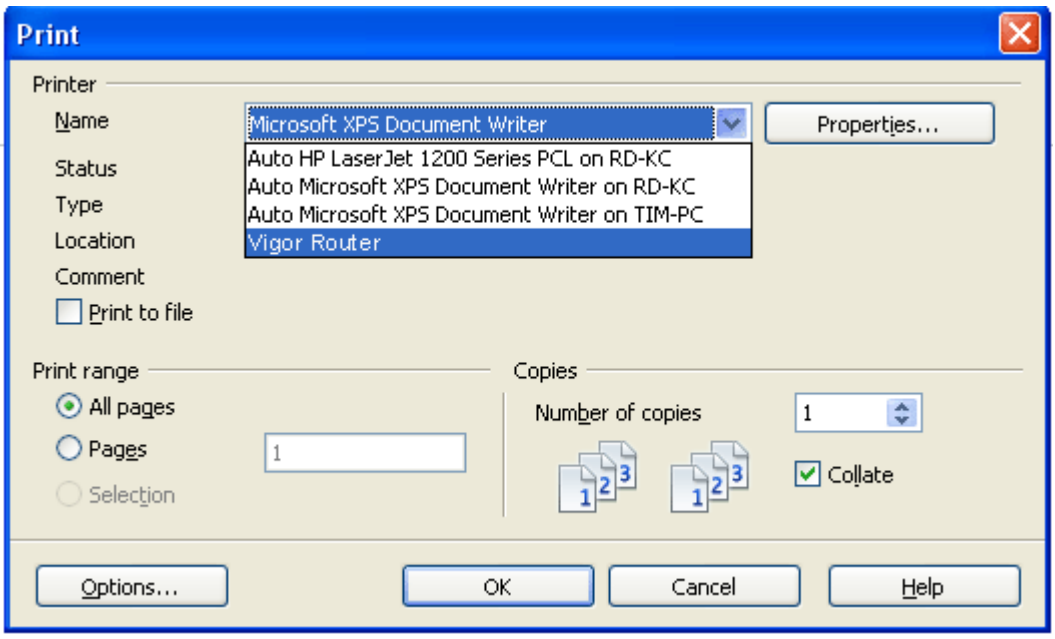
4. Next, open **Applications>>Bonjour**. Check the service that you want to use via Bonjour.



5. Open the DNSSD page again. The available items will be changed as the follows. It means the Vigor router (based on Bonjour protocol) is ready to be used as a printer server, FTP server, SSH Server, Telnet Server, and HTTP Server.



6. Now, any page or document can be printed out through Vigor router (installed with a printer).



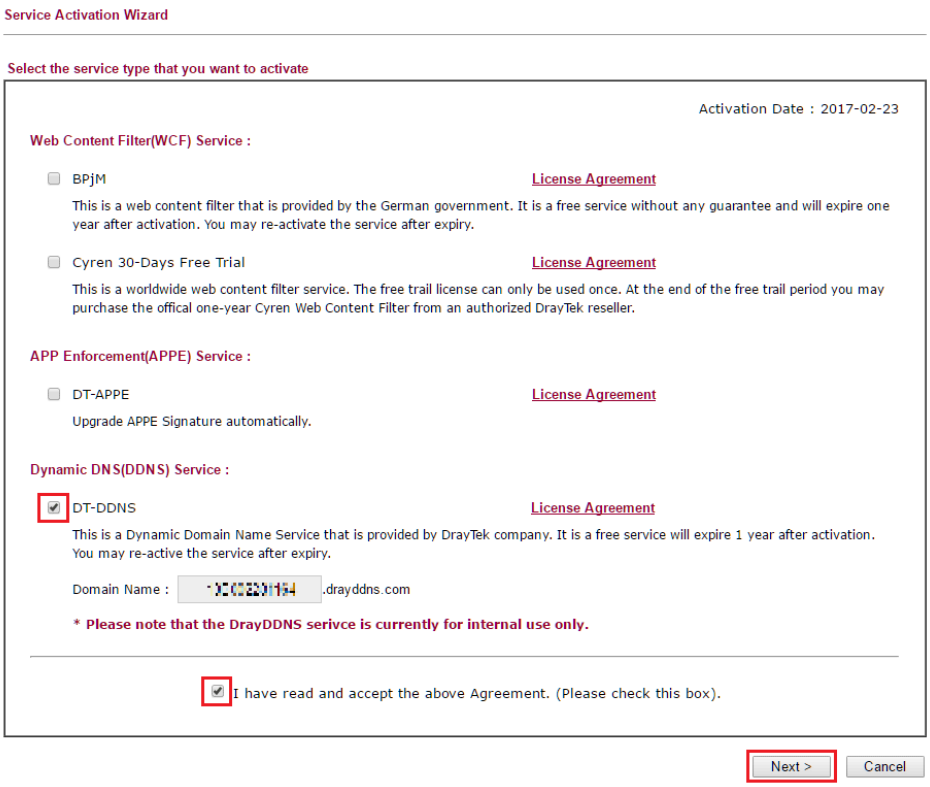
Application Notes

A-1 How to use DrayDDNS?

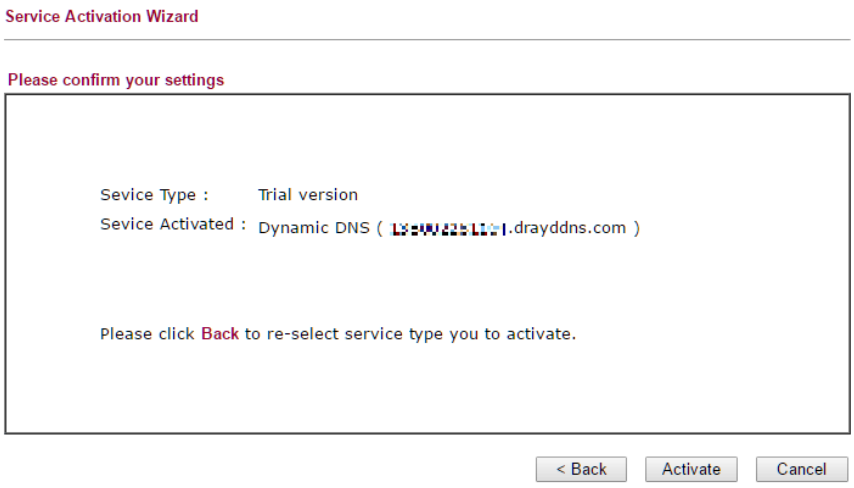
Vigor router supports various DDNS service providers, user can set up user-defined profile to update the DDNS even the service provider is not on the list. Now, DrayTek starts to support our own DDNS service - DrayDDNS. We will provide a domain name for each Vigor Router, this single domain name can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

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	---	---	Not Activated
APP Enforcement	---	---	Not Activated
DDNS	2017-02-23	2018-02-23	DT-DDNS

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

Configure DDNS Profile

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

   a. Tick **Enable Dynamic DNS Setup**

   b. Click an available profile index

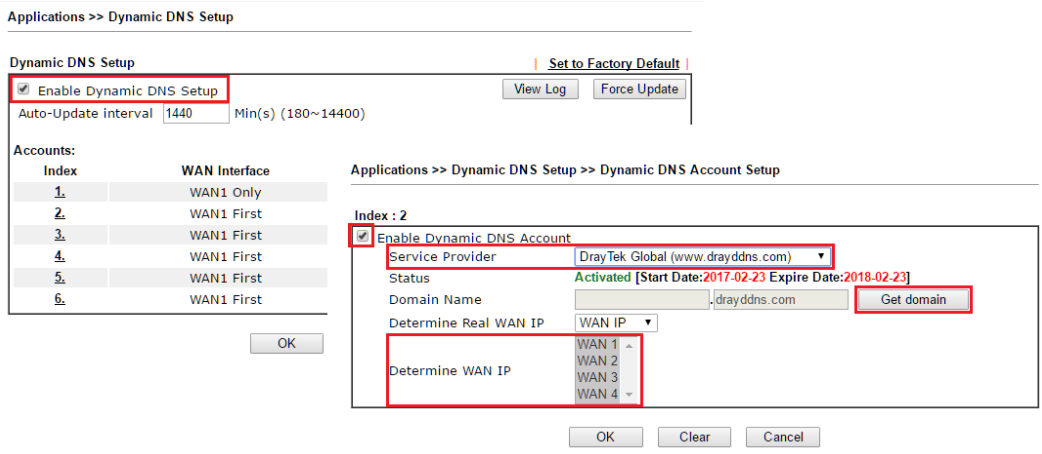
   c. Tick **Enable Dynamic DNS Account**

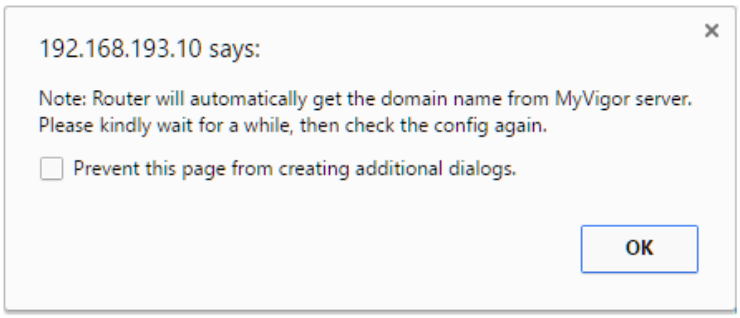
   d. Select **DrayTek Global (www.drayddns.com)** as **Service Provider**

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

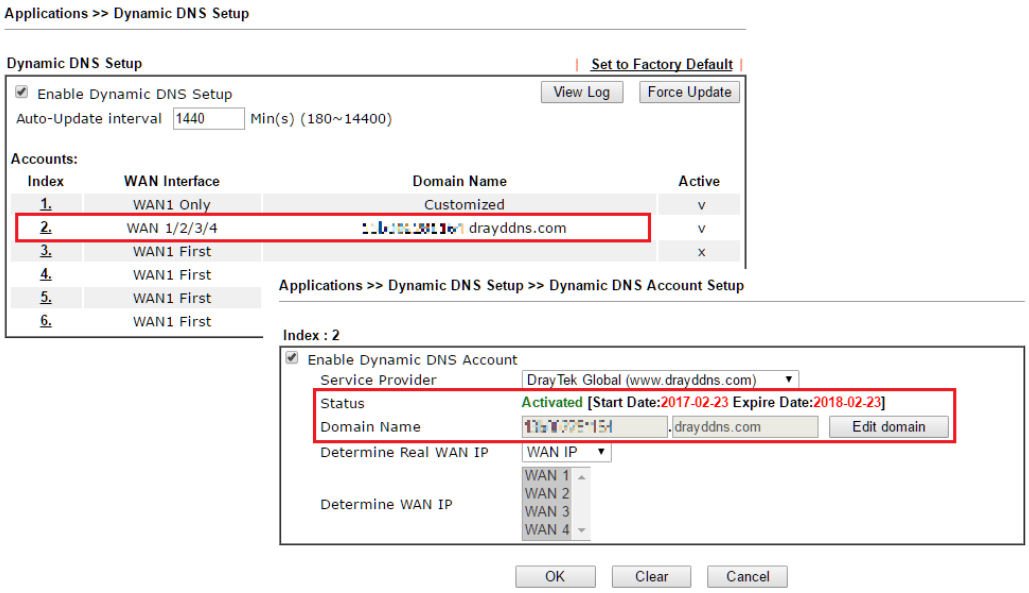
   f. Click **Get domain**

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





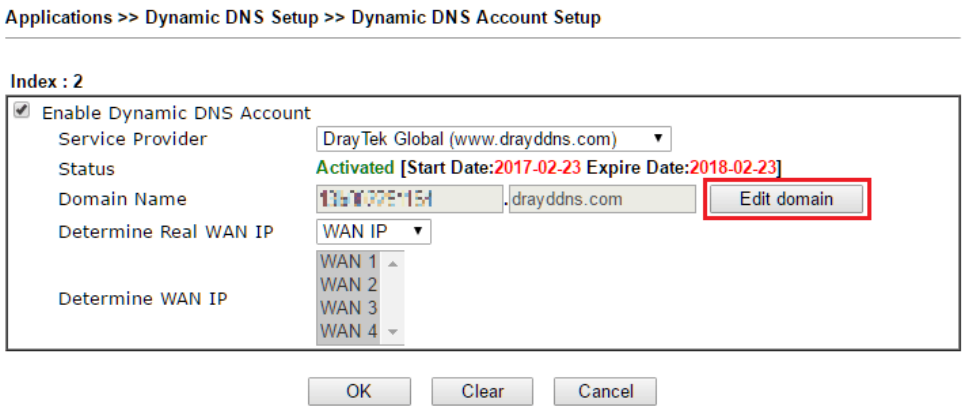
2. Wait few seconds for router to get the domain name, then, we can click the profile to check the information of license and domain name.



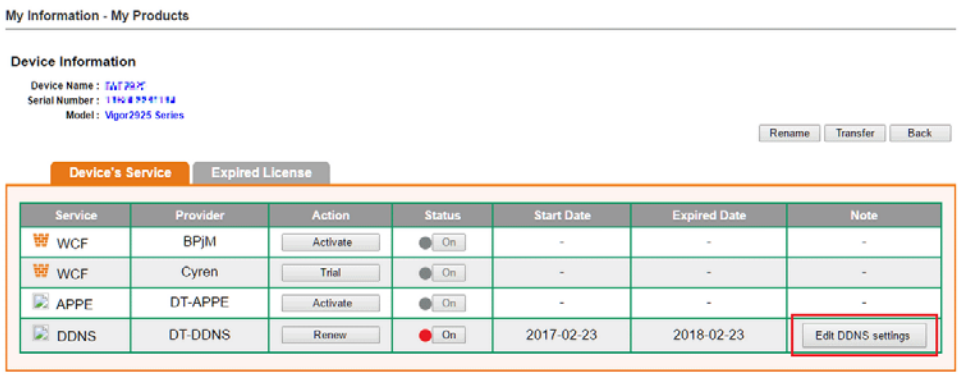
Modify Domain Name

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.

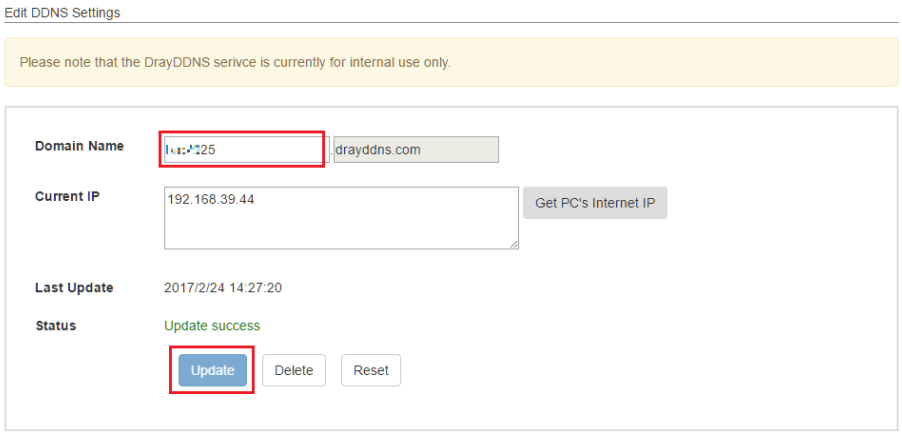
1. Please visit https://myvigor.draytek.com/ or go to **Applications >> Dynamic DNS Setup >> DrayDDNS** profile and click **Edit domain**.



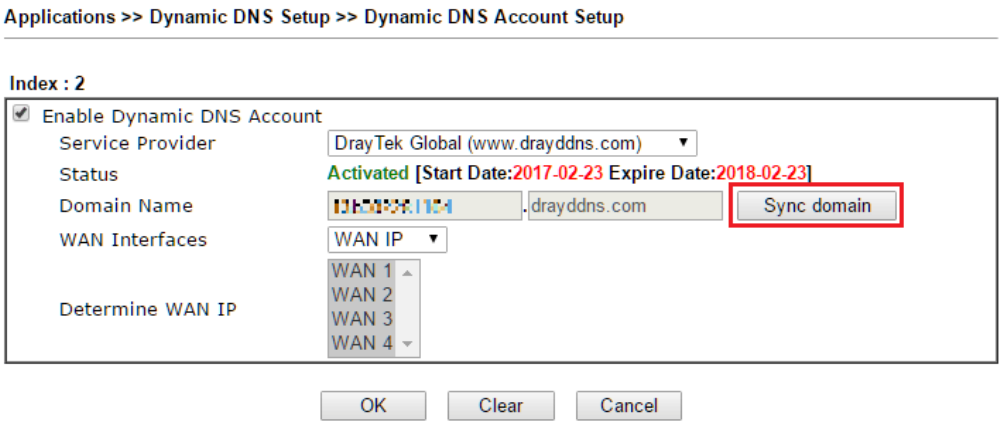
2. Log in to MyVigor Website, choose the profile, then click **Edit DDNS settings**.



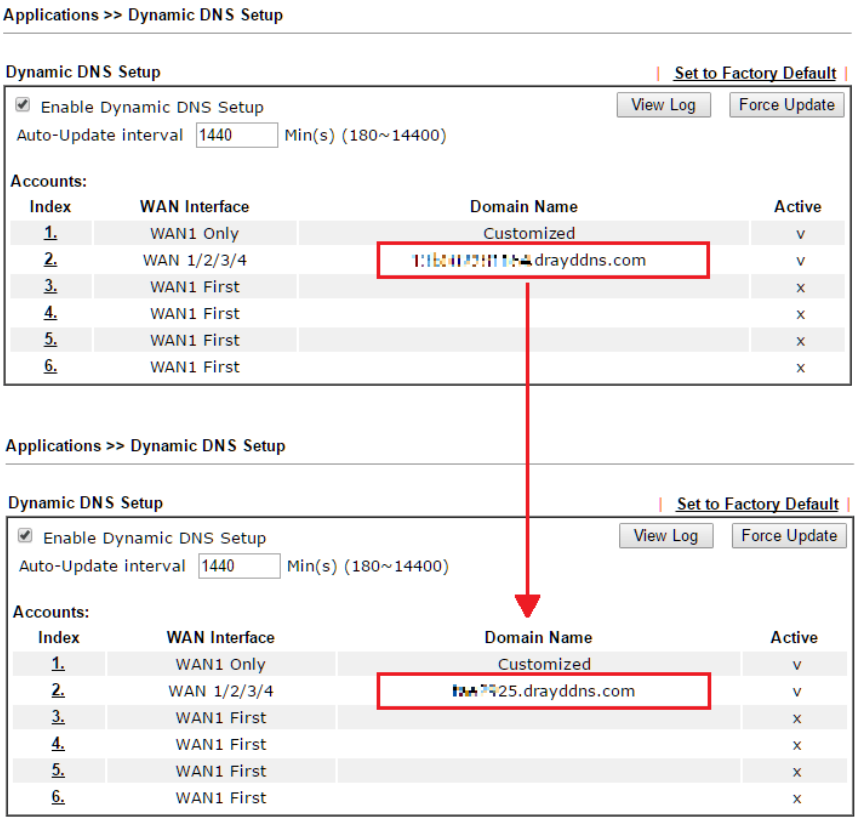
3. Input the desired **Domain name (e.g., XXXX25)** and click **Update.**



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

Online Status

Physical Connection — **System Uptime: 0day 2:25:59**

IPv4	IPv6

LAN Status	Primary DNS: 168.95.192.1	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets
10.1.7.1	2069	1036

WAN 1 Status — >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	iwiz	PPPoE	2:25:53	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
1.169.185.242	168.95.98.254	14851	9506	11281	912

Note that,

Username: jo***

Password: jo********

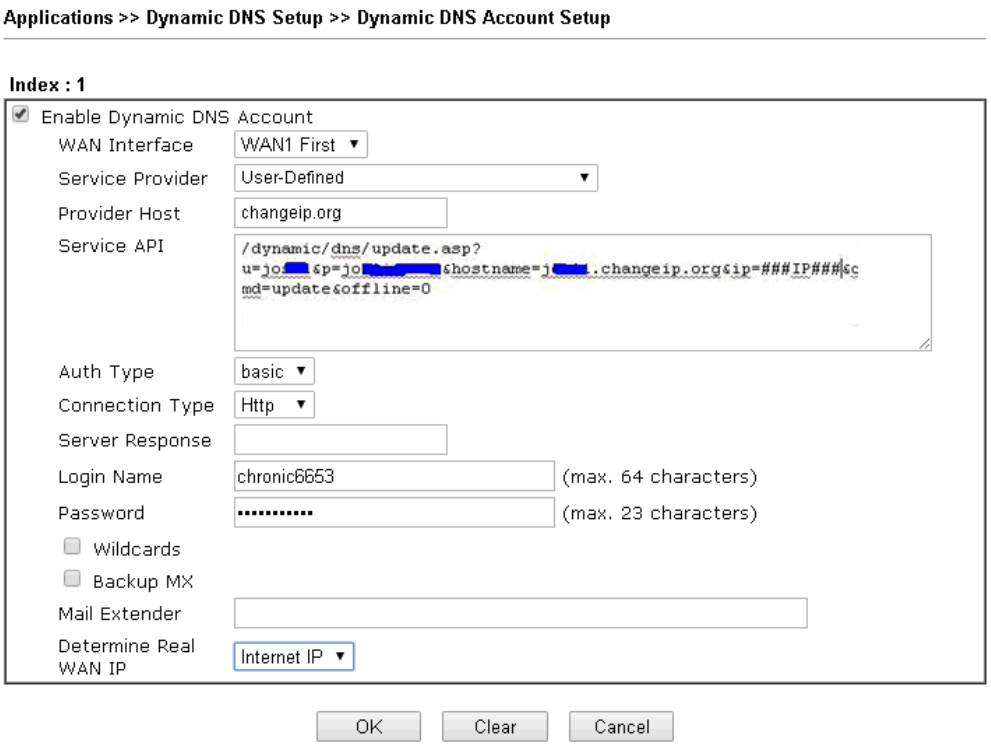
Host name: j*****.changeip.org

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 customized DDNS client.



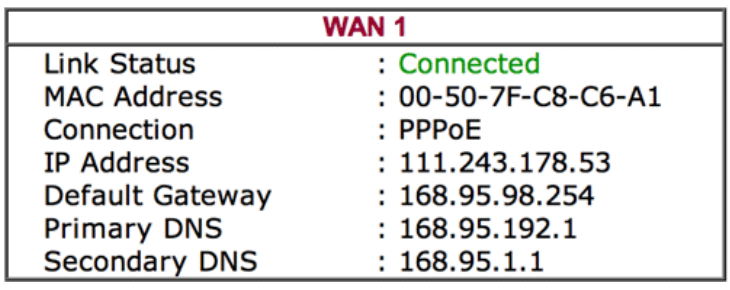
2. Set the Service Provider as **User-Defined**.

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



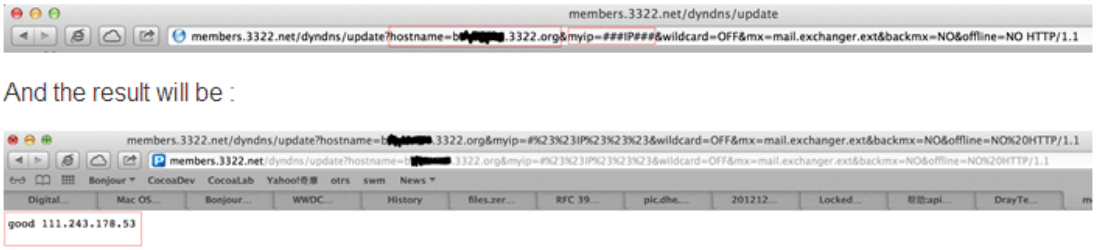
Username: bi*******

Password: 88********

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

WAN IP address: 111.243.178.53

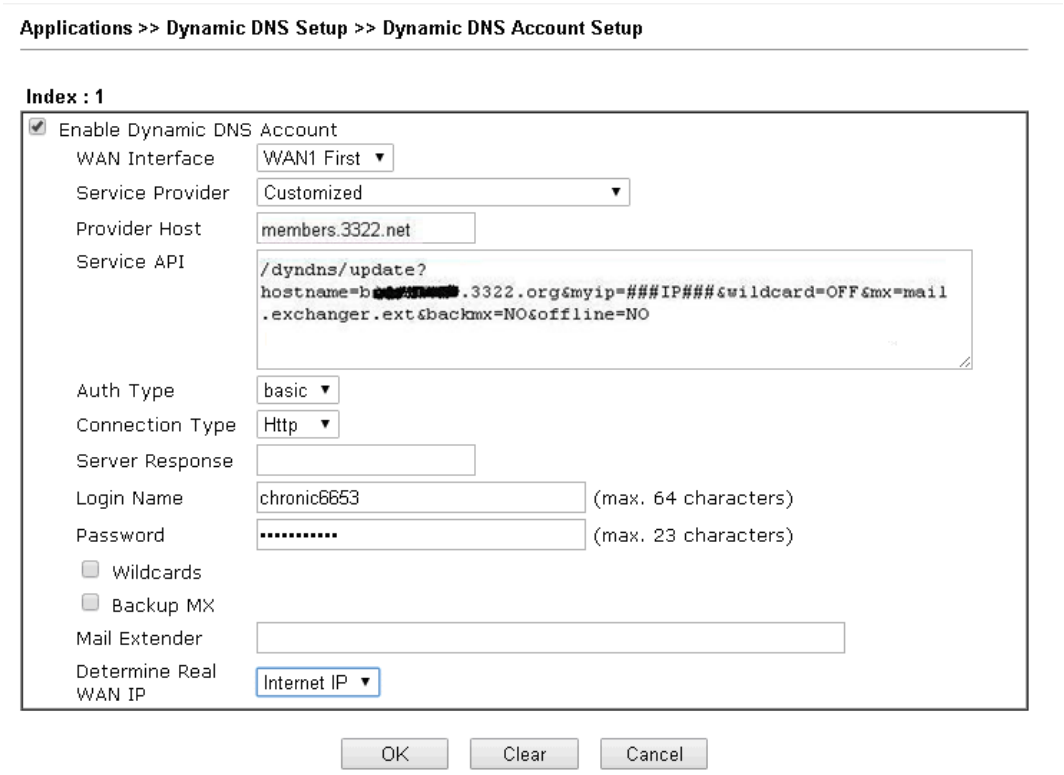
To update the IP to the DDNS server via editing the HTML script, we can Enter the following script on the browser:



"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 Customized DDNS client.



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

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

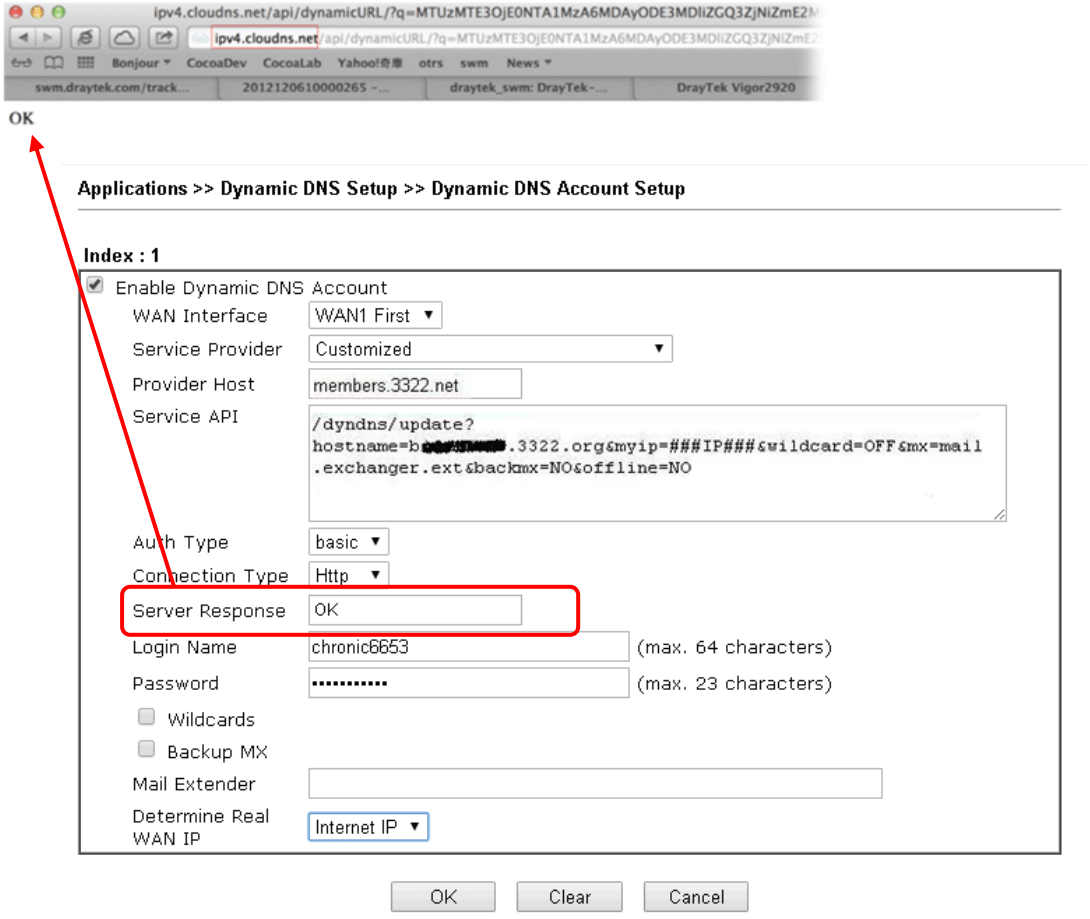
4. Set the Service API as:
/dyndns/update?hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail.exchanger.ext&backmx=NO&offline=NO

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-5 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:

Load Balance

You may manually create policies to balance the traffic across network interface.

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

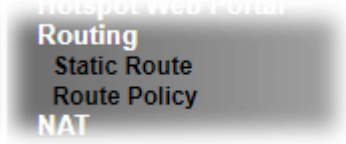
Packets will be sent through another Interface or follow another Policy when the original interface goes down (**Failover to**). Once the original interface resumes service (**Failback**), the packets will be returned to it immediately.

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 Note on www.draytek.com.

Web User Interface

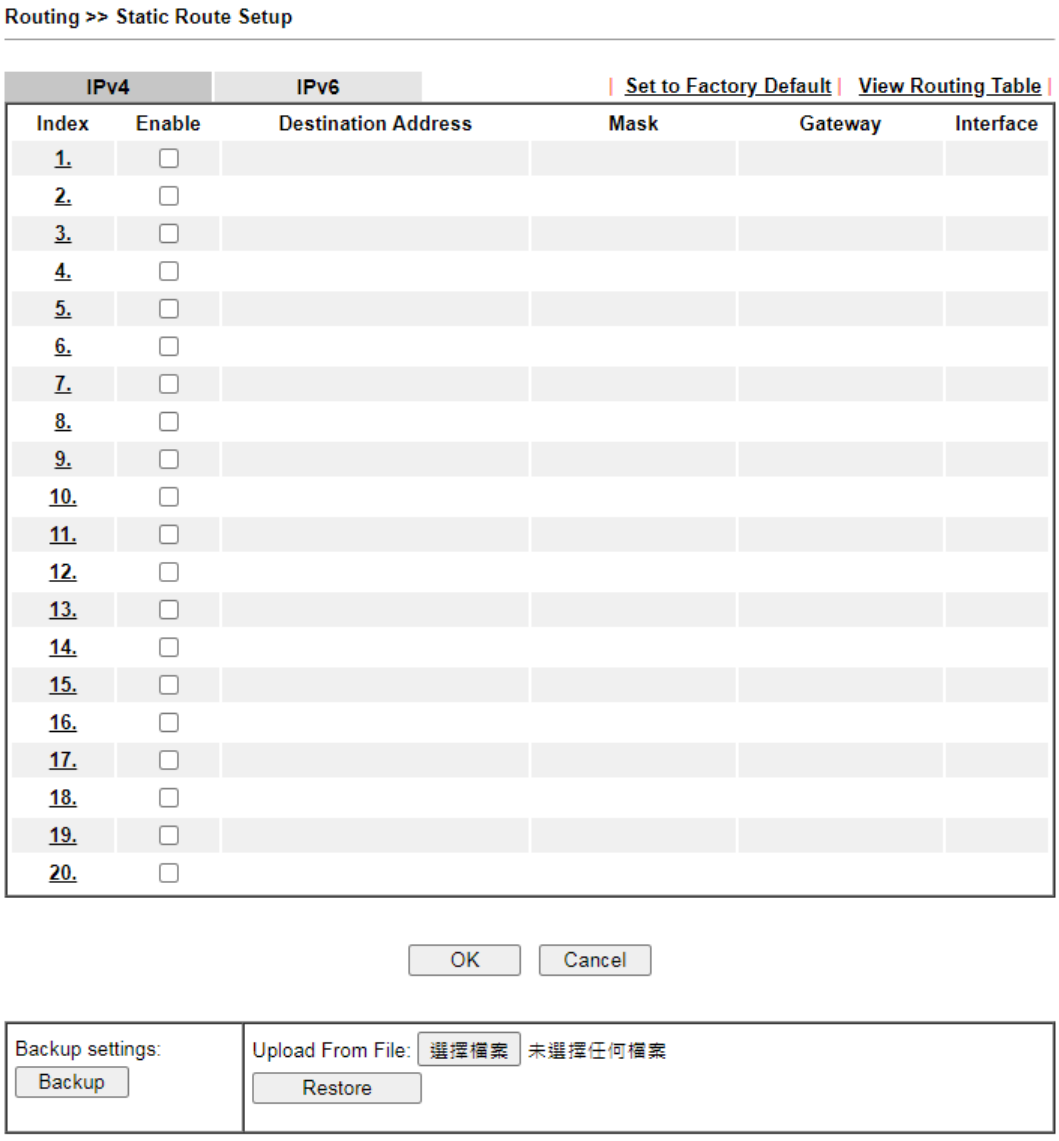


II-5-1 Static Route

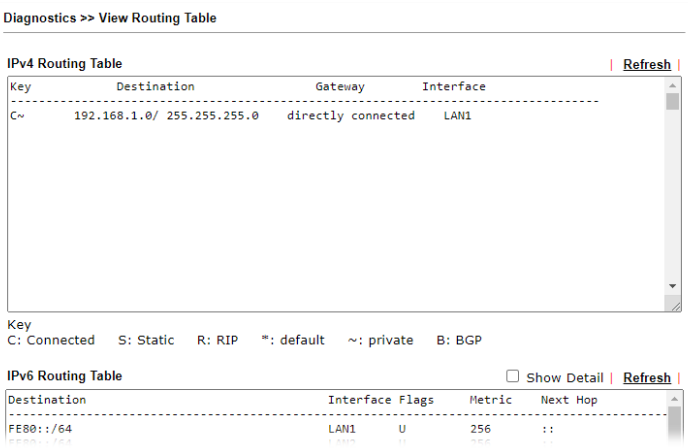
Go to **Routing** >> **Static Route**. You can create static routes so that traffic to specific IP addresses go through a particular LAN or WAN.

The Static Route Setup screen has separate tabs for IPv4 and IPv6. Select the appropriate tab to begin.

Static Route for IPv4



Available settings are explained as follows:

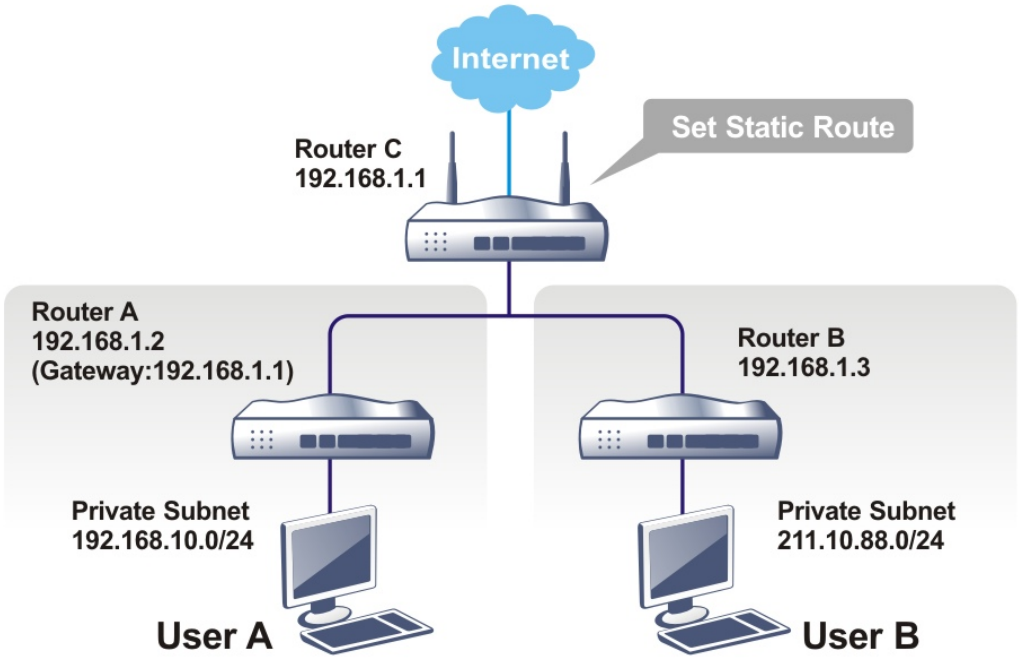
Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing Routing Table	Displays the routing table for your reference. 
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Enable	Enables or disables the static route.
Destination Address	Beginning destination address.
Mask	Subnet mask of the destination address.
Gateway	IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Interface	The LAN or WAN that should be used to contact the gateway.
Backup	Click it to backup the configuration of static route settings.
Restore	Click it to restore the configuration of static route settings. Before clicking, make sure upload the configuration file onto Vigor router.

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.

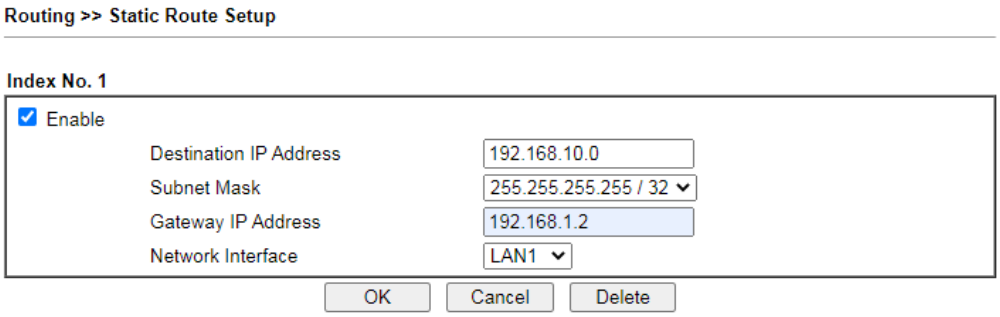
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



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.

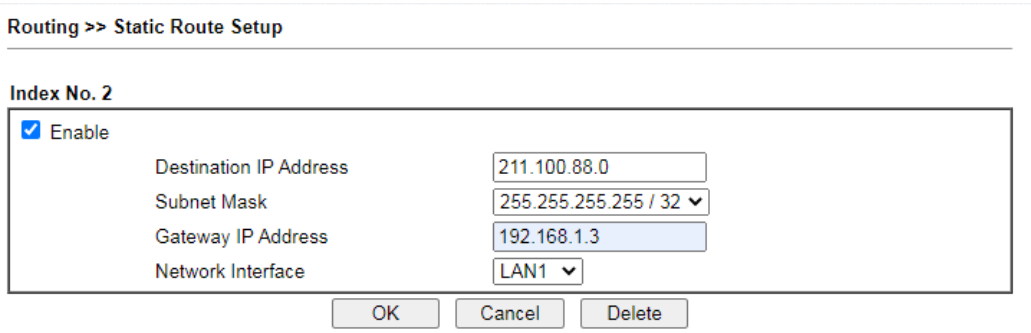
2. Click the **LAN >> Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



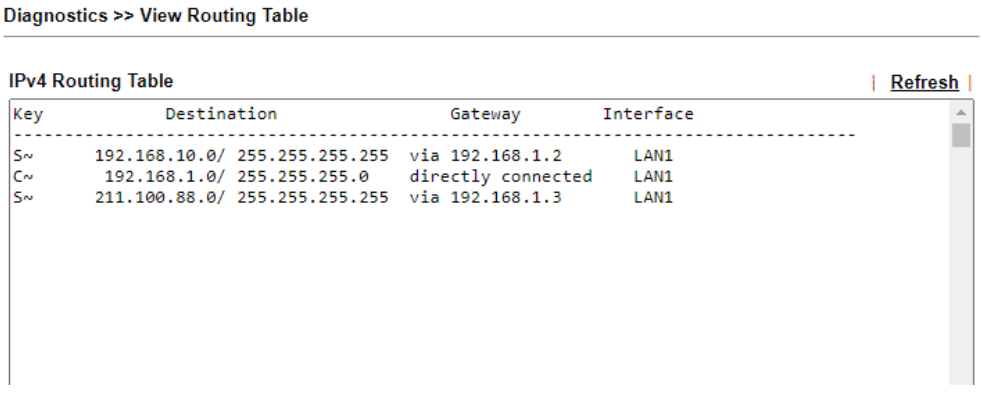
Available settings are explained as follows:

Item	Description
Enable	Enables or disables the static route.
Destination IP Address	Beginning destination address. Enter an IP address as the destination of the static route.
Subnet Mask	Subnet mask of the destination address. Enter the subnet mask for the static route.
Gateway IP Address	Enter the IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Network Interface	Use the drop down list to specify an interface for such static route. The LAN or WAN that should be used to contact the gateway.

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**.

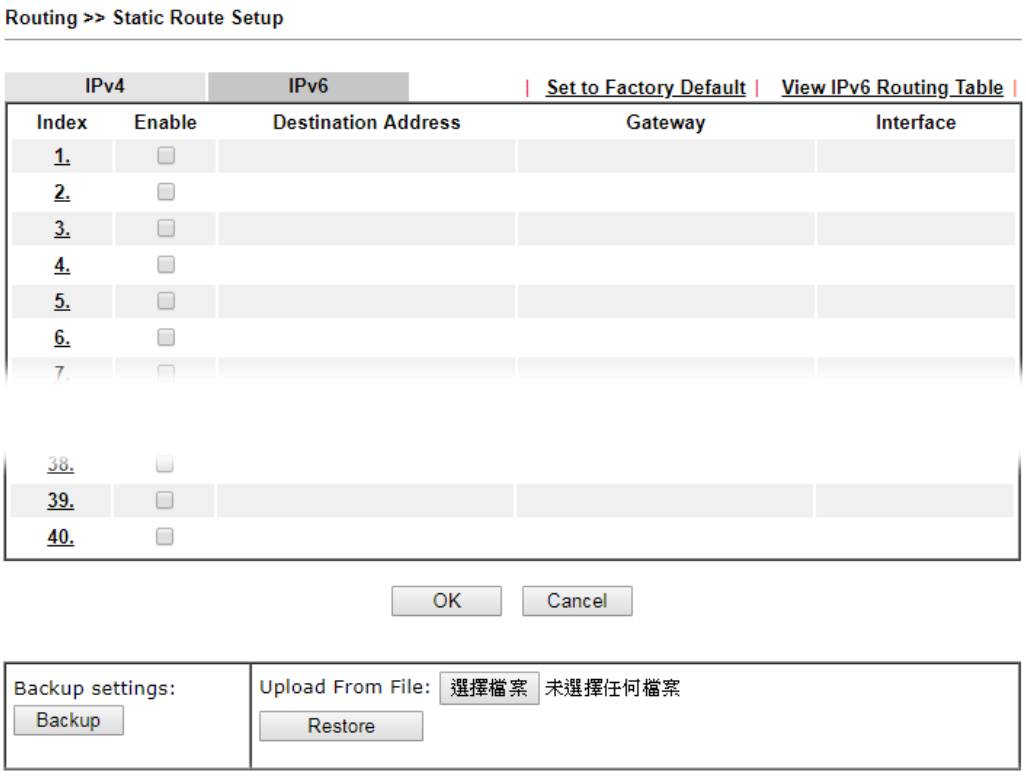


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



Static Route for IPv6

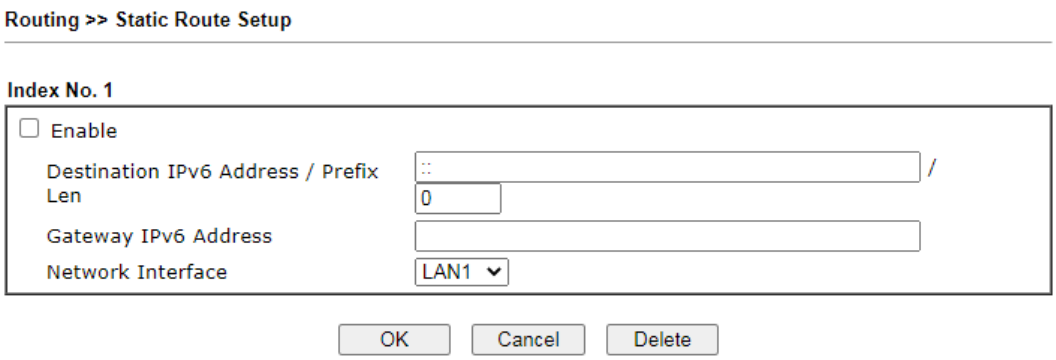
You can set up to 40 profiles for IPv6 static route. Click on a route index on the IPv6 tab to configure an IPv6 static route.



Available settings are explained as follows:

Item	Description
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Enable	Enables or disables the static route.
Destination Address	Beginning destination address.
Gateway	IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Interface	The LAN or WAN that should be used to contact the gateway.
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.
Backup	Click it to backup the configuration of static route settings.
Restore	Click it to restore the configuration of static route settings. Before clicking, make sure upload the configuration file onto Vigor router.

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



Available settings are explained as follows:

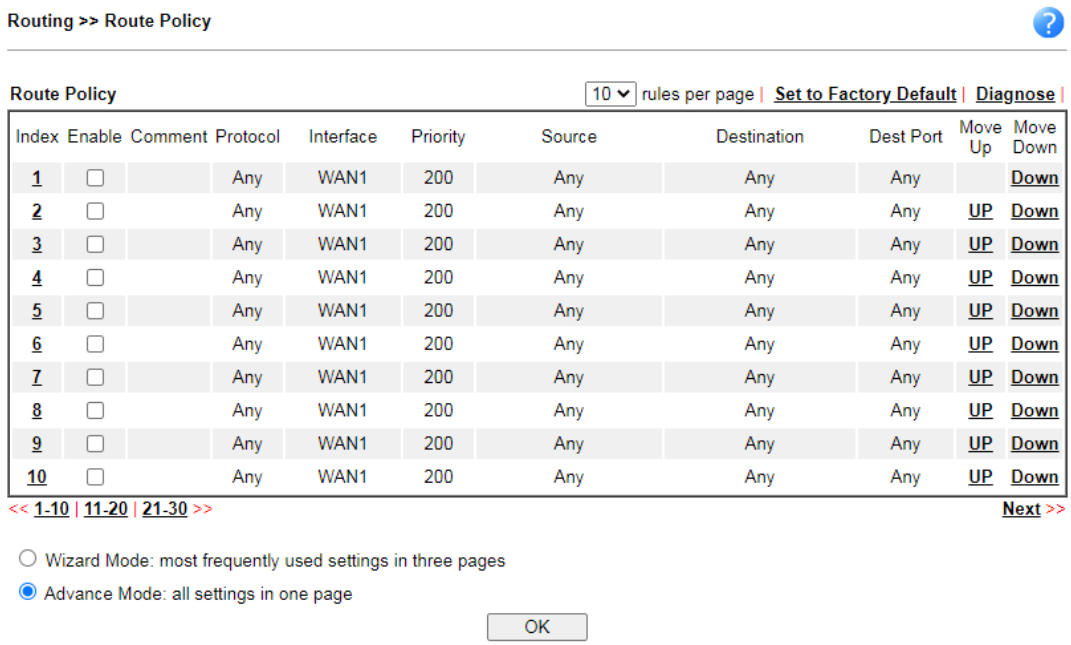
Item	Description
Enable	Enables or disables the static route.
Destination IPv6 Address / Prefix Len	Beginning destination address and the number of bits in the subnet mask of the destination IPv6 address. Enter the IP address with the prefix length for this entry.
Gateway IPv6 Address	IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Network Interface	The LAN or WAN that should be used to contact the gateway.

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

II-5-2 Route Policy

The Route 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 **Auto Load Balance** set in **WAN >> Internet Access**, 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.



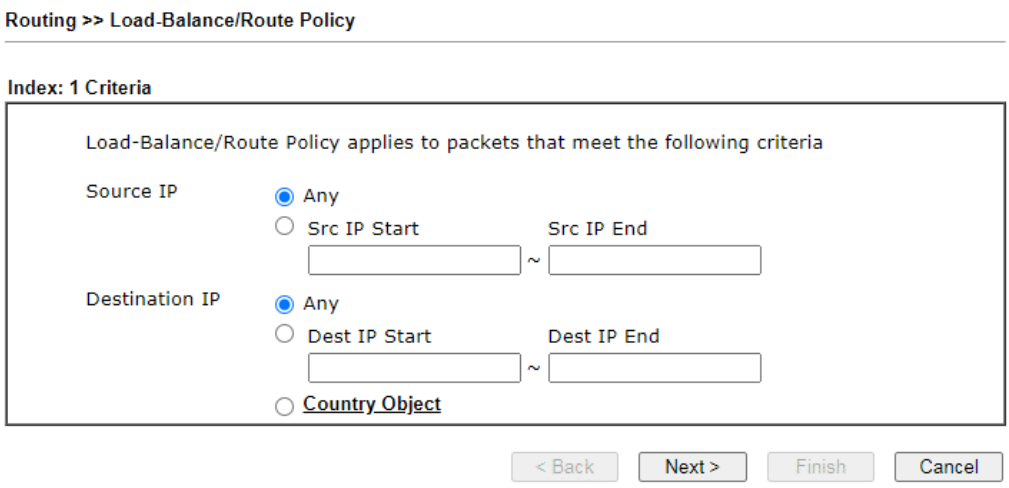
Available settings are explained as follows:

Item	Description
Rules per page	The number of rules to display on a single page.
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.
Source	The beginning and ending source IP address.
Destination	The beginning and ending destination IP address.
Dest Port	The beginning and 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.

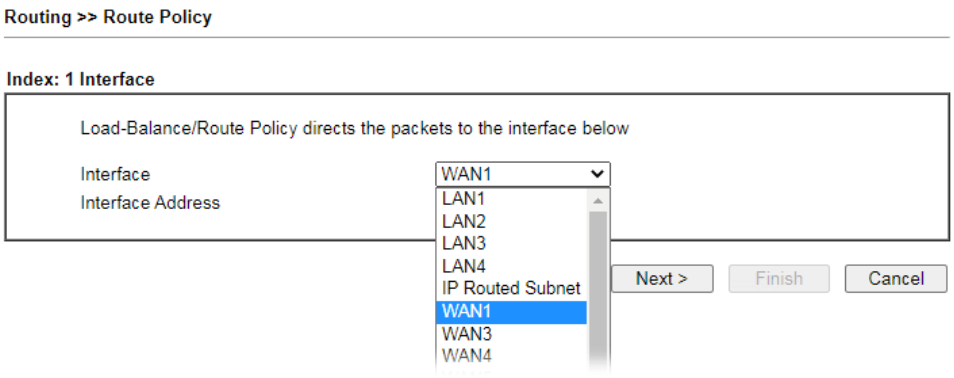
1. Click the **Wizard Mode** radio button.
2. Click **Index 1**. The setting page will appear as follows:



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. **Country Object** – Specify a country object. All the IPs coming from the country (countries) specified in the object will be passed through the WAN interface.

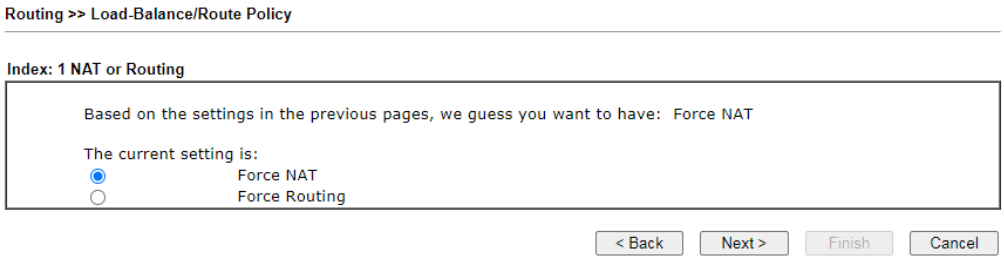
3. Click **Next** to get the following page.



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 DMZ Subnet. Packets match with the above criteria will be transferred to the interface chosen here. Select an interface from the list.

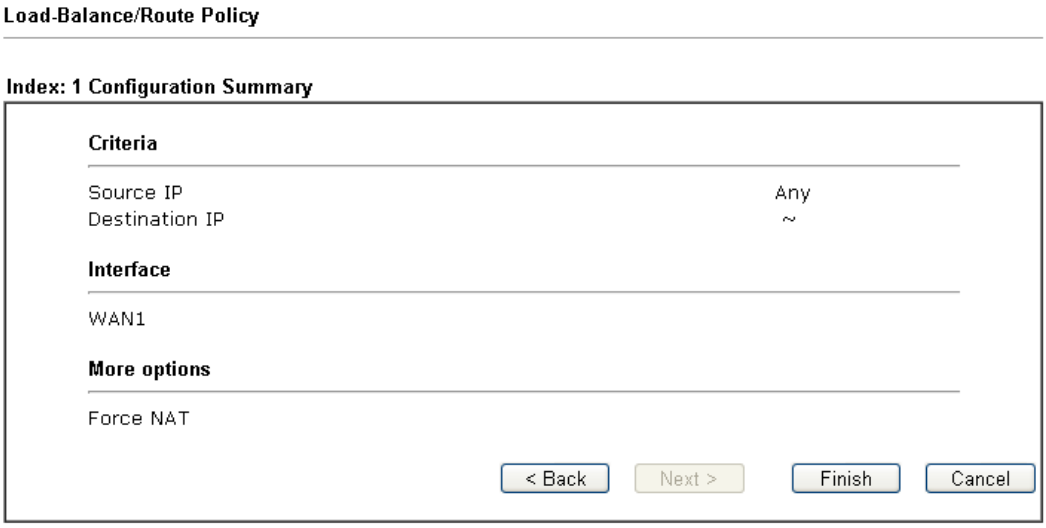
4. Specify an interface and click **Next.** The following page will appear only if you choose WAN1 ~WAN7 as Interface.



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.

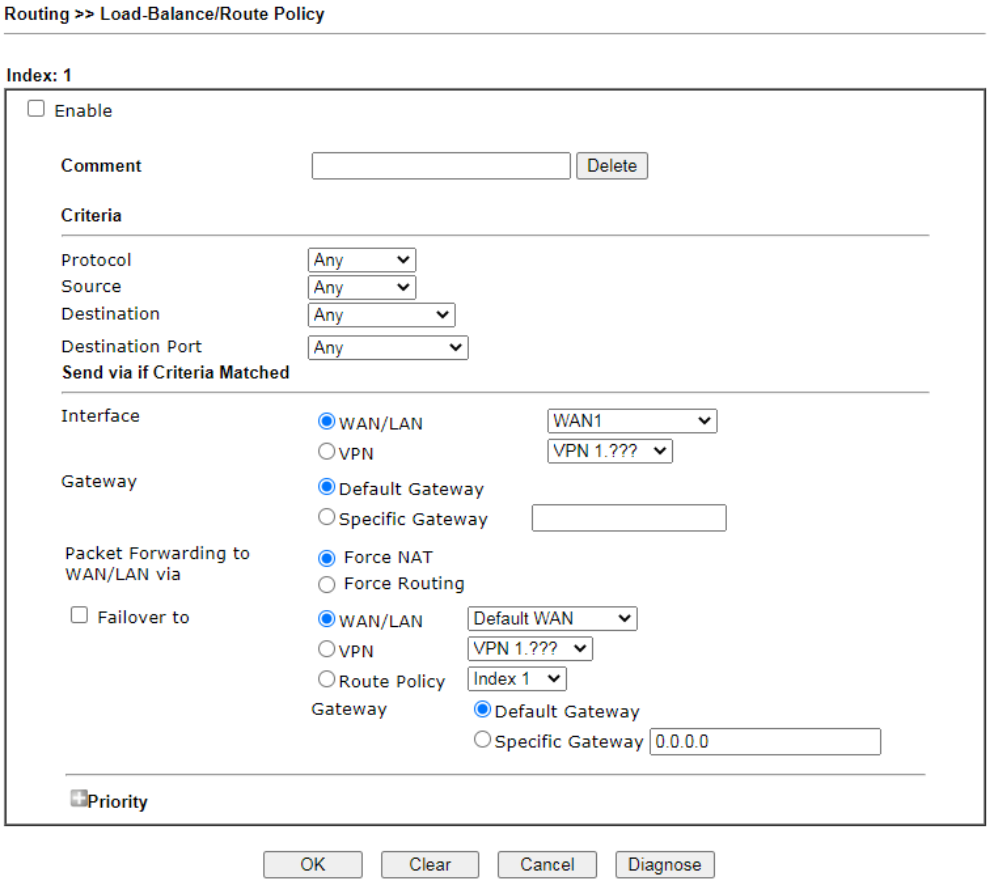
5. After choosing the mechanism, click **Next** to get the summary page for reference.



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.



Note:
Force NAT(Routing): NAT(Routing) will be performed on outgoing packets, regardless of which type of subnet (NAT or IP Routing) they originate from.

Available settings are explained as follows:

Item	Description
Enable	Select to enable rule and unlock all fields for configuration.
Comment	Type a brief explanation for such profile.
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

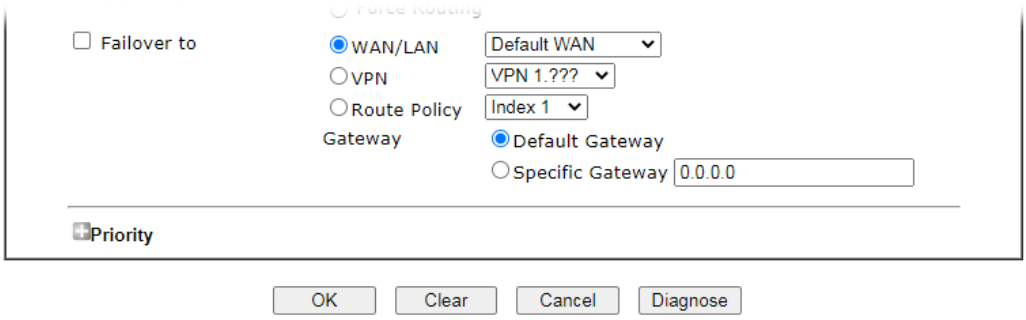
	defined by the specified network IP address and subnet mask. - **Network** – Enter an IP address here. - **Mask** – Use the drop down list to choose a suitable mask for the network. ● **IP Object / IP Group** – Use the drop down list to choose a preconfigured IP object/group. **Destination -** Destination 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. ● **Country Object** – Use the drop dwon list to choose a preconfigured object. Then all IPs within that country will be treated as the destination IP. **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 via 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). **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. **Packet Forwarding to WAN/LAN via** – When you choose LAN/WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. ● **Force NAT** - The source IP address will not be used to connect to the remote destination. Network Address Translation (NAT) will be used, where a common IP address will be used. ● **Force Routing** - The source IP address will be preserved when connecting to the remote destination. **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 IP** – 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

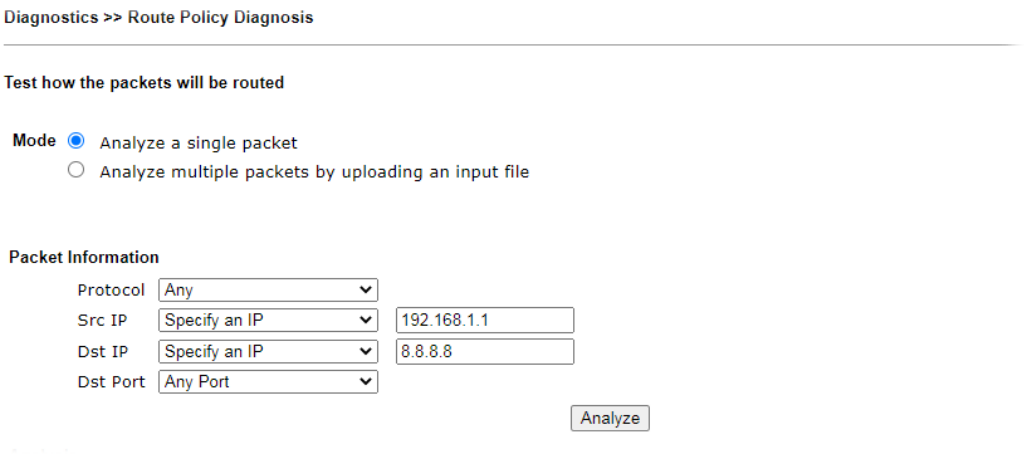
The Diagnose function allows you to determine how a specific type of traffic from a host to a destination will be routed, and which routes, route policies and load balance rules match the criteria of the traffic.



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.

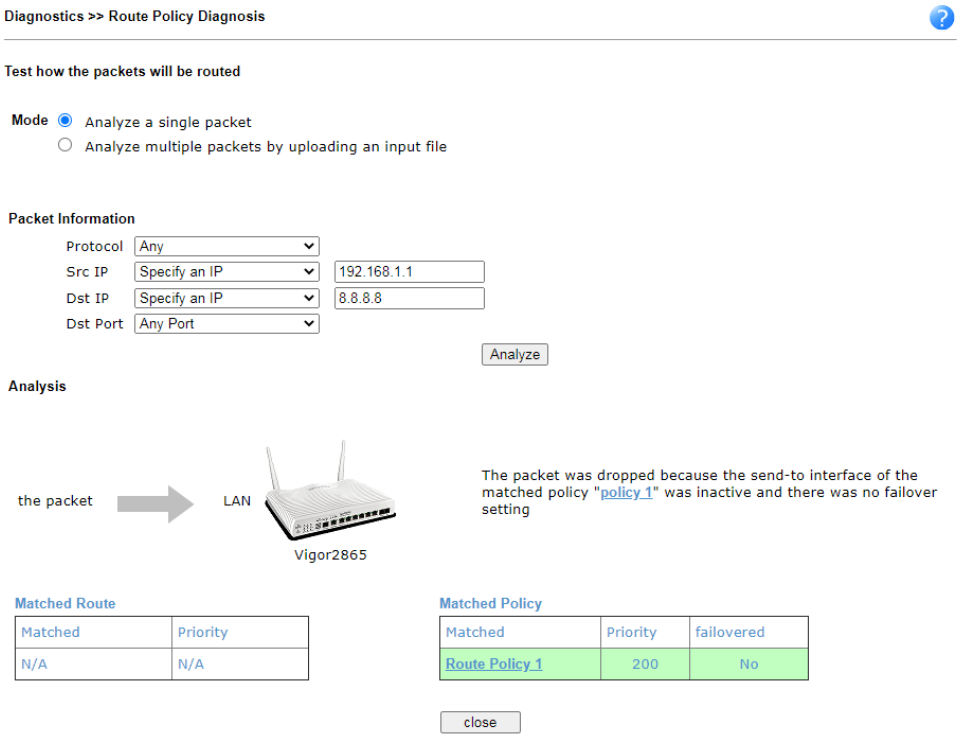


Available settings are explained as follows:

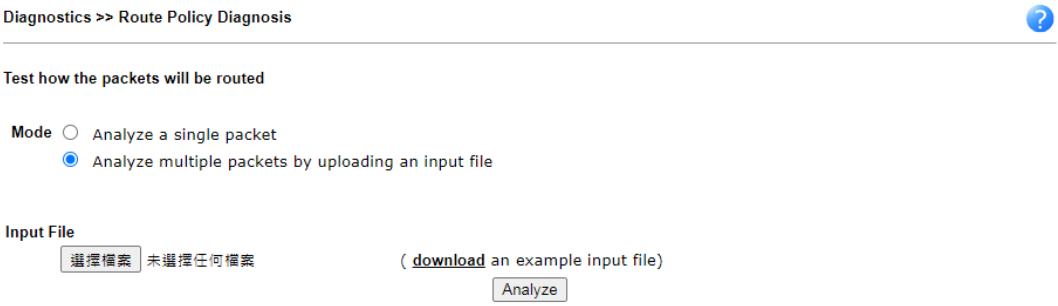
Item	Description
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. **Protocol -** Specify a protocol for diagnosis. **Src IP** – IP address of host where the traffic originates. ● **Specify an IP** - One source IP address. ● **Any IP**- Source IP address is not specified. Any IP from LAN 1/LAN 2/LAN 3/LAN 4. ● **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
N7	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

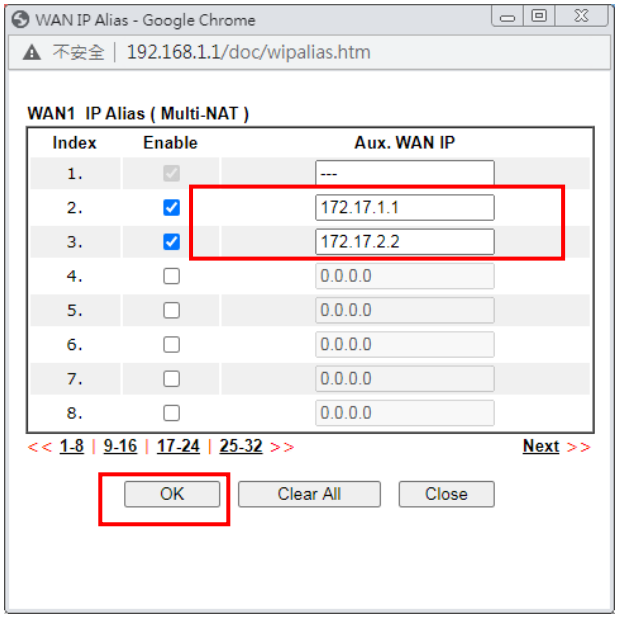
Application Notes

A-1 How to set up Address Mapping with Route Policy?

Address Mapping is used to map a specified private IP or a range of private IPs of NAT subnet into a specified WAN IP (or WAN IP alias IP). Refer to the following figure.

This document introduces how to set up address mapping with Route Policy. When a WAN interface has multiple public IP addresses, Administrator may specify the outgoing IP for certain internal IP address by a Route Policy.

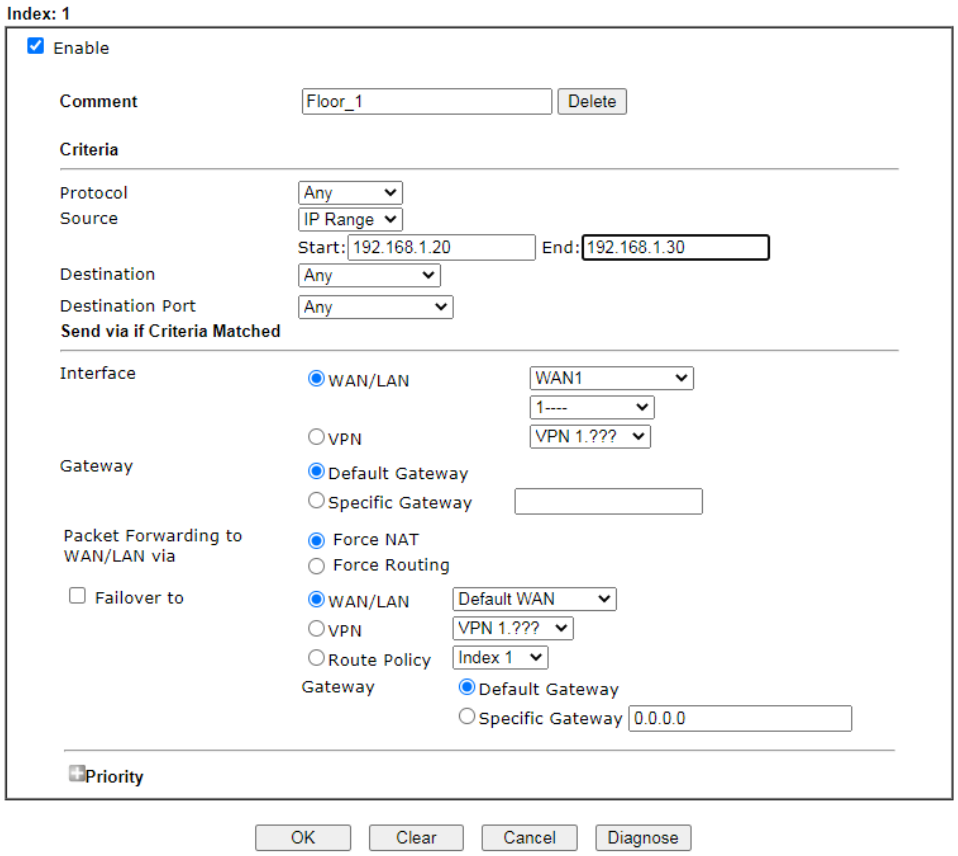
1. Set up WAN IP Alias. Go to **WAN >> Internet Access >> Details** Page, and click on **WAN IP Alias** button.



- Check **Enable**.
- Enter the WAN IP address.
- Click **OK** to save.

After setting up the WAN IP Alias, the IP addresses will be shown in the drop-down list of Interface in Route Policy setting.

2. Go to **Routing>> Route Policy**. Create a Route Policy for specific IP address to send from specific WAN IP Address.



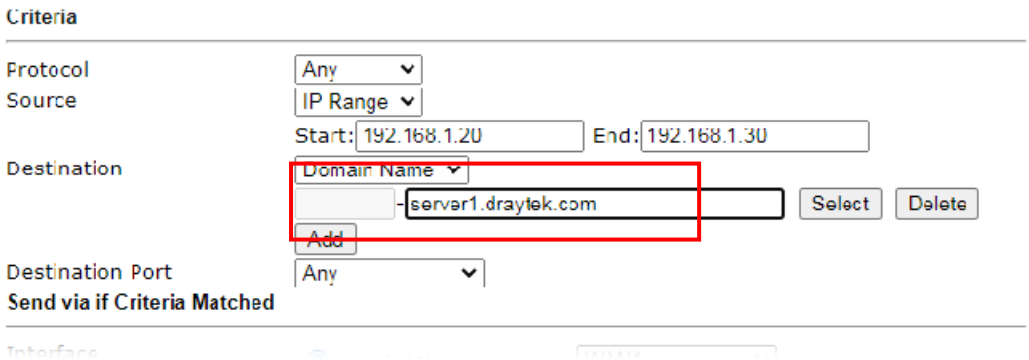
- Enable this policy.
- Enter **Source IP** as the range of private IP address.
- Leave the Destination IP and Port as **Any**.
- Select **Interface** as WAN, and then select Interface address from the drop-down list. (The List can be edited in **WAN IP Alias** setting.)
- Enable **Failover to** other WAN so the traffic will be sent via other Interface when the path fails. But do not enable this option if you want the traffic only to use a designated IP address.
- Click **OK** to save.

3. After the above configuration, packet source from the range between 192.168.1.20 and 192.168.1.30 sent to the Internet will use the public IP 172.17.1.1.

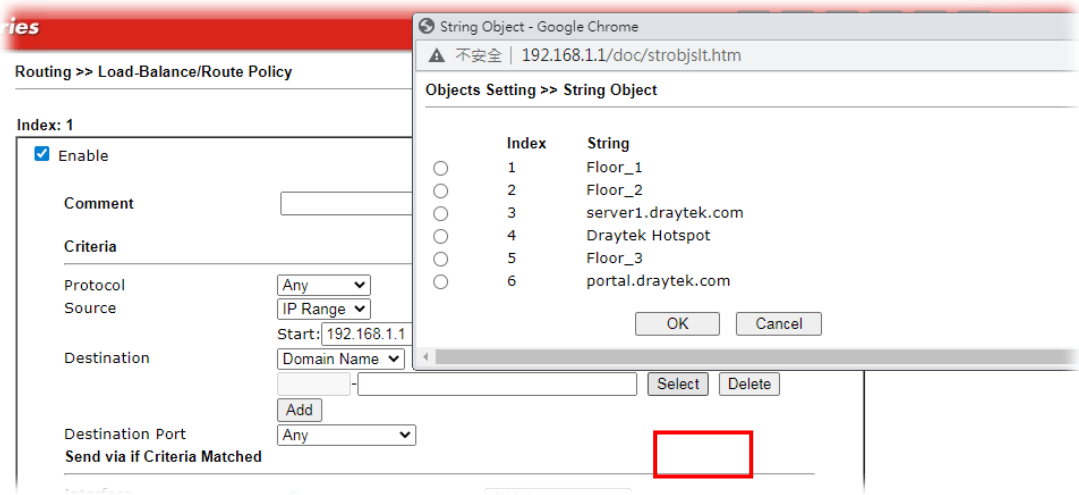
A-2 How to use destination domain name in a route policy?

Route Policy supports using a domain name as destination criteria. It provides a more direct way to set up route polices if the network administrator is trying to specify the gateway for the traffic that destined for a certain website.

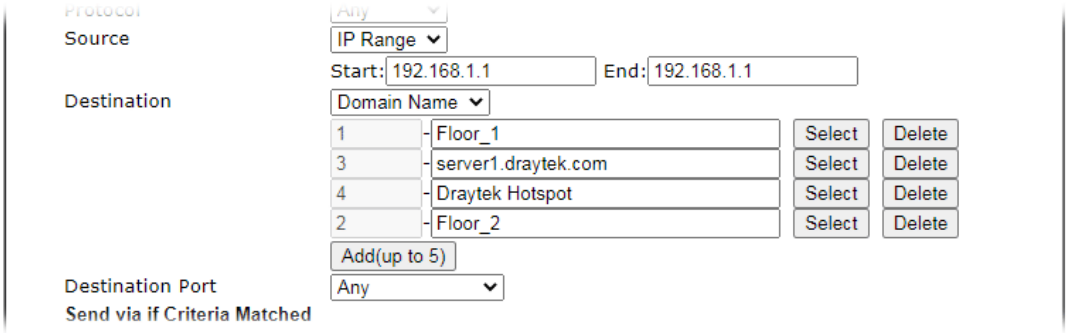
To use a destination domain name as criteria, just select **Domain Name** as **Destination** in Criteria, and enter the domain name in the empty field.



Or you may click **Select**, and use a string that is pre-defined in Objects Settings >> String Object as the domain name.

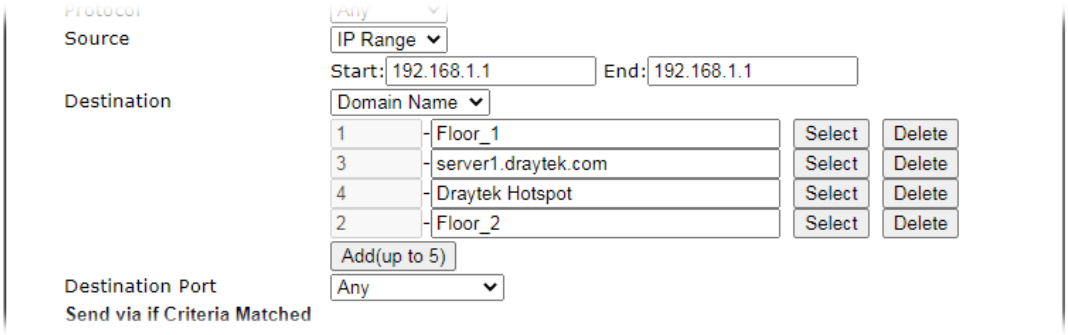


Click **Add** too add more domain names, we can set up to 5 domain names in one route policy.

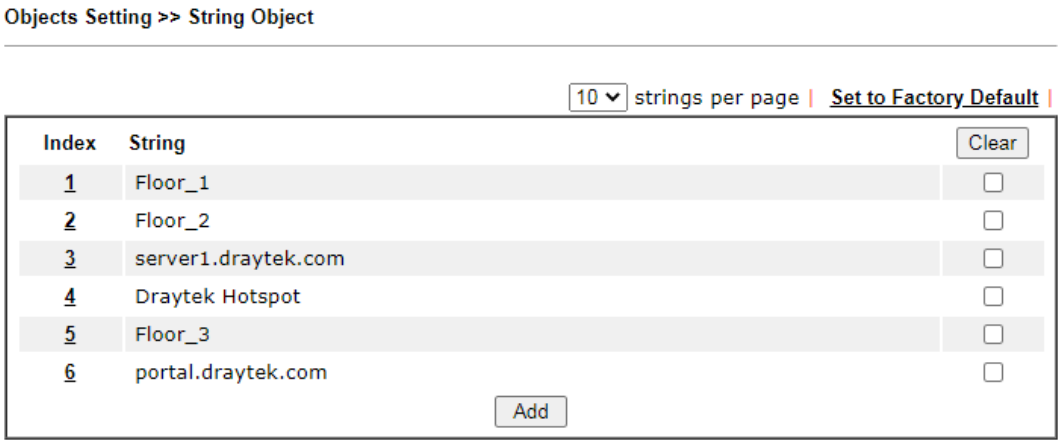


Auto-create String Objects

If you manually enter the domain name in a route policy, after clicking **OK** to apply the route policy, those domain names will be given a number.



That means the router has automatically created string objects for those domain names, so that they can be used in other route policies or other functions.

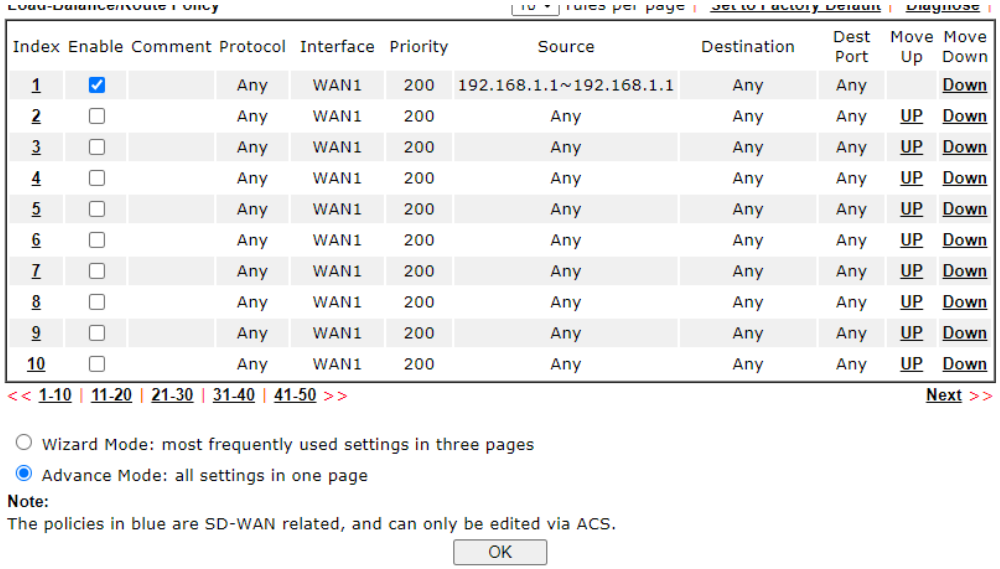


A-3 Introduction to Route Policy

This document introduces the Route Policy. This feature allows network administrator to manage the outbound traffic more specifically.

The Policy set in Route Policy always has higher priority than Default Route and Auto Load Balance set in **WAN >> General Setup**, and always has lower priority than the Firewall Rules. Administrator may also define a priority to this policy.

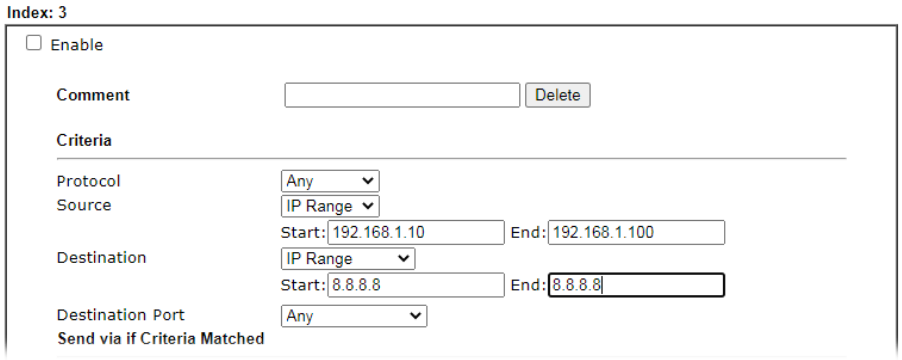
To configure Route Policy, go to **Routing>> Route Policy**. The following image is a screen-shot of Route policy page. It lists all the policies and shows whether the policy is enabled, what are the criteria to match, and through which the interface should the traffic to go if the criteria are matched, and also its priority.



Index	Enable	Comment	Protocol	Interface	Priority	Source	Destination	Dest Port	Move Up	Move Down
1	☑		Any	WAN1	200	192.168.1.1~192.168.1.1	Any	Any		Down
2	☐		Any	WAN1	200	Any	Any	Any	UP	Down
3	☐		Any	WAN1	200	Any	Any	Any	UP	Down
4	☐		Any	WAN1	200	Any	Any	Any	UP	Down
5	☐		Any	WAN1	200	Any	Any	Any	UP	Down
6	☐		Any	WAN1	200	Any	Any	Any	UP	Down
7	☐		Any	WAN1	200	Any	Any	Any	UP	Down
8	☐		Any	WAN1	200	Any	Any	Any	UP	Down
9	☐		Any	WAN1	200	Any	Any	Any	UP	Down
10	☐		Any	WAN1	200	Any	Any	Any	UP	Down

To set up a Route Policy, just click on an Index number. At the bottom of the page, there are two configuration modes could be choose: the Wizard Mode provides a simple and basic configuration; while Advance Mode allows more options. Here we select Advance Mode.

1. First, set the criteria of the packets to apply this policy.



   a. Select a Protocol.

   b. Enter the Source IP address range, the Source IP could be a single address if the Start and End are the same.

   c. Enter the Destination IP address range.

   d. Select the Destination Port.

   The above configuration is an example that if a packet is sent from192.168.1.10~192.168.1.100 to 8.8.8.8, no matter what the protocol or destination port is, it will follow this route policy.

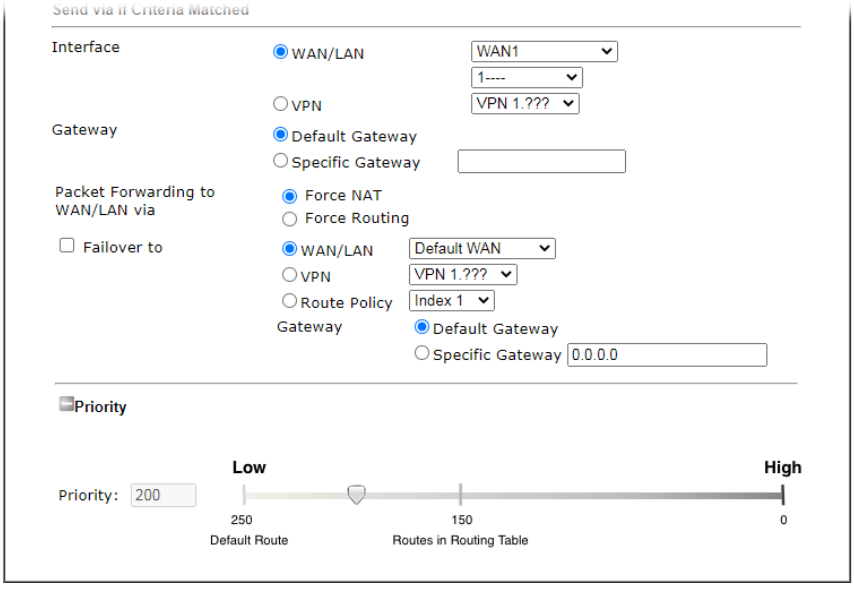
2. Next, we select an interface and gateway through which should the packet be sent if it matches the criteria.

a. Select an Interface.

b. Select a Gateway IP. Note that if Interface is chosen to be a LAN, it is necessary to designate a specific gateway.

The above configuration is an example that if a packet matches the criteria of this Route Policy, it will be sent to the default gateway then the destination through VPN1.

3. In **Advance Mode**, if the Interface is selected as WAN or VPN, there are some more options:



- **Failover to**: Enables packet to be sent through other Interface or follow another Policy when detects a path failure in the original interface. The above configuration indicates that the packets will be sent through WAN2 when the original route is disconnected.
- **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 packet 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 want the traffic go via the primary interface as soon as possible.
- **Priority**: Administrator may set priority between 1 and 249 for this Route policy, where smaller number indicates higher priority. When two policies are having the same priority, the first (according to the policy index order) matched policy will be implemented.

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 (2.4GHz/5GHz)

This function is available on wireless models only (models with –n or –ac suffixes).

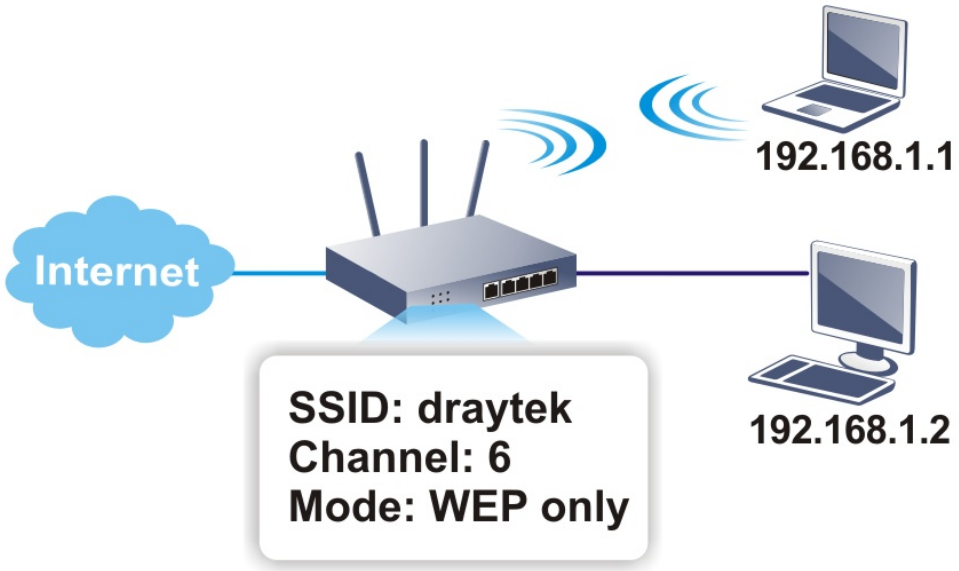
In recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches virtually every location on earth. Billions of people exchange information daily with wireless communication products. The Vigor2860 series of wireless routers (with "n", "n-plus", or "ac" in the model name), designed with maximum flexibility and efficiency in mind, is ideal for use in a small office or home. In a business environment, any authorized personnel can bring a WLAN-equipped tablet, PDA or notebook into a meeting room and connect to the network without drilling holes through walls or tearing up flooring to lay a clot of LAN cabling. Wireless networking enables high mobility so WLAN users can access all LAN resources in the same manner just as they would on a wired LAN, but without the cables.

All Vigor2135 wireless routers support 2.4 GHz. ac models add support for 5 GHz frequencies. Channel operations of 20 and 40 MHz are possible on the 2.4 GHz spectrum, and 20, 40 and 80 MHz are supported on the 5 GHz spectrum. "ac" models (2865ac) support data rates of up to 1.3 Gbps on 802.11ac 80 MHz channels, whereas "n" models support data rates of up to 300 Mbps on 802.11n 40 MHz channels.

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 wireless network settings, such as SSID, channels, encryption protocol, can be configured in General Settings.



Multiple SSIDs

Vigor wireless routers support up to four SSIDs (Service Set Identifiers) per band for wireless connections. A service set is a group of wireless network clients that have the same

networking parameters. Each service set can be configured to have a unique name (SSID) and specific download and upload rates, and can be used by different categories of users.

Real-time Hardware Encryption

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

Complete Security Standard Selection

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

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

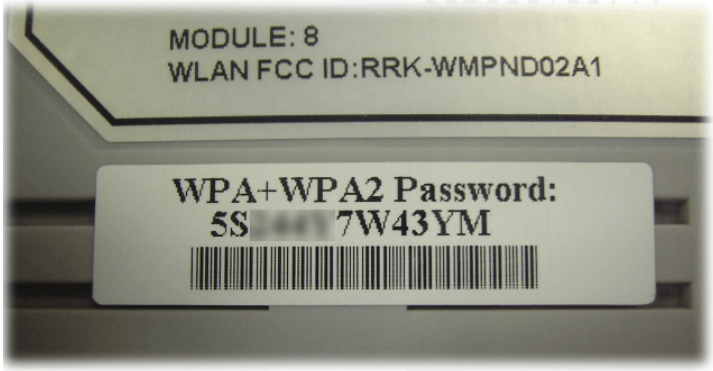
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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

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

Info

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



Separate the Wireless and the Wired LAN- WLAN Isolation

WLAN Isolation allows you to separate wireless LAN clients from wired ones, either for the purpose of quarantining certain users, or restricting their access to LAN resources. When WLAN isolation is enabled on an SSID, its users will only be able to connect to the WAN (i.e., internet). This is ideal for providing visitors Internet access while keeping the wired network secure.

For the highest degree of security, you may consider adding firewall rules to filter access by MAC address.

Manage Wireless Stations - Station List

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

DFS Restrictions

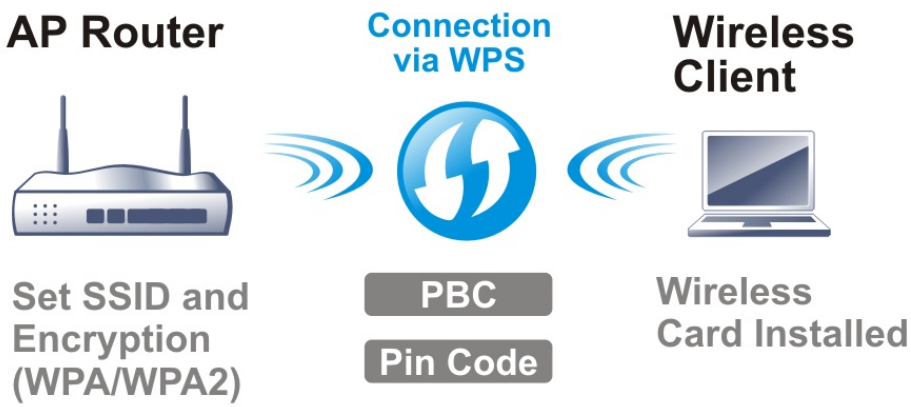
In certain parts of the world, there are radar systems that are primary users of the 5 GHz band. WLAN equipment on the 5 GHz band is considered secondary users and must not cause interference to the primary users. By utilizing a feature called Dynamic Frequency Selection, the wireless router detects the presence of radar signals and relocates the wireless network to a clear channel. DFS channels vary by region, and we must obtain certification from the authorities before making them available for use on the Vigor router. We are working on DFS certification in Europe and will open up those channels by releasing new firmware once we pass certification. In Europe, these DFS channels will be made available 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140.

At this time, we have no plans to pursue DFS certification in the USA, so DFS channels will not be available in the foreseeable future. The U.S. DFS channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140 will not be available on routers sold in the United States.

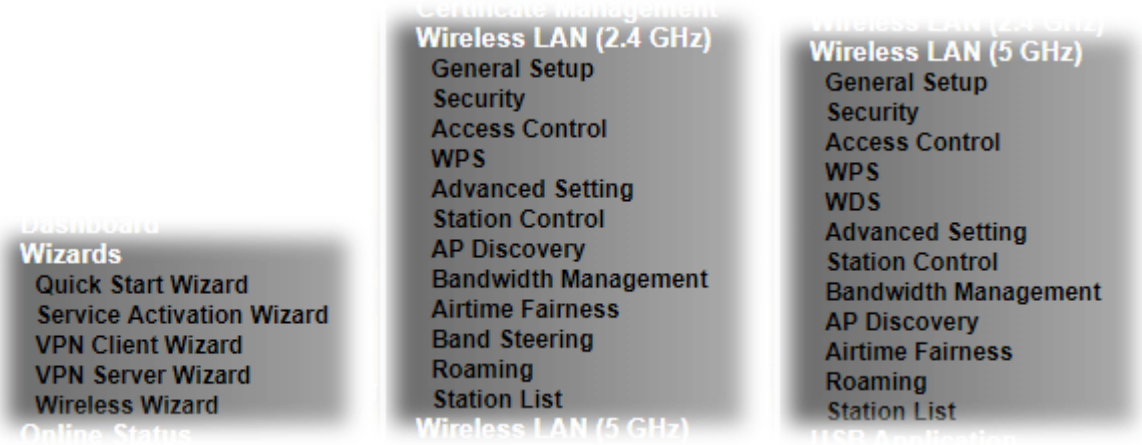
In the rest of world, there are restrictions on DFS channels as well. Uncertified DFS channels will be unavailable for selection depending on the country code programmed in the router.

WPS

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



Web User Interface



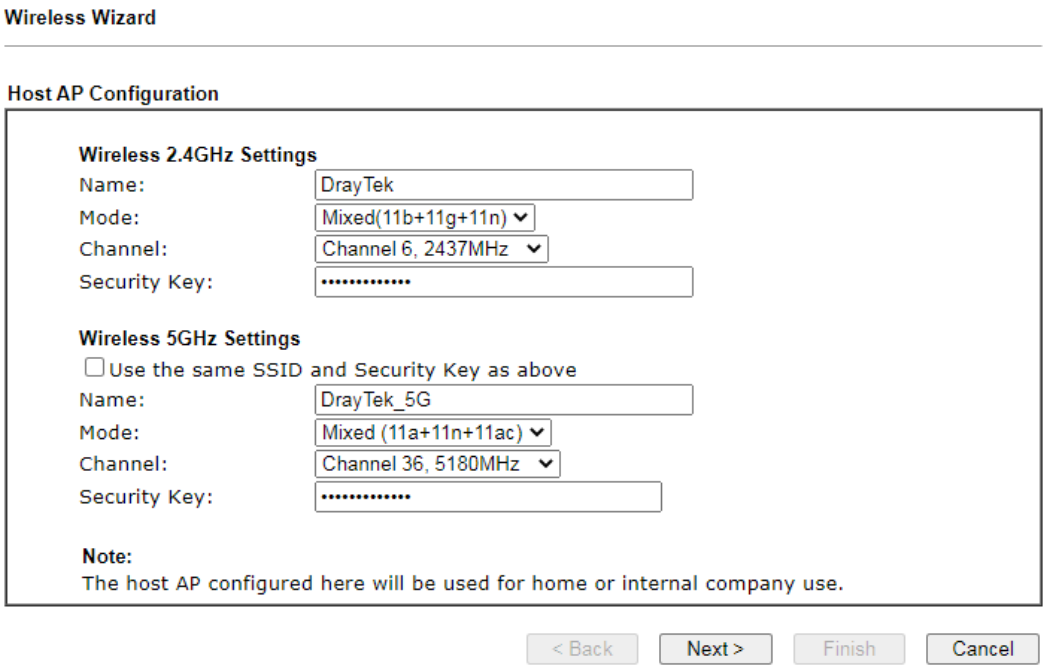
III-1-1 Wireless Wizard

On Wi-Fi-equipped models, you can configure the wireless access point (AP) using the Wireless Wizard. The Host AP Configuration sets up SSID 1 for use by internal users, who are allowed to access both the LAN and the WAN (Internet), whereas the Guest AP Configuration sets up SSID 2 for use by visitors, who are allowed only WAN access and whose access speeds can optionally be throttled.

The Wireless Wizard allows you to quickly configure a host SSID (for internal use, such as in a home or business environment), and optionally a guest SSID (for wireless clients that are restricted to Internet access only, typically used by visitors).

Follow the steps listed below:

1. On the menu bar, click on **Wizards**, and then **Wireless Wizard**.
2. The Host AP Configuration page appears. This page sets up SSID 1 for use by internal users. SSID 1 configured using the wizard will have no access speed throttling (by means of the Rate Control feature), and both the LAN and the WAN will be accessible.



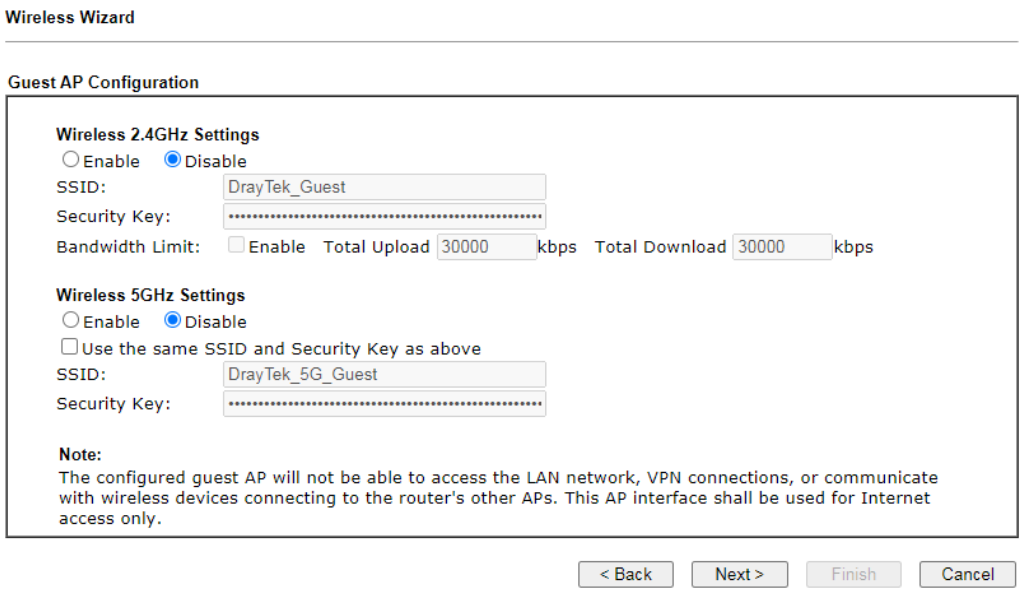
Available settings are explained as follows:

Item	Description
Wireless 2.4GHz Settings	
Name	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Mode	Allowed Wi-Fi modes. 802.11b is the original Wi-Fi mode on the 2.4 GHz band and supports raw data rates up to 11 Mbit/s. 802.11g allows for enhanced throughput up to 54 Mbit/s. 802.11n provides throughput up to 300 MHz. Available selections are • 11b Only • 11g Only • 11n Only (2.4 GHz) • Mixed(11b+11g) • Mixed(11g+11n) • Mixed(11b+11g+11n) The selections labeled “Mixed” enable multiple simultaneously-active modes.
Channel	Wi-Fi channel used for this SSID. If set to Auto, the router uses the best available channel.
Security Key	The Pre-shared Key (PSK) used by WPA2/PSK (Wireless Protected Access 2/Pre-shared Key) to encrypt wireless traffic. The key is composed of 8 to 63 ASCII characters. You may also specify the key using 64 hexadecimal digits, prefixed with the sequence 0x (“0x321253abcde…”).
Wireless 5GHz Settings	
Use the same SSID and Security Key as	If selected, the SSID Name and Security Key from the 2.4 GHz section will be used.

above	
Name	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Mode	Allowed Wi-Fi modes. 802.11a is the original Wi-Fi mode on the 5 GHz band and supports raw data rates up to 11 Mbit/s. 802.11n enhances the throughput and provides up to 300 MHz. The newest standard, 802.11ac, can achieve 1.3 Gbit/s of data throughput on the 5 GHz band. Available selections are • 11a Only • 11n Only (5GHz) • Mixed(11a+11n) • Mixed(11a+11n+11ac) The selections labeled "Mixed" enable multiple simultaneously-active modes.
Channel	Wi-Fi channel used for this SSID. If set to Auto, the router uses the best available channel.
Security Key	The Pre-shared Key (PSK) used by WPA2/PSK (Wireless Protected Access 2/Pre-shared Key) to encrypt wireless traffic. The key is composed of 8 to 63 ASCII characters. You may also specify the key using 64 hexadecimal digits, prefixed with the sequence 0x ("0x321253abcde…").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

3. Click **Next** to proceed to the Guest AP Configuration page. The Guest AP Configuration page appears. This page sets up SSID 2 for use by guest users. SSID 2 configured using the wizard can optionally be set up with access speed throttling (by means of the Rate Control feature), and only the WAN (the Internet) will be accessible.

   SSID 2 shares the same Mode and Channel settings as SSID 1 configured on the previous page.



   Available settings are explained as follows:

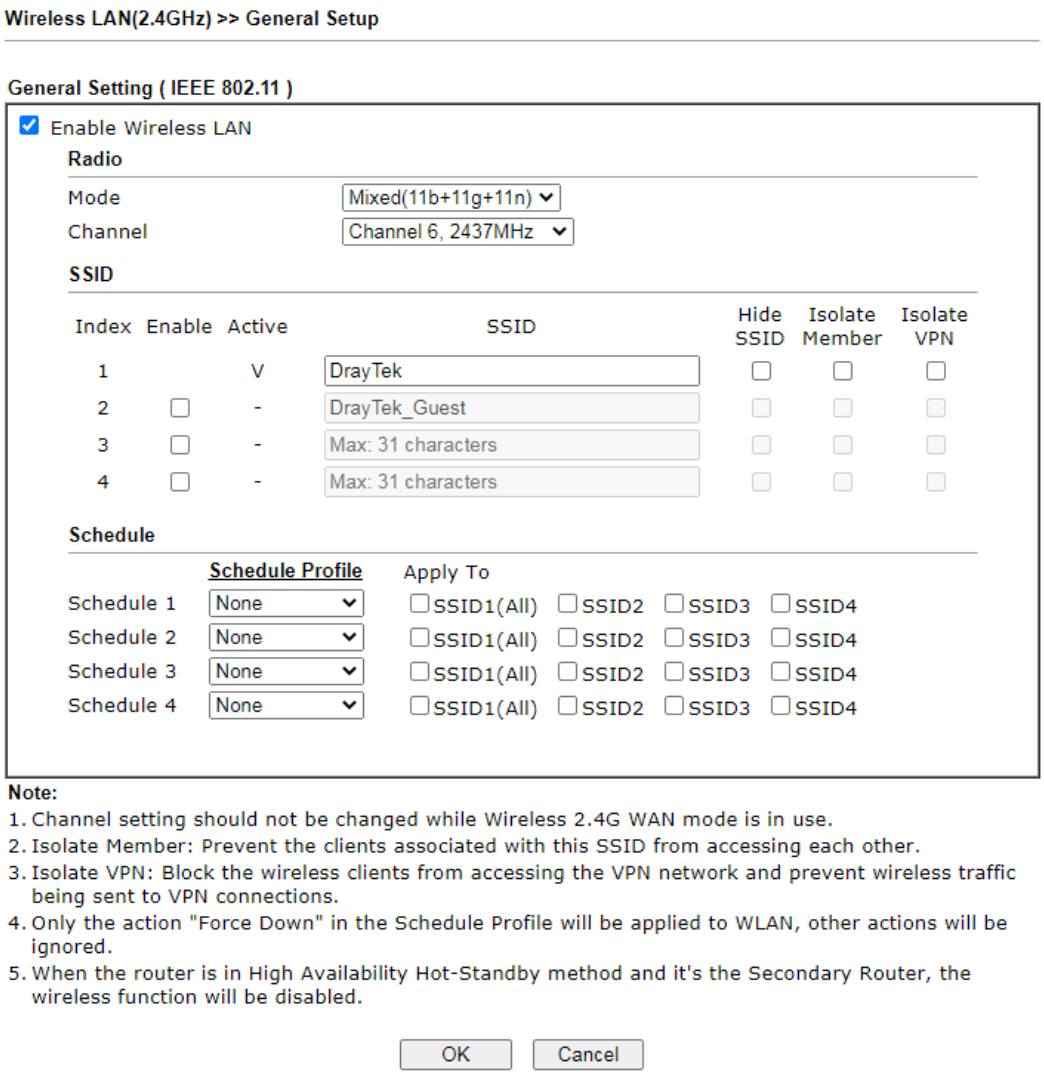
User-configurabe Item	Description
Wireless 2.4GHz Settings	
Enable/Disable	Enable or disable the SSID for guest use.
SSID	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Security Key	The Pre-shared Key (PSK) used by WPA2/PSK (Wireless Protected Access 2/Pre-shared Key) to encrypt wireless traffic. The key is composed of 8 to 63 ASCII characters. You may also specify the key using 64 hexadecimal digits, prefixed with the sequence 0x (“0x321253abcde…”).
Bandwidth Limit	**Enable** – Check the box to set the bandwidth limit for data transmission in upload and download. It controls the data transmission rate through wireless connection. **Total Upload** – Check Enable and Enter the transmitting rate for data upload. Default value is 30,000 kbps. **Total Download** – Enter the transmitting rate for data download. Default value is 30,000 kbps.
Wireless 5GHz Settings	
Enable/Disable	Click it to enable or disable settings in this page.
Use the same SSID and Security Key as above	If selected, the SSID Name and Security Key from the 2.4 GHz section will be used.
SSID	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Security Key	The Pre-shared Key (PSK) used by WPA2/PSK (Wireless Protected Access 2/Pre-shared Key) to encrypt wireless traffic. The key is composed of 8 to 63 ASCII characters. You may also specify the key using 64 hexadecimal digits, prefixed with the sequence 0x (“0x321253abcde…”).
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

4. Click **Next** to proceed to the Configuration Summary page. The **Configuration Summary** page displays all the settings you have entered.

5. Click **Finish** to save the settings, **Back** to make changes, or **Cancel** to exit the wizard without saving the settings.

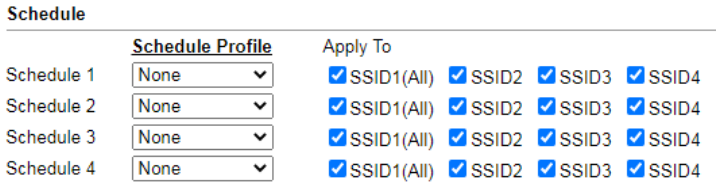
III-1-2 General Setup

The **Wireless LAN>>Genera Setup** section lets you configure the most basic settings of your wireless network, including the SSIDs, WLAN channels and bandwidth control.



Available settings are explained as follows:

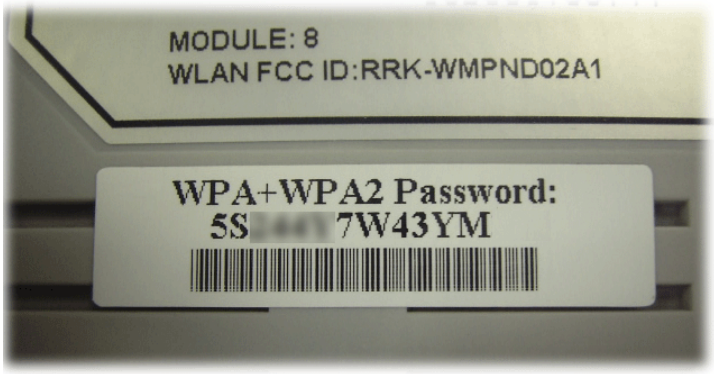
Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	Select the 802.11 mode allowed on the band. On the 2.4 GHz band, the following wireless mode options are available: • 11b Only • 11g Only • 11n Only (2.4 GHz) • Mixed (11b+11g) • Mixed (11g+11n) • Mixed (11b+11g+11n) On the 5 GHz band on ac models (2865ac and 2865Vac), the following options are available: • 11a Only

	• 11n Only (5 GHz) • Mixed (11a+11n) • Mixed (11a+11n+11ac)
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting "**Auto**". The list of available channels varies depending on the locale for which the router is intended.
SSID	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Hide SSID	Select to keep SSIDs from showing up when scans are performed by wireless clients, which makes it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless client and software used, the user may see only an AP listed without the SSID, or the AP might not even show up.
Isolate	**Member** – Check this box to disallow communication between wireless clients (stations) on the same SSID. **VPN** – Check this box to block wireless clients (stations) from accessing VPN clients.
Schedule Profile	Set the wireless LAN to be disabled at certain time intervals. You may choose up to 4 schedules out of the 15 schedules defined in **Applications >> Schedule**. Only "Force Down" schedule profiles take effect, and the wireless function will be turned off for the duration of the profile. The default setting is blank for all schedules, meaning wireless function will always work.
Apply To	Selected SSID (2 /3 /4) will be forced up /down based on the schedule profile used. 

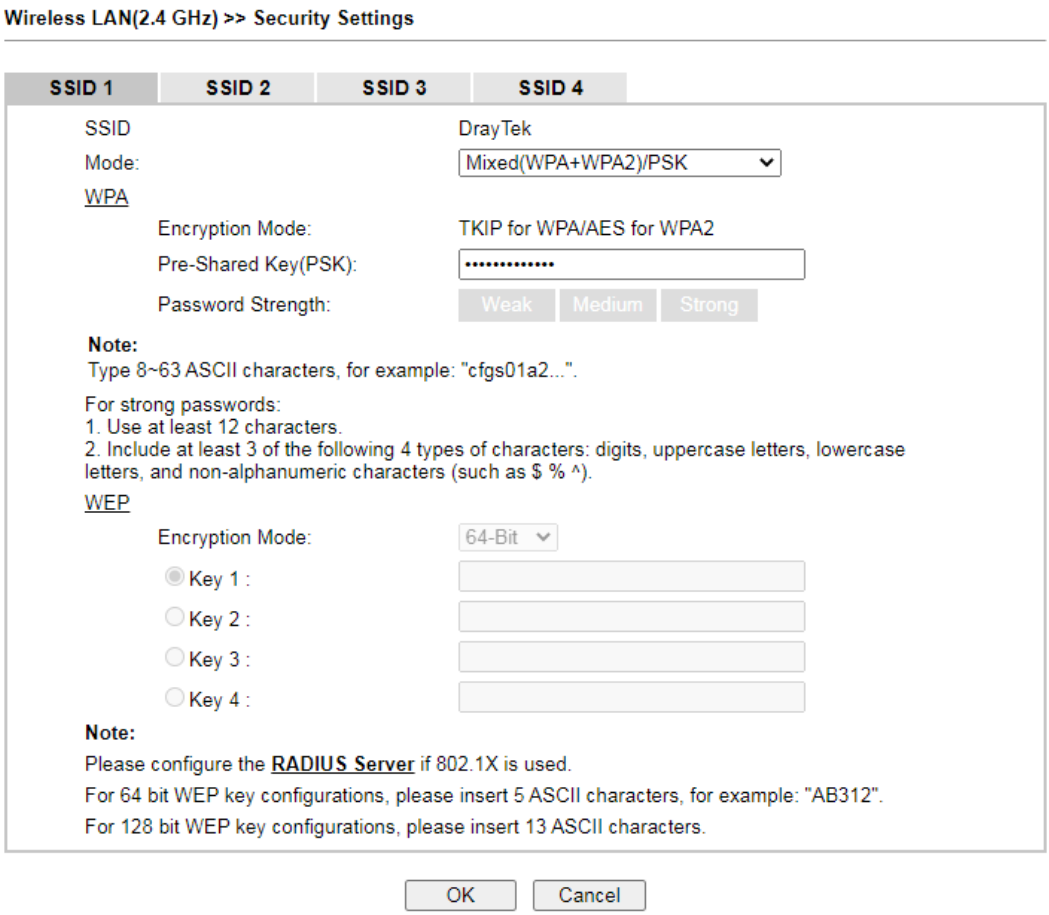
To save changes on the General Settings page, select **OK**; to discard changes, select **Cancel**.

III-1-3 Security

Every router has a default wireless password (PSK) which is provided on a label attached to 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.

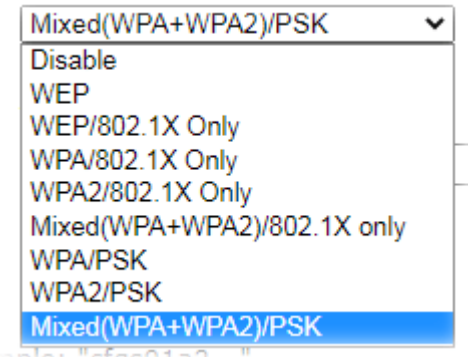


For extra security you can set your own wireless password by clicking the **Wireless LAN>>Security Settings** entry on the Web User Interface. Each of the 4 SSIDs can be configured independently using their own tab page.



Available settings are explained as follows:

Item	Description
Mode	This dialog box lists all available security modes.

	 **Info** You should also set **RADIUS Server** simultaneously if 802.1x mode is selected. **Disable** – Encryption mechanism is disabled. **WEP** – Allow only connections from WEP clients. Encryption key should be entered in the WEP Key section. **WEP/802.1x Only -** Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. Allow only connections from WEP clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. **WPA/802.1x Only -** Allow only connections from WPA clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. **WPA2/802.1x Only-** Allow only connections from WPA2 clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. **Mixed (WPA+WPA2/802.1x only) -** Allow connections from both WPA and WPA2 clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. **WPA/PSK -** Allow connections only from WPA clients. Encryption key should be entered in the PSK field. **WPA2/PSK -** Allow connections only from WPA2 clients. Encryption key should be entered in the PSK field. **Mixed (WPA+ WPA2)/PSK -** Allow connections from both WPA and WPA2 clients. Encryption key should be entered in the PSK field.
WPA	WPA encrypts each frame transmitted from the radio using the key, which is either entered in the PSK (Pre-Shared Key) field, or or automatically negotiated via 802.1x authentication from a RADIUS server. **Pre-Shared Key (PSK)** - Enter 8~63 ASCII characters, for example, “012345678..” , or 64 hexadecimal digits with a leading “0x”, for example, "0x321253abcde...". **Password Strength** – The system will display the strength of the password, indicated by the words “weak”, “medium” or “strong”.
WEP	WEP keys can either be 64-bit or 128-bit. **64-Bit** - Either 5 ASCII characters, for example “12345”, or 10 hexadecimal digitals with a leading “0x”, such as “0x4142434445”. **128-Bit** - Either 13 ASCII characters, for example

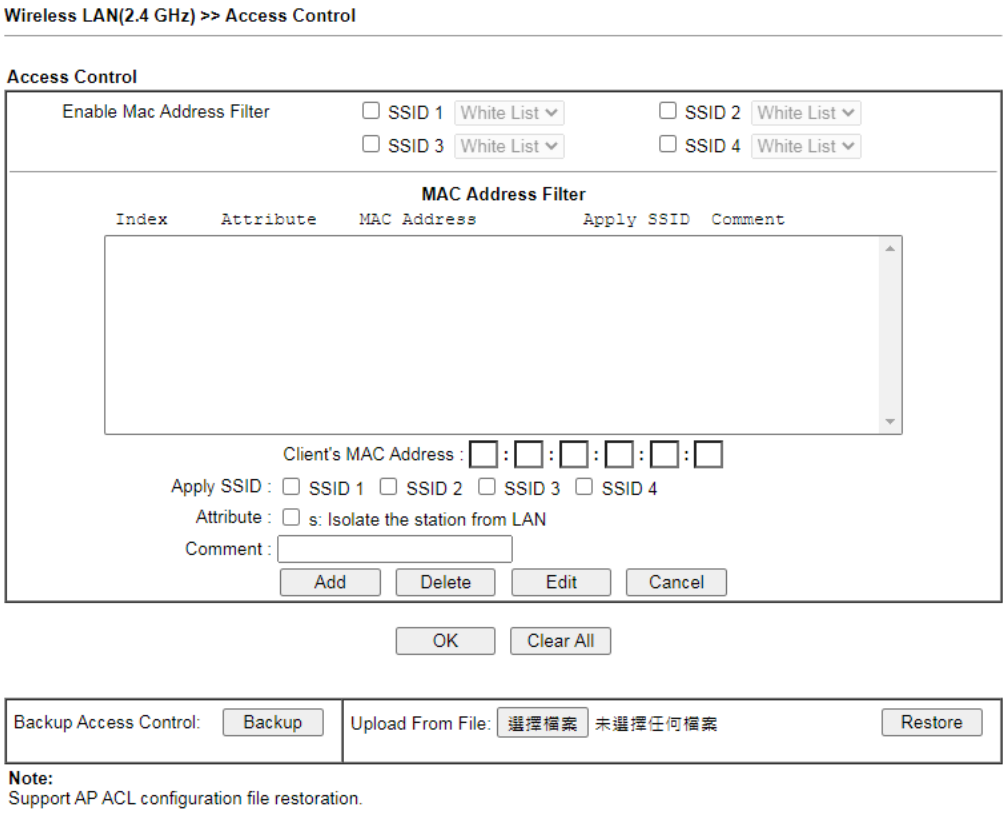
	"ABCDEFGHIJKLM", or 26 hexadecimal digits with a leading "0x", for example "0x41424344454647484 94A4B4C4D". Up to four keys can be entered here, but only one key can be selected at any time. The keys can be entered in ASCII or Hexadecimal. All wireless devices intending to connect to the same SSID must support the same WEP encryption bit size and have the same key.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

III-1-4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by referencing a MAC address black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only allow certain wireless clients 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 the SSIDs that you would like to have MAC Address filter enabled. Select **White List** or **Black List** in the combo box next to each enabled SSIDs. **White List** - Only allow wireless clients whose MAC addresses are listed in the MAC Address Filter list. **Black List** - Only allow wireless clients whose MAC addresses are not listed in the MAC Address Filter list.

MAC Address Filter	Displays all MAC addresses in the filter list.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	Select the SSIDs to which the above MAC address filter will be applied.
Attribute	**s: Isolate the station from LAN -** select to isolate the wireless client from LAN.
Comment	Enter a brief description for the specified client's MAC address.
Add	Add a new filter entry to the MAC Address filter list using the information entered above.
Delete	Delete the selected MAC address from the list.
Edit	Update the selected MAC address in the list using the information entered above.
Cancel	Clear the contents of all the above fields. This will discard all changes without saving to the MAC Address Filter list.
OK	Click to save the MAC Address Filter list.
Clear All	Remove all entries from the MAC Address Filter 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.

To save changes on this page, select **OK**.

III-1-5 WPS

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

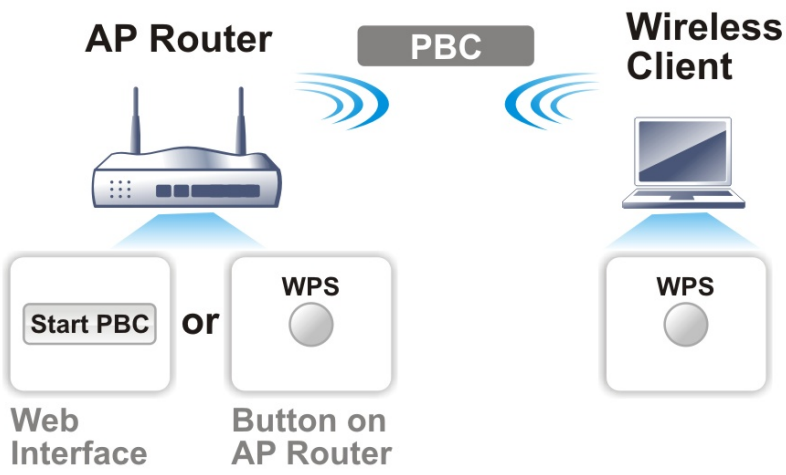
Info	WPS works with wireless stations with WPS or WPS2 support. It does not work with WEP.

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

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

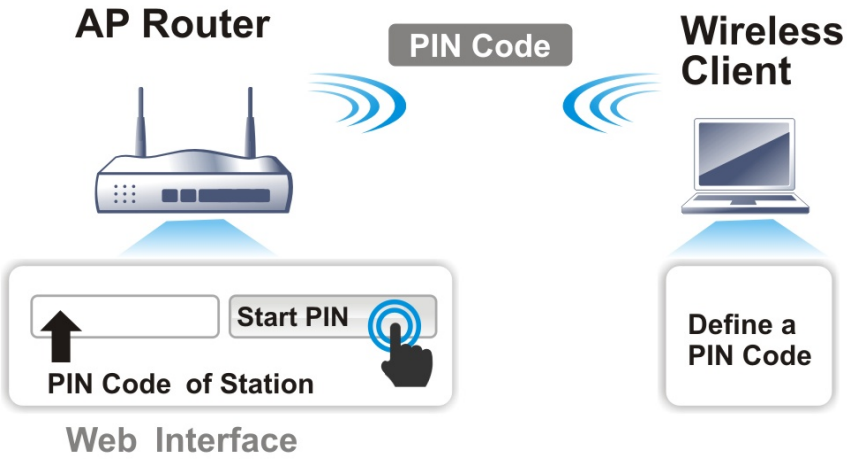
Using the PBC button

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

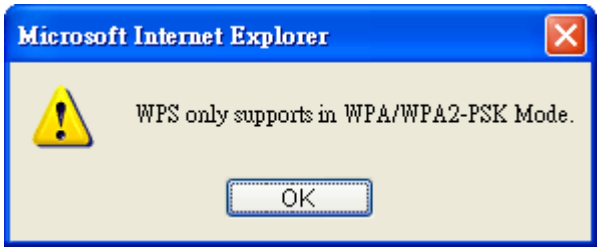


Using a PIN code

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

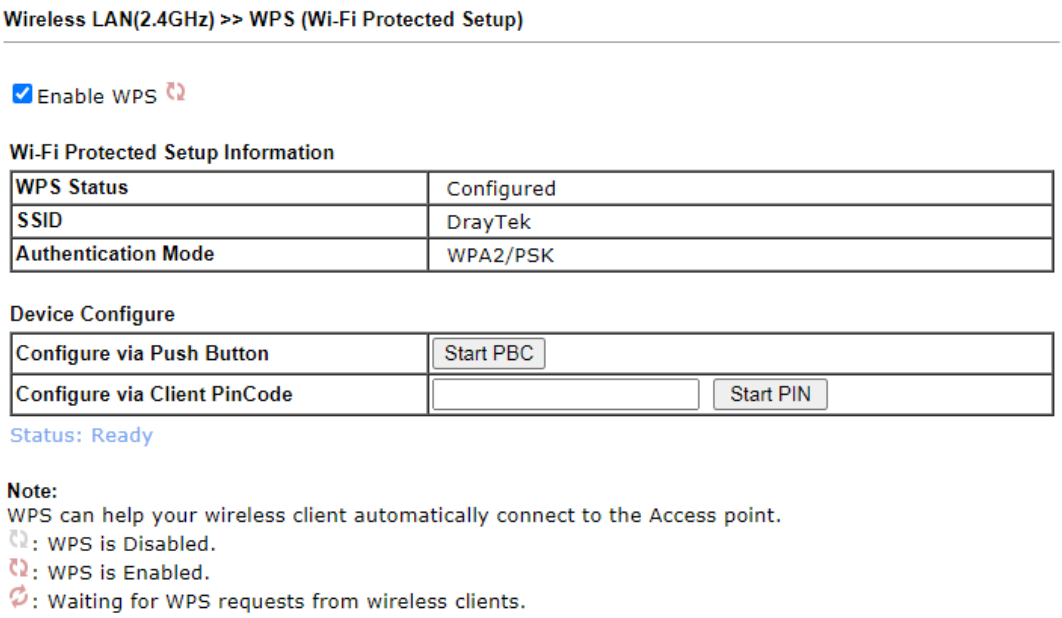


WPS is only supported when the encryption protocol is set to WPA-PSK or WPA2-PSK. If other protocols (such as WEP) have been selected in **Wireless LAN>>Security**, you will see the following message box:



Please click **OK** to dismiss dialog box, return to **Wireless LAN>>Security** and select WPA-PSK or WPA2-PSK mode before attempting to enable WPS again.

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



Available settings are explained as follows:

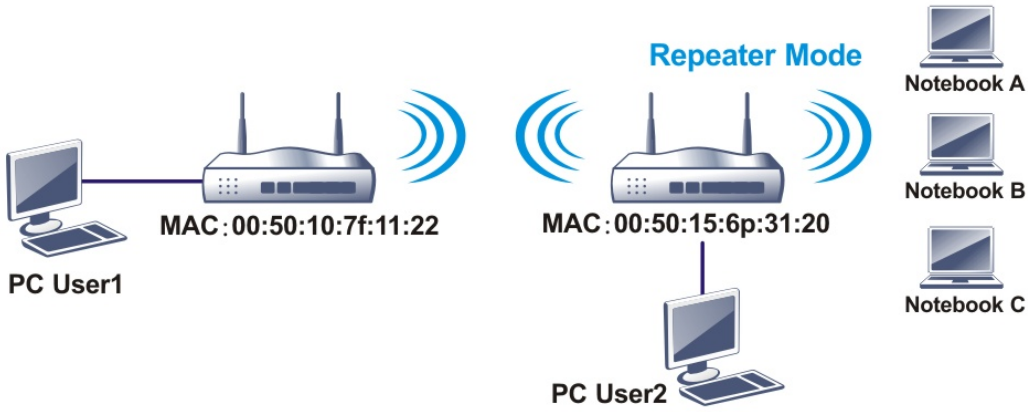
Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Displays system information related to WPS. The message “Configured” means that the wireless security (encryption) function of the router is properly configured and functioning properly.
SSID	Displays the SSID1. WPS is supported on SSID1 only.
Authentication Mode	Displays the current authentication mode of the router.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. The router will wait for about 2 minutes for WPS connection requests from wireless clients. The WPS LED on the router will blink fast when WPS is in progress, and will return to normal condition after two minutes.
Configure via Client PinCode	Enter a PIN code, and click the **Start PIN** button. The WPS LED on the router will blink rapidly when WPS is in progress, for up to 2 minutes or until a successful WPS connection from a wireless client has been established.

III-1-6 WDS (for 5GHz)

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

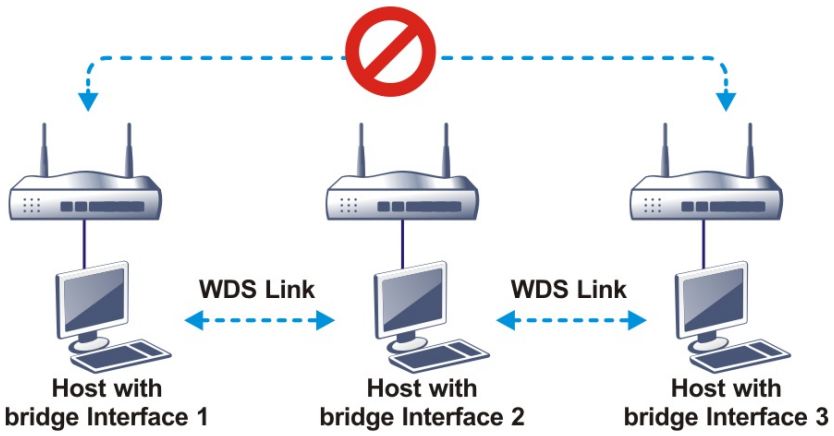
- **Bridge mode**, which bridges traffic between two LANs wirelessly.

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

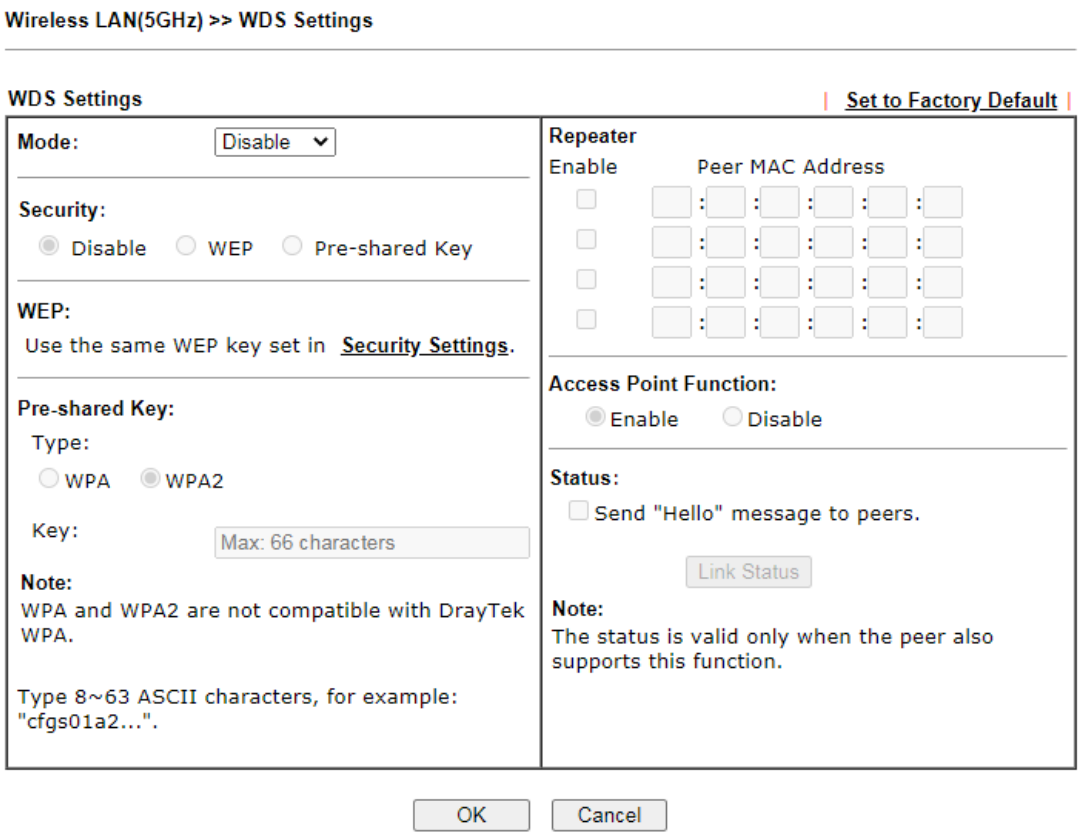


The main difference between these two modes is that, in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links, whereas in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following example, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 cannot communicate with hosts connected to Bridge 3 through Bridge 2.



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



Available settings are explained as follows:

Item	Description
Mode	Choose the WDS mode. **Disable** – WDS is disabled. **Repeater** – WDS is enabled in Repeater mode.
Security	Choose one of the types for the router. The setting you choose here will make the following WEP or Pre-shared key field valid or not. **Disable** – Security is disabled. **WEP** - Security is enabled. **Pre-shared key** – Security is enabled.
Pre-shared Key	**Type** – Select either WPA or WPA2 as the encryption protocol. **Key** – Enter 8 ~ 63 ASCII characters or 64 hexadecimal digits with a leading “0x”.
Repeater	If Repeater was selected as the WDS mode, enter the peer MAC addresses in these fields. Up to four peer MAC addresses may be entered in this page. Select the checkbox in front of a MAC address to enable it.
Access Point Function	Select **Enable** to make this router serve as an access point; select **Disable** to disable access point function.
Status	Click to send a “hello” message to peers. This only works if the peer also supports this function.

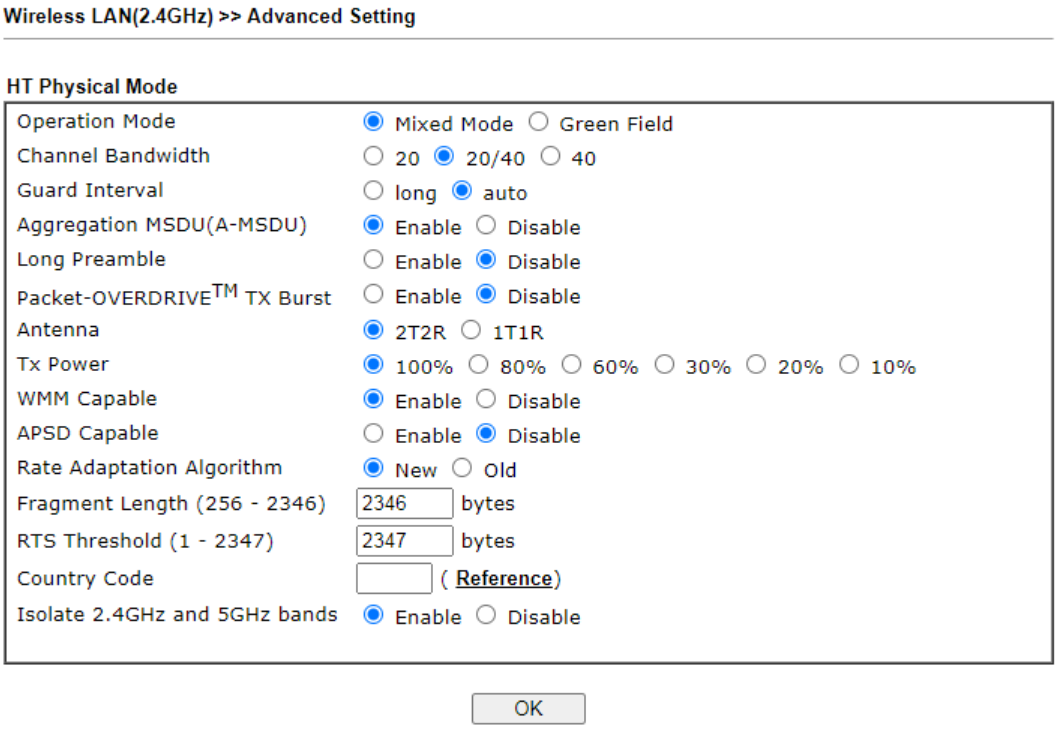
To save changes on this page, select **OK**; to discard changes, select **Cancel**.

III-1-7 Advanced Setting

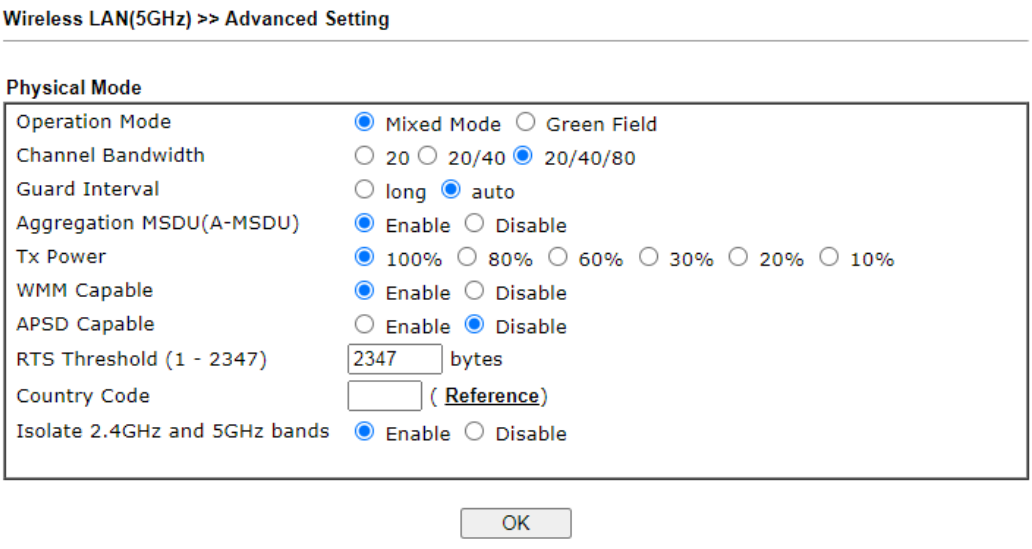
On this page you can configure advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

If the Vigor router supports dual-band WLAN, you will see separate Advanced Setting sections for 2.4GHz and 5GHz.

2.4 GHz Advanced Setting page



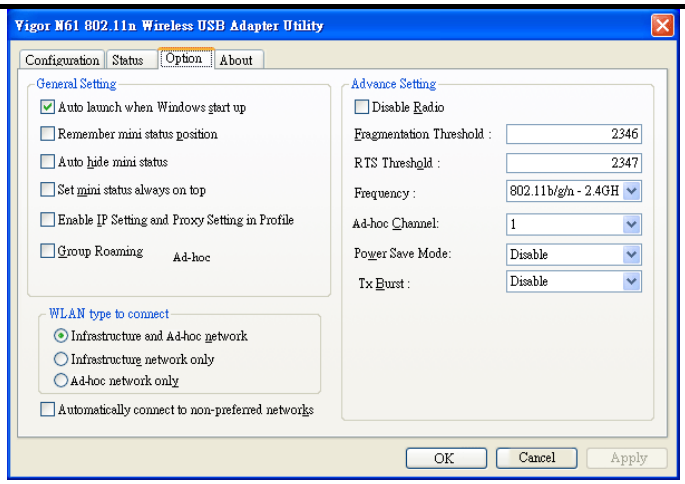
5 GHz Advanced Setting page



Available settings are explained as follows:

Item	Description

Operation Mode	**Mixed Mode** – The router can transmit data using all protocols supported by 802.11a/b/g and 802.11n standards. However, all wireless transmissions will be slowed down when any 802.11g or 802.11b wireless client is connected. **Green Field** – Select this mode to achieve the highest throughput. This mode supports data transmission between 802.11n systems only. In addition, it does not have protection mechanism to prevent conflicts with neighboring 802.11a/b/g devices.
Channel Bandwidth	**20** –Vigor Router will utilize 20 MHz channels for data transmission and reception between the AP and wireless stations. **40** –Vigor Router will utilize 40 MHz for data transmission and reception between the AP and wireless stations. **20/40** – Vigor Router will utilize either 20 MHz or 40 MHz for data transmission and reception depending on the number of nearby wireless APs. 20MHz will be used when there are more than 10 wireless APs; otherwise 40MHz will be used. Selecting this setting ensures the best performance for data transit on networks with both 20 MHz and 40 MHz clients.
Guard Interval	Enabling this setting ensures the integrity of wireless traffic by inserting guard intervals between symbols to reduce the adverse effects of propagation delays, and signal multipath or reflections. If you choose auto as guard interval, the router will choose short guard interval (which increases wireless performance) or long guard interval for data transmit depending on the station capability.
Aggregation MSDU (A-MSDU)	Aggregation MSDU can combine frames of different sizes to improve performance at the MAC layer for clients from certain manufacturers. The default setting is **Enable**.
Long Preamble	This option determines the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync fields which yield better transmission speeds. However, some older 802.11b wireless devices only support long preamble which uses 128-bit sync fields. Click **Enable** to use Long Preamble to maintain compatibility with these devices.
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* (by checking **Tx Burst**). It is active only when both the Access Point and Station (in wireless client) support and invoke this function at the same time. **Note:** Vigor N61 wireless adapter supports this function. Therefore, you can install it on your PC to take advantage of Packet-OVERDRIVE (Refer to the following picture of Vigor N61 wireless utility window: choose Enable for TxBURST on the **Option** tab).

	 **Info** * Real transmission rate depends on the environment of the network.
Antenna	Vigor router can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.
TX Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.
WMM Capable	WMM stands for Wi-Fi Multimedia. It provides basic Quality of Service (QoS) by prioritizing traffic based on four access categories defined in the IEEE 802.11e standard. The access categories are AC_VO, AC_VI, AC_BE and AC_BK, which corresponds to traffic types of voice, video, best effort and low priority (background) data, respectively. To apply WMM parameters to wireless data transmission, click the **Enable** radio button.
APSD Capable	APSD (Automatic Power-Save Delivery) is an enhancement over the power-saving mechanisms supported by Wi-Fi networks. It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption. Not all wireless clients support APSD properly, and the only way to find out if APSD is appropriate for your network is to experiment. The default setting is **Disable**.
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old". Sets the way the Wireless transmission rate is adjusted dynamically. In most cases, selecting "New" will result in better performance than "Old".
Fragment Length (256 - 2346)	Set the Fragment threshold. You are advised to leave the default value, 2346, untouched.

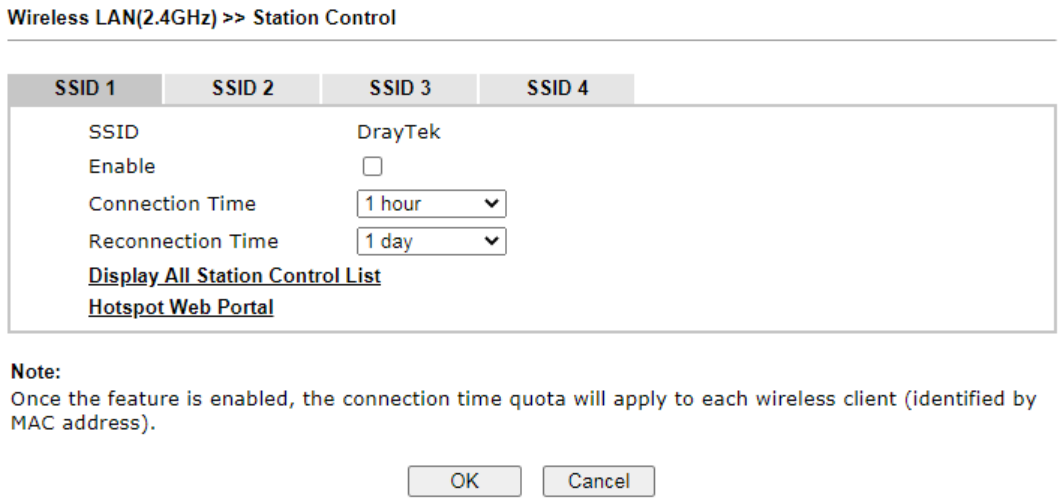
RTS Threshold (1 – 2347)	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold. Do not modify default value if you don't know what it is, default value is 2347. Adjusts the 802.11 maximum transmit frame size, which might reduce chances of collision with hidden stations. You are advised to leave the default value, 2347, untouched.
Country Code	Vigor router broadcasts country codes according to the 802.11d standard. However, some wireless stations will detect/scan access points looking for country codes to determine which country it is in, and utilize channels appropriate to the country. The wireless client might get confused if there are multiple access points in the vicinity broadcasting different country codes. In such cases, it might be necessary to change the country code of the access point to ensure these clients can successfully establish a wireless connection.
Isolate 2.4GHz and 5GHz bands	The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa. For WLAN 2.4GHz and 5GHz set with the same SSID name: ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if **Isolate Member** (in **Wireless LAN>>General Setup**) is NOT enabled for such SSID. ● Yet, if the function of **Isolate Member** (in **Wireless LAN>>General Setup**) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.

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

III-1-8 Station Control

Station Control is used to specify the duration that the wireless client can connect to the Vigor router. If this function is disabled, wireless clients can connect to the router as long as the router is powered on and the wireless feature is enabled.

This feature is especially useful for free WiFi service. For example, a coffee shop may offer free Wi-Fi service to its guests for one hour every day. In this scenario, the connection time can be set to "1 hour" and reconnection time set to "1 day". In this way, every guest can surf the net for at most one hour, thus freeing up resources for other guests.



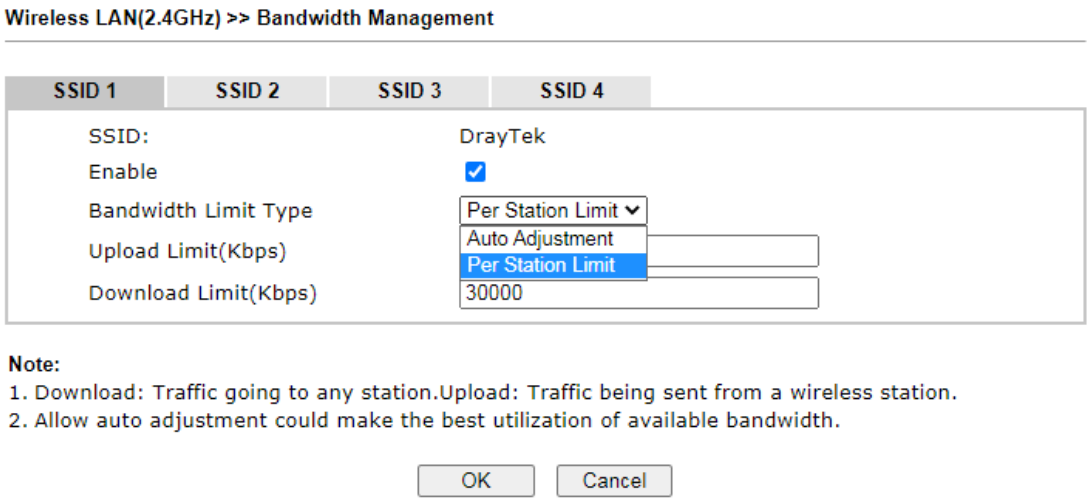
Available settings are explained as follows:

Item	Description
SSID	Display the selected SSID.
Enable	Select to enable station control function for this SSID.
Connection Time / Reconnection Time	In the Connection Time dropdown box, select the maximum amount of time that a wireless client is allowed to connect within the period of time selected in the Reconnection Time dropdown box. Select **User defined** to manually enter the time in days, hours and minutes.
Display All Station Control List	Click to display all wireless clients that are under Station Control.
Hotspot Web Portal	Click to jump to the **Hotspot Web Portal** page.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

III-1-9 Bandwidth Management

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 Bandwidth Management to make the bandwidth usage more efficient.



Available settings are explained as follows:

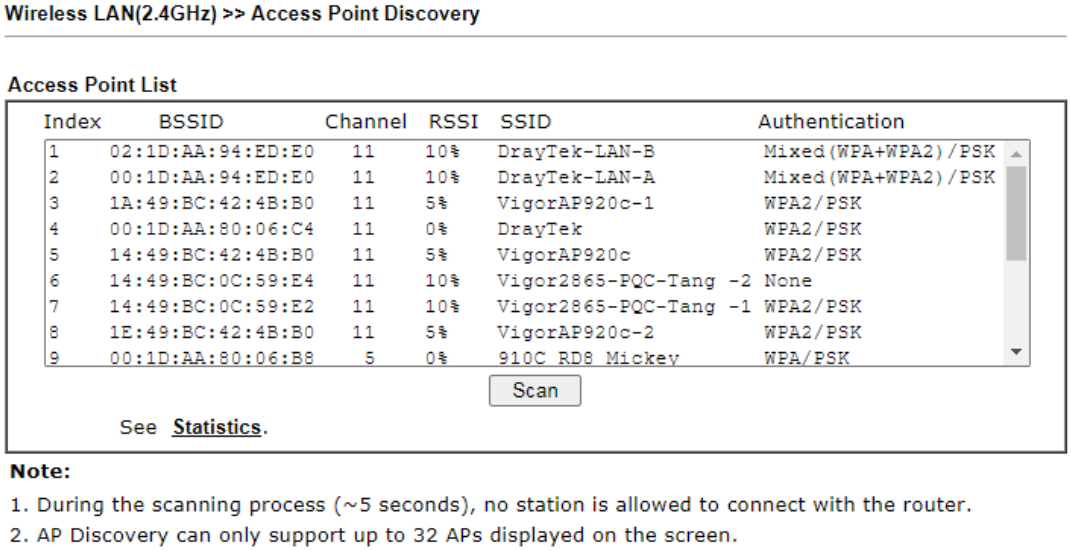
Item	Description
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Bandwidth Limit Type	**Auto Adjustment -** Bandwidth limit is determined by the system automatically. **Per Station Limit** – Bandwidth limit is determined according to the limitation of the wireless client.
Total Upload Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to Vigor2135.
Total Download Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data client(stations) connecting to Vigor2135.
Upload Limit	It is available when Per Station Limit is selected. Type a value to define the maximum data traffic (uploading) for each wireless client connecting to Vigor2135ac.
Download Limit	It is available when Per Station Limit is selected Type a value to define the maximum data traffic (downloading) for each wireless client connecting to Vigor2135ac.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

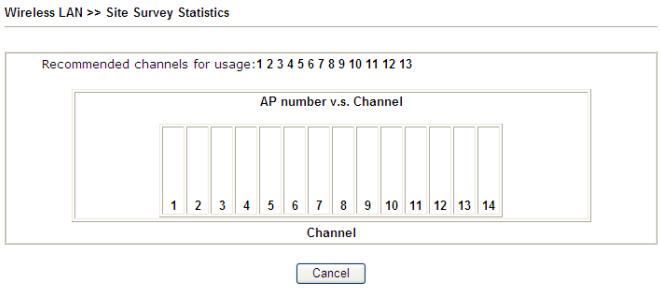
III-1-10 AP Discovery

Vigor router can scan all regulatory channels to find working APs in the neighborhood. The scanning result can be used to determine the most desirable channel to use, or to locate an AP for establishing a WDS link. Note that during the scanning process (about 5 seconds), no client is allowed to connect to the Vigor. Only APs operating on the same band as the Vigor can be discovered.

Click the **Scan** button to start the AP discovery process.



Available settings are explained as follows:

Item	Description
Scan	Click to start the AP discovery process. The results will be shown on the box above this button.
Statistics	Shows channel usage by the neighboring APs. 
Add to WDS Settings	This field is available for WLAN (5GHz). **Add to** - To establish a WDS link to an AP that was found in an AP scan, click its entry in the Access Point List window, and its MAC address will be copied to the AP's MAC address field. Select the WDS mode you wish to use, Bridge, and click **Add to**. The AP will be configured in **Wireless LAN >> WDS Settings**.

III-1-11 Airtime Fairness

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

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

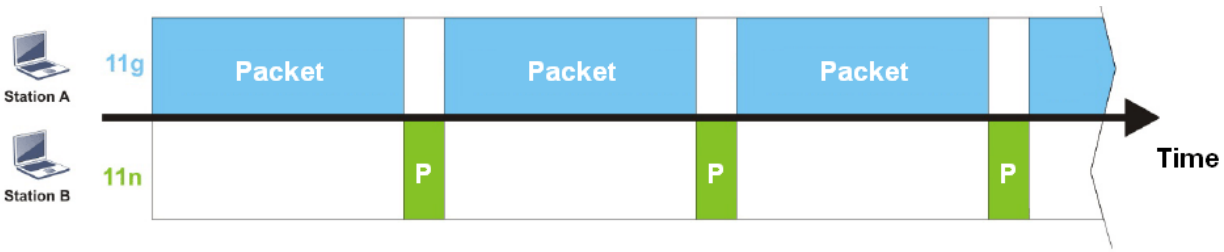
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

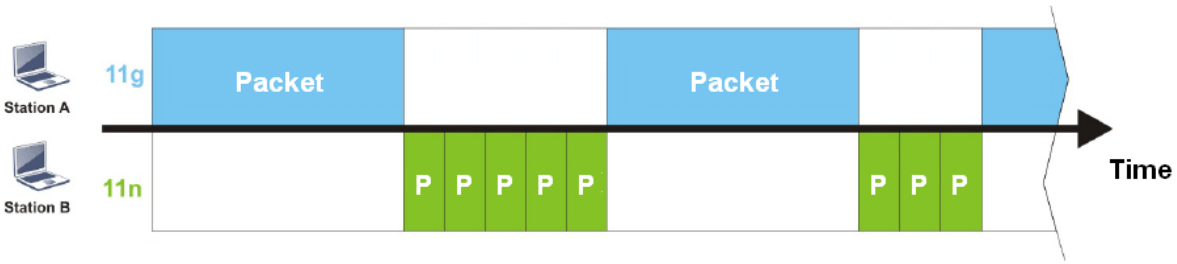
The principle behind the IEEE802.11 channel access mechanisms is that each station has *equal probability* to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

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

Take the following figure as an example, there are 2 wireless stations on the wireless network, Station A (11g) and Station B (11n), both of which transmit data packets to the Vigor router. Even though they have equal opportunity to access the wireless channel, Station B (11n) gets only a little airtime and waits too much because Station A (11g) takes longer to send one packet. In other words, transmission from Station B (fast rate) is effectively being throttled by Station A (slow rate).



To alleviate this problem, Airtime Fairness tries to assign *similar airtime* to each station (A and B) by controlling TX traffic. In the following figure, Station B (11n) has higher opportunities to send data packets than Station A (11g). In this way, Station B (fast rate) gets its fair share of airtime and its speed is not limited by Station A (slow rate).



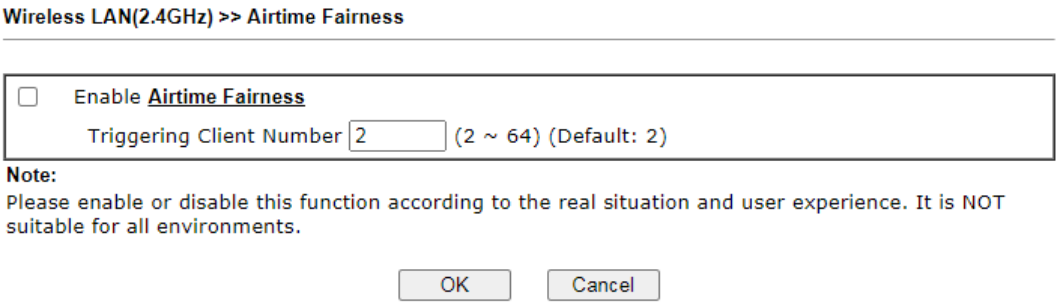
This is similar to automatic Bandwidth Limit, where the dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4 GHz and 5 GHz bands are independent, but stations connected to different SSIDs on the same band are prioritized as a group, because they all use the same wireless channel. Under certain environments, this function can reduce the adverse effects of slow wireless devices and improve the overall wireless performance.

Environments that can benefit by applying airtime fairness:

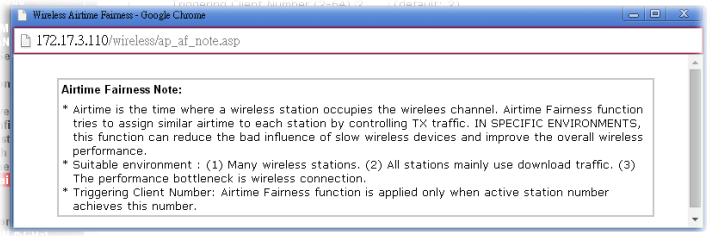
(1) Many wireless stations.

(2) All stations mainly use download traffic.

(3) The performance bottleneck is wireless connection.



Available settings are explained as follows:

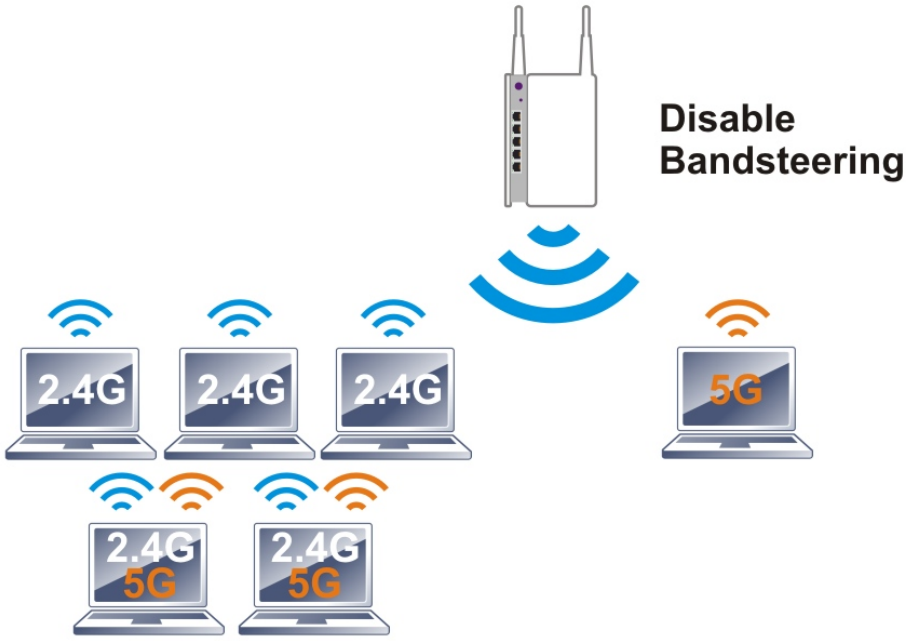
Item	Description
Enable Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. **Airtime Fairness** – Click the link to display the following explanation of airtime fairness note.  **Triggering Client Number –** Airtime Fairness function is applied only when there are at least this many active wireless stations.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

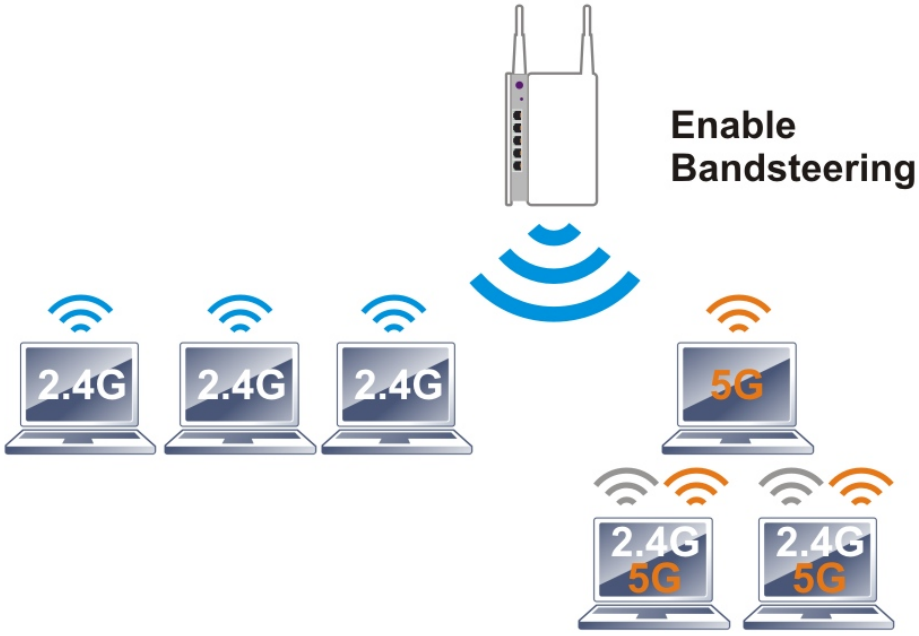
Info	Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

III-1-12 Band Steering (2.4 GHz)

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



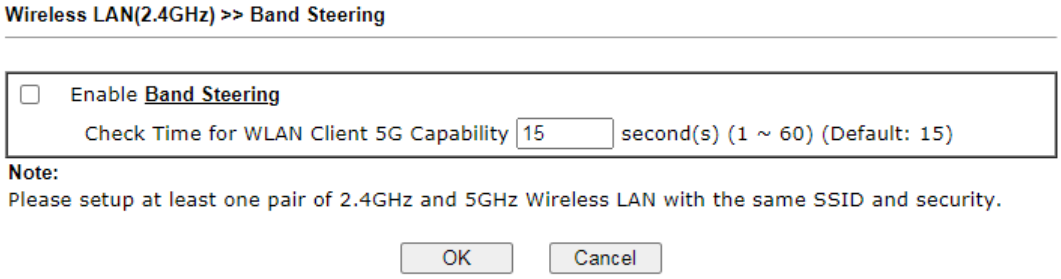
If a dual-band client is detected, the AP will let the wireless client connect to the less congested wireless band, such as the 5GHz band, to reduce network congestion.



Info

For Band Steering to work properly, the same SSID and security settings must be configured on both 2.4 GHz and 5 GHz bands.

To configure Band Steering, go to the **Wireless LAN (2.4GHz)>>Band Steering** page:

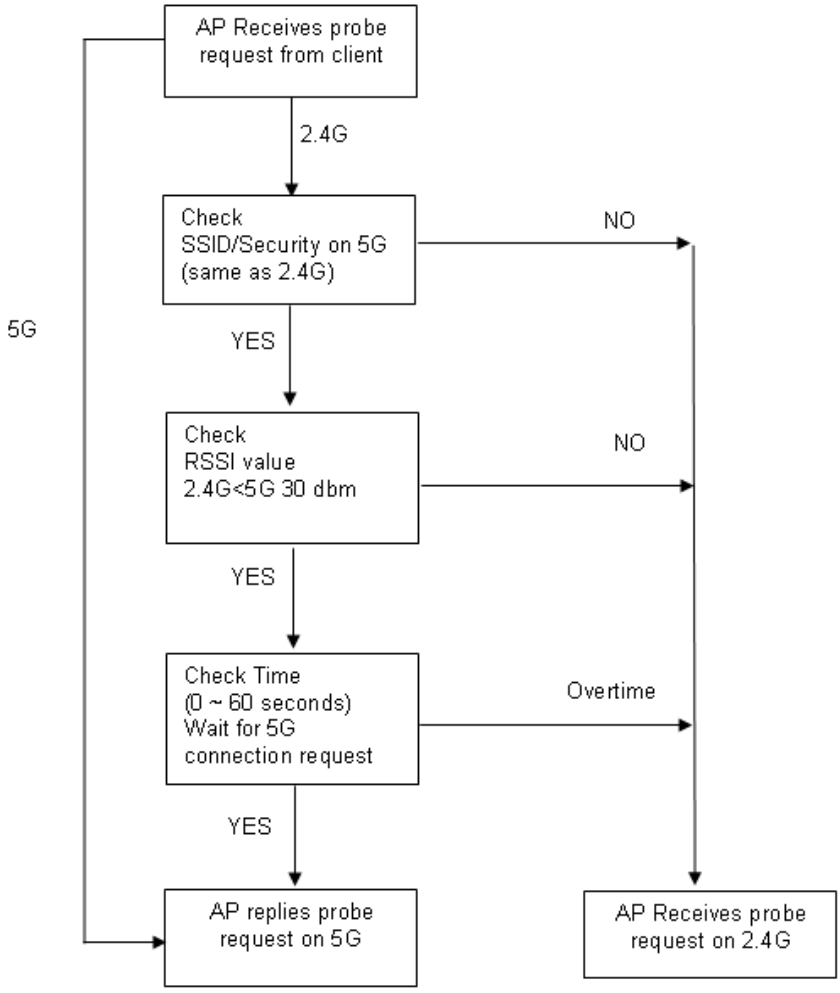


Available settings are explained as follows:

Item	Description
Enable Band Steering	When enabled, the router will detect if wireless clients are capable of dual-band or not within the time limit. **Check Time…**. – When a wireless client attempts to connect, the router will block attempts to connect to the 2.4 GHz band for the specified period of time (default is 30 seconds), which hopefully will entice the client to connect to the 5 GHz band. If the client fails to connect to the 5 GHz band within the specified interval, it will then be able to connect to the 2.4 GHz band.

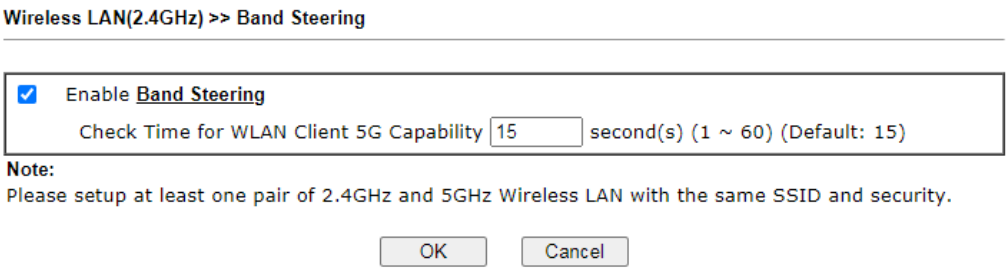
To save changes on this page, select **OK**; to discard changes, select **Cancel**.

The following diagram shows how Band Steering works.



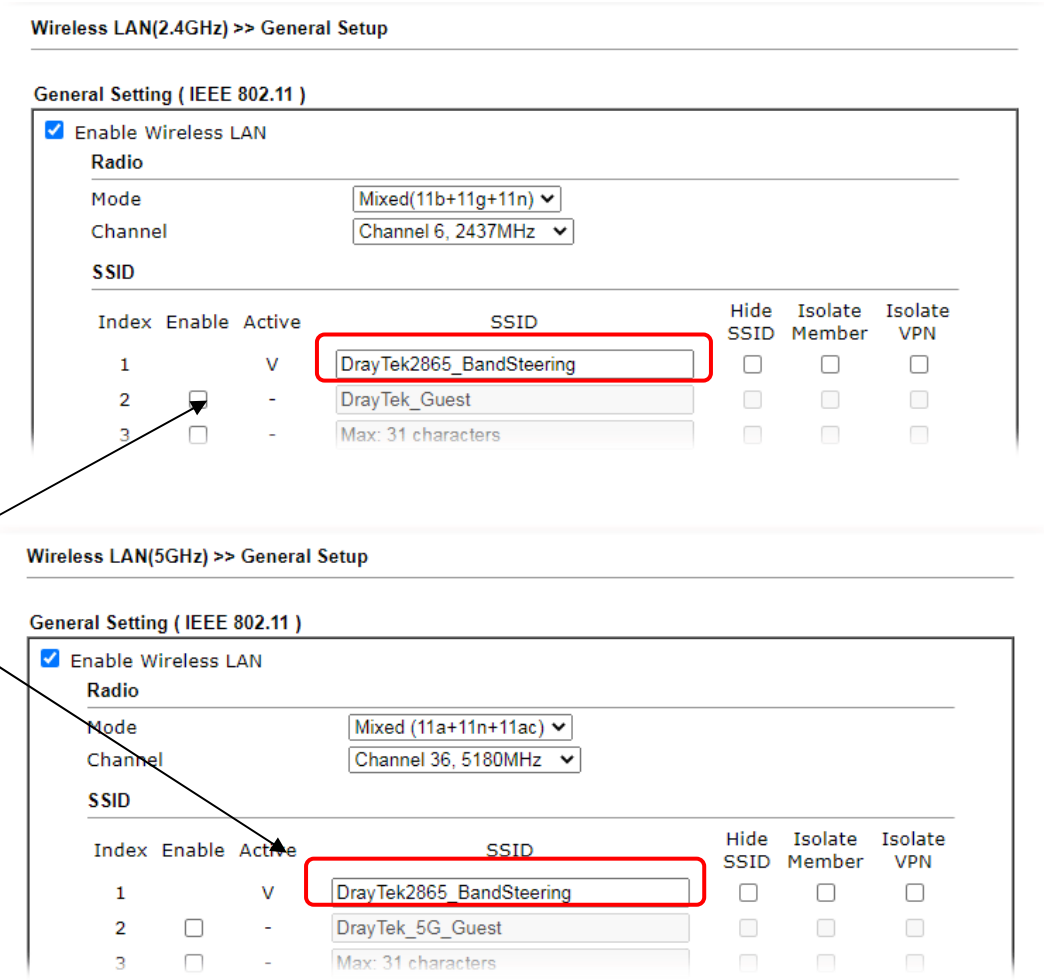
Example: How to Use Band Steering?

1. Open **Wireless LAN(2.4GHz)>>Band Steering**.
2. Check the box of **Enable Band Steering** and use the default value (15) for check time setting.



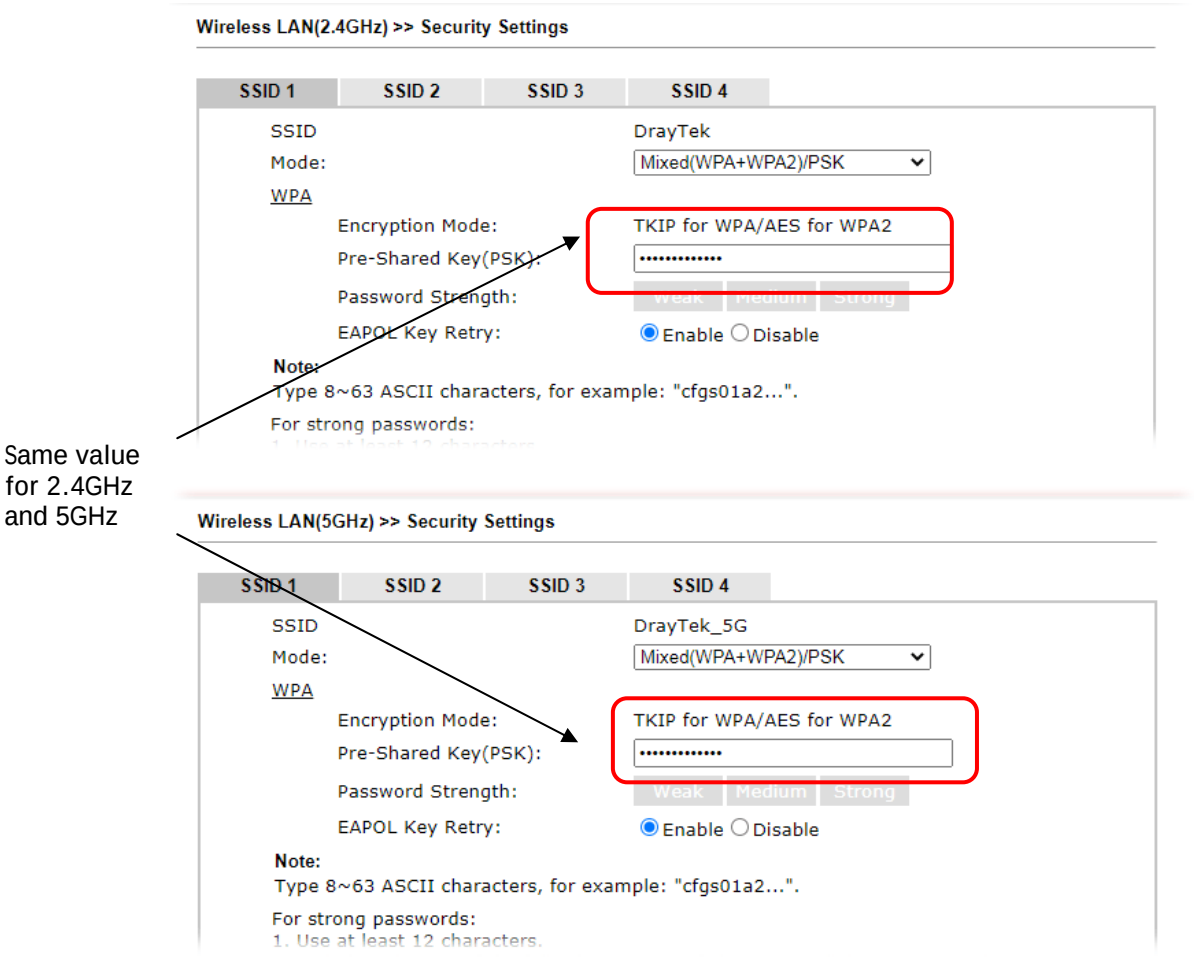
3. Click **OK** to save the settings.

4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *DrayTek2865_BandSteering* for both pages. Click **OK** to save the settings.



Same settings for 2.4GHz and 5GHz

5. Open **Wireless LAN (2.4GHz)>>Security** and **Wireless LAN (5GHz)>>Security.** Configure Security as *12345678* for both pages. Click **OK** to save the settings.

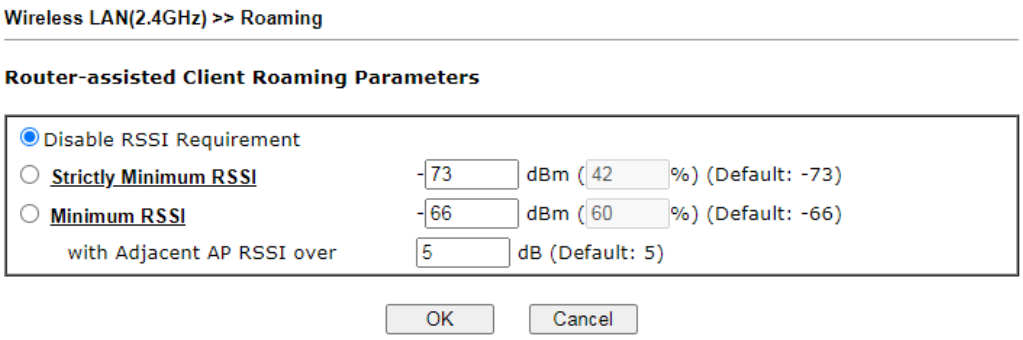


6. The Vigor will now steer wireless clients to the less congested wireless band, such as 5GHz to reduce network congestion.

III-1-13 Roaming

WiFi roaming allows wireless stations to switch connections between access points within an area to achieve better coverage and signal quality. It usually is up to the wireless station to switch to another access point with stronger signal strength while it is already connected, but Vigor wireless routers have an AP-assisted client roaming feature that could facilitate roaming on wireless stations. Depending on the roaming configuration, the Vigor monitors the Received Signal Strength Indicator (RSSI) of wireless stations and disconnect stations whose RSSI falls below a certain (configurable) threshold, thus forcing stations to seek out other WiFi hosts to connect to.

To configure wireless roaming settings, go to Wireless LAN >> Roaming.



Available settings are explained as follows:

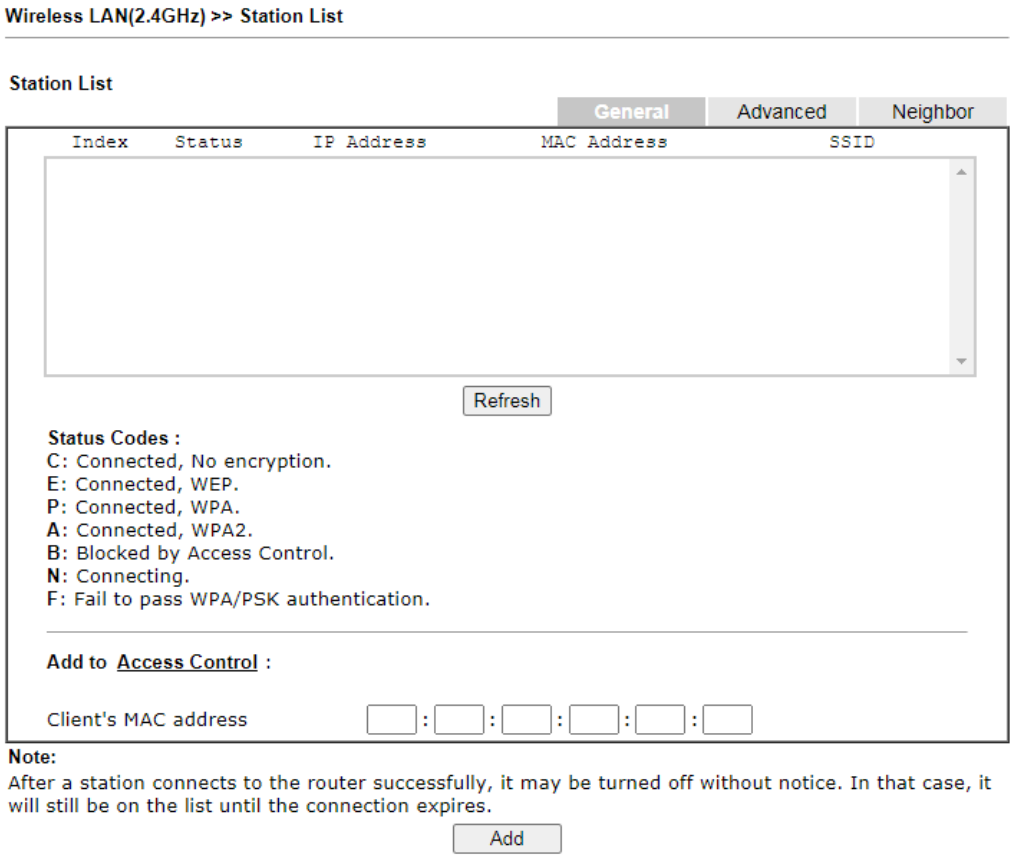
Item	Description
Disable RSSI Requirement	The Vigor router does not pay attention to the RSSI level of wireless stations. Selecting this option means the Vigor router will not interfere with the roaming behavior of wireless stations.
Strictly Minimum RSSI	The Vigor router will immediately disconnect the wireless station if its RSSI falls below the configured value.
Minimum RSSI	**Minimum RSSI -** The Vigor router will disconnect wireless clients whose RSSI falls below the minimum threshold only if there is also a neighboring wireless host (router or AP) that has an RSSI value (defined in the field of With Adjacent AP RSSI over) higher than a certain threshold. In order for this option to work, other wireless hosts connected to the same LAN subnet need to support the exchange of RSSI information with peer wireless hosts via Ethernet. **With Adjacent AP RSSI over -** Specify a value as a threshold.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

III-1-14 Station List

Station List provides an overview of all currently connected wireless clients and their status. As an added convenience, you may choose to add a particular wireless client to the Access Control by double clicking its entry in the list to populate the MAC address field, followed by clicking the Add button.

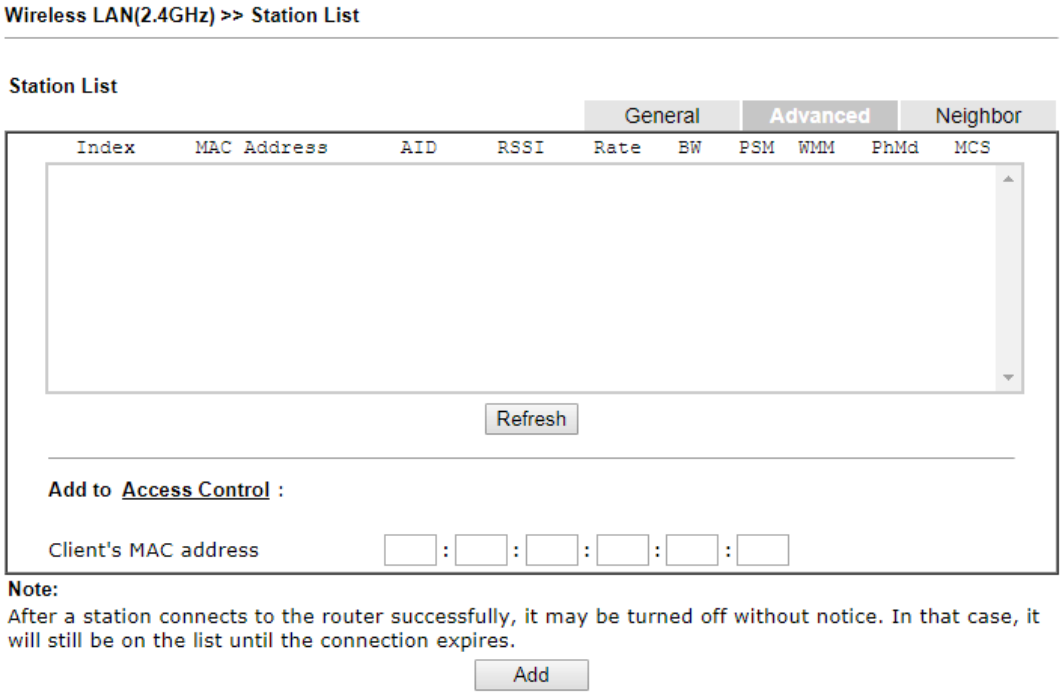
There are 3 tabs on the Station List screen: General, Advanced and Neighbor. Both General and Advanced show wireless stations connected to the Vigor router, whereas Neighbor shows nearby wireless stations connected to other access points that are detected by the Vigor router.



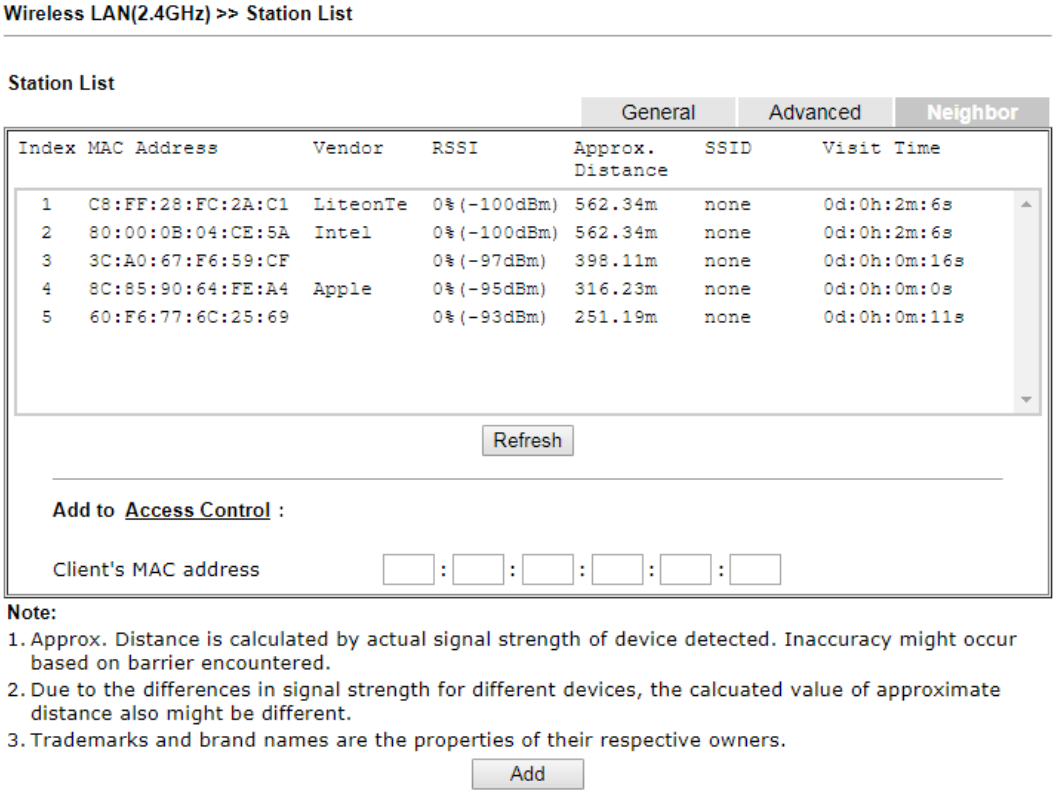
Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the station list.
Add	Click to add the address in the Client's MAC address field to Access Control.

Below shows the Advanced tab, which lists the same clients as the General tab, but with more detailed information.



Below shows the Neighbor tab, which lists wireless clients seen by the router but are not connected to the router's built-in access point.



Part IV 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.

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

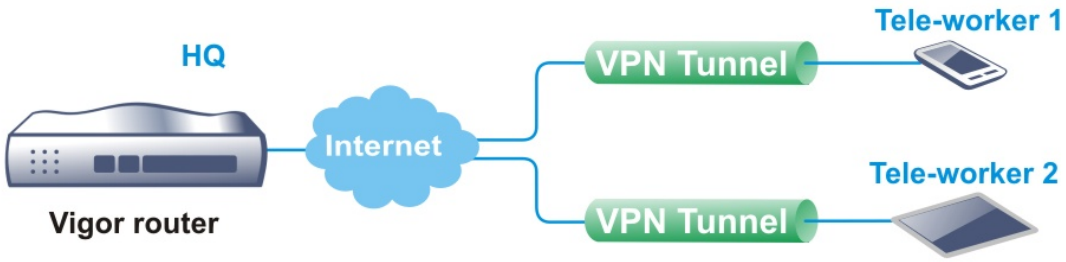
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is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

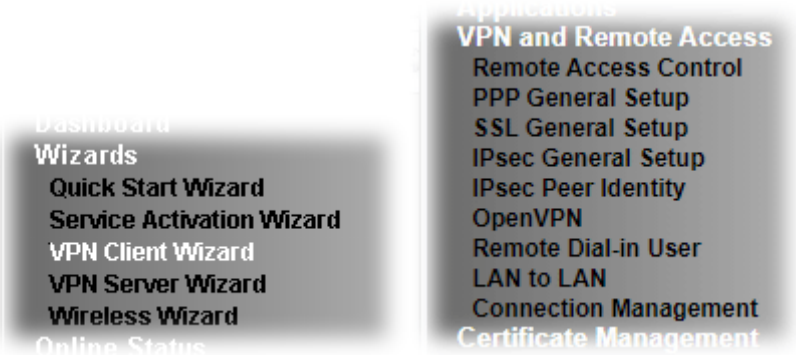
IV-1 VPN and Remote Access

A Virtual Private Network (VPN) is an extension of a private network that allows users to access network resources that available on the private network across shared or public networks such as the Internet, as if users are directly connected to the private network.

Here are some uses of VPNs:

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

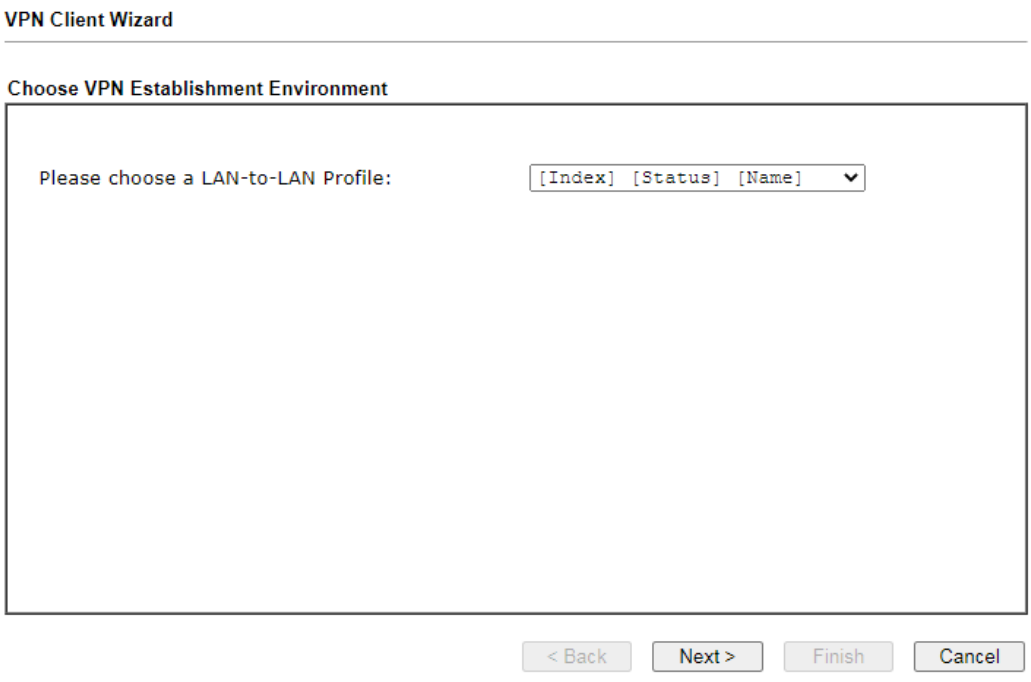




IV-1-1 VPN Client Wizard

The VPN Client Wizard will configure the router as a *client* to connect to a remote VPN server using a LAN-to-LAN VPN tunnel. The wizard will guide you through the setup process.

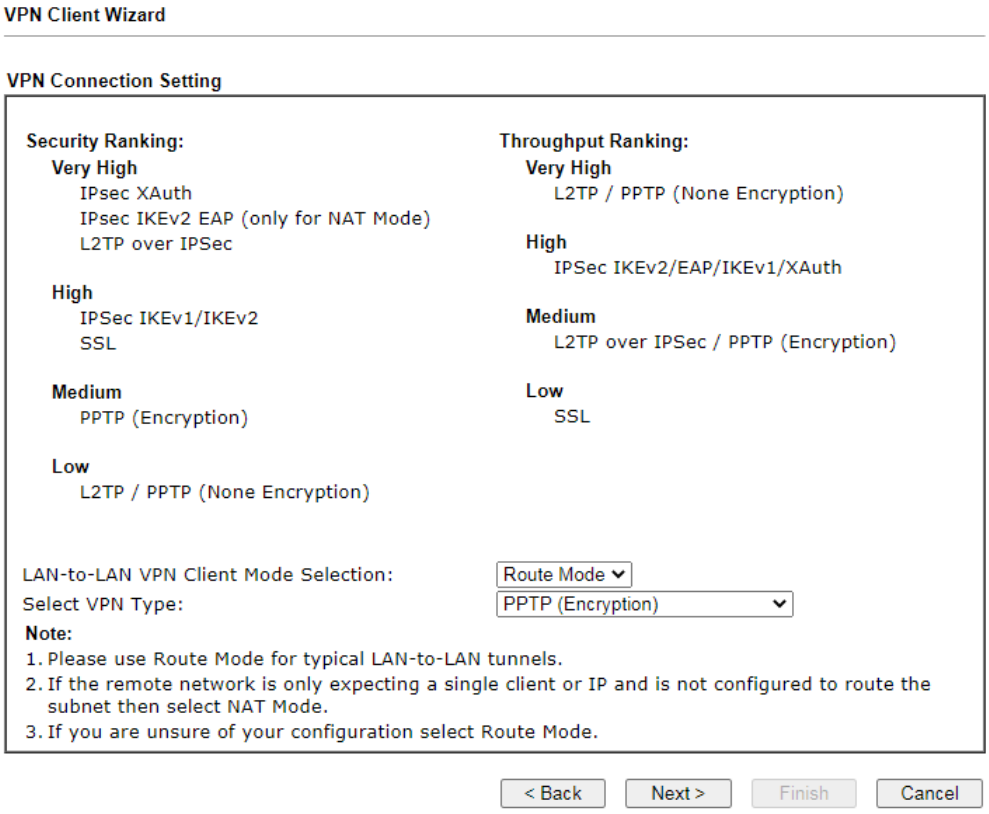
1. On the menu bar, click on **Wizards,** and then **VPN Client Wizard**.



Available settings are explained as follows:

Item	Description
Please choose a LAN-to-LAN Profile	The profile used to store this tunnel configuration. Selecting an index that has already been setup previously will result in the existing setup getting overwritten by the wizard.

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

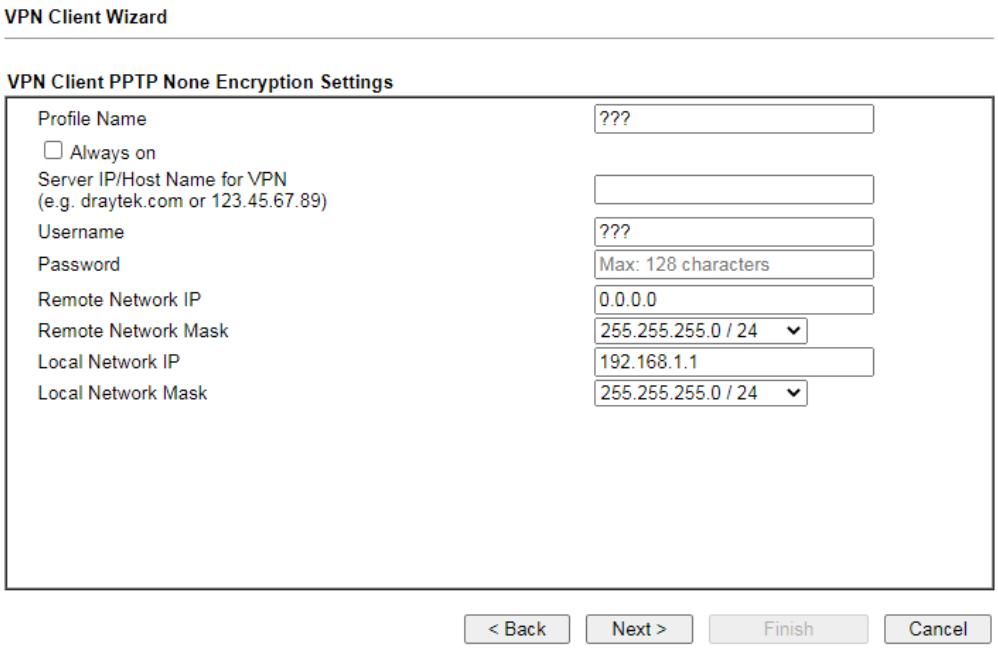


Available settings are explained as follows:

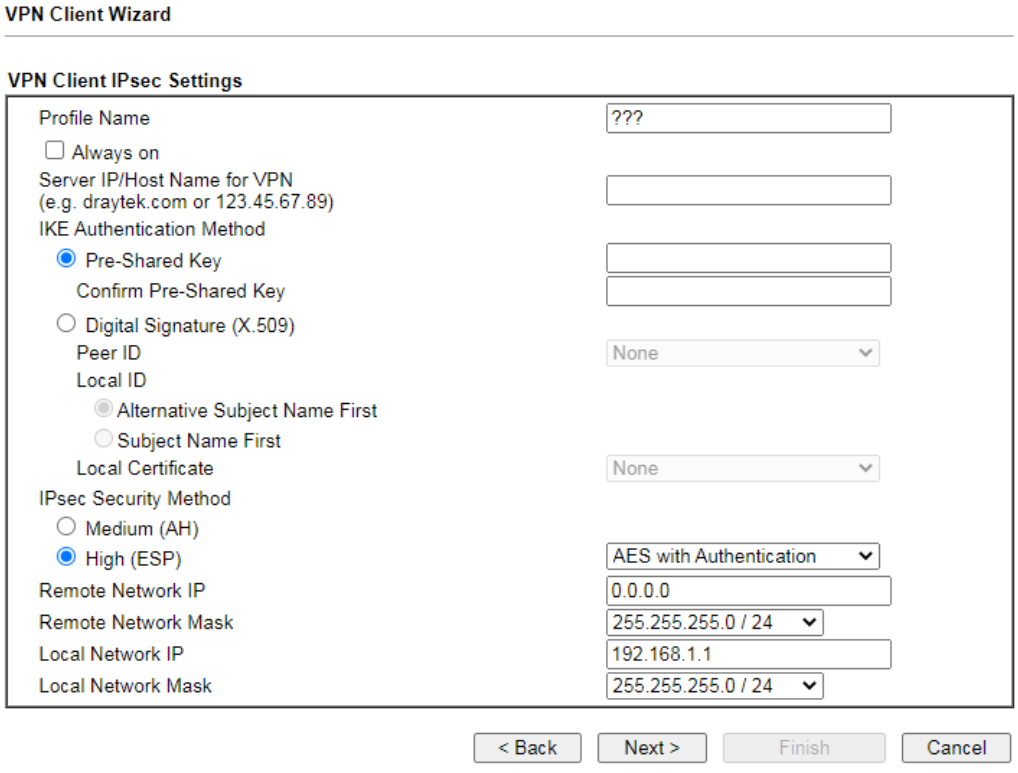
Item	Description
LAN-to-LAN Client Mode Selection	**Route Mode –** All traffic between the local network and the remote network bear the originating IP addresses. Select this if the VPN server can establish routes to handle inter-LAN traffic routing. **NAT Mode –** The VPN client (local router) uses a single IP address assigned by the VPN server (remote router) and uses NAT to keep track of the connections. Select this if the VPN server expects only one IP address on the local network to communicate with the remote network.
Select VPN Type	Select a VPN protocol for the LAN-to-LAN tunnel. Different VPN protocols offer different levels or security and performance.

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

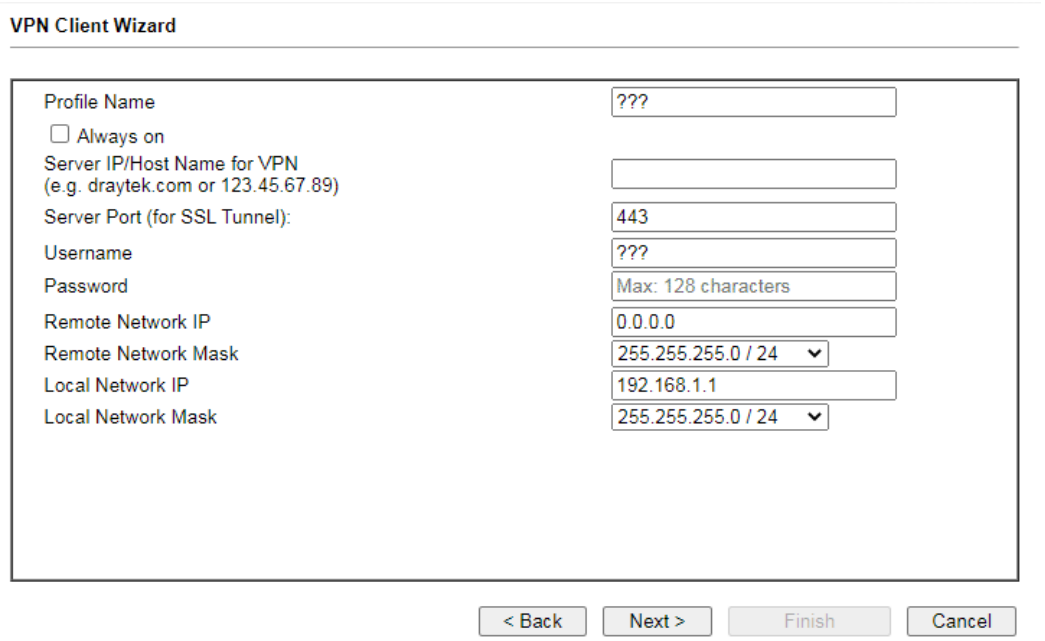
If you have selected **PPTP (None Encryption)** or **PPTP (Encryption)**, the following configuration screen appears.



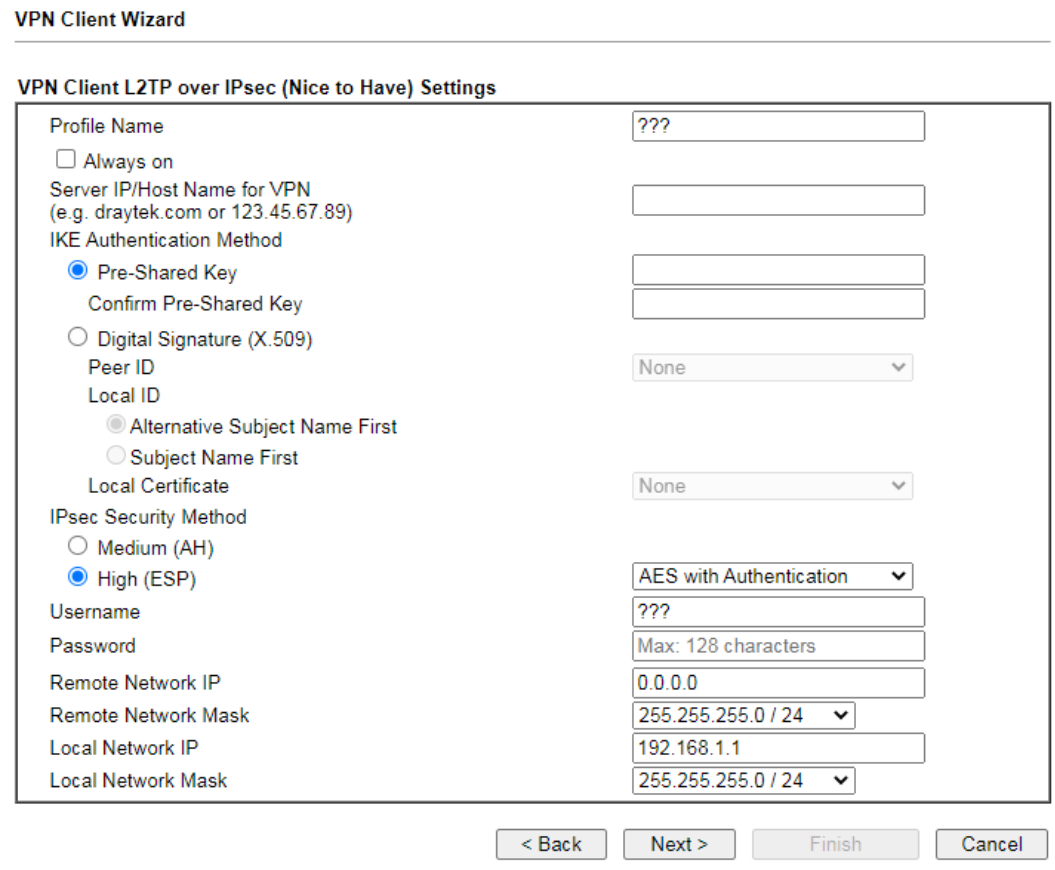
If you have selected **IPsec**, the following configuration screen appears.



If you have selected **SSL/L2TP**, the following configuration screen appears.



If you have selected **L2TP over IPsec (Nice to Have)** or **L2TP over IPsec (Must)**, the following configuration screen appears.

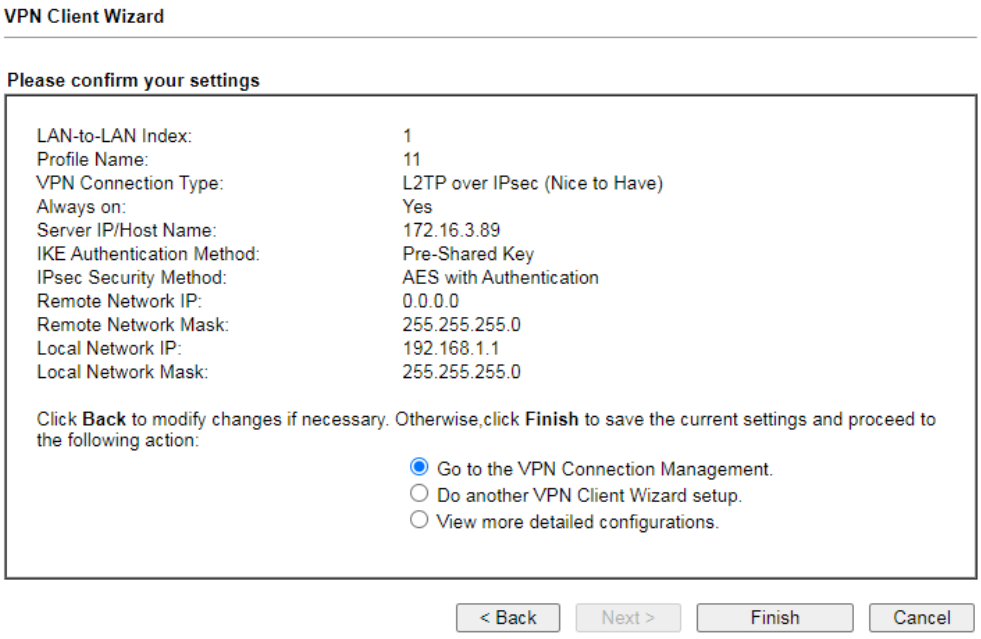


Available settings are explained as follows:

Item	Description

Profile Name	Name that identifies this profile. The maximum length of the Profile Name is 10 characters.
Always On	If selected, the router will maintain the VPN connection.
Server IP/Host Name for VPN	Enter the IP address or hostname of the server of the remote VPN server.
IKE Authentication Method	IKE Authentication Method to be used. Choose between **Pre-shared Key** and **Digital Signature (X.509)**. **Pre-shared Key** ● **Pre-Shared Key-** Specify a key for IKE authentication. ● **Confirm Pre-Shared Key-**Confirm the pre-shared key. **Digital Signature (X.509)** ● **Peer ID** – Select Peer ID from the dropdown list. Peer IDs are managed using VPN and Remote Access >> IPsec Peer Identity. ● **Local ID** – Select **Alternative Subject Name First** or **Subject Name Firs**t. ● **Local Certificate** – Select a certificate from the dropdown list. Local certificates are managed using **Certificate Management >> Local Certificate.**
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 enter 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 you have entered all the required information, click **Next** to proceed to the confirmation page. The confirmation page shows a summary of all the settings. If you need to make adjustments to the settings, click **Back** to return to the previous page. Otherwise, select one of the following actions and click **Finish** to save the changes to the LAN-to-LAN VPN profile.



Available settings are explained as follows:

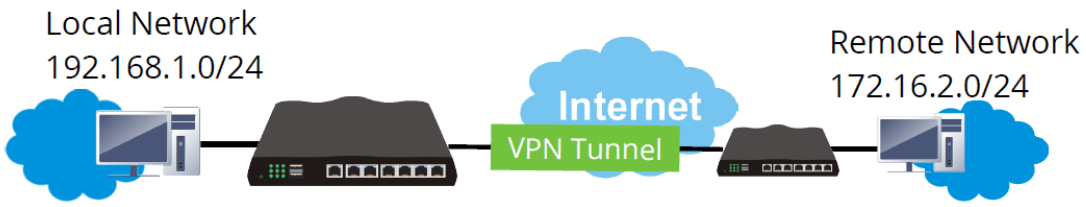
Item	Description
Go to the VPN Connection Management	Proceed to **VPN and Remote Access>>Connection Management** to manage VPN sessions.
Do another VPN Client Wizard Setup	Rerun the VPN Client Wizard to configure another LAN-to-LAN VPN profile.
View more detailed configuration	Open this profile in **VPN and Remote Access>>LAN to LAN** to make additional configuration changes.

IV-1-2 VPN Server Wizard

The VPN Server Wizard can be used to set the router up as a *server* that accepts inbound VPN connections from a VPN server using a LAN-to-LAN VPN tunnel.

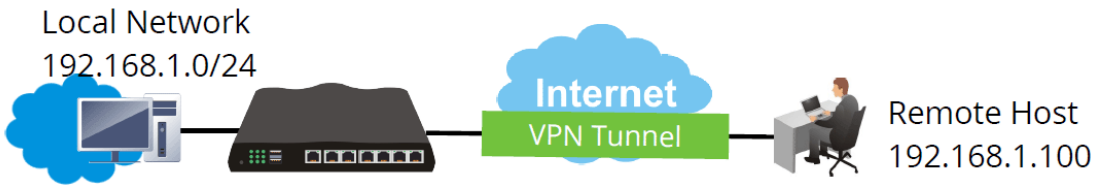
Site-to-Site (LAN-to-LAN)

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



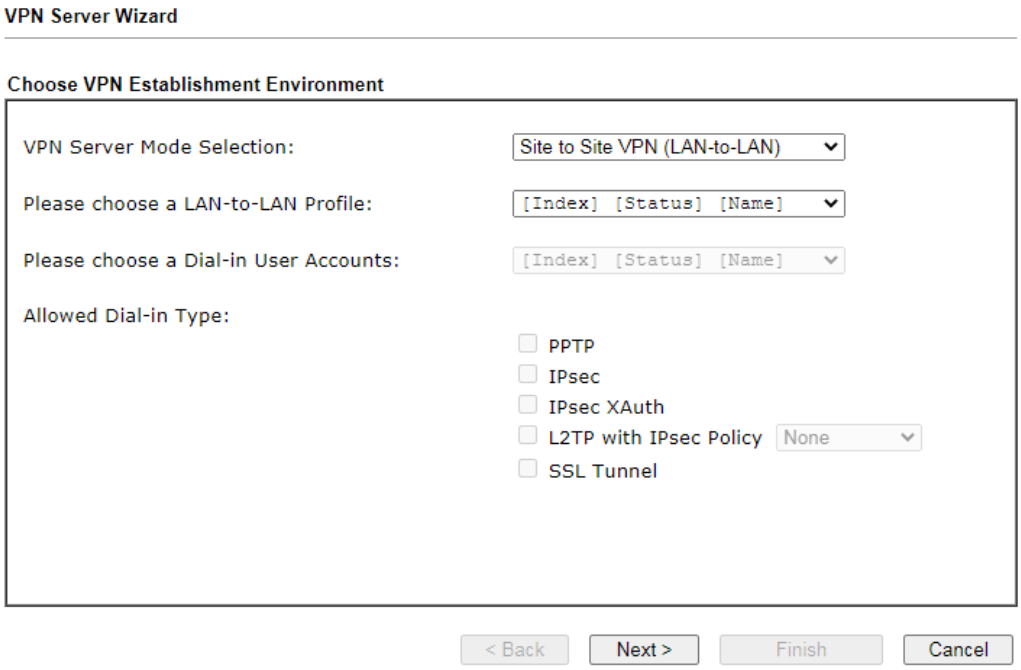
Remote Access (Remote Dial-in)

- 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.



The wizard will guide you step by step through the setup process.

1. On the menu bar, click on **Wizards,** and then **VPN Server Wizard**.

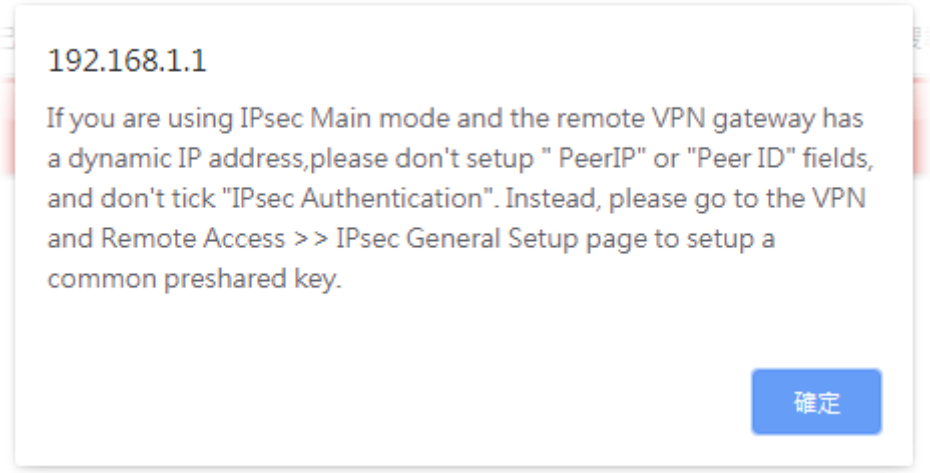


Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	Type of VPN Server to be configured. **Site to Site VPN (LAN-to-LAN)** - Configures the VPN server for inbound connections from other routers. **Remote Dial-in User (Teleworker)** - Configures VPN server for inbound connections from remote users.
Please choose a LAN-to-LAN Profile	If the VPN Server Mode selected was **Site to Site VPN (LAN-to-LAN)**, choose a LAN-to-LAN profile to store this configuration.
Please choose a Dial-in User Accounts	If the VPN Server Mode selected was **Remote Dial-in User (Teleworker)**, choose a Dial-in user profile to store this configuration.
Allowed Dial-in Type	Select all VPN protocols that are allowed for this LAN-to-LAN Profile or Dial-in User Account. 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**.

3. The following dialog box appears, reminding you to not configure IPsec fields if the remote location has a dynamic IP address.

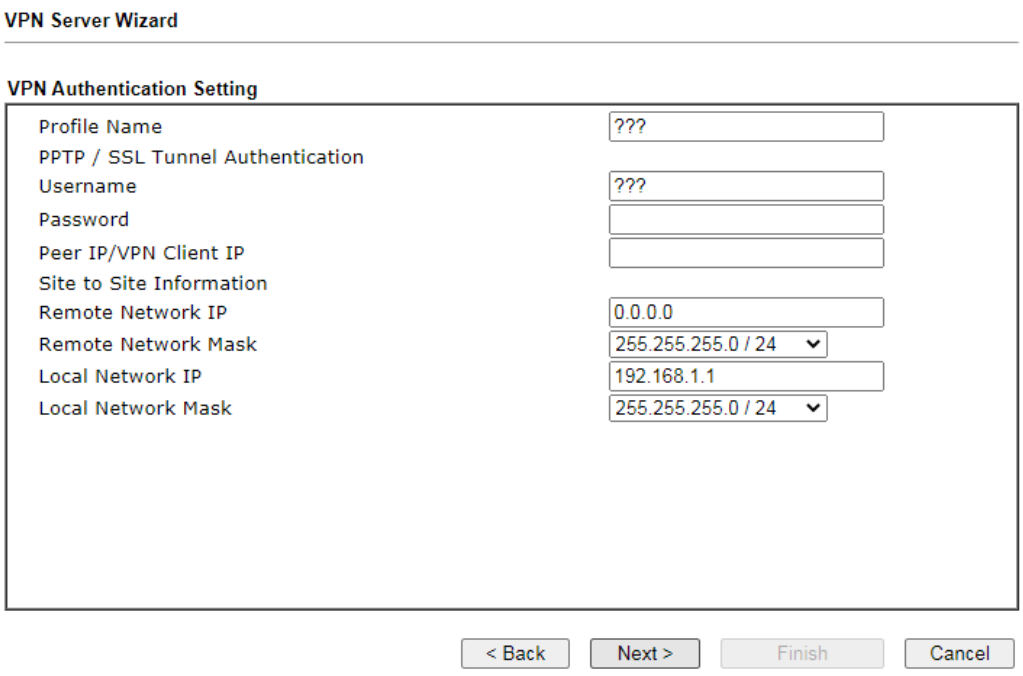


Click **OK** to dismiss the dialog box and proceed to the next page.

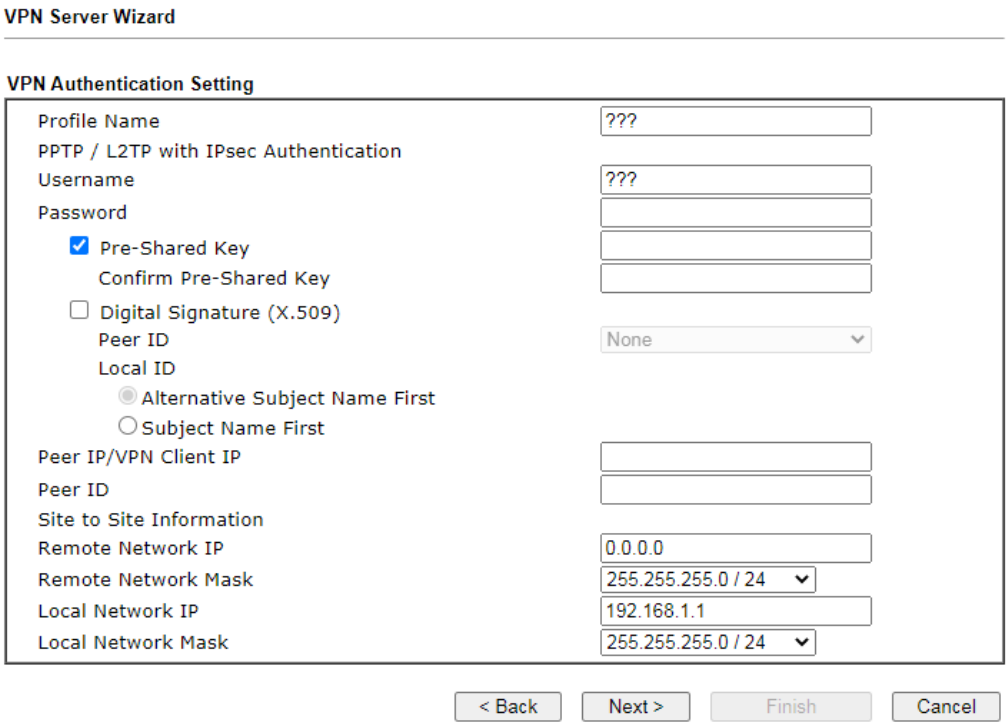
If you have chosen to configure a LAN-to-LAN VPN profile, proceed to step 4.

If you have chosen to configure a Remote Dial-in User VPN profile, proceed to step 5.

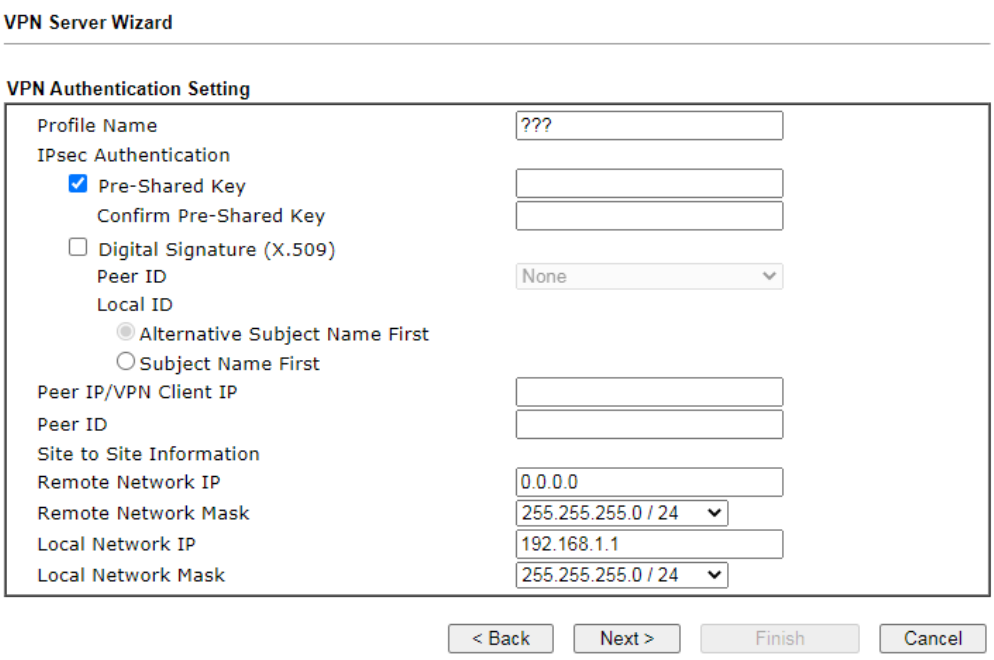
4. The **Site to Site VPN (LAN-to-LAN)** configuration page appears as follows if you have selected **PPTP/SSL**.



If you have selected **PPTP & IPsec & L2TP** (three types) or **PPTP & IPsec** (two types) or **L2TP with Policy (Nice to Have/Must),** the following configuration screen appears.



If you have selected **IPsec,** the following configuration screen appears.

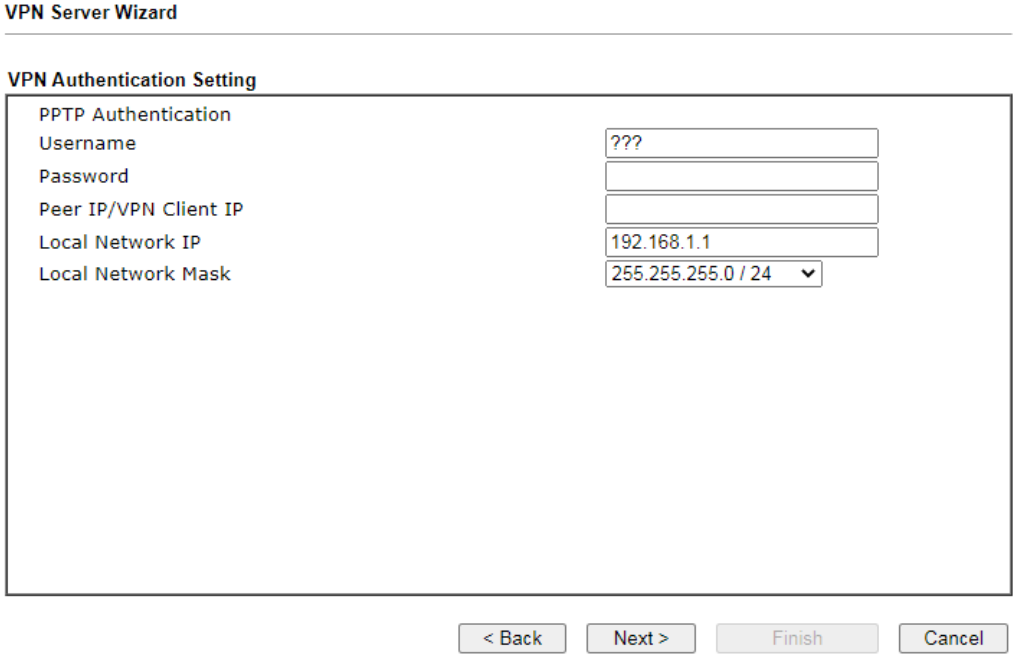


Available settings are explained as follows:

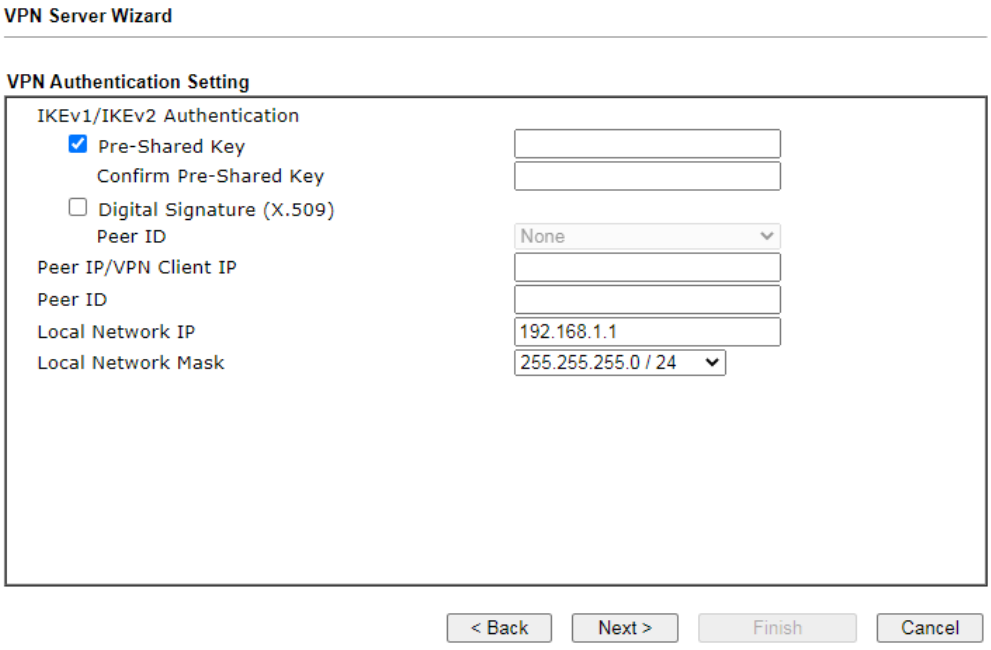
Item	Description
Profile Name	Name to identify this VPN profile.
User Name	Used by the remote LAN to establish a VPN connection. The length of the user name is limited to 11 characters.

Password	Used by the remote LAN to establish a VPN connection. The length of the password is limited to 11 characters.
IPsec / IPsec XAuth / L2TP with IPsec / SSL Tunnel Authentication	
Pre-Shared Key	For PPTP / IPsec / IPsec XAuth / L2TP with IPsec / SSL Tunnel authentication, you have to configure a pre-shared key and/or digital signature. Note that, if the remote client has a dynamic IP address, do not enable any of the settings (PSK / Digital Signature) in this section. Instead, configure the global IPsec settings by using VPN and Remote Access>>IPsec General Setup. **Pre-Shared Key** - Select to enter an IPsec Pre-shared Key specific to this profile. The length of the PSK is limited to 64 characters. **Confirm Pre-Shared Key** - Re-enter the Pre-shared Key again to confirm.
Digital Signature (X.509)	**Digital Signature (X.509) -** Select to enable X.509 digital signature. **Peer ID** – Select a predefined X.509 digital signature as the Peer ID. Peer IDs must be configured first using VPN and Remote Access>>IPsec Peer Identity. **Local ID** – Specifies whether the Subject Name or the Alternative Subject Name of the X.509 Peer ID is to be checked first. Select either **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. If values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Peer ID	Enter the ID name for the remote client. The maximum length of the peer ID is 47 characters. If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Site to Sit Information	
Remote Network IP	Enter the IP address of the remote network.
Remote Network Mask	Enter the subnet mask of the remote network.
Local Network IP	Enter the local network IP for TCP / IP configuration.
Local Network Mask	Enter the local network mask for TCP / IP configuration.

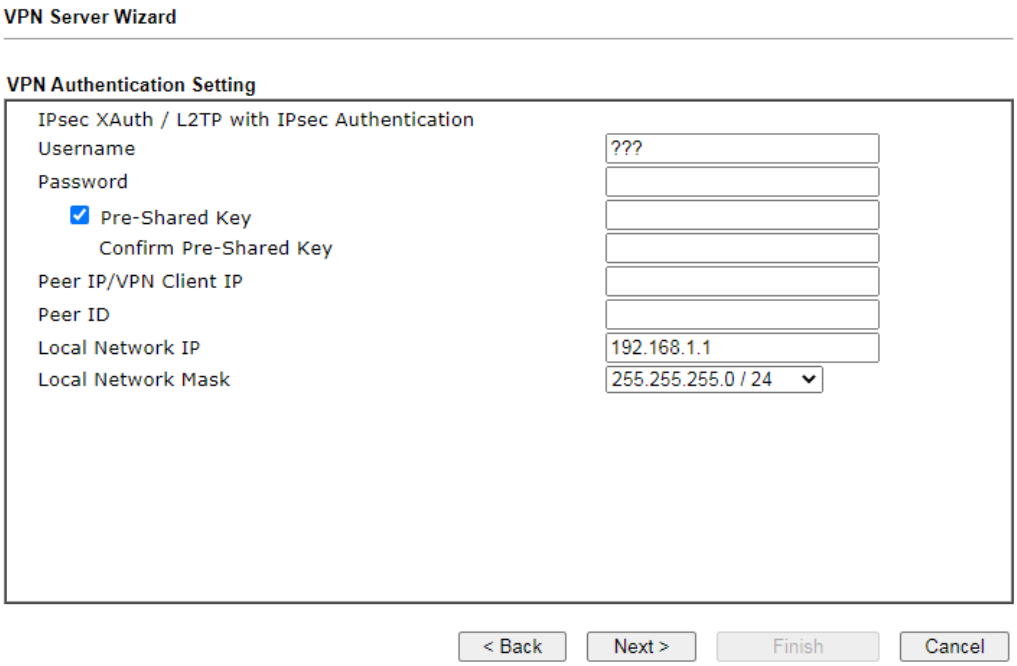
5. The Remote Dial-in User (Teleworker) VPN configuration page appears as follows if you have selected **PPTP/SSL/IKEv2 EAP**.



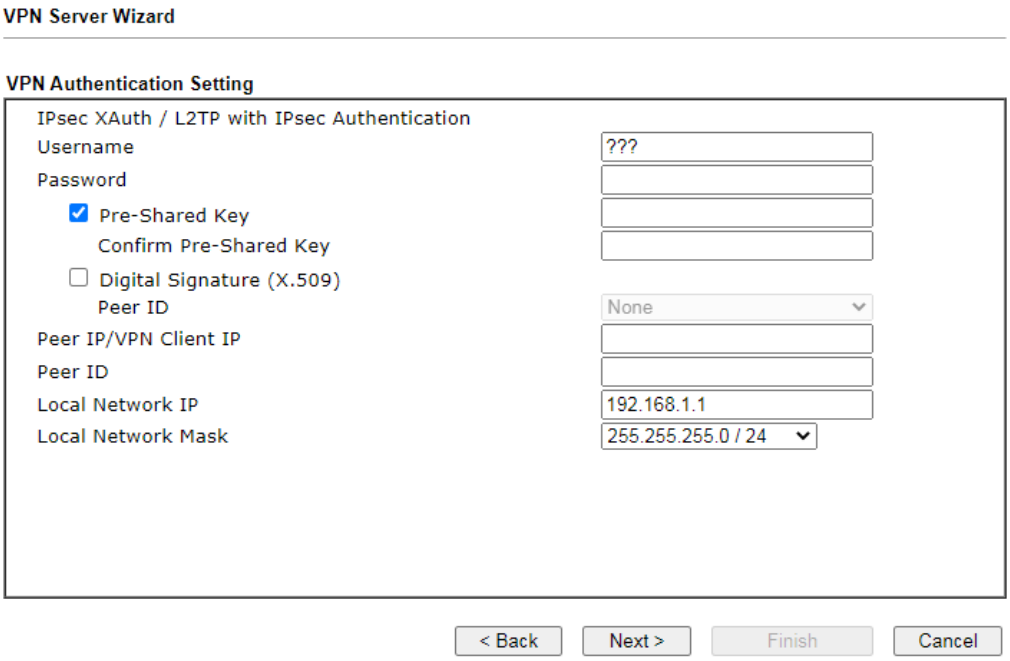
If you have selected **IKEv1/IKEv2,** the following configuration screen appears.



If you have selected **IPsec XAuth/L2TP with IPsec Policy (None),** the following configuration screen appears.



If you have selected **IPsec XAuth/L2TP with IPsec Policy (Nice to Have)/L2TP with IPsec Policy (Must),** the following configuration screen appears.

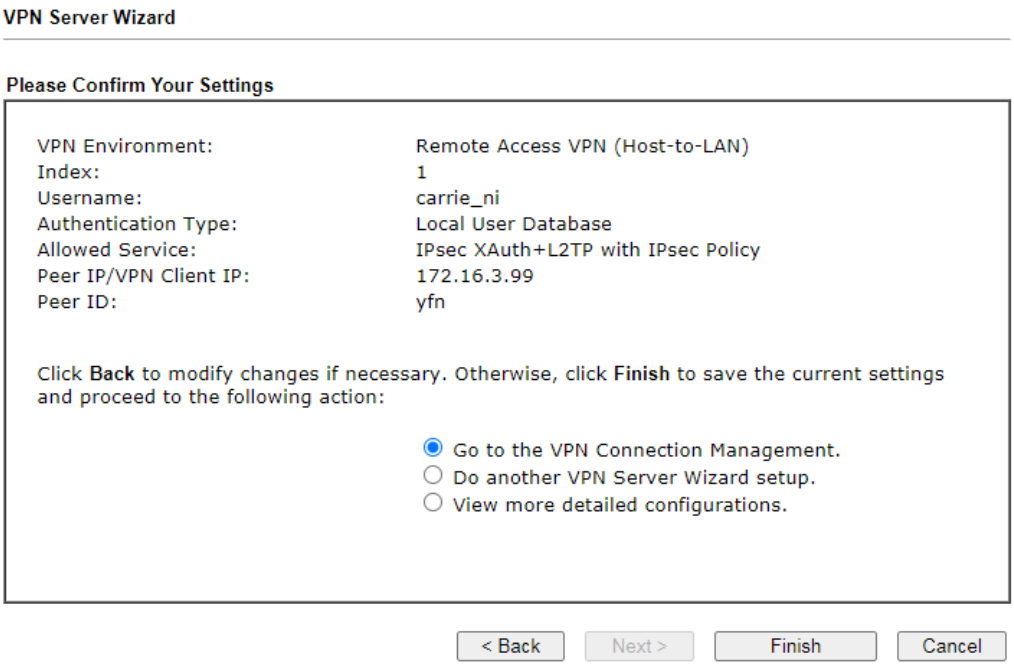


Available settings are explained as follows:

Item	Description
User Name	Used by the remote LAN to establish a VPN connection. The length of the user name is limited to 11 characters.
Password	Used by the remote LAN to establish a VPN connection.

	The length of the password is limited to 11 characters.
IKEv1/IKEv2 / IPsec XAuth / L2TP with IPsec /SSL Tunnel Authentication	
Pre-Shared Key	For IKEv1/IKEv2 / IPsec / IPsec XAuth / L2TP with IPsec / SSL Tunnel authentication, you have to configure a pre-shared key and/or digital signature. Note that, if the remote client has a dynamic IP address, do not enable any of the settings (PSK / Digital Signature) in this section. Instead, configure the global IPsec settings by using VPN and Remote Access>>IPsec General Setup. **Pre-Shared Key** - Select to enter an IPsec Pre-shared Key specific to this profile. The length of the PSK is limited to 64 characters. **Confirm Pre-Shared Key** - Re-enter the Pre-shared Key again to confirm.
Digital Signature (X.509)	**Digital Signature (X.509) -** Select to enable X.509 digital signature. **Peer ID** – Select a predefined X.509 digital signature as the Peer ID. Peer IDs must be configured first using VPN and Remote Access>>IPsec Peer Identity.
Peer IP/VPN Client IP	Enter the WAN IP address or VPN client IP address for the remote client. If values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Peer ID	Enter the ID name for the remote client. The maximum length of the peer ID is 47 characters. If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Local Network IP	Enter the local network IP for TCP / IP configuration.
Local Network Mask	Enter the local network mask for TCP / IP configuration.

6. After finishing the configuration, click **Next** to proceed to the confirmation page.



Available settings are explained as follows:

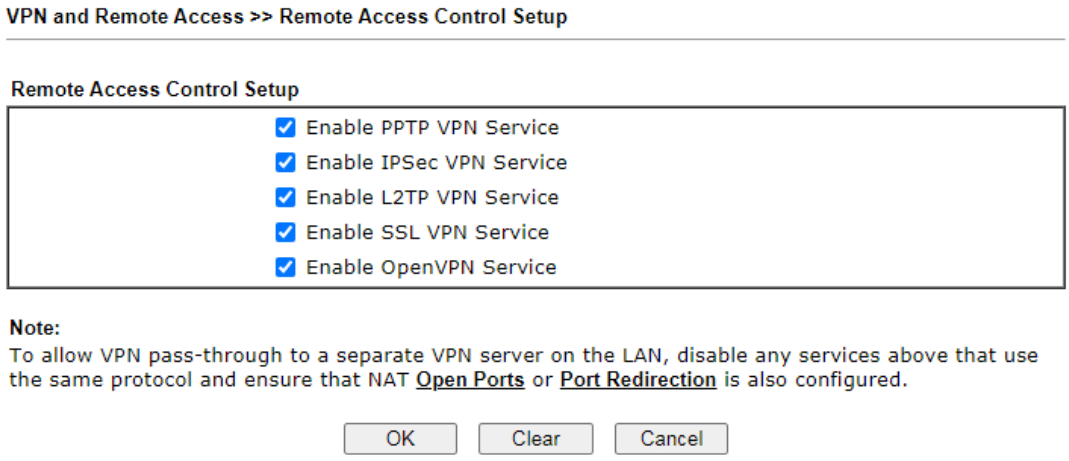
Item	Description
Go to the VPN Connection Management	Proceed to **VPN and Remote Access>>Connection Management** to manage VPN sessions.
Do another VPN Server Wizard Setup	Rerun the VPN Server Wizard to configure another LAN-to-LAN VPN profile.
View more detailed configuration	Open this profile in **VPN and Remote Access>>LAN to LAN** to make additional configuration changes.

7. Click **Finish** to save the profile, or **Back** to make changes, or **Cancel** to exit the wizard without saving.

IV-1-3 Remote Access Control

The Vigor router supports several protocols for VPNs, all of which can be enabled or disabled independently of one another.

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**.

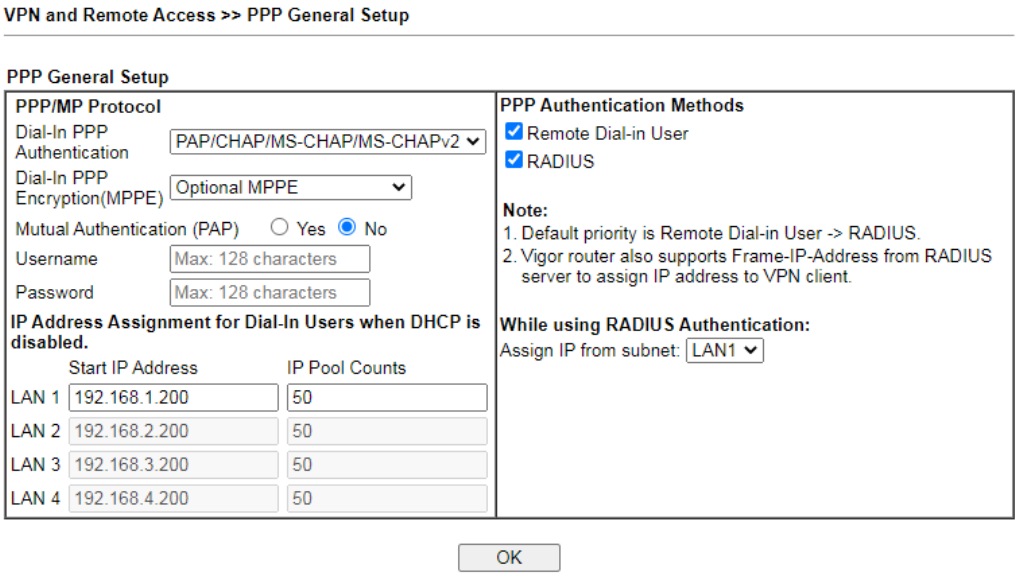


Item	Description
Enable PPTP VPN Service	This is the one of the earliest VPN protocols and is natively supported by all Microsoft Windows versions since Windows 95, all Android devices, iOS devices before version 10, and Mac OS X before version 10.12. It is easy to set up, has low overhead, and moderately secure.
Enable IPSec VPN Service	This is a network protocol that encrypts traffic between two network locations. Windows, by means of Windows Firewall, natively supports IPsec tunnels between endpoints with static IP addresses. For computers with dynamically-assigned IP addresses, DrayTek provides the SmartVPN client .
Enable L2TP VPN Service	This is a tunneling protocol used in VPNs. It does not encrypt network traffic unless used in conjunction with IPsec.
Enable SSL VPN Service	This type of VPN uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are also used to encrypt traffic to and from websites. Since SSL and TLS work on top of TCP and UDP, which are the most common internet protocols, they are less likely to be have issues with firewalls and gateways.
Enable OpenVPN Service	This type of VPN offers a convenient way for users to build VPN between local end and remote end.

To save changes on the page, select **OK**; to discard changes, select **Cancel**; to clear settings on this page and revert to default settings, select **Clear**.

IV-1-4 PPP General Setup

This page allows configuration of Point-to-Point Protocol (PPP) used by PPTP and L2TP VPN connections. From the Main Menu select **VPN and Remote Access >> PPP General Setup** to bring up the following configuration page.



Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	**PAP Only** - Authenticate dial-in users using the PAP protocol only. **PAP/CHAP/MS-CHAP/MS-CHAPv2** - Attempt to authenticate dial-in users using various CHAP protocols, and if the remote VPN client fails to authenticate, fall back to PAP.
Dial-In PPP Encryption (MPPE)	Specifies if PPP encryption (MPPE) is to be used for dial-in VPN connections. **Optional MPPE** - MPPE is optional. If the VPN client supports MPPE, PPP data will be encrypted. **Require MPPE (40/128bits) -** Require PPP encryption for dial-in VPN connections. Both 40- and 128-bit encryption schemes are allowed. 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 -** Require 128-bit PPP encryption for all dial-in VPN connections.
Mutual Authentication (PAP)	Specifies if mutual authentication is to be used. Some VPN peers (e.g., certain Cisco routers) require bi-directional authentication used for providing stronger security. When mutual authentication is enabled, Username and Password fields should also be populated using values from the VPN peer. The maximum lengths of these fields are 23 and 19 characters, respectively. **Yes** – Enable mutual authentication.

	No – Disable mutual authentication.
IP Address Assignment for Dial-In Users when DHCP is disabled	**LAN1** - When the router's DHCP server is disabled, the router will assign IP addresses to dial-in VPN users starting with the IP address specified in Start IP Address. The total number of dial-in VPN IP addresses to be given out is specified in IP Pool Counts. LAN2 ~ LAN4 will be available if it is enabled. Refer to LAN>>General Setup for enabling the LAN interface.
PPP Authentication Methods	The credentials to be used for PPP authentication will be obtained from the selected sources, in the following order: **Remote Dial-in User** – The usernames and passwords in VPN and Remote Access >> Remote Dial-in User section will be used. **RADIUS** – An external RADIUS server is to be used for authentication. Please be sure to set up the RADIUS server in Applications >> RADIUS/TACACS+ section.
While using Radius or LDAP Authentication	When the dial-in VPN user is authenticated using credentials from the Remote Dial-in User section, an IP address from the LAN specified in the user profile will be assigned. When the user is authenticated using credentials from other sources (RADIUS), the assigned IP address will be drawn from the address pool of the LAN specified here.

To save changes on the page, select **OK**.

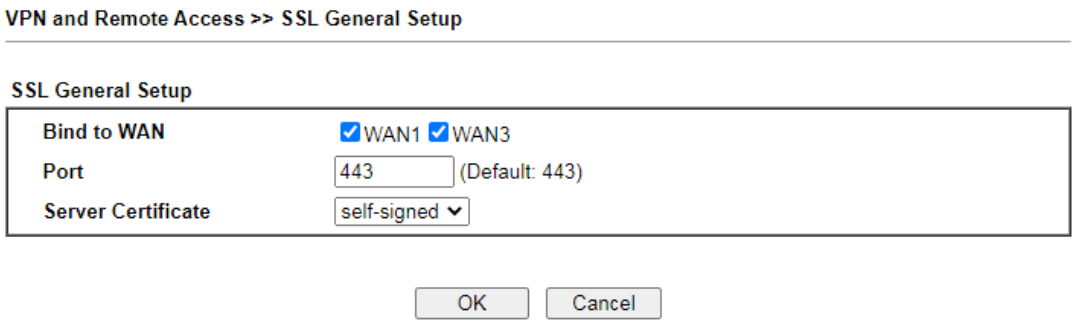
IV-1-5 SSL General Setup

SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that encrypts traffic using SSL, which is the same technology used on secured websites. Because of SSL's prominence as an encryption protocol on the Internet, most networks have few restrictions on SSL traffic, and as a result SSL VPN is more likely to work when other VPN technologies experience difficulties due to obstacles such as firewalls and Network Address Translation (NAT).

In short,

- 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.

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



Available settings are explained as follows:

Item	Description
Bind to WAN	Select the WAN interfaces to accept inbound SSL VPN connections.
Port	The port to be used for SSL VPN server. This is separate from the management port (HTTPS Port) which is configured in **System Maintenance>>Management.** The default setting is 443.
Server Certificate	Specify the certificate to be used for SSL connections. Select a certificate from imported or generated certificates on the router, or choose Self-signed to use the router's built-in default certificate. The selected certificate can be used in SSL VPN server and HTTPS Web Proxy.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

IV-1-6 IPsec General Setup

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

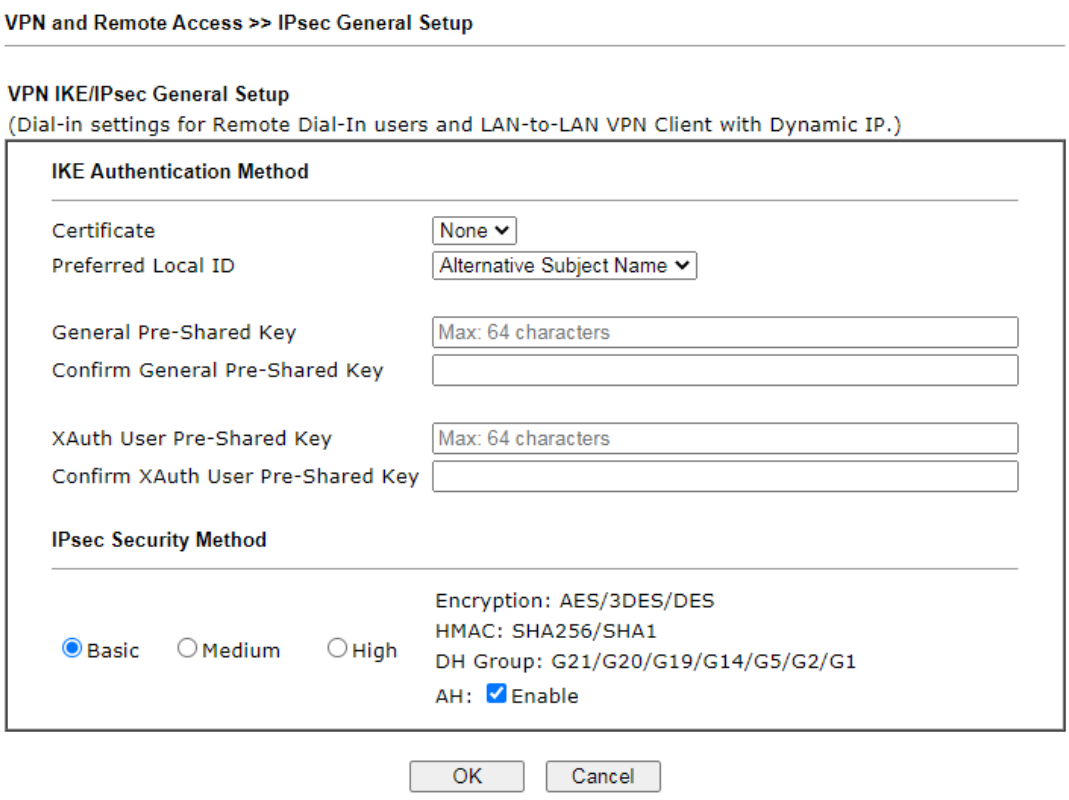
There are two phases of IPsec.

- 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.

AH (Authentication Header) 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.

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



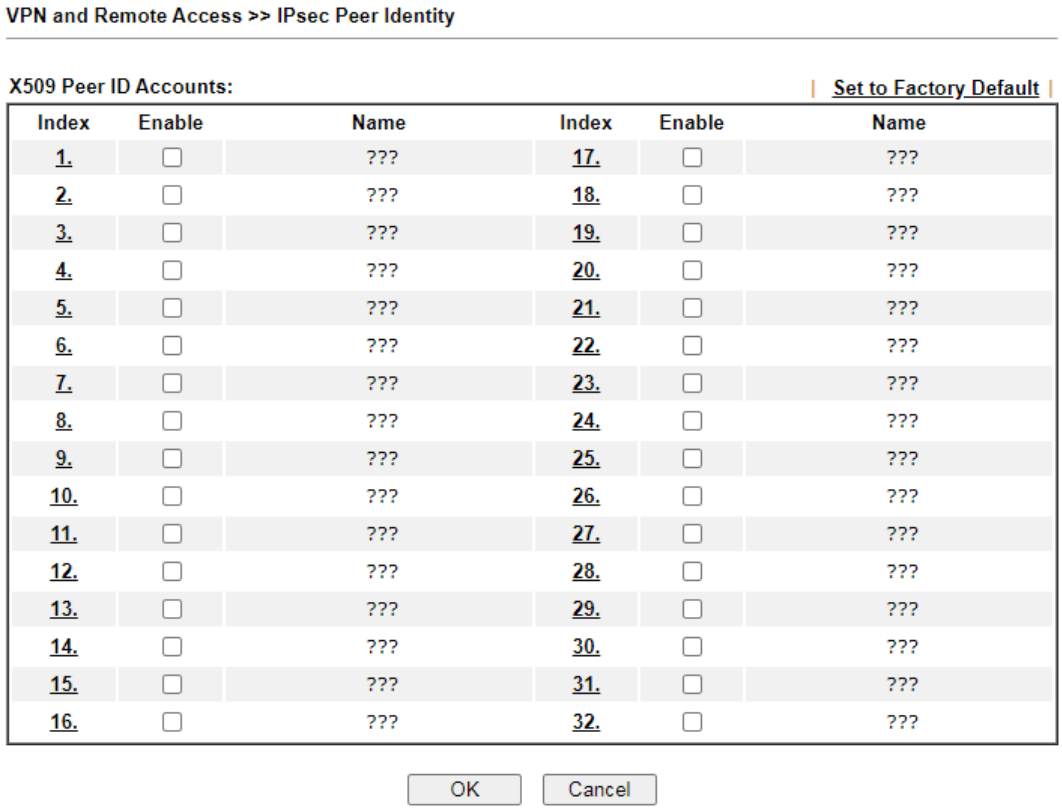
Available settings are explained as follows:

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.

To save changes on the page, select **OK**; to discard changes, select **Cancel**.

IV-1-7 IPsec Peer Identity

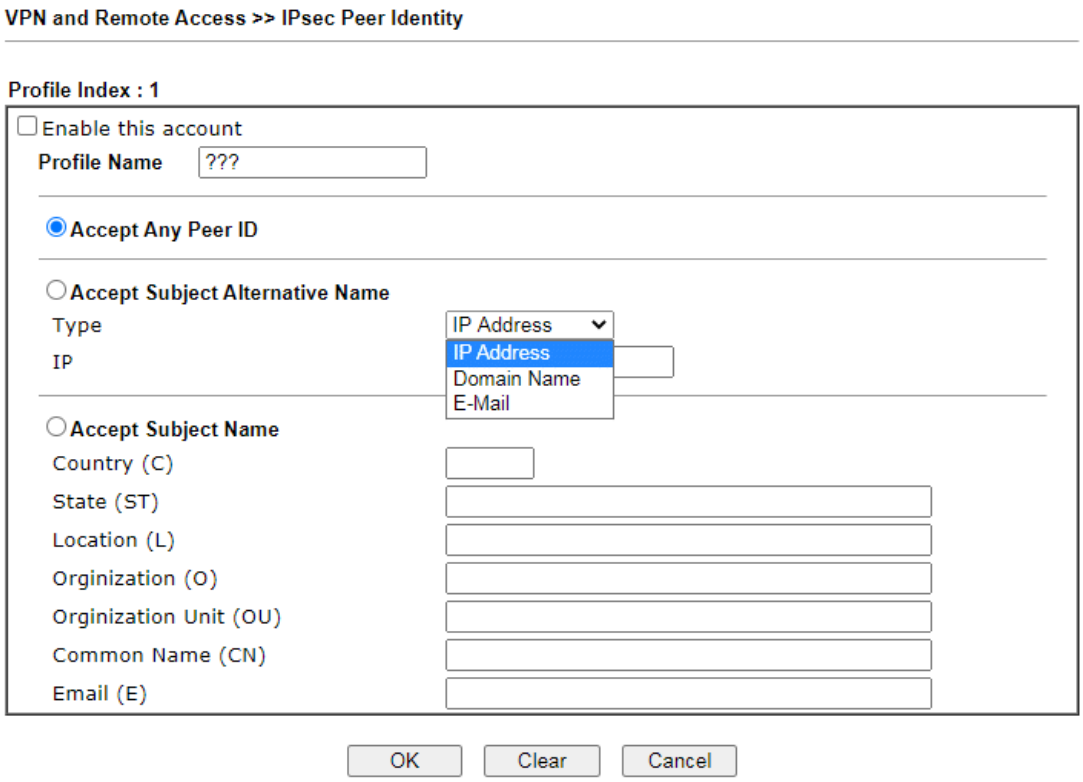
This screen allows creating profiles of subject alternative names (SANs) and distinguished names/subject names that can be used for IPsec peer authentication in LAN-to-LAN or remote user dial-in VPN connections.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the index number of the profile the view or edit its settings.
Enable	Check to enable the profile.
Name	User-entered name that identifies the profile.

The following setup screen is shown after a profile index has been clicked.



Available settings are explained as follows:

Item	Description
Enable this account	Check to enable such account profile.
Profile Name	A name that allows you to identify this profile. The maximum length of the name you can set is 32 characters.
Accept Any Peer ID	When this option is selected, the router accepts any subject alternative name or subject name as valid, regardless of the type and value.
Accept Subject Alternative Name	When this option is selected, the router accepts the type and value of the specified subject alternative name as valid authentication. Supported subject alternative types are **IP Address**, **Domain Name** and **E-Mail**.
Accept Subject Name	When this option is selected, the router performs peer authentication by matching the values of the different subject name fields. These fields include **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN),** and **Email (E)**.

To save changes on the page, select **OK**; to discard changes, select **Cancel**; to clear settings on this page and revert to default settings, select **Clear**.

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.

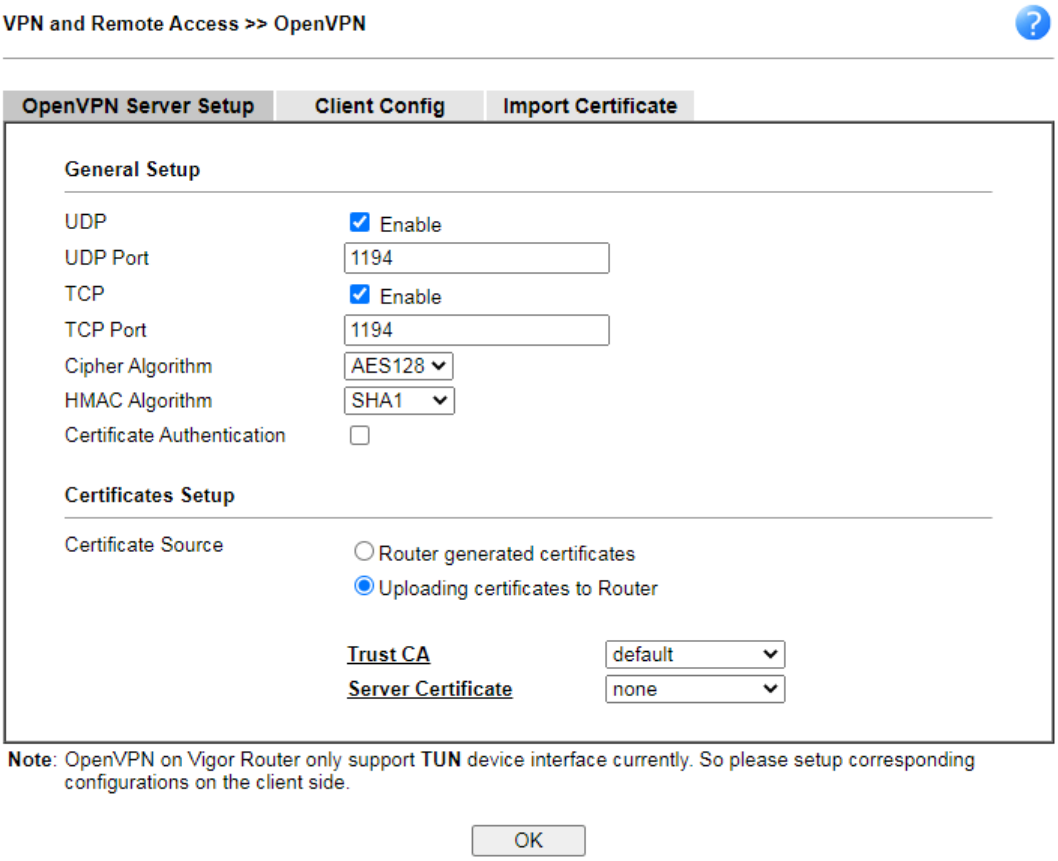
OpenVPN offers a convenient way for users to build a VPN between the local end and the remote end. There are two advantages of OpenVPN:

- 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:

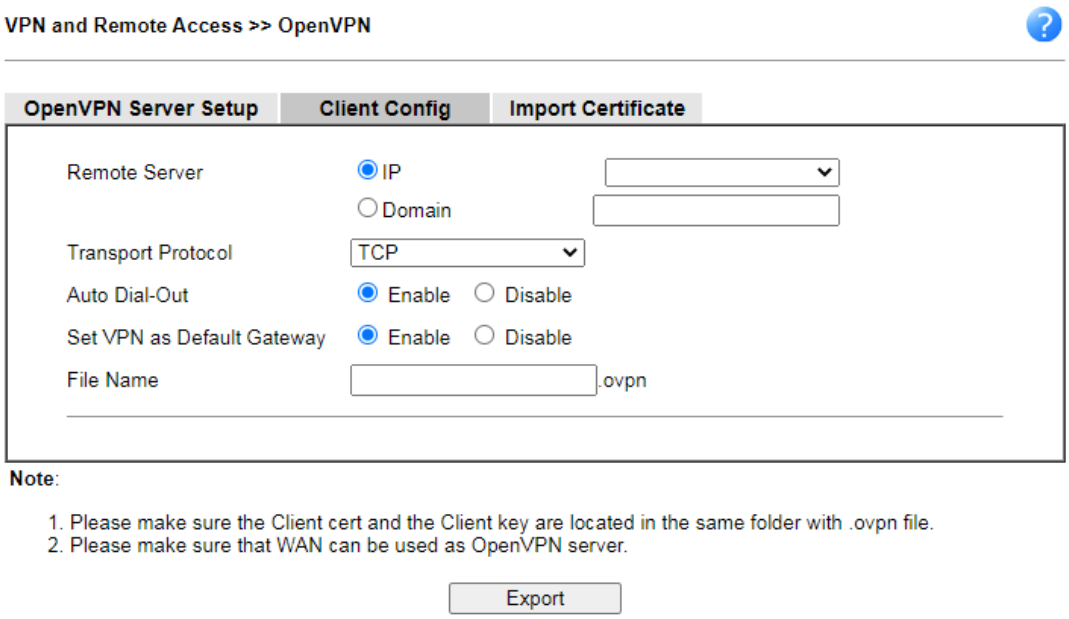
Item	Description
General Setup	
UDP	**Enable -** Select checkbox to enable UDP protocol for OpenVPN connections. **UDP Port** – Enter the UDP port number.
TCP	**Enable -** Select checkbox to enable TCP protocol for OpenVPN connections. **TCP Port** – Enter the TCP port number.
Cipher Algorithm	Select 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.

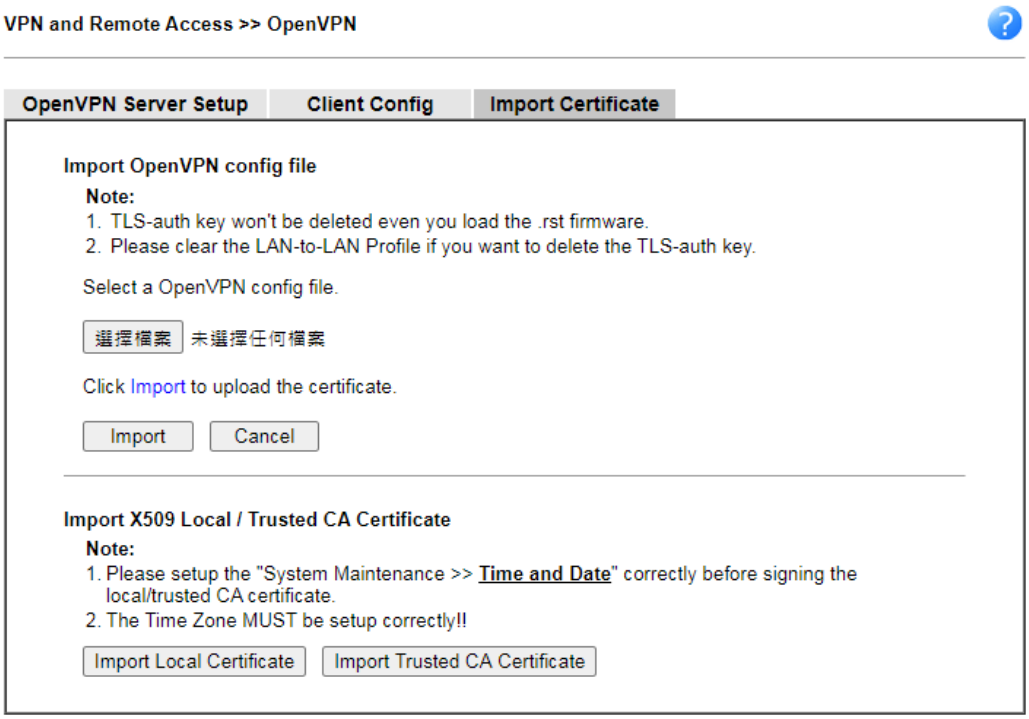


Available settings are explained as follows:

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.
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 Gateway	**Enable** - If selected, the Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel. **Disable** - Select to disable the function.
File Name	Enter the filename of the configuration file to be downloaded from the router.
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-1-8-3 Import Certificate

On this page, you can import the certificate from other places for a remote OpenVPN client to connect to the router.



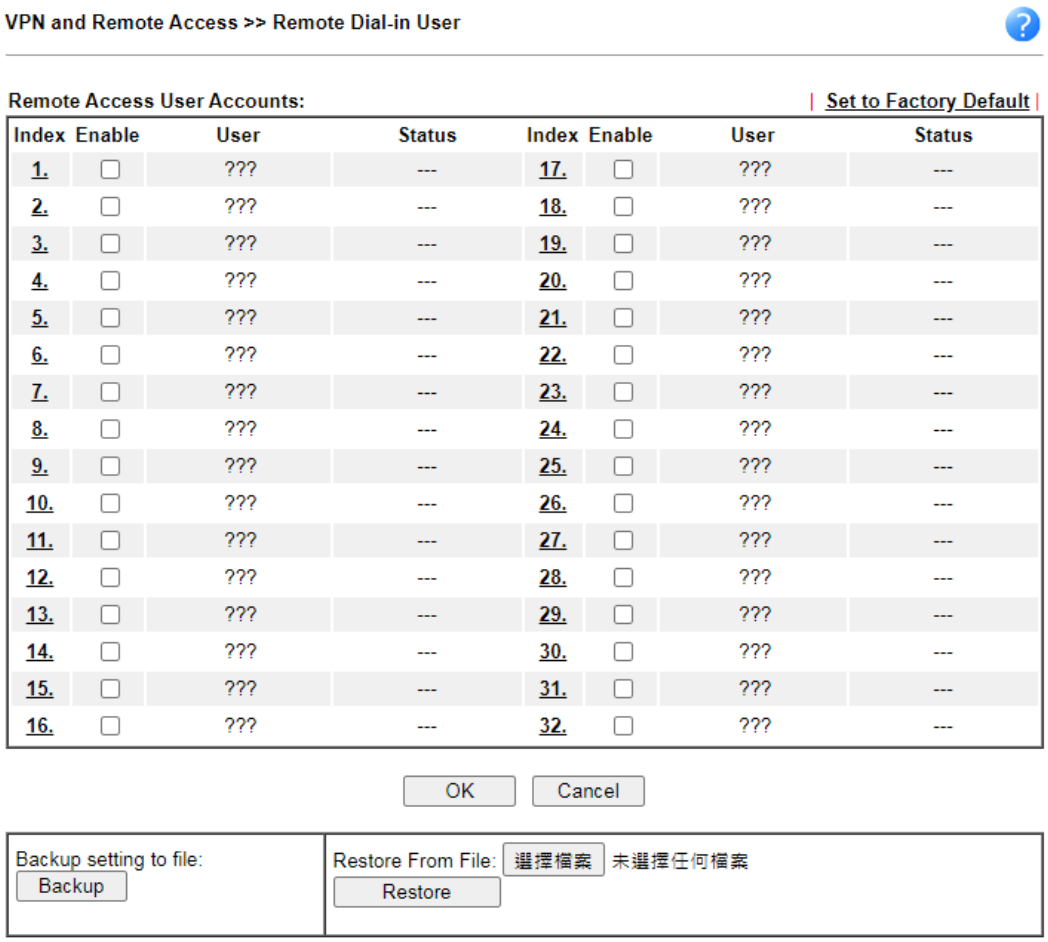
Available settings are explained as follows:

Item	Description
Select an OpenVPN config file	**Browse** - Click to select a file. **Import** - Click to import a configuration file.
Import Local Certificate	Click to access into Local Certificate page for importing a certificate.
Import Trusted CA Certificate	Click to access into Trusted CA Certificate page for importing a certificate.

IV-1-9 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profiles, so that users can be authenticated via VPN connection.

Remote dial-in user profiles can be set up on this screen.



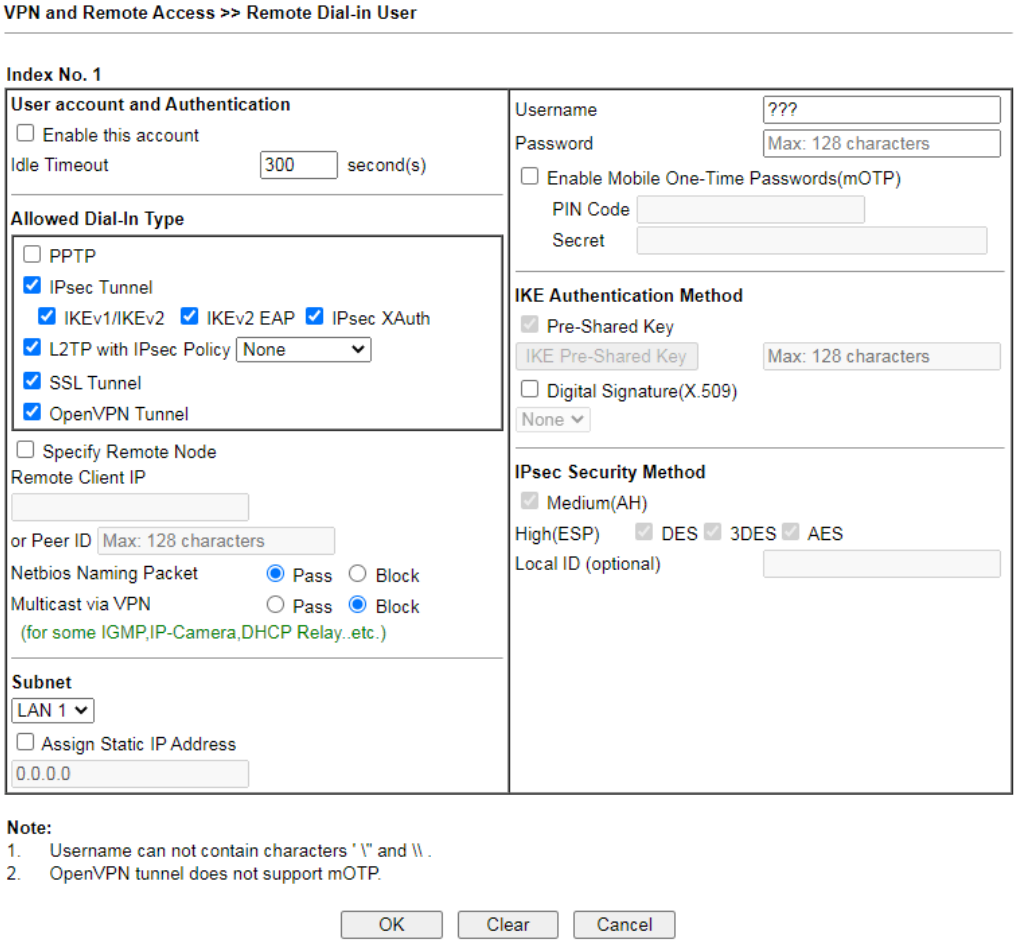
Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all remote-dial-in user profiles.
Index	Click the index number of the profile the view or edit its settings.
Enable	Check to enable the user 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	Shows the LAN subnet and IP address assignment method. Example: LAN1-DHCP means that the IP address of the VPN connection will be drawn from the DHCP pool of the LAN1 subnet. The color of the status indicates the current state of the profile: Green – Profile is being used by a dial-in VPN connection.

	Red – Profile is not being used. Black – Profile is disabled.
Backup	Click **Backup** to save the configuration.
Restore	Click **Select** to choose a configuration file. Then click **Restore** to apply the file.

To save changes on the page, select **OK**; to discard changes, select **Cancel**.

The following setup screen is shown after a profile index has been clicked.



Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Select to enable this profile to be used by remote dial-in users. **Idle Timeout** - Allowed idle time before the router disconnects the VPN connection. Default timeout value is 300 seconds.
Allowed Dial-In Type	Select all VPN protocols allowed for this profile. For L2TP, specify how IPsec should be applied. Options are: ● **None** – IPsec cannot be used with L2TP connections. ● **Nice to Have** – IPsec is preferred but not mandatory for L2TP connections. ● **Must** – IPsec is required when establish L2TP connections.

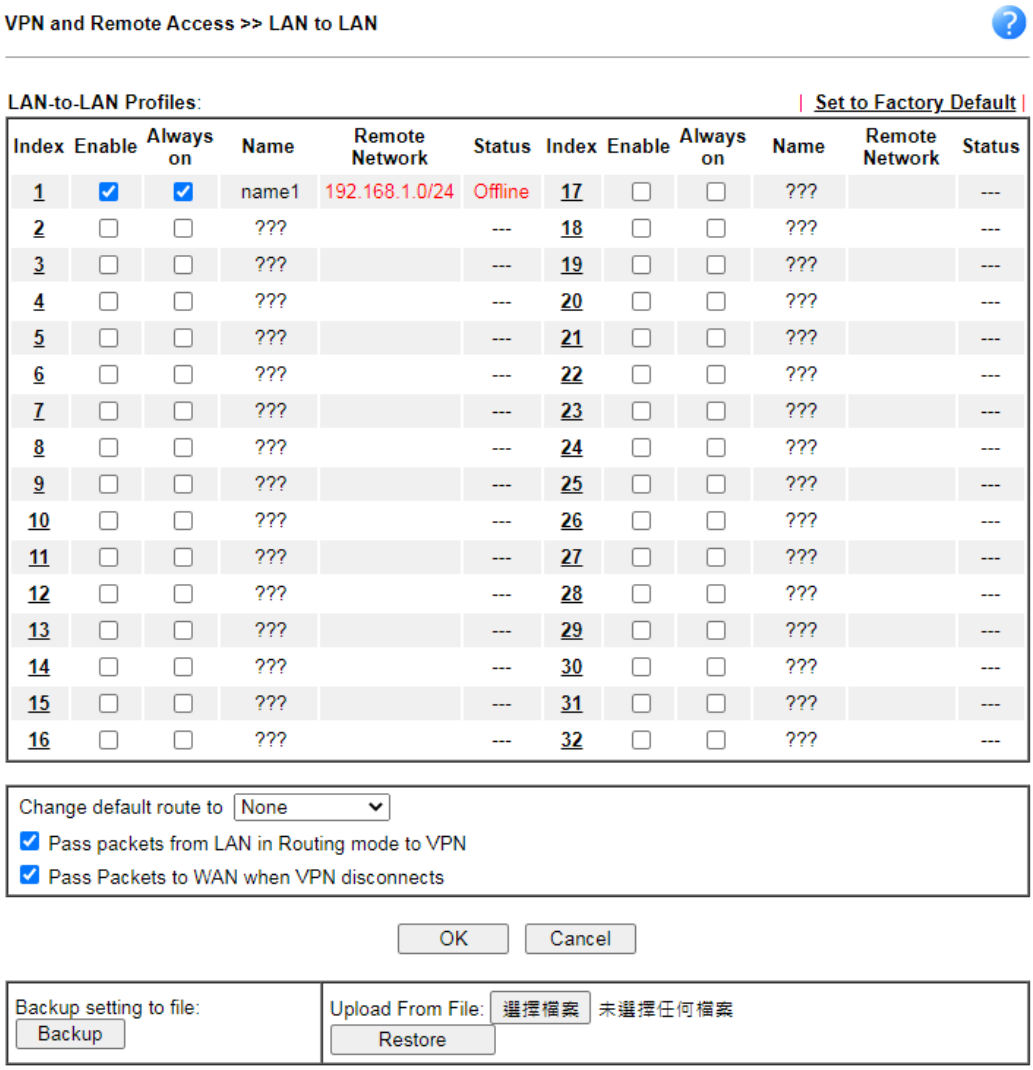
	Specify Remote Node - The IP address of the remote VPN client (Remote Client IP) or the Peer ID (used in IKE aggressive mode) can be optionally specified. The router will reject the connection if either of these values are entered in the profile but the remote client does not pass the value, or passes the wrong value. **Netbios Naming Packet -** Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel. ● **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** - Specifies whether to allow multicast packets to traverse through the VPN tunnel. ● **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	The VPN client will receive an IP address from the DHCP pool or IP address range specified in IP Address Assignment for Dial-In Users for the selected LAN subnet. **Assign Static IP Address** – Alternatively, a static IP address can be set by selecting the Assign Static IP Address checkbox. **User Name** - Used for PPTP, L2TP or SSL Tunnel dial-in type. The length of the name is limited to 23 characters. **Password** - Used for PPTP, L2TP or SSL Tunnel dial-in type. The length of the password is limited to 19 characters. **Enable Mobile One-Time Passwords (mOTP) -** Select to enable one-time passwords (Mobile-OTP). Enter the PIN Code and Secret. DrayTek's SmartVPN client has built-in support for mOTP. Third-party mOTP clients can be used to generate passwords when using other VPN clients. For more information on mOTP, visit Mobile-OTP's homepage. ● **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).
IKE Authentication Method	**Pre-Shared Key** - This checkbox is available when Remote Client IP or Peer ID is specified. Check the checkbox and click IKE Pre-shared Key to enter an IKE PSK (1~63 characters) that will be used only for this profile. **Digital Signature (X.509) –** To enable authentication using X.509 Peer IDs, check the checkbox then select an X.509 profile. X.509 profiles can be configured in **VPN and Remote Access >> IPsec Peer Identity**.
IPsec Security Method	Select all the IPsec protocols that are allowed to be used for this profile. **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) -** 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 when establishing a LAN-to-LAN VPN connection using IKE aggressive mode.

To save changes on the page, select **OK**; to discard changes, select **Cancel**; to clear settings on this page and revert to default settings, select **Clear**.

IV-1-10 LAN to LAN

This section allows you to configure up to 32 LAN-to-LAN VPN connections. LAN-to-LAN connections can be configured to allow dial-in only, dial-out only, or both dial-in and dial-out.



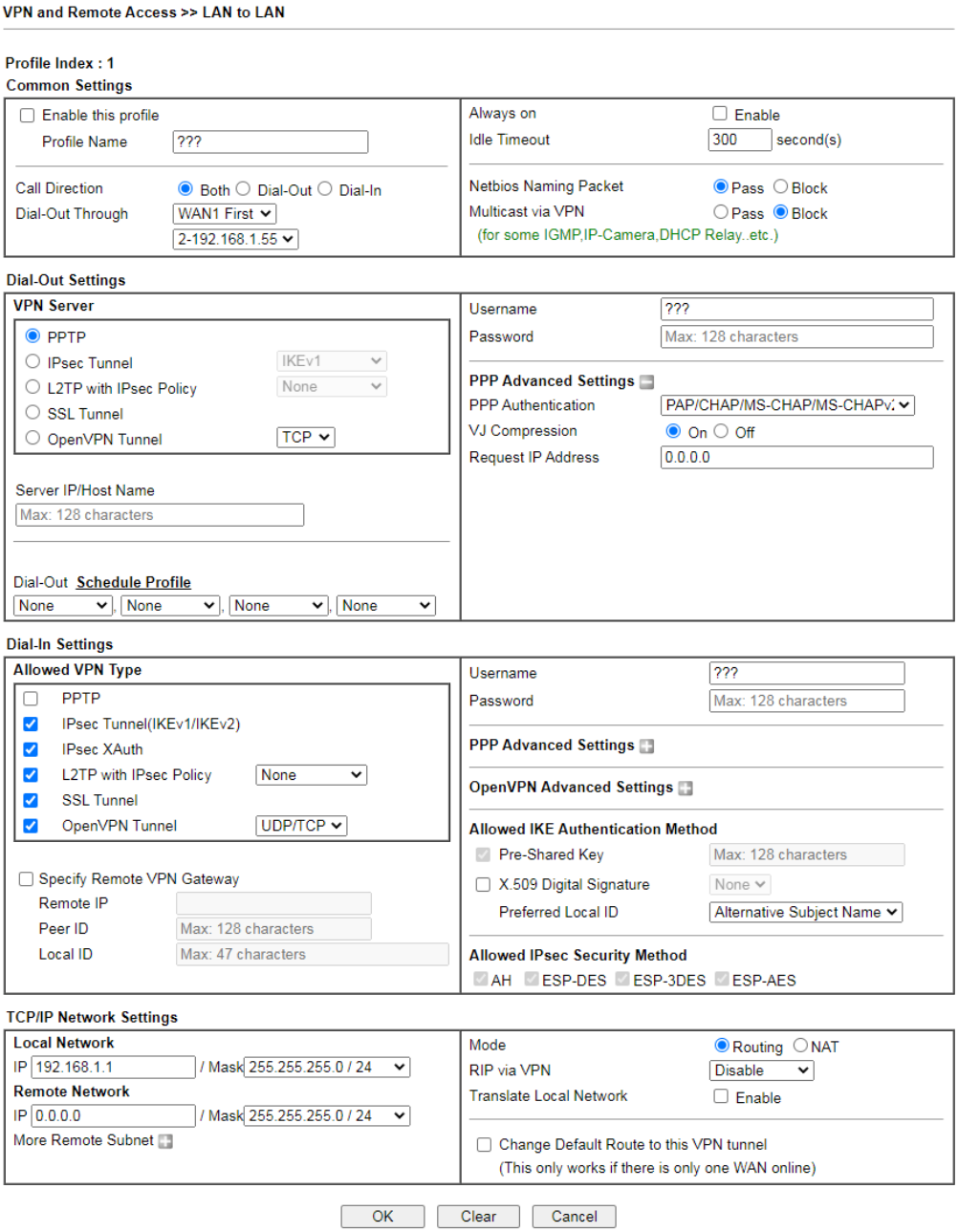
Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the index number of the profile to view or edit its settings.
Enable	Check to enable the LAN-to-LAN VPN profile.
Always On	Check to make the dial-out connection always on.
Name	Displays the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Remote Network	Displays the name of the remote network.
Status	Shows the status of the profile. Online – LAN-to-LAN VPN is connected.

	Offline – LAN-to-LAN VPN is disconnected. --- – Profile is disabled.
Change default route to	Select a profile as the default route.
Pass packets from LAN in Routing mode to VPN	If enabled, the packets from LAN will pass through the VPN tunnel.
Pass Packets to WAN when VPN disconnects	If enabled, the packets can pass through via WAN when the VPN disconnects.
Backup	Click **Backup** to save the configuration.
Restore	Click **Select** to choose a configuration file. Then click **Restore** to apply the file.

To edit each profile, click each index to edit each profile.

1. The setup screen is shown after a profile index has been clicked. There are 6 sections: Common Settings, Dial-Out Settings, Dial-In Settings, and TCP/IP Network Settings.



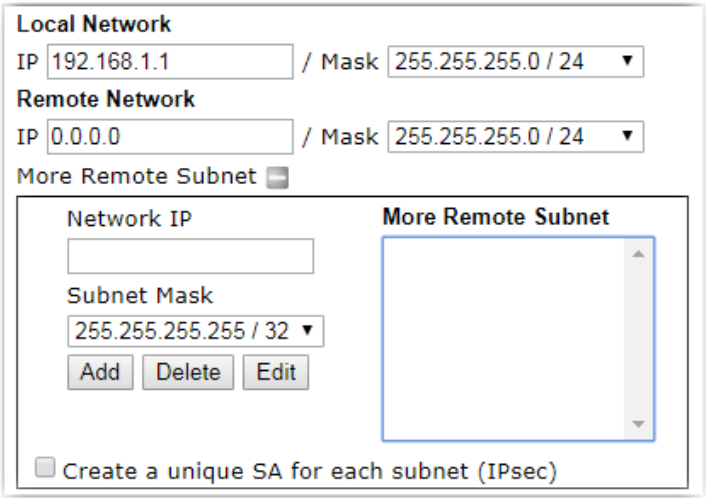
Available settings are explained as follows:

Item	Description
Common Settings	**Enable this profile -** Select to enable the profile. **Profile Name -** Specify a name that allows you to identify this profile. **Call Direction -** Specify the allowed call direction of this LAN-to-LAN profile. Four choices are available for connection mode: ● **Both** – Profile is to be used to initiate (dial out) or accept (dial in) connections. ● **Dial-Out** – Profile is to be used to initiate outgoing connections. ● **Dial-In** – Profile is to be used to accept incoming connections.

	Dial-Out Through - Select the WAN connection for connections made using this profile. This setting is useful for dial-out only. • **WANx First** - While connecting, the router will use WANx as the first channel for VPN connection. If WANx fails, the router will use another WAN interface instead. • **WANx Only** - While connecting, the router will use WANx as the only channel for VPN connection. **Always On** - Select this option to maintain an always on dial-out connection. **Idle Timeout** - The router will close connection if no activity is observed in the VPN connection for this many seconds. Default value is 300 seconds. **Netbios Naming Packet** - Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel**.** • **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 -** Specifies whether to allow multicast packets to traverse through the VPN tunnel. • **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.
Dial-Out Settings	**VPN Server** - Select the VPN protocol to be used**.** **Server IP/Host Name** - IP address or DNS host name of remote VPN host. **Dial-Out Schedule Profile -** Connect and disconnect according to schedule profiles. The default setting of this field is blank and the function will always work. **User Name -** Enter a username for establishing VPN connection. **Password -** Enter the password for establishing VPN connection. **PPP Advanced Settings** - Click it to expand the advanced settings for PPP. • **PPP Authentication -** PAP Only – Authenticate dial-in users using the PAP protocol only. PAP/CHAP/MS-CHAP/MS-CHAPv2 – Attempt to authenticate dial-in users using various CHAP protocols, and if the remote VPN client fails to authenticate, fall back to PAP. • **VJ compression -** Specifies whether to enable Van Jacobson (VJ) header compression, which improves throughput on slow connections. • **Request IP Address** - Enter the IP address.
Dial-In Settings	**Allowed VPN Type -** Select permissible VPN protocols for dial-in connections. • **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/OpenVPN Tunnel-** Allow the remote dial-in user to trigger an SSL/OpenVPN 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. **PPP Advanced Settings** - Click it to expand the advanced settings for PPP. • **VJ Compression -** Specifies whether to enable Van Jacobson header compression, which improves throughput on slow connections. • **Assign Peer IP Address** - Enter the IP address of the peer. **Allowed IKE Authentication Method -** This section is available when IPsec tunnel is selected as the dial-out protocol. Available options are IKE Pre-shared key and X.509 digital signature. • **Pre-Shared Key** - To use a pre-shared key, select this radio-button and then click the IKE Pre-Shared Key button to enter the PSK. • **X.509 Digital Signature** - To use an X.509 digital signature, select this radio button and then select an X.509 IPsec Peer Identity profile. To enable authentication using X.509 Peer IDs. X.509 profiles can be configured in **VPN and Remote Access >> IPsec Peer Identity**. **Preferred Local ID** – Select whether to first match

	Subject Alternative Name or Subject Name during authentication. • **Alternative Subject Name** – The alternative subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first. • **Subject Name** – The subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first. **Allowed IPsec Security Method** - This setting is available when IPsec Tunnel is selected as the dial-out protocol. • **AH-** Authentication Header (AH) means data will be authenticated, but not be encrypted. Select to use Authentication Header protocol. By default, this option is active. • **ESP-DES/ESP-3DES/ESP-AES -** 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	This section configures the whether the local router applies NAT when linking the local network to the remote network, and whether IP address translation occurs when. The view changes depending on the setting of the field From first subnet to remote network, you have to do. Select NAT if the remote VPN server expects only one IP address on the local network; otherwise, select Route. TCP/IP Network Settings has different settings depending on whether NAT or Route mode is selected. **Local Network –** The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP. • **IP / Mask -** Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required. **Remote Network -** The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP. • **IP/ 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. **More Remote Subnet** - Click to bring up a dialog box to enter additional static routes for subnets destined for the remote network.



Mode - If the remote network only allows one IP address for the local network, select **NAT**; otherwise, select **Route**.

RIP via VPN - Specifies the direction of Routing Information Protocol (RIP) packets. Available options are:

- TX/RX Both – can transmit or receive RIP packets
- TX Only – can only transmit but not receive RIP packets
- RX Only – can only receive but not transmit RIP packets
- Disable – RIP is disabled.

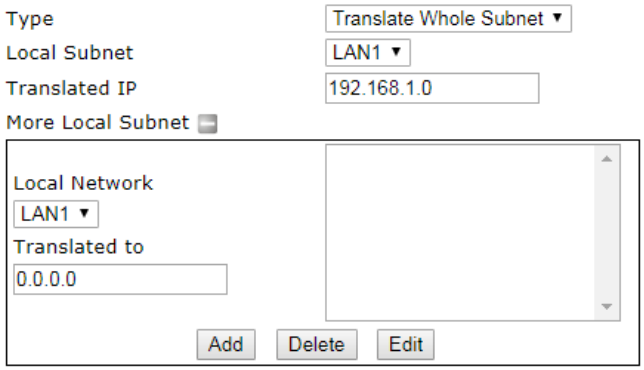
When the Mode is set to Routing

When **Routing** is selected, the available fields in the TCP/IP Network Settings section will be shown as:

Translate Local Network - Check the box to enable the function. 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.

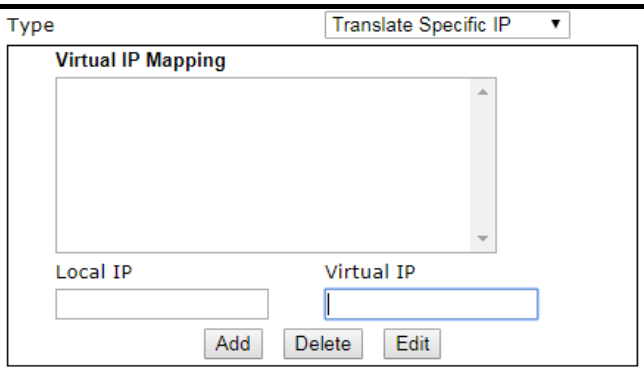
- **Type** - There are two types (**Translate Whole Subnet**, **Translate Specific IP**) for you to choose.

  When **Translate Whole Subnet** is selected as **Type**, available settings are listed as below:



  - **Local Subnet** - Select the LAN whose IP addresses are to be translated.
  - **Translated IP** - Specify an IP address.
  - **More Local Subnet** - Click it to add more subnets.

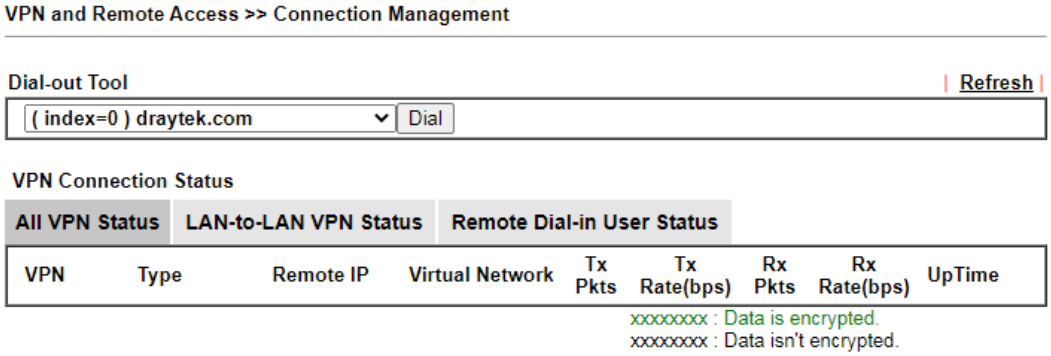
  When **Translate Specific IP** is selected as **Type**, available settings are listed as below:

	 - **Virtual IP Mapping –** A pop up dialog will appear for you to specify the local IP address and the mapping virtual IP address.
When the Mode is set to NAT	When **NAT** is selected, the available fields in the TCP/IP Network Settings section will be shown as: **RIP via VPN -** Specifies the direction of Routing Information Protocol (RIP) packets. Available options are: ● TX/RX Both – can transmit or receive RIP packets ● TX Only – can only transmit but not receive RIP packets ● RX Only – can only receive but not transmit RIP packets ● Disable – RIP is disabled. **Change Default Route to this VPN tunnel -** Select this option to direct all traffic that is not LAN-bound to this VPN tunnel. This option is functional when there is only one active WAN.

2. To save changes on the LAN to LAN profile page, select **OK**; to reset the entire page to blank, select **Clear**; to discard changes, select **Cancel**.

IV-1-11 Connection Management

You can initiate outbound LAN-to-LAN VPN sessions, and view and disconnect all current LAN-to-LAN and dial-up VPN sessions.



Available settings are explained as follows:

Item	Description
Refresh	Click to manually reload the page to refresh VPN connection information.
Dial-out Tool	**Dial -** Click this button to execute dial out function. If the connect is successfully made, it will show up in the VPN Connection Status section below.
VPN Connection Status	**VPN** - Displays the VPN profile number and the profile name. **Type** - Displays the VPN protocol used for the connection **Remote IP** - Displays the remote IP address of the VPN connection. **Virtual Network** - Displays the IP subnet used by the VPN connection. **Tx Pkts** - Displays the number of packets that have been transmitted through the VPN connection. **Tx Rate(Bps)** - Displays the current upstream speed of the VPN connection. **Rx Pkts** - Displays the number of packets that have been received through the VPN connection. **Rx Rate(Bps)** - Displays the current downstream speed of the VPN connection. **UpTime** - Displays the elapsed time of the VPN connection. **Drop** - Click this button to disconnect this VPN connection.

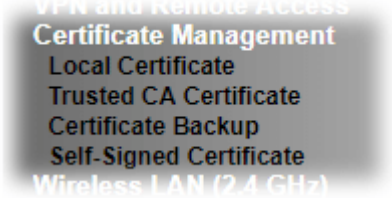
IV-2 Certificate Management

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

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

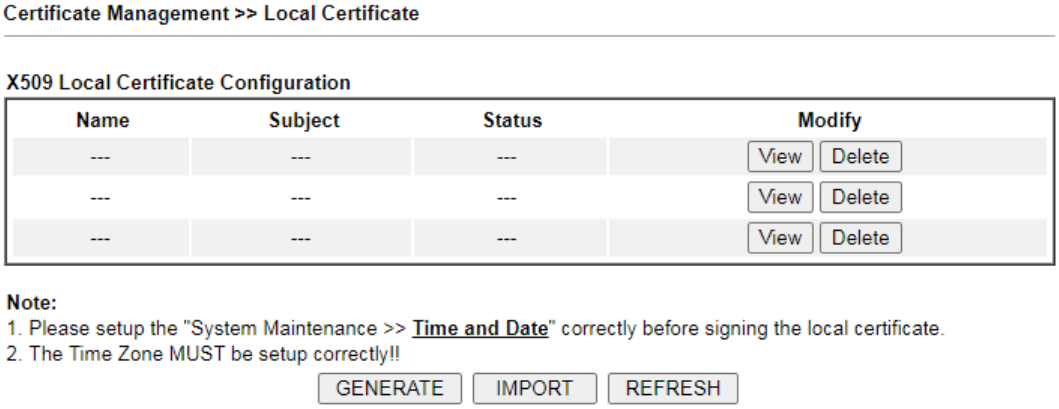
Web User Interface

The image below shows the menu items for Certificate Management.



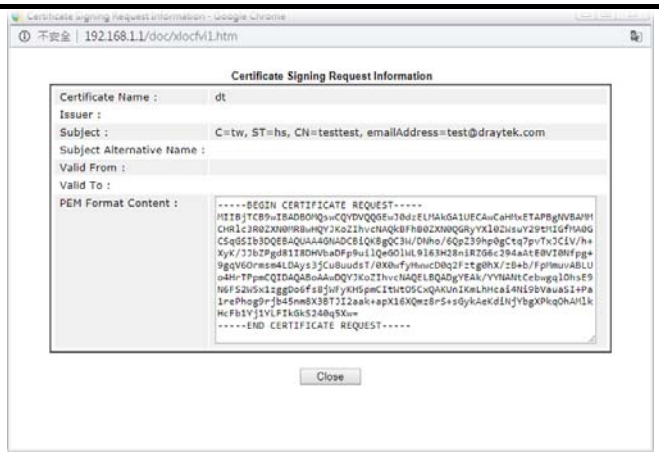
IV-2-1 Local Certificate

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



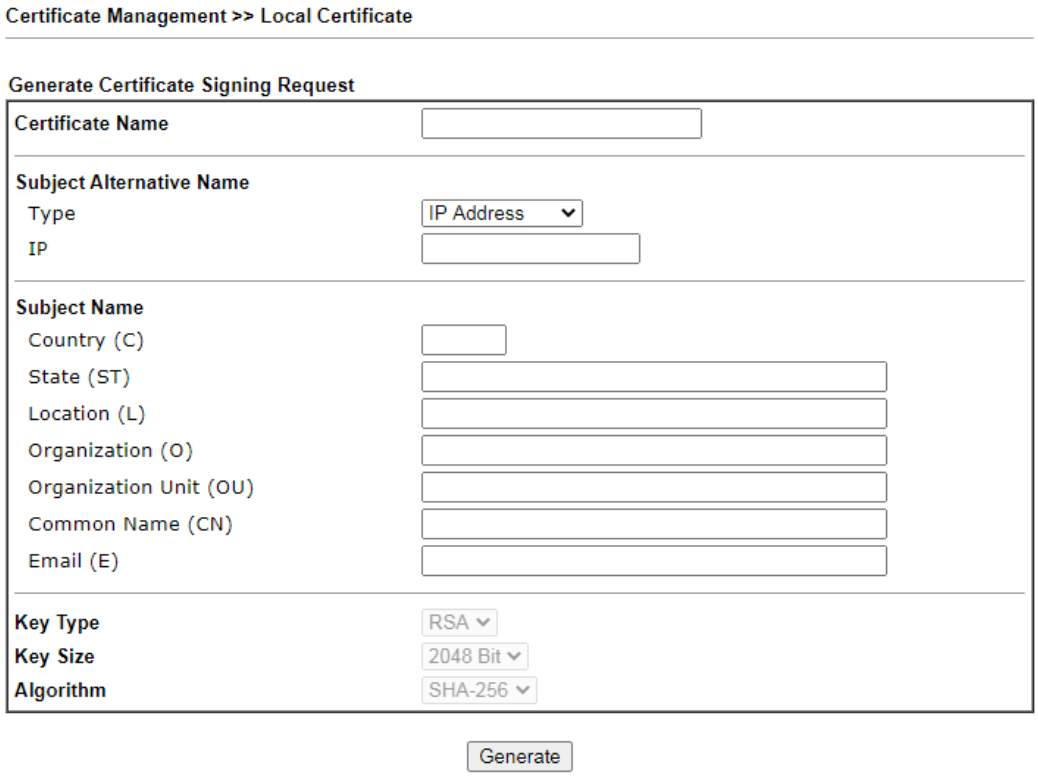
Available settings are explained as follows:

Item	Description
Name	Displays the Name that identifies the certificate.
Subject	Displays the Subject Name entries of the certificate.
Status	Displays the status of the certificate. Status is one of Requesting.
Modify	**View** – Click to view details about the certificate. A screen that looks like the following will be displayed, showing the Subject Name, Subject Alternative Name, and the certificate content.

	 **Delete** – Click to remove the certificate.
Generate	Click to fill out details about a certificate, and start the generation process.
Import	Click to update an existing certificate.
Refresh	Click to refresh the page to display the latest certificate information.

GENERATE

Use this screen to submit a request to your root CA to generate a certificate.

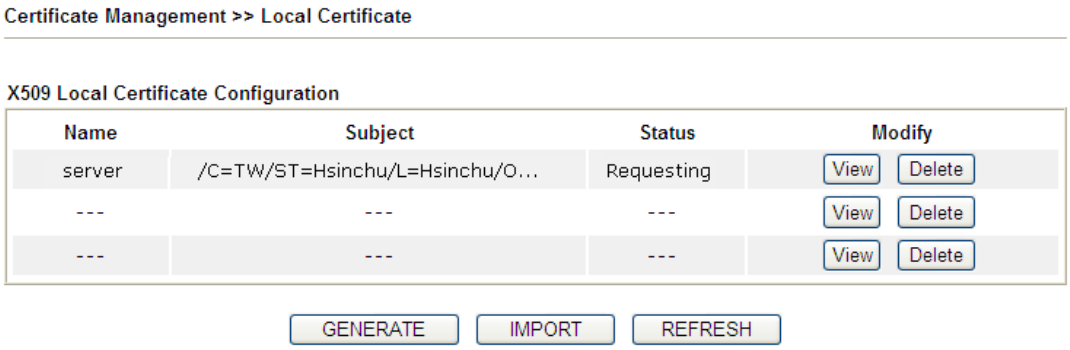


Available settings are explained as follows:

Item	Description
Certificate Name	Name that identifies the certificate.

Type	Select the type of Subject Alternative Name and enter its value.
Country (C)	Country in which your organization is located.
State (ST)	State or province where your organization is located.
Location (L)	City where you're your organization is located.
Organization (O)	Legal name of your organization.
Organization Unit (OU)	Department within your organization that you wish to be associated with this certificate.
Common Name (CN)	Fully-qualified domain name / WAN IP that will be used to reach your server.
Email (E)	Email address of the entry.
Key Type	Key type is hard set to RSA.
Key Size	Choose between 1024 and 2048 bit.
Algorithm	Choose between SHA-1 and SHA-256.
Generate	Click to submit generate request to the CA server.

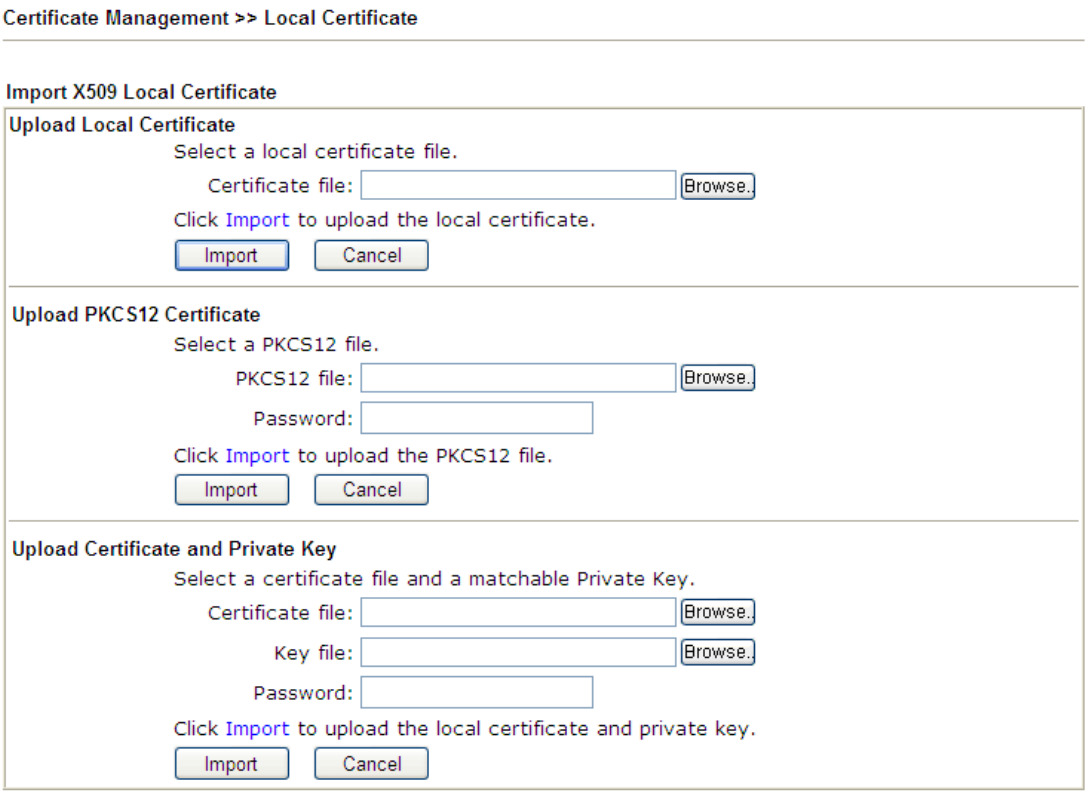
After clicking the **Generate** button, you will be taken back to the main Local Certificate screen, showing the certificate request in progress:



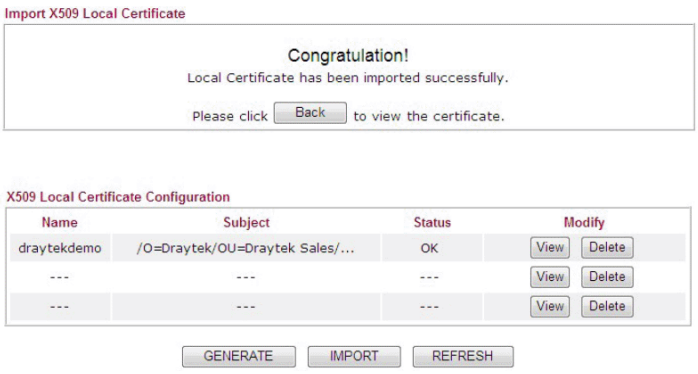
IMPORT

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.

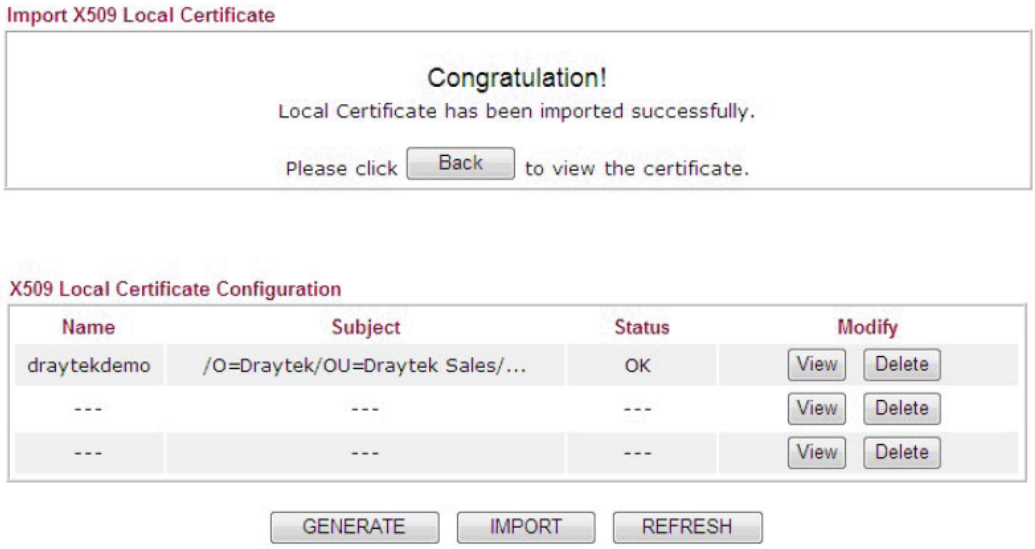


Available settings are explained as follows:

Item	Description
Upload Local Certificate	**Certificate file -** Click **Browse** to select a local certificate file. **Import -** Click to import selected certificate file to router. **Cancel -** Click to return to the main Local Certificate screen. 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. **PKCS12 file** - Click **Browse** to select a PKCS12 certificate file. **Password** - Enter the password associated with the certificate and key files. **Import** - Click to import selected certificate file to router.

	Cancel - Click to return to the main Local Certificate screen.
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. **Certificate file -** Click **Browse** to select a local certificate file. **Key file** - **Password** - Enter the password associated with the certificate and key files. **Import -** Click to import selected certificate file to router. **Cancel -** Click to return to the main Local Certificate screen.

If the import was successful, you will see the following confirmation screen:



REFRESH

Click this button to refresh the information listed below.

IV-2-2 Trusted CA Certificate

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

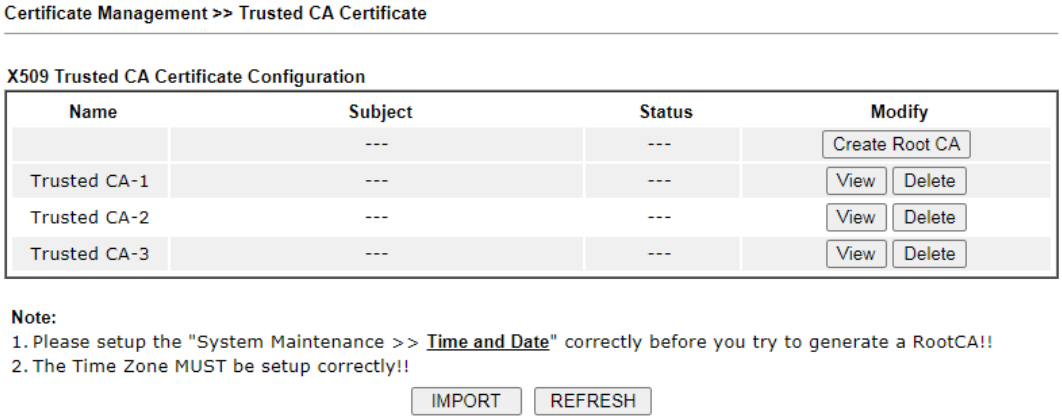
When the local client and remote client are required to make certificate authentication (e.g., IPsec X.509) for data passing through SSL tunnel and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

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

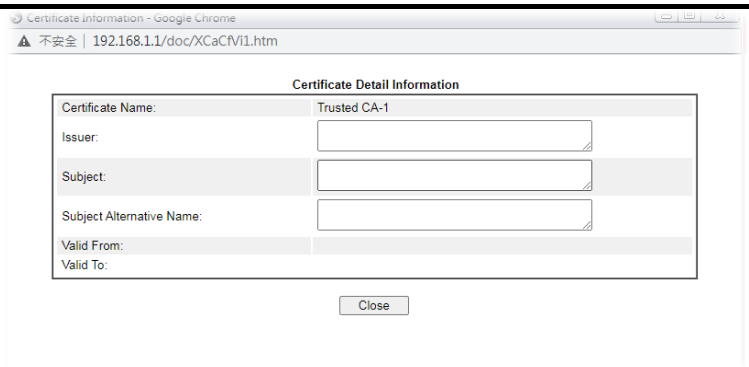
Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.

You can create, import and view root and trusted certificate authority certificates on this screen.



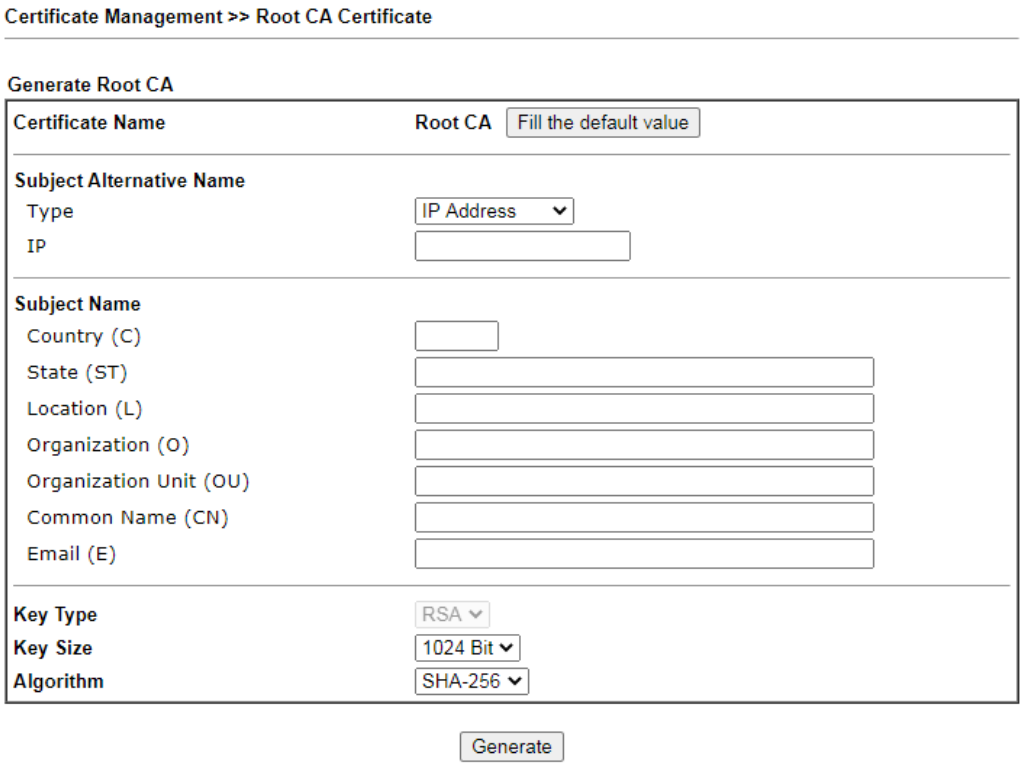
Available settings are explained as follows:

Item	Description
Create Root CA	Click to create a new root CA.
Name	Name that identifies the certificate.
Subject	Shows the Subject Name of the certificate.
Status	Displays the status of the certificate.
Modify	**Create –** Click to fill out details about a certificate, and start the generation process. **View –** Click to view details of the certificate.

	 **Delete -** Click to delete the certificate.
Import	Click to import an existing certificate.
Refresh	Click to refresh the page to display the latest certificate information.

Creating a Root CA

Click **Create Root CA** to open the following page.



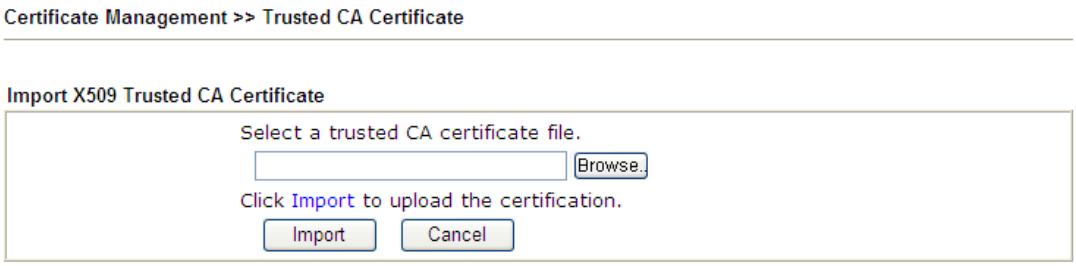
Available settings are explained as follows:

Item	Description
Certificate Name	Display the name of root CA. **Fill the default value** - Click to enter the default value for this Root CA.
Type	Select the type of Subject Alternative Name and enter its value.
Country (C)	Country in which your organization is located.
State (ST)	State or province where your organization is located.

Location (L)	City where you're your organization is located.
Organization (O)	Legal name of your organization.
Organization Unit (OU)	Department within your organization that you wish to be associated with this certificate.
Common Name (CN)	Fully-qualified domain name / WAN IP that will be used to reach your server.
Email (E)	Email address of the entry.
Key Type	Key type is hard set to RSA.
Key Size	Choose between 1024 and 2048 bit.
Algorithm	Choose between SHA-1 and SHA-256.
Generate	Click to submit generate request to the CA server.

Importing a Trusted CA

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window.

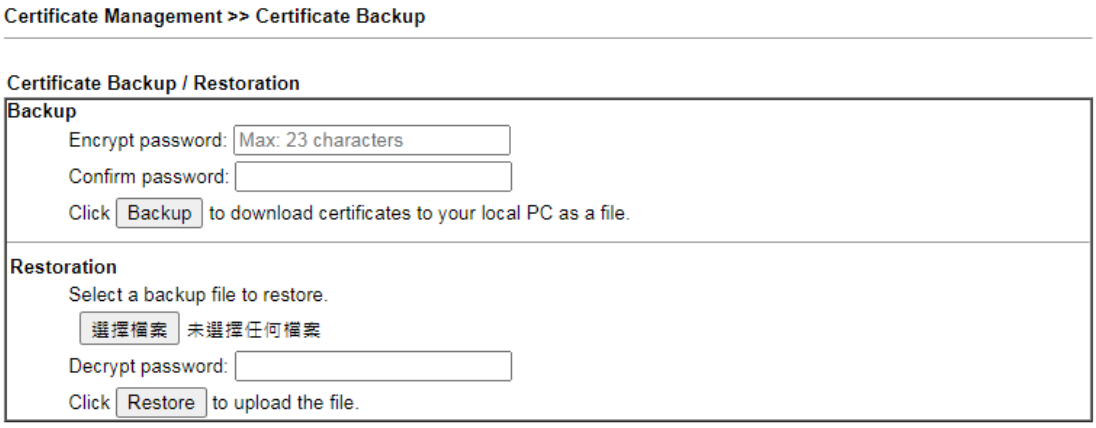


Available settings are explained as follows:

Item	Description
Browse	Click Browse to select a local certificate file.
Import	Click to import selected certificate file to router. The one you imported will be listed on the Trusted CA Certificate window.
Cancel	Click to return to the main Trusted CA Certificate screen.

IV-2-3 Certificate Backup

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



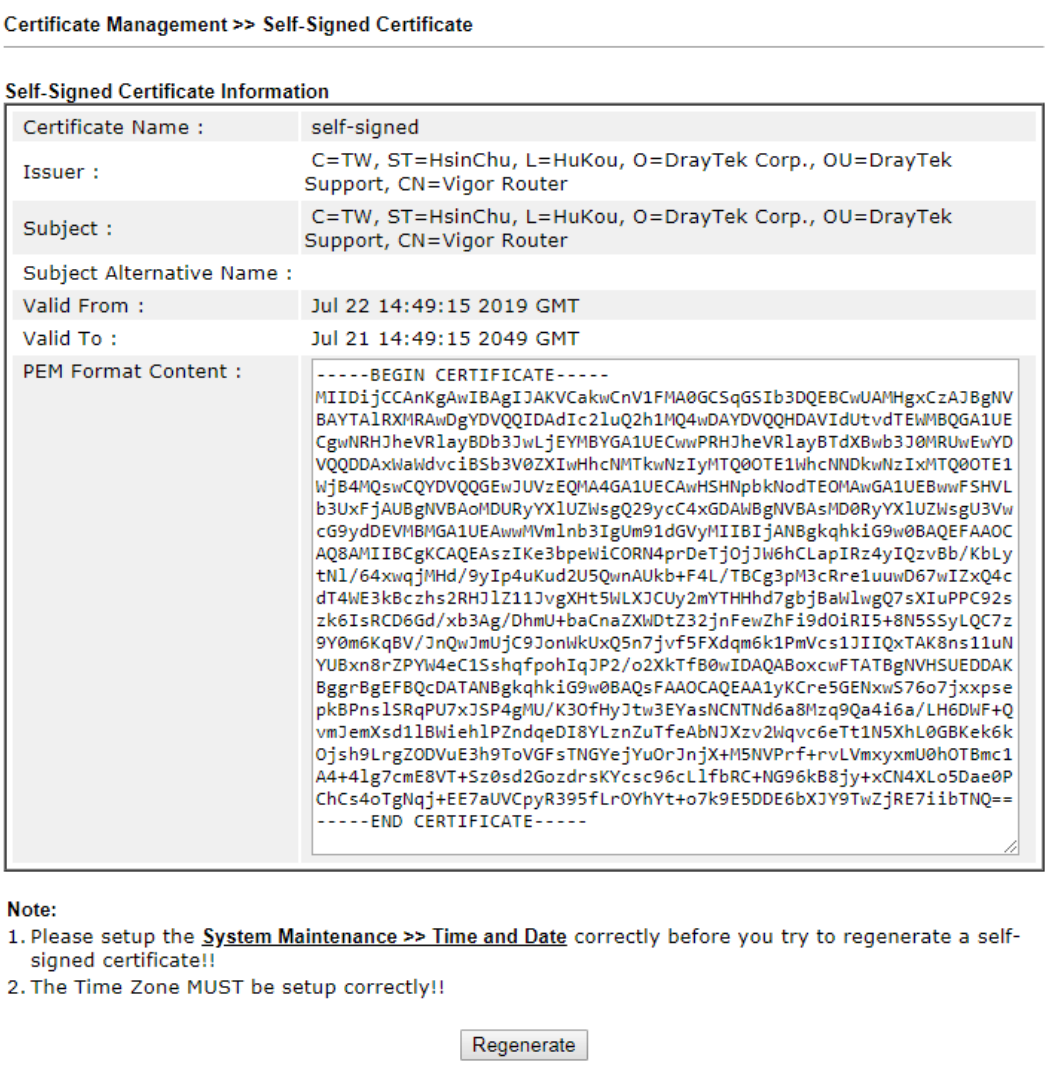
Available settings are explained as follows:

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.

IV-2-4 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 **Regenerate** to open the Regenerate Self-Signed Certificate window. Enter all requested information including certificate name (used to differentiate different certificates), subject alternative name type and relational settings for subject name. Then click GENERATE.

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

Basic

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

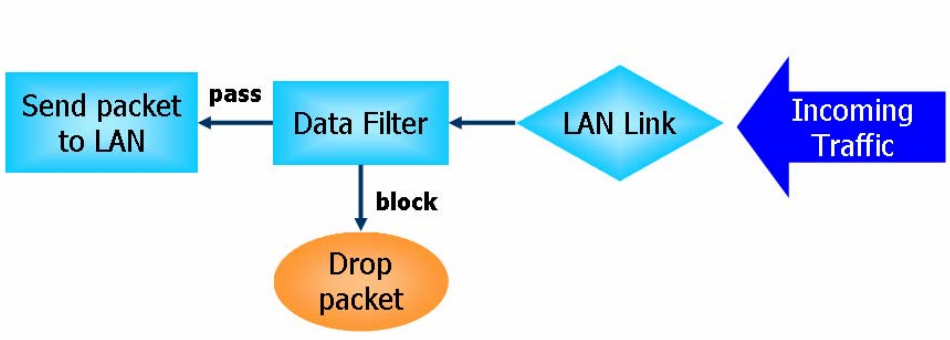
Firewall Facilities

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

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

Data Filter

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



Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

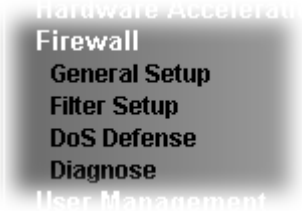
Vigor's DoS Defense functionality detects DoS attacks and mitigates their damage by inspecting every incoming packet, and malicious packets will be blocked. If Syslog is enabled, alert messages will also be sent. Abnormal traffic flow such as flood and port scan attacks that exceed allowable thresholds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

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

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

Web User Interface

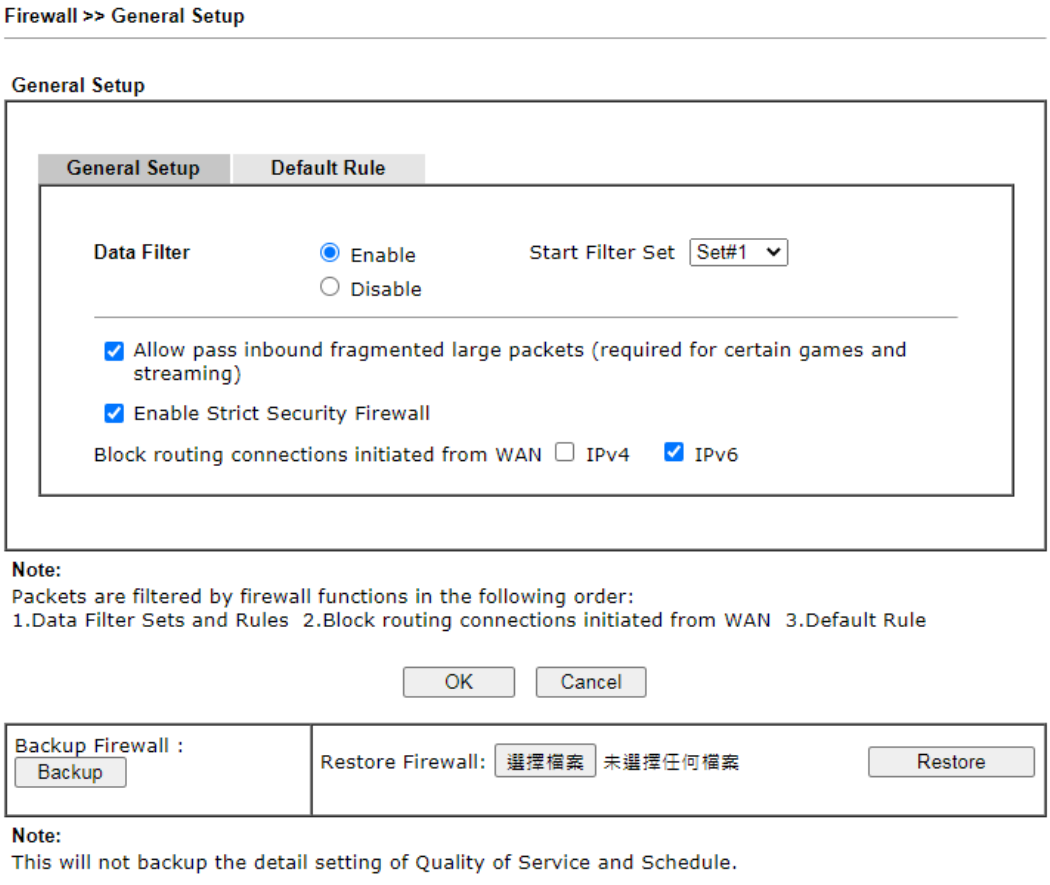
Below shows the menu items for Firewall.



V-1-1 General Setup

General Setup Page

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



Available settings are explained as follows:

Item	Description
Data Filter	Select **Enable** to activate the Data Filter function, and then choose a Start Filter Set.

Allow pass inbound fragmented large packets	Certain games and video streaming service use fragmented UDP packets to transfer data. Enabling this option allows these applications to function properly. If this option is not enabled, the router will attempt to reassemble fragmented packets up to a certain value (e.g., 15xx~2102) kilobytes long. Packets larger than the certain value will be discarded. If this option is enabled, the router always passes fragmented packets without reassembling them, regardless of the size of the packet.
Enable Strict Security Firewall	If this option and the Web Content Filter (WCF) are both enabled, web traffic will be blocked if the WCF server fails to respond to lookup requests.
Block routing connections initiated from WAN	**IPv6** - IPv6 does not make use of Network Address Translation (NAT), so all LAN hosts receive public IPv6 IP addresses that are exposed to the WAN. Enable this option to block WAN hosts from connecting to LAN hosts using IPv6. **IPv4** - For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, enable this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on private LAN subnets.
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.

To save changes on the page, click **OK**. To discard changes, click **Cancel**.

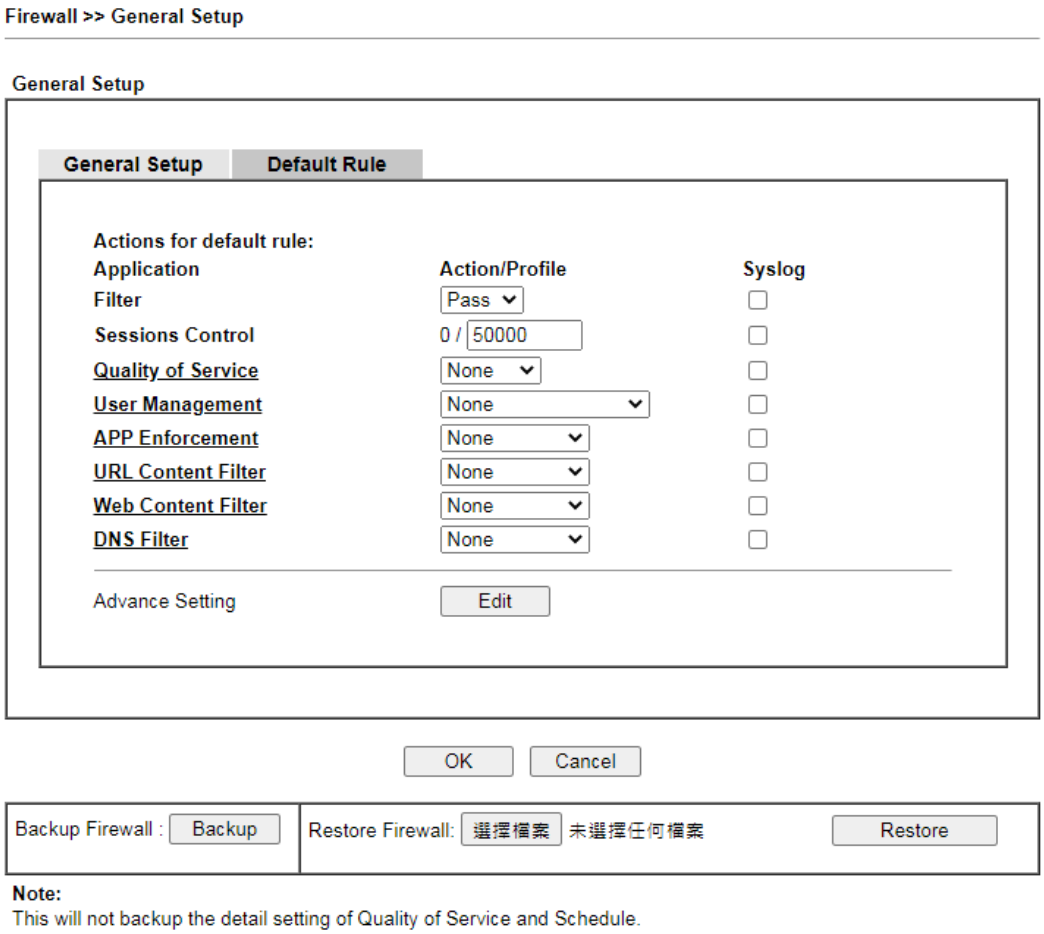
Traffic is filtered by firewall functions in the following order:

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

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.

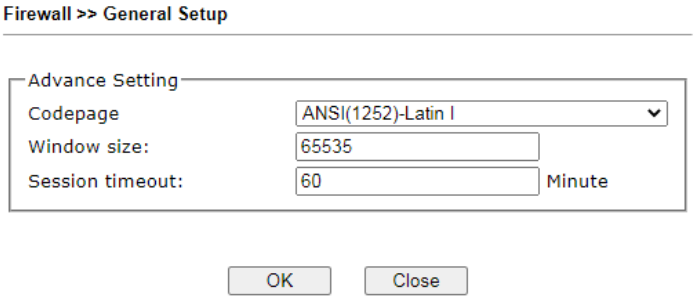
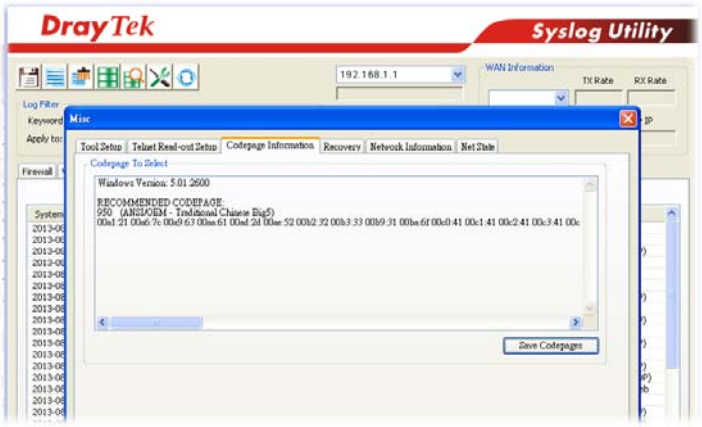
The default rule applies to all traffic that is not constrained by other filters or rules.



Available settings are explained as follows:

Item	Description
Filter	Select **Pass** or **Block** for the packets that do not match with the filter rules. When the setting is Block, all other fields on the page are disabled because they are not applicable.
Sessions Control	The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions allowed, which is configurable. The default maximum is 60000, which is also the upper limit of the value.
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.
User Management	This setting is only available when **Rule-Based** is selected in **User Management>>General Setup**. The default firewall rule will be applied to the selected user or user group. Refer to the chapter on User Management for more details on the feature. ● **None**: User Management does not apply to the default rule.

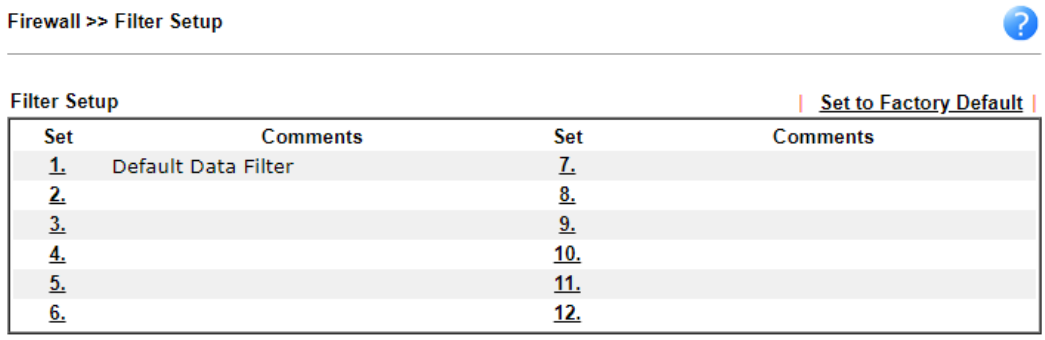
	• **User Object**: The default rule only applies to the selected user. • [**Create New User**]: Select this to create a new user. • User Group: The default rule only applies to the selected User Group. • [**Create New Group**]: Select this to create a new user group. • **ALL**: The default rule applies to all defined users. • **Create New User** or **Create New Group** item will appear for you to click to create a new one if there is no user profile or group profile existed. **Syslog** - Select to allow User Management to log messages in Syslog.
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. **Syslog** - Select to allow APP Enforcement to log messages in Syslog.
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. **Syslog** - Select to allow URL Content Filter to log messages in Syslog. Logging action is configured at the profile level in CSM>>URL Content Filter Profile, Log.
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. **Syslog** - Select to allow Web Content Filter to log messages in Syslog. Logging action is configured at the profile level in the Web Content Filter Profile Table section in CSM>>Web Content Filter Profile, Log.
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 configuration window for Advanced Settings. However, it is **recommended** to use the default settings.

	 **Codepage** – Sets the codepage used by the URL content filter to match URLs against keywords in profiles. Choosing the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed. If you are unsure of which codepage to use, please start the Syslog application, and the recommended codepage will be shown in the Codepage Information tab in the Setup dialog box.  **Window size** – Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 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** – Sets the timeout sessions are allowed to idle before they are removed from the system.
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.

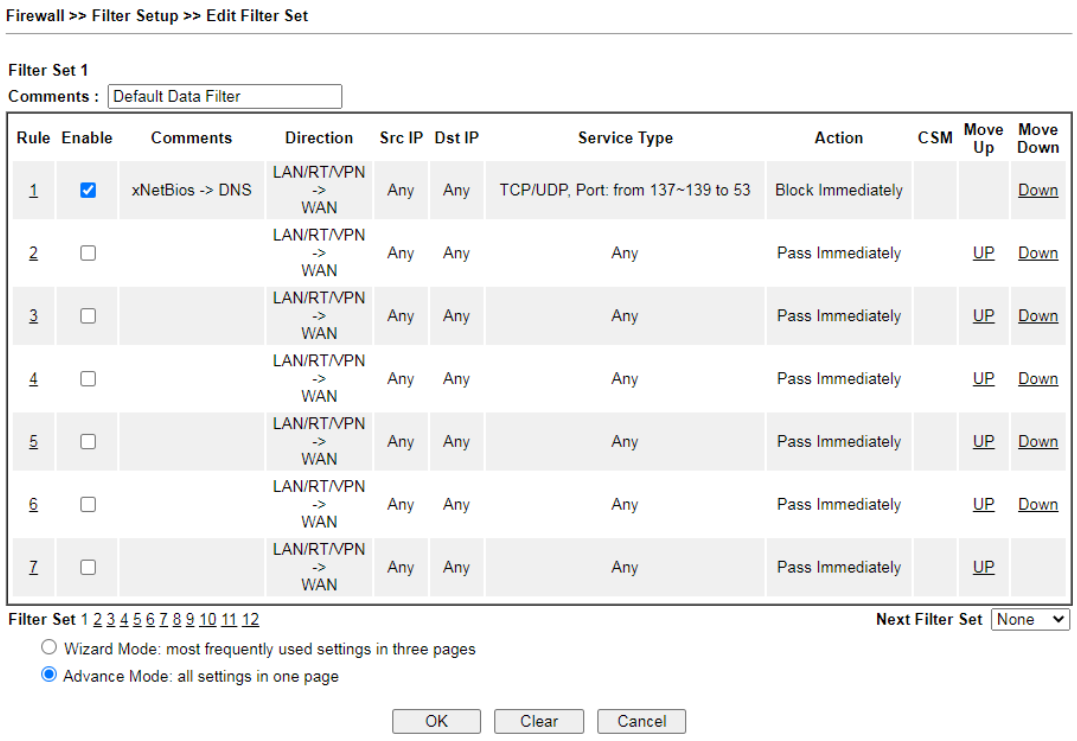
After finishing all the settings here, please click **OK** to save the configuration.

V-1-2 Filter Setup

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



To edit a filter set, click on its set number. The following Filter Set page will be shown. Each filter set contains up to 7 rules.



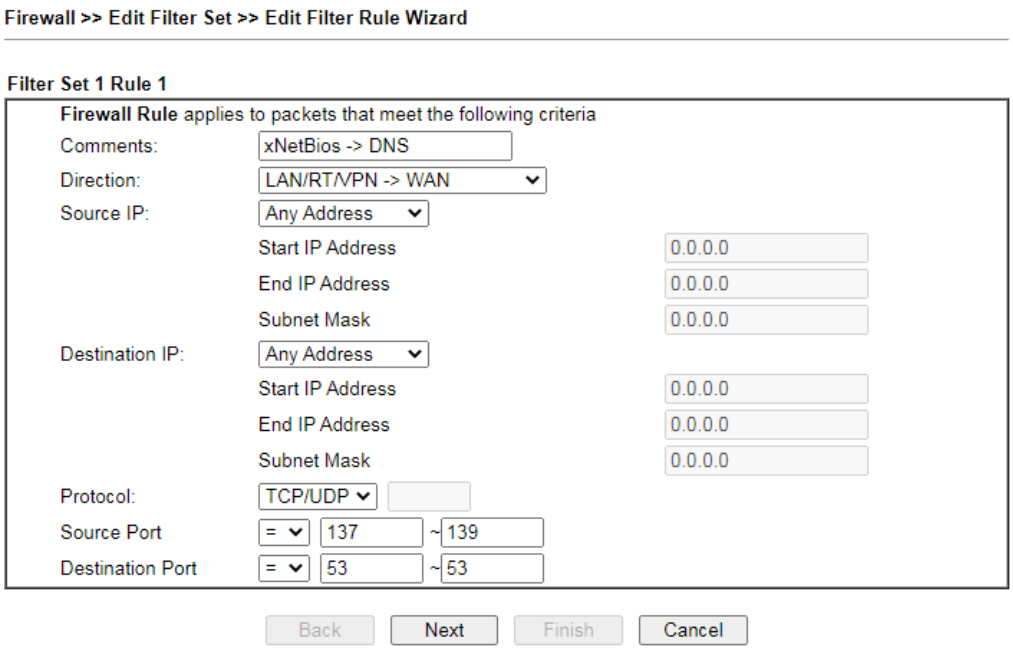
Available settings are explained as follows:

Item	Description
Filter Rule	To edit the filter rule, click the filter rule number to bring up the Edit Filter Rule page. See the following section for details on the Edit Filter Rule page.
Enable	Select to enable the filter rule.
Comments	Optional comment entered in the settings page to identify the rule.
Direction	Displays the direction of packet.
Src IP / Dst IP	Displays the IP address of source /destination.
Service Type	Displays the type and port number of the packet.

Action	Displays the packets to be passed /blocked.
CSM	Displays the content security managed
Move Up/Down	Use **Up** or **Down** link to change the order of the filter rules.
Next Filter Set	Select the filter set for the firewall to process after the current filter set, or None if the current filter set is the last one to be processed. Be careful not to create a loop when setting next 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. **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.

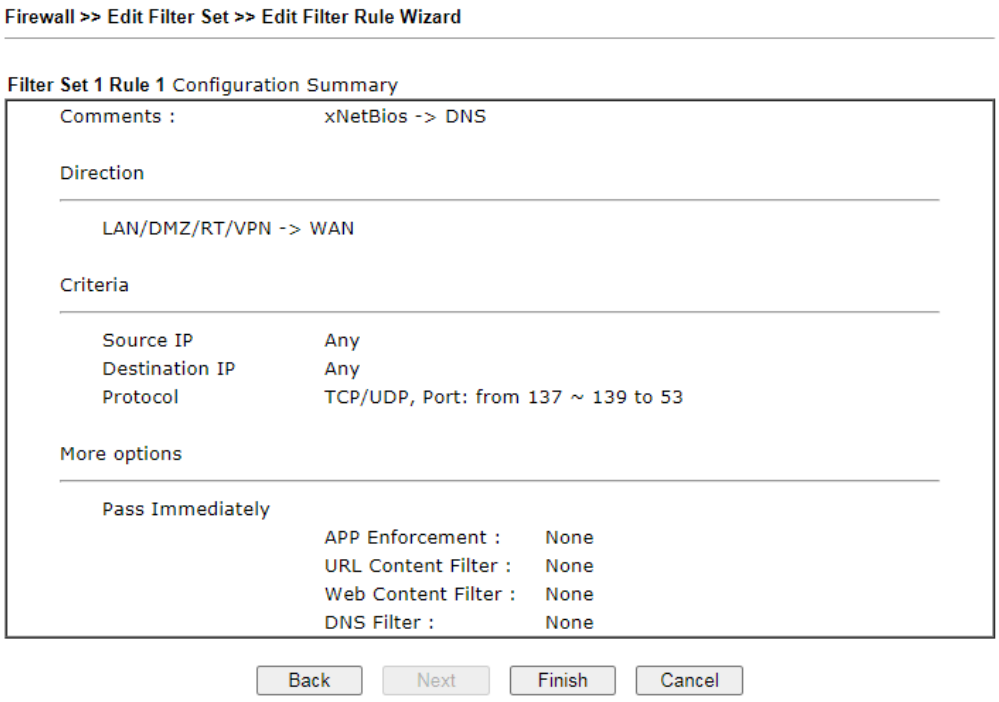
Source Port / Destination Port	*(=)* – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. *(!=)* – when the first and last value are the same, it indicates all the ports 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.

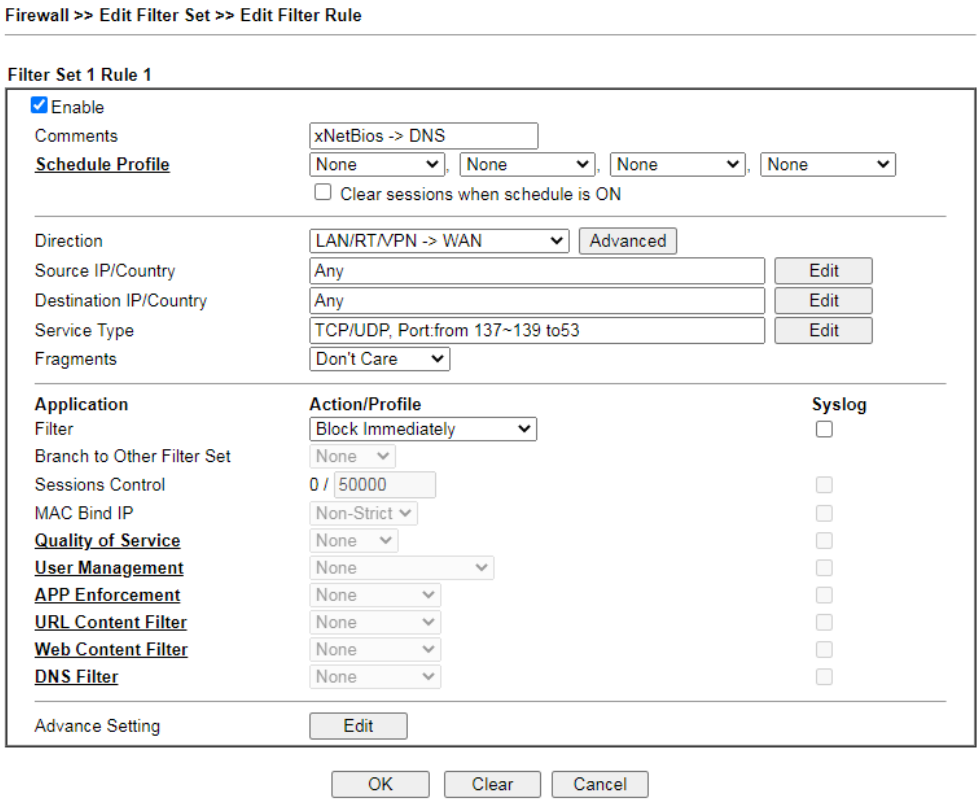
4. After choosing the mechanism, click **Next** to get the summary page for reference.



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

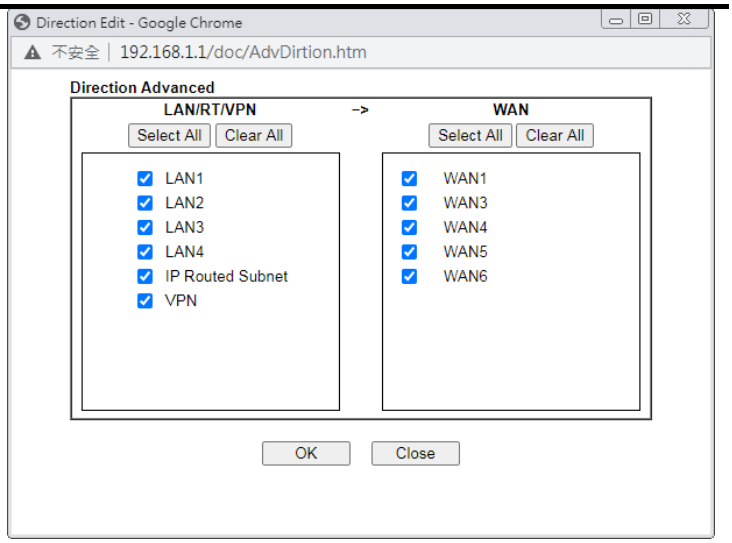
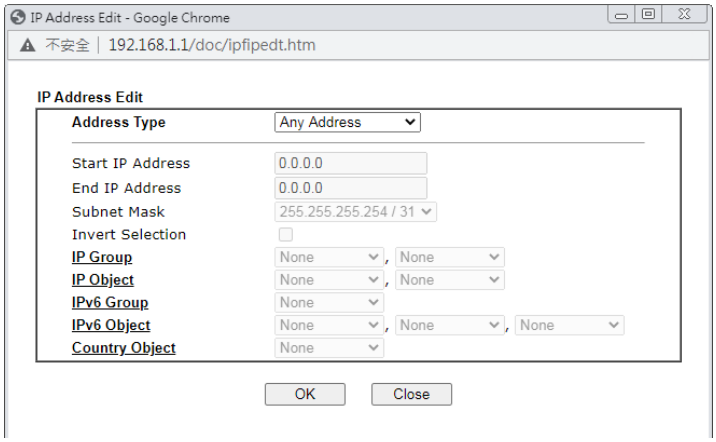
To use **Advance** Mode, do the following steps:

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

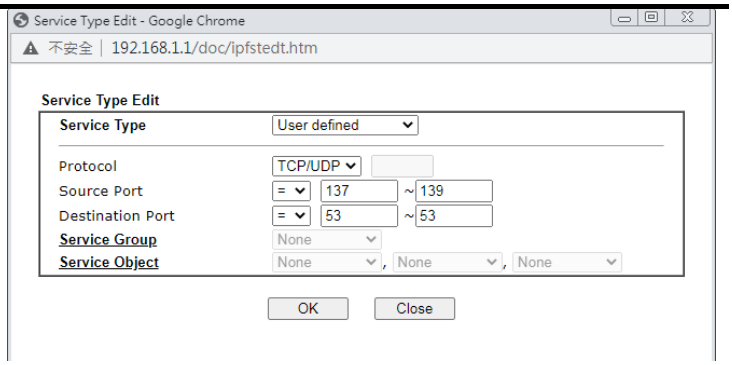


Available settings are explained as follows:

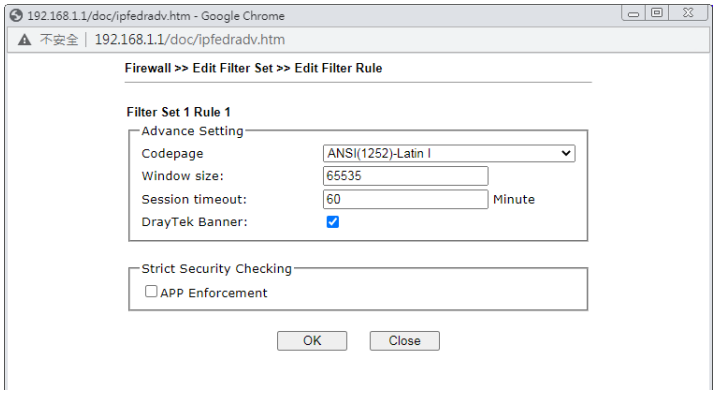
Item	Description
Enable	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Schedule Profile	Select Schedule indexes to allow the rule to be enabled at specific times. You may choose up to 4 out of the 15 schedules in Applications >> Schedule. The rule is always enabled when no indexes have been selected.
Clear sessions when schedule ON	Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset.
Direction	Specify the direction of traffic flow to which this filter rule applies. **Note:** RT stands for the routing domain for 2nd subnet or other LAN. **Advanced** - After choosing the direction, click the Advanced button to specify interfaces for traffic flow.

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Source IP/ Country
and
Destination IP / Country</td><td>Click Edit to bring up the following dialog box to configure the source and destination IP addresses or country objects.
 

To set the IP address manually, please choose an Address Type and enter required information.
Address Type – Select from one of the following:
● Any Address – All IP addresses
● Single Address – Enter one IP address in Start IP address
● Range Address – Enter the Start and End IP Addresses
● Subnet Address – Enter the Start IP Address and the Subnet Mask. Example: Start IP Address 192.168.1.1 and Subnet Mask 255.255.255.128 means is the same as having the Start IP Address as 192.168.1.1 and the End IP Address as 192.168.1.127.
● Group and Objects – Allows selection of predefined IP Groups and IP Objects. For details on IP Groups and Objects, see the chapter on Objects Setting.
● Country Object - Allows selection of predefined country objects.</td></tr>
<tr><td>Service Type</td><td>Click Edit to bring up the following dialog box to configure the Service Type.</td></tr>
</table>

	 **Service Type** - To set the service type manually, please choose **User defined** as the Service Type. ● **User defined** – Configure the protocol, source and destination ports manually. ● **Group and Objects** – Select preconfigured Service Groups or Objects. **Protocol -** Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -** ● (=) – any port that falls within the specified range ● (!=) – any port that falls outside of the specified range ● (>) – a port whose number is greater than the specified value ● (<) – a port whose number is smaller than the specified value **Service Group/Object** - Use the drop down list to select the desired Service Groups or Objects.
Fragments	Action to be taken for fragmented packets. This option is valid for **Data Filter** rules 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	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** – Block the packet if this the last matching rule for this packet in the filter. **Pass If No Further Match** – Pass the packet if this is the last matching rule for this packet in the filter.
Branch to other Filter Set	If the packet matches the filter rule, and the Filter action is **Block If No Further Match** or **Pass If No Further Match**, you can specify the next filter set to be applied, thus skipping the rest of the rules in the current filter set.
Sessions Control	The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions allowed, which is configurable. The default maximum is

	60000, which is also the upper limit of the value.
MAC Bind IP	**Strict** – Ensure that both the MAC address and the IP address of the source and/or destination clients. **Non-Strict** – Do not check the IP address when processing IP Objects that specify MAC addresses.
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.
User Management	This setting is only available when **Rule-Based** is selected in **User Management>>General Setup**. The default firewall rule will be applied to the selected user or user group. Refer to the chapter on User Management for more details on the feature. ● **None**: User Management does not apply to the default rule. ● **User Object**: The default rule only applies to the selected user. ● [**Create New User**]: Select this to create a new user. ● User Group: The default rule only applies to the selected User Group. ● [**Create New Group**]: Select this to create a new user group. ● **ALL**: The default rule applies to all defined users. ● **Create New User** or **Create New Group** item will appear for you to click to create a new one if there is no user profile or group profile existed. **Syslog** - Select to allow User Management to log messages in Syslog.
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. **Syslog** - Select to allow APP Enforcement to log messages in Syslog.
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. **Syslog** - Select to allow URL Content Filter to log messages in Syslog. Logging action is configured at the profile level in CSM>>URL Content Filter Profile, Log.
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. **Syslog** - Select to allow Web Content Filter to log messages in Syslog. Logging action is configured at the profile level in the Web Content Filter Profile Table section in CSM>>Web Content Filter Profile, Log.
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 configuration window for Advanced Settings. However, it is recommended to use the default settings.  **Codepage** – Sets the codepage used by the URL content filter to match URLs against keywords in profiles. Choosing the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed. If you are unsure of which codepage to use, please start the Syslog application, and the recommended codepage will be shown in the Codepage Information tab in the Setup dialog box. **Window size** – Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 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** – Sets the timeout sessions are allowed to idle before they are removed from the system. **DrayTek Banner** – Select to display the following screen for web pages that are blocked by the Firewall. The default setting is Enabled.

	 Strict Security Checking **APP Enforcement** – If this option is selected, when the router cannot identify the application that generated the outbound traffic due to limited system resources, the session will be blocked; if this option is not selected, the session will be allowed.

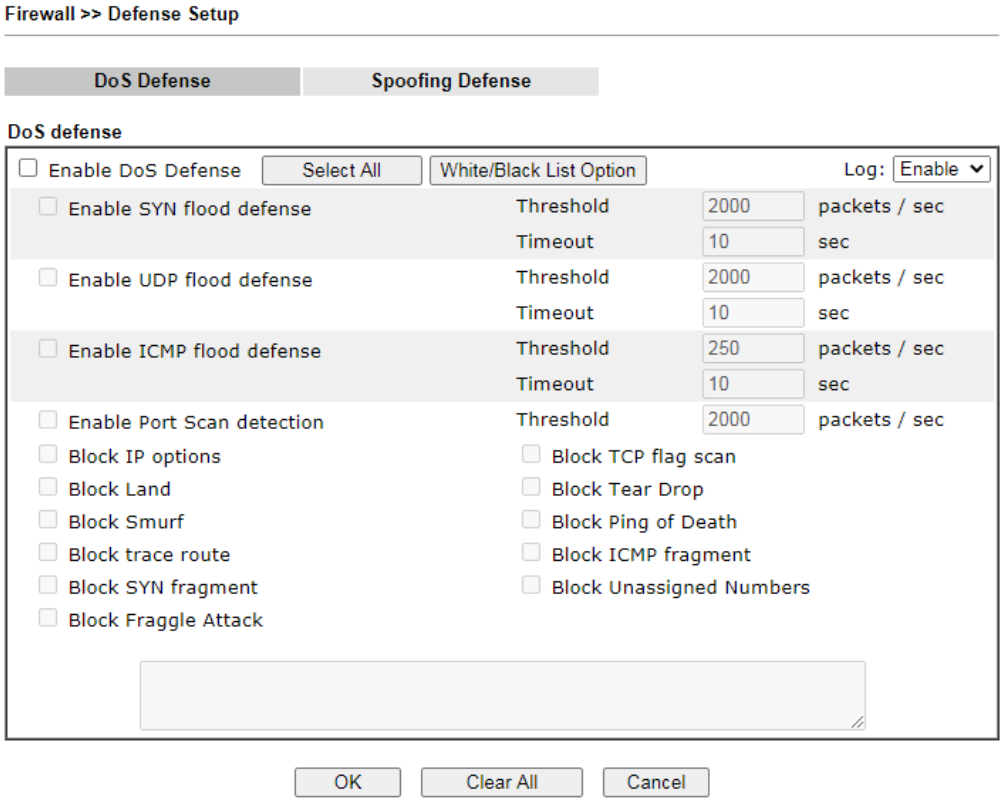
3. When you finish the configuration, please click **OK** to save and exit this page.

V-1-3 Defense Setup

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

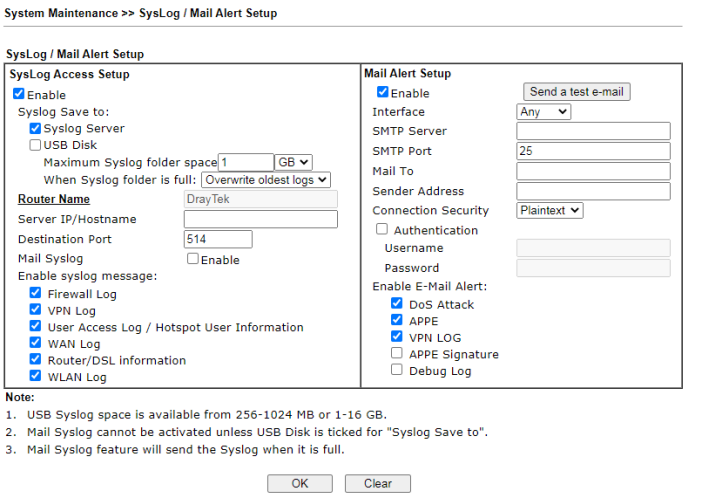
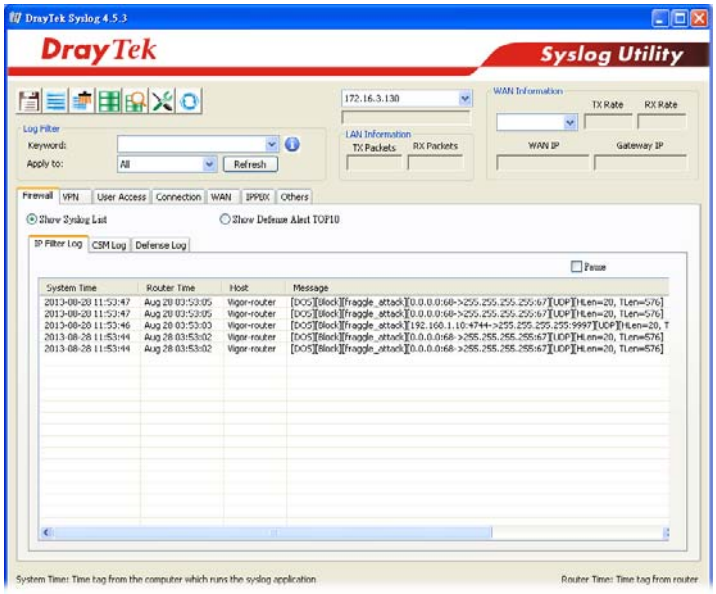
To configure DoS Defense, select DoS Defense under the Firewall menu item on the Web UI menu bar.



Available settings are explained as follows:

Item	Description
Enable Dos Defense	Select to enable DoS Defense. **Select All -** Click to select all DoS Defense options. **White/Black List Option** – Set white/black list of IPv4/IPv6 address.
Enable SYN flood defense	Select to enable SYN flood defense. When the arrival rate of SYN packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. This is to prevent TCP SYN packets from exhausting router resources. The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Select to enable UDP flood defense. When the arrival rate of UDP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. The default values of threshold and timeout are 2000

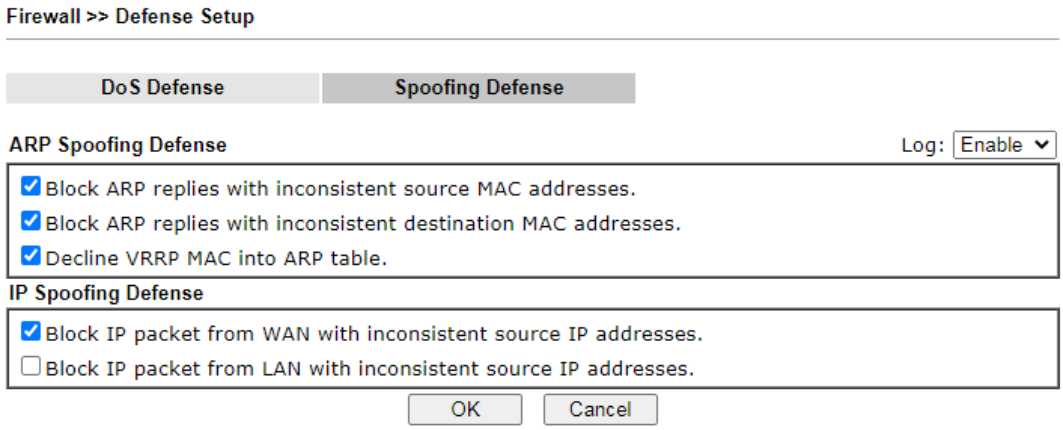
	packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Select to enable ICMP flood defense. When the arrival rate of ICMP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. The default values of threshold and timeout are 250 packets per second and 10 seconds, respectively.
Enable Port Scan detection	Select to enable Port Scan detection. Port Scans attack your network by sending packets to a range of ports in an attempt to find services that would respond. When Port Scan detection is enabled, the router sends warning messages when it detects port scanning activities that exceed the Threshold rate. The default threshold is 2000 packets per second.
Block IP options	Select to enable Block IP options. The Vigor router will ignore IP packets with IP option field set in the datagram header. IP options are rarely used and could be abused by attackers as they carry information about the private network otherwise not available to the external network, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages, etc, which external eavesdroppers can use to discover details about the private network.
Block Land	Select to Block LAND attacks. LAND attacks happen when an attacker sends spoofed SYN packets with both source and destination addresses set to that of the target system, which causes the target to reply to itself continuously.
Block Smurf	Select to Block Smurf attacks. The router will ignore any broadcasting ICMP echo request.
Block trace route	Select to Block traceroutes. The router will not forward traceroute packets.
Block SYN fragment	Select to Block SYN packet fragments. The router will drop any packets having both the SYN and more-fragments bits set.
Block Fraggle Attack	Select to Block Fraggle Attacks. Broadcast UDP packets received from the Internet are blocked. Activating this feature might block some legitimate packets. Since all broadcast UDP packets coming from the Internet are blocked, RIP packets from the Internet could also be dropped.
Block TCP flag scan	Select to Block TCP Flag Scans. TCP packets with abnormal flag settings will be dropped. TCP flag scanning activities that are blocked include no flag scan, FIN without ACK scan, SYN FIN scan, Xmas scan and full Xmas scan.
Block Tear Drop	Select to Block Tear Drop attacks. Some clients may crash when they receive ICMP datagrams (packets) that exceed the maximum length. The router discards any fragmented ICMP packets having lengths greater than 1024 octets.
Block Ping of Death	Select to Block Ping of Death, where fragmented ping packets are sent to target hosts so that those hosts could crash as they reassemble the malformed ping packets.
Block ICMP Fragment	Select to Block ICMP Fragments. ICMP packets with the more-fragments bit set are dropped.

Block Unassigned Numbers	Select to Block Unassigned Protocol Numbers, and the router will block packets having unassigned protocol numbers. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
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.

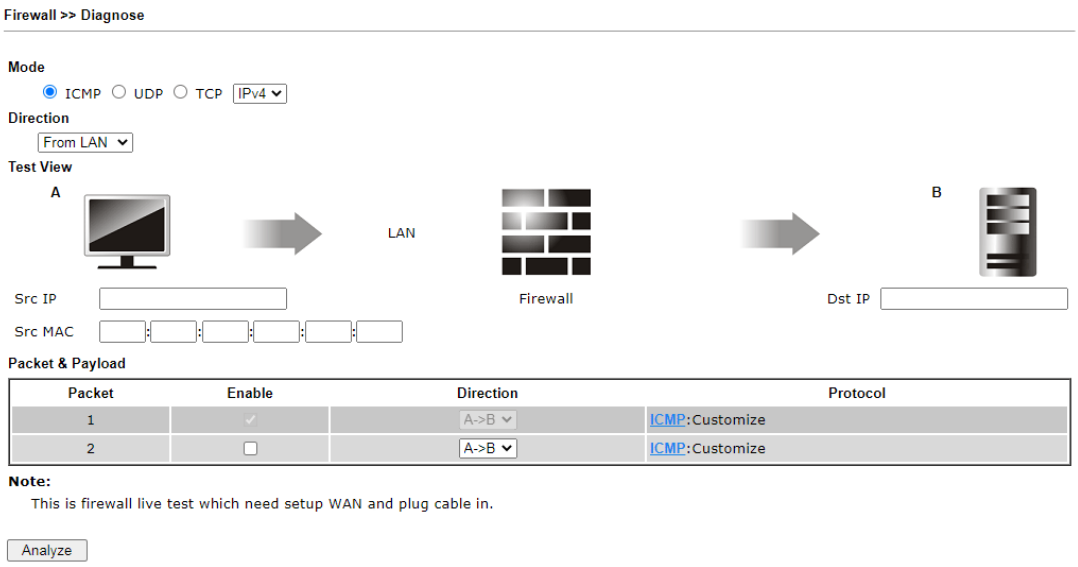


V-1-4 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet. The test result, including firewall rule profile, IP address translation in packet transmission, state of the firewall fuctions and etc., also will be shown on this page.

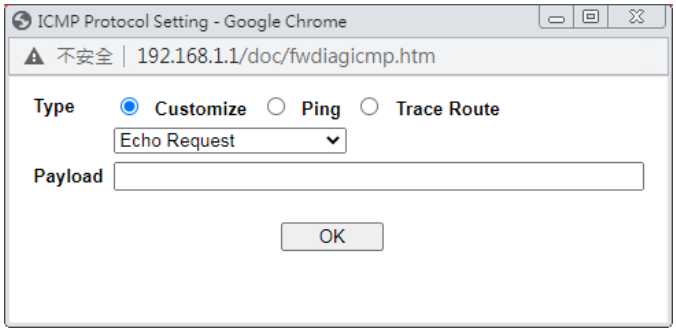
Info

The result obtained by using Diagnose is offered for RD debug. It will be different according to actual state such as netework connection, LAN/WAN settings and so on.

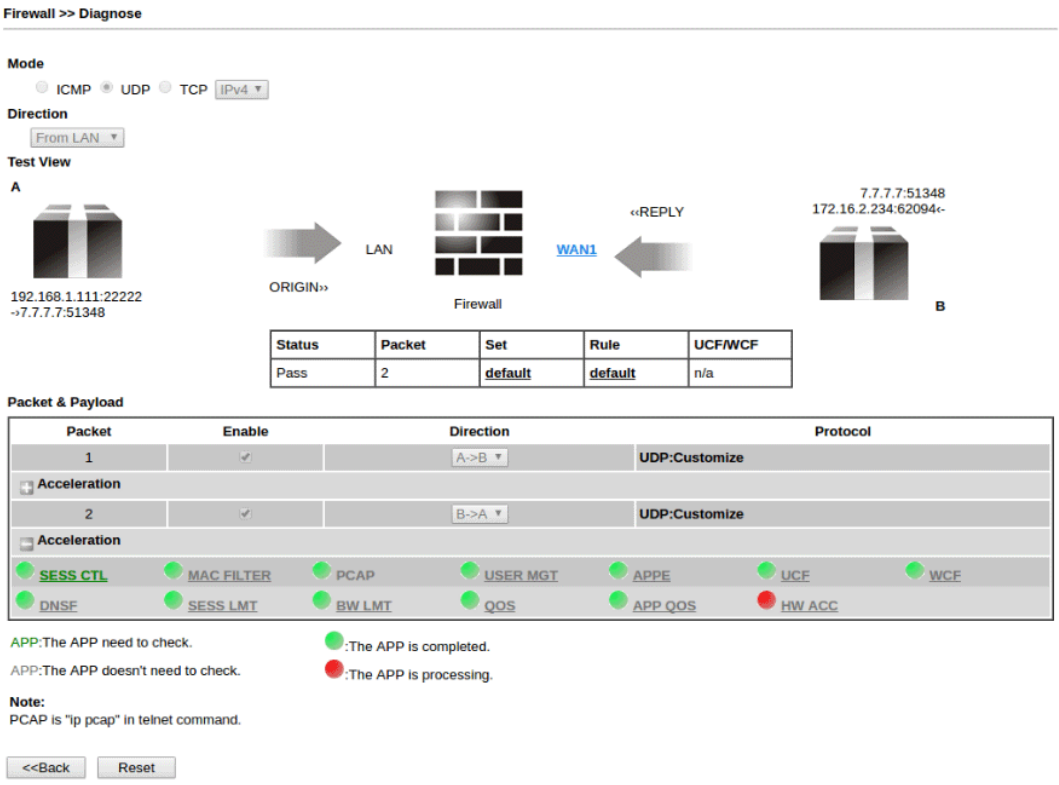


Available settings are explained as follows:

Item	Description
Mode	To have a firewall rule test, specify the service type (ICMP, UDP, TCP) of the packet and type of the IP address (IPv4/IPv6).
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test. Different way means the firewall will process the connection initiated from LAN or from WAN.
Test View	This is a dynamic display page. According to the direction specified, test view will display the figure to guide you typing IP address, port number, and MAC address. Later, after clicking the Analyze button, the information for the firewall rule profile and address translation will be shown on this page.
Src IP	Enter the IPv4/IPv6 address of the packet's source.
Src Port	Enter the port number of the packet's source.
Src MAC	Enter the MAC address of the packet's source.
Dst IP	Enter the IPv4/IPv6 address of the packet's destination.

Dst Port	Enter the port number of the packet's destination.
Packet & Payload	In firewall diagnose, two packets belong to one connection. In general, two packets are enough for Vigor router to perform this test. **Enable** – Check the box to send out the test packet. **Direction** – The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet. **Protocol** – It displays the mode selected above and the state. If required, click the mode link to configure advanced setting. The common service type (Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http(GET) related to that mode (ICMP / UDP / TCP) will be shown on the following dialog box.  ● **Type** – Choose Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http (GET). ● **Payload** – It is available when Customize is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transfered with protocol (ICMP/UDP/TCP) which is different to Type setting.
Analyze	Execute the test and analyze the result.

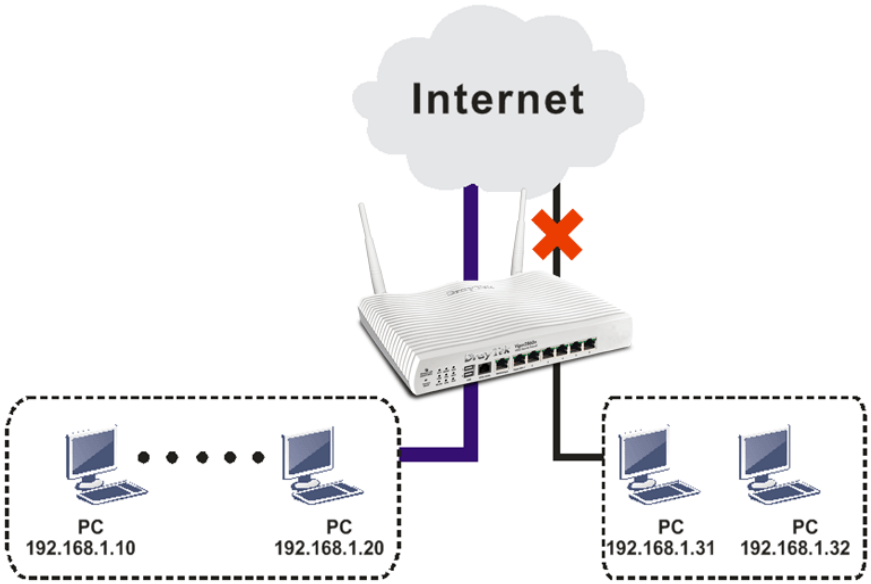
The following figure shows the test result after clicking **Analyze**. Processing state for the fuctions (MAC Filter, QoS, User management, etc.,) related to the firewall will be displayed by green or red LED.



Application Notes

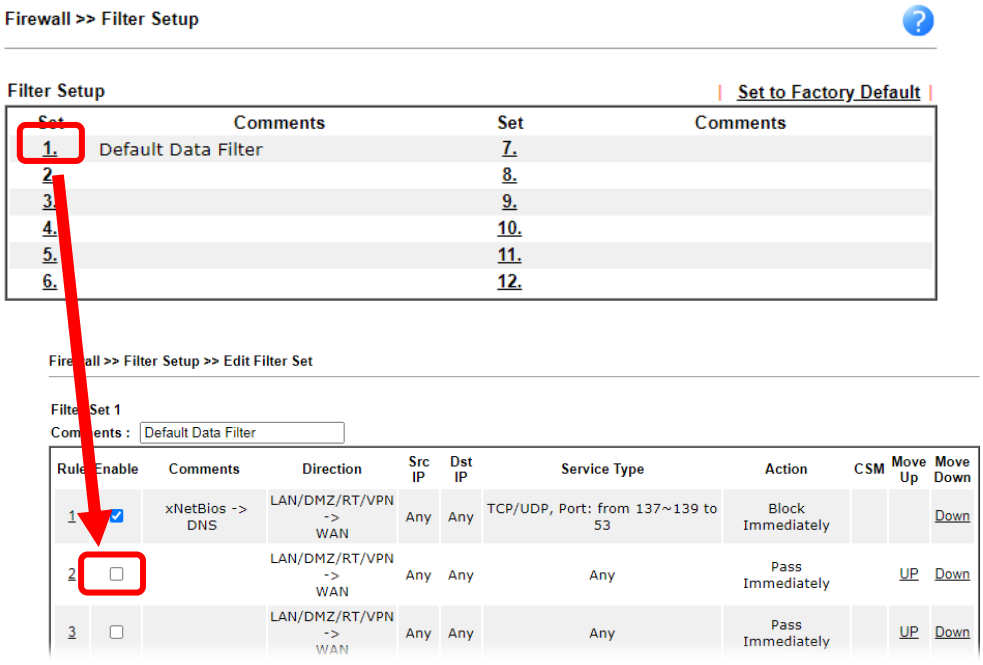
A-1 How to Configure Certain Computers Accessing to Internet

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.

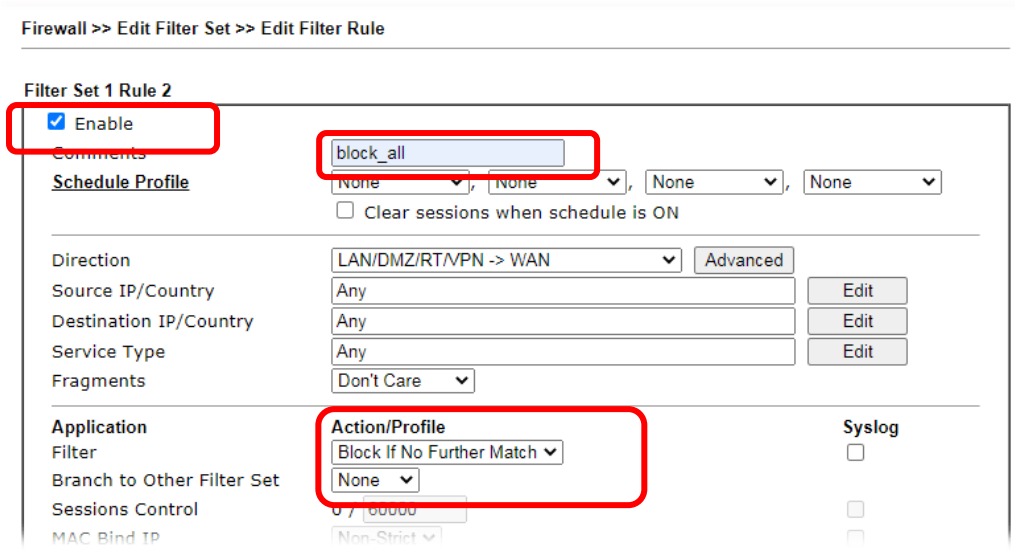


The way we can use is to set two rules under **Firewall**. For **Rule 1** of **Set 2** under **Firewall>>Filter Setup** is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

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 **Enable**. Enter the comments (e.g., **block_all**). Choose **Block If No Further Match** for the **Filter** setting. Then, click **OK**.

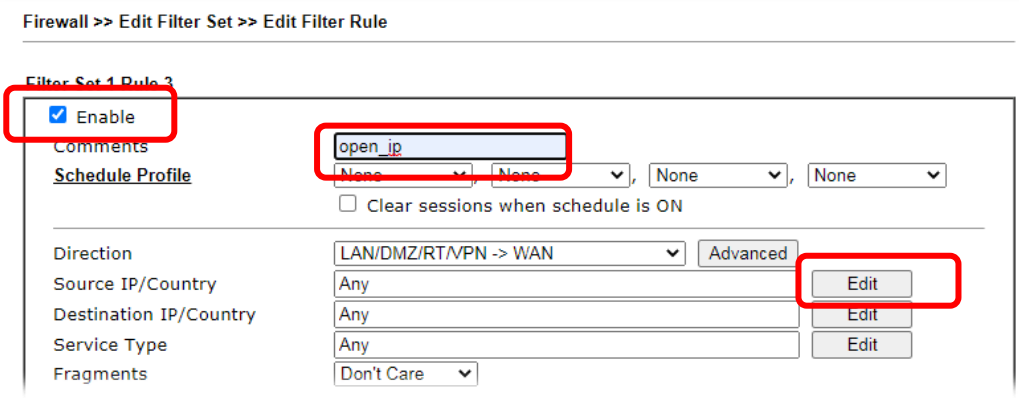


Info

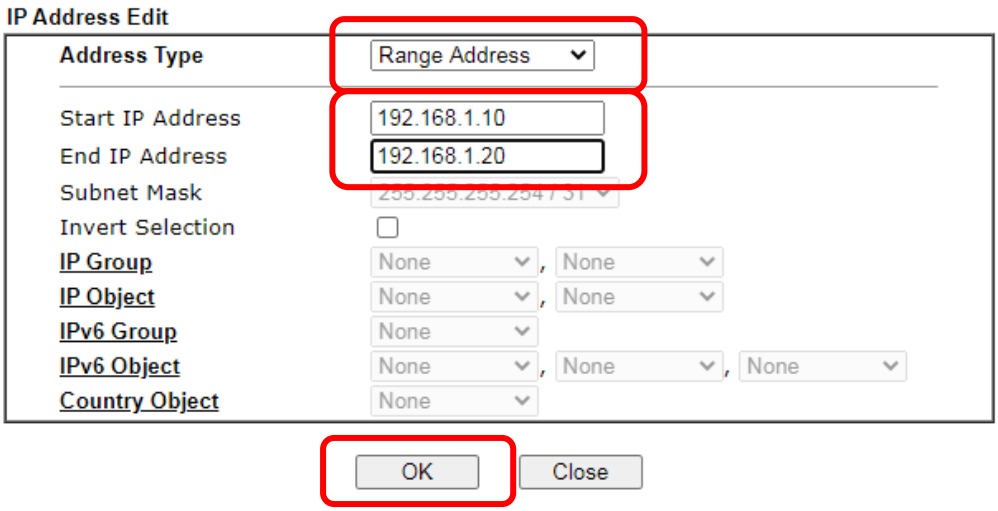
In default, the router will check the packets starting with Set 2, Filter Rule 2 to Filter Rule 7. If Block If No Further Match for is selected for Filter, the firewall of the router would check the packets with the rules starting from Rule 3 to Rule 7. The packets not matching with the rules will be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

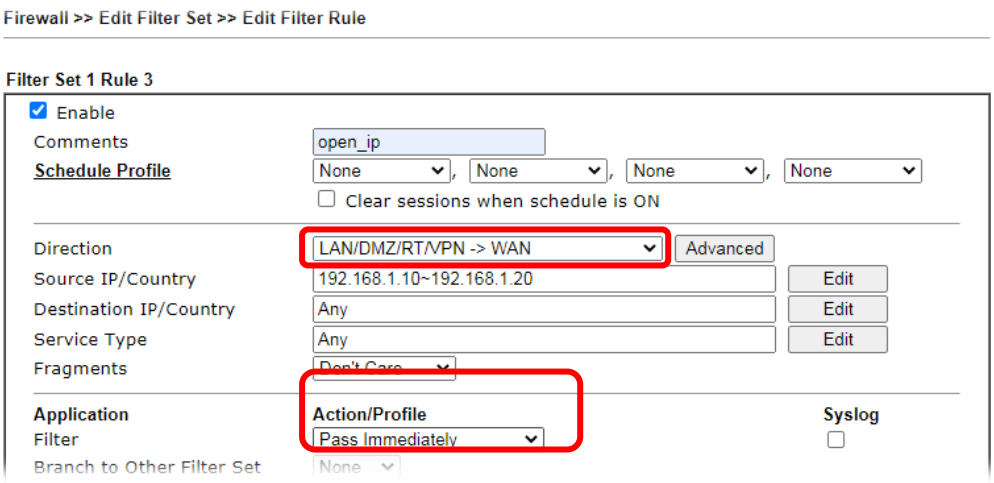
5. Check the box of **Check to enable the Filter Rule**. Enter the comments (e.g., **open_ip**). Click the **Edit** button for **Source IP**.



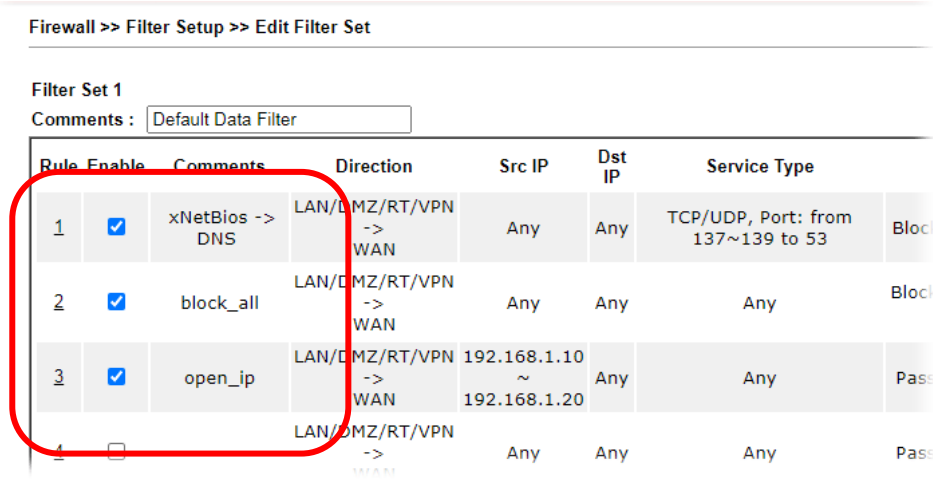
6. A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.



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**.



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)

Content Security Management (CSM) allows the network administrator to restrict Internet traffic based on the content type, thus ensuring appropriate use of network resources and also reducing the likelihood of threats from malicious network content.

APP Enforcement Filter

The APP Enforcement Filter can be used to prevent users from using undesirable or inappropriate network applications such as online chat and peer-to-peer programs. The filter works by detecting and blocking network traffic of applications by means of traffic patterns.

URL Content Filter

The URL Content Filter scans URL strings in HTTP requests for predefined keywords to restrict browsing activities.

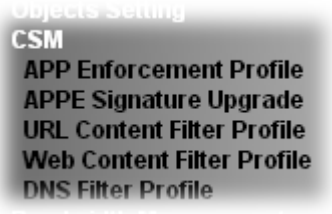
Web Content Filter

Users can also be prevented from browsing certain types of websites by using the Web Content Filter. This filter classifies website domain names into different categories, which can be selectively blocked.

Filter profiles must first be created before these CSM Filters can be enabled. Once profiles have been configured, they can be applied to the Default Rule under Firewall>>General Setup, or Filter Rules in Filter Sets under Firewall>>Filter Setup.

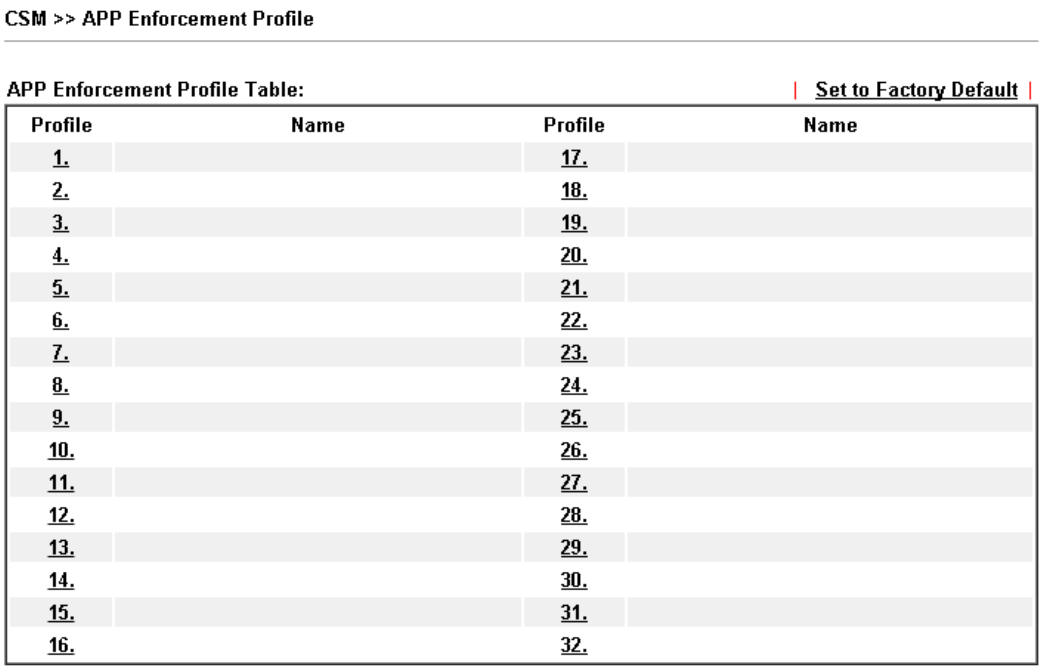
Info	The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface



V-2-1 APP Enforcement Profile

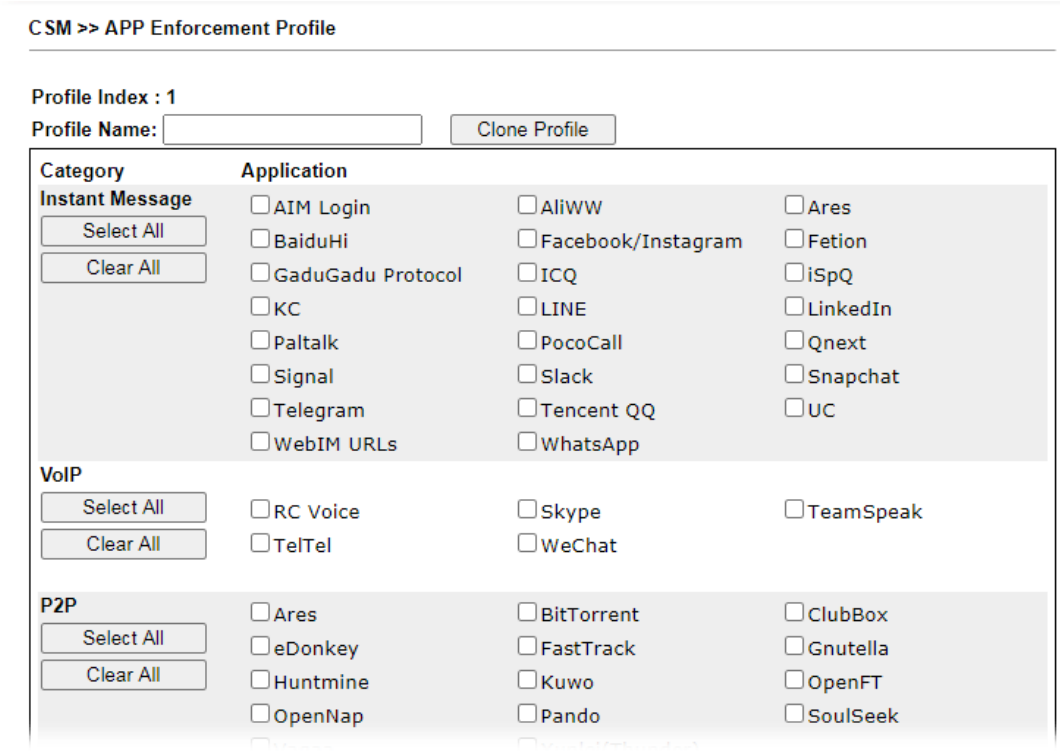
Up to 32 policy profiles for APP Enforcement can be configured.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Profile	Index of the profile. Click to bring up the configuration page of the profile.
Name	Name of the profile.

To configure a profile, click on its profile number, and the following profile configuration page will appear:



Available settings are explained as follows:

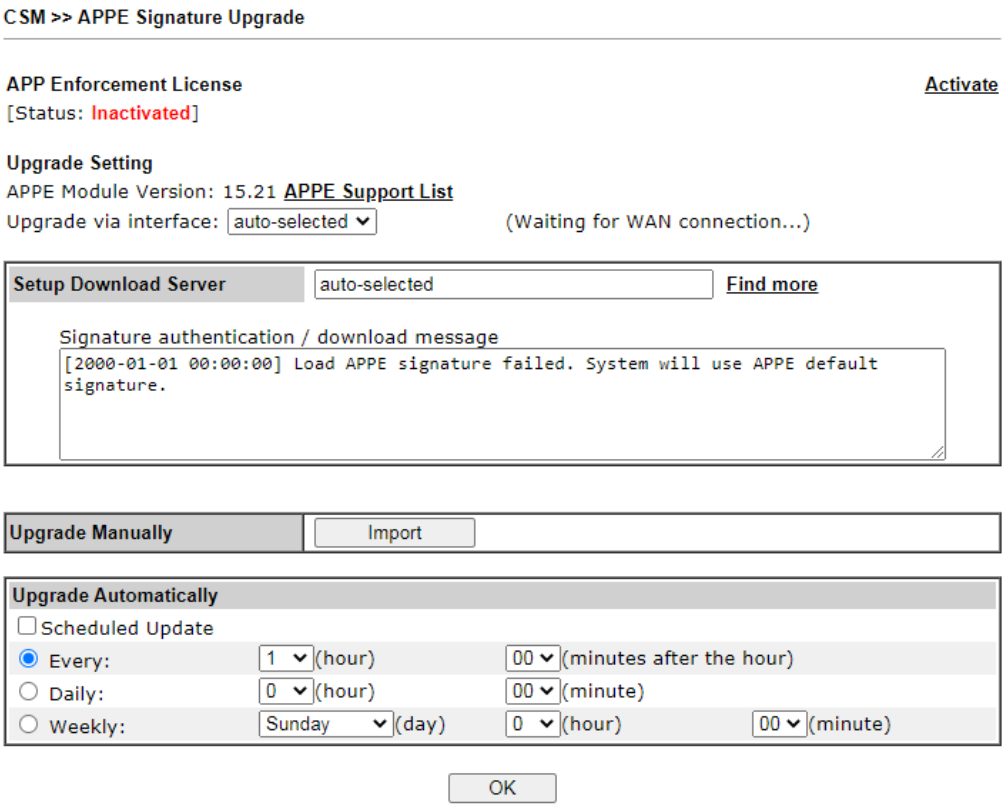
Item	Description
Profile Name	Name that identifies this profile. Maximum length is 15 characters.
Clone Profile	Click it to clone settings configured by an existed profile.
Category	Apps are classified into several categories. Each category contains several apps to be blocked.
Select All	Click to select all of the items on this page.
Clear All	Click to deselect all selected items.
Enable	Select this checkbox to block the app.

To save changes on the page, click **O**K. To discard changes, click **Cancel**.

V-2-2 APPE Signature Upgrade

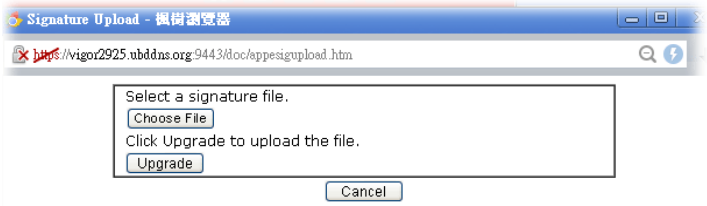
The APP Enforcement Profile feature identifies applications by matching their network traffic to signatures. DrayTek periodically releases APPE signature upgrades to ensure that new applications or new versions can be detected.

Upgrade checks can be performed manually or automatically.



Available settings are explained as follows:

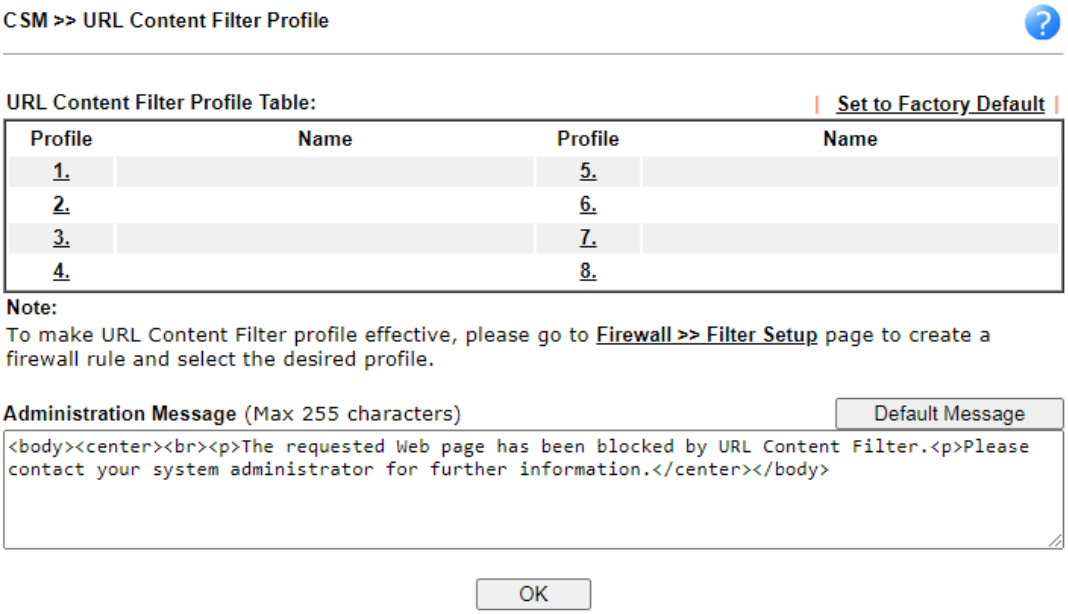
Item	Description
APP Enforcement License	**Status -** Display current license status.
Upgrade Setting	**APPE Module Version** – Shows the current version of the APPE signature. **Upgrade via interface** – Select a WAN interface to download the new APPE signature.
Setup Download Server	Specify a download server by typing its URL of the server. Click the **Find more** for a list of download servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address. **Signature authentication/download message** –Displays download status messages.
Upgrade Manually	Use this functionality if you wish to upgrade using a previously-downloaded signature file. **Import** – Clicking the button brings up the following page.

	 Click **Choose File** to select the signature file. Click **Upgrade** to initiate the upgrade process.
Upgrade Automatically	**Scheduled Update -** Select to enable automatic periodic checking for signature updates.

Click **OK** to save changes on the page.

V-2-3 URL Content Filter Profile

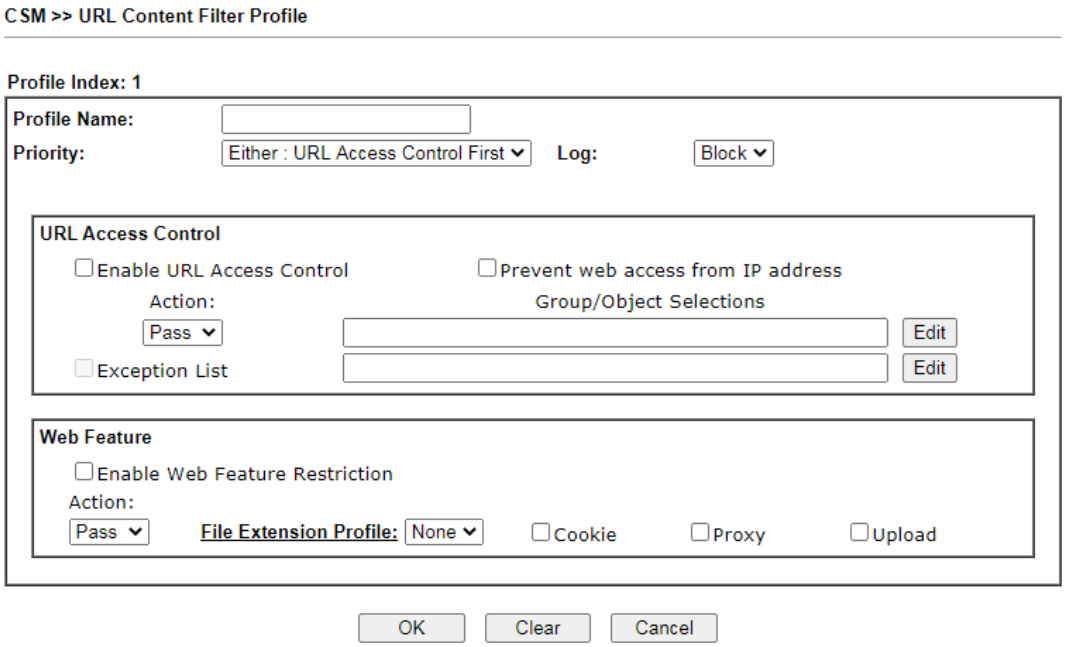
To set up URL Content Filter Profiles, click **CSM** on the Main Menu bar, and then click **URL Content Filter Profile** to open the profile setting page.



Each item is explained as follows:

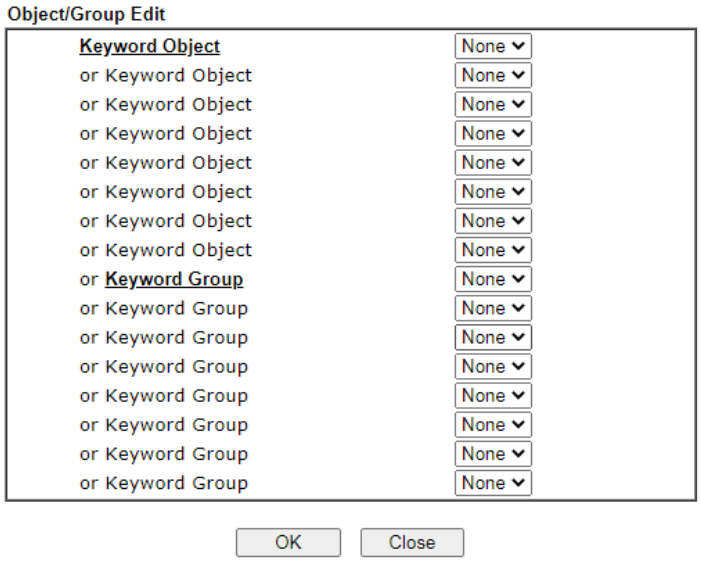
Item	Description
Set to Factory Default	Clear all profile settings.
Profile	Index number of the profile.
Name	Name that identifies the profile.
Administration Message	The message to be displayed in the browser when access to a URL has been blocked. A custom message can be entered with HTML formatting in the text box. **Default Message** - Click to reset the administration message to the factory default.

To set up a profile, click the profile number under Index column to bring up the configuration page.



Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies the URL Content Filter profile. The maximum length of the Profile Name is 15 characters.
Priority	The order of evaluation of URL Access Control and Web Feature below: **Both: Pass** – Router will allow access only to web resources that match conditions specified in both URL Access Control and Web Feature. The Action setting of both URL Access Control and Web Feature will be disabled and the values set to Pass. **Both:Block** – Router will block access to web resources that match conditions specified in both URL Access Control and Web Feature. The Action setting of both URL Access Control and Web Feature will be disabled and the values set to Block. **Either: URL Access Control First** – Router will block or allow access to web resources that match conditions specified in either URL Access Control or Web Feature. URL Access Control is applied first, followed by Web Feature. **Either: Web Feature First** – Router will block or allow access to web resources that match conditions specified in either URL Access Control or Web Feature. Web Feature is applied first, followed by URL Access Control.
Log	**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. **All** – Both passed and blocked access attempts will be recorded in Syslog.
URL Access Control	**Enable URL Access Control** - Select to activate URL Access Control. **Prevent web access from IP address** - URLs containing IP addresses (e.g., 192.168.1.1) will be blocked. Only URLs with

	domain addresses (e.g., www.draytek.com) will be allowed. This is to prevent users from circumventing URL Access Control. **Action** – This setting is enabled only when Priority is set to Either: URL Access Control First or Either: Web Feature First. ● **Pass –** Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked. ● **Block –** Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed. **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** – Shows the Keyword Groups and/or Objects selected for this URL Content Filter Profile. To add or remove Keyword Groups and Objects to the selection, click the **Edit** button to bring up the following screen.  Up to 8 Keyword Objects and 8 Keyword Groups can be selected. To add, remove or modify Groups or Objects, click the Keyword Object or Keyword Group hyperlinks to bring up the **Objects Setting >> Keyword Object** or **Objects Setting >> Keyword Group** pages.
Web Feature	**Enable Restrict Web Feature -** Check to enable the web feature restriction. **Action -** This setting is enabled only when Priority is set to **Either: URL Access Control First** or **Either: Web Feature First**. ● **Pass** – Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked. ● **Block** – Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed. **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** - Select to block cookies from Internet websites. **Proxy** - Select to block web proxy servers that relay HTTP traffic. **Upload** – Select to block HTTP uploads from the LAN to the Internet.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To clear all settings, click **Clear**.

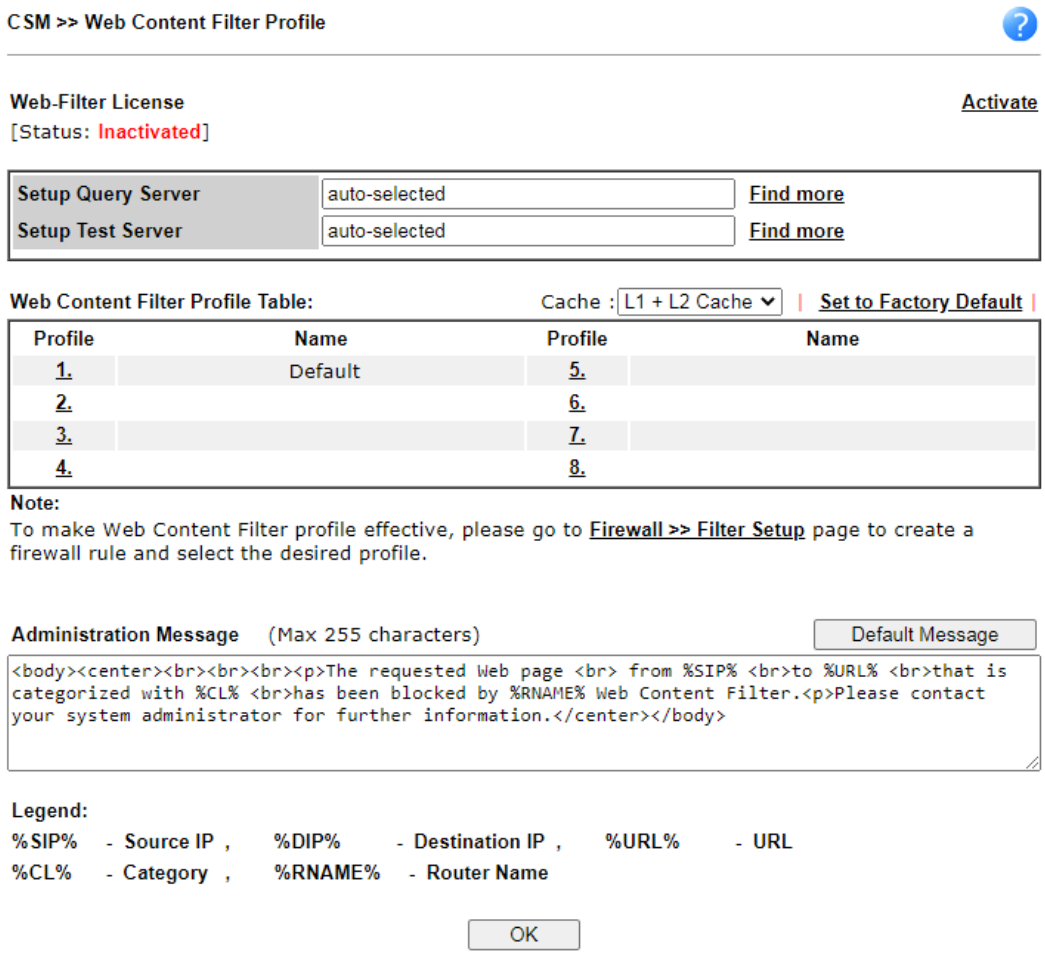
V-2-4 Web Content Filter Profile

Trial WCF service can be activated using the **Service Activation Wizard**.

If you wish to continue using WCF beyond the trial period, you can obtain a full WCF subscription by contacting your local DrayTek channel partner or dealer. WCF subscriptions can be activated using the **Activate** link on **CSM >> Web Content Filter Profile** (described in this section) or **System Maintenance**.

From the main menu, click **CSM**, followed by **Web Content Filter Profile** to load the profile configuration page.

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

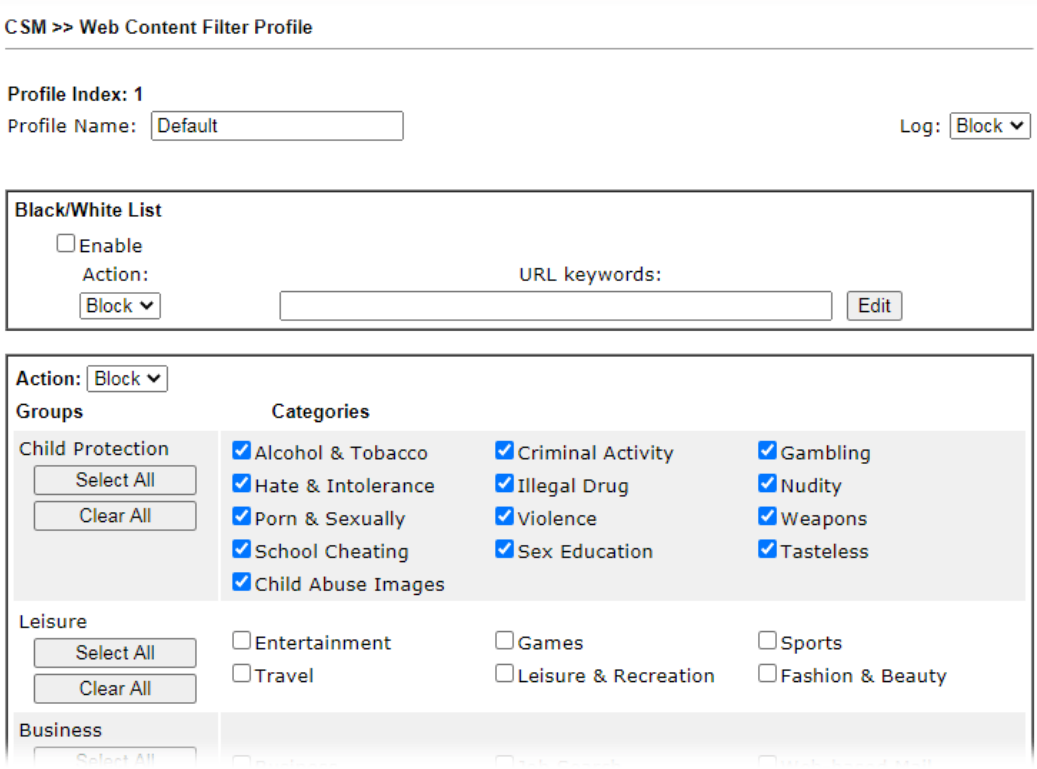


Available settings are explained as follows:

Item	Description
Activate	Click to visit the MyVigor webnsite to activate WCF service. You will need to log in to your MyVigor account to proceed with the activation process. If you do not already have a MyVigor account, you can create one at this time.
Setup Query Server	Specify a WCF query server by typing address of the server. Click the Find more for a list of query servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address. It is recommended that the default setting auto-selected be used.
Setup Test Server	Specify a WCF test server by typing address of the server. Click the Find more for a list of test servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address. It is recommended that the default setting auto-selected be used.
Cache	**None** – The router verifies every HTTP URL requested by communicating with the WCF server on the Internet. This mode provides the most precise URL matching but has the lowest performance. **L1** – The router caches the HTTP URLs that have been checked against the WCF server. URLs will be looked up in the L1 cache before reaching out to the WCF server. When the cache is full, the oldest entry will be deleted to accommodate new URLs. **L2** – After a URL has been checked and found to pass WCF, the source and destination IPs are cached for about 1 second in the L2 cache. This is to allow a webpage to be loaded without further verifying the same URLs against the L1 cache or the WCF server. **L1+L2 Cache** – The router will utilize both L1 and L2 caches.
Set to Factory Default	Clear all profile settings.
Profile	Index number of the profile.
Name	Name that identifies the profile.
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.

Up to 8 WCF profiles can be set up. To configure a profile, click its profile number to bring up its configuration page. Filter profile settings are specific to WCF providers. If you already

have an active WCF subscription, activating a WCF subscription to a provider that is different from your current provider will clear all existing profile configuration.



Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies the WCF profile. The maximum length of the Profile Name is 15 characters.
Log	**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. **All** – Both passed and blocked access attempts will be recorded in Syslog.
Black/White List	Keyword objects and groups can be applied to the URL to override WCF category filtering. **Enable –** Select to enable blacklisting or whitelisting. **Action** - Action to take when a URL matches keyword group and object selections. ● **Pass** – Allow access to the URL. ● **Block** – Disallow access to the URL. **URL Keywords –** Displays selected keyword group and objects. Click the **Edit** button to modify keyword selections.
Groups and Categories	Select categories to be included in the filter. **Action** - Action to take when a URL matches keyword group and object selections. ● **Pass** – allow access to the URL. ● **Block** – disallow access to the URL. **Select All -** Click to select all categories within the group.

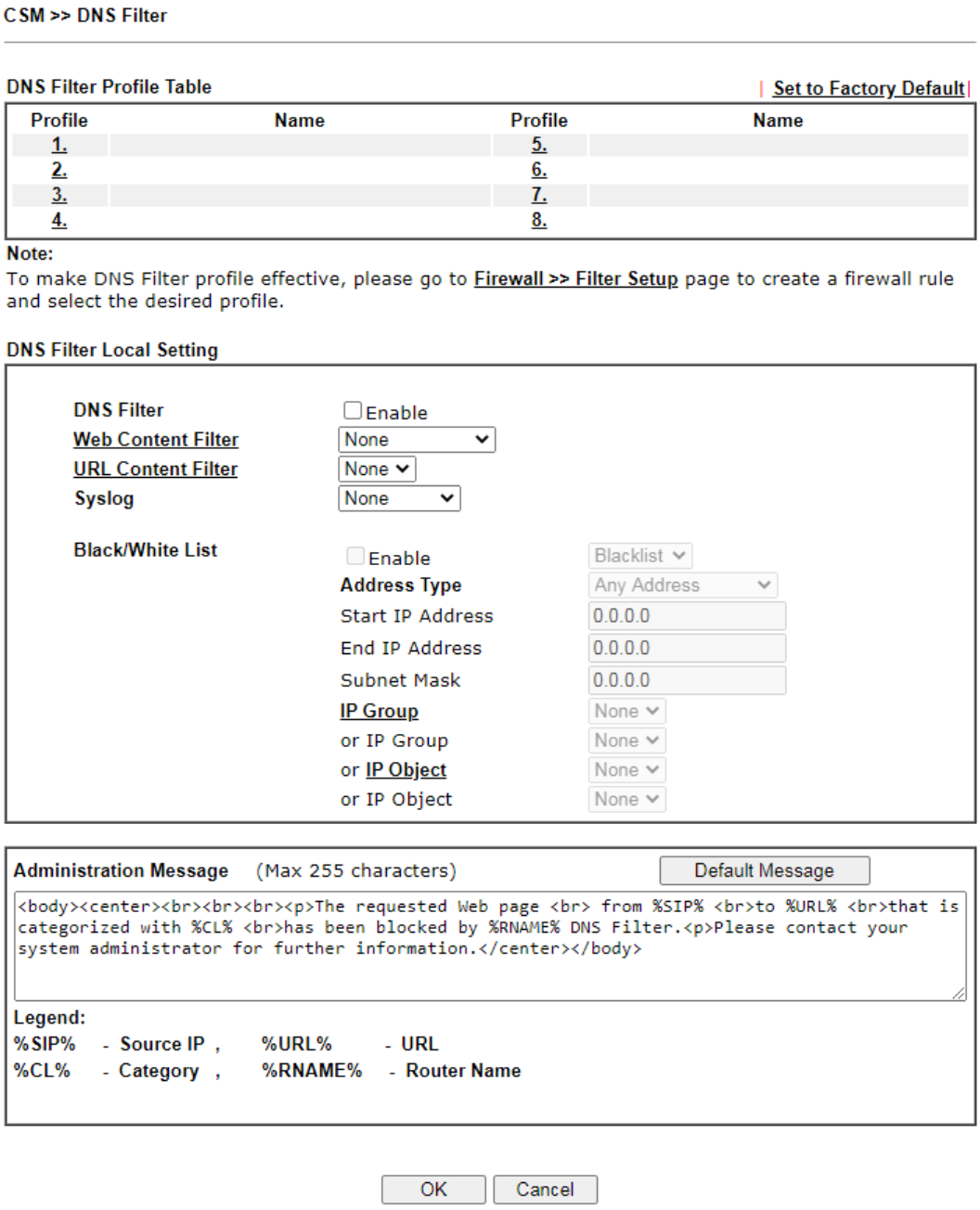
	Clear All - Click to deselect all categories within the group.

To save changes on the page, click **OK**. To discard changes, click **Cancel**.

V-2-5 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

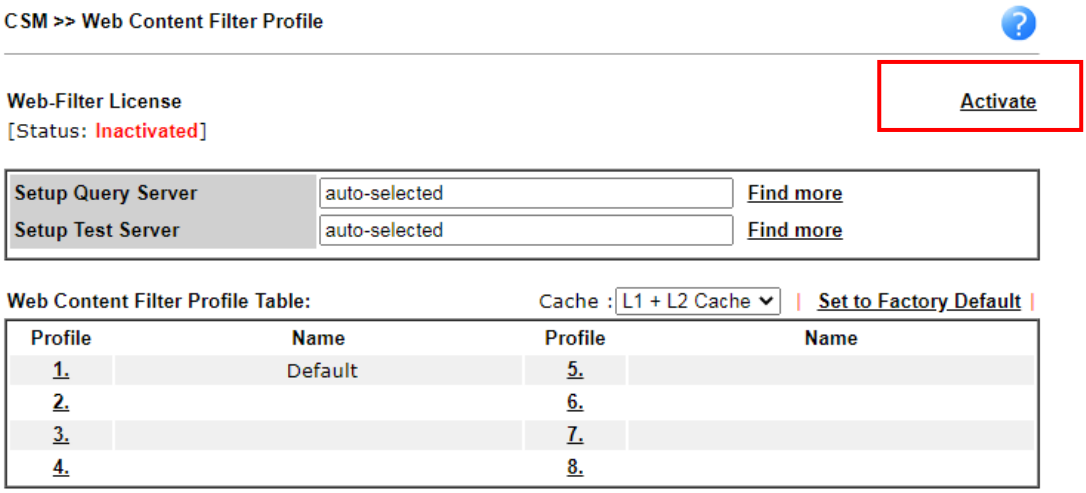
A-1 How to Create an Account for MyVigor

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.

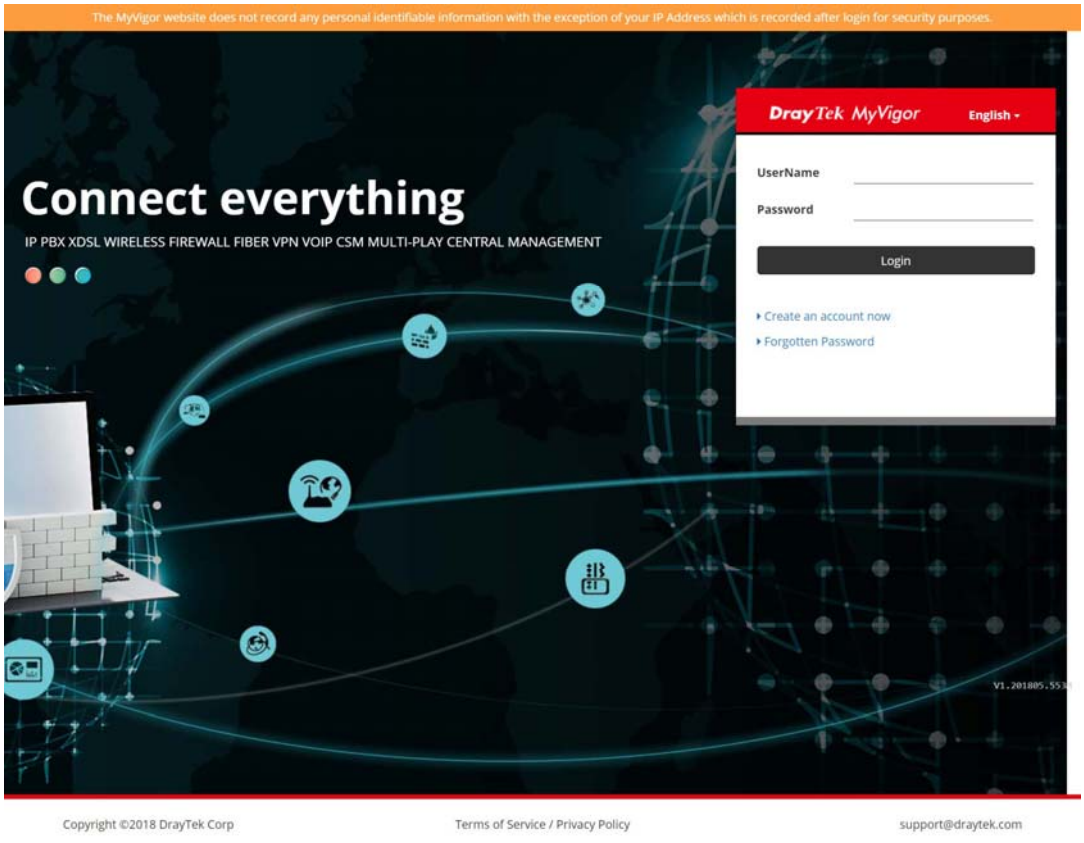
To access into MyVigor for getting more information, please create an account for MyVigor.

Create an Account via Vigor Router

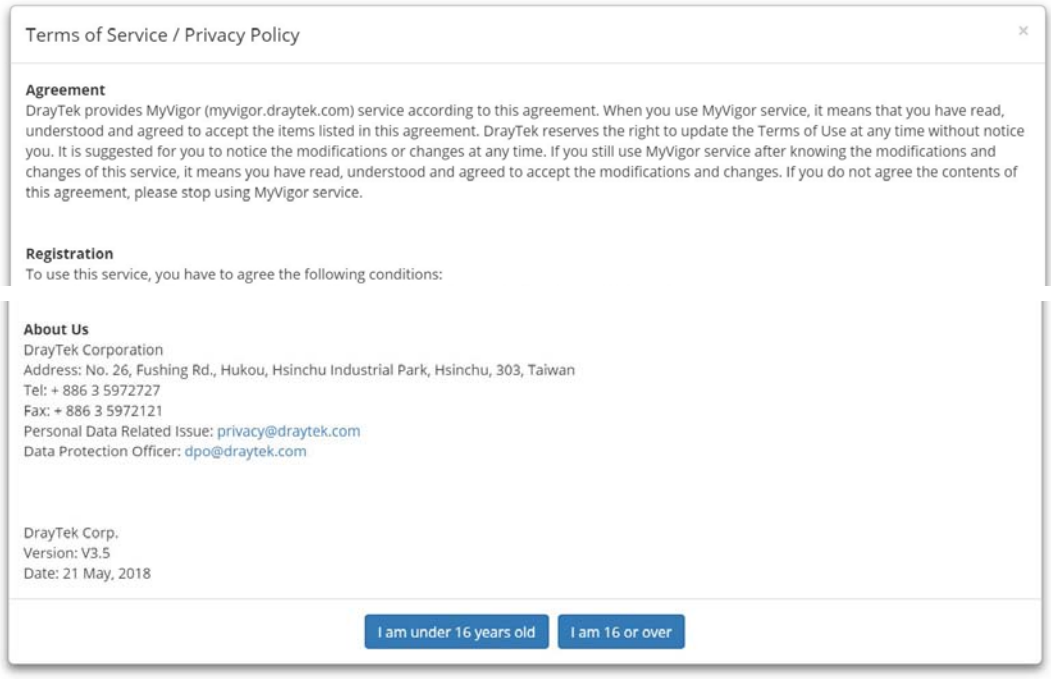
1. Click **CSM>> Web Content Filter Profile**. The following page will appear.



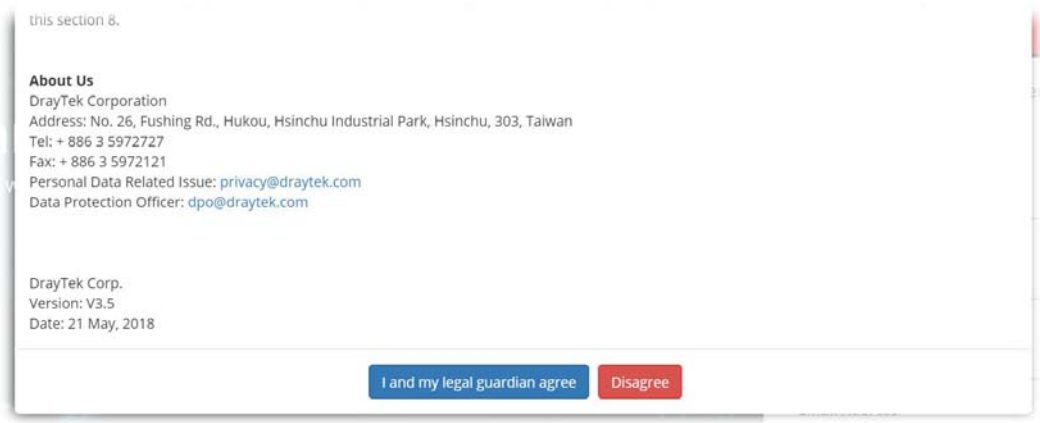
2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.



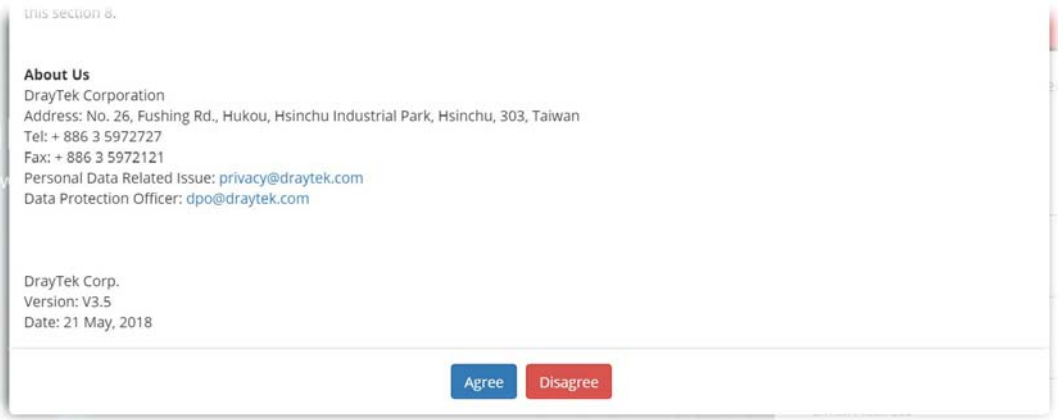
3. Click the link of **Create an account now**.
4. The system will ask if you are 16 years old or over.
   - If yes, click **I am 16 or over**.



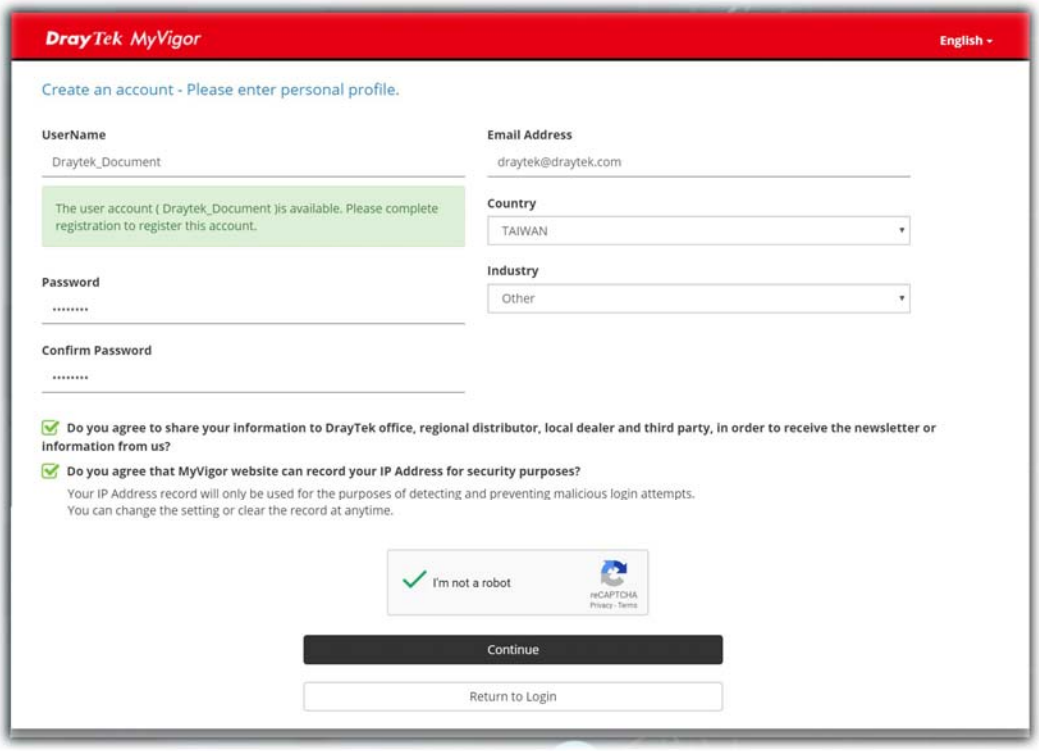
   - If not, click **I am under 16 years old** to get the following page. Then, click **I and my legal guardian agree**.



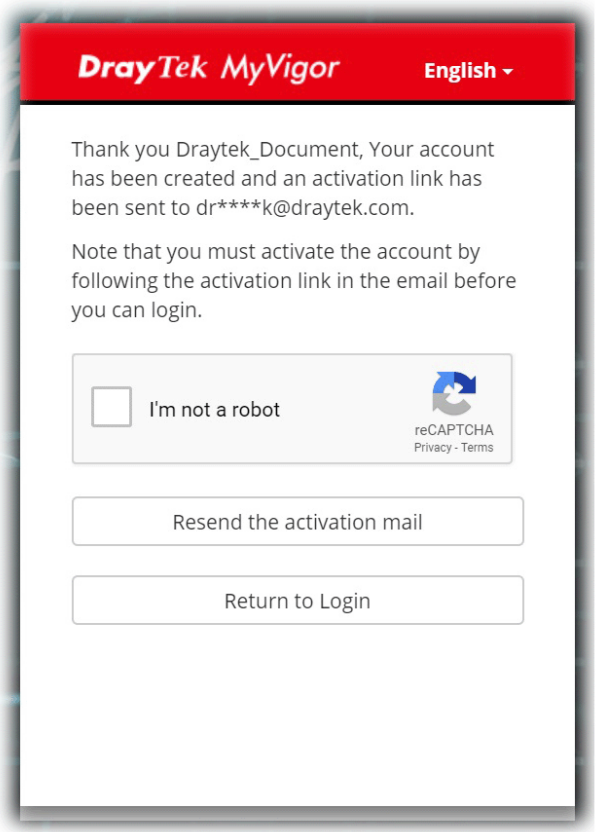
5. After reading the terms of service/privacy policy, click **Agree**.



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**.

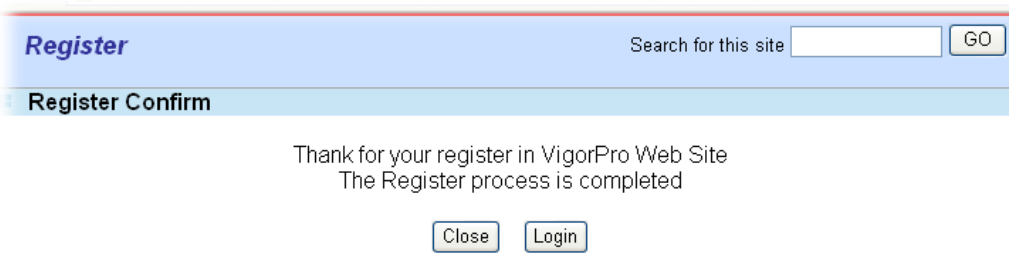
****** This is an automated message from myvigor.draytek.com.******

Thank you (**Mary**) for creating an account.

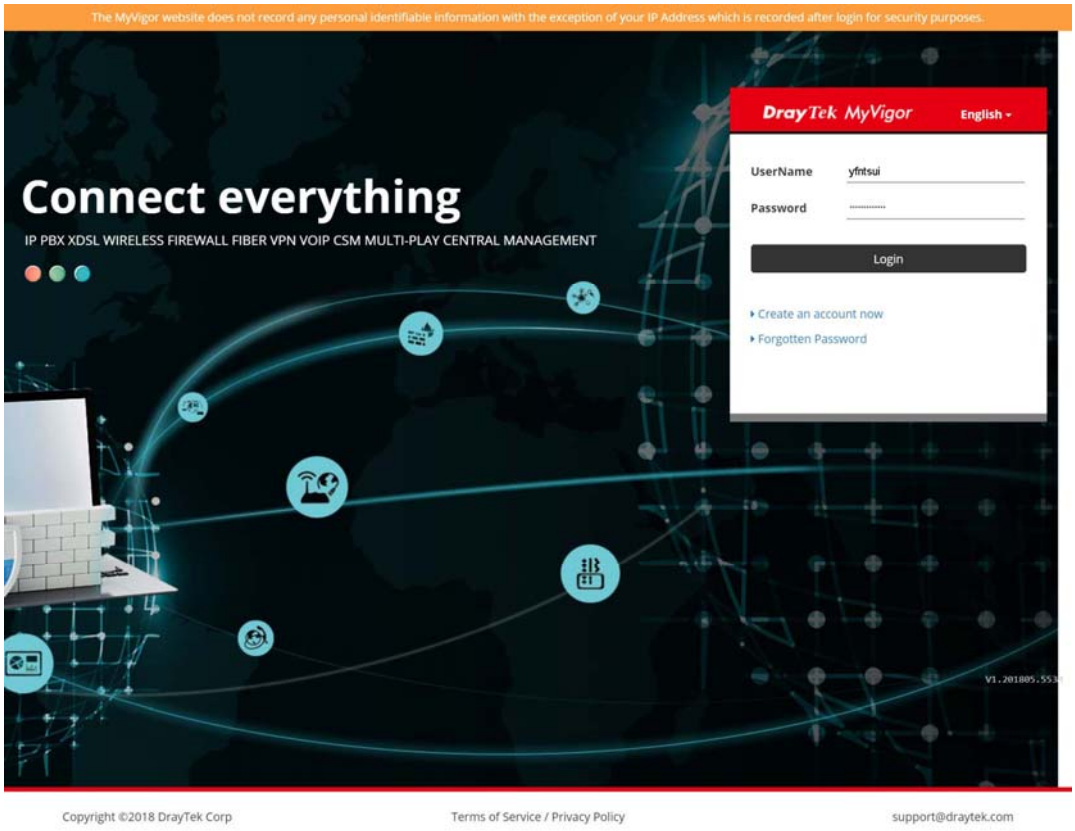
Please click on the activation link below to activate your account

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 Enter 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.

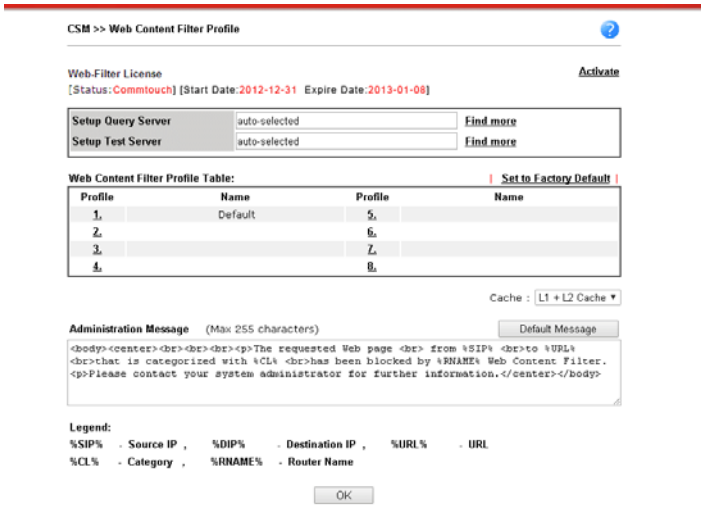
URL Content Filter,

Benefits: Free, flexible for customize webpage.

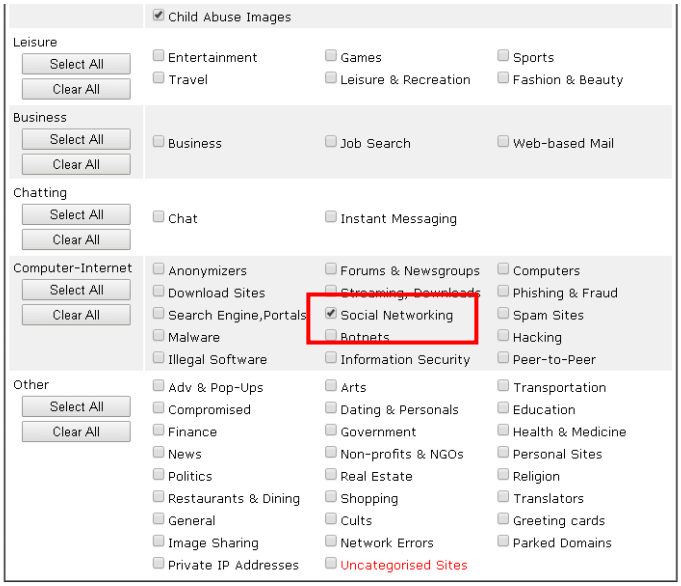
Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

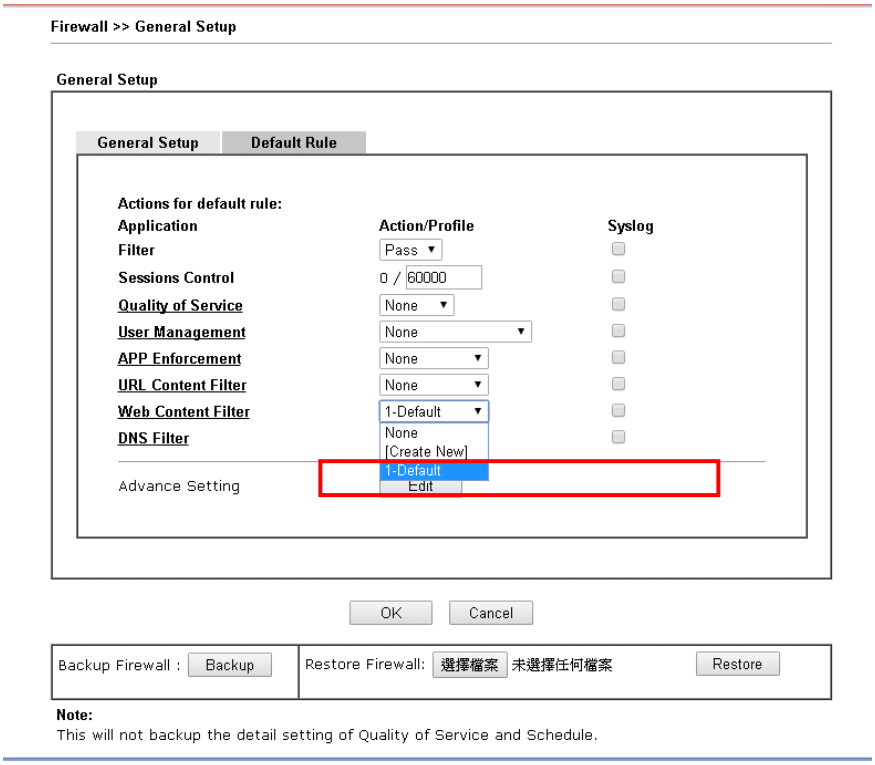
1. Make sure the Web Content Filter license is valid.



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**.

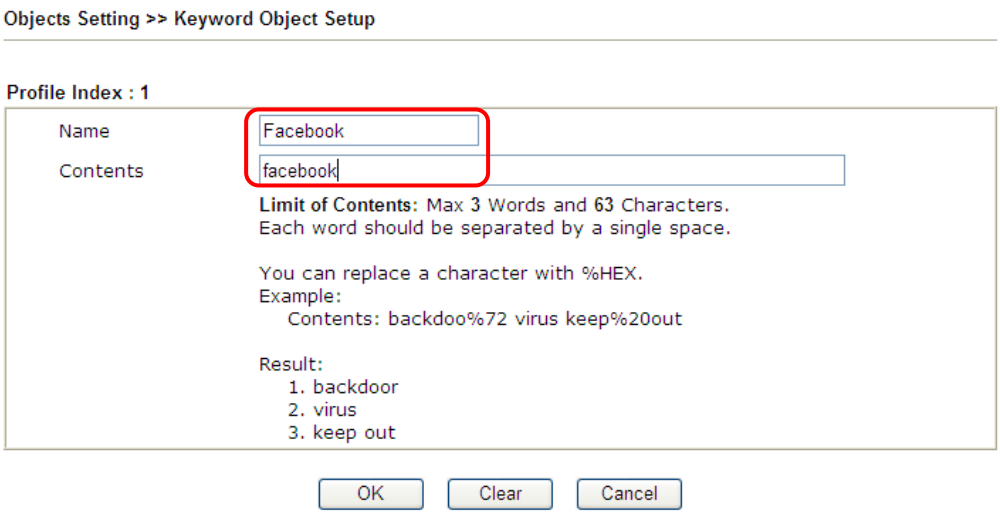


4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

II. Via URL Content Filter

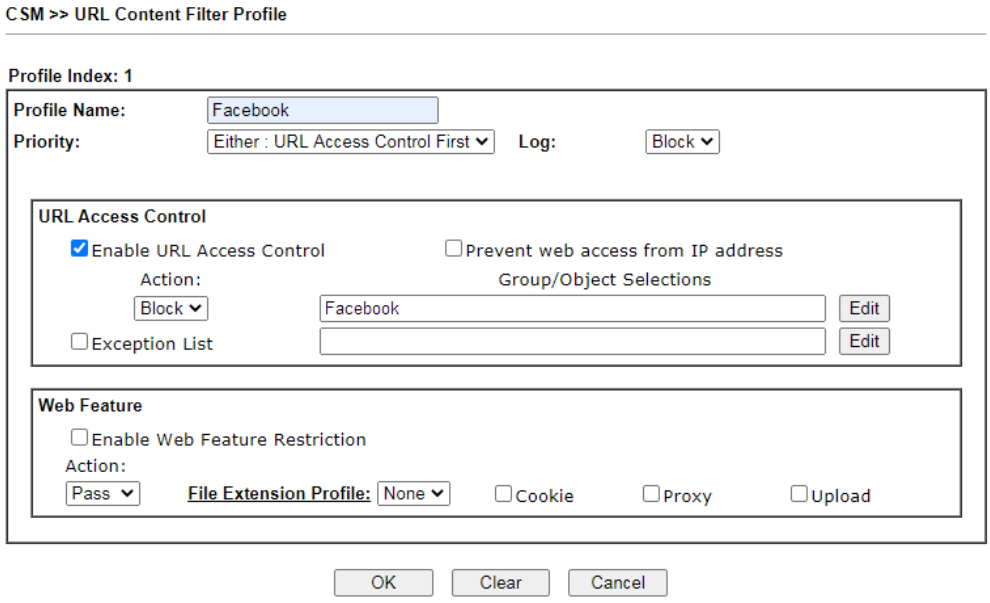
A. Block the web page containing the word of "Facebook"

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.



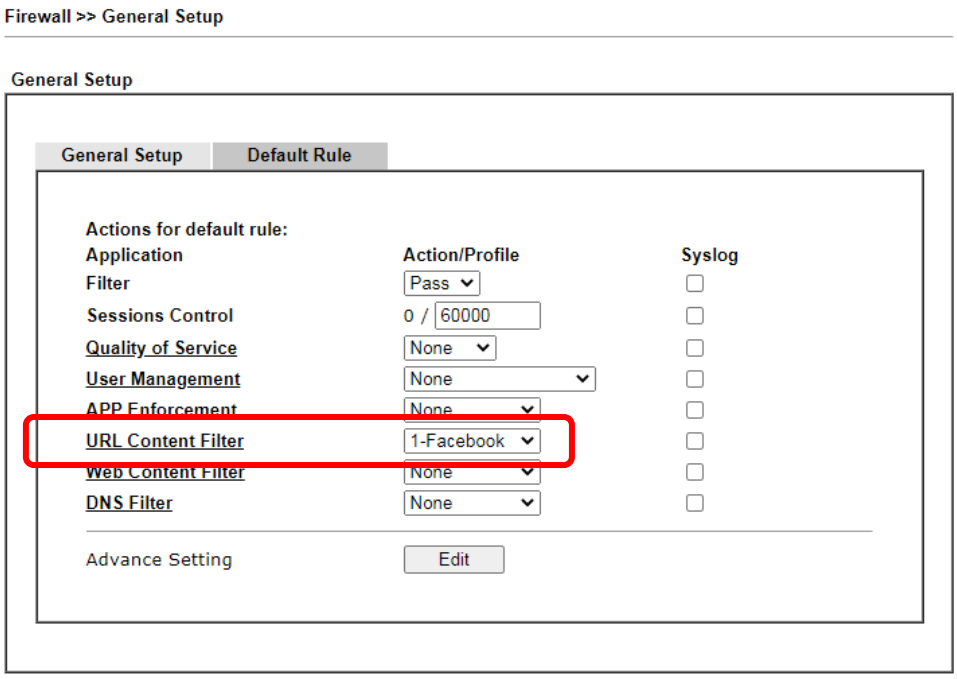
3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.



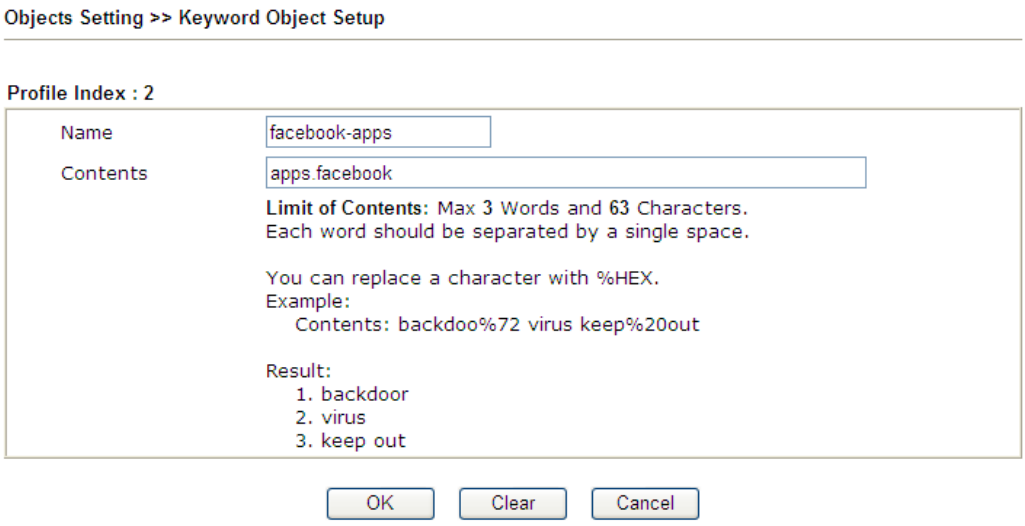
5. When you finished the above steps, click **OK**. Then, open **Firewall>>General Setup**.

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.



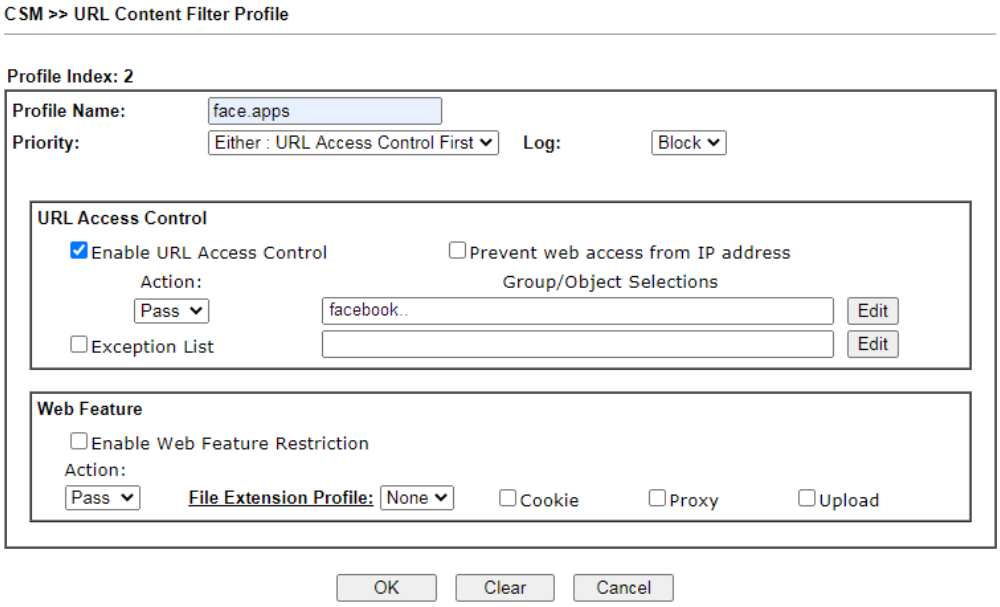
B. Disallow users to play games on Facebook

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.



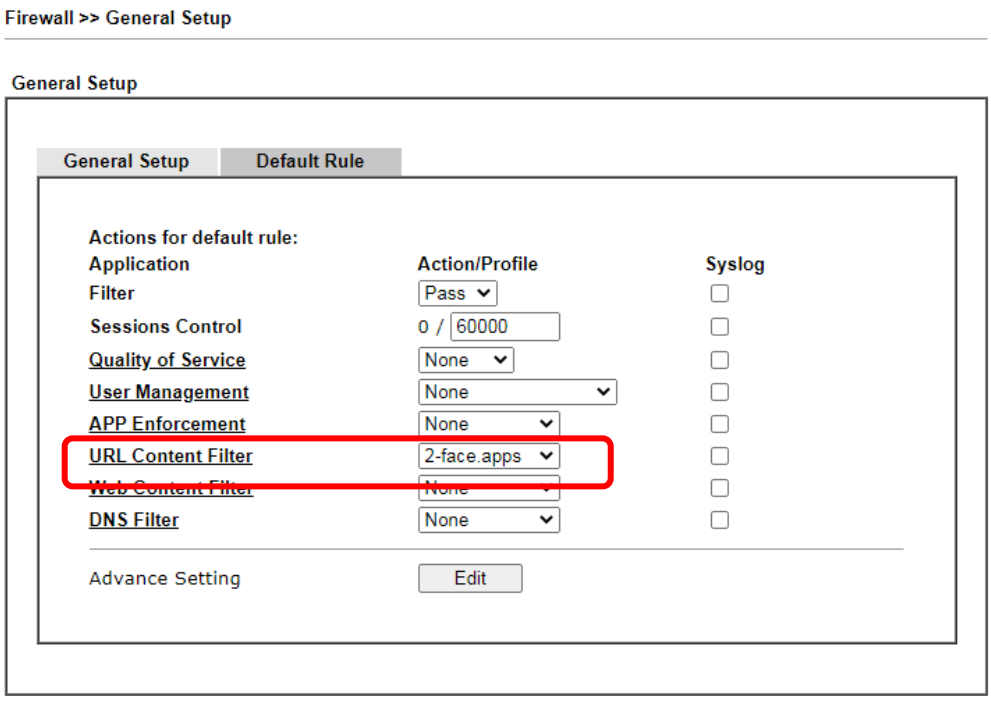
3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

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.



Part VI Management

System Maintenance

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, 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).

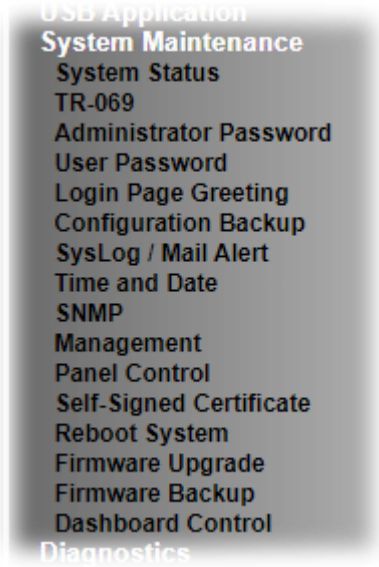
User Management

It is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password.

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, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade, Firmware Backup and Dashboard Control.

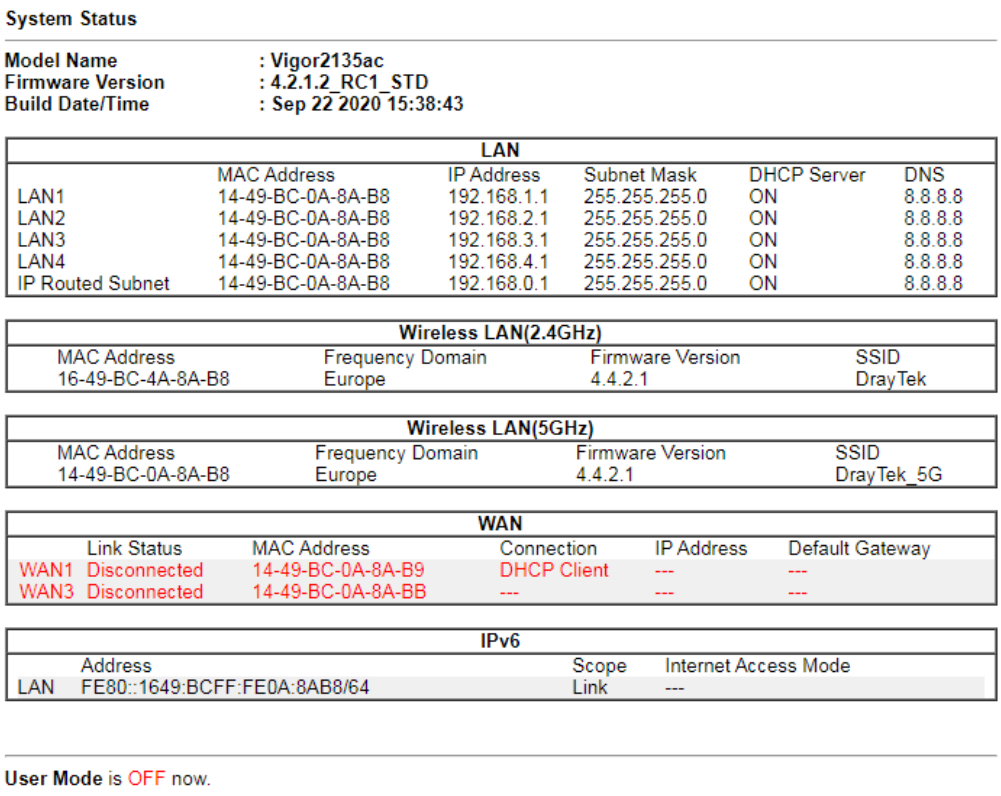
Below shows the menu items for System Maintenance.



Web User Interface

VI-1-1 System Status

The **System Status** displays basic network information of Vigor router including LAN and WAN interface status. Also available is the current firmware version and firmware related information.



System Status

Model Name : **Vigor2135ac**
Firmware Version : **4.2.1.2_RC1_STD**
Build Date/Time : **Sep 22 2020 15:38:43**

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	14-49-BC-0A-8A-B8	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	14-49-BC-0A-8A-B8	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	14-49-BC-0A-8A-B8	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	14-49-BC-0A-8A-B8	192.168.4.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	14-49-BC-0A-8A-B8	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN(2.4GHz)

MAC Address	Frequency Domain	Firmware Version	SSID
16-49-BC-4A-8A-B8	Europe	4.4.2.1	DrayTek

Wireless LAN(5GHz)

MAC Address	Frequency Domain	Firmware Version	SSID
14-49-BC-0A-8A-B8	Europe	4.4.2.1	DrayTek_5G

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	14-49-BC-0A-8A-B9	DHCP Client	---	---
WAN3	Disconnected	14-49-BC-0A-8A-BB	---	---	---

IPv6

	Address	Scope	Internet Access Mode
LAN	FE80::1649:BCFF:FE0A:8AB8/64	Link	---

User Mode is OFF now.

Available settings are explained as follows:

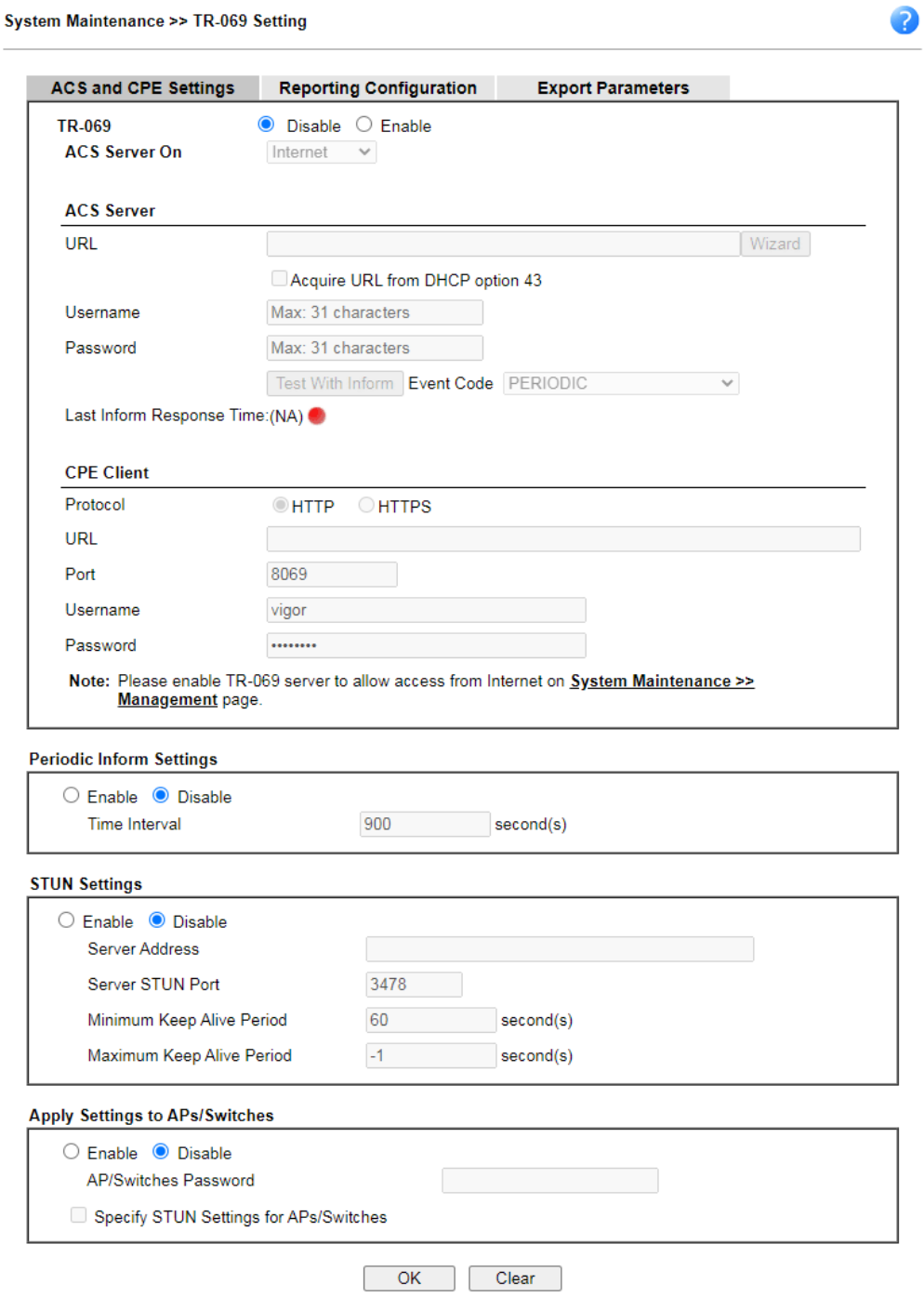
Item	Description
Model Name	Displays the model name of the router.
Firmware Version	Displays the firmware version of the router.
Build Date/Time	Displays the date and time of the current firmware build.
LAN	**MAC Address** **-** Displays the MAC address of the LAN Interface. **IP Address** **-** Displays the IP address of the LAN interface. **Subnet Mask** **-** Displays the subnet mask address of the LAN interface. **DHCP Server** **-** Displays the current status of DHCP server of the LAN interface. **DNS** **-** Displays the assigned IP address of the primary DNS.

WAN	**Link Status** **-** Displays current connection status of the WAN interface. **MAC Address** **-** Displays the MAC address of the WAN Interface. **Connection** **-** Displays the connection type of the WAN interface.. **IP Address** **-** Displays the IP address of the WAN interface. **Default Gateway** **-** Displays the assigned IP address of the default gateway.
IPv6	**Address -** Displays the IPv6 address for LAN. **Scope -** Displays the scope of IPv6 address. For example, **IPv6 Link Local** is non-routable and can only be used for local connections. **Internet Access Mode –** Displays the connection mode of the WAN interface.

VI-1-2 TR-069

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

VI-1-2-1 ACS and CPE Settings



Available settings are explained as follows:

Item	Description
TR-069	Enables or disables TR-069 functionality.

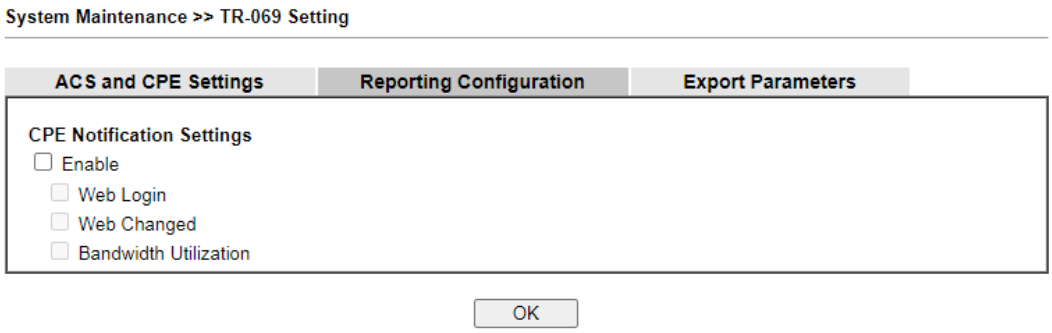
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server.
ACS Server	This section specifies the settings of the ACS Server. **URL –** Enter the URL for connecting to the ACS. Please refer to the Auto Configuration Server user's manual for detailed information. ● **Wizard** – Click it to enter the IP address of VigorACS server, port number and the handler. ● **Acquire URL form DHCP option 43** – Select to acquire the ACS URL from DHCP option 43. **Username/Password –** Enter the credentials required to connect to the ACS server. ● **Test With Inform** – Click to send an inform message using the selected Event Code to test if the CPE is able to communicate with the VigorACS server. ● **Event Code** – Select an event for the inform test. **Last Inform Response Time** – Displays the time of the most recent Inform Response message received from the VigorACS.
CPE Client	This section specifies the settings of the CPE Client. **Http / Https** – Select Https if the connection is encrypted; otherwise select Http. **Port** – In the event of port conflicts, change the port number of the CPE. **Username** and **Password** – Enter the username and password that the VigorACS will use to connect to the CPE.
Periodic Inform Settings	**Enable** – The default setting is Enable, which means the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field. ● **Time Interval** - Set interval time or schedule time for the router to send notification to CPE. **Disable** - Select **Disable** to turn off periodic notifications.
STUN Settings	STUN allows the ACS Server to connect to the CPE Client even when the client is behind a network address translator (NAT). **Disable** - The default setting is Disable. **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 periodically transmit binding requests to the server for the purpose of maintaining the binding with the Gateway. Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server. 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 with the Gateway. Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server. A

	value of -1 indicates that no maximum period is specified.
Apply Settings to APs/Switches	This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2135 at the same time. **Disable** – TR-069 and Related settings will not be applied to VigorAPs. **Enable** – TR-069 settings will be applied to VigorAPs after clicking **OK**. The VigorAP password must be specified. ● **AP Password** – Enter the password of the VigorAP that you want to apply Vigor2135's TR-069 settings. **Specify STUN Settings for APs/Switches** – After clicking the **Enable** radio button for Apply Settings to APs, if you want to apply specific STUN settings (i.e., different from the Vigor2135 STUN settings) to VigorAPs to meet specific requirements, check this box and enter the server IP address, server port, and minimum and maxmum keep alive periods respectively.

Select **OK** to save changes on the page, or **Clear** to reset all settings to factory defaults.

VI-1-2-2 Reporting Configuration

Information related to the router's health are divided into several categories and listed in this field. After checking the item(s), Vigor router will arrange and send corresponding data to VigorACS as a reference for the system administrator.



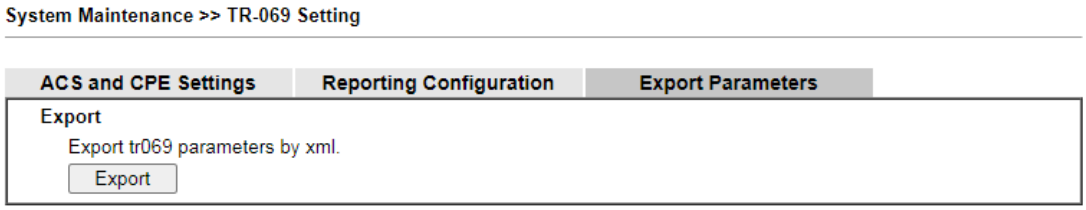
Available settings are explained as follows:

Item	Description
CPE Notification Settings	**Enable** - Check the box to select the notification item(s). Vigor router will send the utilization status to VigorACS.

Click **OK** to save changes on the page.

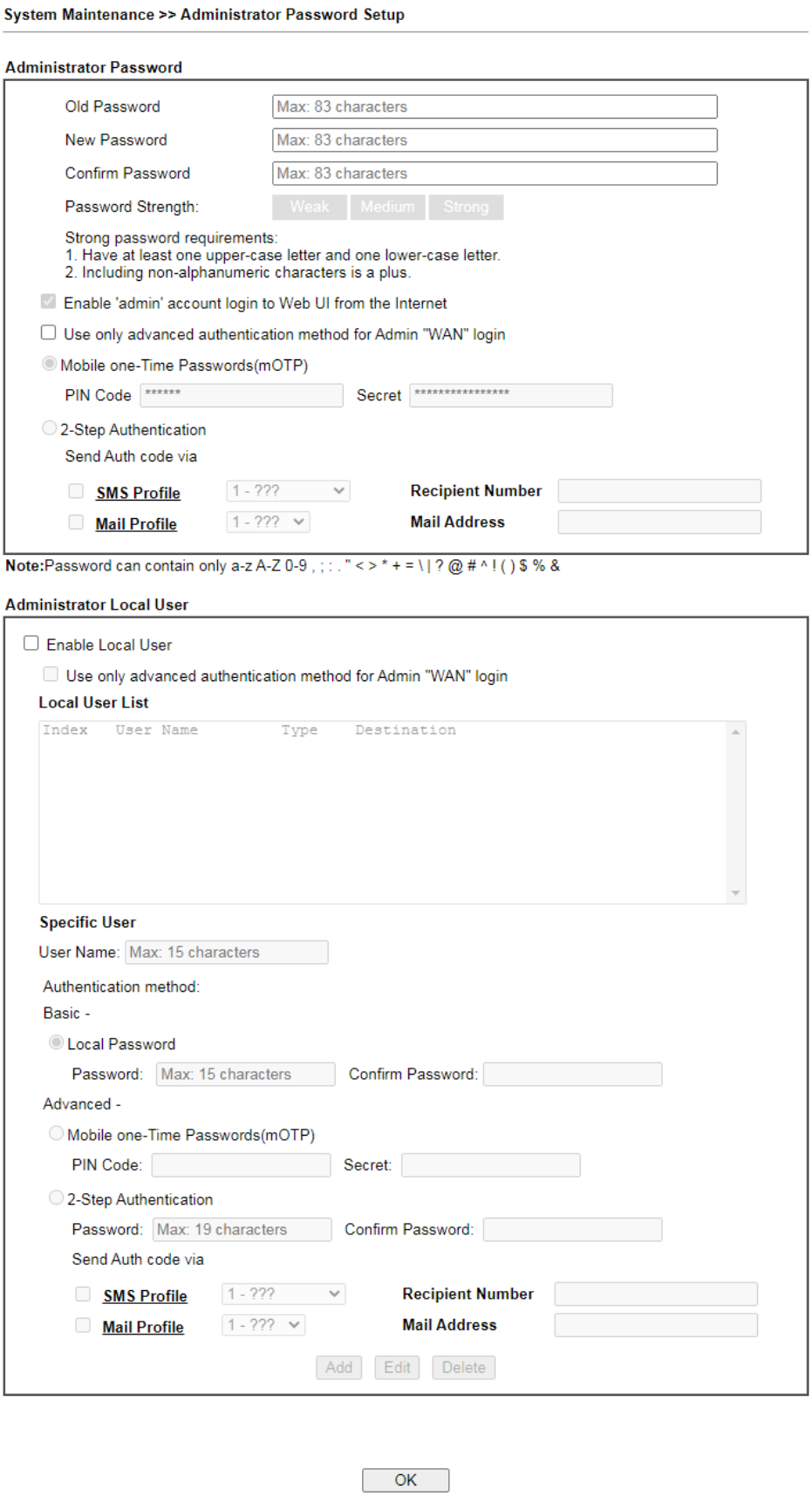
VI-1-2-3 Export Parameters

Click **Export** to save the TR-069 parameter settings as an ".xml".



VI-1-3 Administrator Password

This page allows you to set or change the administrator password.



Available settings are explained as follows:

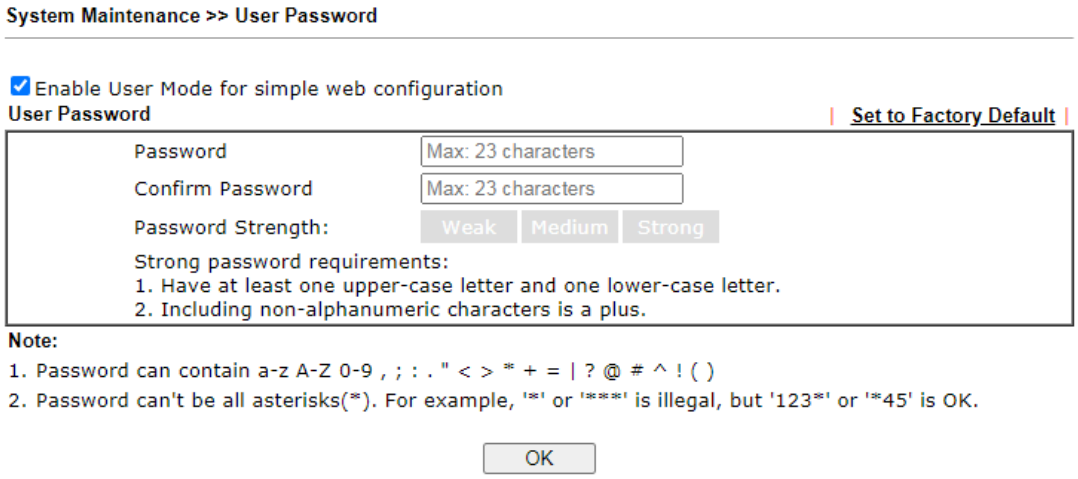
Item	Description
Administrator Password	The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. **Old Password** - Enter the current password. The factory default is "admin". **New Password** – Enter the new password. The maximum length of the password is 23 characters. **Confirm Password** – Enter the new password again for confirmation. **Enable 'admin' account login to Web UI from the Internet** – Select to allow the administrator to log in from the Internet. This option is enabled when Administrator Local User is enabled (see below). **Use only advanced authentication method for Admin "WAN" login** – Advanced authentication method can offer a **more secure** network connection. Select to require mOTP or 2-step authentication when logging in from the WAN. ● **Mobile one-Time Password (mOTP)** – Select to allow the use of mOTP passwords. Enter the PIN Code and Secret settings for getting one-time passwords. ● **2-Step Auth code via SMS Profile and/or Mail Profile –** Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password.
Administrator Local User	Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router. This feature allows you to add more administrators who can then log in to the web interface, with the same privileges as the administrator. **Enable Local User** – Check the box to allow other users to administer the router. ● **Use only advanced authentication method for Admin "WAN" login** – Advanced authentication method can offer a **more secure** network connection. In general, the above basic password setting will be used for authentication if such option is disabled. Simply check the box to enable the following settings. ● **Local User List** – Shows all the users that are set up to administer the router. ● **Specific User –** Create the new user account as the local user. Then specify the authentication method (dividing into Basic and Advanced) for the user account. ➢ **User Name** – Enter a user name. ● **Authentication method –** Select from **Basic** or **Advanced** authentication methods. **Basic** – Static passwords will be used to authenticate users. ➢ **Local Password** – Enter the password for the local user. **Advanced** - Mobile One-time Passwords (mOTP) or

	2-step authentication will be used to authenticate users. ➢ **Mobile one-Time Password (mOTP)** – Select to allow the use of mOTP passwords. Enter the mOTP PIN Code and Secret that will be used to generate the one-time passwords. ➢ **2-Step Authentication via SMS Profile and/or Mail Profile –** Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password. ● **Add** – After entering the user name and password above, click this button to create a new local user. The new user will be shown on the Local User List immediately. ● **Edit** – If you wish to change a user in the Local User List, select it, perform the necessary modifications, and click this button to update the user. ● **Delete** – If you wish to delete a user in the Local User List, select it and click this button to remove it.

Click **OK** to save changes on the page, and you will be directed to the login screen. Please log in with the new password.

VI-1-4 User Password

This page allows you to set new password for user operation.



Available settings are explained as follows:

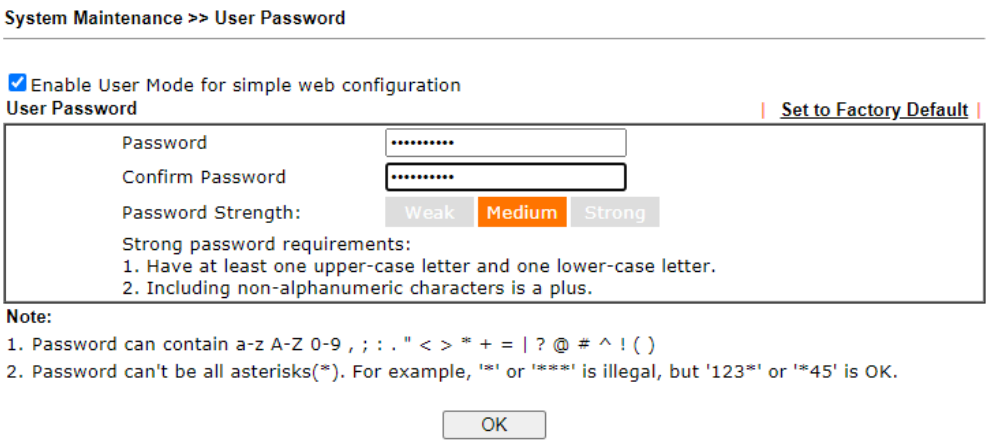
Item	Description
Enable User Mode for simple web configuration	Check this box to enable User Mode for web user interface with the password typed here for simple web configuration. The simple web user interface settings differ from those on the full web user interface seen when logged in using the administrator password.
Password	Enter the password. The maximum length of the password is 31 characters.
Confirm Password	Enter the password again for verification.
Password Strength	Shows the security strength of the password specified above.
Set to Factory Default	Click to return to the factory default setting.

Click **OK** to save changes on the page, and you will be directed to the login screen. Please window will appear. Please log in with the new password.

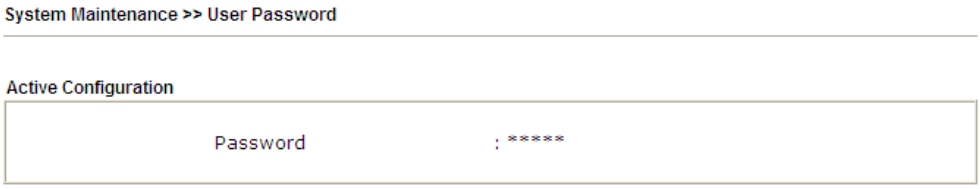
Here are the steps involved in setting up the router for User Mode Access:

1. Navigate to **System Maintenance>>User Password** in the web user interface.

2. Check the box of **Enable User Mode for simple web configuratio**n to enable user mode operation. Enter a new password in the Password field and click OK.



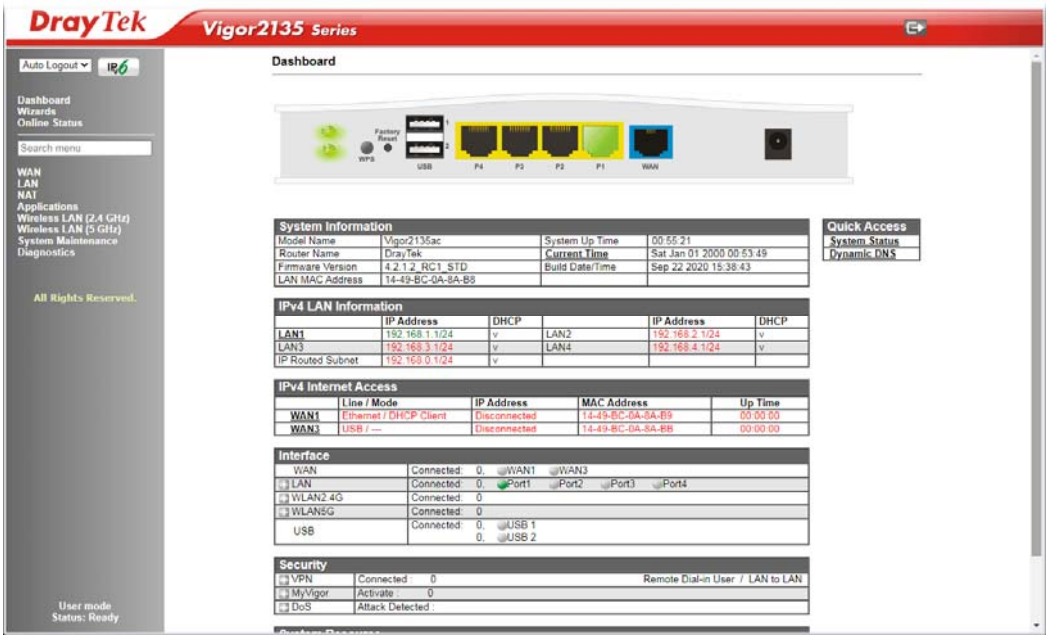
3. The following screen will appear. Click **OK**.



4. Log out the Vigor router web user interface by clicking the Logout button.

5. The following window will be shown. Enter the new user password in the **Password** field and click **Login**.

6. The main screen with User Mode will be shown:



Only basic settings are available in User Mode. These are a subset of the Admin Mode settings.

Info	Setting in User Mode can be configured as same as in Admin Mode.

VI-1-5 Login Page Greeting

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.

This section allows you to customize the login page by adding a message and/or setting the page title.

Available settings are explained as follows:

Item	Description
Login Page Logo	Set an image which will be shown above the log in window. **Default -** The **Enable Greeting** feature is available to set the login page title. **Blank -** No image / no greeting. **Upload a file -** Choose an image file and click Upload. Later the selected image will be shown on the log in window.
Enable Greeting	Check this box to enable the login customization function.
Login Page Title	Enter a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Enter words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not enter URL redirect link here.
Preview	Click to preview the customized login window based on the settings entered on this page.

Set to Factory Default	Click to return to the factory default setting.

Below shows an example of a customized login page with the values entered in the **Login Page Title** and **Welcome Message and Bulletin** fields.

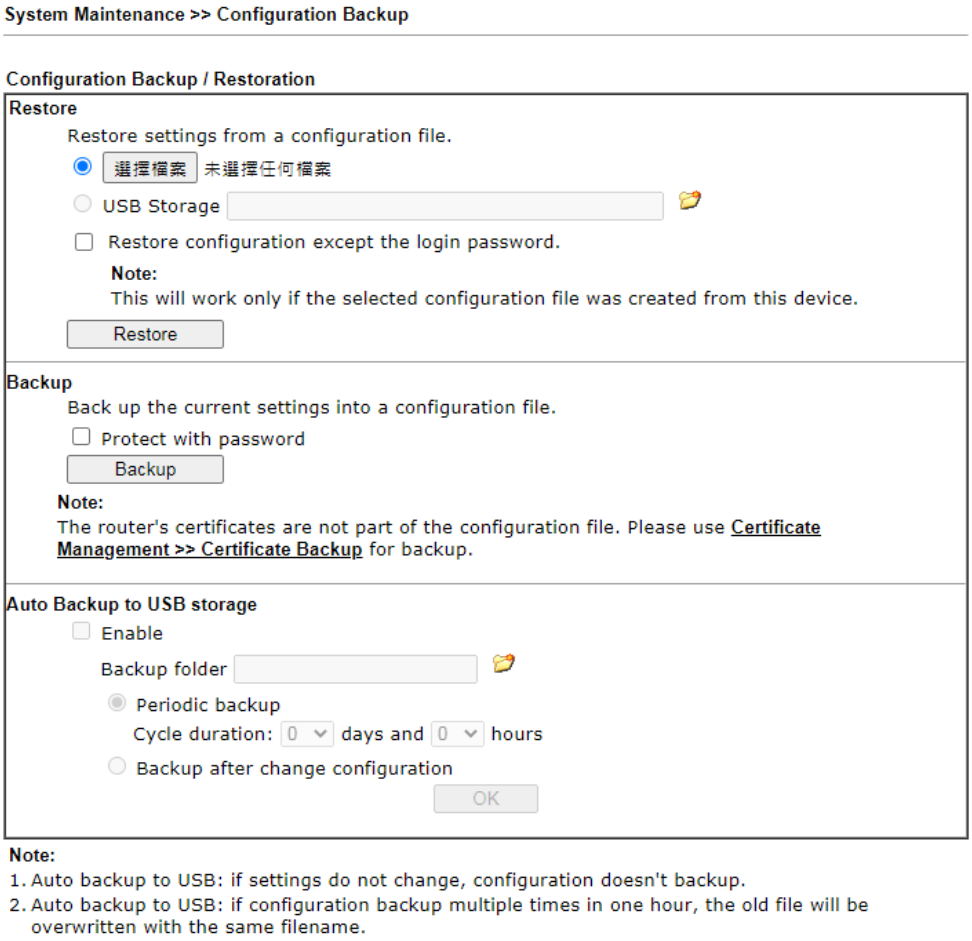
VI-1-6 Configuration Backup

This function allows the backup and restoration of router settings. In addition to restoring Vigor2135's own configuration backup, it is possible to restore backups from certain DrayTek routers such as Vigor2820, Vigor2830 and Vigor2850 series on the Vigor2135.

Backing up the Configuration

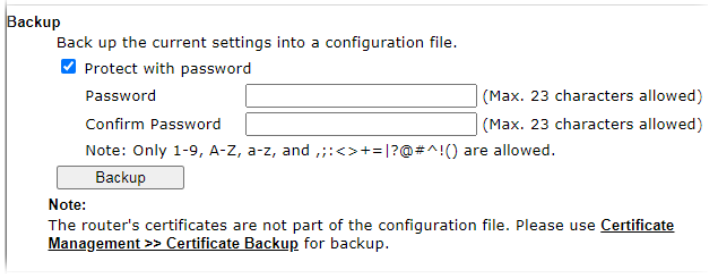
Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following page will be shown.

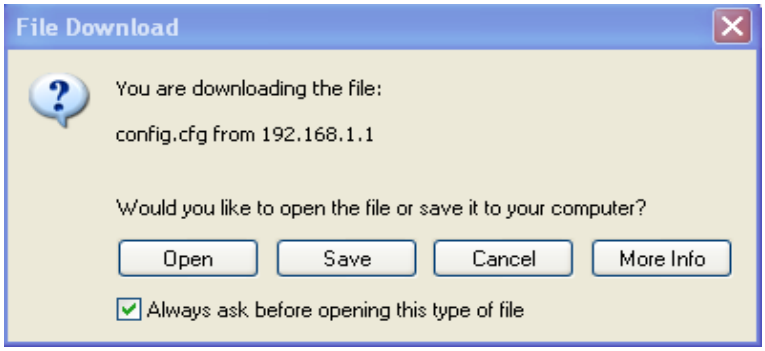


Available settings are explained as follows:

Item	Description
Restore	**Restore settings from a configuration file** – Click the **Select File** button to specify a file to be restored or click **USB Storage** (if a USB storage disk connected) to choose the configuration file. **Restore configuration except the login password** – Select to exclude the password from getting restored from the backup. **Restore** - Click to initiate restoration of configuration. If the backup file is encrypted, you will be asked to enter the password.
Backup	Click it to perform the configuration backup of this router.

	Protect with password- Select to encrypt the backup with a password. You will be prompted to enter the password as shown below:  ● **Password** – Enter a new password for encrypting the configuration file. ● **Confirm Password** – Enter the new password again for confirmation. **Backup** - Click to initiate the backup process.
Auto Backup to USB storage	The configuration can be stored to a USB connecting to Vigor router as a backup. **Enable** - Check the box to enable the function. **Backup folder** – Set the path for downloading. **Periodic backup** – Set the circle duration for backup. **Backup after change configuration** – Backup will be executed whenever the configuration is changed.

2. Click the **Backup** button, and the File Download dialog will be shown. Depending on your browser, you may be prompted to select a location to save the file, or the file may be saved in the default download location of your browser.



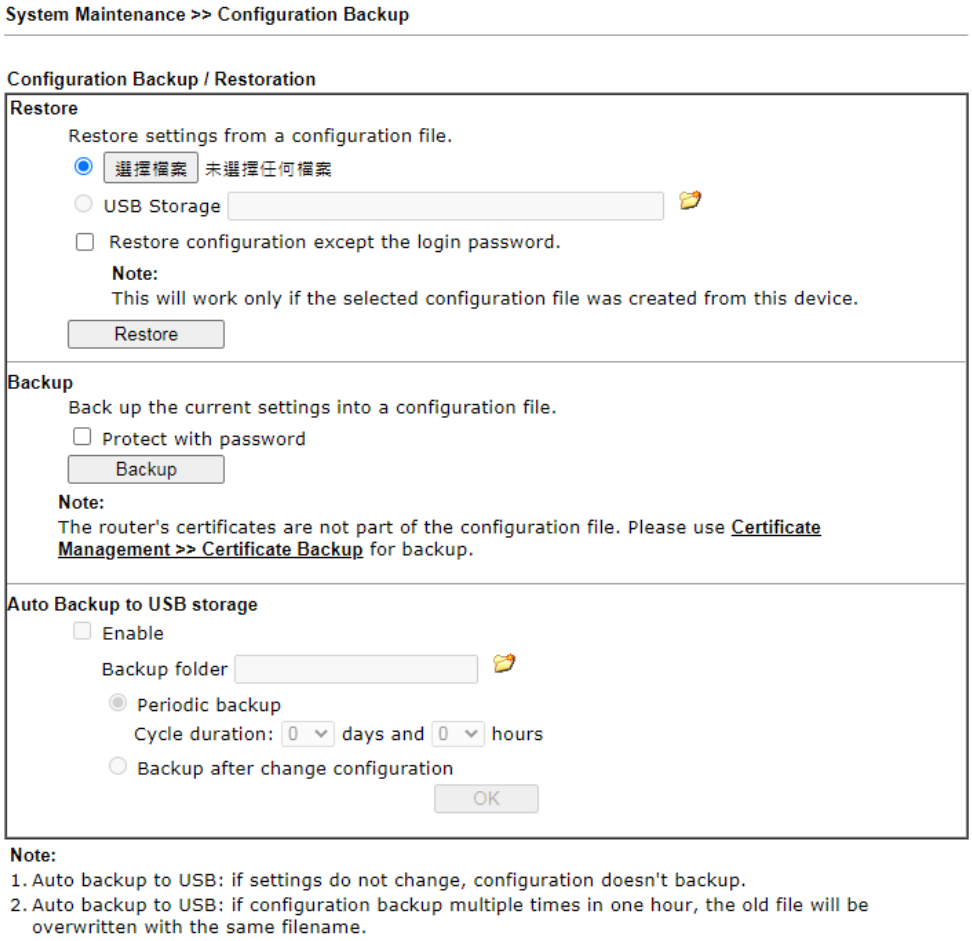
The configuration will download automatically to your computer as a file named **config.cfg**.

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	Configuration Backup does not include certificates stored on the router. Please back up certificates separately by going to Certificate Management >> Certificate Backup.

Restoring the Configuration

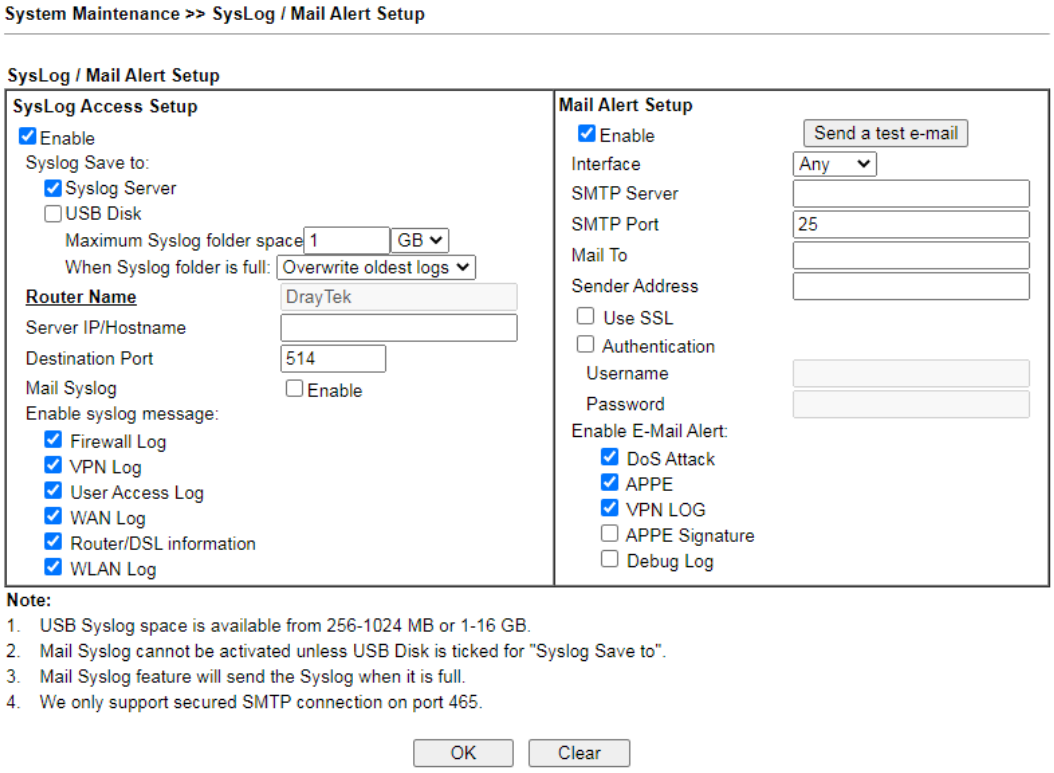
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be shown.



2. Click the **Choose File** button under **Backup** to bring up the open file dialog box to select the configuration file to be uploaded and restored.
3. Click the **Restore** button and wait for few seconds.

VI-1-7 Syslog/Mail Alert

SysLog function is provided for users to monitor router.



Available settings are explained as follows:

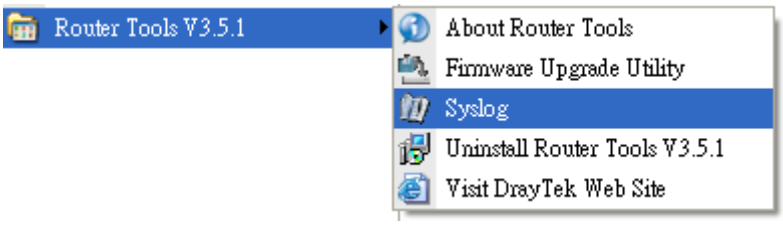
Item	Description
SysLog Access Setup	**Enable** - Select to enable the Syslog function. **Syslog Save to** – Check Syslog Server and / or USB Disk. ● **Syslog Server** – Events will be sent to a Syslog server. ● **USB Disk** – Events will be saved to a USB storage device connected to the router. ● **Maximum Syslog folder space** - Set a space (unit GB/MB) to store event logs. ● **When Syslog folder is full** - Specify the action (overwrite the olderest logs or stop logging) to be executed.
Router Name	Shows the name of the router set in **System Maintenance >> Management**. This name will be used to identify the router in the Syslog entries. To set or modify the router name, click the hyperlink and you will be taken to **System Maintenance >> Management** where you can enter the value. **Server IP Address /Hostname -** Enter the IP address / hostname of the Syslog server. **Destination Port -** Enter the port for the Syslog server.

	Mail Syslog – Select to enable sending Syslog messages by email. **Enable syslog message -** Select the events to be recorded by syslog.
Mail Alert Setup	**Enable** - Select to enable the Mail Alert. **Send a test e-mail -** Click to send a test email message using the settings below. **Interface** - Specify the WAN interface for a mail passing through. **SMTP Server** - Enter the address of the SMTP server used to send email. **SMTP Port -** Enter the port of the SMTP server. Default setting is 25. **Mail To -** Enter the email address of the recipient. **Sender Address -** Enter the email address of the sender. **Use SSL -** Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method. **Authentication -** Select this checkbox and enter the username and password if the SMTP server requires authentication. ● **User Name -** Enter the user name for authentication. ● **Password -** Enter the password for authentication. **Enable E-mail Alert -** Select the event types that will trigger email alerts.

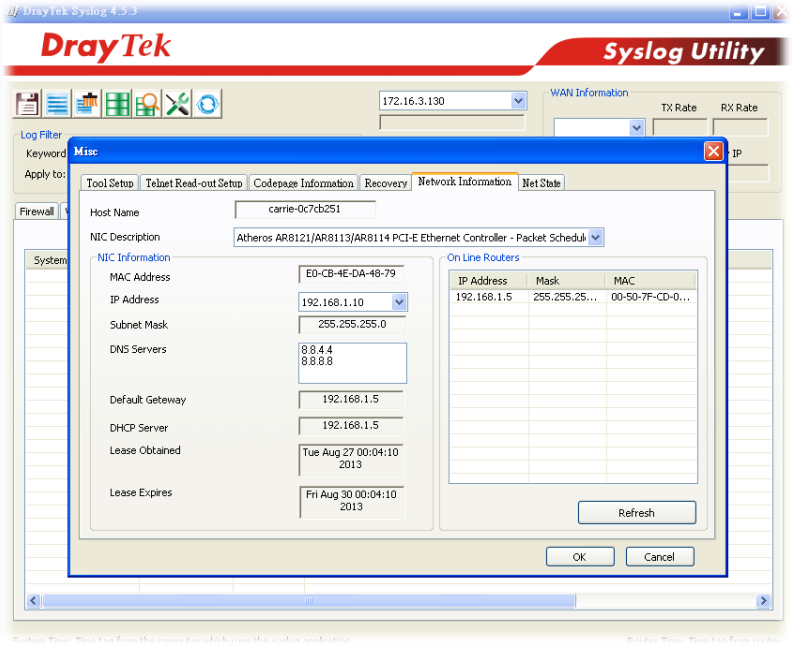
Select **OK** to save changes on the page, or **Clear** to reset all settings to factory defaults.

To view the Syslog message, please follow the steps below:

1. On the **Syslog / Mail Alert Setup** screen, enter the monitor PC's IP address in the **Server IP Address** field.
2. Install the Router Tools from DrayTek web site. After installation, start Syslog by clicking on **Router Tools>>Syslog** in the Windows Start Menu.

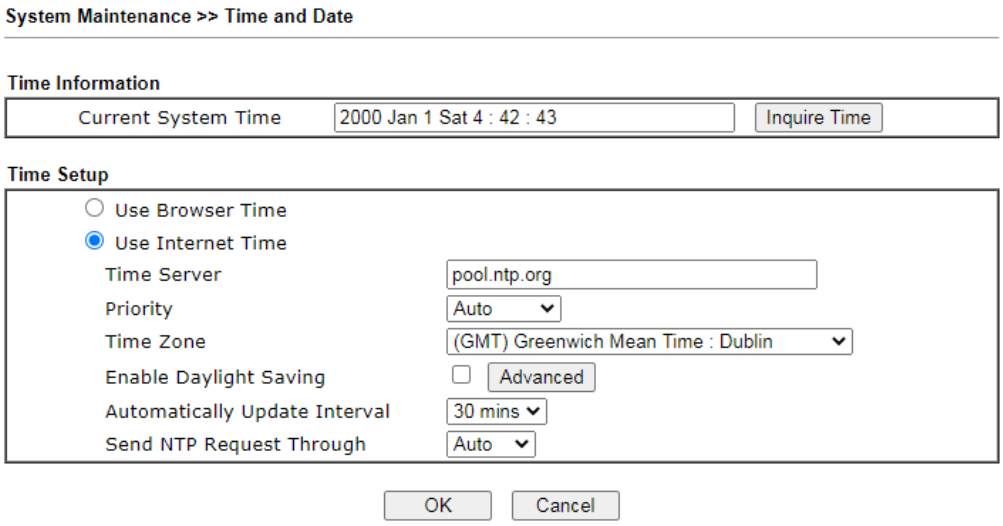


3. In the Syslog application, select the router you wish to monitor. Rember to select the network adapter to be used to connect to the router under Network Information, or else Syslog traffic cannot be received from the router.

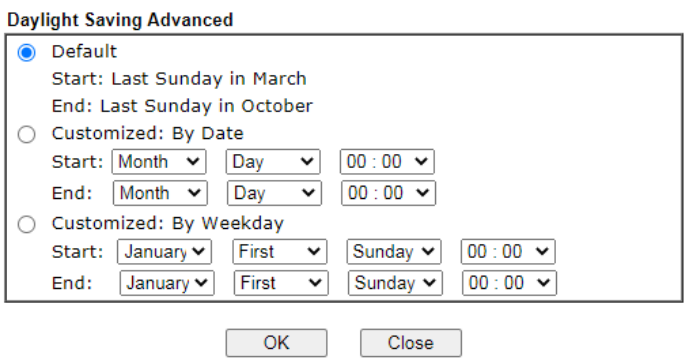


VI-1-8 Time and Date

This section allows you to configure settings related to the system date and time.



Available settings are explained as follows:

Item	Description
Current System Time	Click **Inquire Time** to retrieve the current time from the time server.
Use Browser Time	Select this option to let the router set its system time using the time reported by the web browser.
Use Internet Time	Select this option to let the browser set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP).
Time Server	Enter the address of the time server.
Priority	Select **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 Daylight Saving Time (DST) if it is applicable to your location. **Advanced** – Click to enter a custom schedule to enable DST.  Use the default time setting or set user defined time for your requirement. **Default** – Uses the default DST schedule for the time zone.

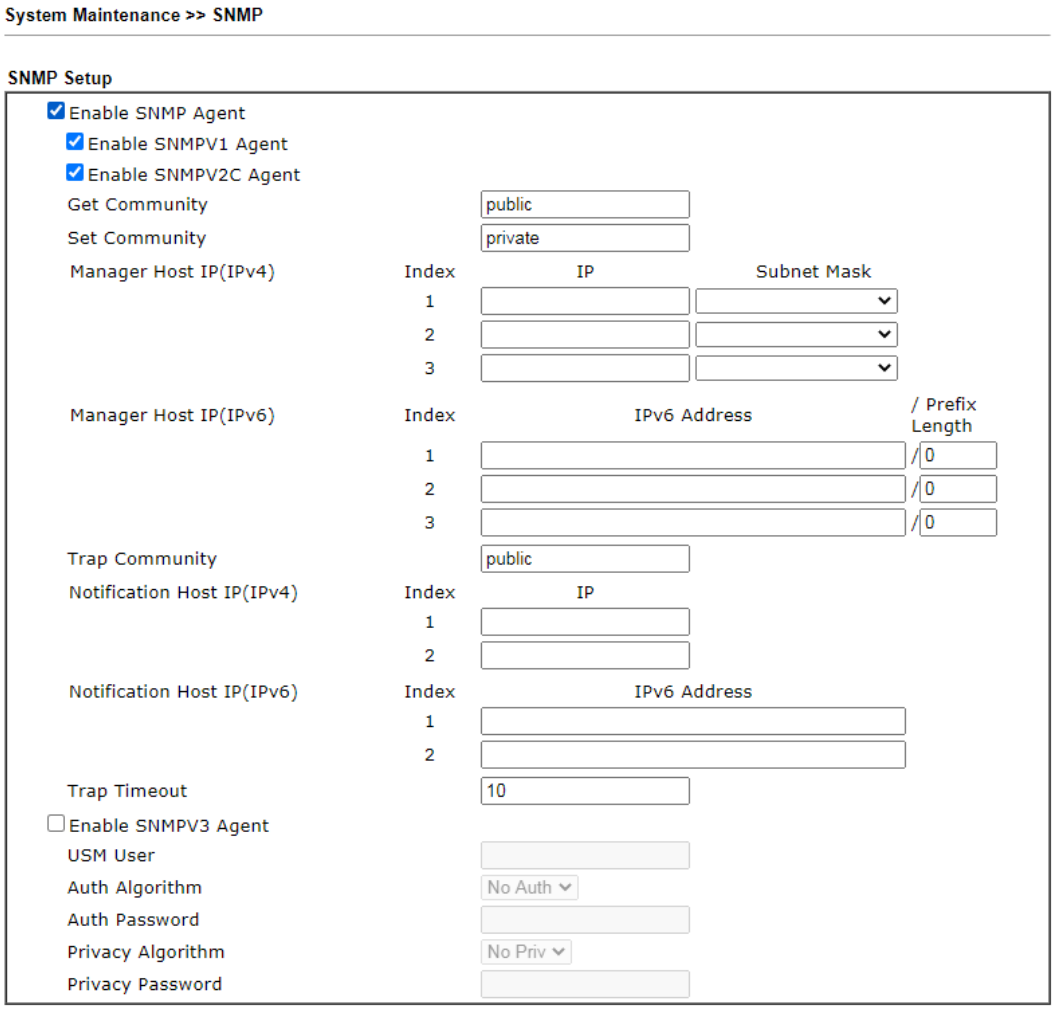
	Date Range – Select this option if DST starts and ends on fixed dates. **Yearly** – Select this option if DST starts and ends on certain days of the week.
Automatically Update Interval	Select the time interval at which the router updates the system time.
Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

VI-1-9 SNMP

This section allows you to configure settings for SNMP and SNMPv3 services.

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



Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check to enable SNMP function. Then, enable SNMPV1 agent/SNMPV2C agent.
Get Community	Enter the Get Community string. The default setting is

	public. Devices that send requests to retrieve information using get commands must pass the correct Get Community string. The maximum allowed length is 23 characters.
Set Community	Enter the Set Community string. The default setting is **private**. Devices that send requests to change settings using set commands must pass the correct Set Community string. The maximum length of the text is 23 characters.
Manager Host IP (IPv4)	Enter the IPv4 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv4 LAN host is allowed to issue SNMP commands.
Manager Host IP (IPv6)	Enter the IPv6 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv6 LAN host is allowed to issue SNMP commands.
Trap Community	Enter the Trap Community string. The default setting is public. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string. The maximum length of the text is 23 characters.
Notification Host IP (IPv4)	Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
Notification Host IP (IPv6)	Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
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.

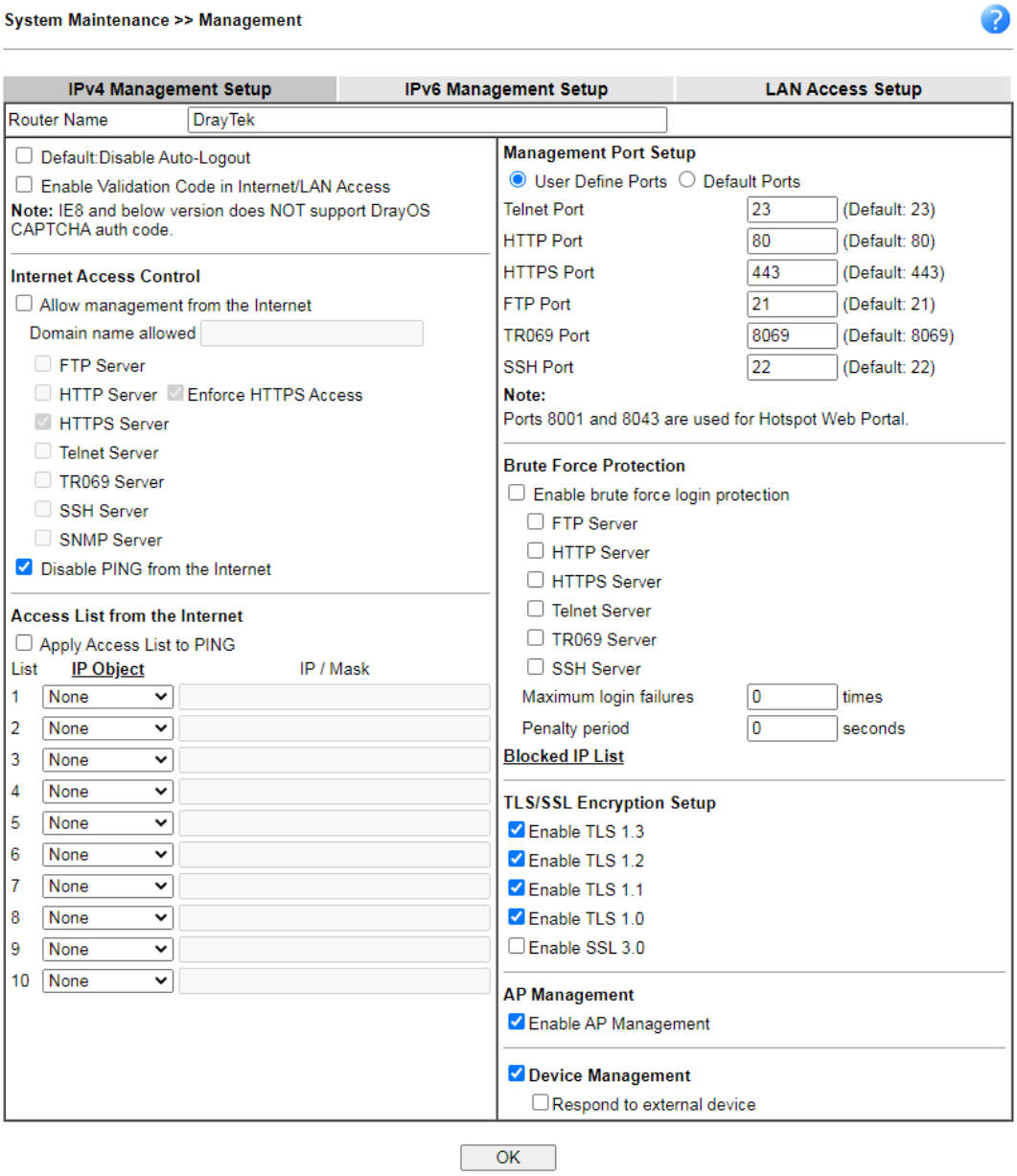
Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

VI-1-10 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.

Management setup for IPv4 and IPv6 are on separate tab pages.

IPv4 Management Setup



Available settings are explained as follows:

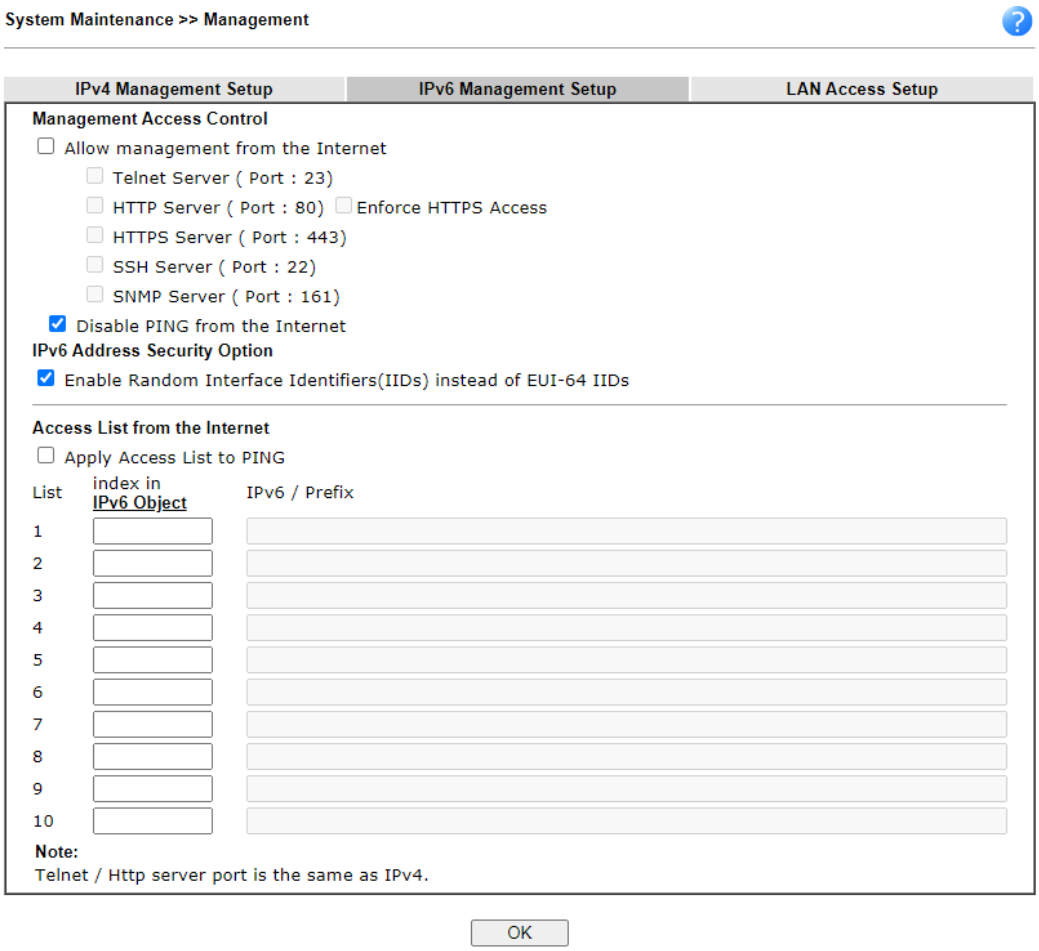
Item	Description
Router Name	Enter the router name as provided by ISP.
Default: Disable Auto-Logout	If enabled, the auto-logout function for web user interface will be disabled.

	 The web user interface will not terminate until you manually click the Logout icon.
Enable Validation Code in Internet/LAN Access	If enabled, Vigor router will require users to enter a validation code as shown in an image when they log in.
Internet Access Control	**Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered. **Domain name allowed** – This setting is only available if DNS filtering is enabled, applying DNS filter profile in firewall rules, or enabling DNS Filter Local Setting. The router will only allow connections to the WebUI using domain addresses configured in either DDNS profiles or this section. If DNS filtering is disabled, this setting will be disabled, and any domain address that resolves to the router's WAN IP address can be used to connect to the WebUI. **Disable PING from the Internet -** Select to reject all PING packets from the Internet. For increased security, this setting 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. **IP Object**- Select a configured IP object. **IP / Mask** - Shows the IP address and/or subnet mask of the selected IP object.
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 –** Select to enable detection of brute force login attempts.

	Maximum login failure – Specify the maximum number of failed login attempts before further login is blocked. **Penalty period –** Set the lockout time after maximum number of login attempts has been exceeded. The user will be unable to attempt to log in until the specified time has passed. **Blocked IP List –** Display, in a new browser window, IP addresses that are currently blocked from logging into the router.
TLS/SSL Encryption Setup	**Enable SSL 3.0/1.0/1.1/1.2/1.3 –** Check the box to enable SSL 3.0/1.0/1.1/1.2/1.3 encryption protocols. For improved security, the HTTPS and SSL VPN servers that are built into the router have been upgraded to TLS 1.x protocol. If you are using an old web browser (eg. IE 6.0) or an old version of the SmartVPN Client, you may need to enable SSL 3.0 to connect to the router. However, it is recommended that you instead upgrade your web browser or SmartVPN client to a version that supports TLS protocols that are far more secure than SSL.
AP Management	**Enable AP Management –** Check to enable the access point management function. If not, menu items related to **Central Management>>AP** will be hidden.
Device Management	Check to enable the device management function. **Respond to external device –** If selected, Vigor2135 will function as a slave device. When an external device (master device) sends packets to the Vigor2135 to attempt to manage it, the Vigor2135 will respond to the request coming from the external device which is able to manage Vigor2135.

Select **OK** to save changes on the page.

IPv6 Management Setup

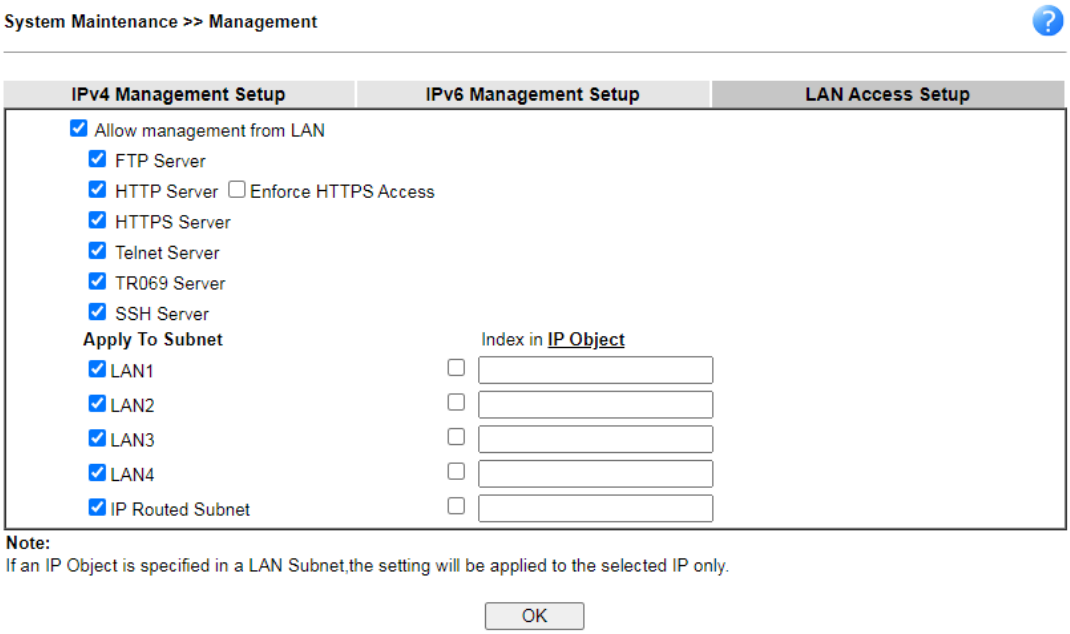


Available settings are explained as follows:

Item	Description
Management Access Control	**Allow management from the Internet** - Check to enable the function. Select the servers that system administrators are allowed to manage from the Internet. **Disable PING from the Internet** - Check to reject all PING packets from the Internet. For increased security, this setting is enabled by default.
IPv6 Address Security Option	**Enable Random Interface Identifiers (IIDs)... -** The IPv6 address will be generated randomly but not using LAN/WAN MAC to prevent the attack from the hacker.
Access List from the Inernet	You could specify that the system administrator can only login from up to 10 designated hosts or networks defined in the list. **Index in IPv6 Object**- Enter the index number of the IPv6 object profile. Related IP address will appear automatically.

Select **OK** to save changes on the page.

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.

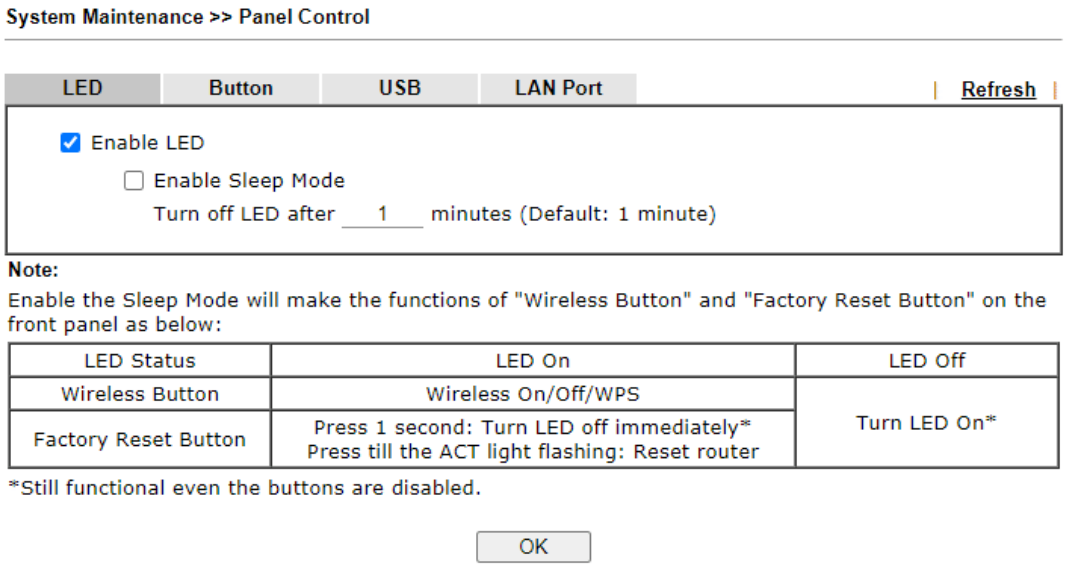
Select **OK** to save changes on the page.

VI-1-11 Panel Control

You may customize the behavior of the LEDs, buttons, WLAN, USB and LAN ports on the front panel.

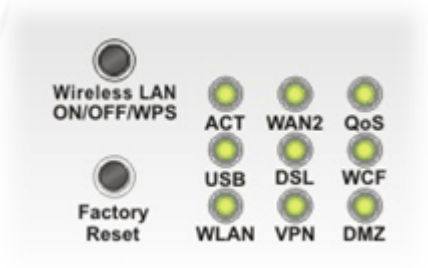
For LED

By default, LEDs on the front panel illuminate or blink during operation to show the status of the various functions on the router. However, you may configure them to remain off at all times, or remain off until a button is pressed to wake them up.



Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable LED	Select to enable the LEDs to function according to the configured settings. Deselect to disable LEDs entirely.
Enable Sleep Mode	Select to let the system turn off the LEDs after the specified number of minutes has elapsed. When Sleep Mode is enabled, the LEDs can be woken up by pressing one of the following buttons: ● Wireless LAN ON/OFF/WPS on the front panel ● Factory Reset on the front panel ● Wake up LED on this configuration page

	
Status	Shows the status of the LEDs. When the following is shown, the LEDs are in sleep mode. **Status :** Sleep [Wake up LED] To wake them up, do one of the following actions: ● press the **Wake up LED** button on this page ● press the **Wireless On/Off/WPS** button on the front panel ● press the **Factory Reset** button on the front panel. When the following is shown, the LEDs are awake. **Status :** Awake, sleep after 1 minutes [LED sleep immediately] To put them to sleep immediately, perform one of the following actions: ● press the **LED sleep immediately** button on this page ● press the Factory Reset button on the front panel
Wake up LED	Click to resume operation of the LED after they have gone to sleep.

Select **OK** to save changes on the page.

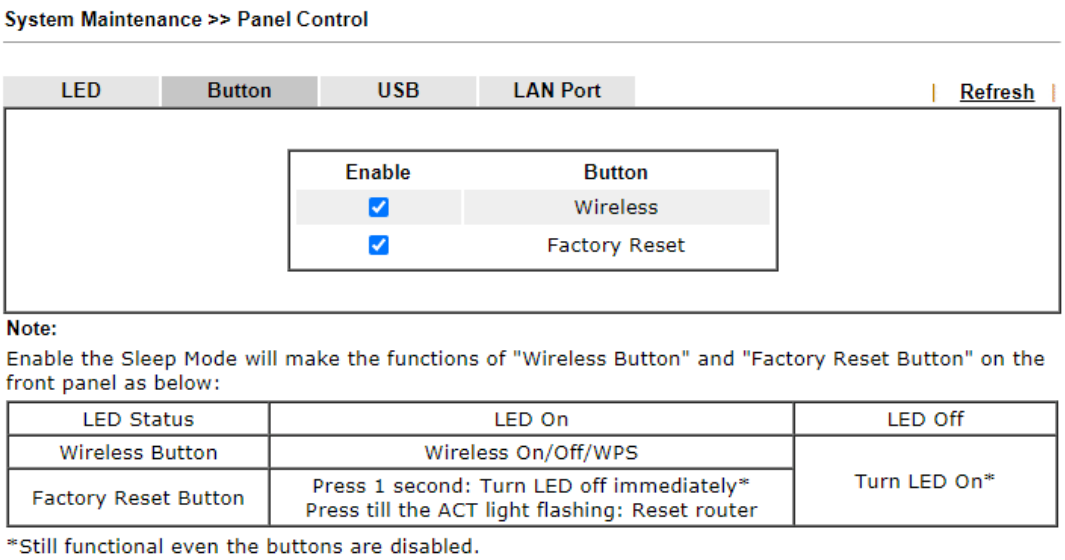
For Button

The primary functions of the **Factory Reset** and **Wireless ON/OFF/WPS** front-panel buttons (reset to factory defaults and wireless control, respectively) are enabled by default, but they can be enabled or disabled as needed.

When the **Factory Reset** button is set to **Disabled**, the router cannot be reset during normal operation. Other functions of the reset button (such as starting up the TFTP server to upload firmware during power on, and controlling the illumination of the front panel LEDs when LED sleep mode is enabled) can still be used.

When the **Wireless ON/OFF/WPS** button is set to **Disabled**, the button cannot be used to turn on or off the wireless network, nor can it be used to start the WPS pairing process. However, the front panel LEDs can be woken up when LED sleep mode is enabled.

Click the **Button** tab to get the following page.



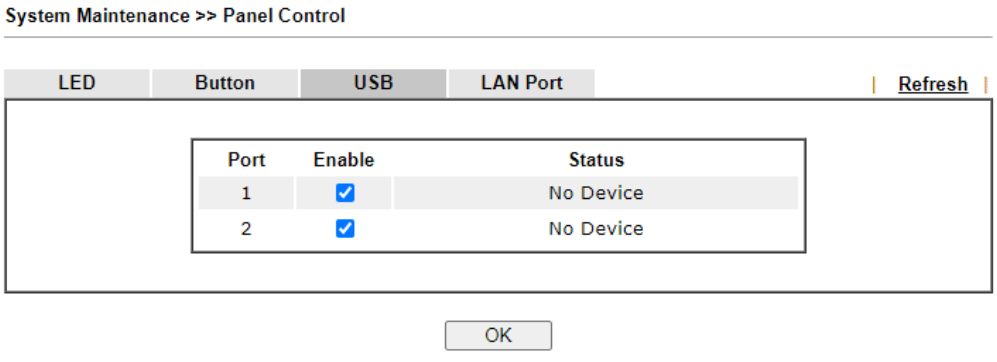
Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information**.**
Enable 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.
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.

Select **OK** to save changes on the page.

For USB

The USB ports can be individually enabled or disabled. When a USB port is disabled, attached devices will not be recognized by the router.



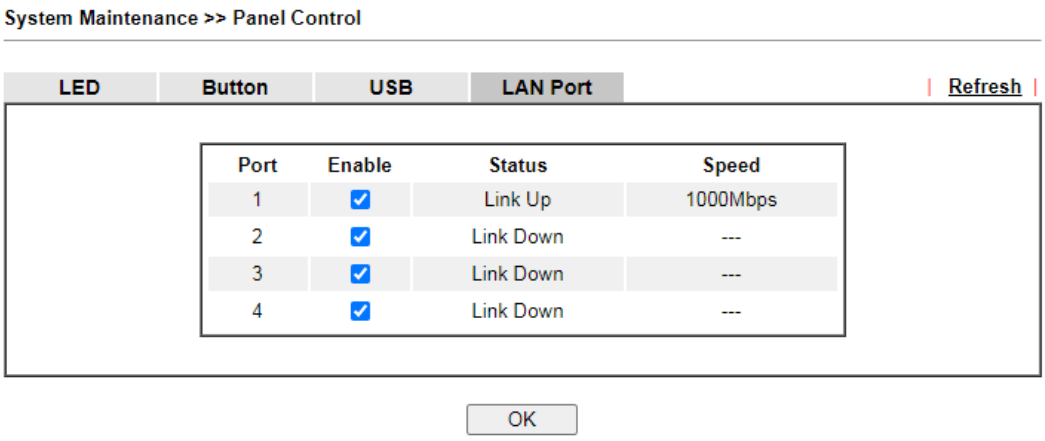
Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information**.**
Port	The number corresponds to the USB port number shown on the front panel.
Enable	Deselect to disable the USB port. The default value is enabled.
Status	Shows the status of the USB port. **No device** – no USB device is connected to the port. **Connected** – a USB device is connected to the port. **---** – the USB port is disabled.

Select **OK** to save changes on the page.

For LAN Port

The 5 LAN ports can be individually enabled or disabled. When a LAN port is disabled, attached devices will not be recognized by the router.



Available settings are explained as follows:

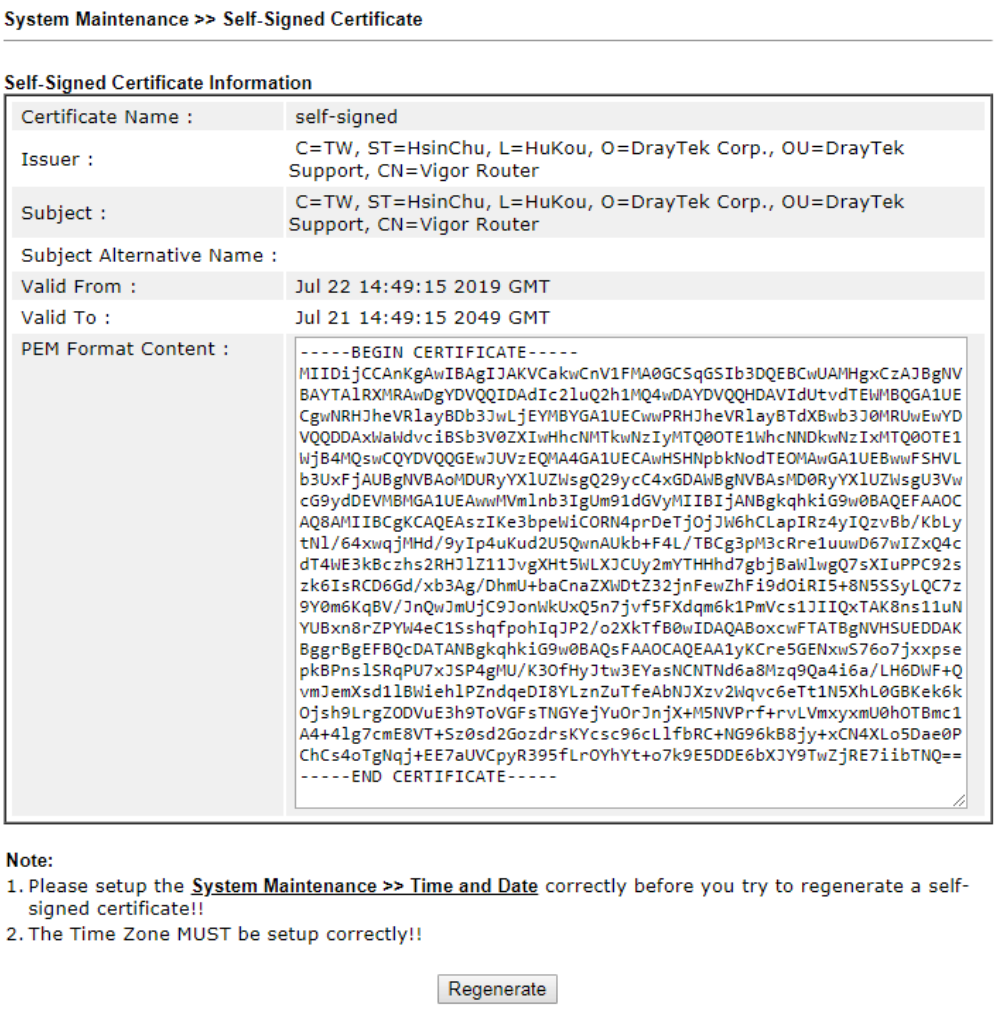
Item	Description
Refresh	Click to refresh the page to display the latest information**.**
Port	The number corresponds to the LAN port number shown on the front panel.
Enable	Deselect to disable the LAN port. The default value is enabled.
Status	Shows the status of the USB port. **Link Up** – An active Ethernet device is connected to the port. **Link Down** – No active Ethernet device is detected. **---** – The LAN port is disabled.
Speed	Shows the negotiated speed of the LAN port. **1000Mbps** – Negotiated speed of the LAN port is 1000 Mbps. **100Mbps** – Negotiated speed of the LAN port is 100 Mbps. **10Mpbs** – Negotiated speed of the LAN port is 10 Mbps. **---** – The LAN port is disabled or there is no active device connected.

Select **OK** to save changes on the page.

VI-1-12 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 can be used for services such as SSL VPN and HTTPS. In addition, it can be created for free by using a wide variety of tools.



System Maintenance >> Self-Signed Certificate

Self-Signed Certificate Information

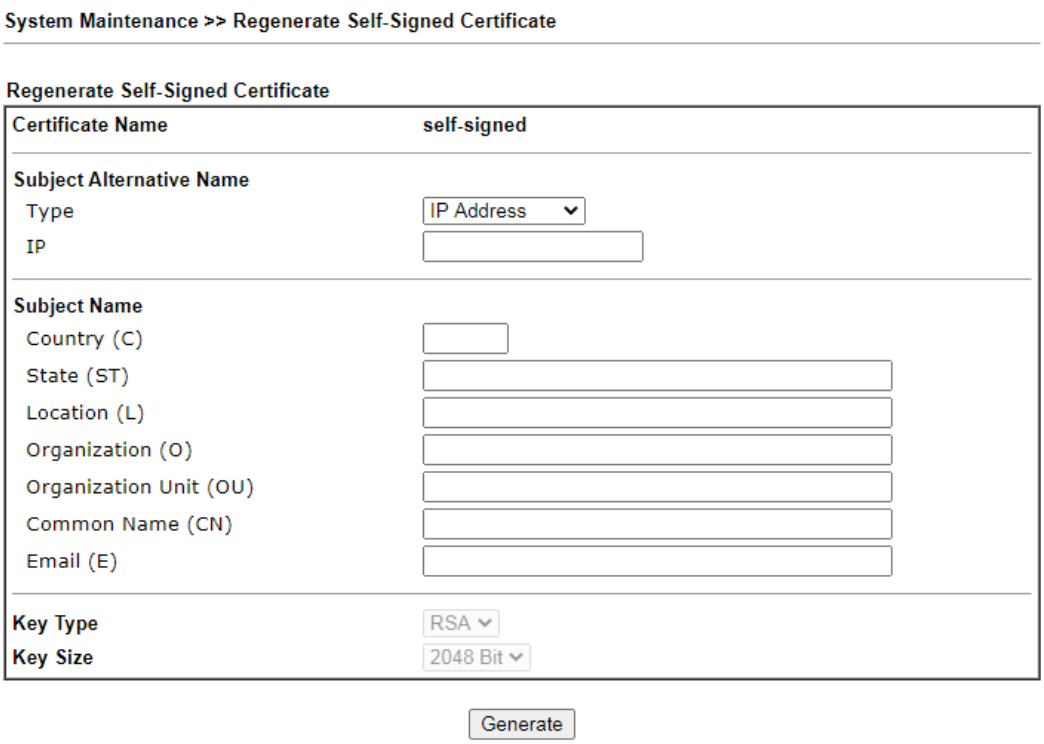
Certificate Name :	self-signed
Issuer :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject Alternative Name :	
Valid From :	Jul 22 14:49:15 2019 GMT
Valid To :	Jul 21 14:49:15 2049 GMT
PEM Format Content :	-----BEGIN CERTIFICATE----- MIIDijCCAnKgAwIBAgIJAKVCakwCnV1FMA0GCSqGSIb3DQEBCwUAMHgxCzAJBgNV BAYTAlRXMRAwDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvdTEWMBQGA1UE CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBwb3J0MRUwEwYD VQQDDAxWaWdvciBSb3V0ZXIwHhcNMTkwNzIyMTQ0OTE1WhcNNDkwNzIxMTQ0OTE1 WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVL b3UxFjAUBgNVBAoMDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsMD0RyYXlUZWsgU3Vw cG9ydDEVMBMGA1UEAwwMVmlnb3IgUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAszIKe3bpeWiCORN4prDeTjOjJW6hCLapIRz4yIQzvBb/KbLy tNl/64xwqjMHd/9yIp4uKud2U5QwnAUkb+F4L/TBCg3pM3cRre1uuwD67wIZxQ4c dT4WE3kBczhs2RHJlZ11JvgXHt5WLXJCUy2mYTHHhd7gbjBaWlwgQ7sXIuPPC92s zk6IsRCD6Gd/xb3Ag/DhmU+baCnaZXWDtZ32jnFewZhFi9dOiRI5+8N5SSyLQC7z 9Y0m6KqBV/JnQwJmUjC9JonWkUxQ5n7jvf5FXdqm6k1PmVcs1JIIQxTAK8ns11uN YUBxn8rZPYW4eC1SshqfpohIqJP2/o2XkTfB0wIDAQABoxcwFTATBgNVHSUEDDAK BggrBgEFBQcDATANBgkqhkiG9w0BAQsFAAOCAQEAA1yKCre5GENxwS76o7jxxpse pkBPnslSRqPU7xJSP4gMU/K3OfHyJtw3EYasNCNTNd6a8Mzq9Qa4i6a/LH6DWF+Q vmJemXsd1lBWiehlPZndqeDI8YLznZuTfeAbNJXzv2Wqvc6eTt1N5XhL0GBKek6k Ojsh9LrgZODVuE3h9ToVGFsTNGYejYuOrJnjX+M5NVPrf+rvLVmxyxmU0hOTBmc1 A4+4lg7cmE8VT+Sz0sd2GozdrsKYcsc96cLlfbRC+NG96kB8jy+xCN4XLo5Dae0P ChCs4oTgNqj+EE7aUVCpyR395fLrOYhYt+o7k9E5DDE6bXJY9TwZjRE7iibTNQ== -----END CERTIFICATE-----

Note:

1. Please setup the **System Maintenance >> Time and Date** correctly before you try to regenerate a self-signed certificate!!
2. The Time Zone MUST be setup correctly!!

Regenerate

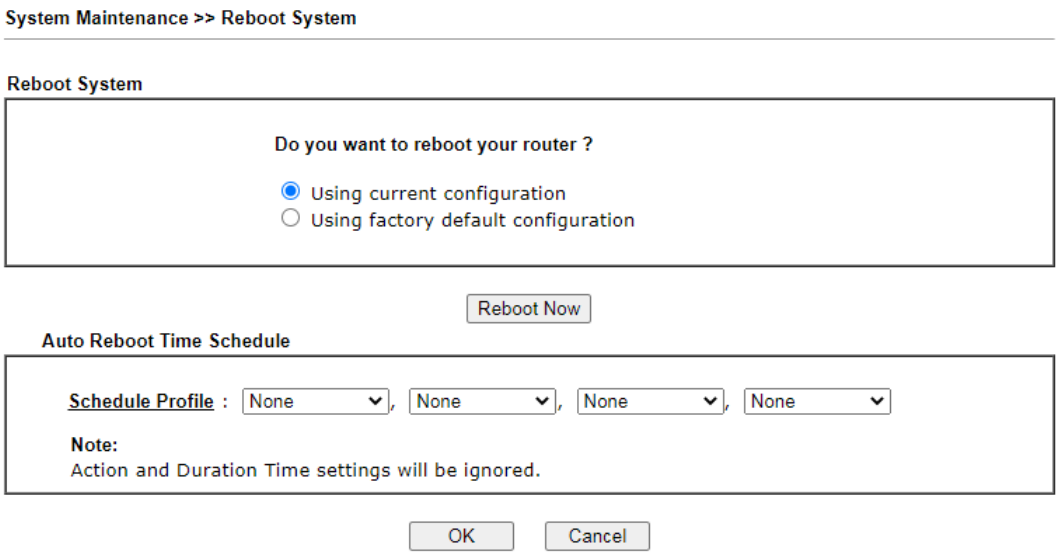
Click **Regeneration** to open **Regenerate Self-Signed Certificate** window.



Enter all requested information including certificate name (used to differentiate different certificates), subject alternative name type and relational settings for subject name. Then click **GENERATE**.

VI-1-13 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to bring up the following page.



Available settings are explained as follows:

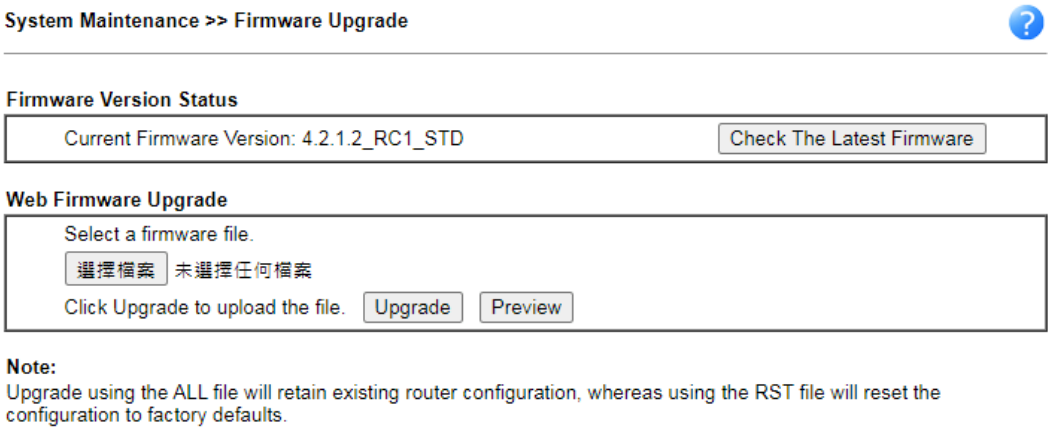
Item	Description
Reboot System	Select one of the following options, and press the **Reboot Now** button to reboot the router. **Using current configuration** – Select this option to reboot the router using the current configuration. **Using factory default configuration** – Select this option to reset the router's configuration to the factory defaults before rebooting.
Auto Reboot Time Schedule	**Schedule Profile** - Select up to 4 user-configured schedules to reboot the router on a scheduled basis.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

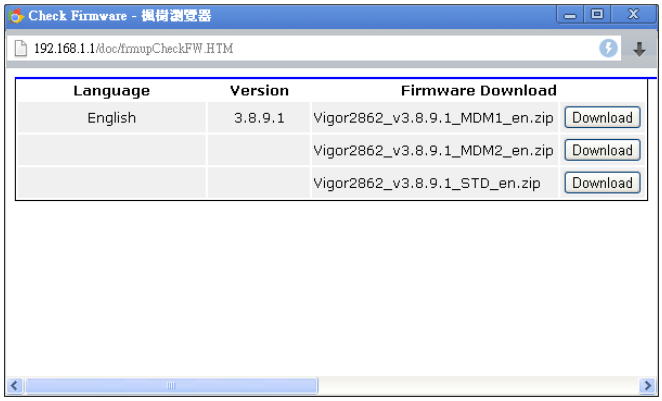
Info	When the system pops up Reboot System web page after you configure web settings, please click Reboot Now to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

VI-1-14 Firmware Upgrade

Click **System Maintenance>> Firmware Upgrade** to upgrade firmware upgrade.

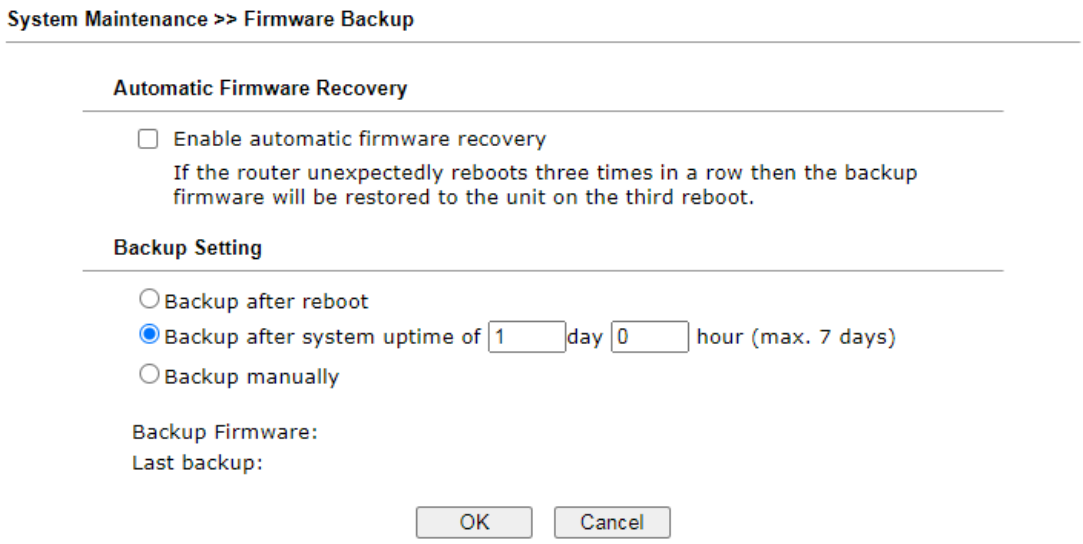


Available settings are explained as follows:

Item	Description
Firmware Versiono Status	**Check The Latest Firmware** – Click to check for updated firmware. Any available new firmware files will be displayed and you can download any one of them by clicking **Download**. After the file has been downloaded, click Select followed by Upgrade to perform the firmware upgrade.  **(重新截圖 for 2135)**
Web Firmware Upgrade	Click **Browse…** to select the firmware file, followed by **Upgrade** to start the upgrade process, or **Preview** to display detailed information about the selected firmware file:

VI-1-15 Firmware Backup

The firmware for Vigor router can be saved on the host as a backup firmware. After that, if the router crashes due to the firmware error, the backup firmware will be applied to make the router run normally.



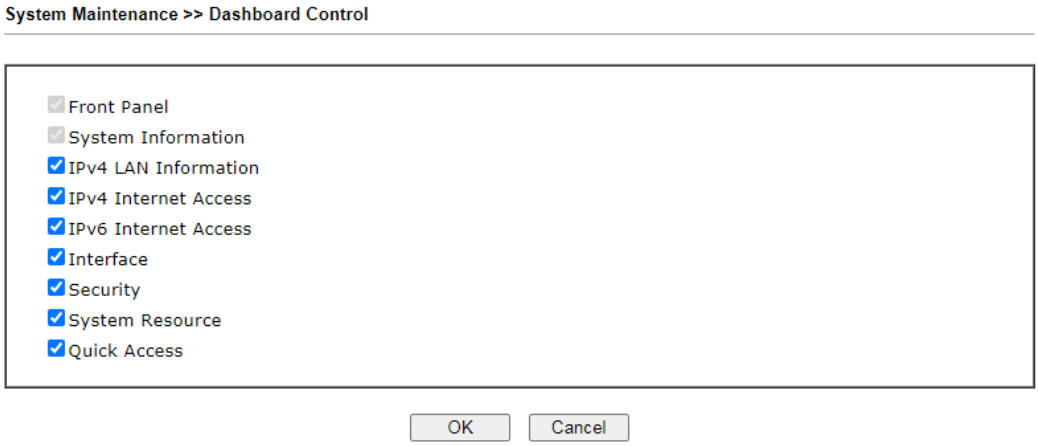
Available settings are explained as follows:

Item	Description
Automatic Firmware Recovery	**Enable automatic firmware recovery**- If this option is enabled, the router will restore the most recently backed-up firmware after the router reboots unexpectedly three times.
Backup Setting	This option controls the backup behavior of the router. ● **Backup after reboot -** The router makes a copy of the current firmware immediately after it reboots ● **Backup after system uptime... -** The router makes a copy of the current firmware after it has run for the specified length of time after boot-up. ● **Backup manually -** the router will not automatically create a backup copy of the firmware. Click this option and click OK, firmware backup will be performed immediately. **Backup Firmware** - Displays recent firmware backup version. **Last backup** - Displays the time of recent firmware backup.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

VI-1-16 Dashboard Control

There are nine groups of setting information which can be displayed on Dashboard as a reference for administrator/user. Except for Front Panel and System Information, the settings information regarding to the groups listed on this page can be hidden if required.



VI-2 Bandwidth Management

Sessions Limit

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

Bandwidth Limit

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

Quality of Service (QoS)

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

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

A typical QoS deployment consists of two components:

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

APP QoS

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

Protocols and applications fall into two categories: Traceable and Untraceable. Traceable applications are those whose traffic can be 100% traced, and can be assigned a specific QoS class. Untraceable applications, on the other hand, are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.

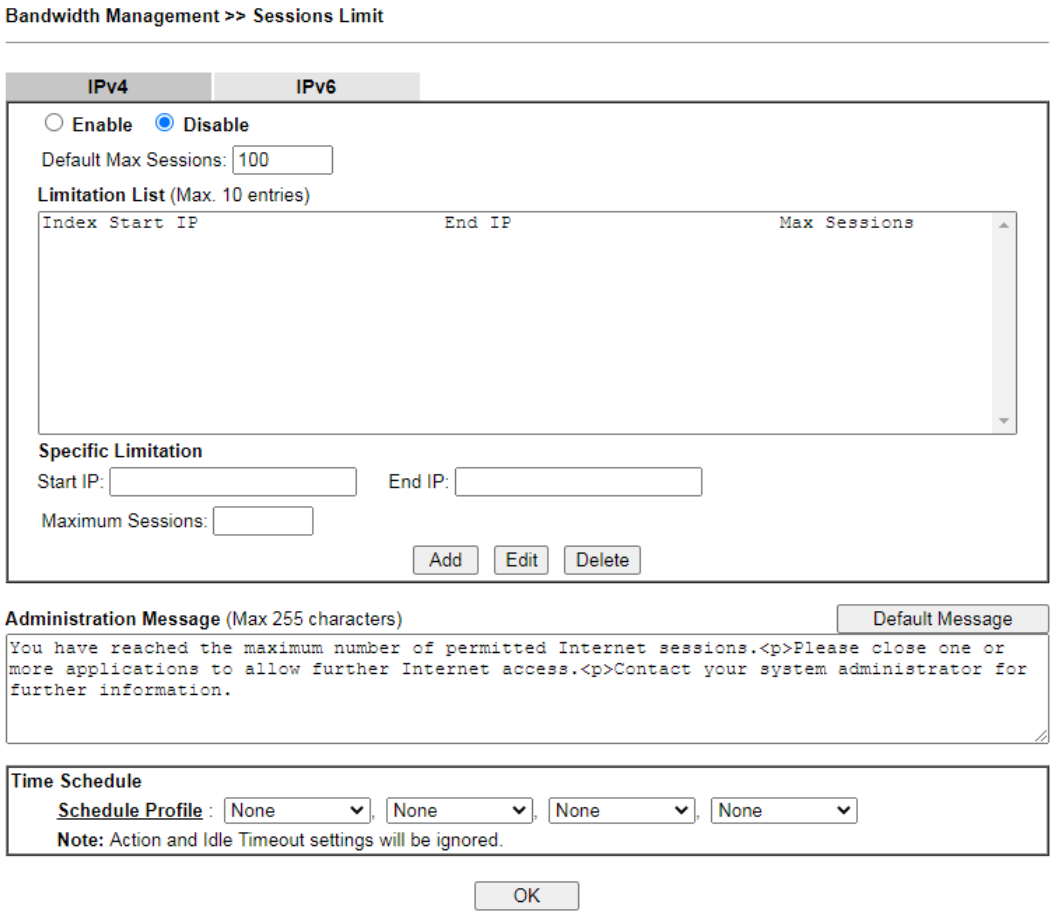
Web User Interface

Bandwidth management ensures efficient allocation of network bandwidth for various applications.

To set up Bandwidth Management, from the Main Menu, select **Bandwidth Management**.

VI-2-1 Sessions Limit

To configure Sessions Limit, from the **Bandwidth Management** menu, select **Sessions Limit** to open the setup page.



Available settings are explained as follows:

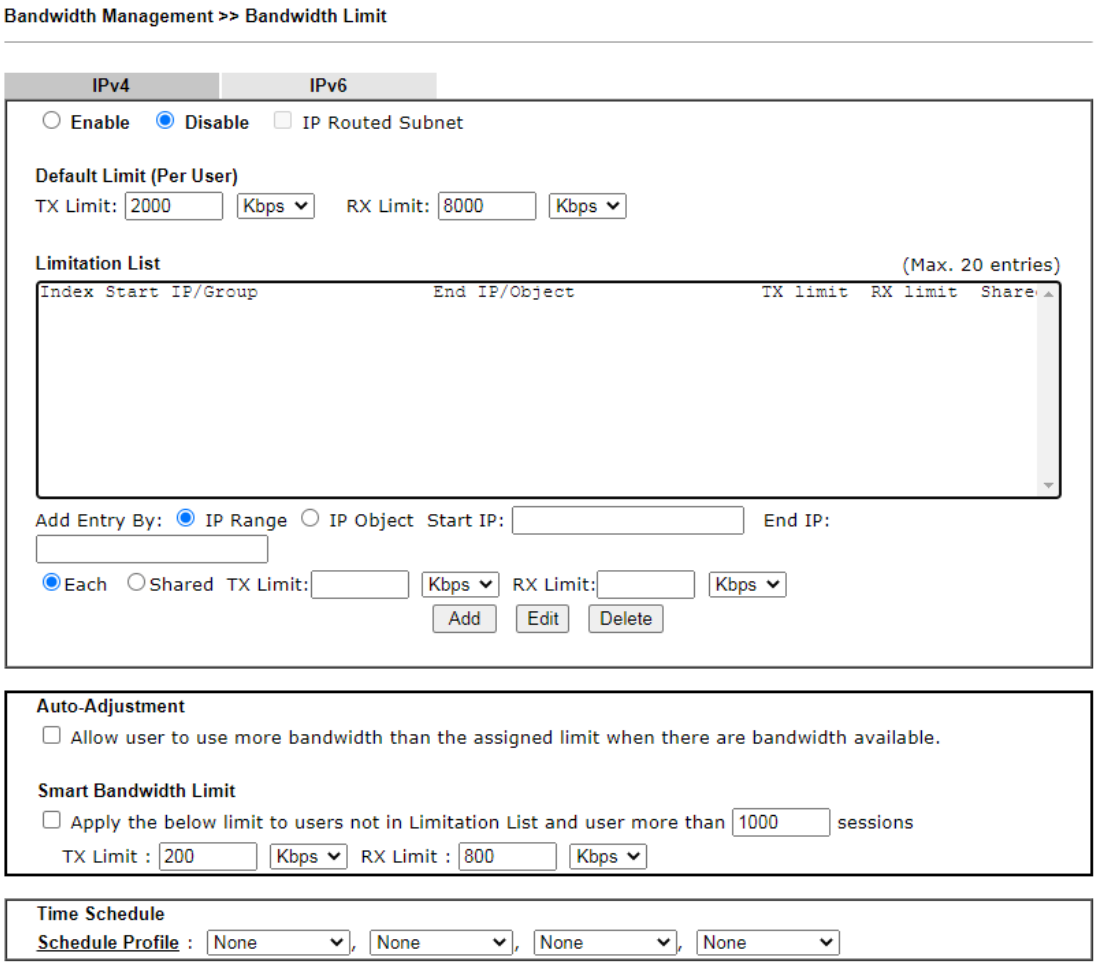
Item	Description
Enable / Disable	**Enable -** Select to activate session limit function. **Disable -** Select to deactivate session limit function. **Default Max Sessions -** The default maximum number of sessions allowed per LAN client, unless overridden by

	specifying a different number in the Limitation List.
Limitation List	Displays specific limitation entries.
Specific Limitation	**Start IP -** The beginning IP address for this limit entry. **End IP -** The ending IP address for limit entry. **Max Sessions -** The maximum number of NAT sessions allowed per LAN client. If no value is entered, the Default Max Sessions value is used. **Add -** Creates a new limit entry using the above Specific Limitation values. **Edit -** To edit an existing entry, select the entry from the Limitation List, make the appropriate changes in Specific Limitation, then click Edit. **Delete -** To delete an entry, select it from the Limitation List, then click the Delete button.
Administration Message	Message to be displayed in a web browser on the LAN client when the maximum number of NAT sessions has been reached. **Default Message** - Click to reset the administration message to the factory default.
Time Schedule	**Schedule Profile** - Specify up to 4 time schedule entries to enable or disable the WAN.

To save changes on the page, click **OK**.

VI-2-2 Bandwidth Limit

To configure the Bandwidth Limit feature, from the **Bandwidth Management** menu, select **Bandwidth Limit** to bring up the configuration page.



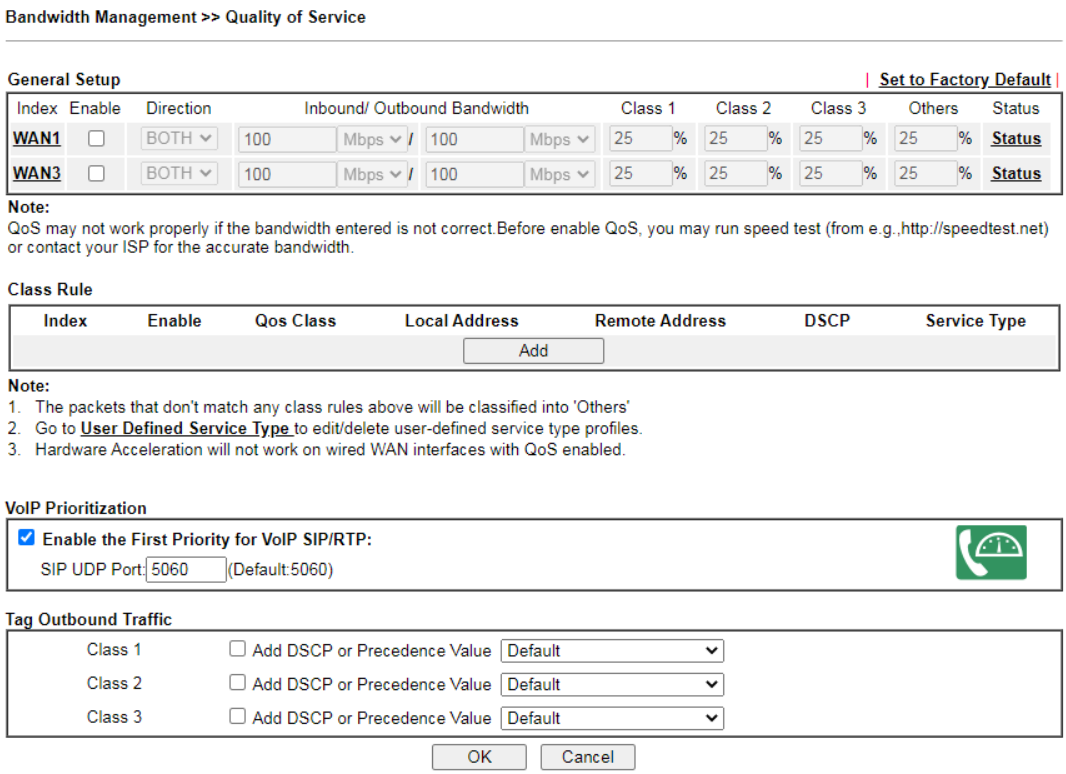
Available settings are explained as follows:

Item	Description
Enable / Disable	**Enable** - Select to activate bandwidth limit function. **Disable** - Select to deactivate bandwidth limit function. **IP Routed Subnet** – Check this box to apply the bandwidth limit to the traffic via IP routed subnet. **Default Limit (Per User)** ● **TX LImit -** Default upstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. ● **RX limit -** Default downstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited and 30000).
Limitation List	Displays specific limitation entries.
Add Entry By	**IP Range -** All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX Limit below. ● **Start IP -** The beginning IP address for this limit entry.

	• **End IP -** The ending IP address for limit entry. **IP Object -** All the IPs specified by the selected IP object or IP group will be restricted by bandwith limit defined by TX Limit and RX Limit below. • **IP Group** – Specify an IP group by using the drop down list. • **IP Object -** Specify an IP object by using the drop down list. **Each** - The specified bandwidth is the limit per LAN client. **Shared -** The specified bandwidth limits are the total allowed for all LAN clients within the range of IP addresses. • **TX limit -** The upstream limit. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. • **RX limit -** The downstream limit. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. **Add -** Creates a new limit entry using the above Specific Limitation values. **Edit -** To edit an existing entry, select the entry from the Limitation List, make the appropriate changes in Specific Limitation, then click Edit. **Delete -** To delete an entry, select it from the Limitation List, then click the Delete button.
Auto-Adjustment	**Allow user to use more bandwidth ….-** Select to let the router automatically adjust the upstream and downstream limits based on available bandwidth.
Smart Bandwidth Limit	This option restricts the bandwidth of LAN clients that are not in the limitation list when the network sessions exceed a predefined threshold. **Apply the below limit to ...** - The number of sessions a LAN client is allowed to have before Smart Bandwidth Limit activates. • **TX limit -** Upstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. • **RX limit -** Downstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited and 30000).
Time Schedule	**Schedule Profile** - Specify up to 4 time schedule entries to enable or disable the WAN.

VI-2-3 Quality of Service

To configure **Quality of Service**, from the main menu, select **Bandwidth Management** menu, then click **Quality of Service** to bring up the configuration page.



Available settings are explained as follows:

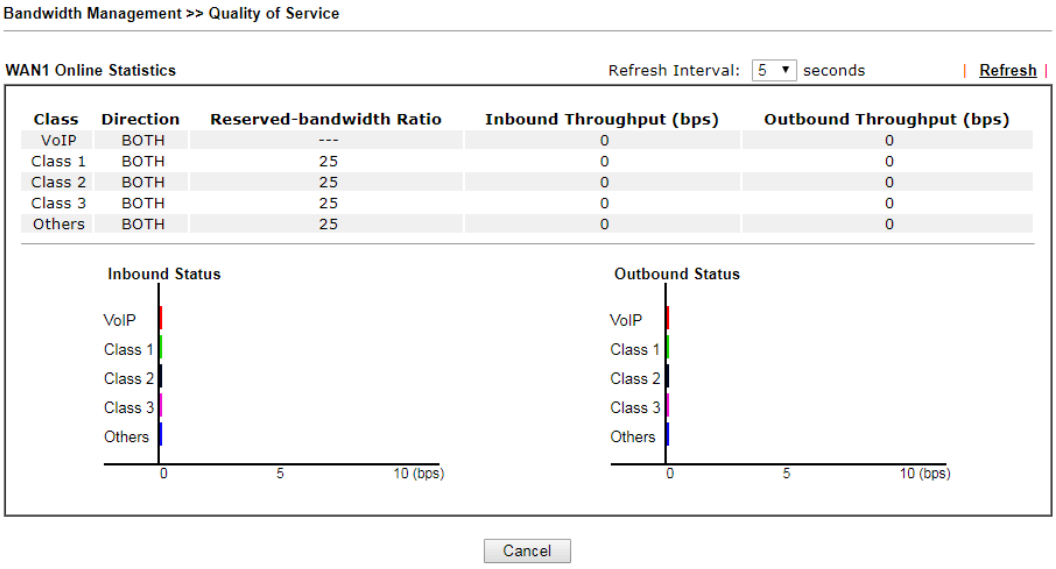
Item	Description
General Setup	**Index** – Link of WAN interface. **Enable** – Check the box to enable the QoS function for WAN interface. If it is enabled, you can configure general QoS setting for each WAN interface. ● **Direction** –Direction of traffic to which QoS is to be applied (Inbound, Outbound, or Both). - **IN -** Apply QoS to incoming traffic only. - **OUT -** Apply QoS to outgoing traffic only. - **BOTH -** Apply to both incoming and outgoing traffic. ● **Inbound/Outbound Bandwidth** – The inbound / outbound bandwidth of the WAN. ● **Class 1 ~ 3 / Others** – Percentage of bandwidth reserved for each class. **Status** – Click to bring up the Online Statistics page that shows snapshots of statistics for the given 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.

Item	Description
	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**.

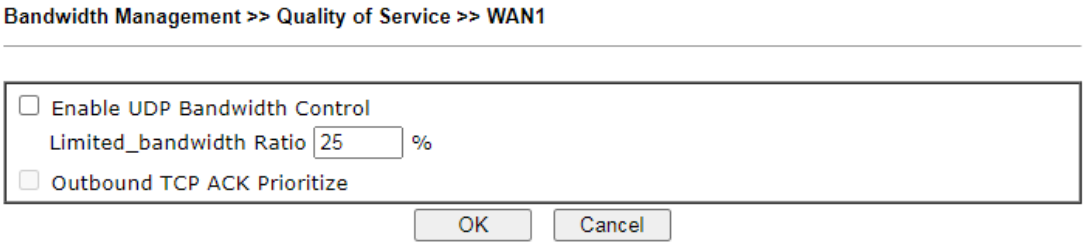
Online Statistics

Click the Status link in the General Setup section to show real-time online statistics of the WAN interface.



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:

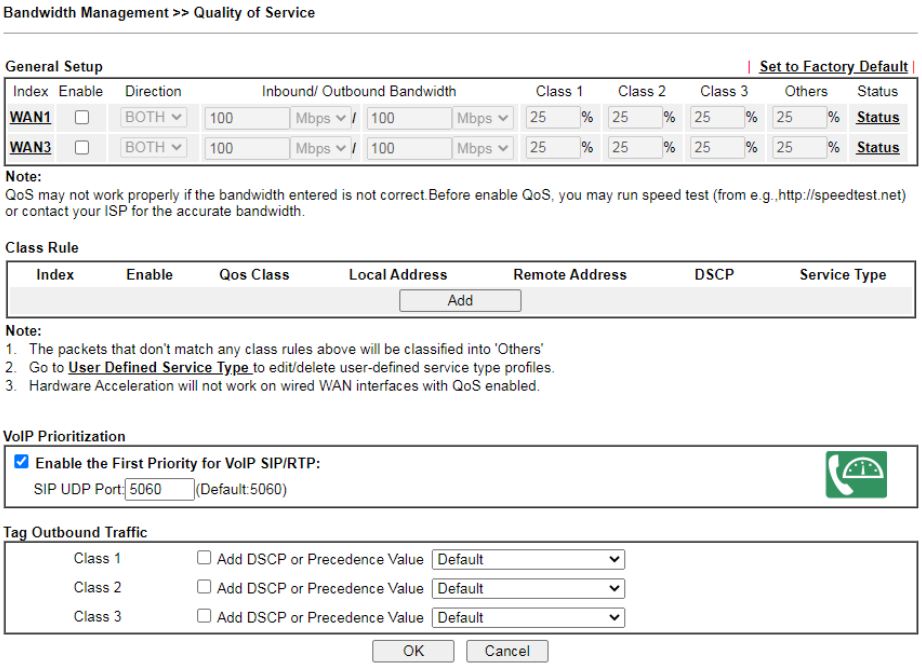
Item	Description
Enable UDP Bandwidth Control	Select to restrict the bandwidth available to UDP traffic. The **Limited_bandwidth Ratio** value is the maximum percentage of bandwidth that can be used by UDP traffic. ● **Limited_bandwidth Ratio -** Enter a percentage value.
Outbound TCP ACK Prioritize	Select to give outbound ACK packets priority over other packets to ensure traffic is not slowed down because the remote host is waiting for ACK packets before further traffic will be sent.

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.

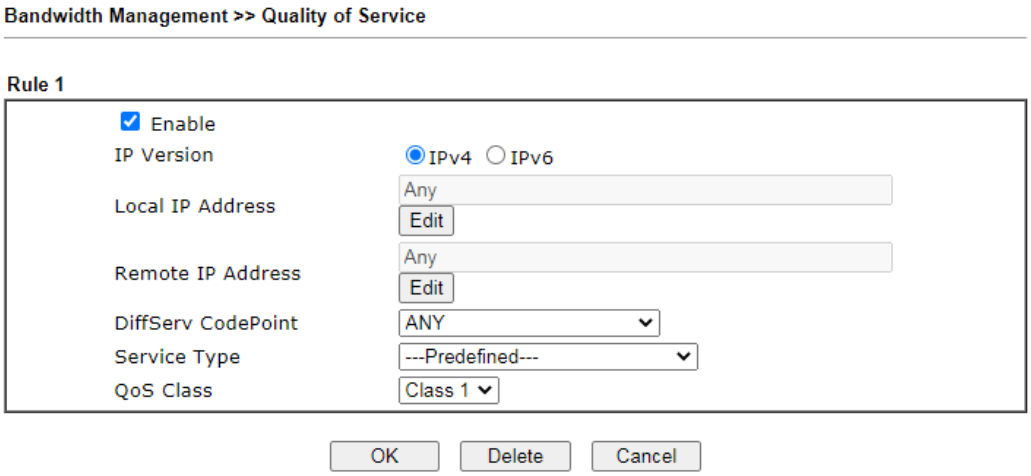
Add / edit a Class Rule for QoS

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.

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.

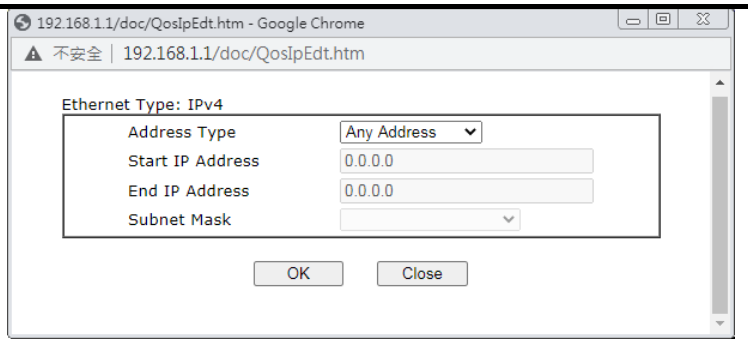


2. For adding a new rule, click **Add** to open the following page.

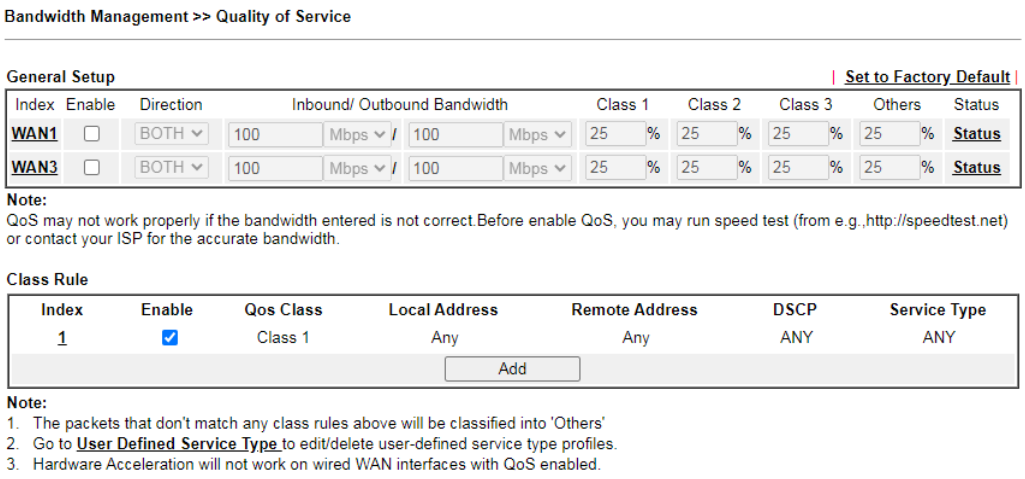


Available settings are explained as follows:

Item	Description
Enable	Select to enable this rule.
IP Version	Protocol (IPv4 or IPv6) to which this rule applies.
Local IP Address	Click the **Edit** button to set the local (LAN) IP address or address range for the rule.
DiffServ CodePoint	DSCP or ToS precedence of packets to which this rule applies.
Remote IP Address	Click the **Edit** button to set the remote (WAN) IP address or address range for the rule.

	 **Address Type** – Type of address: Any Address, Single Address, Range Address, Subnet Address. ● **Single Address** - Specify IP address. ● **Range Address** - Specify Start IP Address and End IP Address. ● **Subnet Address** - Specify Start IP Address and Subnet Mask.
Service Type	Service Type to which this rule applies. Service is a predefined or user-defined type of traffic that uses certain protocols or ports. To set up a custom service, select User Defined to set the service name, the protocol, and port number.
QoS Class	Specify the QoS class (1, 2 or 3) for this rule.

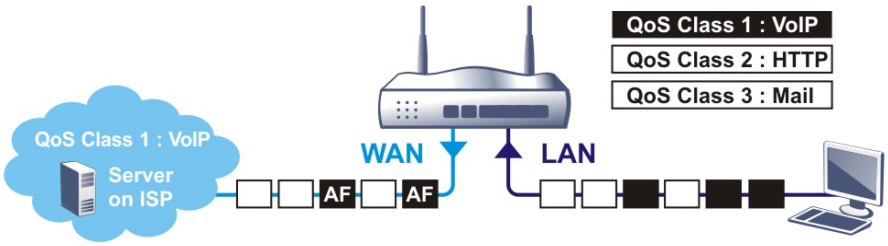
3. After finishing all the settings here, please click **OK** to save the configuration.

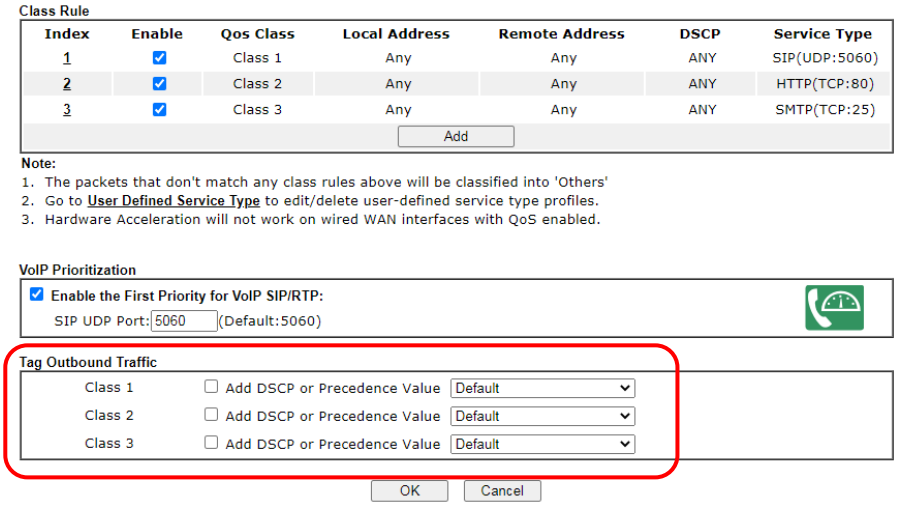


Retag the Packets for Identification

Packets originating from the LAN that are destined for the WAN can have the DS flag changed to a different value by enabling Tag Packet and specifying the DSCP or IP Precedence value.

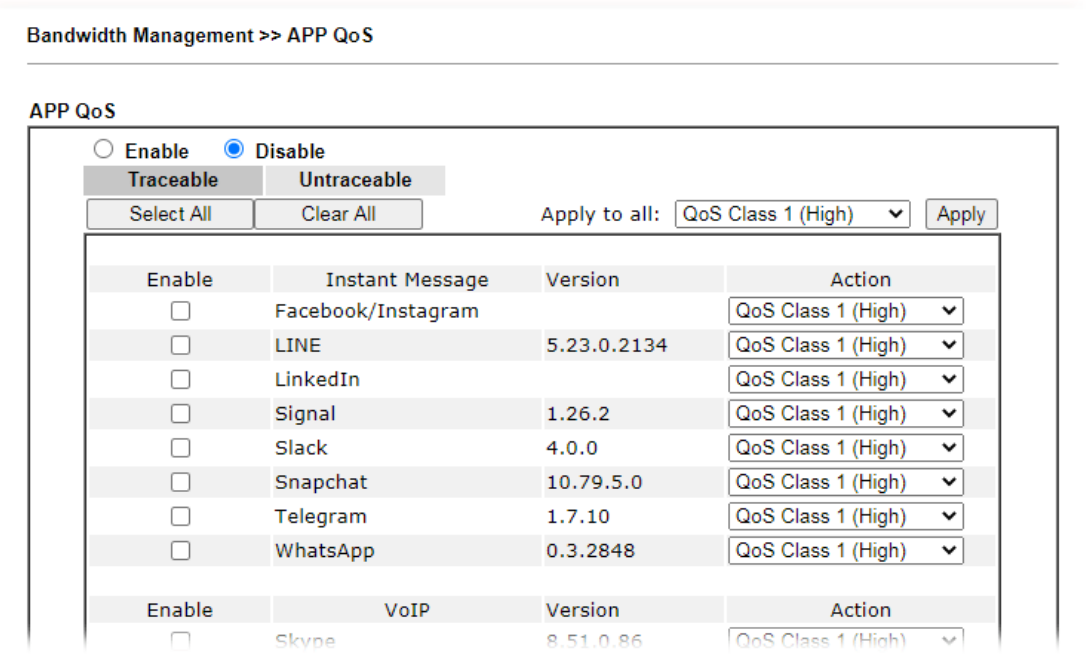
In the following illustration, outbound VoIP packets from the LAN arrive at the Vigor router with the QoS value unset. The router sets the DSCP value to AF before forwarding them to the ISP server via the WAN interface.





VI-2-4 APP QoS

To configure APP QoS, from the main menu, select **Bandwidth Management** menu, then click **APP QoS** to bring up the configuration page.



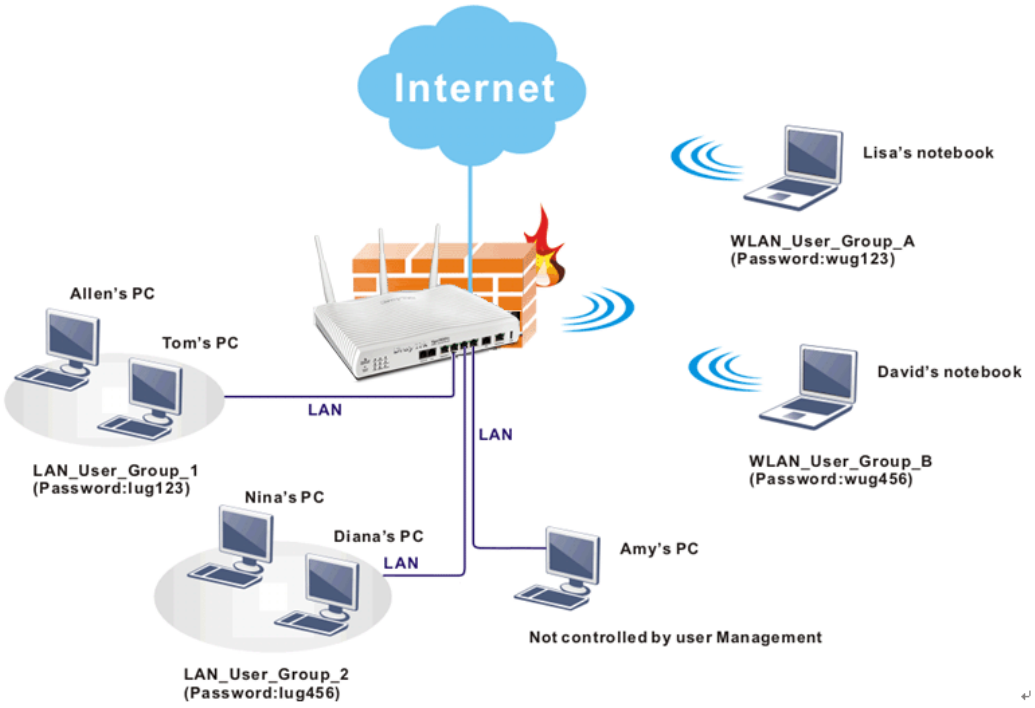
Available settings are explained as follows:

Item	Description
Enable/Disable	Enables or disables the APP QoS feature.
Traceable	Traceable applications are those whose traffic can be 100% traced. All protocols under this tab can have a specific QoS class assigned. **Enable** - Select to enable OoS for the application. **Apply to all** - Select a QoS class to be applied to all protocols. You can override the QoS class for specific protocols using the Action dropdown listbox.
Untraceable	Untraceable applications are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class. All protocols under this tab can have a specific QoS class assigned. **Enable** - Select to enable OoS for the application. **Action** - Select a QoS class to be applied to all applications.
Select All	Click to select all Enabled checkboxes.
Clear All	Click to deselect all Enabled checkboxes.

After changes have been made, click **OK** to save changes, or **Cancel** to discard.

VI-3 User Management

User Management allows the network administrator to manage Internet access at the user level. After a user has been authenticated by means of a username and password, he or she can be granted Internet access, and optional firewall rules and WAN access policies can be applied.

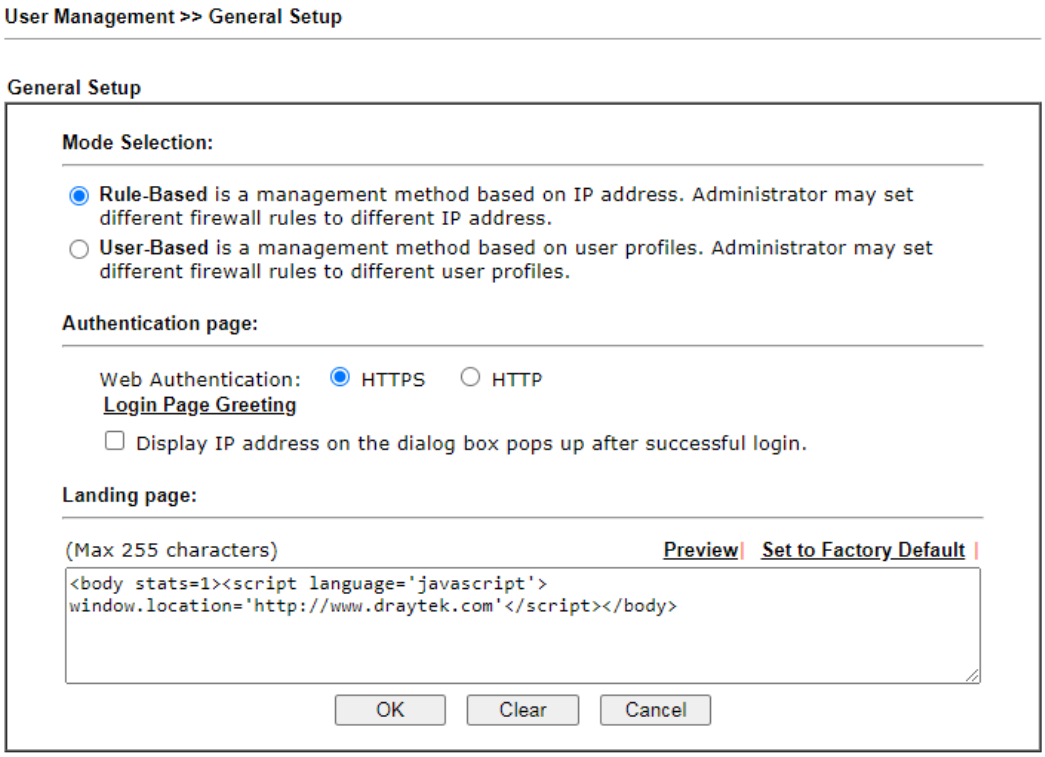


Info	In general, filter rules configured in the Firewall apply globally. However, in user management, the filter rules can be selectively applied to user profiles.

Web User Interface

VI-3-1 General Setup

Global settings for User Management can be configured in this section.



Available settings are explained as follows:

Item	Description
Mode Selection	The User Management Mode. **User-Based** – Router applies filter rules configured in **User Management>>User Profile**. **Rule-Based** – Router applies filter rules configured in **Firewall>>General Setup** and **Filter Rule**.
Authentication page	**Web Authentication** - Web protocol for the web authentication page. ● HTTP – Web page will be unencrypted. ● HTTPS – Web page will be encrypted. **Login Page Greeting** - Click to be redirected to **System Maintenance >> Login Page Greeting**, where you can configure the message that is shown to the user after a

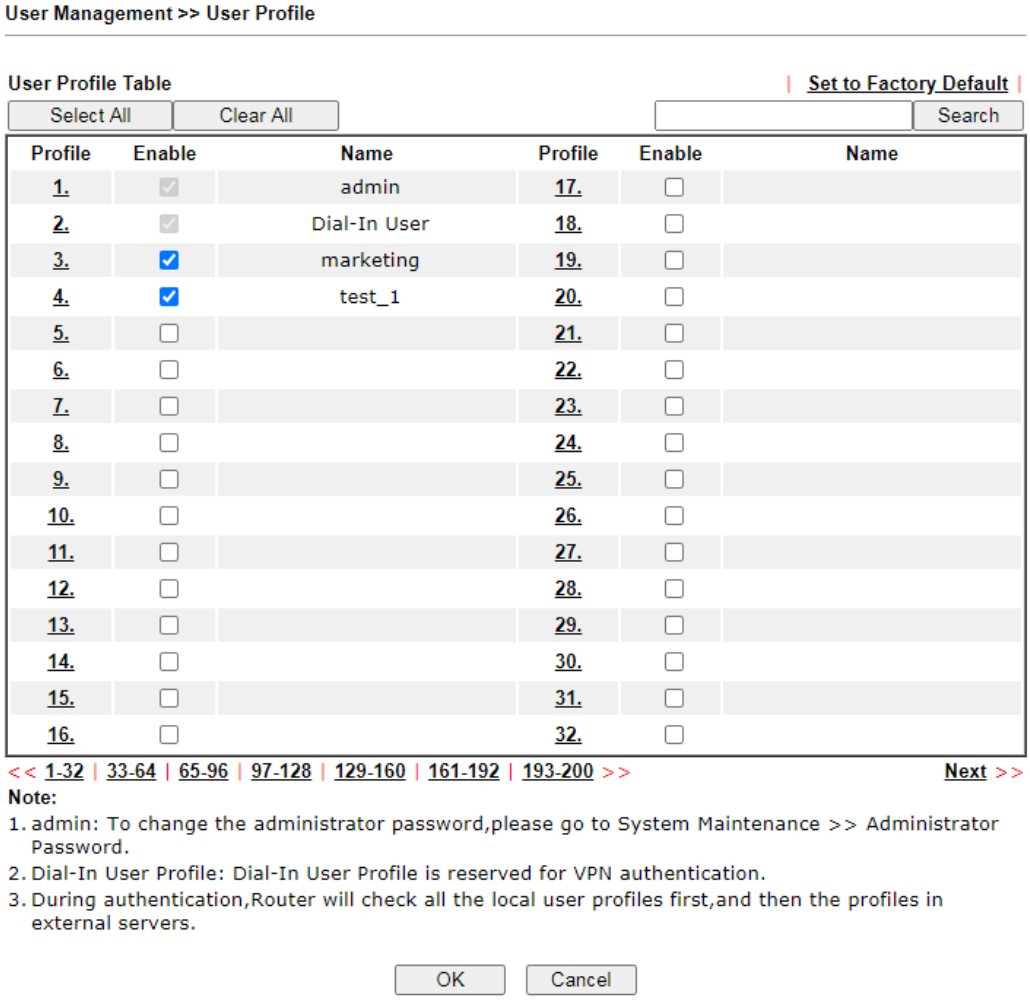
	successful login. **Display IP Address on tracking window** – Select to display the IP address of the client on the tracking window.
Landing Page	HTML code to be shown on the Login Page Greeting.

Click **OK** to save changes, **Clear** to restore settings to factory defaults, or **Cancel** to discard changes.

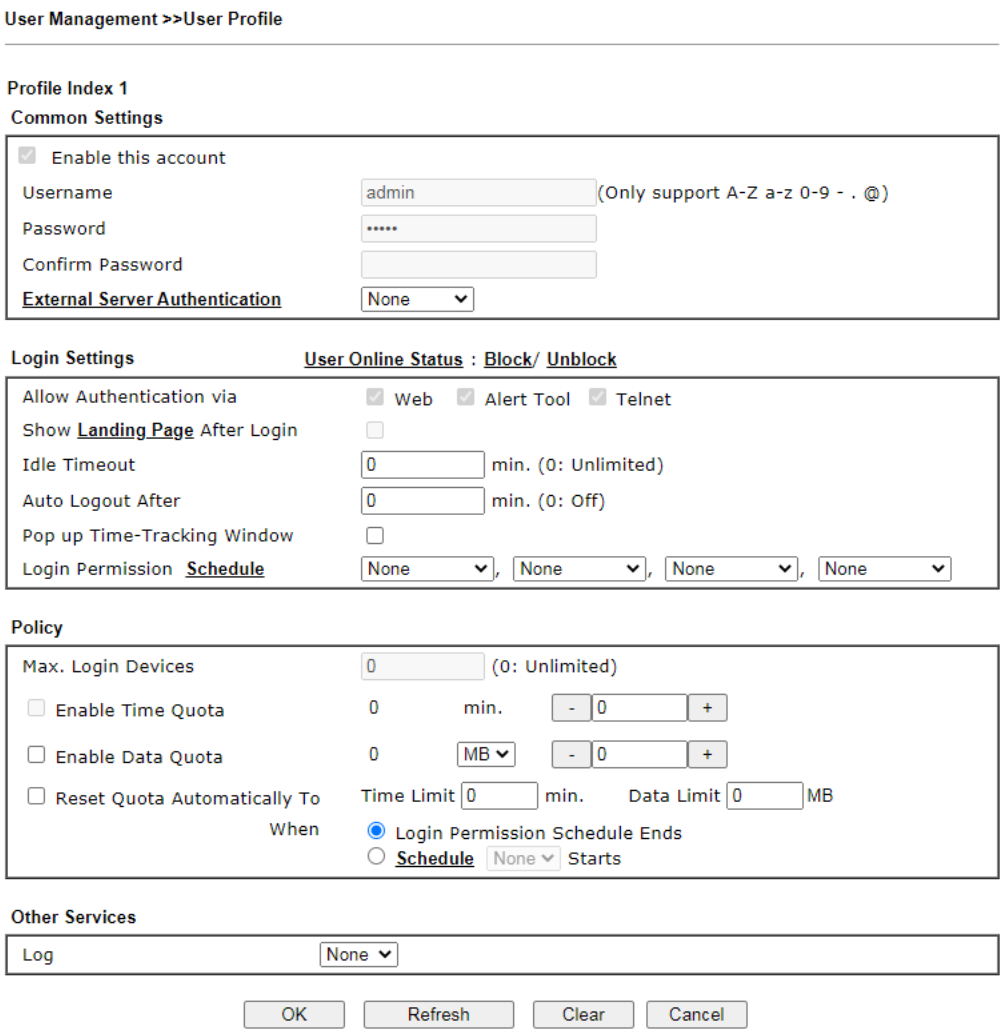
VI-3-2 User Profile

This page allows you to create up to 200 user profiles for use with User Management.

Select **User Management>>User Profile** from the menu bar, then click a profile number to configure.

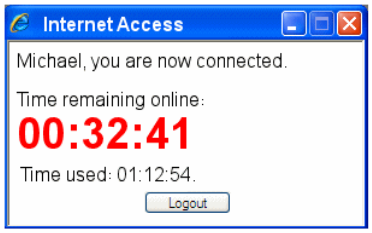


Profiles 1 (admin) and 2 (Dial-In User) are reserved profiles. The admin profile applies to the router administrator login, while the Dial-in User profile applies to all VPN dial-in users.



Available settings are explained as follows:

Item	Description
Common Settings	
Enable this account	Select to enable this user profile.
Username	Login name (e.g., *LAN_User_Group_1*, *WLAN_User_Group_A*, *WLAN_User_Group_B*, etc.) for this user profile. Maximum length is 24 characters.
Password	Password (e.g., *lug123*, *wug123*,*wug456*, etc.) for this user profile. Maximum length is 24 characters. When a user tries to access the Internet and User Management is enabled, he or she must supply a valid user name and password combination for authentication. The profile with matching user name and password will be applied to the session.
Confirm Password	Enter the password again for confirmation.
External Server Authentication	The router will authenticate dial-in users using either a built-in (None) or external service (LDAP, Radius or TACACS+). The Password setting is ignored when an external authentication service is used.
Login Settings	
Allow Authentication via	The authentication methods allowed for this user.

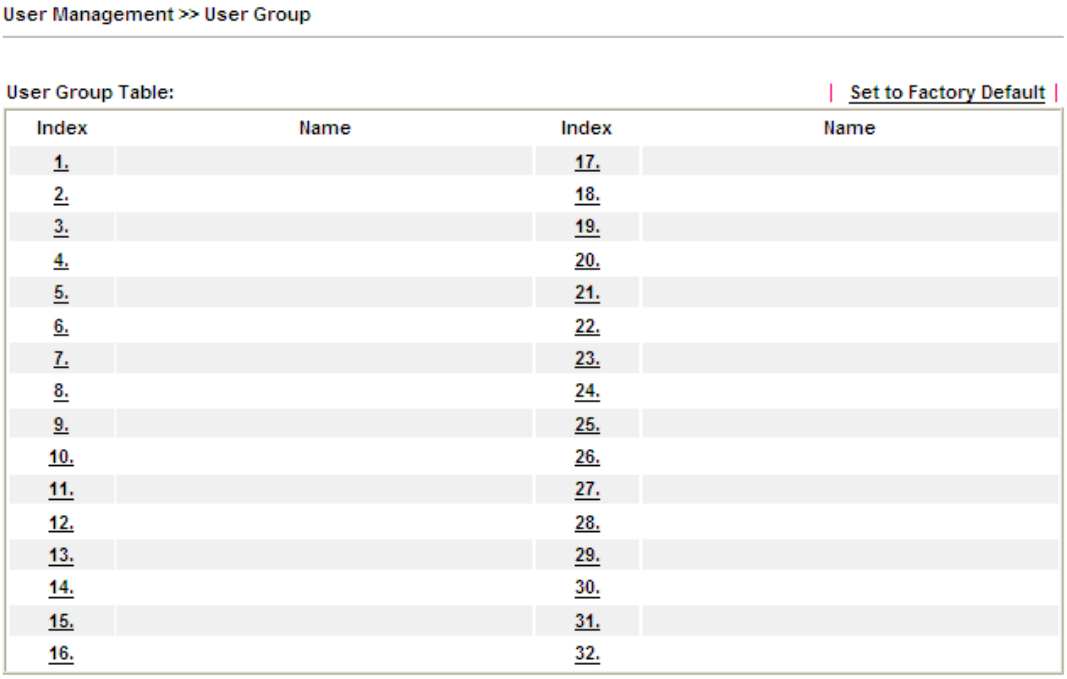
	Web – If selected, user will need to authenticate by entering a username and password when attempting to access an external website for the first time. The user will be redirected to the external website after a successful authentication. **Alert Tool** – If selected, the user can enter the user name and password into the DrayTek Alert Tool. A window with remaining time of connection for such user will be displayed. The Alter Tool can be downloaded from the DrayTek website. **Telnet** – If selected, the user can authenticate by logging in to the router using telnet.
Show Landing Page After Login	When a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in **User Management>>General Setup**. Check this box to enable such function.
Idle Timeout	If there is no WAN traffic to and from the LAN client for the specified amount of time (in minutes), the WAN session is reset and the user will need to re-authenticate before Internet access is once again allowed. The default Idle Timeout value is 10 minutes.
Auto Logout After	Such account will be forced to logout after a certain time set here.
Pop up Time-Tracking Window	If enabled, a browser window will pop up showing the session time remaining. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection.
Login Permission Schedule	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.
Policy	
Max. Login Devices	The maximum number of concurrent logins allowed for this profile. The default setting is 0 which means no limit.
Enable Time Quota	If selected, the user is allowed Internet access for the specified amount of time after a successful authentication. The first value is the remaining time of the current login session, whereas the second value is the value to increment or decrement from the remaining time quota by clicking + /- buttons. Both values are in minutes. Click + / - to increase / decrease the time quota for such profile. **Note:** A dialog will be popped up showing the remaining time remained when the user after the user has successfully authenticated. 

	When the time is up, all Internet connections are terminated.
Enable Data Quota	If selected, the user is allowed to use the specified amount of data after a successful authentication. The first value is the remaining data quota of the current login session, whereas the second value is the value to increment or decrement from the remaining data quota by clicking +/ - buttons. The unit for both values can be set to either MB (megabytes) or GB (gigabytes) using the MB/GB dropdown box. Click + / - to increase / decrease the data quota for such profile.
Reset quota automatically	Select to enable this option. Reset the time and data quotas to the preset default values when a time schedule ends. **Time Limit** – Enter value for default time quota. **Data Limit** – Enter value for default data quota. **Login Permission Schedule Ends -** When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically. **Schedule** – Specify a time schedule index number for this profile.
Other Services	
Log	Activities of the user can be recorded by Syslog. **None** – Logging is disabled. **Login** – Login and logout activities are logged. **Event** – Allowed and blocked traffic are logged. **All** – Both Login and Event types are logged.
Allow this profile to be used by	This option is available for profiles with index number 3 to 200. **Internal RADIUS-** Check the box to enable security authenticated via internal RADIUS server. **Local 802.1X -** Check the box to enable security authenticated via internal 802.1X server.

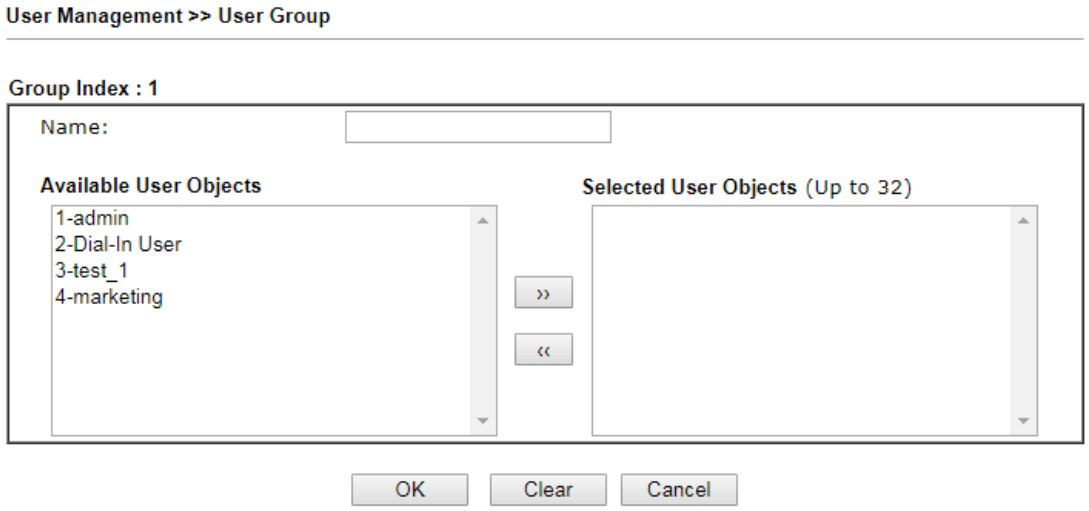
Click **OK** to save changes, **Clear** to restore settings to factory defaults, or **Cancel** to discard changes. Click **Refresh** to reload the page with the most recent data usage information (data and time quotas).

VI-3-3 User Group

This page allows you to place multiple user profiles into groups. These groups can be used to set up filter rules in **Firewall>>General Setup**.



Click an index number link to its setup page:



Available settings are explained as follows:

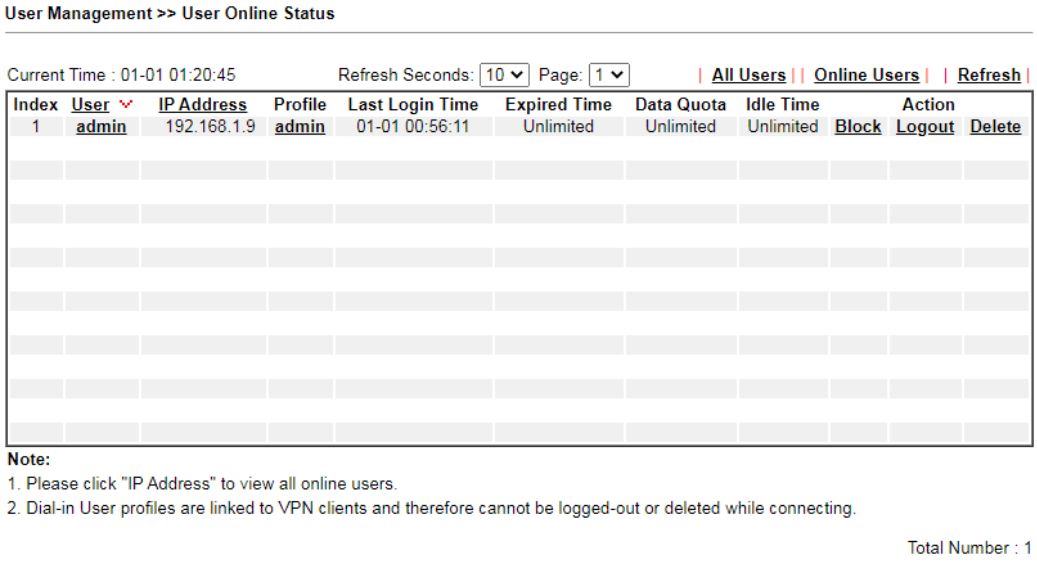
Item	Description
Name	Name that identifies this user group.
Available User Objects	Shows a list of User Objects that have not been placed into the current group.

>> <<	Click >> to move selected user objects in the Available User Objects on the left to the Selected User Objects on the right, thus adding them to the current group. Click << to move selected user objects in the Selected User Objects on the right to the Available User Objects on the left, thus removing them from the current group.
Selected Keyword Objects	Shows a list of User Objects that have been placed into the current group.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To remove all user objects from the current group, click **Clear**.

VI-3-4 User Online Status

This page displays the users that are currently logged into the router. The list refreshes periodically to show the most up-to-date information.



Available settings are explained as follows:

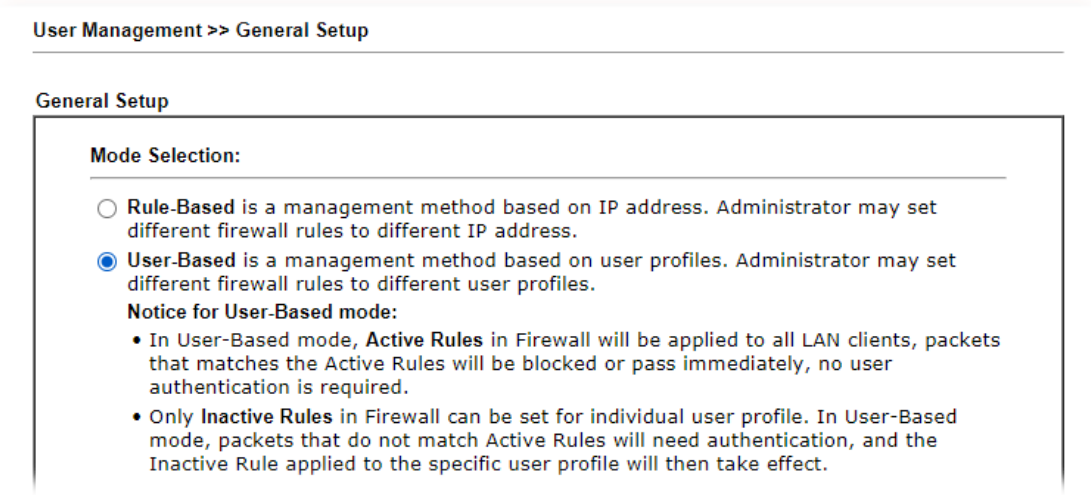
Item	Description
Refresh Seconds	The time interval between automatic screen refreshes, in seconds. Select one of 10, 15 and 30 seconds.
Refresh	Click to manually refresh the displayed data.
Index	Index of the user entry.
User	The name of the user that is logged on. Clicking this will bring up the following page which allows setting time and data quotas of the user. For details, refer to the description on the **Enable Time Quota** and **Enable Data Quota** items in the **User Profile** section.
IP Address	IP LAN address of the device that initiated the login.
Profile	Name of the user profile. If the logged-in user is a VPN user, Dial-in User will be displayed. Otherwise it will be the same as User.

Last Login Time	The most recent login time of the user.
Expired Time	The expiration time of the current login session.
Data Quota	Display the quota for data transmission. The remaining data quota of this login session.
Idle Time	Amount of time the session has been idled.
Action	**Block** – Stops user from accessing the Internet. **Unblock** –Resumes Internet access of a blocked user. **Logout** – Terminates the current login session. **Delete** – Removes the user entry from the User Online Status page.

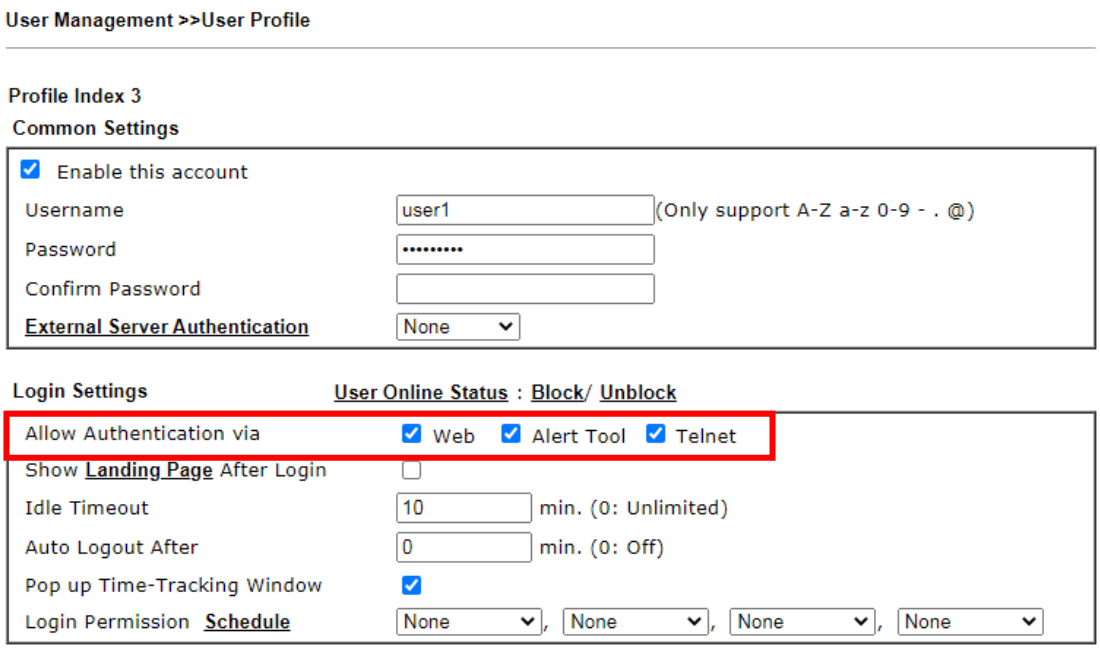
Application Notes

A-1 How to authenticate clients via User Management

Before using the function of User Management, please make sure **User-Based** has been selected as the **Mode** in the **User Management>>General Setup** page.



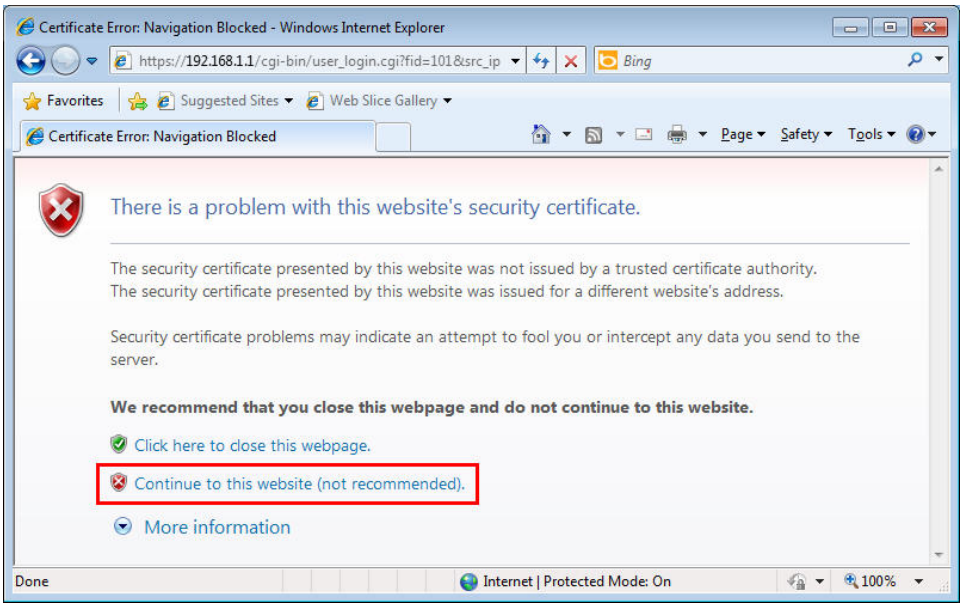
With **User Management** authentication function, before a valid username and password have been correctly supplied, a particular client will not be allowed to access Internet through the router. There are three ways for authentication: **Web**, **Telnet** and **Alert Tool**.



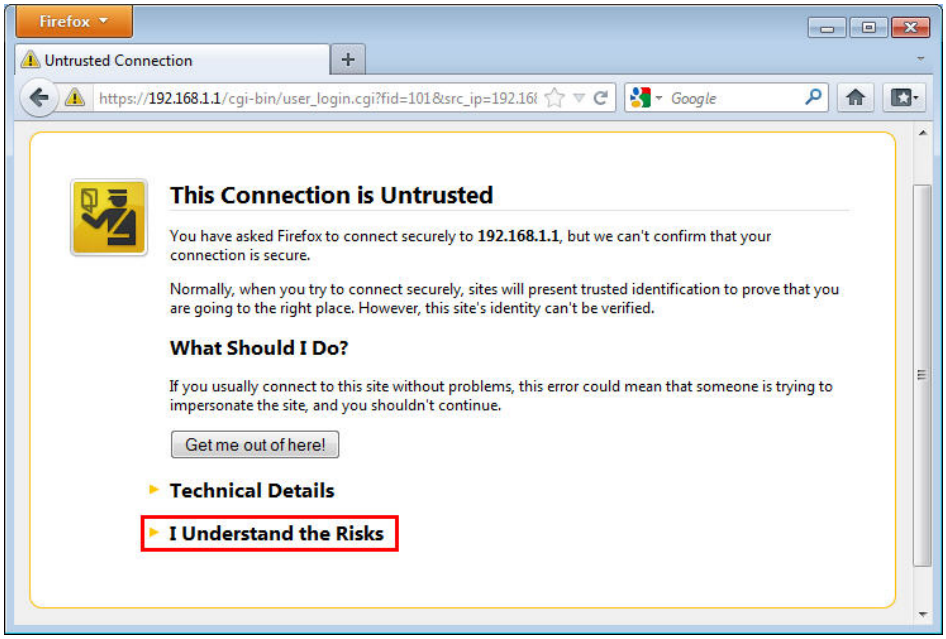
Authentication via Web

- If a LAN client who hasn't passed the authentication opens an external web site in his browser, he will be redirected to the router's Web authentication interface first. Then, the client is trying to access http://www.draytek.com and but brought to the Vigor router. Since this is an SSL connection, some web browsers will display warning messages.

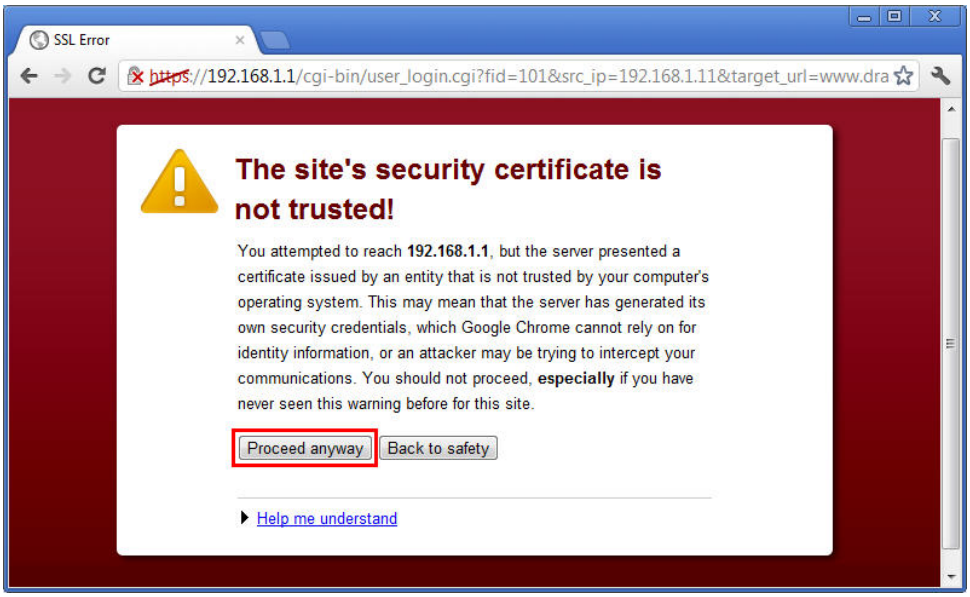
- With Microsoft Internet Explorer, you may get the following warning message. Please press **Continue to this website (not recommended)**.



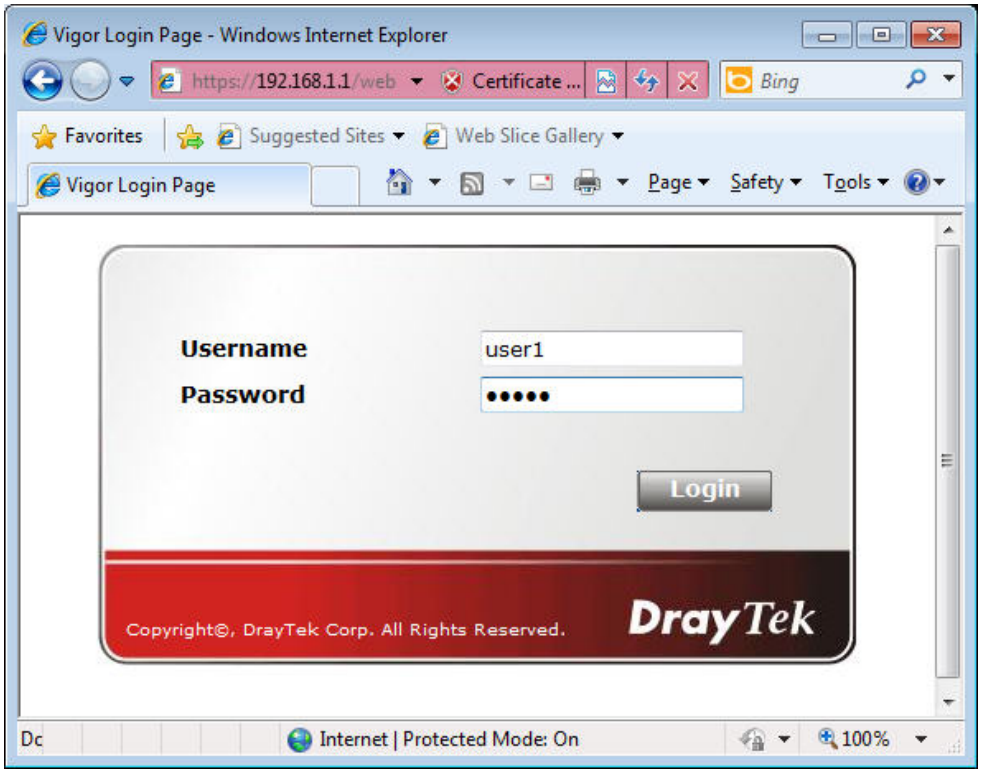
- With Mozilla Firefox, you may get the following warning message. Select **I Understand the Risks**.



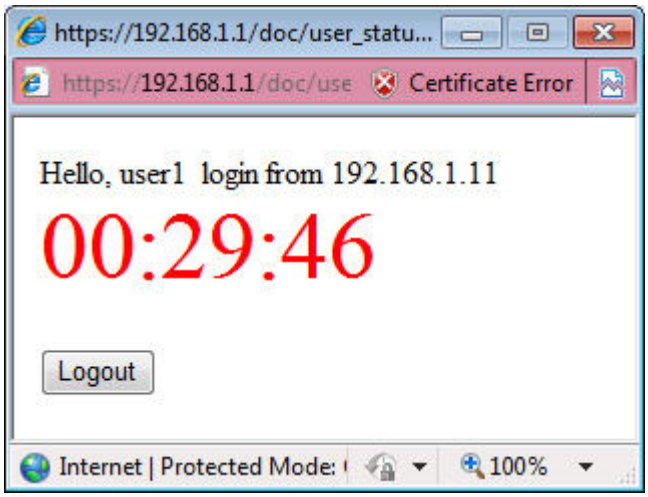
- With Chrome browser, you may get the following warning. Click **Proceed anyway**.



After that, the web authentication window will appear. Input the user name and the password for your account (defined in **User Management**) and click **Login**.

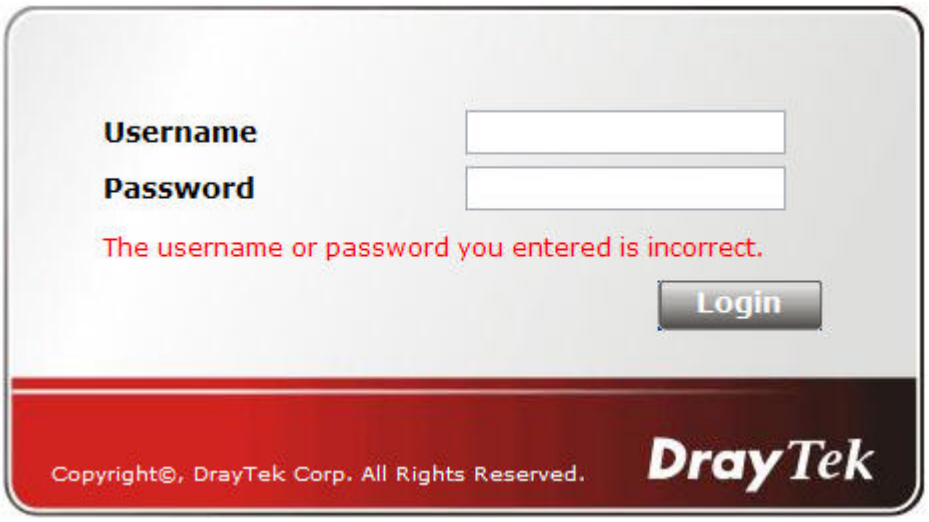


If the authentication is successful, the client will be redirected to the original web site that he tried to access. In this example, it is http://www.draytek.com . Furthermore, you will get a popped up window as the following. Then you can access the Internet.



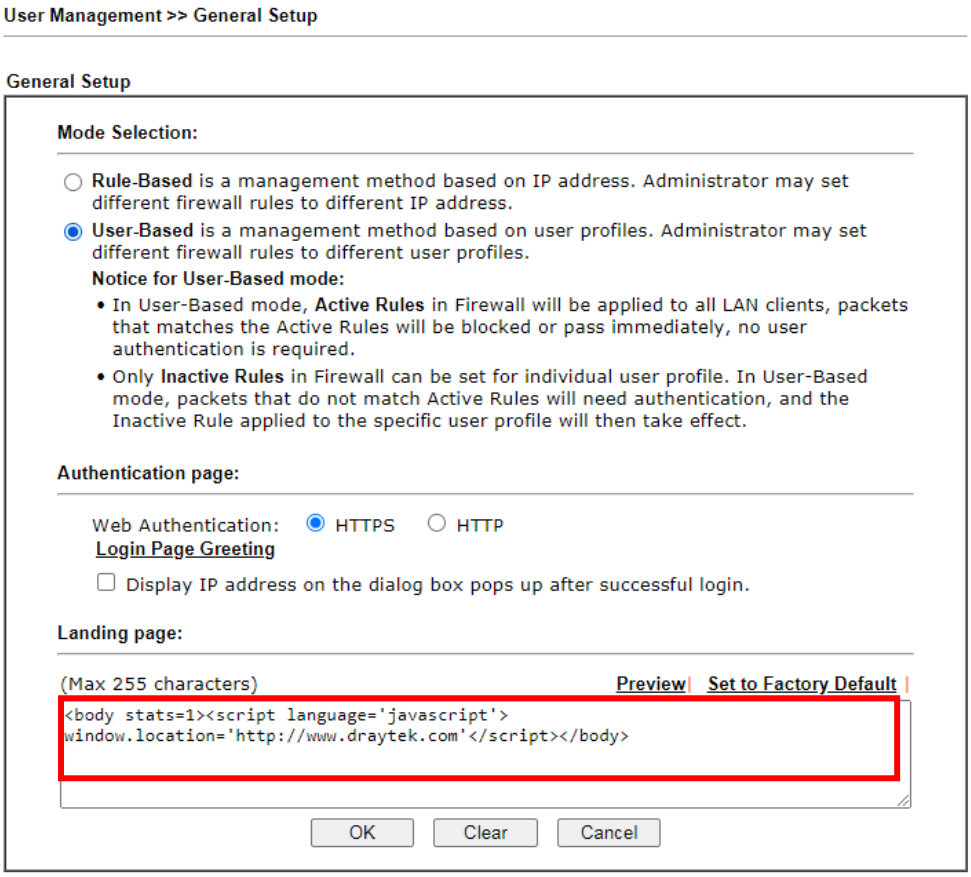
Note, if you block the web browser to pop up any window, you will not see such window.

If the authentication is failed, you will get the error message, **The username or password you entered is incorrect**. Please login again.

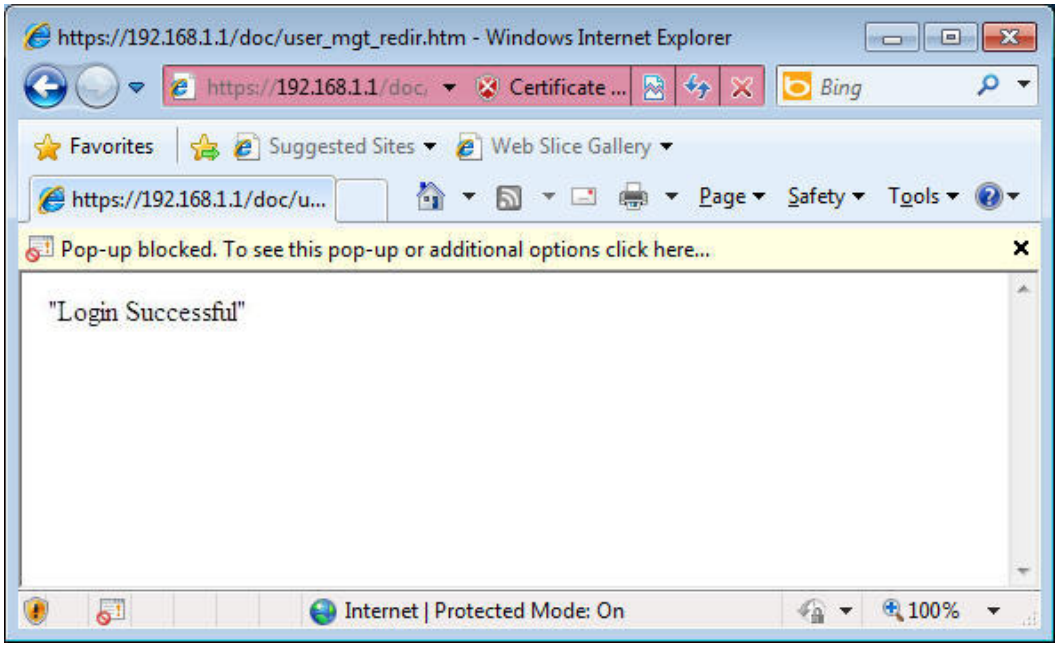


- In above description, you access an external web site to trigger the authentication. You may also directly access the router's Web UI for authentication. Both HTTP and HTTPS are supported, for example http://192.168.1.1 or https://192.168.1.1 . Replace 192.168.1.1 with your router's real IP address, and add the port number if the default management port has been modified.

  If the authentication is successful, you will get the **Welcome Message** that is set in the **User Management >> General Setup** page.



With the default setup **<body stats=1><script language='javascript'> window.location='http://www.draytek.com'</script></body>,** you will be redirected to http://www.draytek.com . You may change it if you want. For example, you will get the following welcome message if you enter **Login Successful** in the **Welcome Message** table.

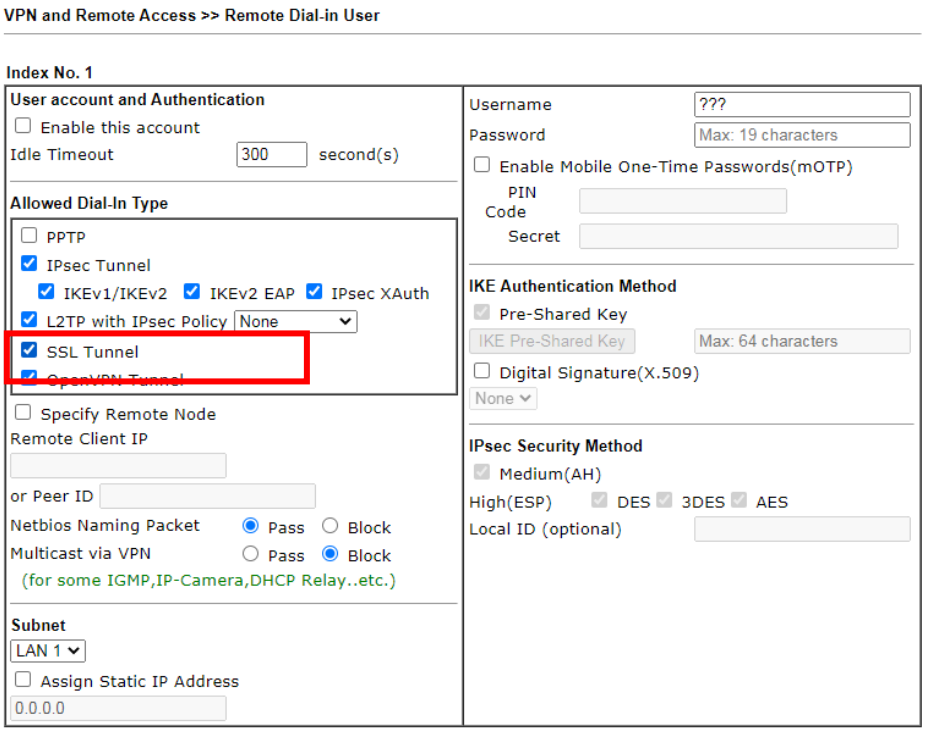


Also you will get a **Tracking Window** if you don't block the pop-up window.

- Don't setup a user profile in **User Management** and a VPN Remote Dial-in user profile with the same Username. Otherwise, you may get unexpected result. It is because the VPN Remote Dial-in User profiles can be extended to the User profiles in User Management for authentication.

There are two different behaviors when a User Management account and a VPN profile share the same Username:

- If **SSL Tunnel** or **SSL Web Proxy** is enabled in the VPN profile, the user profile in User Management will always be invalid for Web authentication. For example, if you create a user profile in User Management with **chaochen/test** as username/password, while a VPN Remote Dial-in user profile with the same username "chaochen" but a different password "1234", you will always get error message **The username or password you entered is incorrect** when you use **chaochen/test** via Web to do authentication.

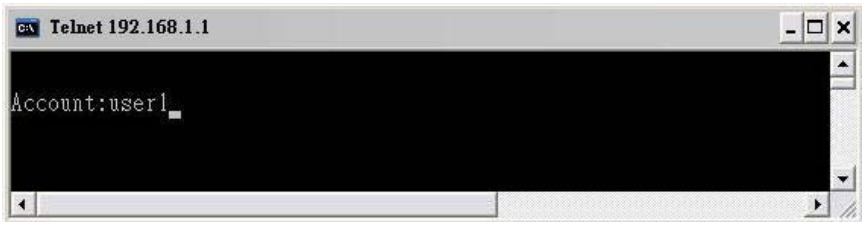


- If **SSL Tunnel** or **SSL Web Proxy** is disabled in the VPN profile, a User Management account and a remote dial-in VPN profile can use the same Username, even with different passwords. However, we recommend you to use different usernames for different user profiles in User Management and VPN profiles.

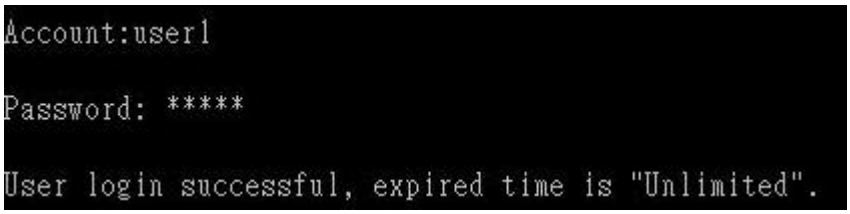
Authentication via Telnet

The LAN clients can also authenticate their accounts via telnet.

1. Telnet to the router's LAN IP address and input the account name for the authentication:



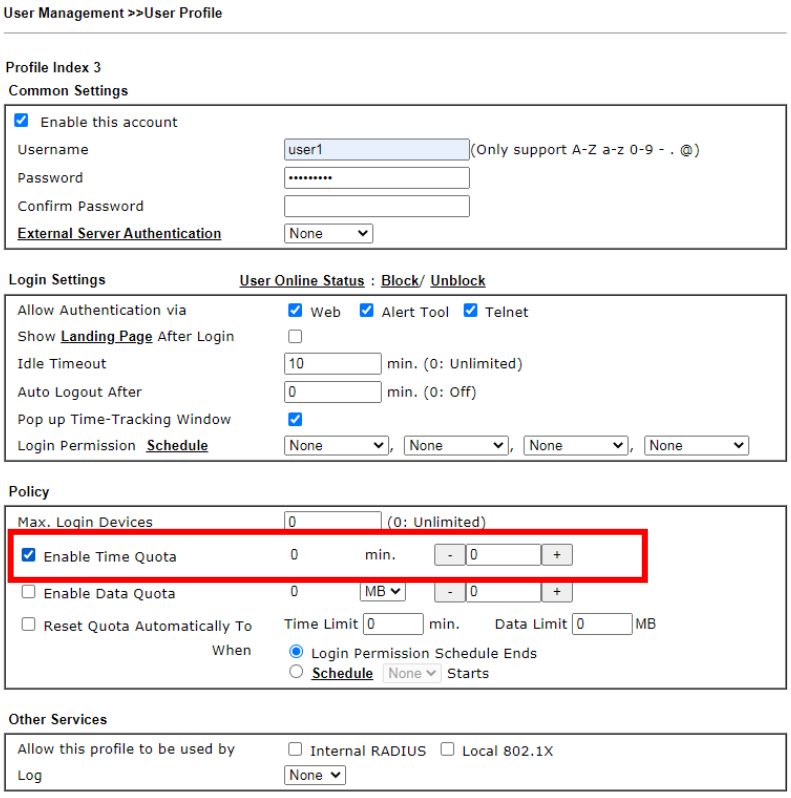
2. Enter the password for authentication and press **Enter**. The message **User login successful** will be displayed with the expired time (if configured).



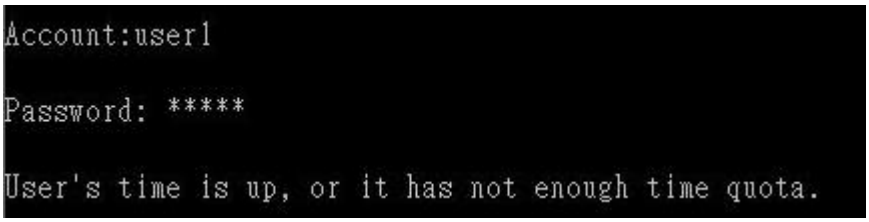
Info

Here expired time is "Unlimited" means the Time Quota function is not enabled for this account. After login, this account will not be expired until it is logout.

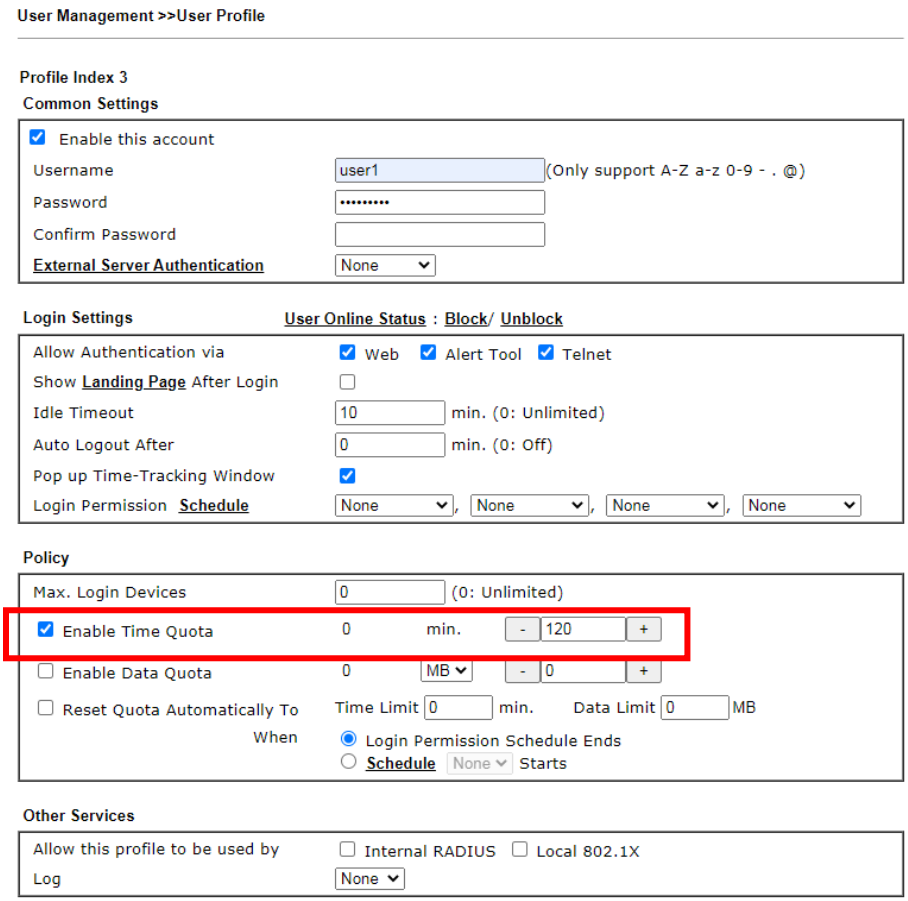
3. In the Web interface of router, the configuration page of **Time Quota** is shown as below.



4. If the Time Quota is set with “0” minute, you will get the following message which means this account has no time quota.



If the **Time Quota** is enabled and time is *not* 0 minute,



You will get the following message. The expired time is shown after you login.

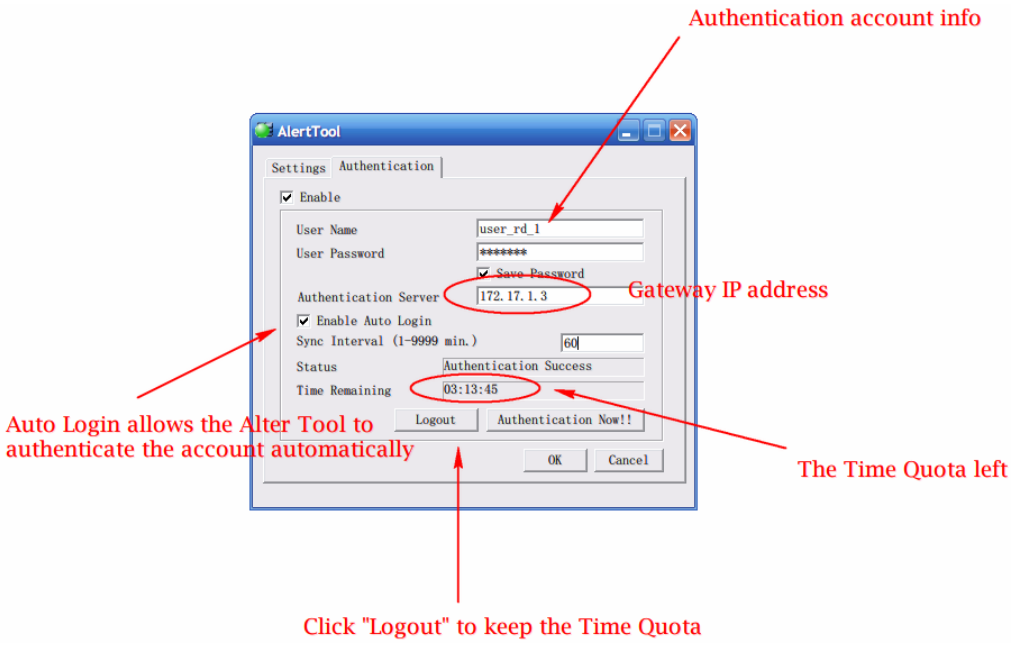
After you run out the available time, you can’t use this account any more until the administrator manually adds additional time for you.

Authentication via VigorPro Alert Notice Tool

Authentication via Web or Telnet is convenient for users; however, it has some limitations. The most advantage with VigorPro Alert Notice Tool to operate the authentication is the ability to do **auto login**. If the timeout value set on the router for the user account has been reached, the router will stop the client computer from accessing the Internet until it does an authentication again. Authentication via VigorPro Alert Notice Tool allows user to setup the re-authentication interval so that the utility will send authentication requests periodically. This will keep the client hosts from having to manually authenticate again and again.

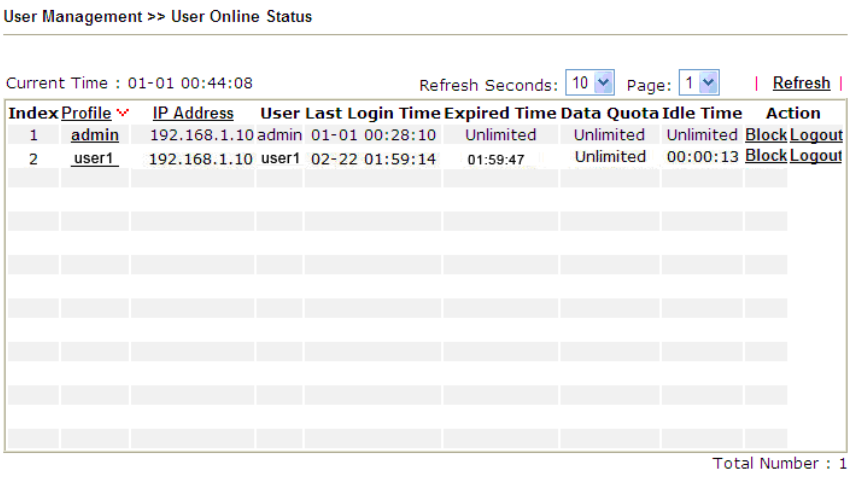
The configuration of the VigorPro Alert Notice Tool is as follows:

1. Click **Authenticate Now!!** to start the authentication immediately.



2. You may get the **VigorPro Alert Notice Tool** from the following link: http://www.draytek.com/user/SupportDLUtility.php

Info 1	Any modification to the Firewall policy will break down the connections of all current users. They all have to authenticate again for Internet access.
Info 2	The administrator may check the current users from **User Online Status** page.

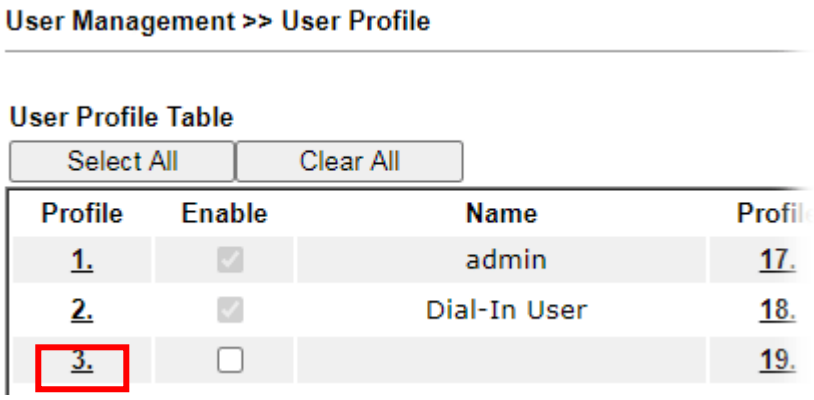


A-2 How to use Landing Page Feature

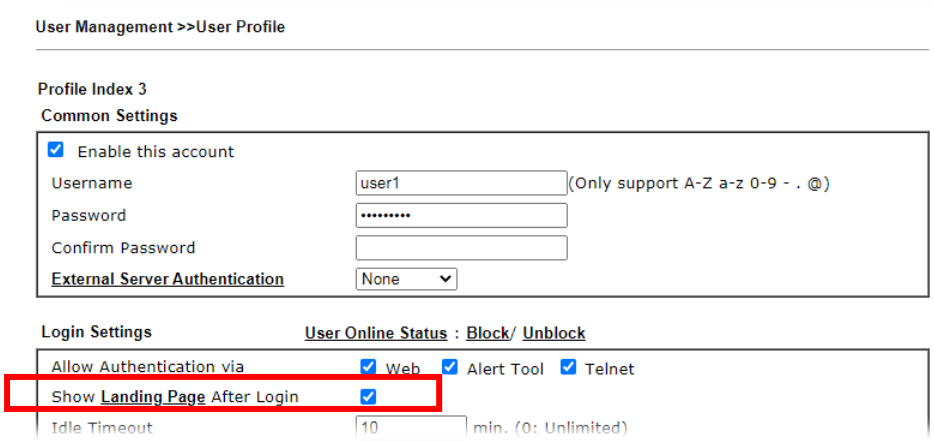
Landing Page is a special feature configured under **User Management**. It can specify the message, content to be seen or specify which website to be accessed into when users try to access into the Internet by passing the authentication. Here, we take Vigor2135 series router as an example.

Example 1 : Users can see the message for landing page after logging into Internet successfully

1. Open the web user interface of Vigor2135.
2. Open **User Management -> General Setup** to get the following page. In the field of **Landing Page**, please Enter the words of "**Login Success**". Please note that the maximum number of characters to be typed here is 255.
3. Now you can enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.



4. In the following page, check the box of **Landing page** and click **OK** to save the settings.



5. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please Enter the correct username and password.

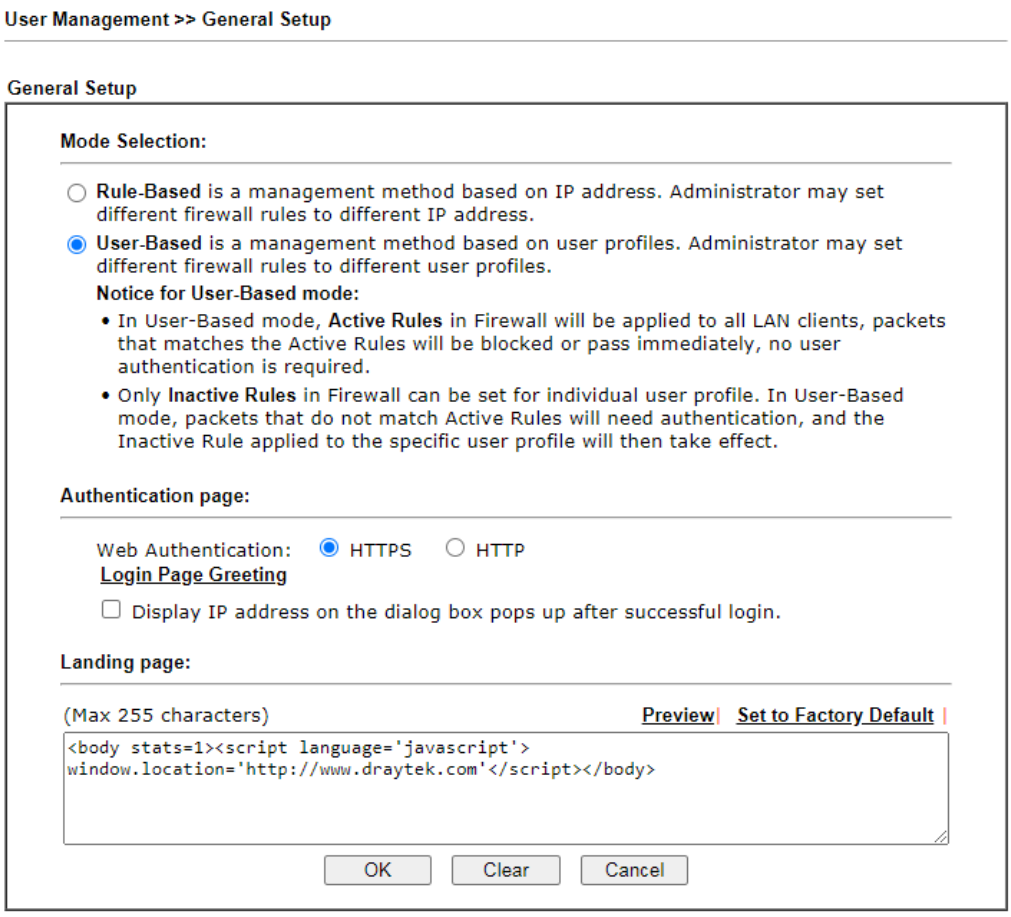
6. Click **Login**. If the logging is successful, you will see the message of Login Success from the browser you use.

Example 2：The system will connect to http://www.draytek.com automatically after logging into Internet successfully

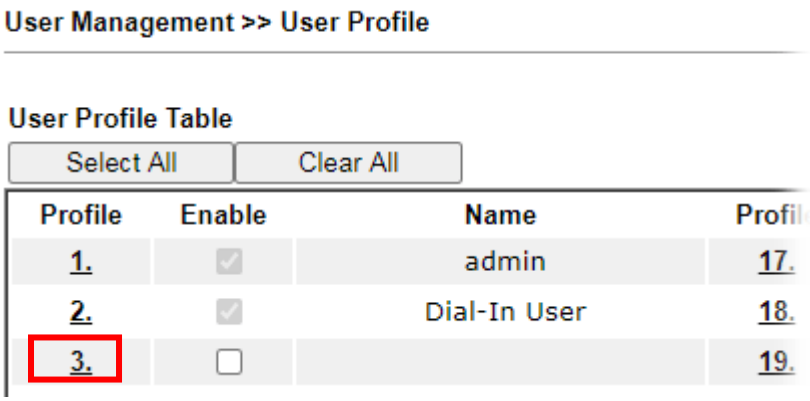
1. In the field of **Landing Page**, please Enter the words as below:

   “ <body stats=1><script language='javascript'>

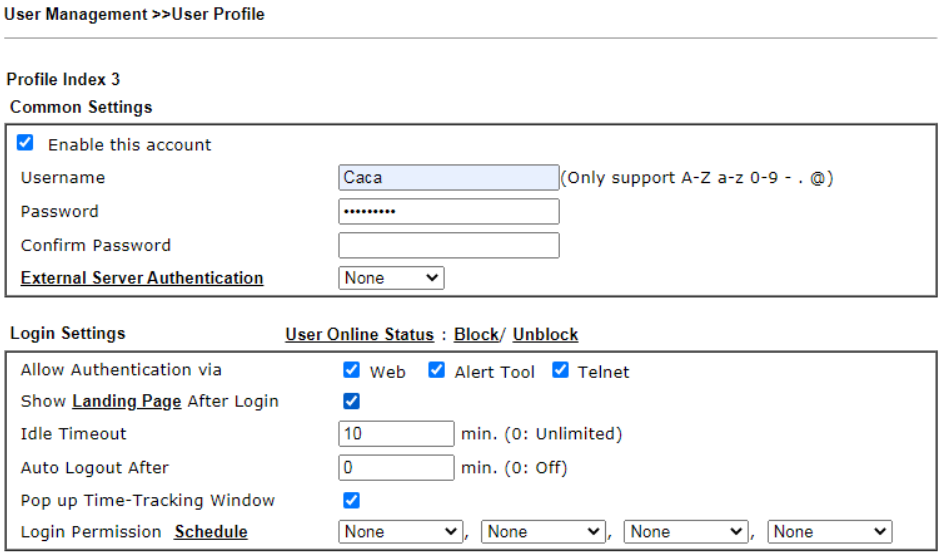
   window.location='http://www.draytek.com'</script></body>”



2. Next, enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.

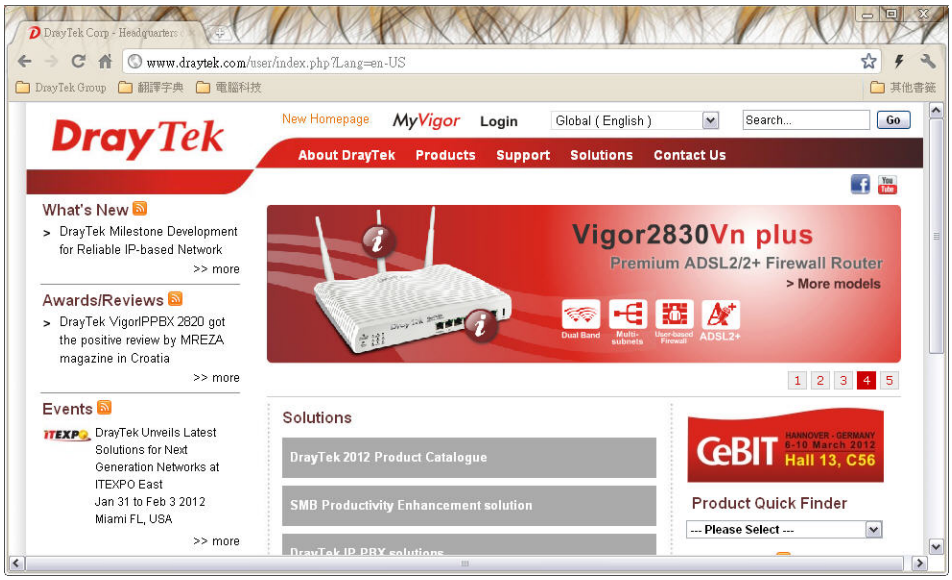


3. In the following page, check the box of **Landing page** and click **OK** to save the settings.



4. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please Enter the correct username and password.

5. Click **Login**. If the logging is successful, you will be directed into the website of www.draytek.com.



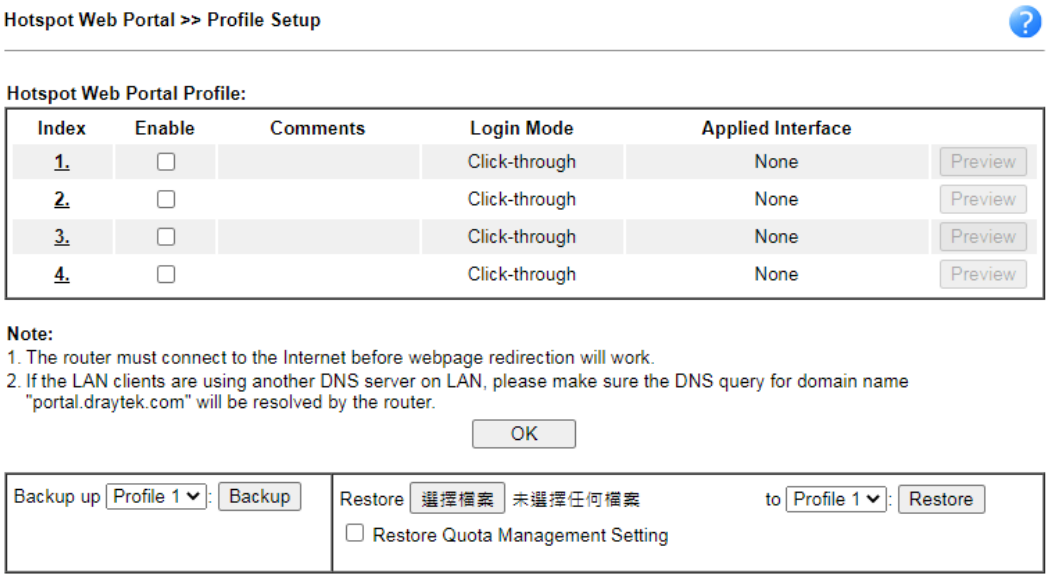
VI-4 Hotspot Web Portal

The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

Web User Interface

VI-4-1 Profile Setup

Select **Profile Setup** to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.



Available settings are explained as follows:

Item	Description
Index	Click the index number link to view or update the profile settings.
Enable	Check the box to enable the profile.
Comments	Shows the description of the profile.
Login Mode	Shows the login mode used by the profile. See the section

	Login Mode for details.
Applied Interface	Shows the interfaces to which this profile applies.
Preview	Click this button to preview the Hotspot Web Portal page that will be displayed to users.
Backup up	**Profile list** - Select a source profile. **Backup** - Click to save the configuration file based on the selected source profile.
Restore ...	**Select** - Click to choose a configuration file. **to**.. - Select a destination profile. It will be restored by the selected configuration file. **Restore** - Click to perform the restoration job. **Restore Quota Management Setting** - If selected, the quota management setting also will be restored onto the destination profile.

VI-4-1-1 Login Method

There are four login methods to choose from for authenticating network clients: **Skip Login**, **Click Through**, **Social Login**, **PIN Login**, and **Social or PIN Login**. Each login mode will present a different web page to users when they connect to the network.

(A) Skip Login, landing page only

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

(B) Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking **Accept** on the page, users will be directed to the landing page (defined in Captive Portal URL) and be granted access to the Internet.

(C) Various Hotspot Login

An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook account, Google account, PIN code, password for RADIUS sever, they will be directed to the landing page and be granted access to the Internet.

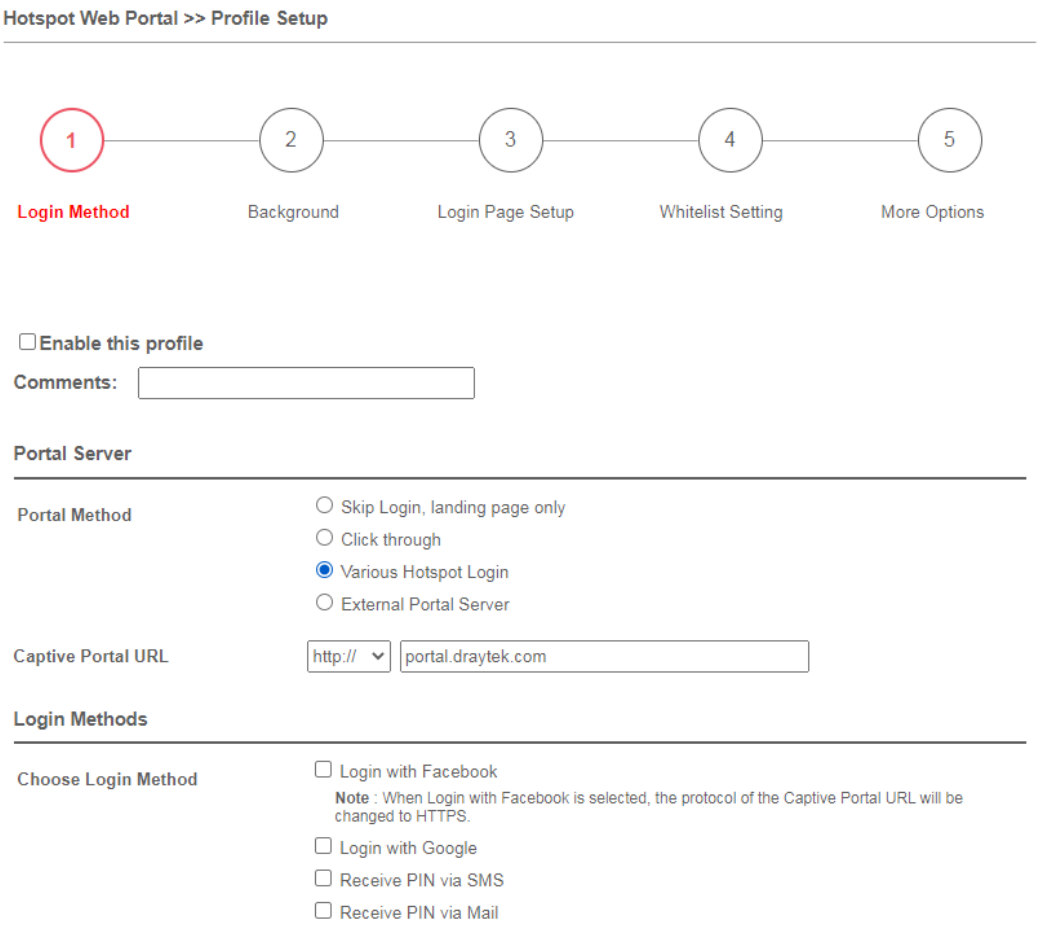
(D) External Portal Server

External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.

VI-4-1-2 Steps for Configuring a Web Portal Profile

1 Login Method

Click the index link (e.g., #1) of the selected profile to display the following page.



Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable this profile.
Comments	Enter a brief description to identify this profile.
Portal Server	
Portal Method	There are four methods to be selected as for portal server. ○ Skip Login, landing page only ○ Click through ◉ Various Hotspot Login ○ External Portal Server
When Skip Loging, landing page only or Click through is selected as Portal Method	
Captive Portal URL	Enter the captive portal URL.
When Various Hotspot Login is selected as Portal Method	
Captive Portal URL	Enter the captive portal URL.
Login Methods	This setting is available when **Various Hotspot Login** is selected as the portal method. **Choose Login Method -** Select one or more desired login methods. ● Login with Facebook ● Login with Google ● Receive PIN via SMS

	• Receive PIN via Mail • Login with RADIUS
Facebook (Login with Facebook**)**	This setting is available when **Login with Facebook** is selected as the login method. **Facebook APP ID** - Enter a valid Facebook developer app ID. If you do not already have an app ID, refer to section A-1 *How to create a Facebook App ID for Web Portal Authentication* for instructions on obtaining an APP ID. **Facebook APP Secret** - Enter the secret configured for the APP ID entered above. Refer to section A-1 *How to create a Facebook App ID for Web Portal Authentication* for details.
Google (Login with Google)	This setting is available when **Login with Google** is selected as the login method. **Google App ID** - Enter a valid Google app ID. If you do not already have an app ID, refer to section A-2 *How to create a Google App ID for Web Portal Authentication* for instructions on obtaining an APP ID. **Google App Secret** - Enter the secret configured for the APP ID entered above. Refer to section A-2 *How to create a Google APP ID for Web Portal Authentication* for details.
SMS Provider (Receive PIN via SMS)	This setting is available when **Receive PIN via SMS** is selected as the login method. **Receiving PIN via SMS Provider** - Select the SMS Provider to send PIN notifications. The SMS providers are configured in **Objects Setting >> SMS / Mail Service Object**.
Mail Server (Receive PIN via Mail)	This setting is available when **Receive PIN via Mail** is selected as the login method. **Receiving PIN via Mail Server** - Select the mail server to send PIN notifications. The mail servers are configured in **Objects Setting >> SMS / Mail Service Object**.
Radius Server (Login with RADIUS)	This setting is available when **Login with RADIUS** is selected as the login method. **Authentication Method** – Click link to configure the external RADIUS server for authenticating web portal clients. **RADIUS MAC Authentication** – Check **Enable** to activate user authentication by MAC address. **MAC Address Format** – Select the MAC address format that is used by the RADIUS server.
When External Portal Server is selected as Portal Method	
Redirection URL	Enter the URL to which the client will be redirected.
RADIUS Server	**Authentication Method** - To configure the RADIUS server, click the External RADIUS Server link and you will be presented with the configuration page. **RADIUS MAC Authentication** - If the RADIUS server supports authentication by MAC address, enable **RADIUS MAC Authentication** and select the MAC address format that is used by the RADIUS server. **MAC Address Format** - Select the MAC address format.
Save and Next	Click to save the configuration on this page and proceed to the

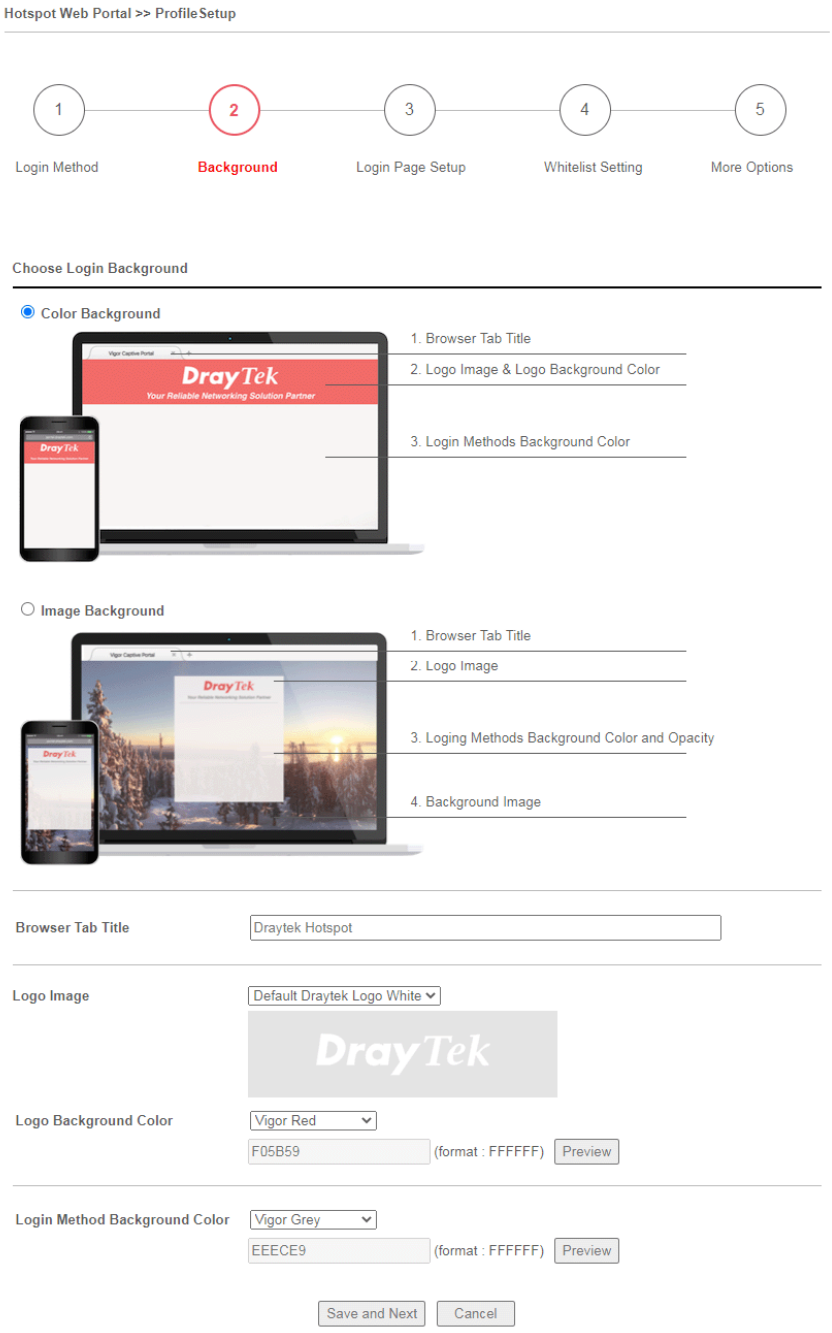
	next page.
Cancel	Click to save the configuration on this page and proceed to the next page.

If you have chosen **Skip Login, landing page only** or **External Portal Server** as the portal method, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

2 Background

If you have selected a Login Mode that requires authentication, select a background for the login page.



Available settings are explained as follows:

Item	Description
Choose Login Background	Select either **Color Background** or **Image Background** as the login page background scheme.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.
Logo Image	The DrayTek Logo will be displayed by default. However, you can

	enter HTML text or upload an image to replace the default logo.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Opacity (10 ~ 100)	Available when **Image Background** is selected. Set the opacity of the background image.
Background Image	Available when **Image Background** is selected. Click **Browse…** to select an image file (.JPG or .PNG format), then click **Upload** to upload it to the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

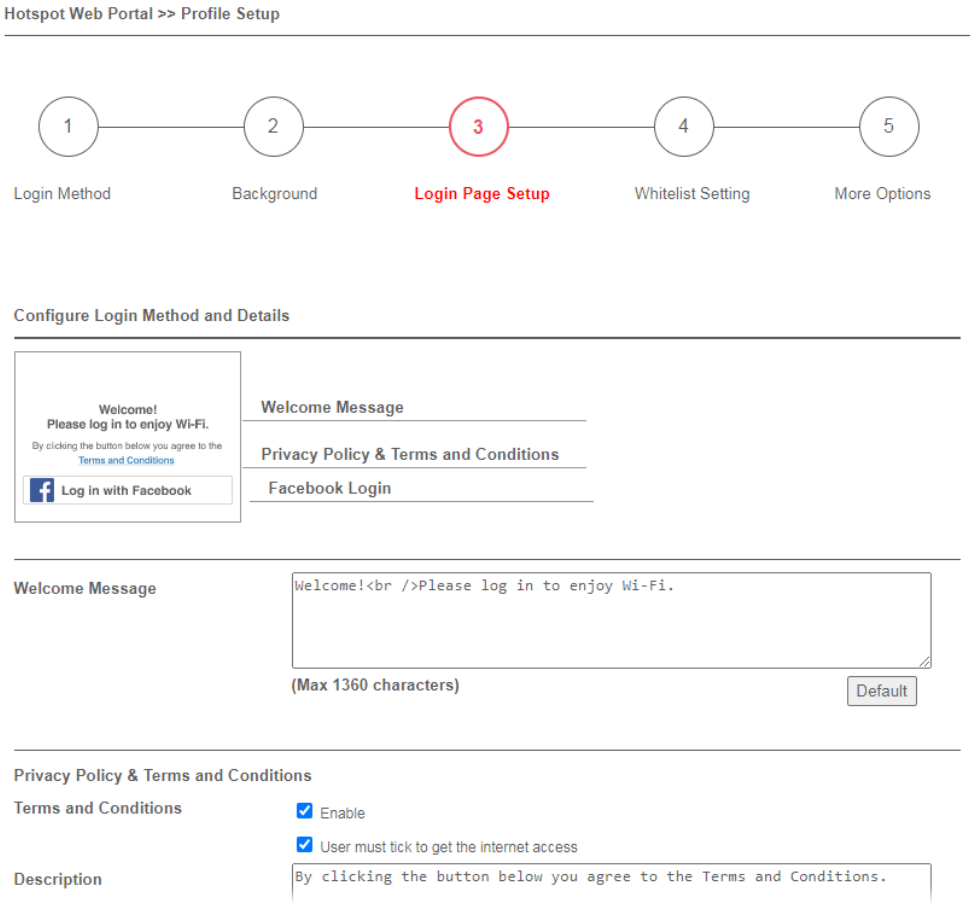
If you have selected **Skip Login, landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup.*

3 Login Page Setup

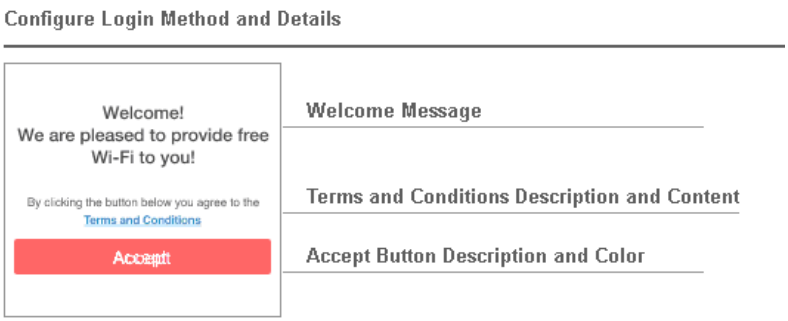
In this step you can configure settings for the login page.

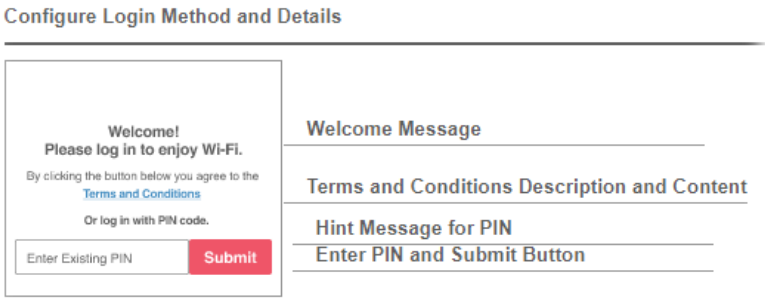
Click Through

This section describes the Login Page setup if you have selected **Click Through** as the Login Method.



Available settings are explained as follows:

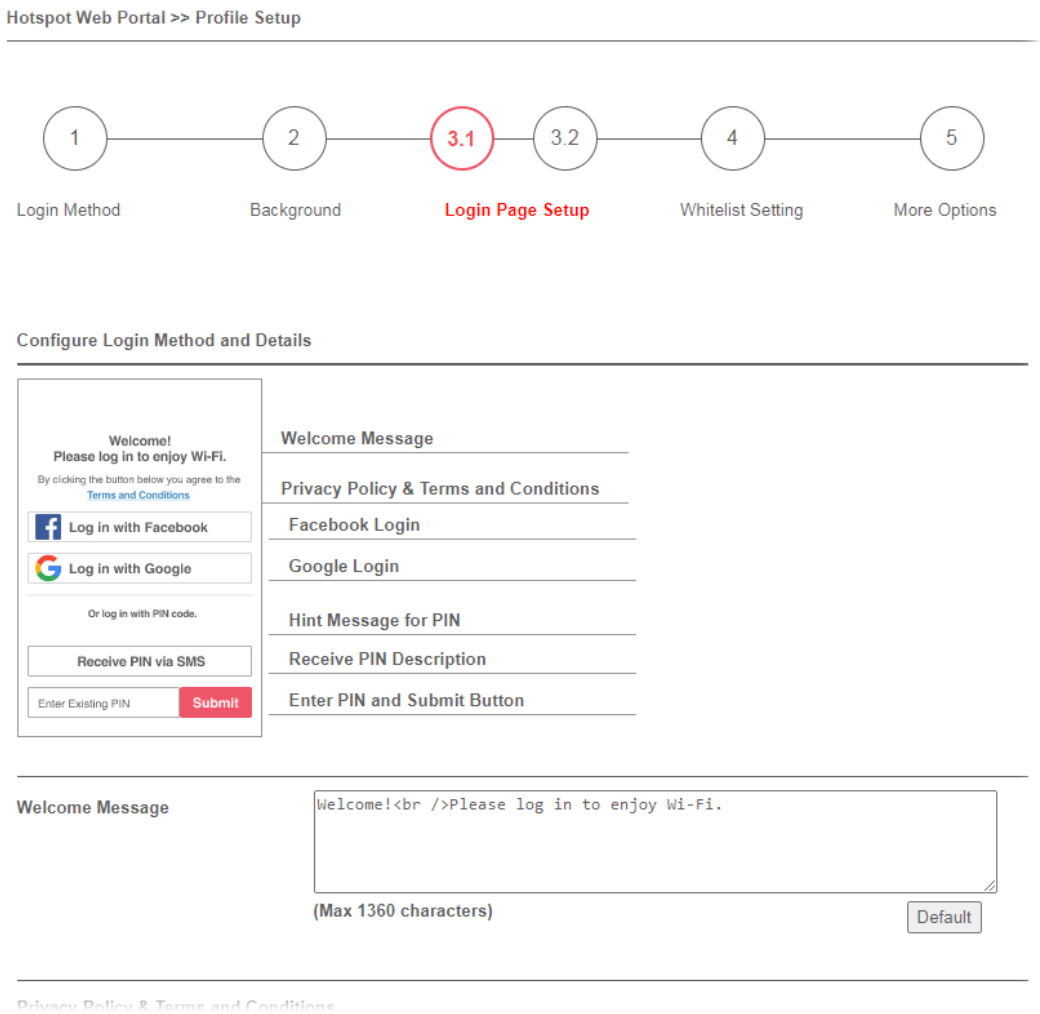
Item	Description
Login dialog will be shown as follows:  However, when **PIN with Voucher** is selected as the login method, Login dialog will be shown as follows:	



Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.
Hint Message for PIN	Enter a message to remind the PIN code.
Enter PIN Description	Enter the existing PIN code.
Submit Button Description	Enter the text to be displayed on the Submit button
Submit Button Color	Select the color of the Submit button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

Various Hotspot Login

This section describes the Login Page setup step if you have selected Various Hotspot Login the login method. You will see only settings that are relevant to the selected login method(s).



Settings that are common to Facebook, Google, PIN, and RADIUS authentication are:

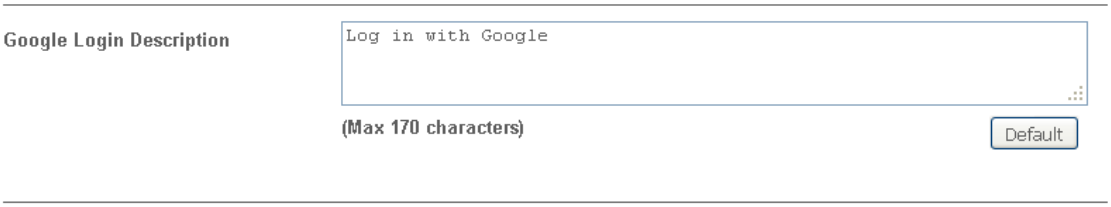
Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.

If you have selected Facebook login, the setting will appear:

Item	Description

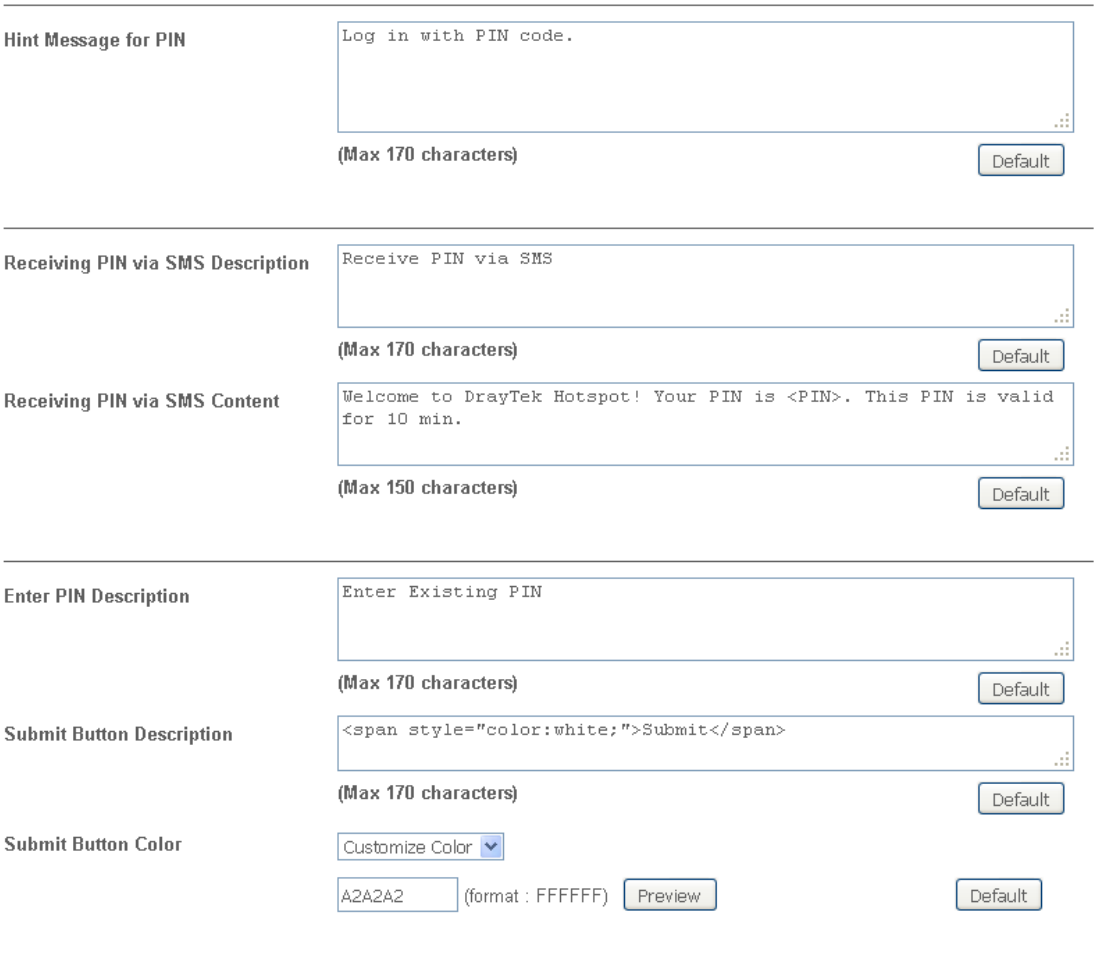
Facebook Login Description	Enter the text to be displayed on the Facebook login button.

If you have selected Google login, the setting will appear:



Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.

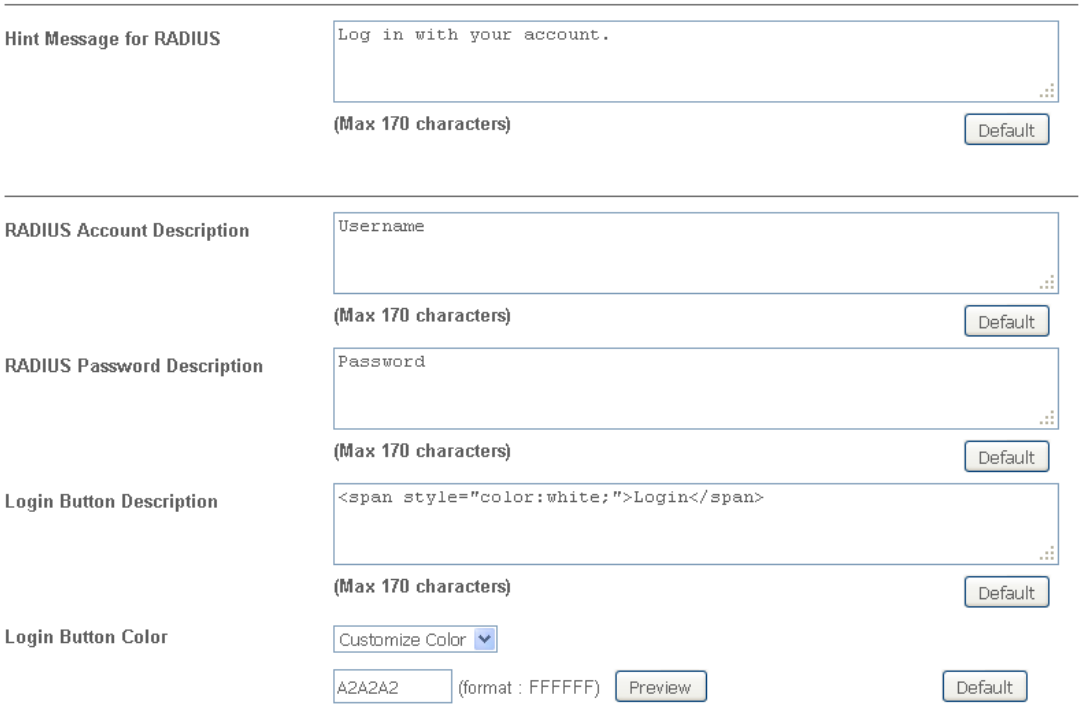
If you have selected PIN login, these settings will appear:



Item	Description
Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by **<PIN>** within the message.

Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.

If you have selected RADIUS account login, these settings will appear:



Item	Description
Hint Message for RADIUS	Enter the text used to prompt the user to login.
RADIUS Account Description	Enter the text to prompt the user to enter the username.
RADIUS Password Description	Enter the text to prompt the user to enter the password.
Login Button Description	Enter the text to be displayed on the login button.
Login Button Color	Select the color of the login button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.

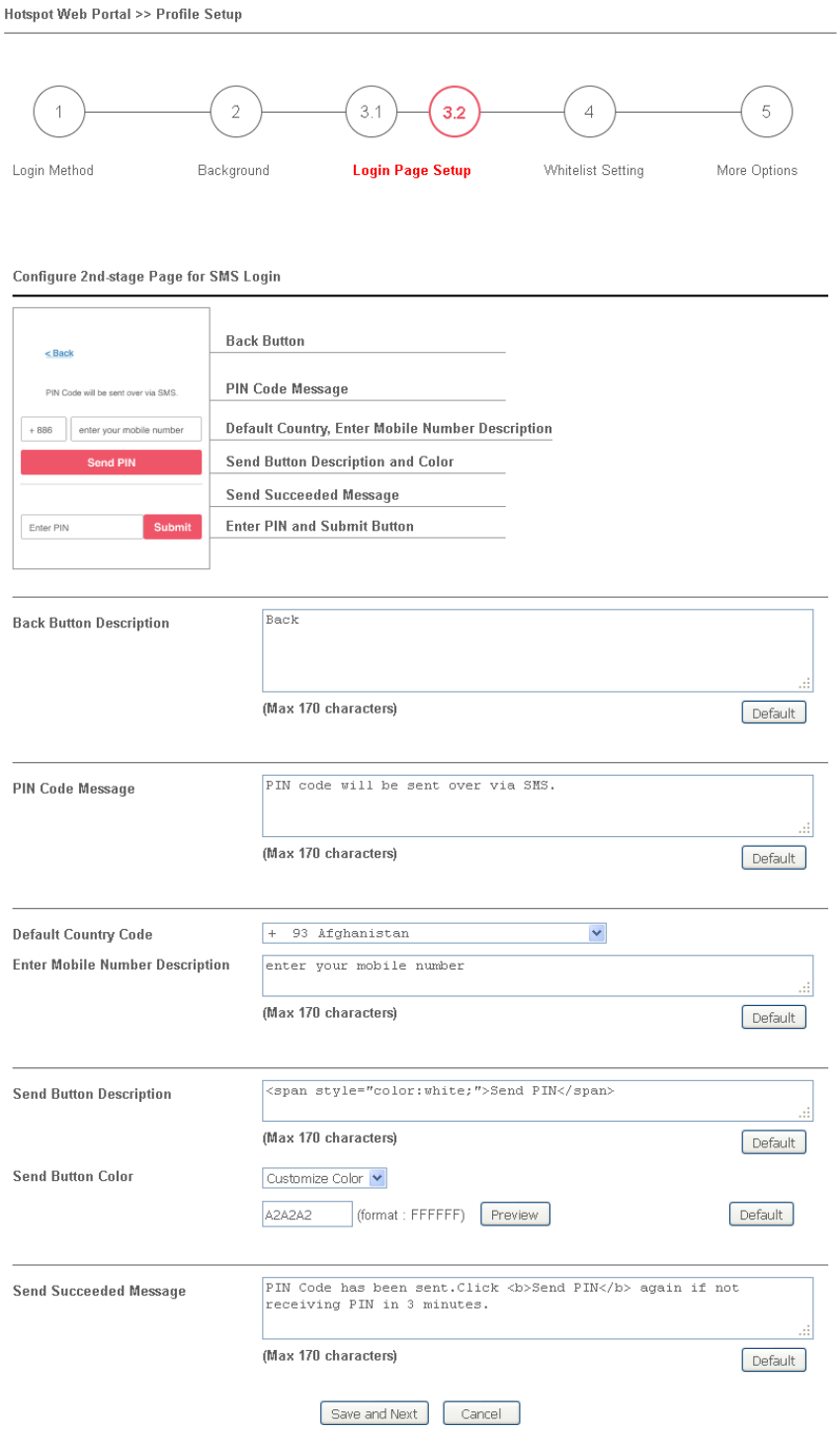
And finally, the save and cancel buttons are always displayed.

Item	Description
Save and Next	Click to save the configuration on this page and proceed to the

	next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

2nd-stage Page for PIN Login

If you have selected **PIN Login** as the login method, you will also need to configure the page that is displayed to users when they request a PIN.



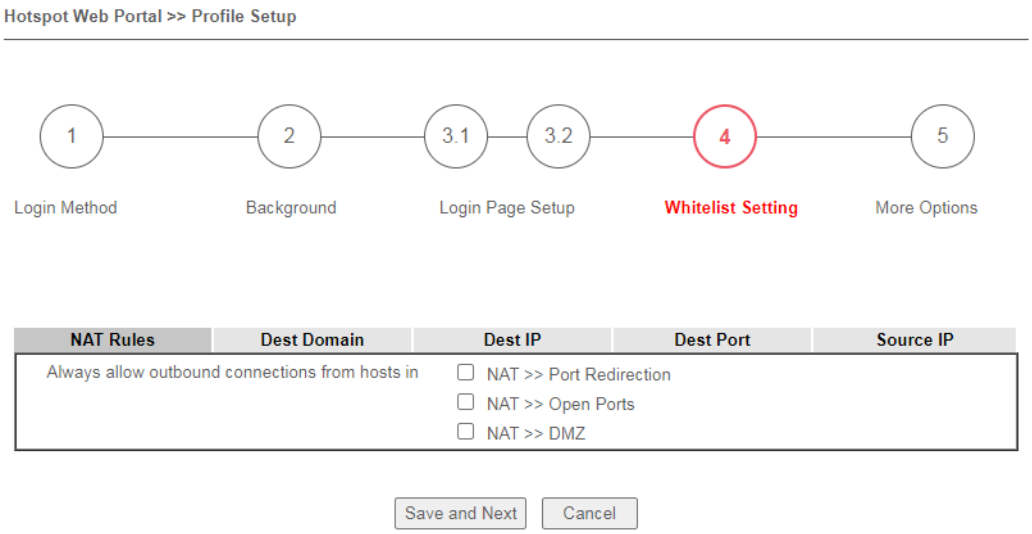
Available settings are explained as follows:

Item	Description

Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country Code	Select the default country code to be displayed using the dropdown menu.
Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

4 Whitelist Setting

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

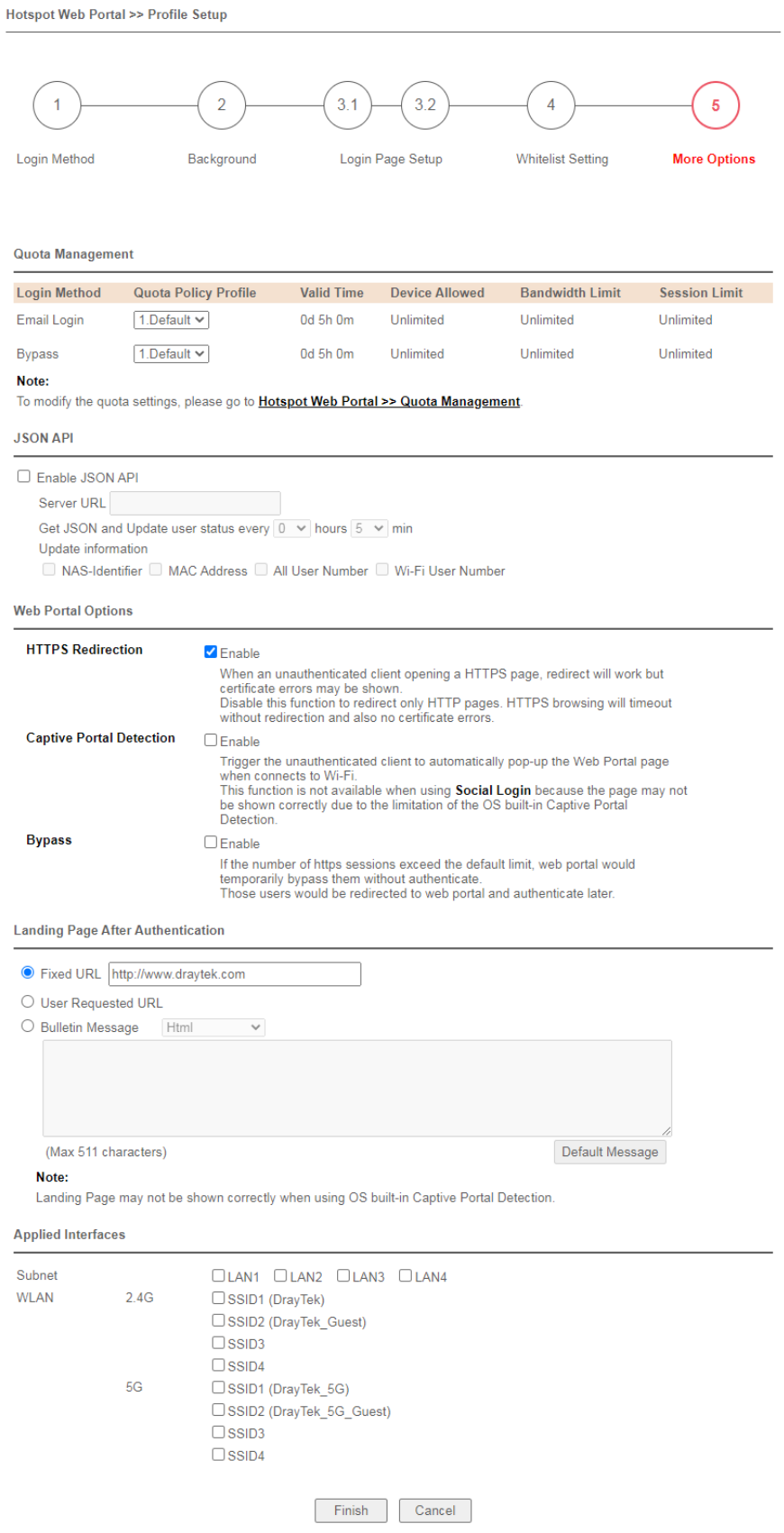


Available settings are explained as follows:

Item	Description
NAT Rules	To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal.
Dest Domain	Enter up to 30 destination domains that are allowed to be accessed.
Dest IP	Enter up to 30 destination IP addresses that are allowed to be accessed.
Dest Port	Enter up to 30 destination protocols and ports that are allowed through the router.
Source IP	Enter up to 30 source IP addresses that are allowed through the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

5 More Options

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



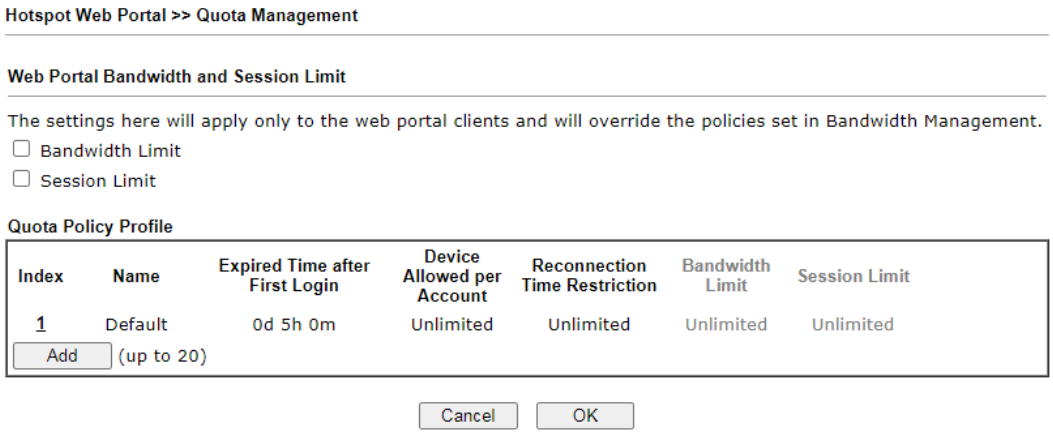
Available settings are explained as follows:

Item	Description
Quota Management	
Quota Policy Profile	Choose a policy profile to apply to web portal clients.
JSON API	
Enable JSON API	Select to enable the function. **Server URL** - Enter the URL of the server.
Web Portal Options	
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is **Social Login**, as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.
Bypass	If this option is selected, the web portal page would temporarily bypass without authentication when the number of HTTPS sessions exceed the default limit.
Landing Page After Authentication	
Fixed URL	Specifies the webpage that will be displayed after the user has successfully authenticated. The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.
User Requested URL	The user will be redirected to the URL they initially requested.
Bulletin Message	The message configured here will be briefly shown for a few seconds to the user. **Default Message –** This button is enabled when **Bulletin Message** is selected. Click to load the default text into the bulletin message textbox.
Applied Interfaces	
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
WLAN	The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Finish	Click to complete the configuration.
Cancel	Click to abort the configuration process and return to the profile summary page.

VI-4-2 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

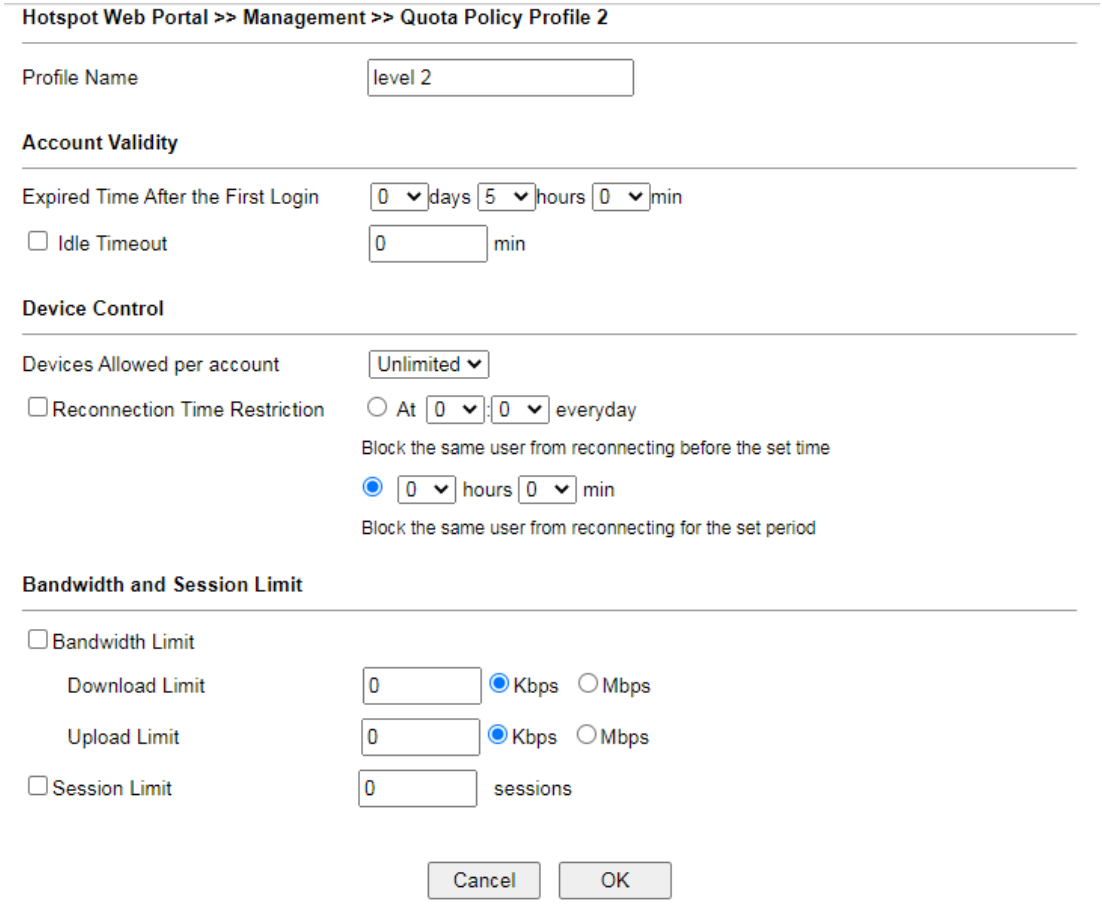
Settings configured in Quota Management will override the policies set in **Bandwidth Management>>Bandwidth Limit** and **Bandwidth Management>>Limit**.



Available settings are explained as follows:

Item	Description
Bandwidth Limit	Check the box to override the policy configured in **Bandwidth Management>>Bandwidth Limit.**
Session Limit	Check the box to override the policy configured in **Bandwidth Management>>Session Limit.**
Quota Policy Profile	**Add** - Create up to 20 policy profiles in such page.

To create a new quotal policy profile, click **Add** to open the followining page.



Available settings are explained as follows:

Item	Description
Profile Name	Enter a name for a new profile.
Account Validity	Set the duration for which the login is valid. **Expired Time After the First Login** – Sets the days, hours, and minutes. After the login has expired, Vigor router will block the client from accessing the network/Internet. **Idle Timeout** – When this option is selected, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed.
Device Control	Set the maximum number of devices that can be connected for each account, and the time restriction for the client accessing Internet via the web portal. **Devices Allowed per account** – Use the drop-down list to select the maximum number of devices that can be connected to the network using the same account. **Reconnection Time Restriction** – Blocks the account from being used to connect devices to the network in one of two ways: ● **At …. Everyday** – After the login expires, the account cannot be used to connect devices to the network until the set time of day. ● **Hours.. min** – After the login expires, the account cannot be used to connect devices to the network for a set period of time.
Bandwidth and Session Limit	**Bandwidth Limit** – Check the box to configure bandwidth limit for web portal client.

	• **Download/Upload Limits** – Set the maximum upload and download speeds. **Session Limit**- Check the box to configure a maximum session limit for web portal clients.

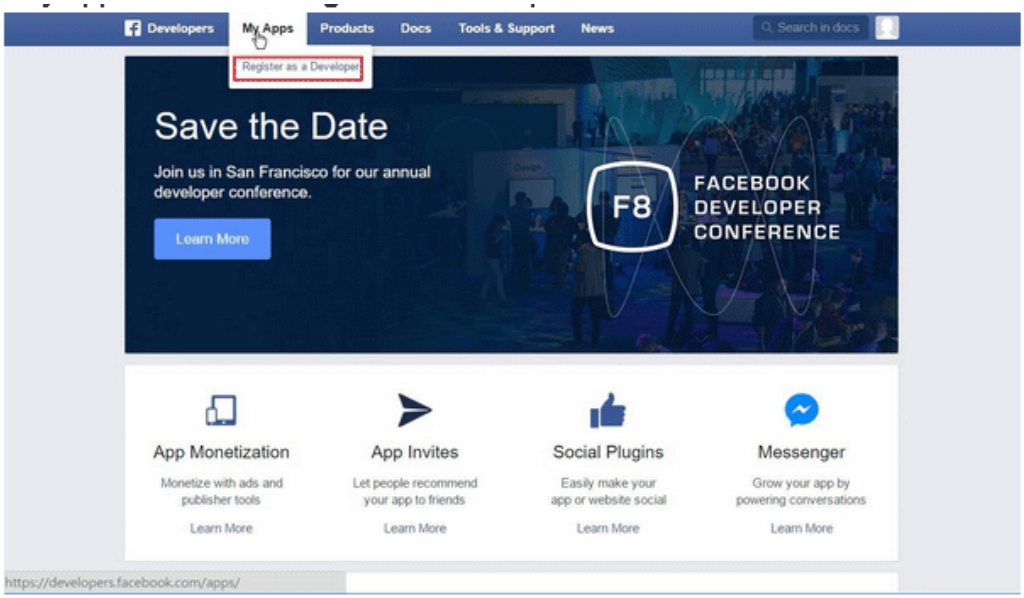
After finishing all the settings here, please click **OK** to save the configuration.

Application Notes

A-1 How to create Facebook APP for Web Portal Authentication?

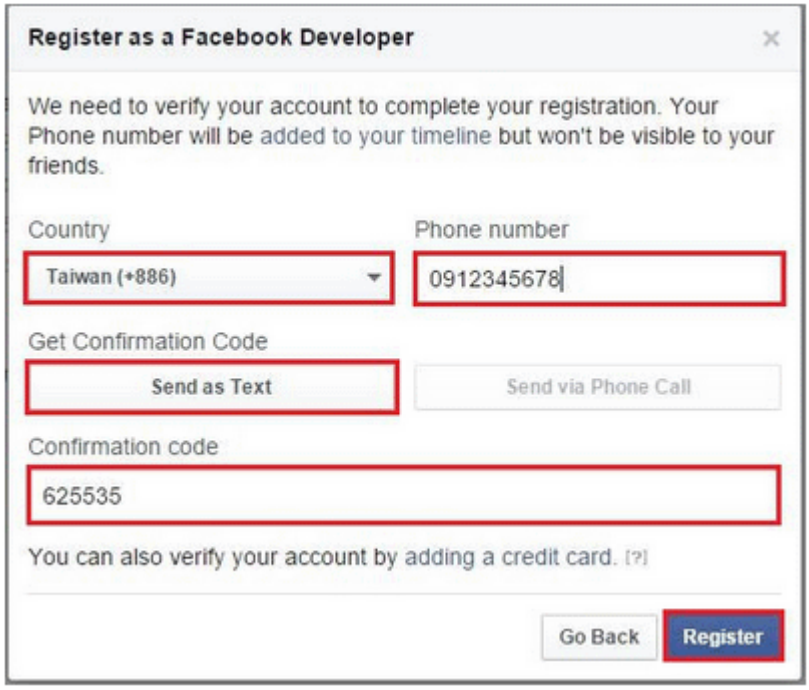
The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

1. Register as FB Developer: Go to https://developers.facebook.com/ and login the FB account.
2. Register the Facebook account as a Developer (If the account has been verified previously, this step can be skipped.)
3. Click **My Apps** then choose **Register as Developer.**

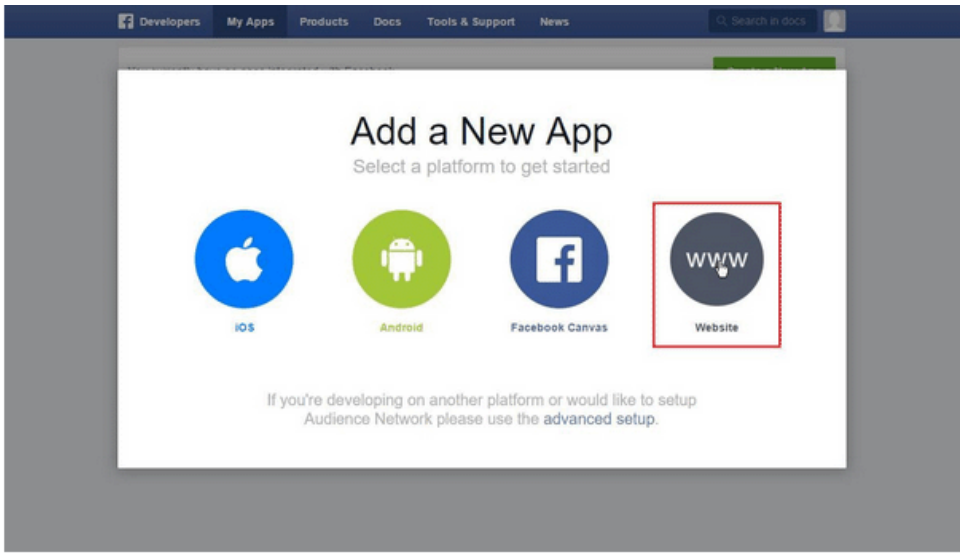


4. Switch to **YES** then click **Next** on pop-up window.

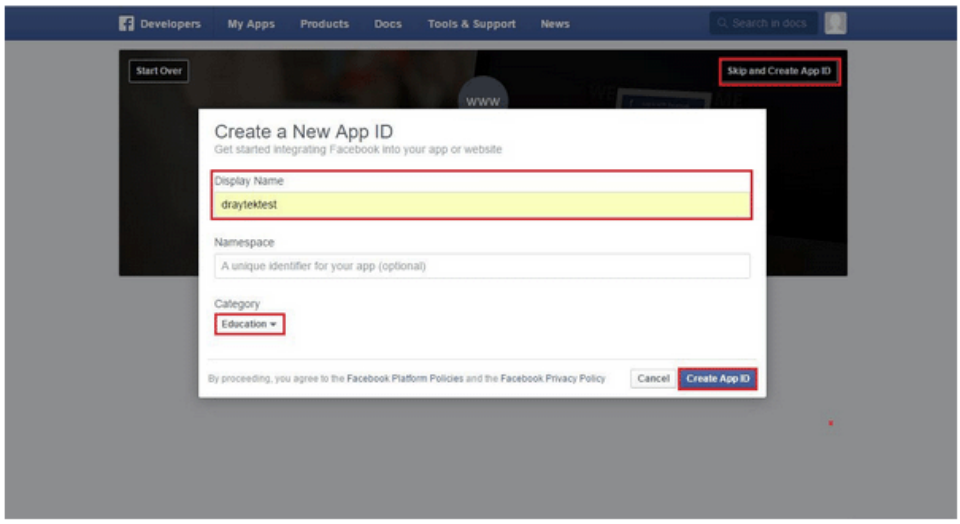
5. Choose **country** then type **phone number**, click **Send as Text** in Get Confirmation Code. Wait confirmation code message received then enter the **confirmation code.** Click **Register** to finish the register process.



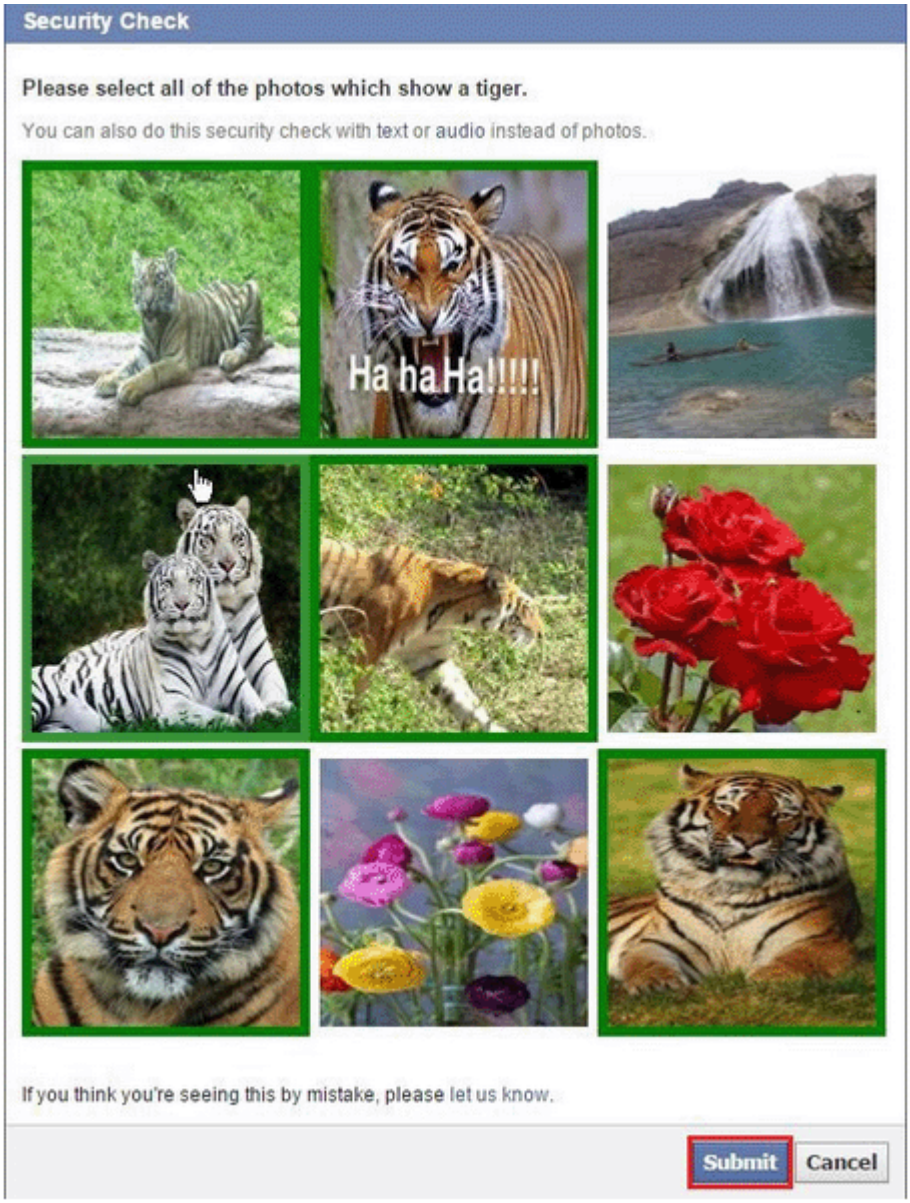
6. Add a New App. Click on **My Apps > Add a New App.** Choose **Website** platform.



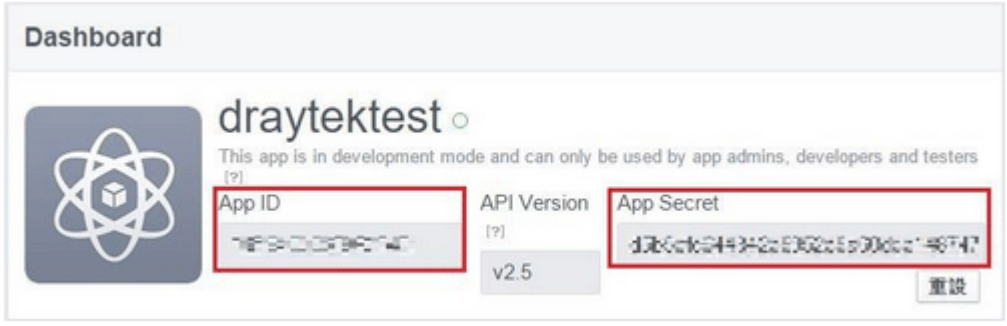
7. Click **Skip and Create App ID** on first use. Type **Display Name.** Choose **Category.** Click **Create App ID.**



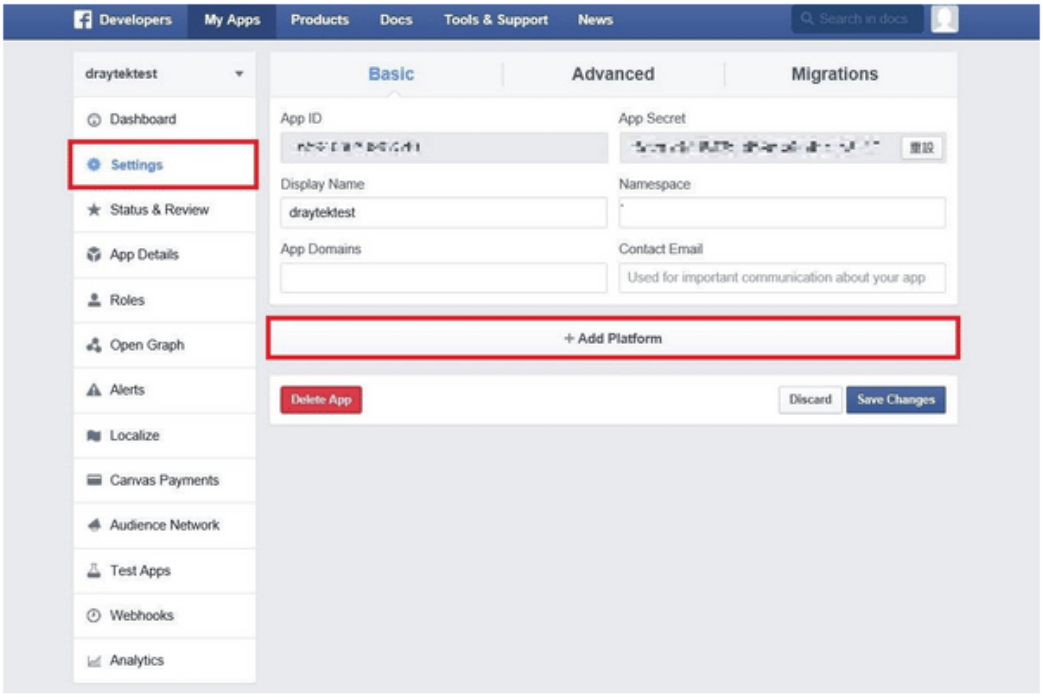
8. Pops up security check window, select the answer, and then click **Submit** to finish the process.



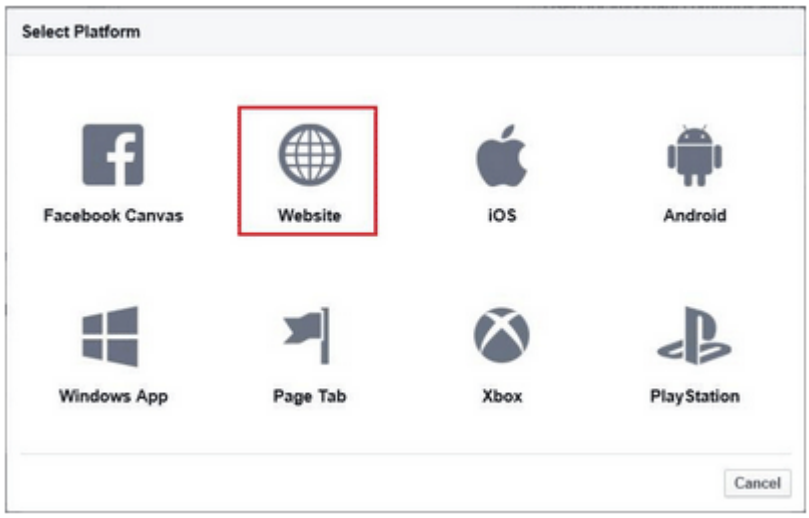
9. On Dashboard, user can get **App ID** and **App Secret**, these information will be used in Vigor Router's Web Portal Setup.



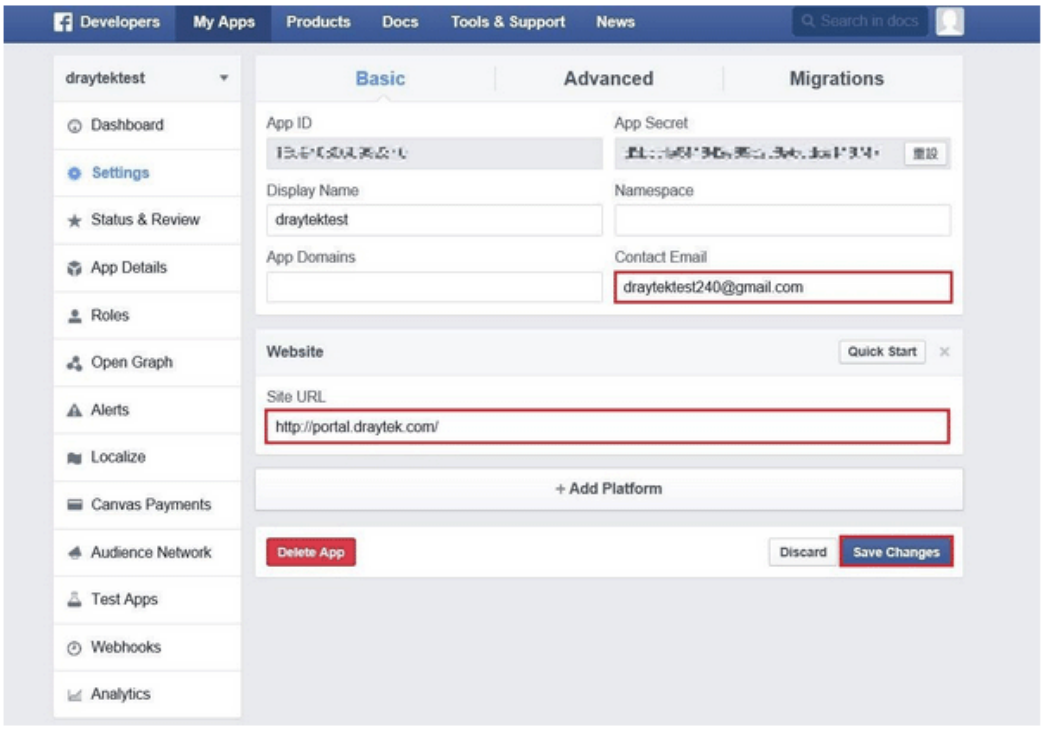
10. Add Platform on My Apps. Go to **Settings** then click **Add Platform.**



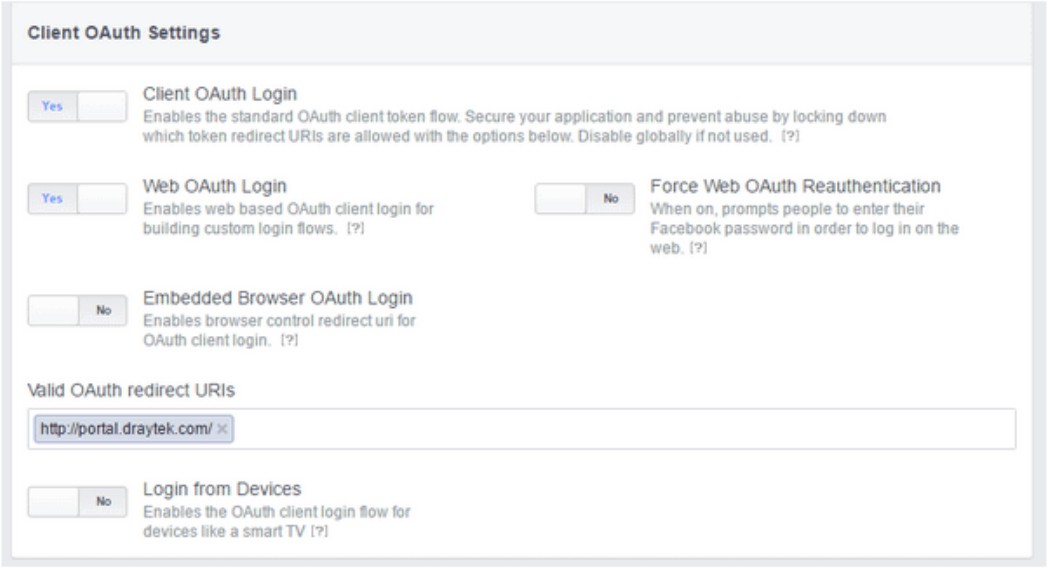
11. Choose **Website** in Select Platform window.



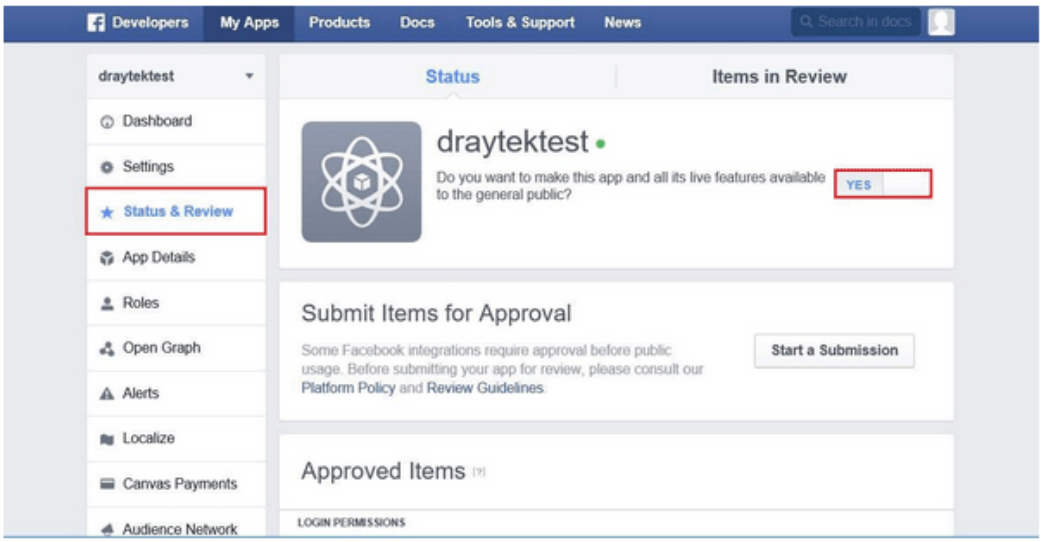
12. Enter the **Site URL** as http://portal.draytek.com. (*Note*: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put http://portal.draytek.com:8080). Enter the **Contact Email.** And **c**lick **Save Change.**



13. Set up Client OAuth. Go to **Settings** >> **Advanced** >>**Client OAuth Settings**, enter "http://portal.draytek.com" in **Valid OAuth redirect URIs**, and save changes.



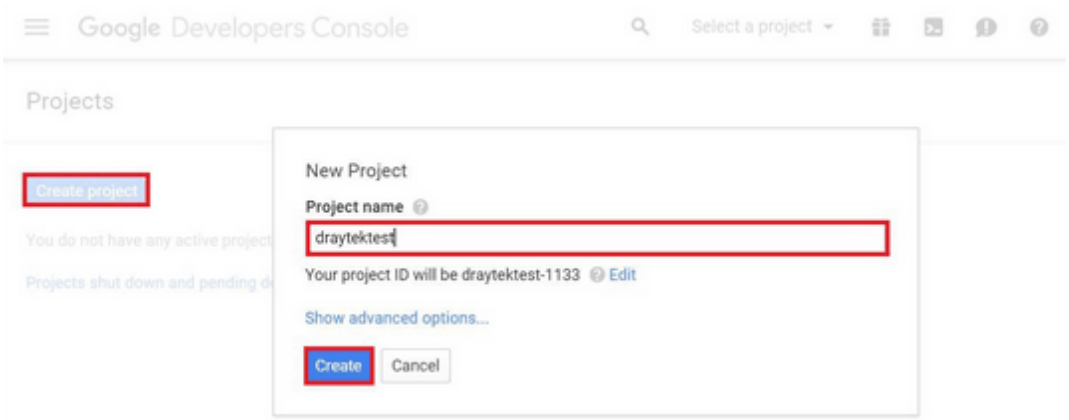
14. Go to **My Apps>>Status & Review**, and switch available status to **YES** to activate the APP.


Developers
My Apps
Products
Docs
Tools & Support
News
Search in docs
draytektest
Dashboard
Settings
Status & Review
App Details
Roles
Open Graph
Alerts
Localize
Canvas Payments
Audience Network
Status
Items in Review
draytektest
Do you want to make this app and all its live features available to the general public?
YES
Submit Items for Approval
Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our Platform Policy and Review Guidelines.
Start a Submission
Approved Items
LOGIN PERMISSIONS

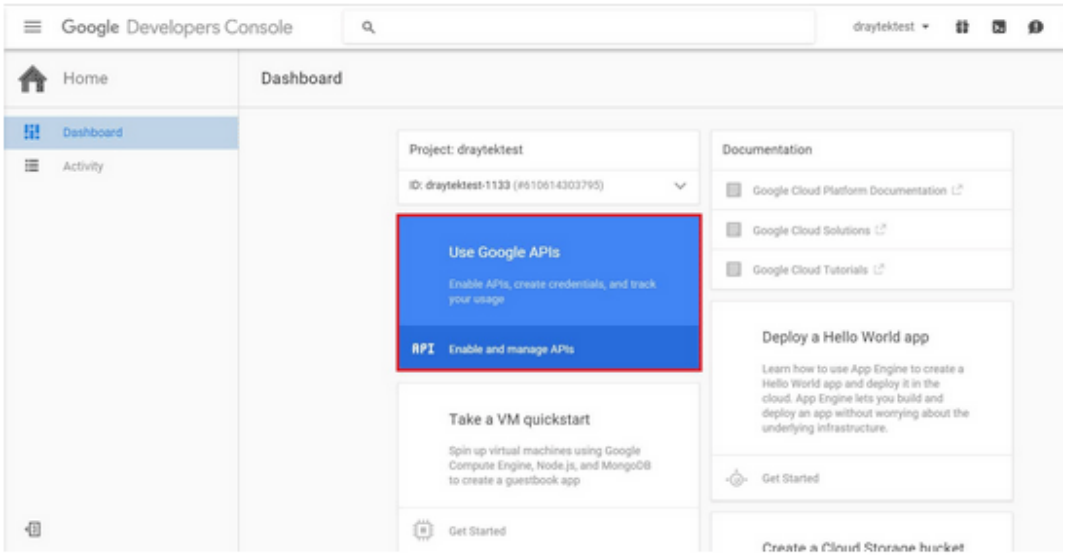
A-2 How to create Google APP for Web Portal Authentication?

The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

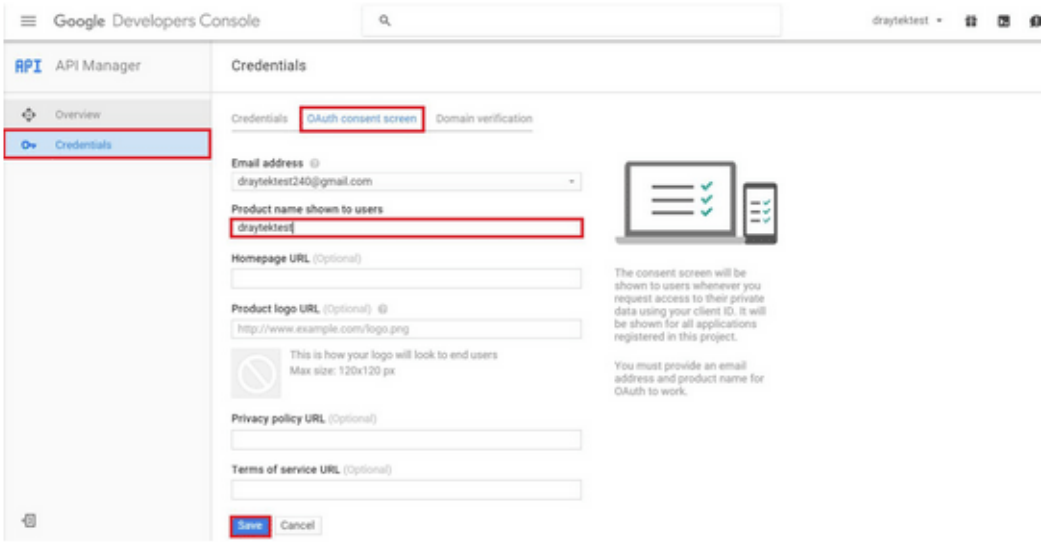
1. Create Developer project. Go to https://code.google.com/apis/console, login with a Google account then click **Create project.** Type **project name** then click **Create.**



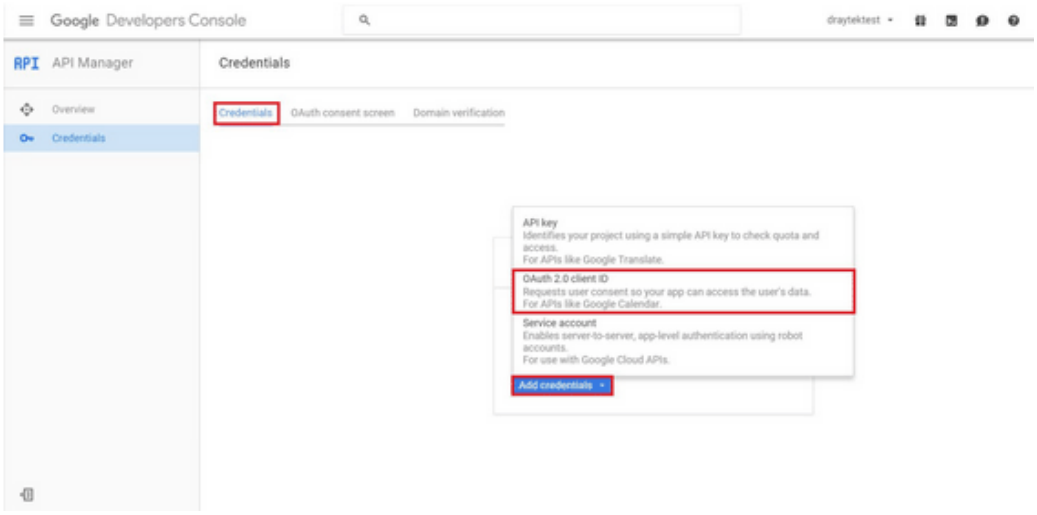
2. On Dashboard, choose **Use Google APIs**.



3. Edit Auth Consent screen. Go to **Credentials > Auth consent screen.** Enter your **email**, **product name** and other optional item then click on **Save.**



4. Create Client ID. Click **Credentials** and Click **Add credentials > OAuth2.0 client ID.**



5. Choose **Web application** as Application Type, then enter **name**. Set **Authorized JavaScript origins** and **Authorized redirect URLs** as http://portal.draytek.com, and click **Create.** (*Note*: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put http://portal.draytek.com:8080).
6. Get **client ID** and **client secret**. Such information will be used in Vigor Router's Web Portal Setup page.

VI-5 Central Management (AP)

Vigor2135 can manage the access points supporting AP management via Central AP Management.

AP Map

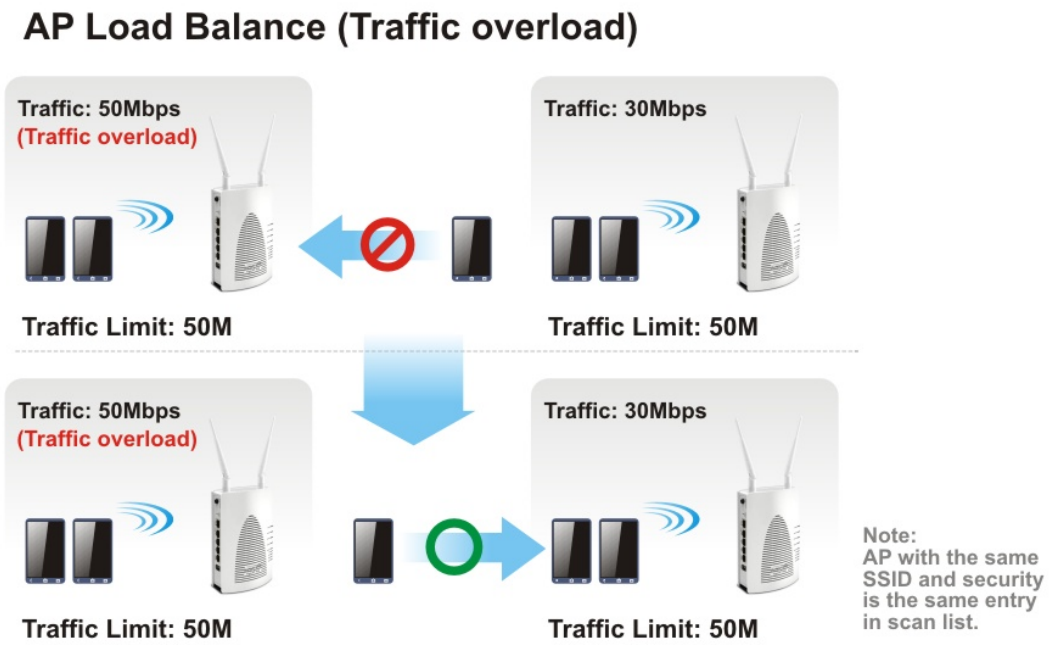
AP Map is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength

AP Maintenance

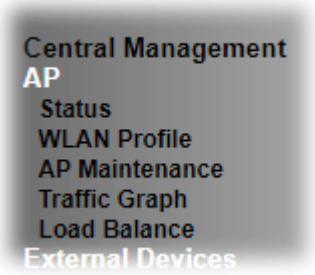
Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

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.

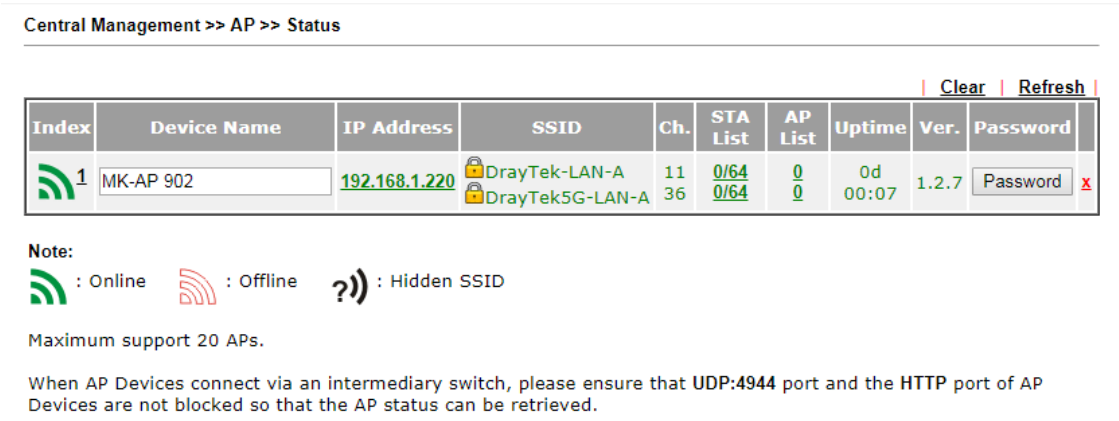


Web User Interface



VI-6-1 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.



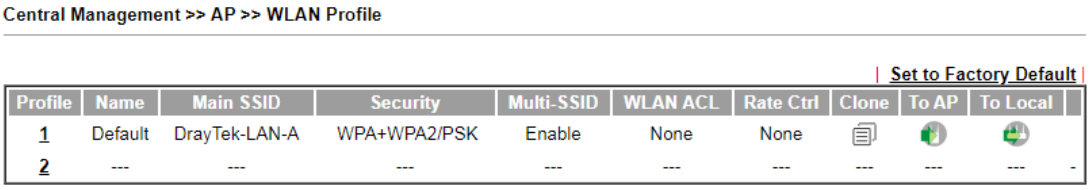
Available settings are explained as follows:

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 Vigor2135.
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.

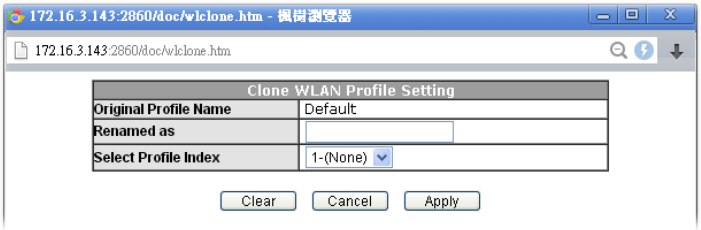
AP List	Display the number of the AP around the device.
Uptime	Display the duration of the AP powered up.
Version	Display the firmware version used by the access point.
Password	Vigor2135 can get related information of the access point by accessing into the web user interface of the access point. This button is used to modify the logging password of the connected access point.

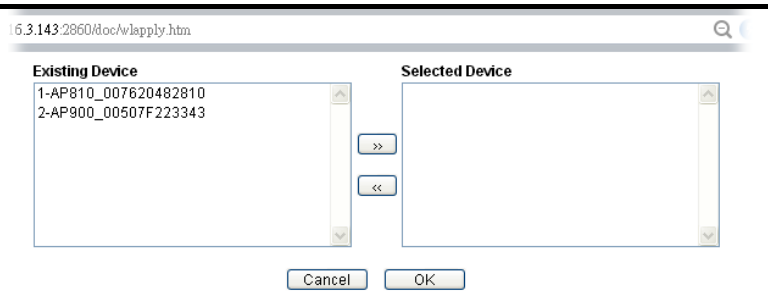
VI-6-2 WLAN Profile

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.

Central Management >> AP >> WLAN Profile

WLAN Profile Edit

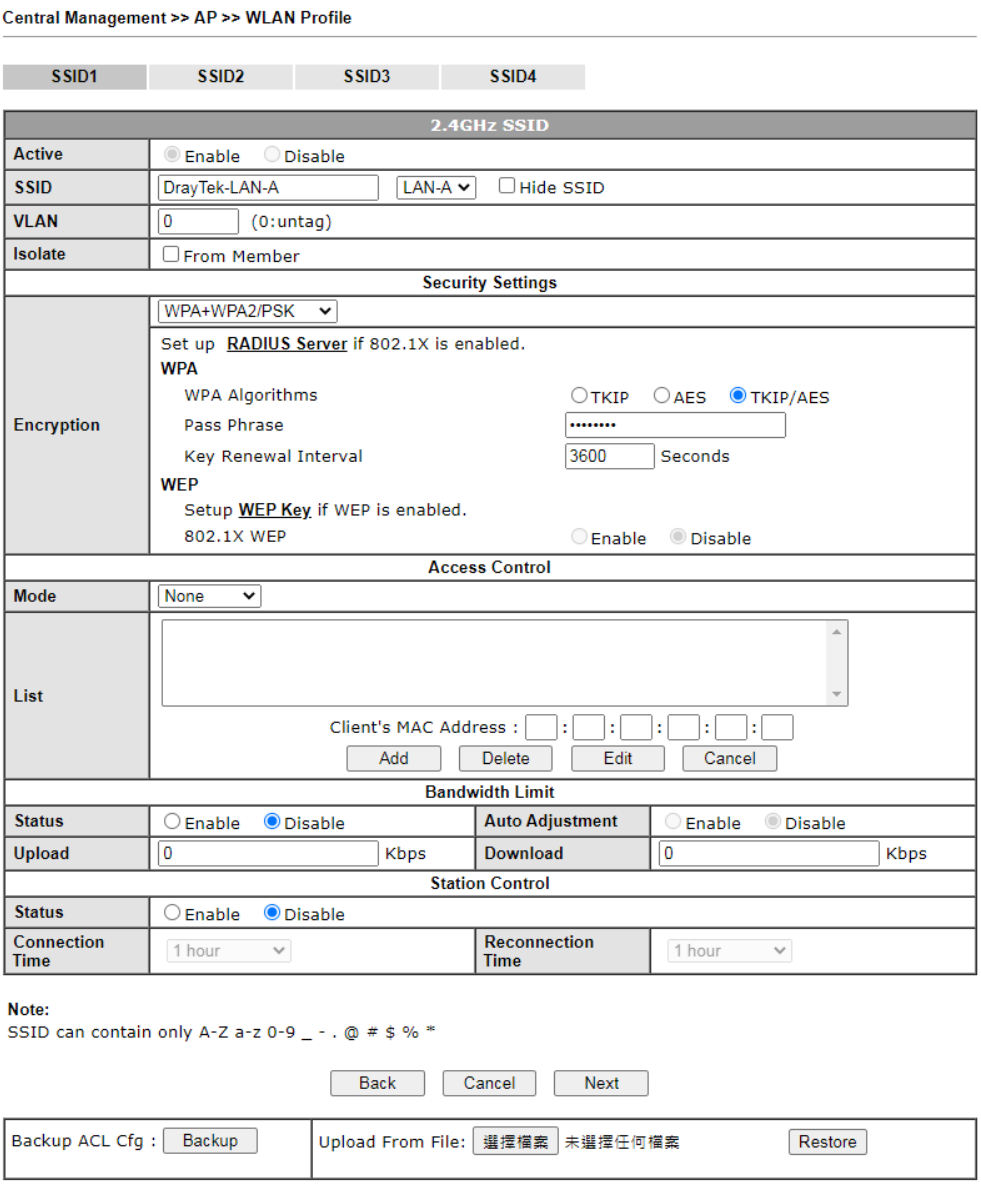
Device Settings	
Profile Name	Default ☐ Auto Provision
Administrator	admin
Password	•••••
2nd Subnet	◉ Enable ○ Disable
Management VLAN	☐ Enable Management VLAN: LAN-A VLAN ID 0 (0 ~ 4095) LAN-B VLAN ID 0 (0 ~ 4095)

WLAN General Setting

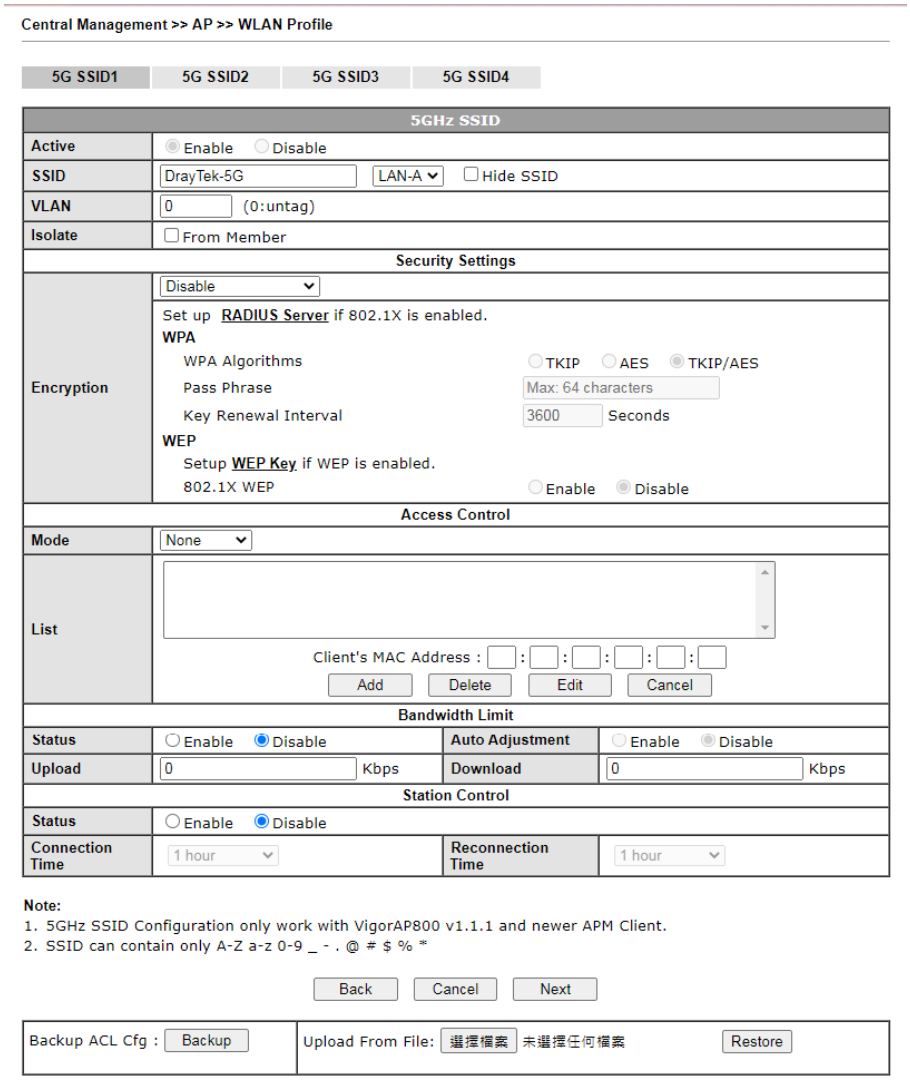
2.4GHz	5GHz	5GHz-2
Wireless LAN	○ Enable ◉ Disable	
Limit Client	☐ Enable 64 (3 ~ 128, default: 64)	
Operation Mode	AP	
2.4G Mode	Mixed(11b+11g+11n)	
2.4G Channel	2462MHz (Channel 11)	
Airtime Fairness	☐ Enable Airtime Fairness: Triggering Client Number 2 (2 ~ 128, default: 2)	
Band Steering	☐ Enable Band Steering: Check Time for WLAN Client 5G Cap. 15 seconds (1 ~ 60, default: 15)	
Roaming	☐ Minimum Basic Rate 1 Mbps ◉ Disable RSSI Requirement ○ Strictly Minimum RSSI - 73 dbm (42 %) (default: -73) ○ Minimum RSSI - 66 dbm (60 %) (default: -66) with Adjacent AP RSSI over 5 dB (default: 5) ☐ Enable Fast Roaming(WPA2/802.1x): PMK Cache Period 10 minutes (10 ~ 600, default: 10)	
WMM	○ Enable ◉ Disable	
Tx Power	100%	
Channel Width	Auto 20/40 MHz	

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.



Central Management >> AP >> WLAN Profile

5G SSID1 | 5G SSID2 | 5G SSID3 | 5G SSID4

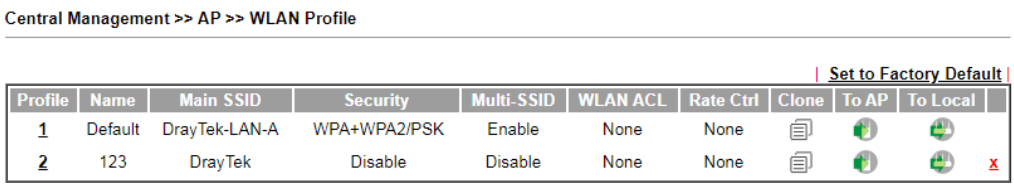
5GHz SSID			
Active	Enable Disable		
SSID	DrayTek-5G LAN-A Hide SSID		
VLAN	0 (0:untag)		
Isolate	From Member		
Security Settings			
Encryption	Disable Set up RADIUS Server if 802.1X is enabled. WPA WPA Algorithms: TKIP AES TKIP/AES Pass Phrase: Max: 64 characters Key Renewal Interval: 3600 Seconds WEP Setup WEP Key if WEP is enabled. 802.1X WEP: Enable Disable		
Access Control			
Mode	None		
List	Client's MAC Address : : : : : : Add Delete Edit Cancel		
Bandwidth Limit			
Status	Enable Disable	Auto Adjustment	Enable Disable
Upload	0 Kbps	Download	0 Kbps
Station Control			
Status	Enable Disable		
Connection Time	1 hour	Reconnection Time	1 hour

Note:
1. 5GHz SSID Configuration only work with VigorAP800 v1.1.1 and newer APM Client.
2. SSID can contain only A-Z a-z 0-9 _ - . @ # $ % *

Back Cancel Next

Backup ACL Cfg : Backup | Upload From File: 選擇檔案 未選擇任何檔案 Restore

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

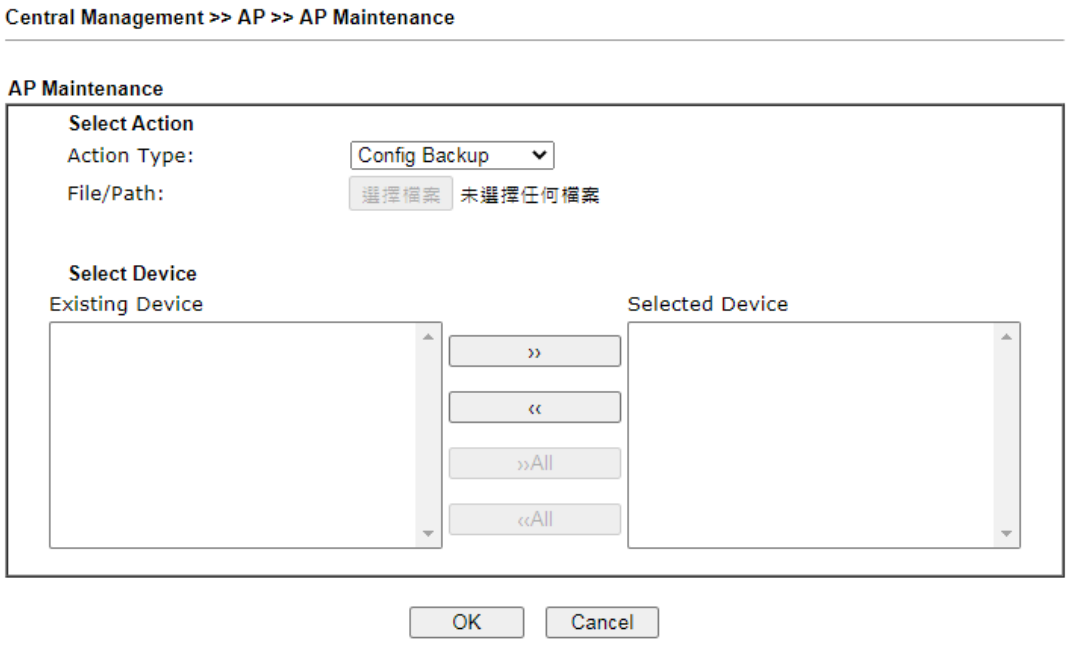
| Set to Factory Default |

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

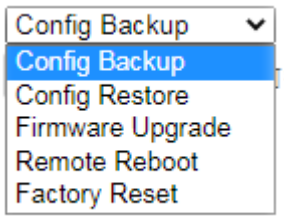
VI-6-3 AP Maintenance

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 Vigor2135.



Available settings are explained as follows:

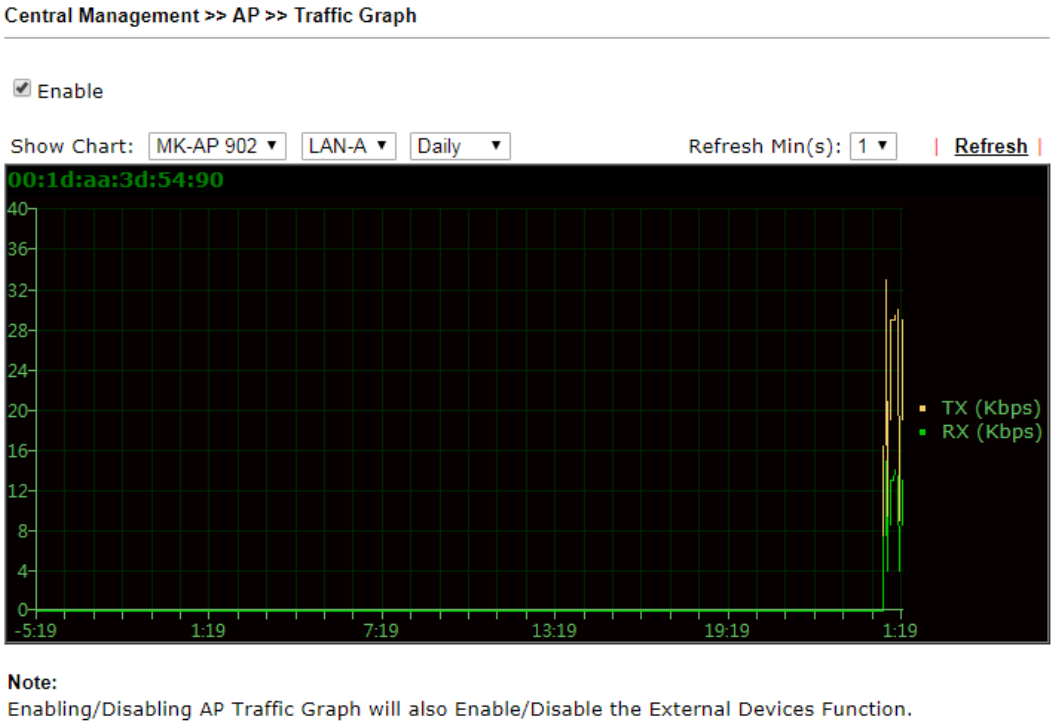
Item	Description
Action	There are four actions provided by Vigor router to manage the access points.  Vigor router can **backup** the configuration of the selected AP, **restore** the configuration for the selected AP, perform the **firmware upgrade** of the selected AP, **reboot** the selected AP remotely 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-6-4 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.

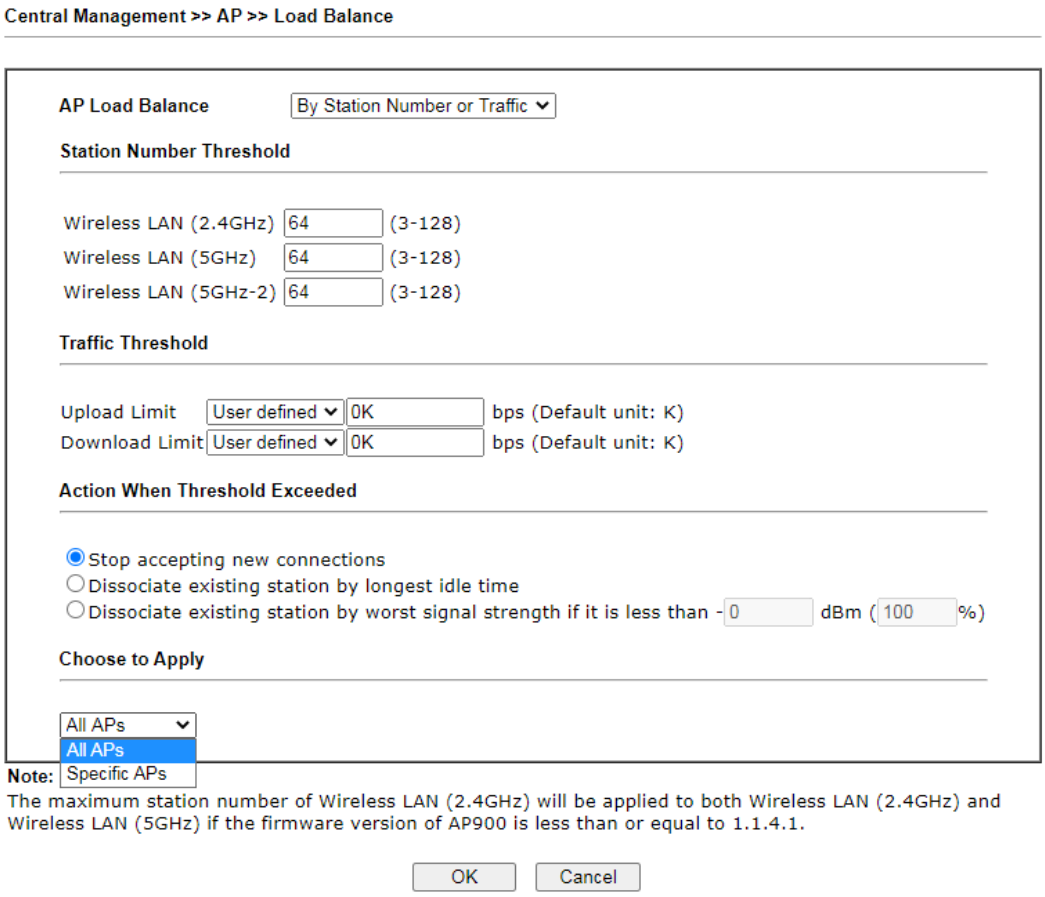


The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).

Info	Enabling/Disabling such function will also enable/disable the External Devices function.

VI-6-5 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:

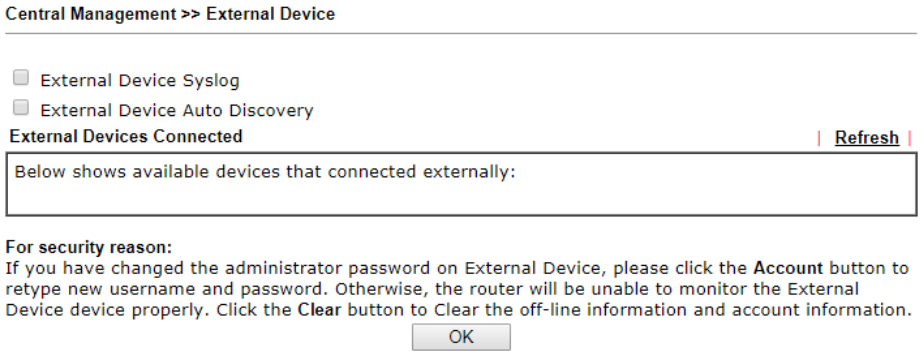
Item	Description
AP Load Balance	It is used to determine the operation mode when the system detects overload between access points. **Disable** – Disable the function of AP load balance. **By Station Number** –The operation of load balance will be executed based on the station number configured in this 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	Determine which AP shall be applied with the load balance. **All APs** – All APs shall be applied with the load balance. **Specific APs** – The function of load balance will be applied to the AP specified in this field.

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

VI-6 Central Management (External Devices)

Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.



Available settings are explained as follows:

Item	Description
External Device Syslog	Check this box to display information of the detected device on Syslog.
External Device Auto Discovery	Check this box to detect the external device automatically and display on this page.

From this web page, check the box of **External Device Auto Discovery** and click **OK**. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.

When you finished the configuration, click **OK** to save it.

Info	Only DrayTek products can be detected by this function.

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.

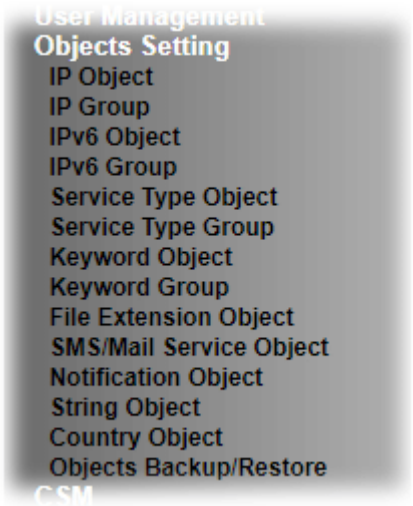
USB

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications.

VII-1 Objects Settings

This section allows the creation of objects and object groups from IP addresses, service types, keywords, file extensions, SMS and email recipients, and notification types. Once set up, these objects can be applied to firewall and content management rules.

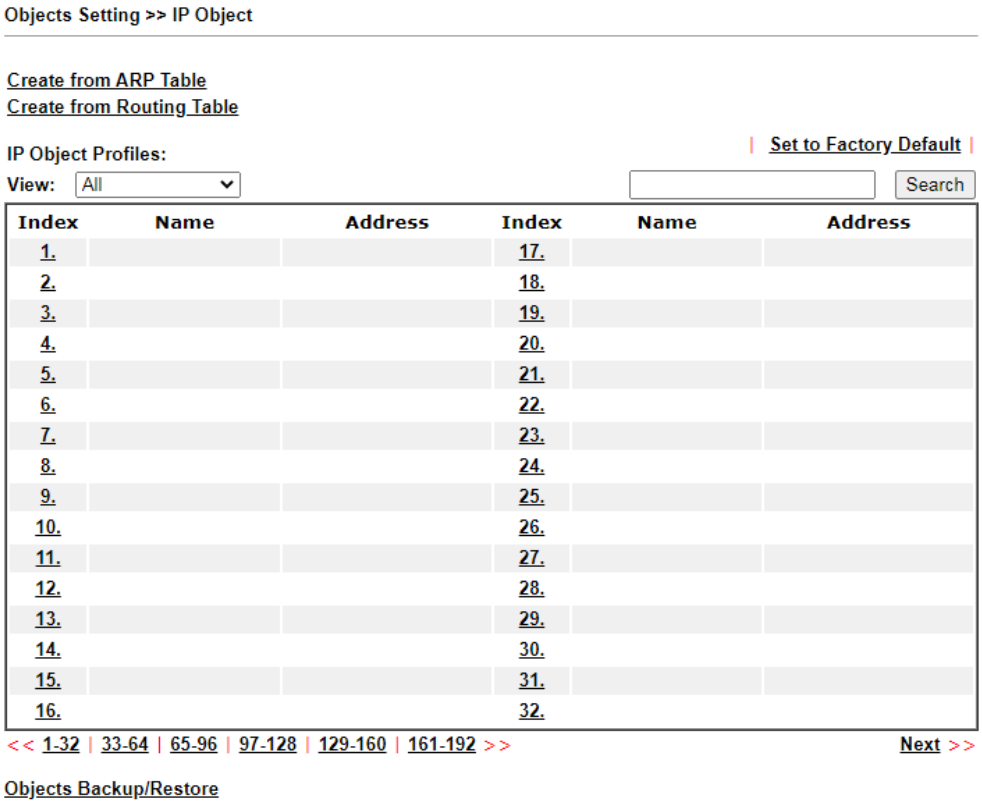
Web User Interface



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 for applying it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

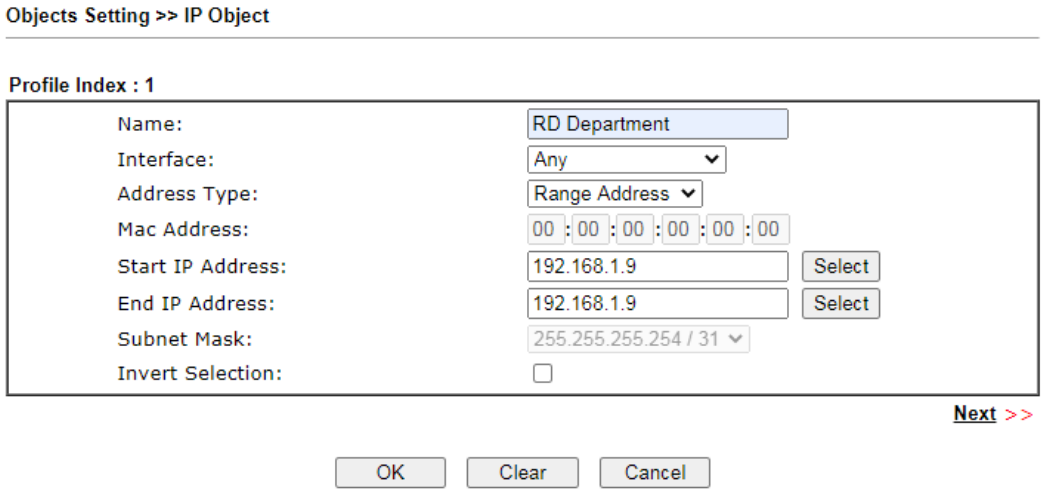
Up to 192 IP Objects can be created.



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 profile settings.
Search	Enter a string of the IP object that you wan to search.
Index	Profile number of the IP object.
Name	Name of the object.
Address	Displays the IP address configured for the object profile.
Objects Backup/Restore	Click it to backup or restore the IP object.

To set up a profile, click the profile number under Index column to bring up the configuration page.

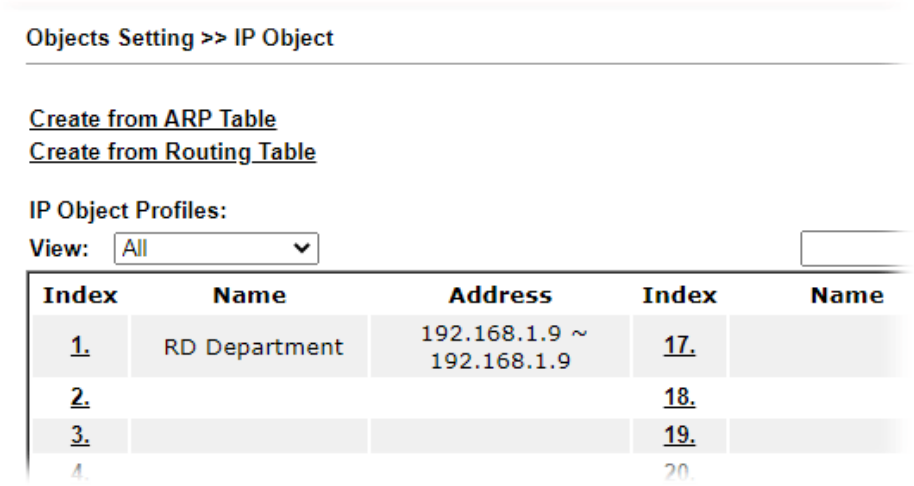


Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Interface	The network interface on which the IP address or addresses are to be found. **Any** – All network interfaces. **LAN/DMZ/RT/VPN** – All network interfaces except WAN. **WAN** – Only WAN interfaces.
Address Type	Type of Addresses. **Any Address** – Object covers all IP addresses. **Single Address** – Object covers one IP address. **Range Address** – Object covers a range of IP addresses. **Subnet Address** – Object covers a range of IP addresses specified in subnet notation. **Mac Address** – Object contains a MAC address.
MAC Address	Enter MAC address of the network device, if Address Type is Mac Address.
Start IP Address	Enter beginning IP address, if Address Type is one of Single

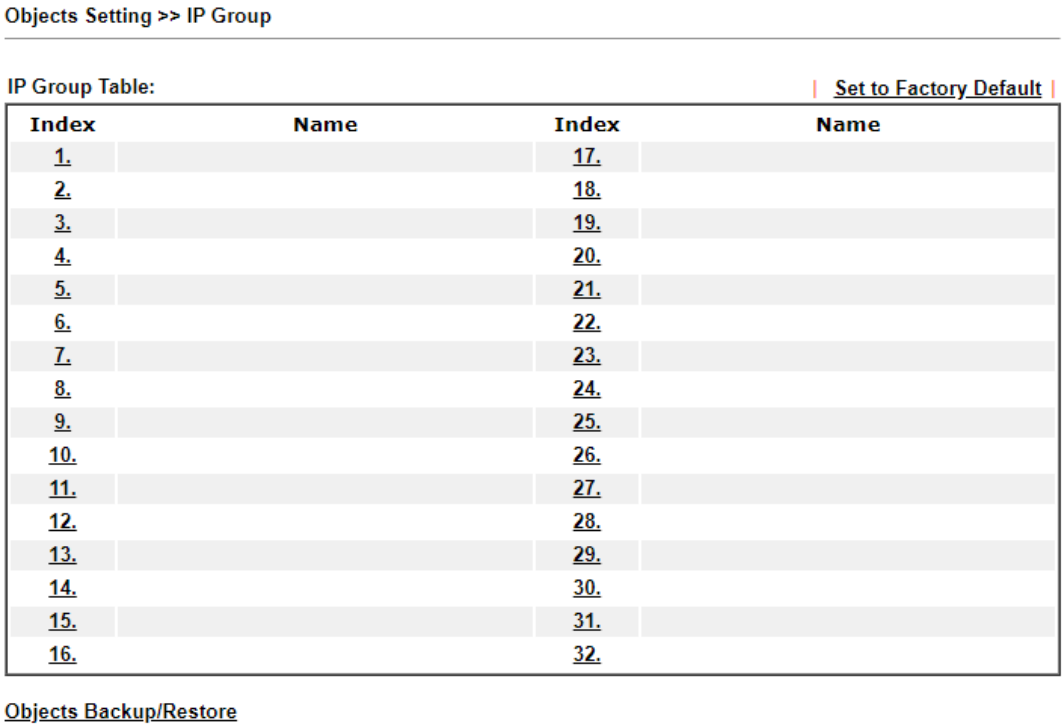
	Address, Range Address and Subnet Address.
End IP Address	Enter ending IP address, if Address type is one of Single Address, Range Address and Subnet Address.
Subnet Mask	Enter subnet mask, if Address type is Subnet Mask.
Invert Selection	If selected, all addresses except the ones entered above will be used.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP object, click **Clear**.



VII-1-2 IP Group

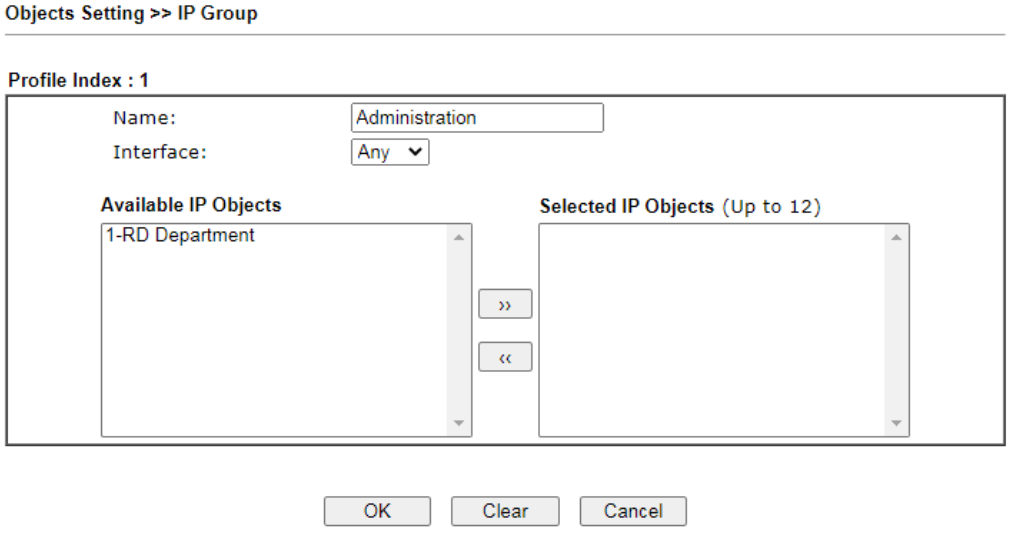
Multiple IP Objects can be placed into an IP Group.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the IP group object.

To set up a profile, click its index to bring up the configuration page.



Available settings are explained as follows:

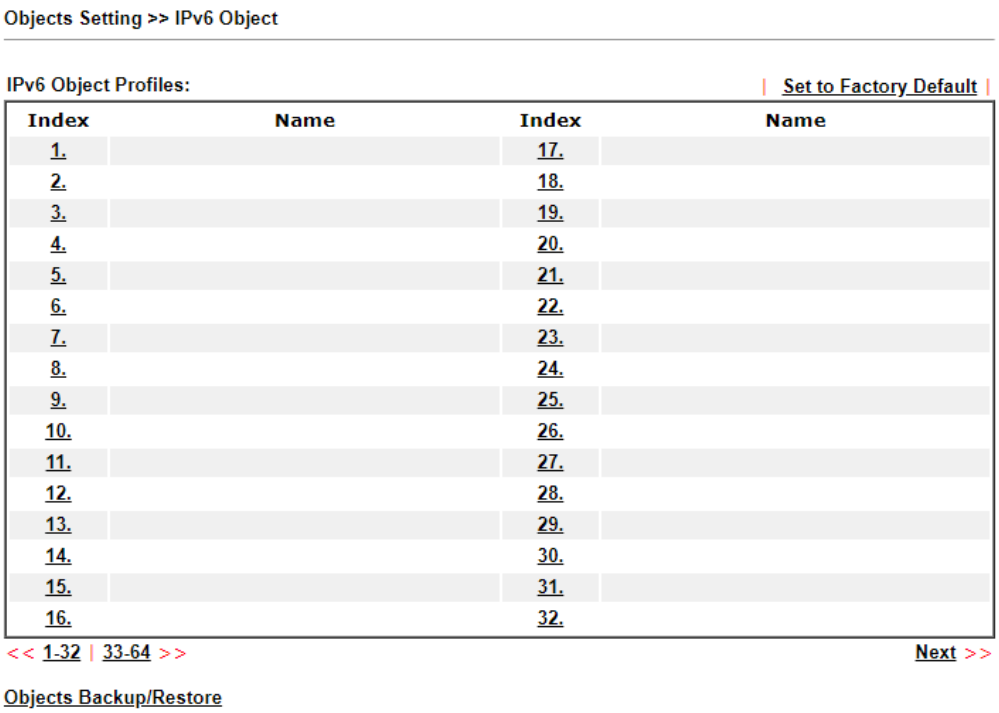
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Interface	Select WAN, LAN or Any to filter IP objects.
Available IP Objects	All available IP objects that are associated with the selected interface.
Selected IP Objects	IP objects that have been added to this profile.

To add an IP object to the IP Group, select it under Available IP Objects, then click the **>>** button. To remove an IP object from the IP Group, select it under Selected IP Objects, then click the **<<** button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP group, click **Clear**.

VII-1-3 IPv6 Object

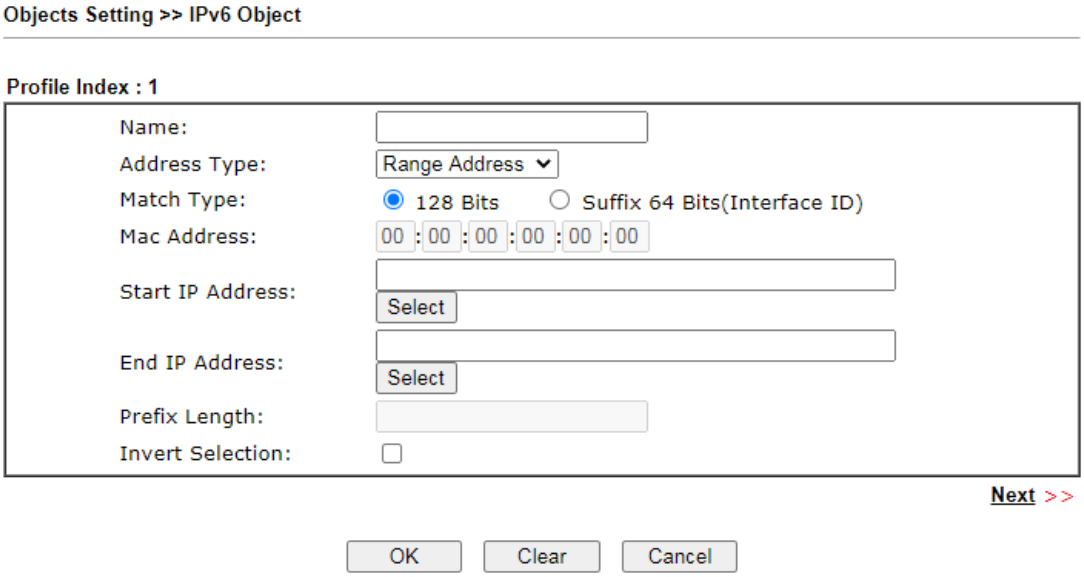
Up to 64 IPv6 Objects can be created.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the IPv6 object.

To set up a profile, click the profile number under Index column to bring up the configuration page.



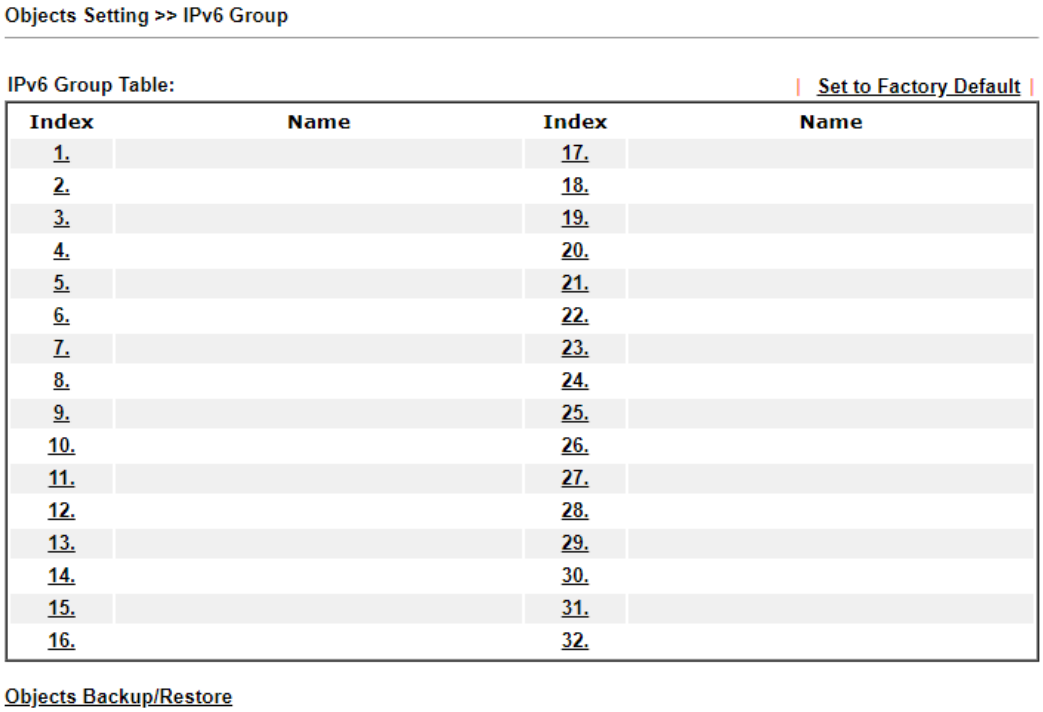
Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Address Type	Type of Addresses. **Any Address** - Object covers all IPv6 addresses. **Single Address** - Object covers one IPv6 address. **Range Address** - Object covers a range of IPv6 addresses. **Subnet Address** - Object covers a range of IPv6 addresses specified in subnet notation. **Mac Address** - Object contains a MAC address.
Match Type	Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
Mac Address	Enter MAC address of the network device, if Address Type is Mac Address.
Start IP Address	Enter beginning IP address, if Address Type is one of Single Address, Range Address and Subnet Address.
End IP Address	Enter ending IP address, if Address type is one of Single Address, Range Address and Subnet Address.
Prefix Length	Enter IPv6 prefix length, if Address type is Subnet Address.
Invert Selection	If selected, all addresses except the ones entered above will be used.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the IPv6 object, click **Clear**.

VII-1-4 IPv6 Group

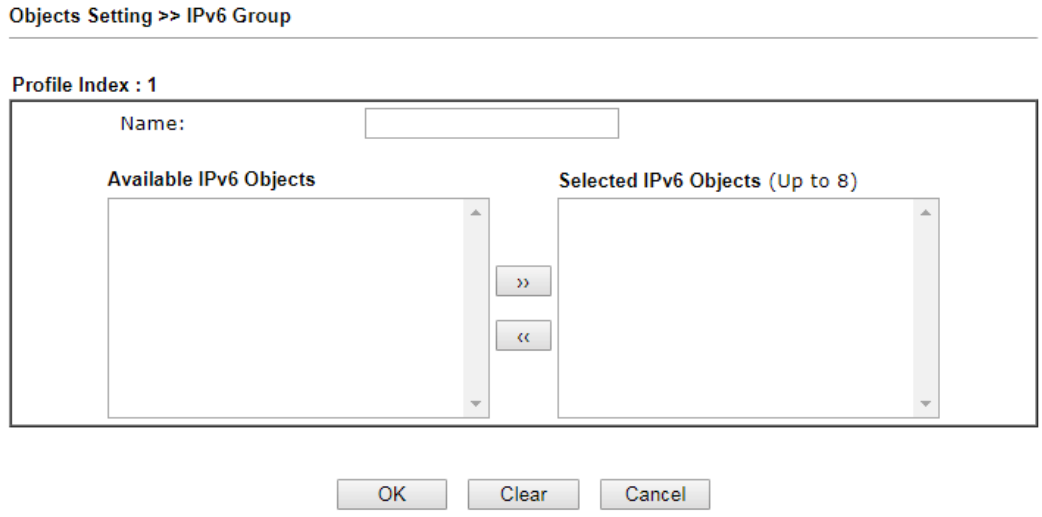
Multiple **IPv6 Objects** can be placed into an **IPv6 Group**.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the IPv6 group.

To set up a profile, click the profile number under Index column to bring up the configuration page.



Available settings are explained as follows:

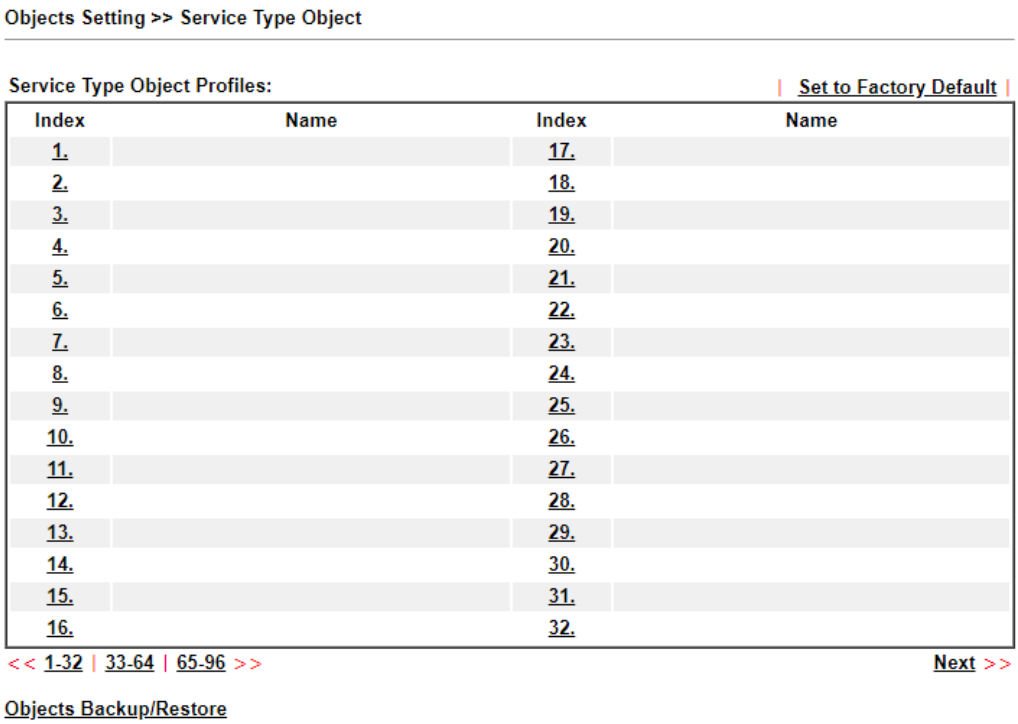
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available IPv6 Objects	All available IP objects that are associated with the selected interface.
Selected IPv6 Objects	IPv6 objects that have been added to this profile.

To add an IPv6 object to the IPv6 Group, select it under Available IPv6 Objects, then click the >> button. To remove an IPv6 object from the IPv6 Group, select it under Selected IPv6 Objects, then click the << button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IPv6 group, click **Clear**.

VII-1-5 Service Type Object

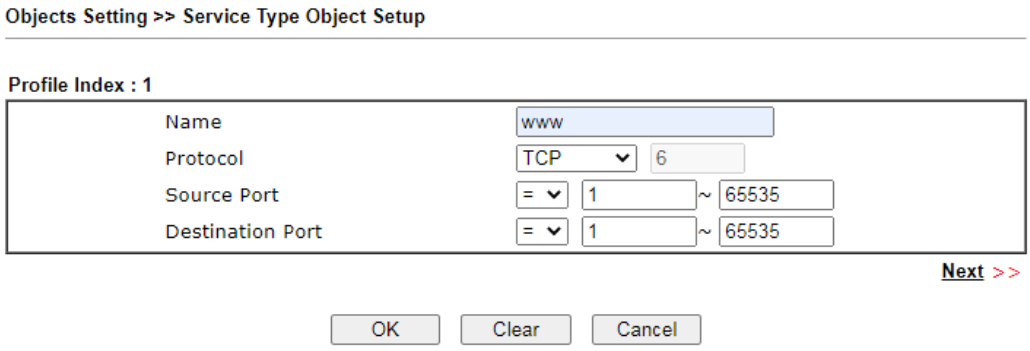
Up to 96 Service Type Objects can be created.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the service type object.

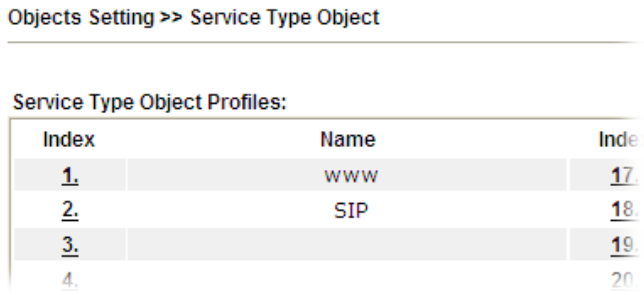
To set up a profile, click the profile number under Index column to bring up the configuration page.



Available settings are explained as follows:

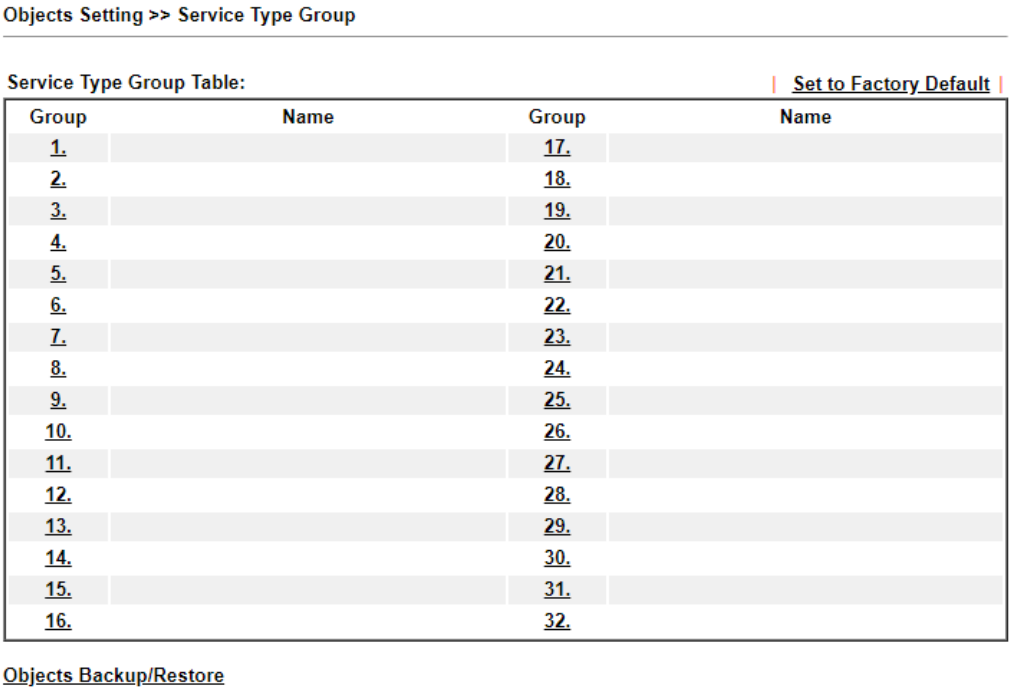
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Protocol	Protocol(s) to which this profile applies. **Any** – All protocols. **ICMP** – Internet Control Message Protocol **IGMP** – Internet Group Management Protocol **TCP** – Transmission Control Protocol **UDP** – User Datagram Protocol **TCP/UDP** – Transmission Control Protocol and User Datagram Protocol **Other** – Other protocols not listed above. Enter protocol number in the textbox.
Source/Destination Port	When protocol selected includes TCP or UDP, the source and destination ports can be specified. = – any port that falls within the specified range. != – any port that falls outside of the specified range. – all port numbers that are greater than the specified value. **<** – all port numbers that are smaller than the specified value.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current service type object, click **Clear**.



VII-1-6 Service Type Group

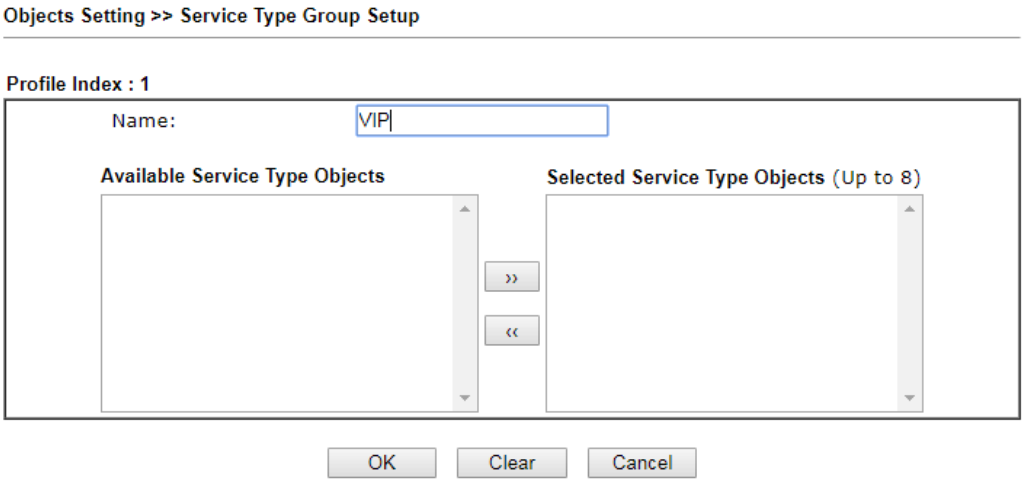
Multiple **Service Type Objects** can be placed into a **Service Type Group**.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the service type group object.

To set up a profile, click the profile number under Index column to bring up the configuration page.



Available settings are explained as follows:

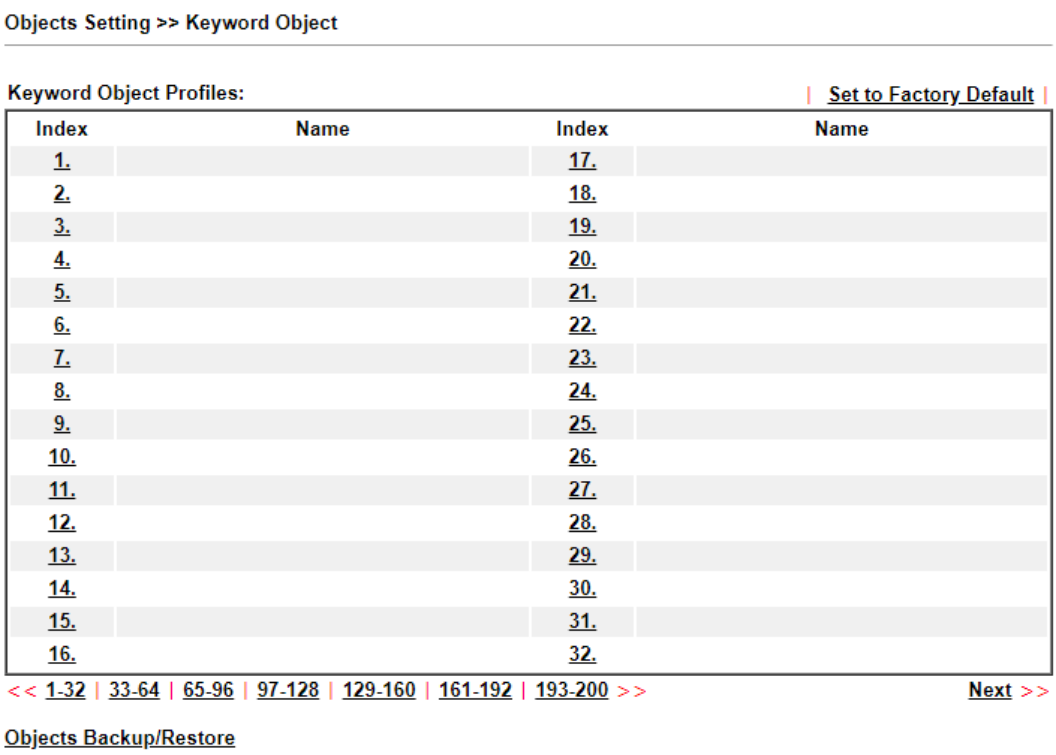
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available Service Type Objects	All available service type objects.
Selected Service Type Objects	Service type objects that have been added to this profile.

To add a Service Type Object to the Service Type Group, select it under **Available Service Type Objects**, then click the **>>** button. To remove a Service Type Object to the Service Type Group, select it under **Selected Service Type Objects**, then click the **<<** button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current service type group, click **Clear**.

VII-1-7 Keyword Object

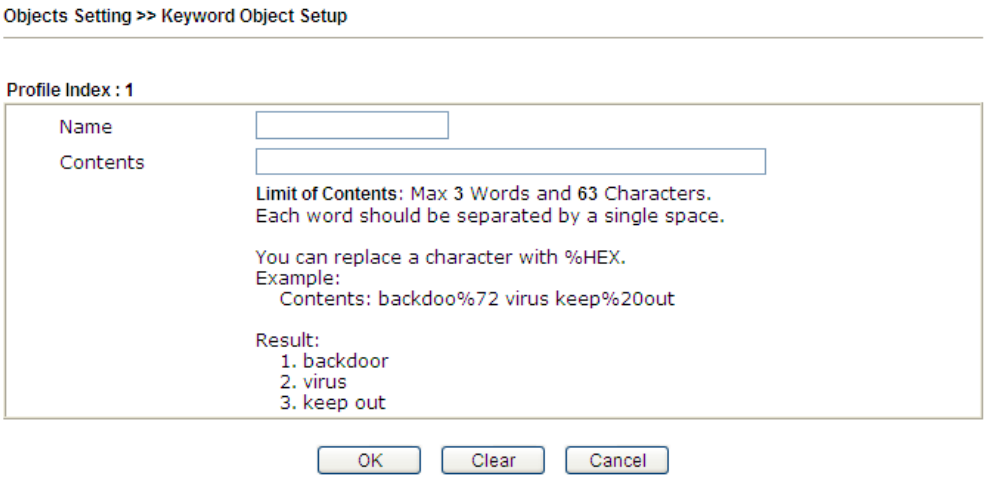
200 Keyword Object Profiles can be created for use as blacklists or white lists in **CSM >>URL Content Filter Profile** and **Web Content Filter Profile**.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the keyword object.

To set up a profile, click its index to bring up the configuration page.



Available settings are explained as follows:

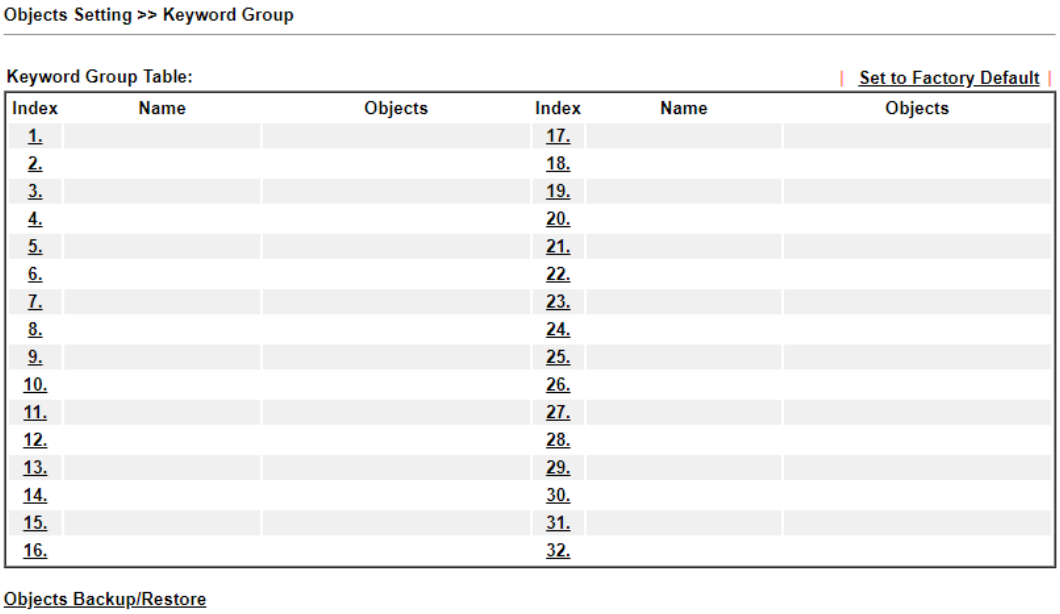
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Contents	Keywords to be matched. Enter the content for this profile. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings. In addition, up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered. For key phrases that contain spaces, replace spaces with the sequence %20. For example, the phrase “keep out” is to be entered as “keep%20out”.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current keyword object, click **Clear**.

VII-1-8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.

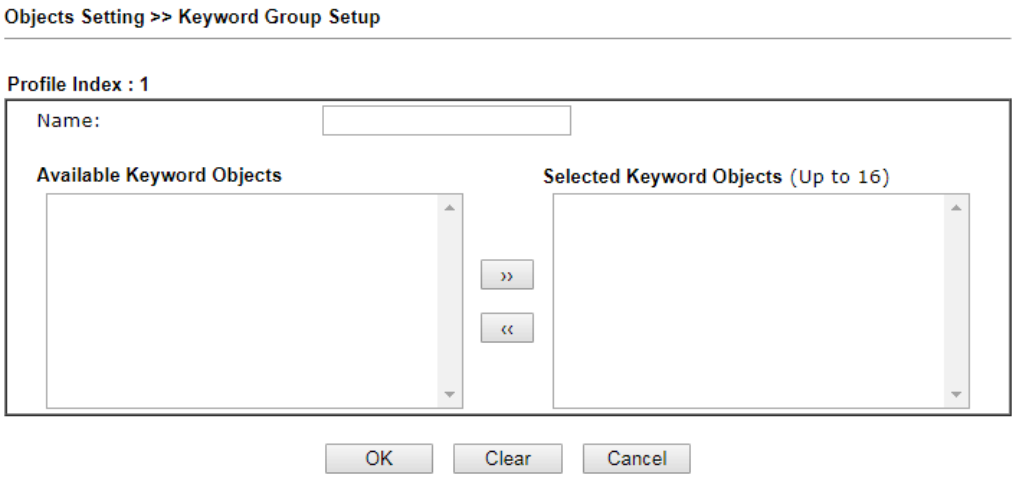
Keyword groups can be chosen as blacklists or white lists in **CSM >>URL /Web Content Filter Profile**.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects	Display the keyword objects under this group.
Objects Backup/Restore	Click it to backup or restore the keyword group.

To set up a profile, click its index to bring up the configuration page.



Available settings are explained as follows:

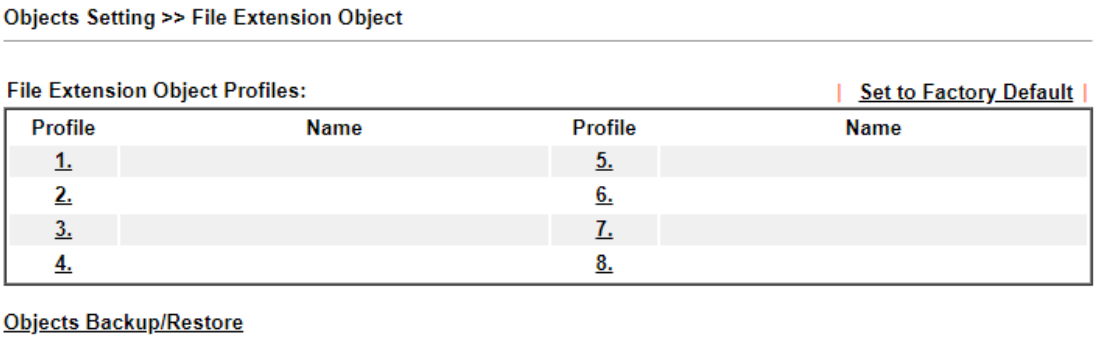
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available Keyword Objects	All keyword objects that have not been added to this profile.
Selected Keyword Objects	Keyword objects that have been added to this profile.

To add a Service Type Object to the Service Type Group, select it under **Available Service Type Objects**, then click the **>>** button. To remove a Service Type Object to the Service Type Group, select it under **Selected Service Type Objects**, then click the **<<** button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current keyword group, click **Clear**.

VII-1-9 File Extension Object

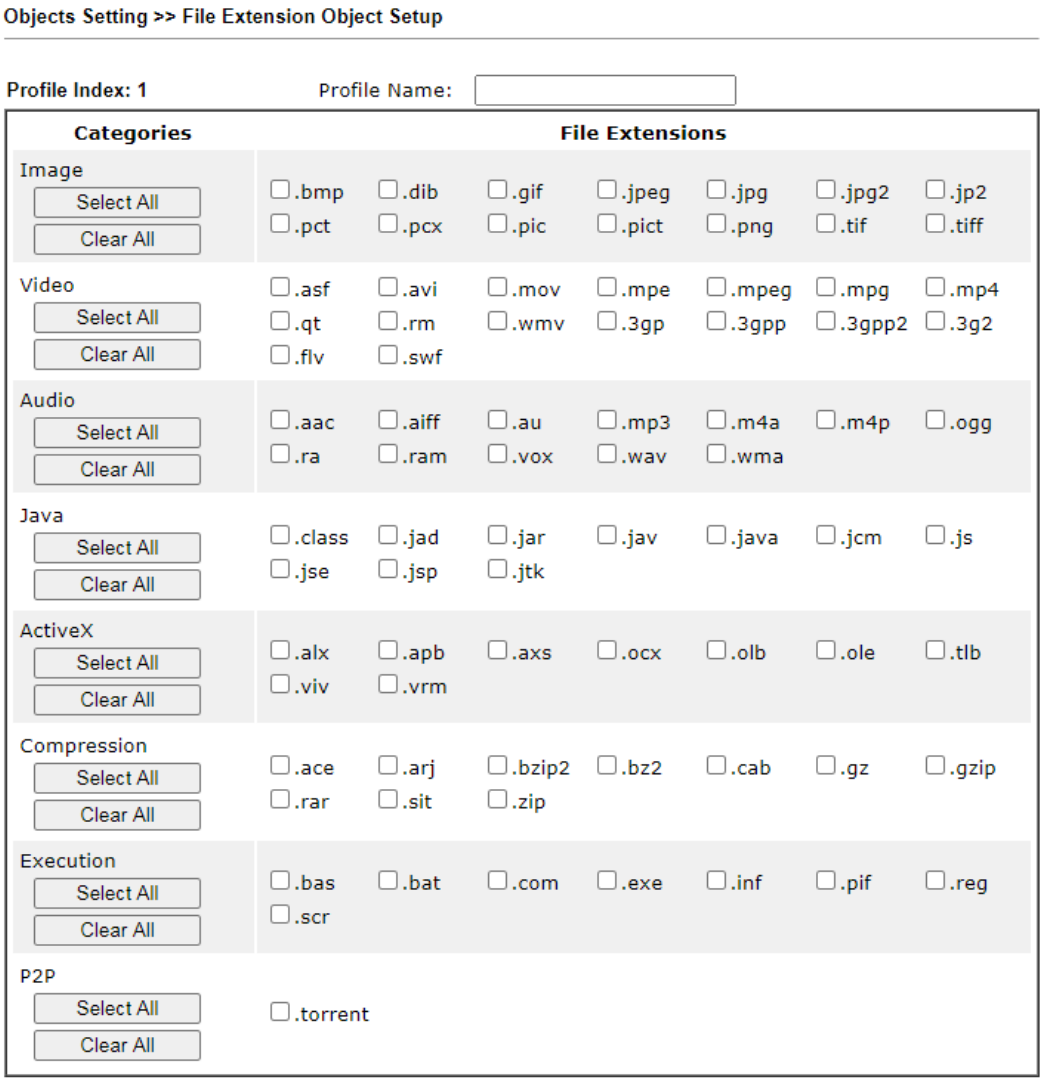
Up to 8 File Extension Objects can be set up for use with **CSM>>URL Content Filter**.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the file extension object.

To set up a profile, click its index to bring up the configuration page.



Available settings are explained as follows:

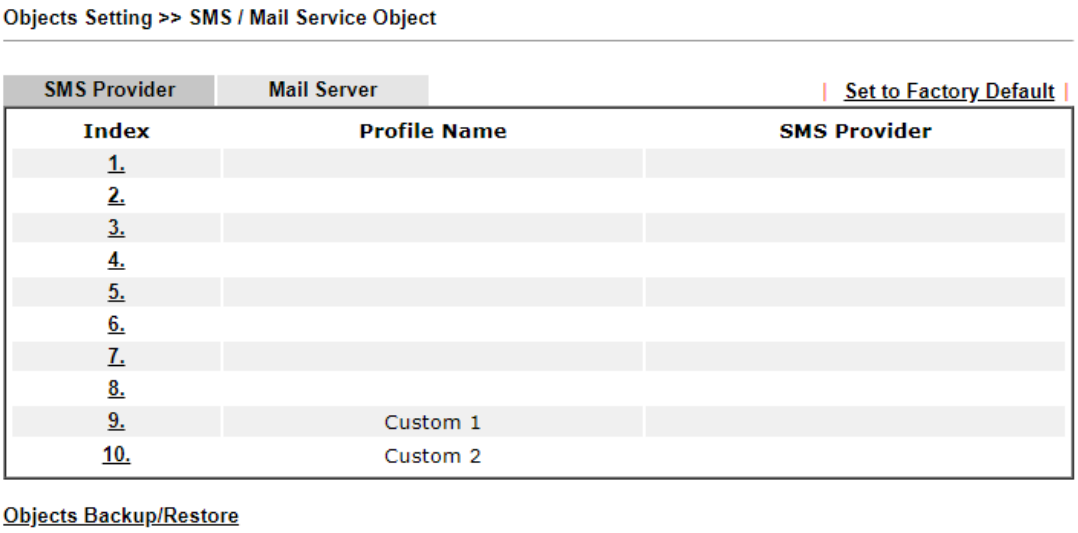
Item	Description
Profile Name	Name that identifies this profile. Maximum length is 7 characters.
Select All	Selects all file extensions for the category.
Clear All	Deselects all file extensions for the category.

Select the file extensions you wish to be included in the profile. To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current file extension object, click **Clear**.

VII-1-10 SMS/Mail Service Object

SMS Service Object

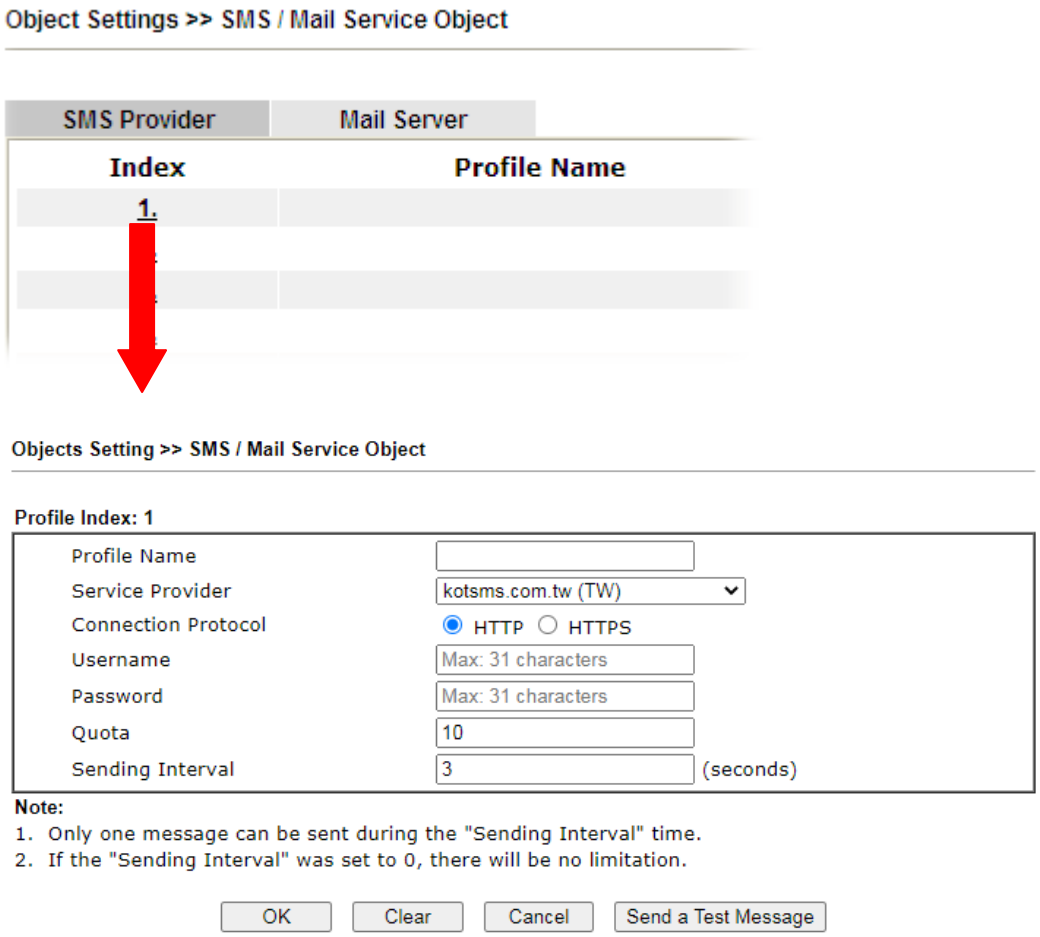
Up to 10 SMS Service Objects can be set up for use with **Application>>SMS Alert Service**.



Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Profile Name	Name that identifies the profile.
SMS Provider	The SMS provider selected for the profile.
Objects Backup/Restore	Click it to backup or restore the service object.

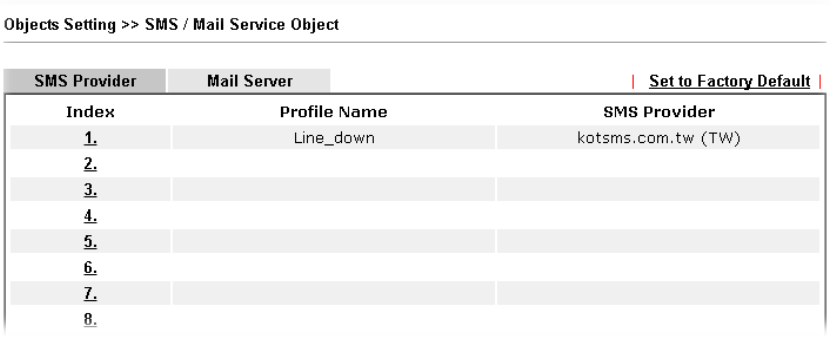
To set up a profile, click the **SMS Provider** tab, and then click its index to bring up the configuration page.



Available settings are explained as follows:

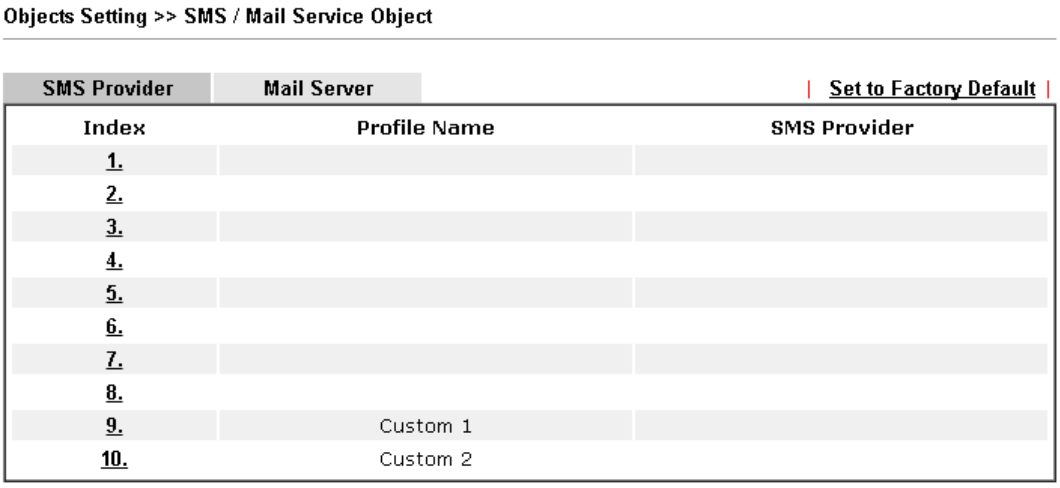
Item	Description
Profile Name	Name that identifies this profile. Maximum length is 31 characters.
Service Provider	Select a Service Provider from the dropdown list.
Connection Protocol	Specify HTTP or HTTPS.
Username	Username used to log in to the service. Maximum length is 31 characters.
Password	Password used to log in to the service. Maximum length is 31 characters.
Quota	Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0.
Sending Interval	Minimum amount of time, in seconds, to wait between sending SMS messages.
Send a Test Message	Click it to send a test e-mail according to above configuration.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the SMS service object, click **Clear**.

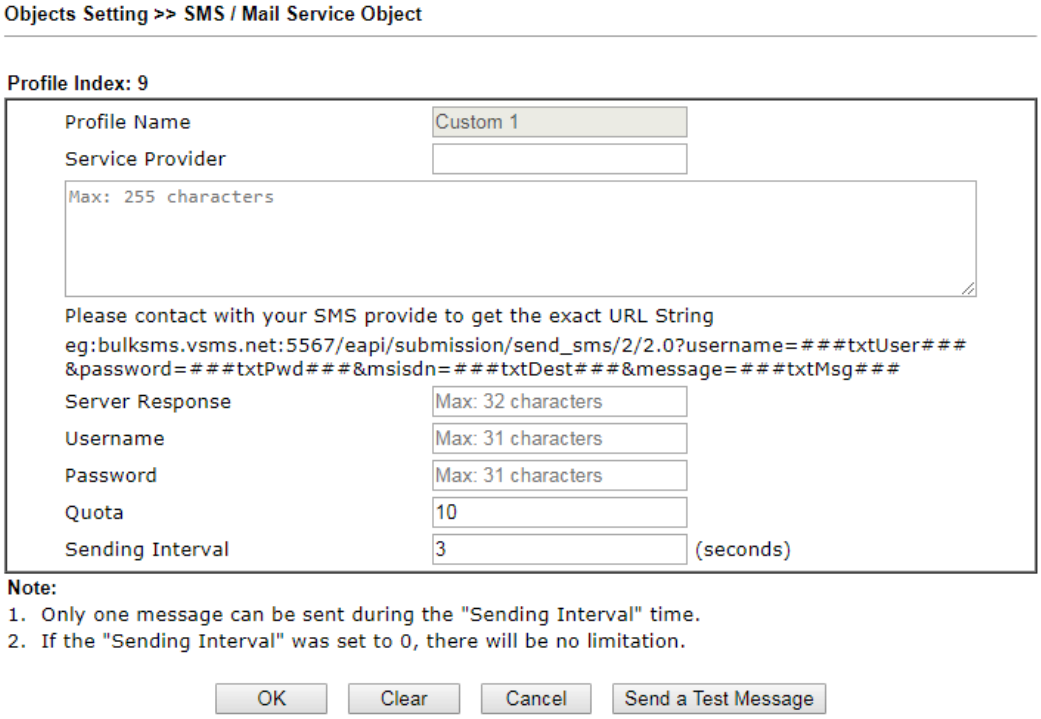

Objects Setting >> SMS / Mail Service Object
SMS Provider
Mail Server
Set to Factory Default
Index
Profile Name
SMS Provider
1.
Line_down
kotsms.com.tw (TW)
2.
3.
4.
5.
6.
7.
8.

Customized SMS Service

The router offers an extensive list of preset SMS service providers for your convenience. However, if your service provider is not among the list of supported service providers, simply use Indexes 9 and 10 to create a customized SMS service profile.



To set up a customized profile, click the SMS Provider tab, and then click one of the 2 indexes (9 and 10) to bring up the configuration page.



Available settings are explained as follows:

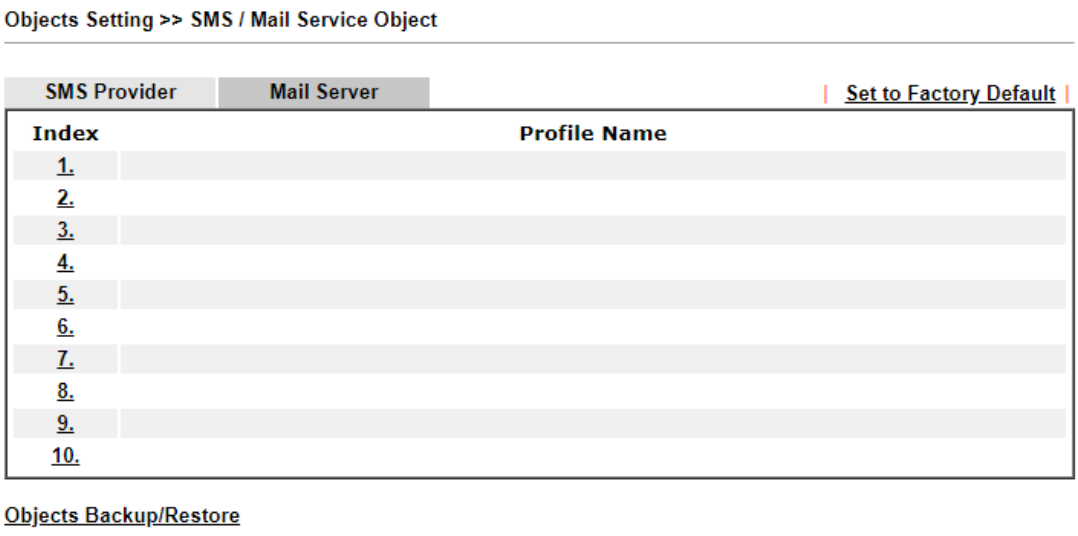
Item	Description
Profile Name	Display-only profile name, which is Custom 1 for Index 9 and Custom 2 for Index 10.
Service Provider	Enter an identifier for the service provider. Maximum length is 23 characters.

Entry box	Enter the URL for the SMS service. Maximum length is 255 characters. Contact the service provider for the appropriate URL to use.
Server Response	Enter the API text defined by the SMS provider. It allows Vigor router to acknowledge that the SMS server has received the request coming from the SMS server.
Username	Username used to log in to the service. Maximum length is 31 characters.
Password	Password used to log in to the service. Maximum length is 31 characters.
Quota	Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0.
Sending Interval	Minimum amount of time, in seconds, to wait between sending SMS messages.
Send a Test Message	Click it to send a test e-mail according to above configuration.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the SMS service object, click **Clear**.

Mail Service Object

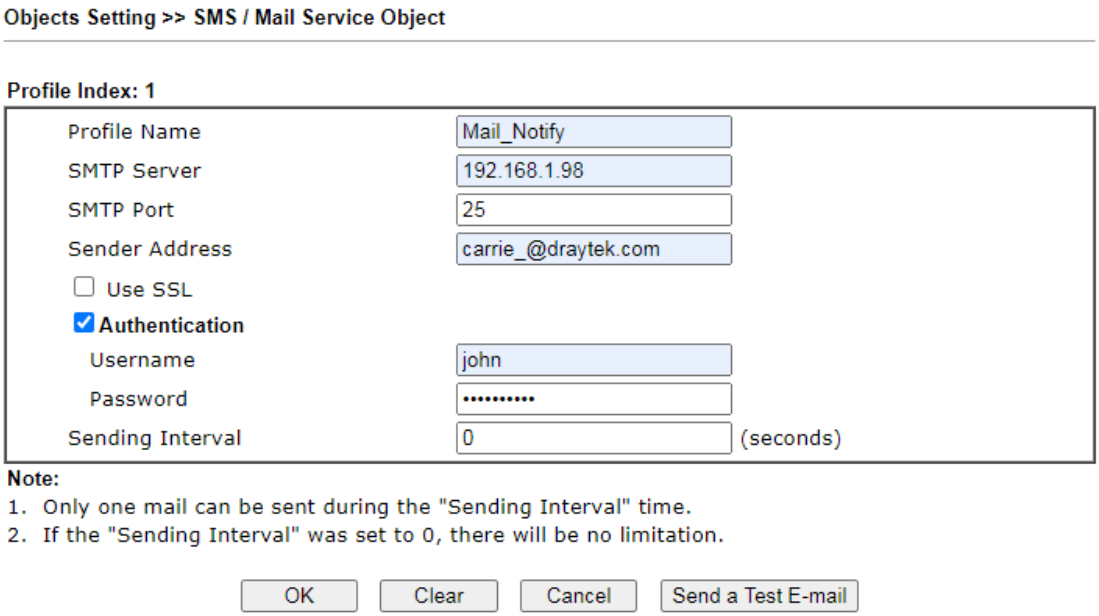
Up to 10 **Mail Service Objects** can be set up for use with **Application>>SMS/Mail Alert Service**.



Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Profile Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the service object.

To set up a profile, click the Mail Server tab, and then click its index to bring up the configuration page.



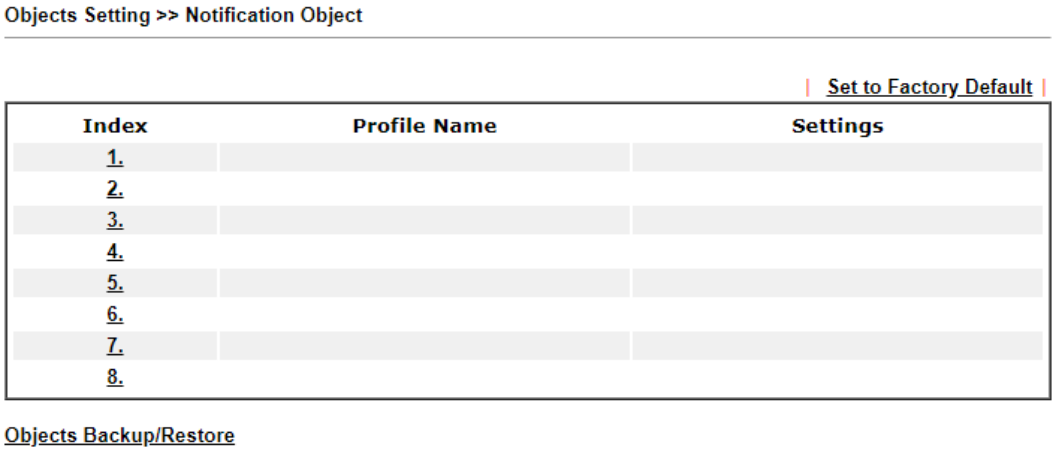
Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 31 characters.
SMTP Server	IP address of the SMTP server.
SMTP Port	Port number of the SMTP server.
Sender Address	E-mail address of the sender.
Use SSL	Check this box to use SMTPS (SMTP over SSL) to communicate with the SMTP server. Note that the de facto port used for SMTPS is 465.
Authentication	Select to send username and password to SMTP server for authentication. **Username** – Username for authentication. Maximum length is 31 characters. **Password** – Password for authentication. Maximum length is 31 characters.
Sending Interval	Minimum amount of time, in seconds, to wait between sending e-mail messages.
Send a Test E-mail	Click it to send a test e-mail according to above configuration.

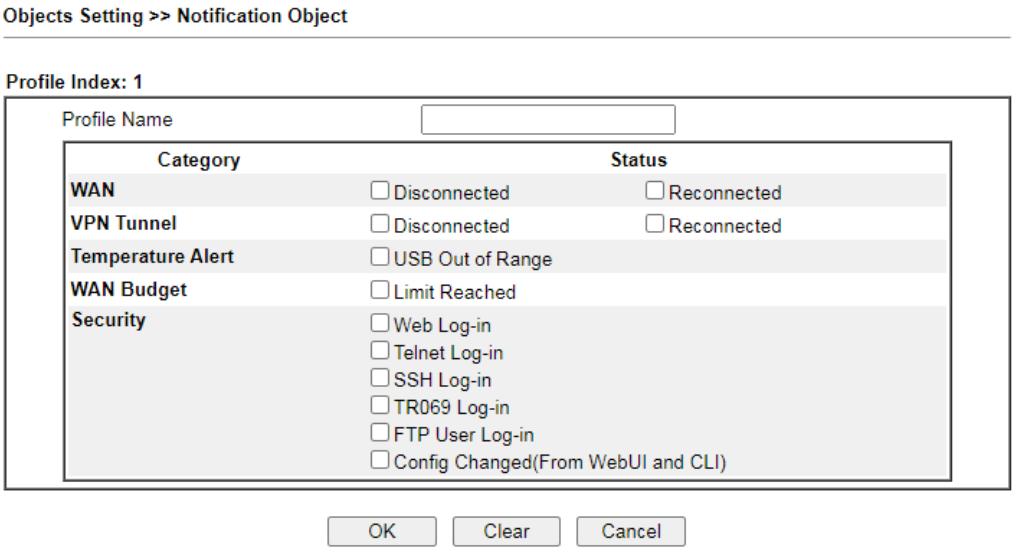
To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the mail service object, click **Clear**.

VII-1-11 Notification Object

Up to 8 Notification Objects can be set up for use in **Application>>SMS Alert Service** and **Application>>Mail Alert Service**.



To set up a profile, click its index to bring up the configuration page.



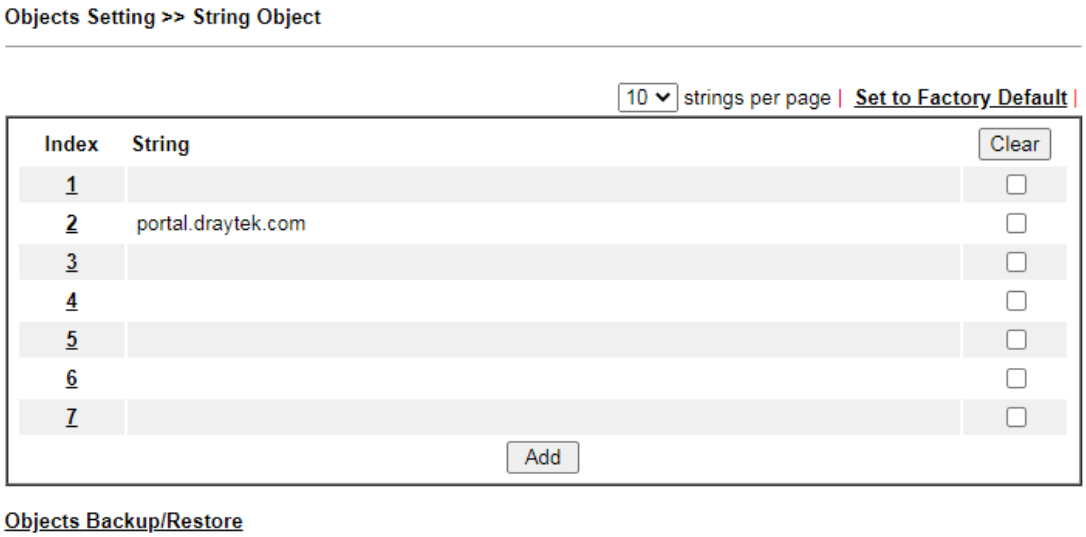
Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 31 characters.
Category	Areas to be monitored.
Status	Select the states to be monitored. For example, the check box of **CPE firmware upgrade fail** under the category of **Central VPN Management** is checked. Once such profile is enabled, Vigor router system will send out notification to the recipient via SMS.

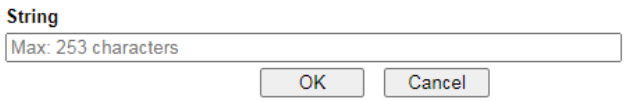
To save changes on the page, click OK. To discard changes, click Cancel.

VII-1-12 String Object

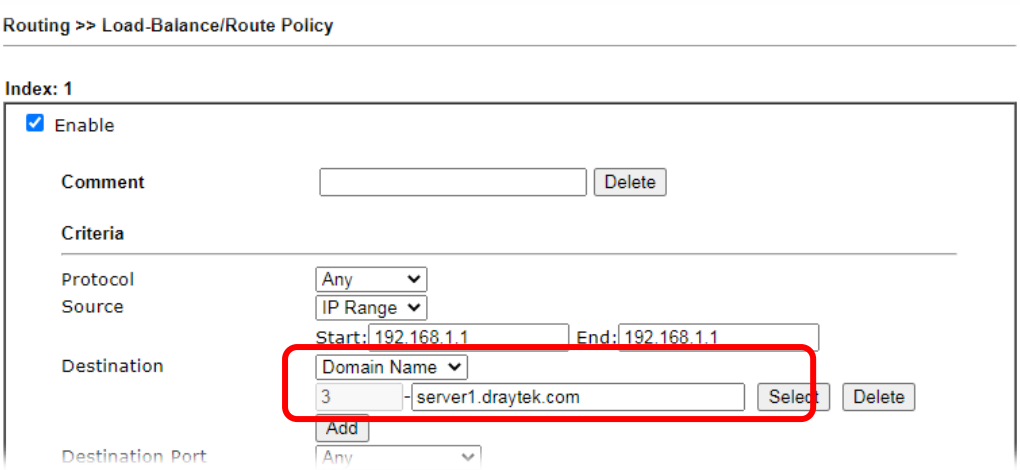
This page allows you to set string profiles which will be applied in route policy (domain name selection for destination) and etc.



Available settings are explained as follows:

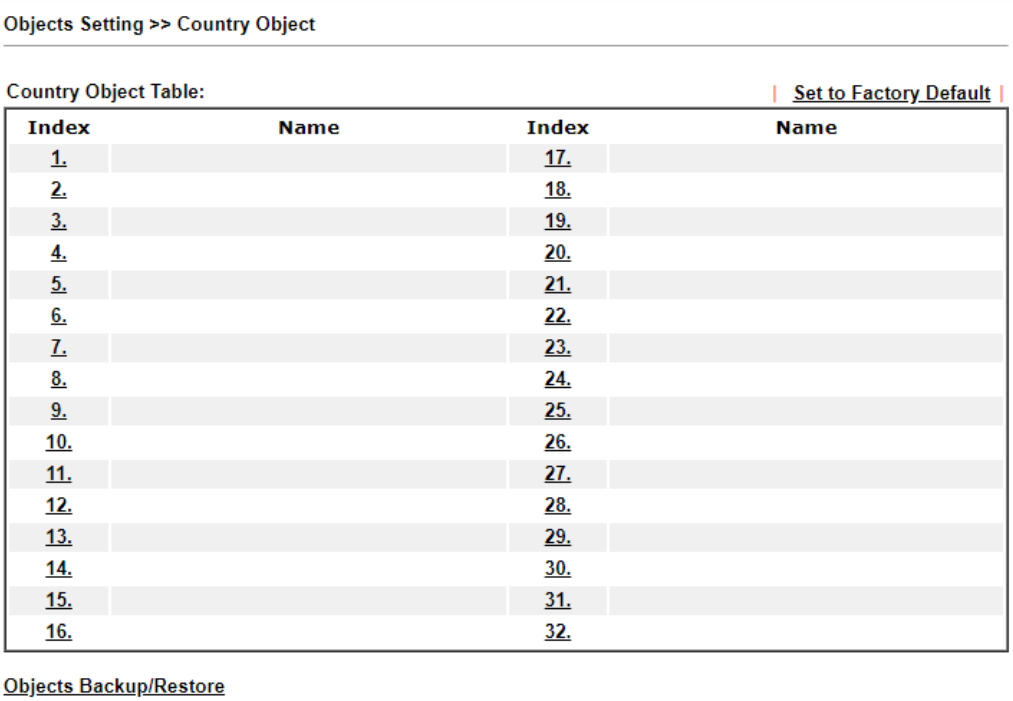
Item	Description
Add	Click it to open the following page for adding a new string object. 
Set to Factory Default	Click it to clear all of the settings in this page.
Index	Display the number link of the string profile.
String	Display the string defined.
Clear	Choose the string that you want to remove. Then click this check box to delete the selected string.
Objects Backup/Restore	Click it to backup or restore the string object.

Below shows an example to apply string object (in route policy):

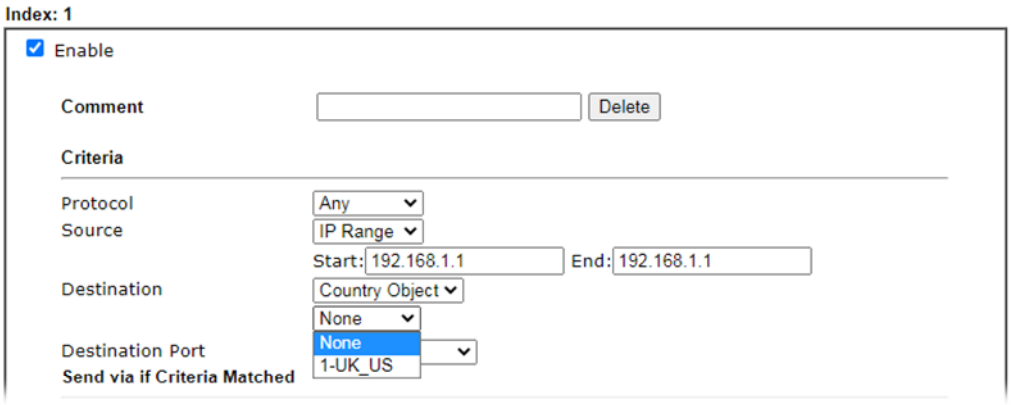


VII-1-13 Country Object

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



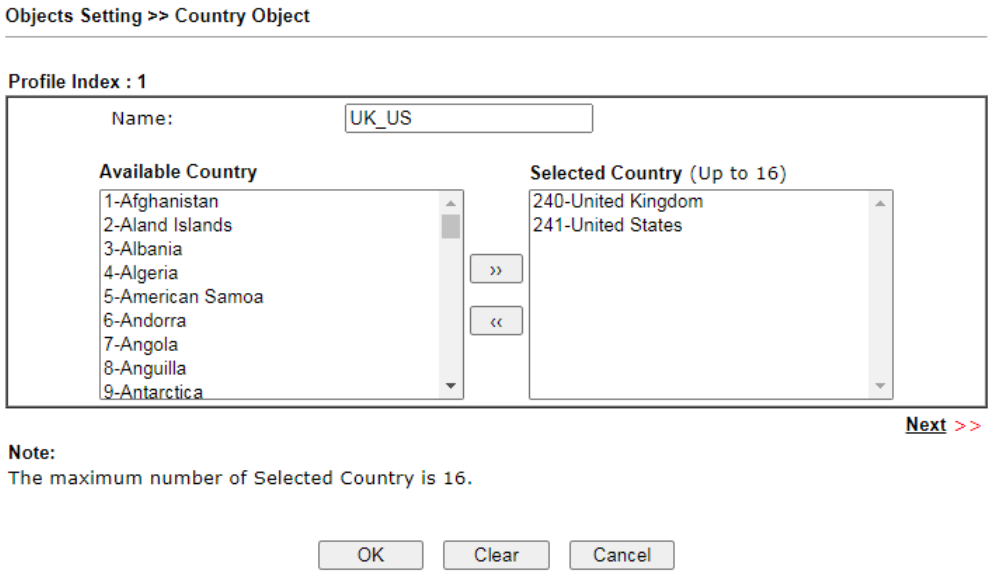
The country object, by grouping IP addresses for multiple countries, can be applied by other functions such as router policy destination (refer to the following figure for example).



To set a new profile, please do the steps listed below:

1. Open **Object Setting>>Country Object**, and click the number (e.g., #1) under Index column for configuration in details.

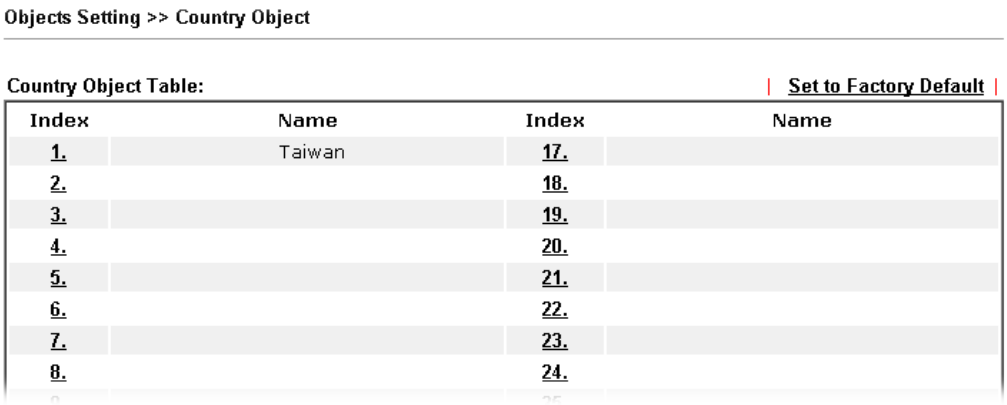
2. The configuration page will be shown as follows:



Available settings are explained as follows:

Item	Description
Name	Enter a name for such profile. The maximum length of the name you can set is 15 characters.
Available Country / Selected Country	Select any country from Available Country. Click >> to move the selected country and place on Selected Country. Note that one country profile can contain 1 up to 16 countries.

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



VII-1-14 Objects Backup/Restore

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

Available settings are explained as follows:

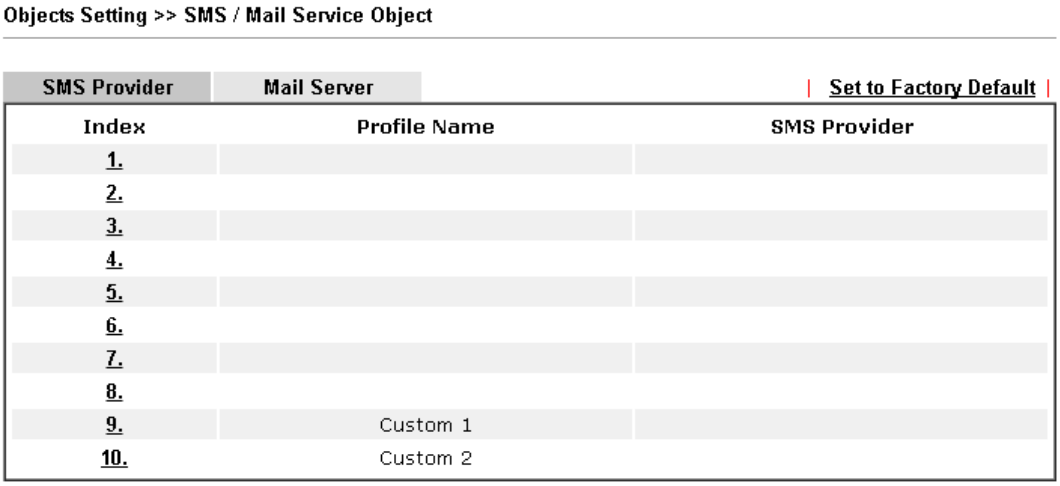
Item	Description
Backup	Usually, the IP objects can be created one by one through the web page of **Objects>>IP Object**. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file. All 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	**Select** – Click it to specify a predefined CSV file. **Restore** – Import the selected CSV file onto Vigor router.

Application Notes

A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

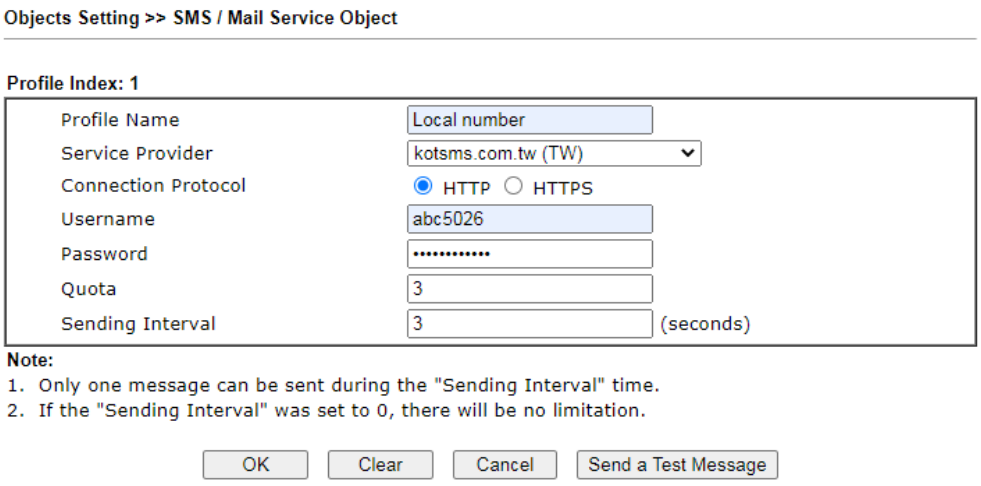
Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open **Object Settings>>SMS/Mail Server Object** to get the following page.

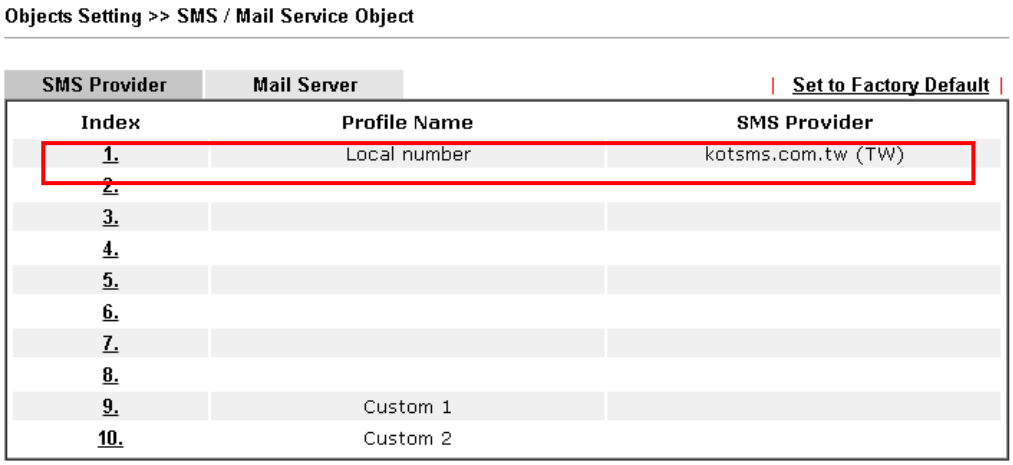


Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

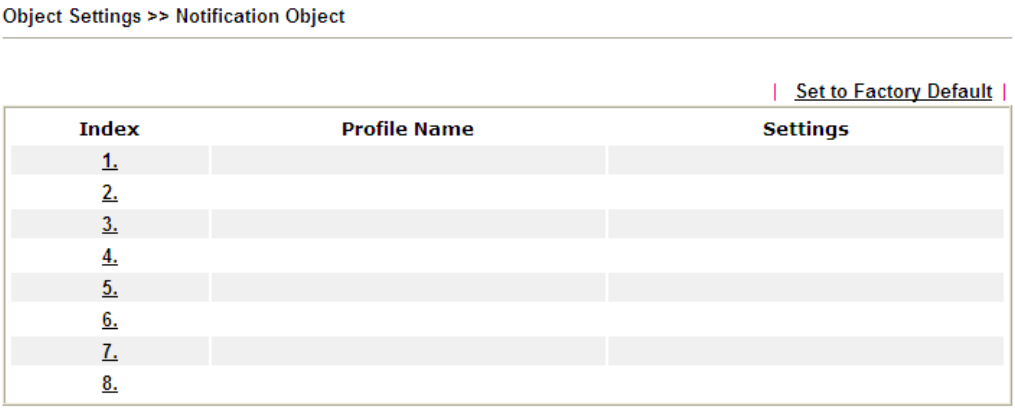
3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, Enter the username and password and set the quota that the router can send the message out.



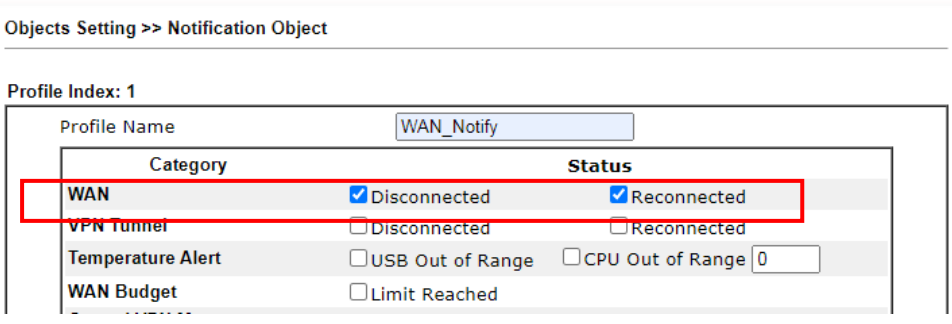
4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.



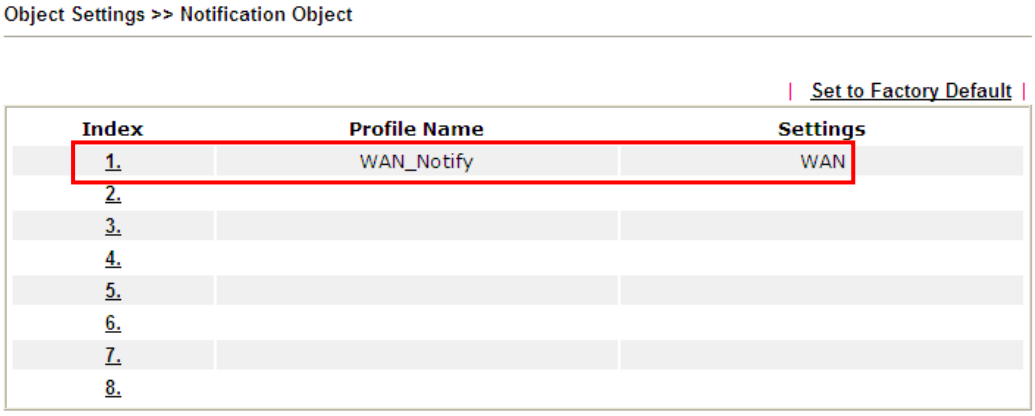
5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.



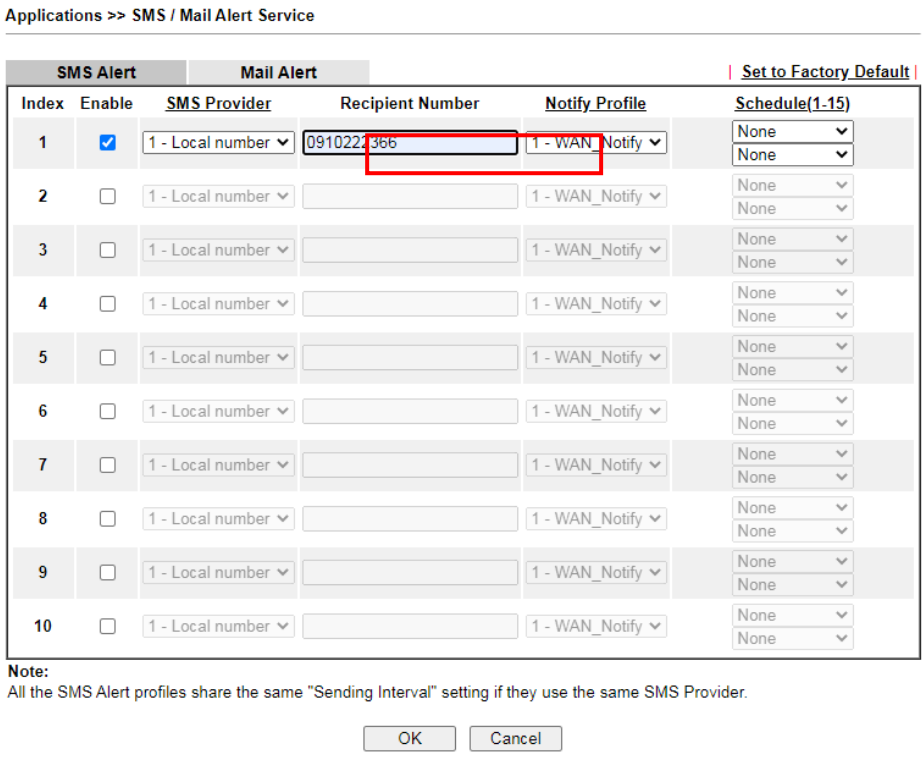
6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, Enter the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.



7. After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.



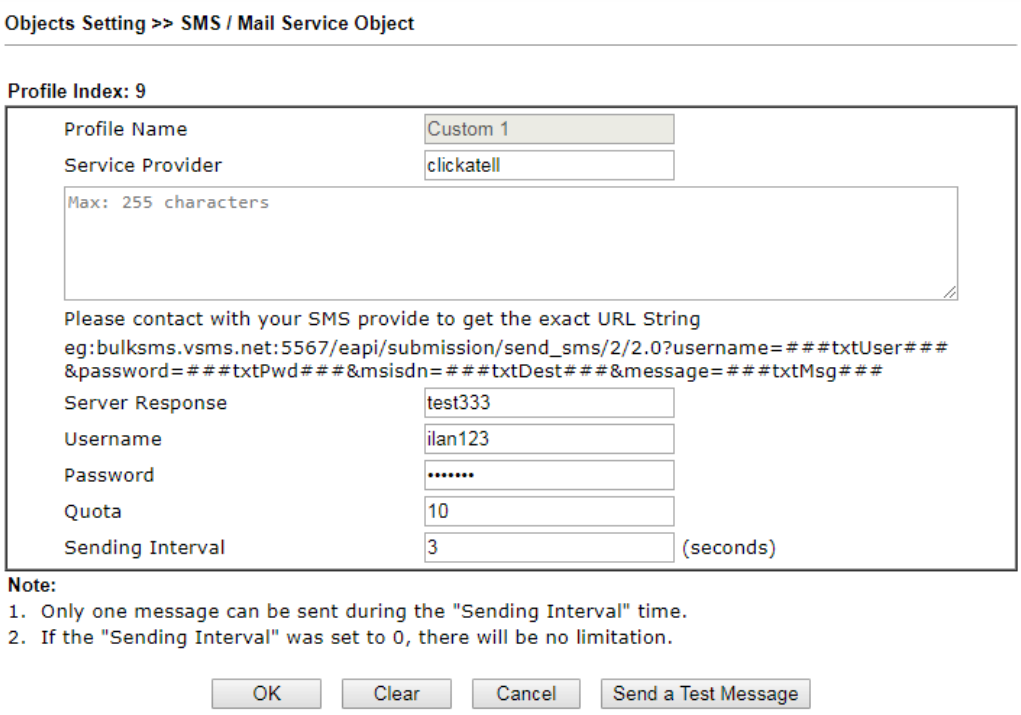
8. Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, Enter the phone number in the field of Recipient Number (the one who will receive the SMS).



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.



VII-2 USB Application

USB devices connected to the Vigor router can function as storage servers, WAN interfaces, network printers or thermometers.

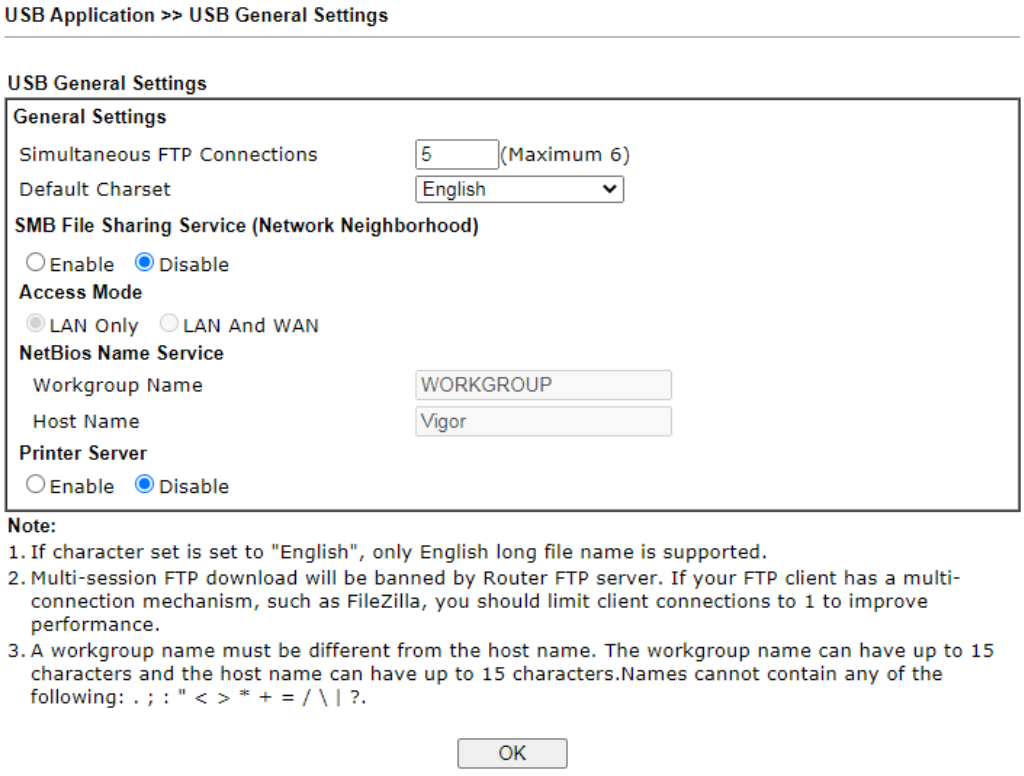
After setting the configuration in USB Application, a USB storage device can be accessed using either the FTP or SMB protocol from LAN clients with the IP address of the Vigor router and the username and password entered in **USB Application>>USB User Management**.

Info	USB modems that are supported by the router are listed in **USB Application>>Modem Support List**. For network connection via USB modem, refer to **WAN>>Internet Access** and **WAN>>General Setup** for detailed information.

Web User Interface

VII-2-1 USB General Settings

This page allows you to configure the file sharing feature of the Vigor router, where USB mass storage devices such as thumb drives and hard drives can be made accessible to LAN clients. Currently, only FAT16 and FAT32 file systems are supported by the Vigor router, so verify that the USB drive contains these file systems. FAT32 is recommended because of its long filename support, which FAT16 lacks.



Available settings are explained as follows:

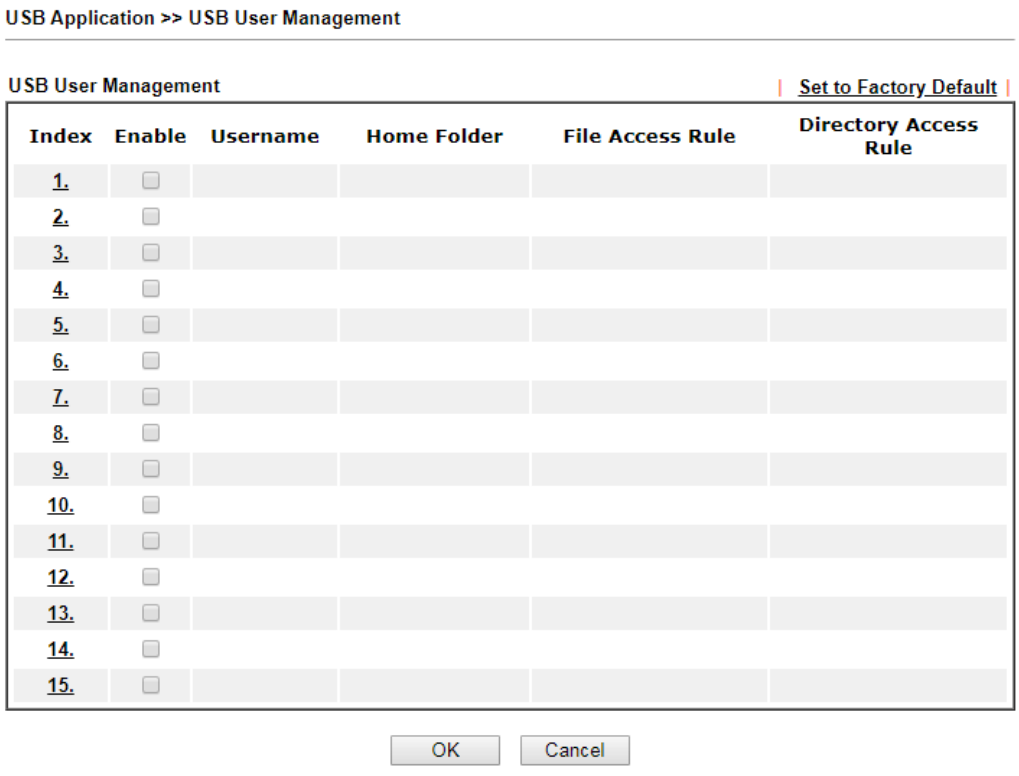
Item	Description
General Settings	**Simultaneous FTP Connections -** Enter the maximum number of simultaneous FTP sessions allowed. The router allows up to 6 simultaneous sessions. **Default Charset -** Select the character set for file and directory names. Currently, the Vigor router supports four

	character sets. The default charset is English.
SMB File Sharing Service	Click **Enable** to enable SMB service (file sharing).
Access Mode	**LAN Only** – Only users on the LAN can connect access the shared USB disk. **LAN And WAN** - Both LAN and WAN users can access SMB server of the router.
NetBios Name Service	For SMB file sharing service, you need to specify a workgroup name and a host name. The two names cannot be identical, and neither can contain any of the following characters: ; : " < > * + = \ | ? **Workgroup Name –** Enter the workgroup name. Maximum allowed length is 15 characters. **Host Name –** Enter the NetBIOS hostname for the router. Maximum allowed length is 23 characters.
Printer Server	**Enable** – Select to allow the Vigor router to act as a print server for printers connected the USB.

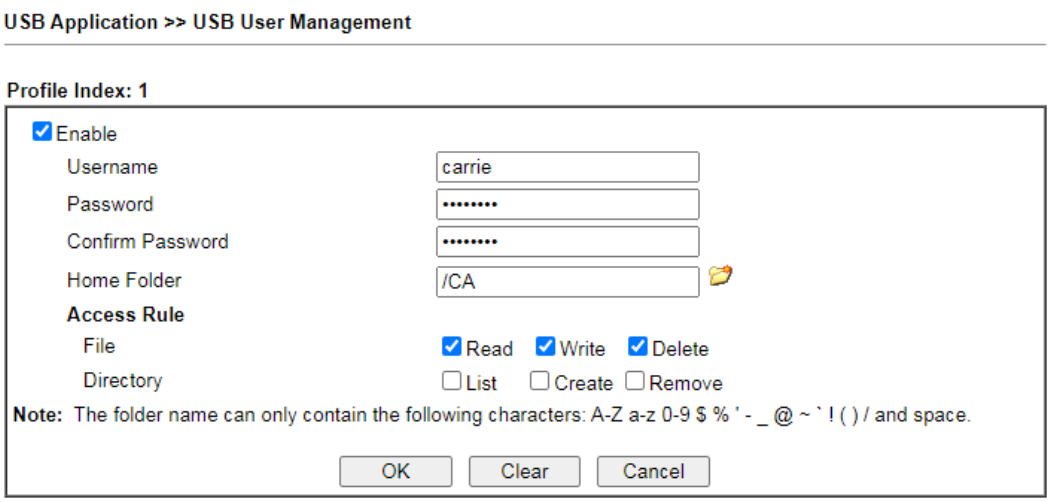
Select **OK** to save changes on the page.

VII-2-2 USB User Management

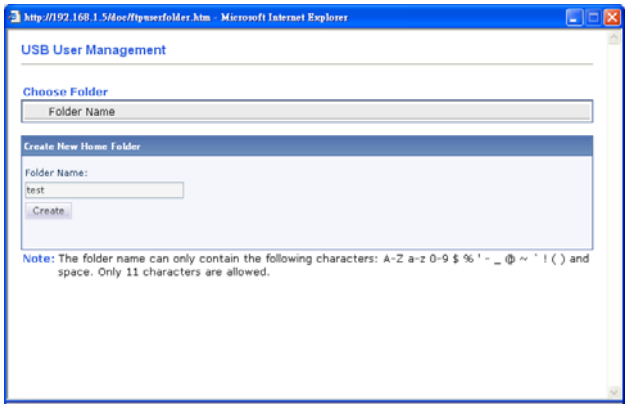
This page allows you to set up profiles for FTP/SMB users. Any user who wants to access the USB storage disk must authenticate using a username and password that have been configured on this page. Please connect a USB storage device before adding or modifying settings on this page, or else an error message will appear requesting you to do so before allowing you to proceed.



Click index number to access into configuration page.



Available settings are explained as follows:

Item	Description
Enable	Check to activate this profile (account) for FTP service and / or SMB service. Later, the user can use the username specified in this page to login into FTP server.
Username	Enter the username for this user profile. Maximum allowed length of the username is 11 characters. **Note:** Anonymous user access is not supported. **Note:** "Admin" cannot be used as a username, as it is reserved for access to web pages on the Vigor router, and for FTP firmware upgrade. **Note:** Ensure that the FTP client does not use passive FTP mode as it is not supported by the Vigor router.
Password	Enter the password for this user profile. Maximum allowed length of the username is 11 characters.
Confirm Password	Enter the password again to confirm.
Home Folder	Enter the folder which will be the root folder for FTP and SMB sessions established using the credentials of this user profile. Only folders and files inside this selected root folder are accessible to the user. In addition, if the user types "/" here, the user can access into all of the disk folders and files in USB storage disk. To browse the list of folders available for selection, or to create a new folder, click the icon.  **Note**: If the USB storage device is write-protected, new

	folders cannot be created. Only existing folders can be selected. **Note**: Only folders directly under the root can be selected as the home folder.
Access Rule	It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here. **File** – Check the items (Read, Write and Delete) for such profile. **Directory** –Check the items (List, Create and Remove) for such profile.

To save changes on this page, ensure that a USB storage device is connected, and click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP object, click **Clear**.

VII-2-3 File Explorer

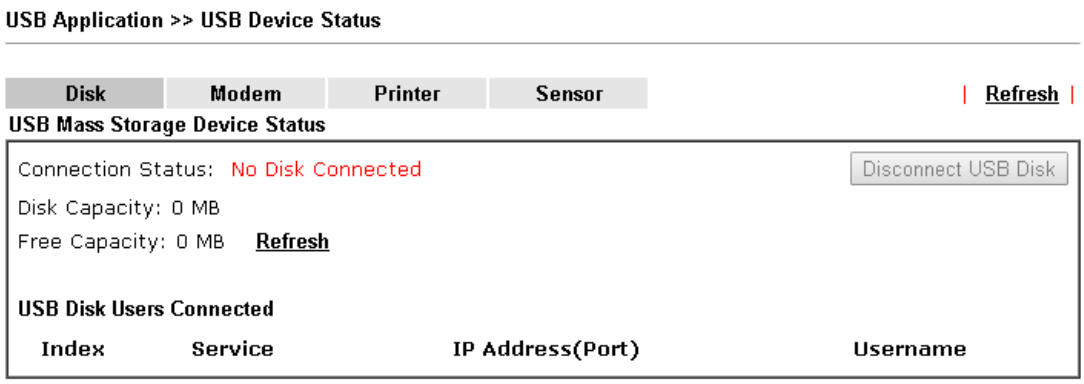
File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

Available settings are explained as follows:

Item	Description
Refresh	Click this icon to refresh the list of files and folders.
Back	Click this icon to return to the parent folder.
Create	Click this icon to add a new folder.
Current Path	Shows current folder.
Upload	To upload a file to the USB storage device, click the **Browse...** button to bring up the file selection dialog box. Select the file you wish to upload, and click the **Upload** button to initiate the upload process.

VII-2-4 USB Device Status

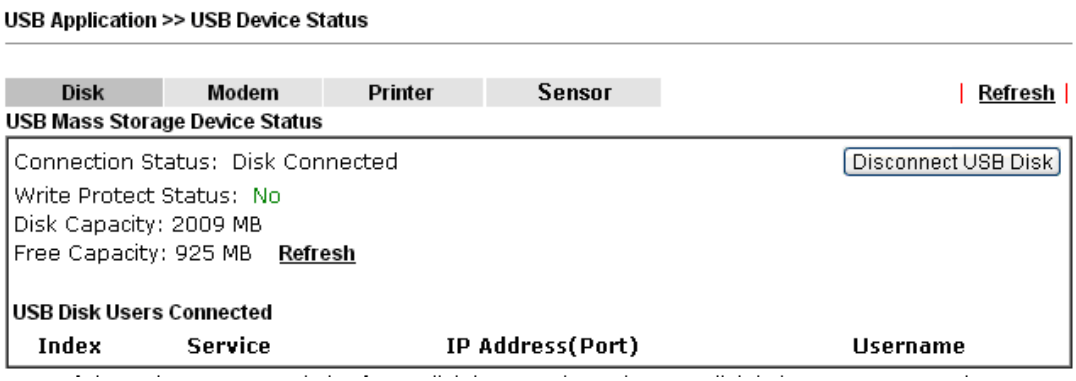
This page allows monitoring of the status of USB devices (disk, modem, printer, and sensor) connected to the Vigor router. To maintain the data integrity of a USB disk that is connected to the router, always click **Disconnect USB Disk** before unplugging the disk from the router.



Available settings are explained as follows:

Item	Description
Connection Status	Shows whether a USB disk is connected or not. If there is no USB device connected to the Vigor router, "No Disk Connected" will be displayed.
Disk Capacity	Shows the total capacity of the USB storage disk.
Free Capacity	Shows the free space on the USB storage disk. Click **Refresh** at any time to get the most up-to-date free capacity.
USB Disk Users Connected	Shows the clients that are connected to the SMB/FTP server. **Index** – The profile index used by the LAN client to establish the connection. **Service** – Shows whether the connection is using FTP or SMB. **IP Address** – Shows the client's IP address. **Username** – Shows the username used to establish the connection.
Disconnect USB Disk	Before unplugging the USB storage device from the router, make sure you click this first to ensure that all data has been written to the disk and all open files are closed.

After a USB storage device has been connected, the **Connection Status** will be updated within a few seconds.



VII-2-5 Temperature Sensor

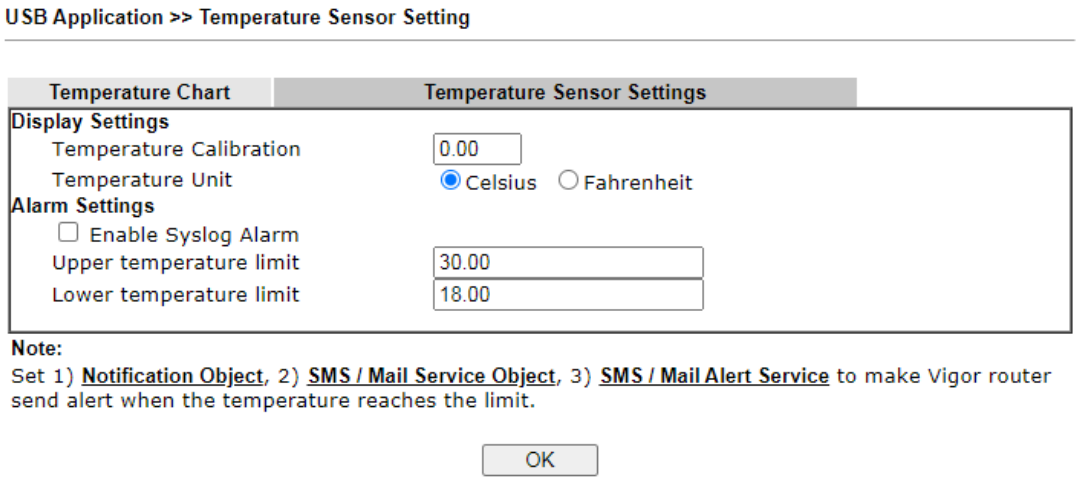
A USB Thermometer is now available. It complements your installed DrayTek router installations which will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

For a list of supported USB thermometers, visit our website at https://www.draytek.com/en/products/usb-thermometer/ or contact your local DrayTek partner.

Temperature Sensor Settings



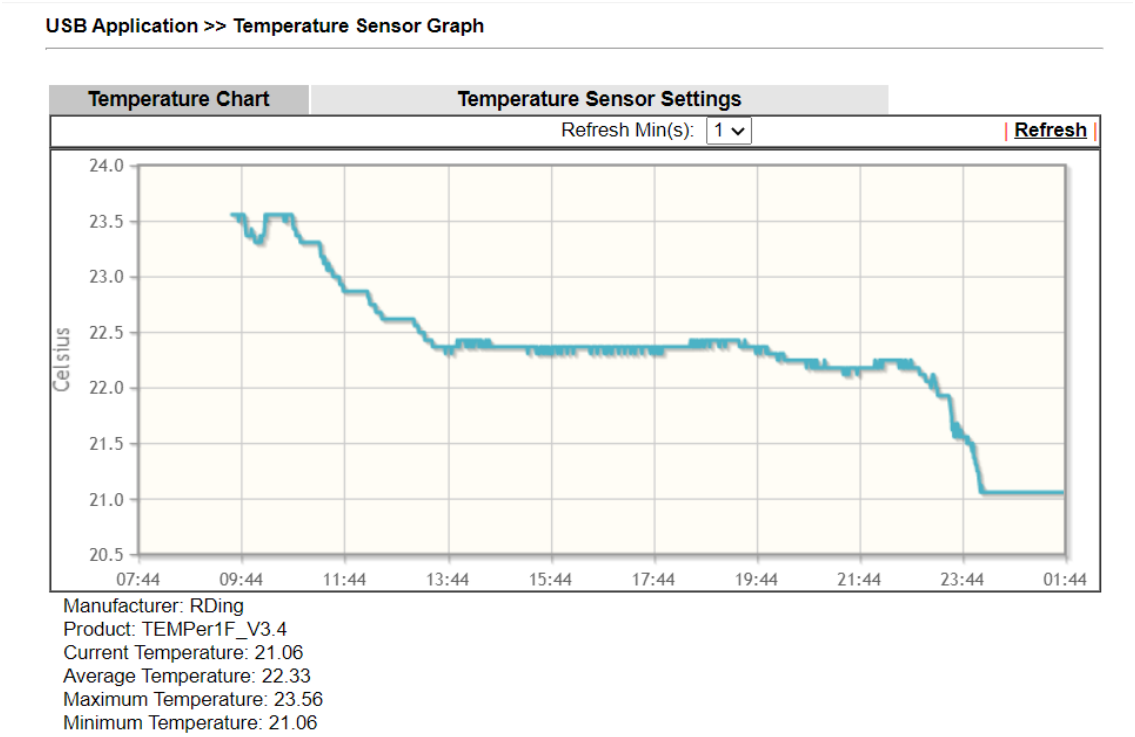
Available settings are explained as follows:

Item	Description
Display Settings	**Temperature Calibration** - Enter the difference between the actual temperature and the temperature as reported by the thermometer. **Temperature Unit -** Select the temperature scale to be used.
Alarm Settings	**Enable Syslog Alarm** - Select to enable recording of the temperature in Syslog.

	Upper temperature limit/Lower temperature limit - Enter the upper and lower temperature limits. If the temperature falls outside of this range, an alert will be sent.

Temperature Chart

Below shows an example of temperature graph:



VII-2-6 Modem Support List

This page lists the brands and models of USB modems that are supported by the Vigor router.

This list is subject to change between different versions of firmware as support for new modems are added.

USB Application >> Modem Support List

The following compatibility test lists 3.5G/LTE modems **supported by Vigor router under certain environment or countries.** If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

Brand	Model	LTE	Access Mode	Status
4G system	XSPlug P3		PPP	Y
Aiko	Aiko 76E		PPP	Y
Alcatel	Alcatel L100V	✓	DHCP	Y
	Alcatel L800	✓	DHCP	Y
	Alcatel W800	✓	DHCP	Y
	Alcatel X500		PPP	Y
	Alcatel Y855	✓	DHCP	Y
Alfa	ALFA Flyppp		PPP	Y
Amoi	Amoi H01		PPP	Y
BandRich	Bandluxe C321		PPP	Y
	Bandluxe C330		PPP	Y
	Bandluxe C331		PPP	Y
	Bandluxe C502		PPP	Y
BigPond	BigPond Next G Wireless		PPP	Y
	Broadband USB Mobile Card		PPP	Y
D-Link	D_LINK DWM156		DHCP	M
	Huawei E150		PPP	Y
	Huawei E153		PPP	Y
	Huawei E172		PPP	Y

VII-2-7 SMB Client Support List

This page shows a list of SMB clients on various platforms, and their levels of compatibility with the Vigor router as determined by our in-house testing. This list is subject to change as support for SMB clients are added or improved.

USB Application >> SMB Client Support List

The following compatibility test lists suggested SMB clients supported by Vigor router.

Platform	Application	Status
Microsoft® Windows® XP	Built in	I
Microsoft® Windows Vista™	Built in	Y
Microsoft® Windows® 7	Built in	Y
Microsoft® Windows® 8	Built in	M
Microsoft® Windows® 10	Built in	Y
OS X® 10.7.5	Built in	Y
OS X® 10.10	Built in	Y
Ubuntu 14.04	Built in	Y
Android™	AndSMB	Y
Android™	ES File Explorer	Y
Android™	File Expert	Y
Android™	File Manager	Y
Android™	Solid Explorer	Y
Android™	SharesFinder	Y
iOS	eXPlayer	Y
iOS	nPlayer	Y

Y: Tested and is supported.
I: Supported but has some issue.
M: Has not been tested but might be supported.

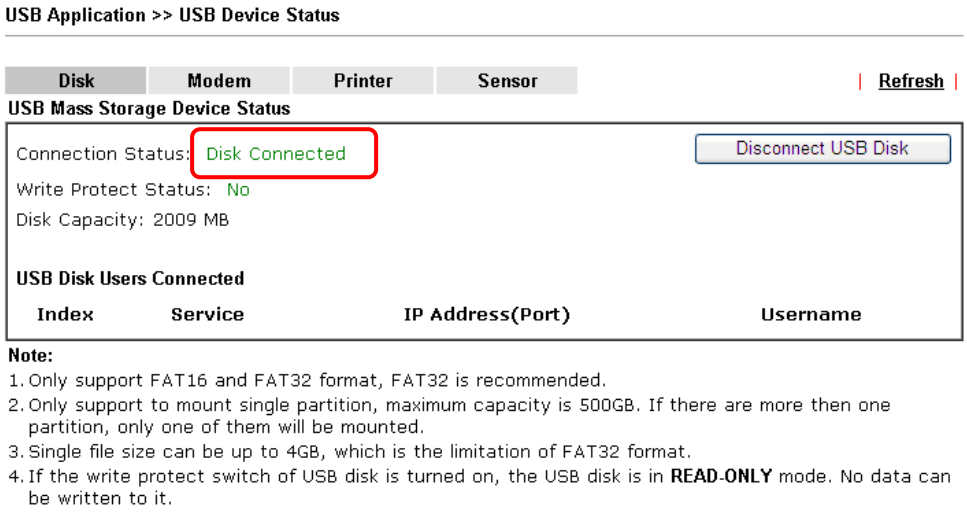
Application Notes

A-1 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SMB server or FTP server.

SMB service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

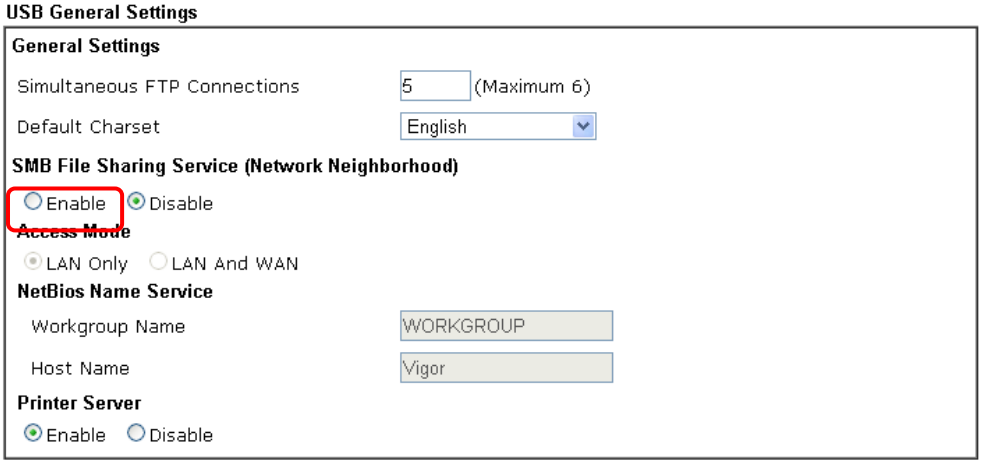
1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:



2. Then, please open **USB Application >> USB General Settings** to enable SMB service.

USB Application >> USB General Settings

USB General Settings

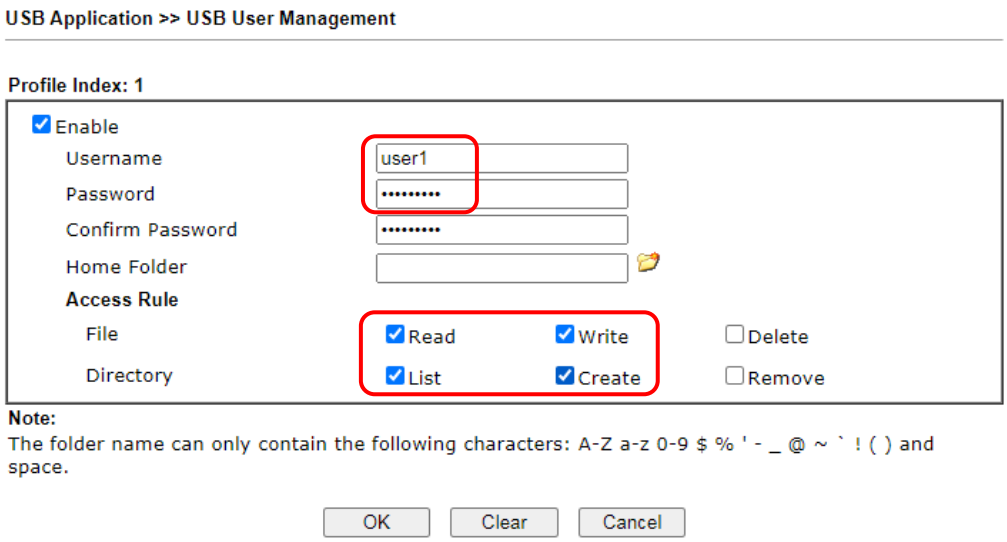


Note:

1. If character set is set to "English", only English long file name is supported.
2. Multi-session FTP download will be banned by Router FTP server. If your FTP client has a multi-connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
3. A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters.Names cannot contain any of the following: . ; : " < > * + = / | ?.

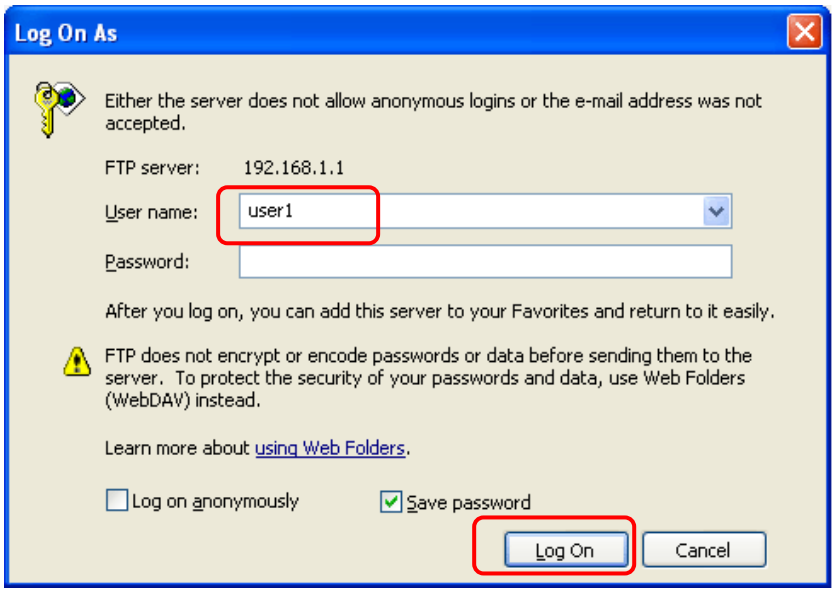
OK

3. Setup a user account for the FTP service by using **USB Application >>USB User Management.** Click **Enable** to enable FTP/SMB User account. In the example below, we have set up a new account with the username "user1", and granted "Read", "Write" and "List" permissions to it.

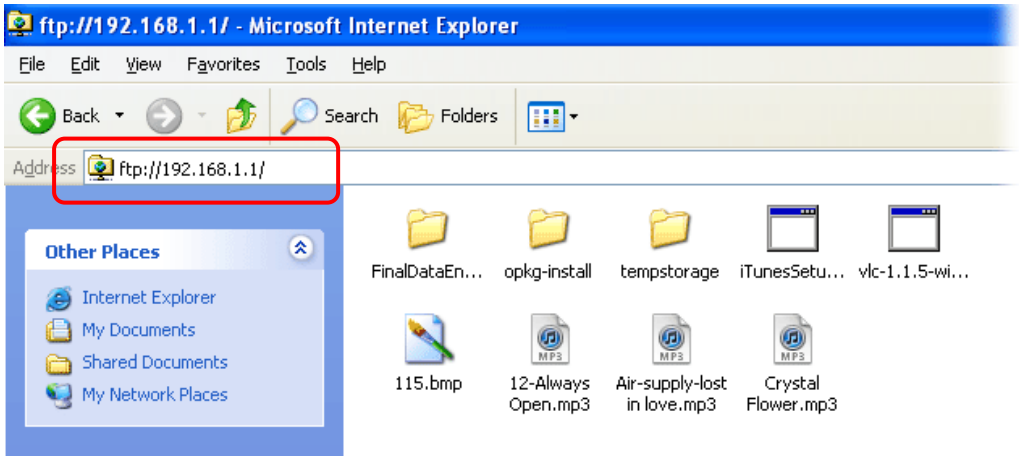


4. Click **OK** to save the configuration.

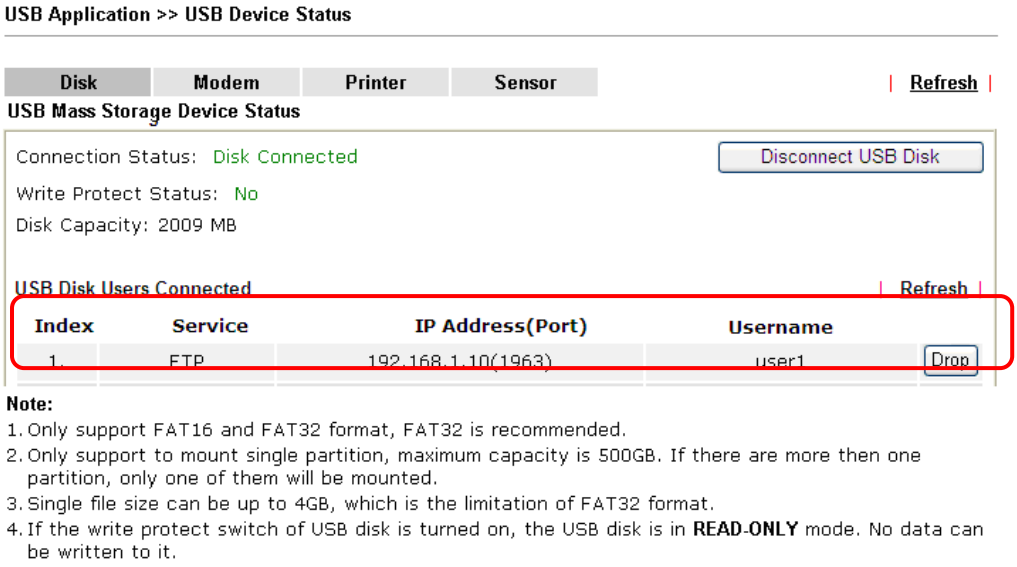
5. To verify that the FTP service is running properly, open a browser window and enter ftp://192.168.1.1 as the destination. Replace 192.168.1.1 with the actual IP address of the router. When prompted to enter the login credentials, enter the username "user1" to login.



6. When the following screen appears, you have successfully connected to the FTP server and verified that it is running properly.



7. If you check **USB Application >> USB Disk Status** on browser, you will see the FTP session initiated by user1.



Note:

1. Only support FAT16 and FAT32 format, FAT32 is recommended.
2. Only support to mount single partition, maximum capacity is 500GB. If there are more then one partition, only one of them will be mounted.
3. Single file size can be up to 4GB, which is the limitation of FAT32 format.
4. If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

Now, users in LAN of Vigor2135 can access into the USB storage device by entering ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management.**

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

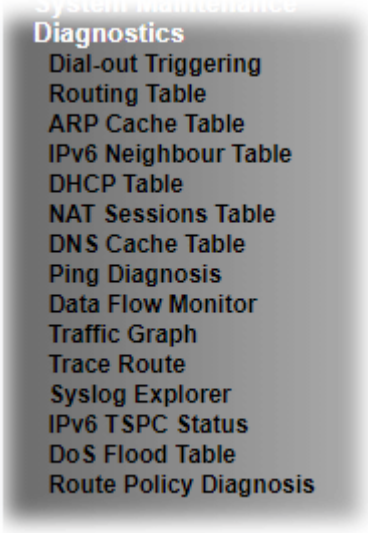
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- 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.

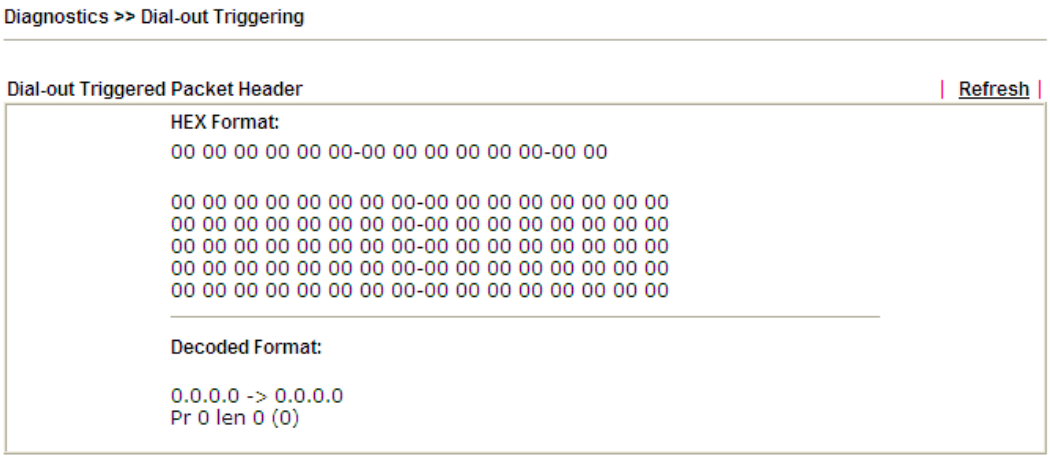
Web User Interface

This section contains utilities that can assist you in analyzing issues and failures during the setup and operation of the router.



VIII-1-1 Dial-out Triggering

This page shows the packet header that is transmitted when a WAN connection (such as a PPPoE connection) is initiated.

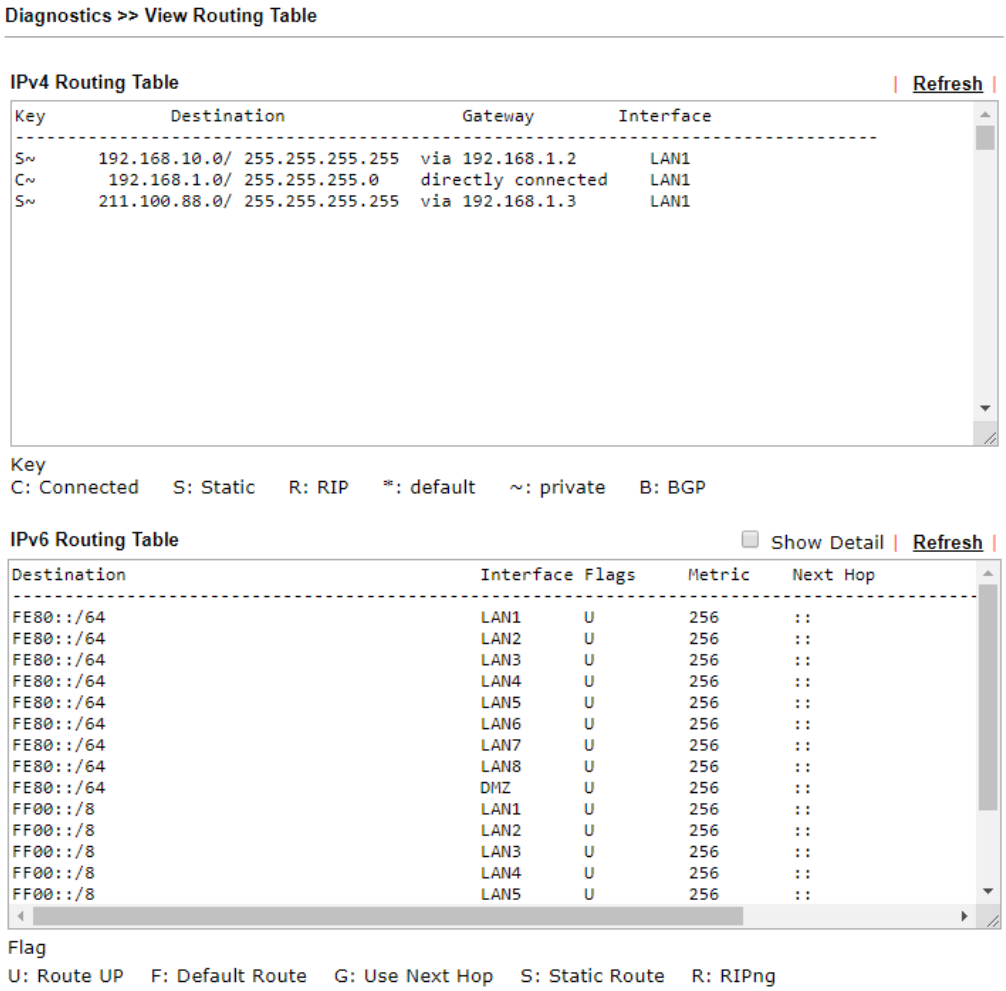


Available settings are explained as follows:

Item	Description
HEX Format	Shows the dial-out triggered packet header in hexadecimal format.
Decoded Format	Shows the dial-out triggered packet header in human-readable format.
Refresh	Click it to reload the page.

VIII-1-2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

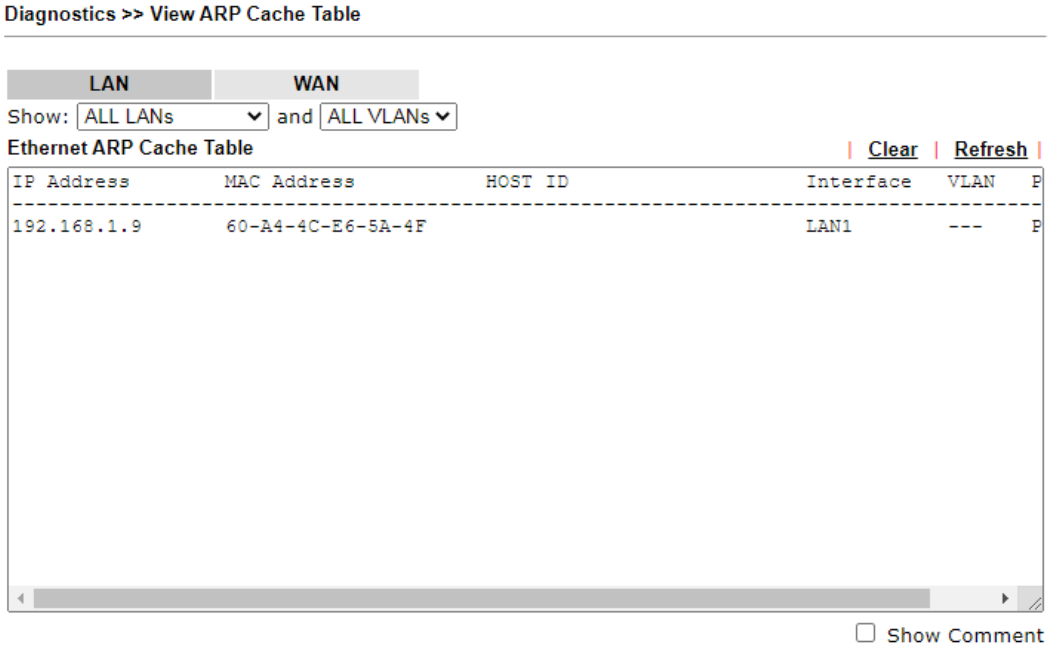


Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-3 ARP Cache Table

Click **Diagnostics** followed by **ARP Cache Table** to view the contents of the ARP (Address Resolution Protocol) cache held in the router. The table shows the mappings between Ethernet hardware addresses (MAC Addresses) and IP addresses.



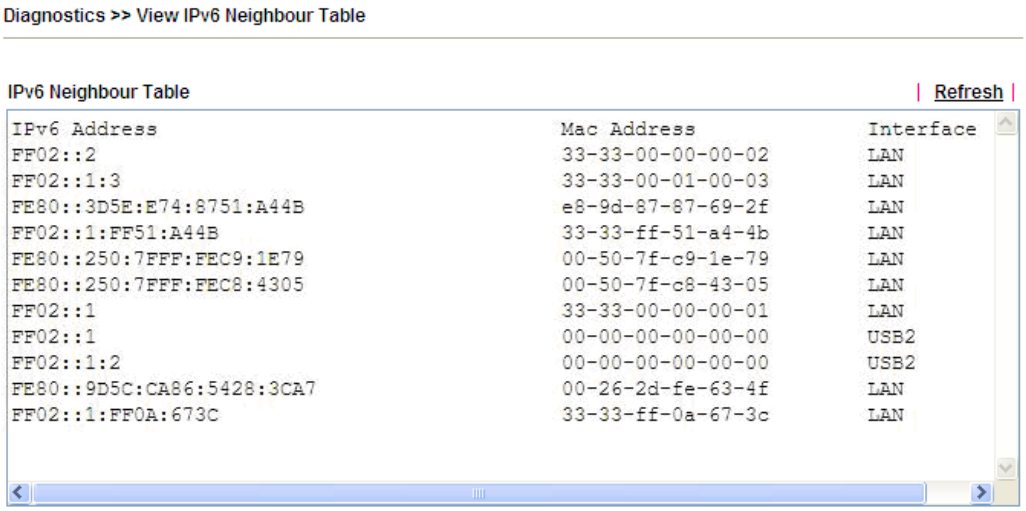
Available settings are explained as follows:

Item	Description
Show	Select the LAN(s) and VLAN(s) to display ARP table information. By default, information on all LANs and VLANs is displayed.
Refresh	Click it to reload the page with the most up-to-date information.

VIII-1-4 IPv6 Neighbour Table

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

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.



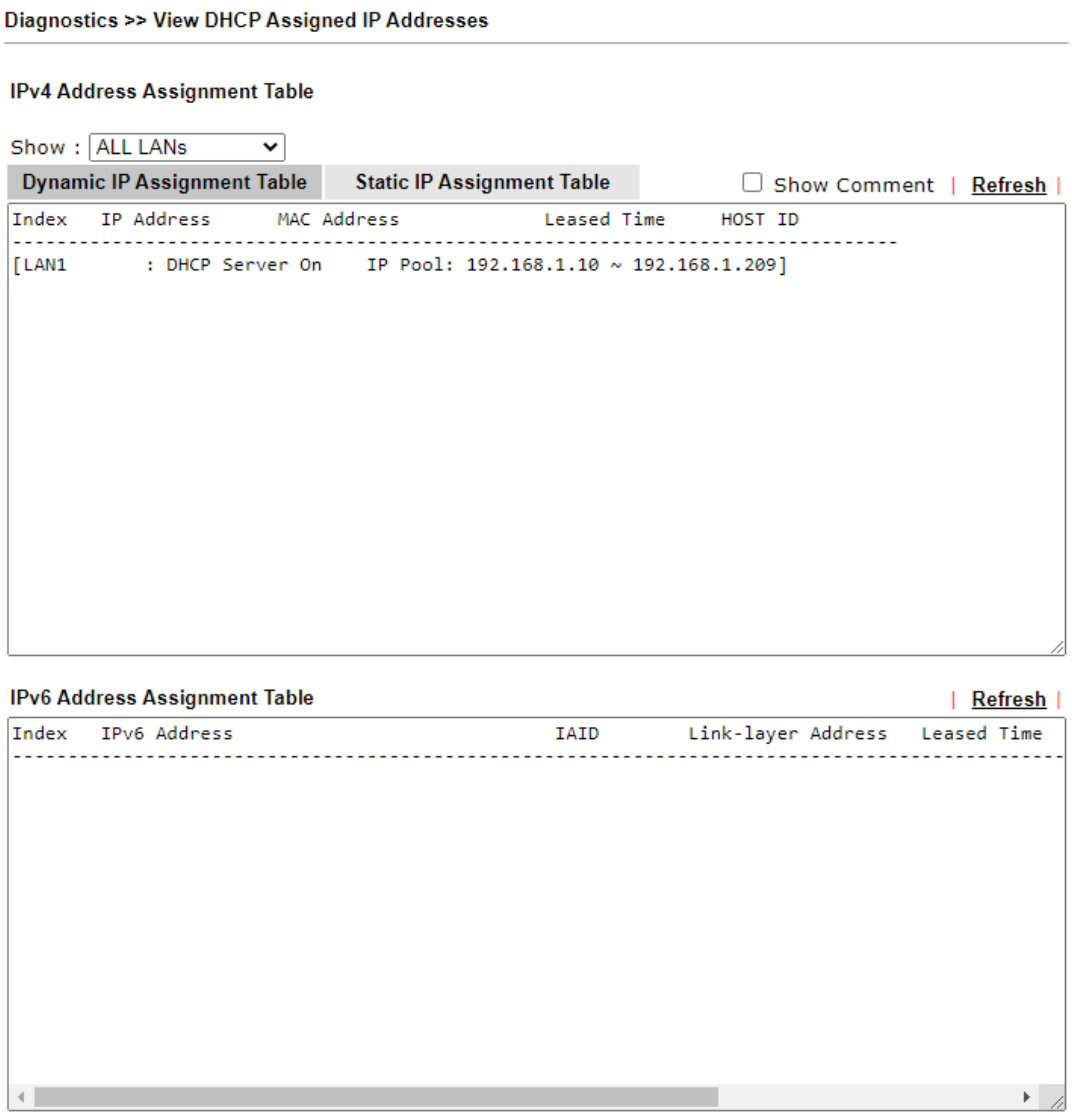
Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page with the most up-to-date information.

VIII-1-5 DHCP Table

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

Click **Diagnostics** and click **DHCP Table** to open the web page.



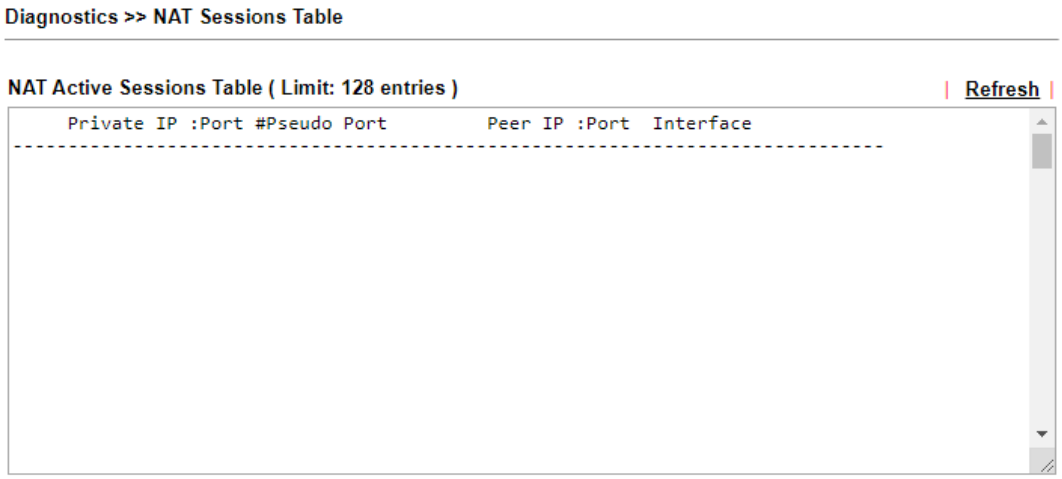
Available settings are explained as follows:

Item	Description
Index	Shows the index of the DHCP entry.
IP Address	Shows the IP address assigned by the router to the MAC address.
MAC Address	Shows the MAC address of this DHCP entry.
Leased Time	Shows the remaining time of the DHCP lease of the device.
HOST ID	Shows the host ID of this network device.
Refresh	Click to reload this page with the most up-to-date information.

VIII-1-6 NAT Sessions Table

This screen shows the 128 newest entries in the 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:	Shows the IP address of the LAN host.
Port #	Shows the port number used on the LAN host for this NAT session.
Pseudo Port	Shows the external port number used on the WAN interface for this NAT session.
Peer IP:	Shows the remote host's IP address.
Port	Shows the port number used on the remote host for this NAT session.
Interface	Shows the WAN interface used for this NAT session.
Refresh	Click to reload this page with the most up-to-date information.

VIII-1-7 DNS Cache Table

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

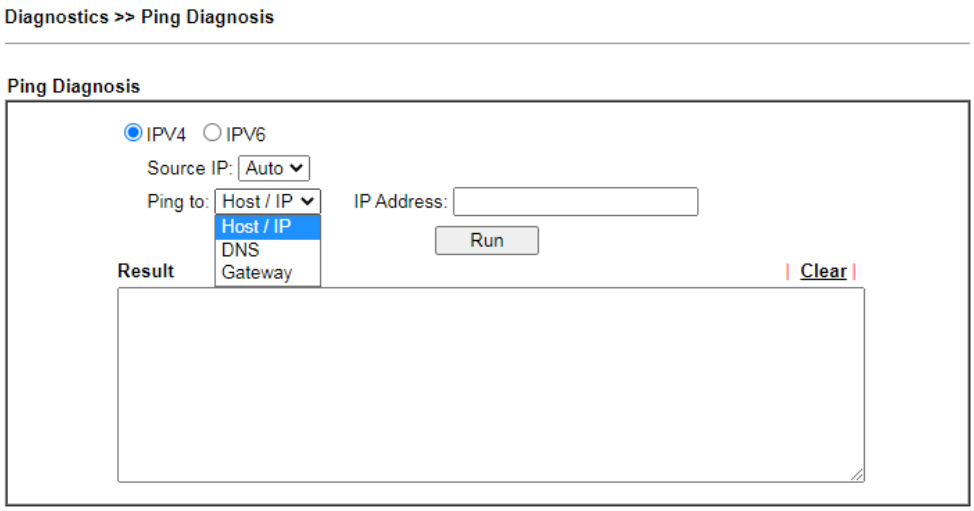
Click **Diagnostics** and click **DNS Cache Table** to open the web page.

Available settings are explained as follows:

Item	Description
Clear	Click to clear all cached DNS lookup entries.
Refresh	Click it to reload the page.
When an entry's TTL is larger than….	When this box is checked, DNS entries whose TTL (time to live, in seconds) exceeds the valued specified here will be deleted from the router's cache automatically. Be sure to click OK after making changes to have them saved.

VIII-1-8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to open the web page.



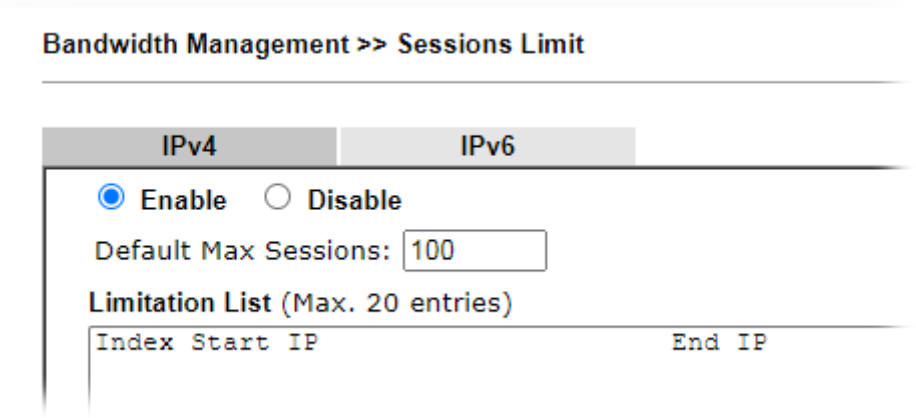
or

Available settings are explained as follows:

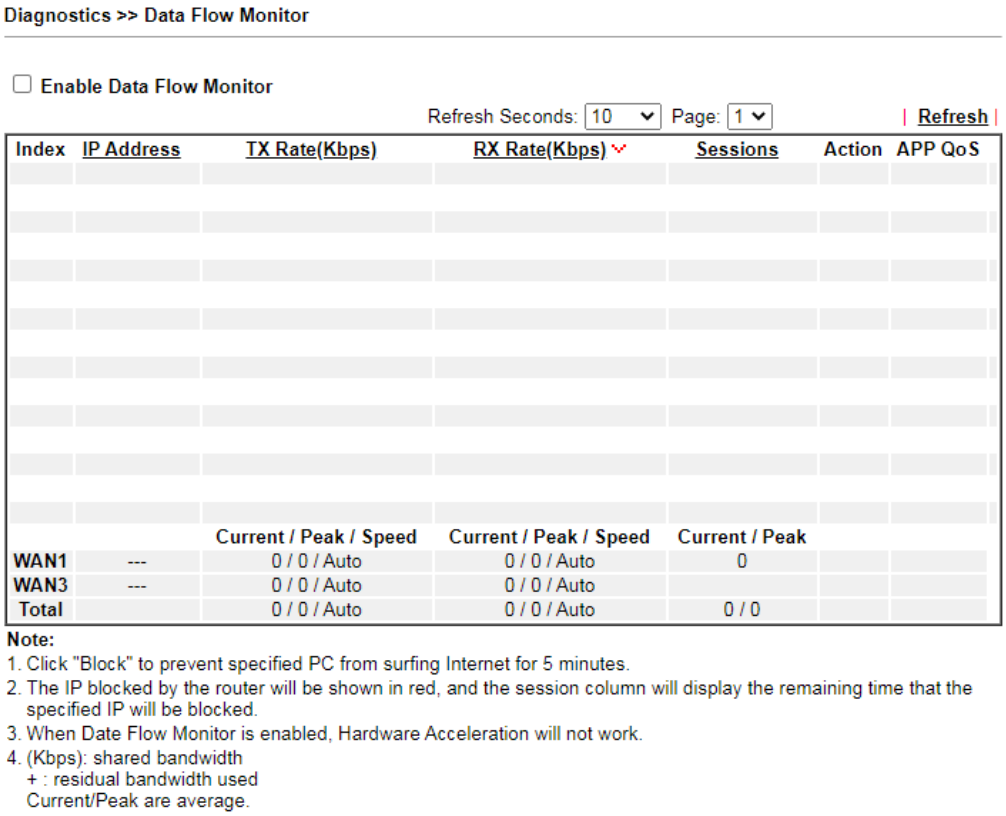
Item	Description
IPV4 /IPV6	Select the protocol to perform the ping operation.
Source IP	Choose **Auto** to be let the router select the WAN interface.
Ping to	Select the type of target to which you wish to ping.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Enter the IPv6 address that you want to ping.
Run	Click this button to initiate the ping process.The result will be displayed on the screen.
Clear	Click this link to clear the ping result.

VIII-1-9 Data Flow Monitor

This page displays the uplink and downlink rates, and number of sessions of each LAN client. The information is refreshed at an interval specified by the user. Before using the Data Flow Monitor, LAN clients that are to be monitored need to have their IP addresses configured in Bandwidth Management, and Bandwidth and Session Limits must be specified. Otherwise, a dialog box will appear reminding you to do so.

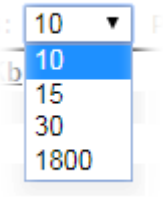
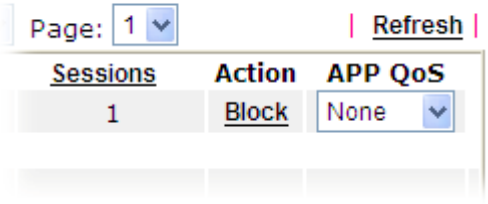
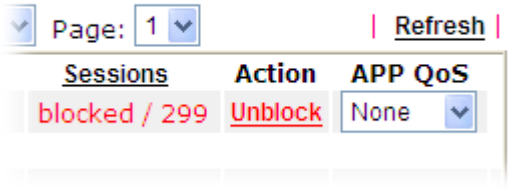
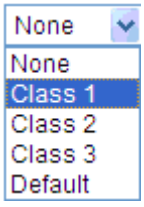


Click **Diagnostics** and click **Data Flow Monitor** to load the web page. You can click IP Address, **TX rate**, **RX rate** or **Sessions** links in the header to sort the displayed data.



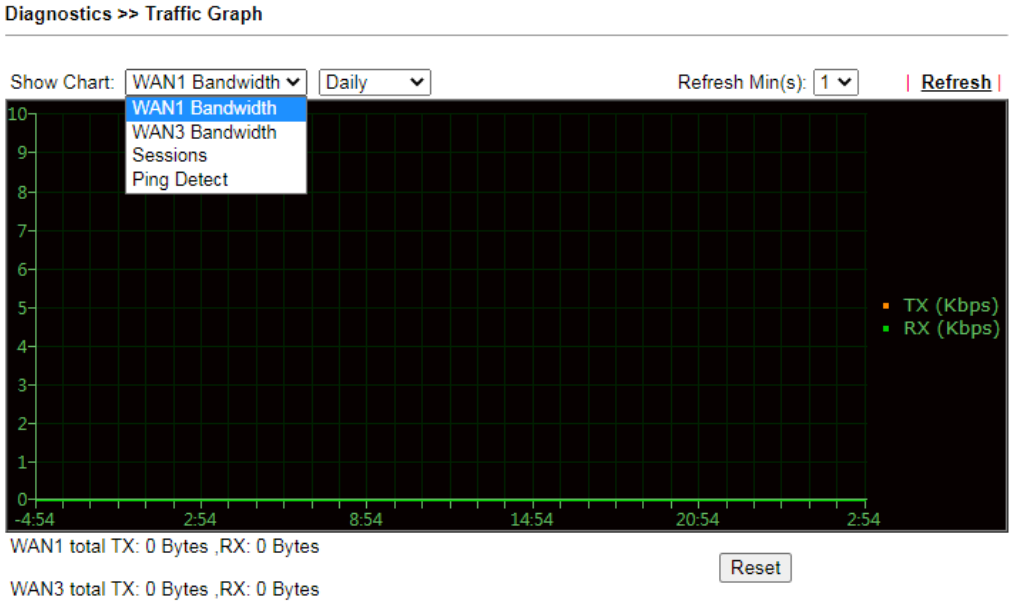
Available settings are explained as follows:

Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Select the desired refresh time interval from the drop-down list. The page will then be refreshed with updated information at the selected interval.

	
Refresh	Click to refresh this page manually.
Index	Shows the index of the data flow.
IP Address	Shows the IP address of the monitored device.
TX Rate (kbps)	Shows the transmission speed of the monitored device.
RX Rate (kbps)	Shows the receiving speed of the monitored device.
Sessions	Shows the number of session that you specified on the 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. 
APP QoS	Use the drop down list to change the priority in data transmission for the specified IP address (host). 
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 WAN1/ WAN3 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.

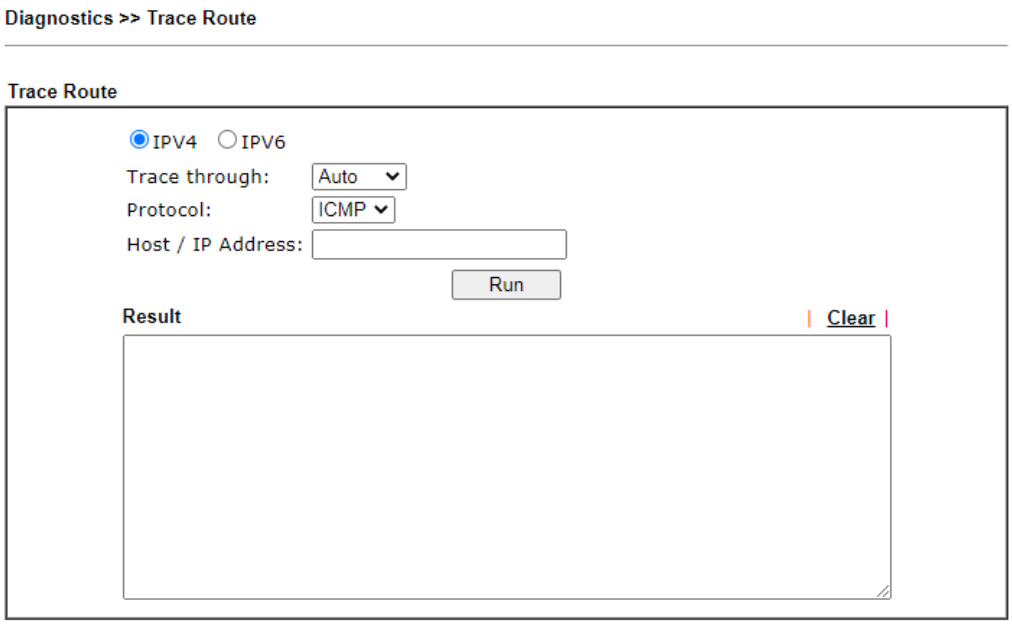


The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/ WAN3 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

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	Select the IP version used to perform the trace route.
Trace through	Select the WAN interface used to perform the trace route.
Protocol	Select either UDP or ICMP used to perform the trace route.
Host/IP Address	Enter the hostname or the IP address of trace route destination.

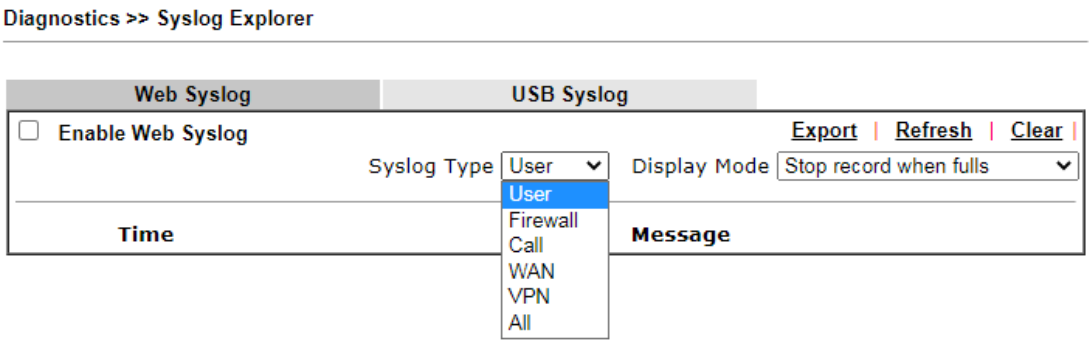
Trace Host/IP Address	Enter the hostname or the IPv6 address of trace route destination.
Run	Click this button to start the trace.
Clear	Click to clear the trace route result.

VIII-1-12 Syslog Explorer

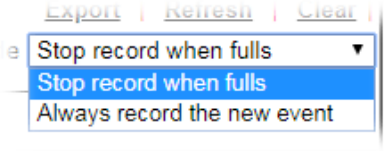
This page displays syslog information in real time. There are two options for displaying syslog information: Web Syslog and USB Syslog.

For Web Syslog

This page displays User/Firewall/call/WAN/VPN Syslog events and their time of occurrence. To enable Web Syslog, check the **Enable Web Syslog** checkbox, specify the type of Syslog events to view, and select the display mode. The log messages will start appearing as events matching the selected type occur.

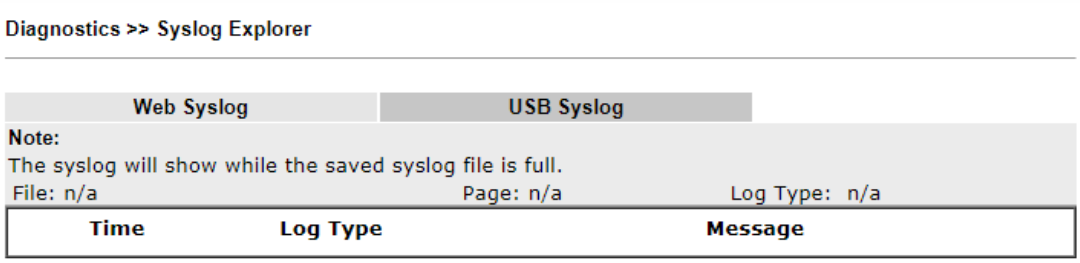


Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable Web Syslog.
Syslog Type	Select the type of Syslog info to monitor.
Export	Click to save the data as a file.
Refresh	Click to refresh this page manually.
Clear	Click to purge Syslog entries from the Web Syslog buffer.
Display Mode	Two display modes are available.  **Stop record when fulls** - When the Web Syslog buffer is full, no further logging will be performed. **Always record the new event** - Events are recorded in a FIFO manner. As the buffer gets full, oldest events are purged to make room for new events.
Time	Displays the time when the event occurred.
Message	Displays the event information.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.



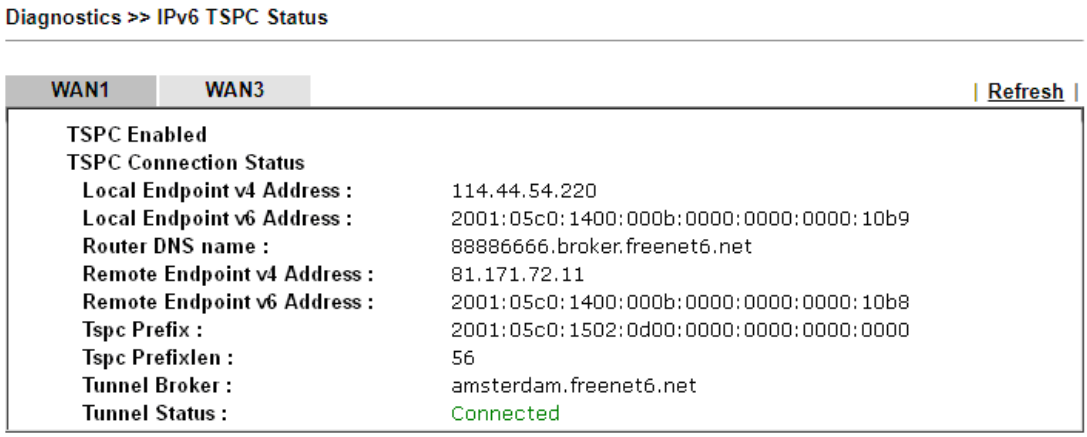
Available settings are explained as follows:

Item	Description
Time	Displays the time of the event occurred.
Log Type	Displays the type of the record.
Message	Displays the information for each event.

VIII-1-13 IPv6 TSPC Status

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

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



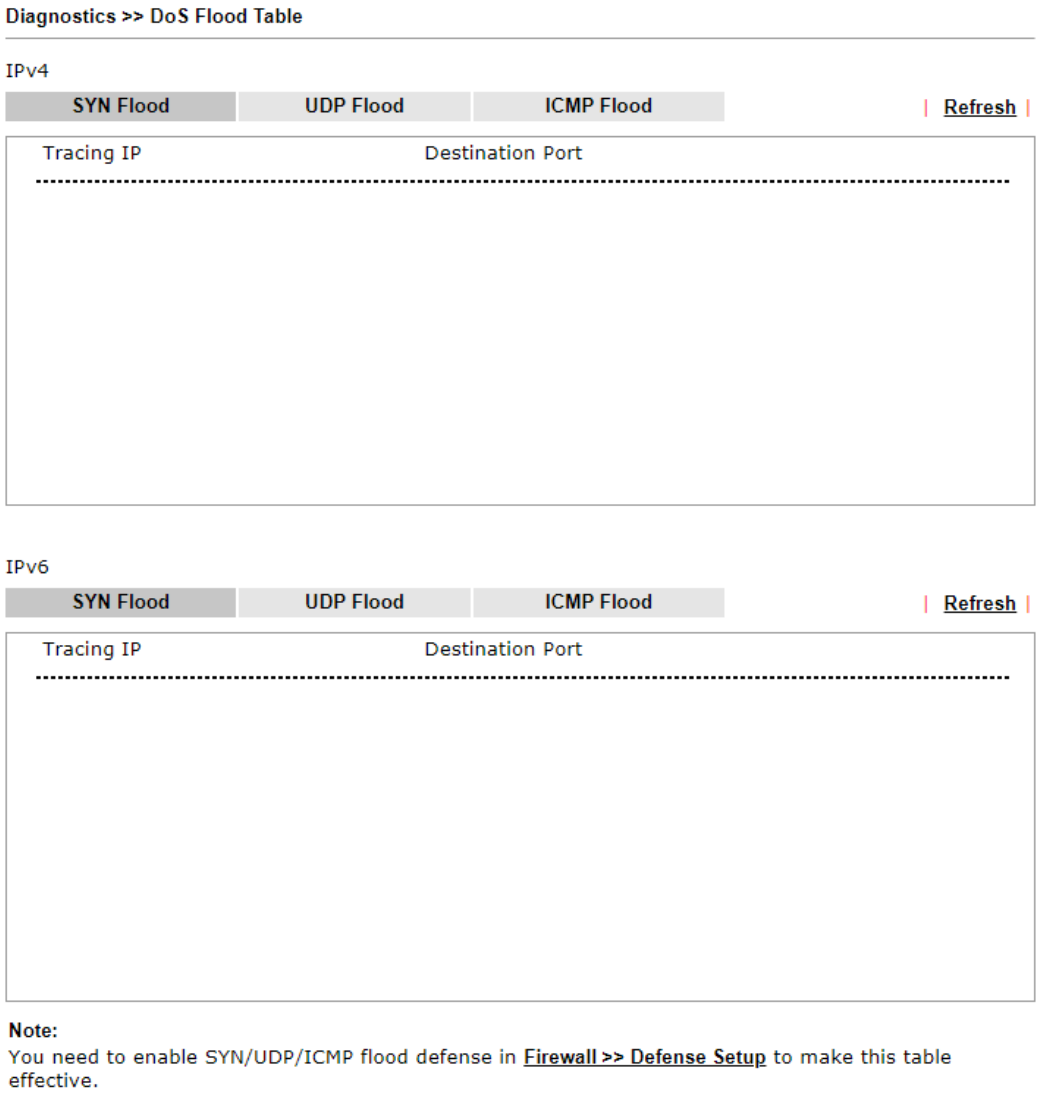
Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to show the latest status.
WAN1 / WAN3	Select the tab that corresponds to the WAN connection that you wish to view the IPv6 TSPC status.

VIII-1-14 DoS Flood Table

This page shows IP addresses that are currently engaging in DoS flood as detected by the DoS Flooding Defense mechanism. It provides useful information to network engineers (e.g., MIS engineers) to diagnose the network environment to identify potentially malicious network traffic and entities. Identified IP addresses and the destination ports used in SYN, UDP, and ICMP Flood attacks will be shown on the respective tab pages.

IP addresses that are suspected to be attacking the network can be blocked by clicking the **Block** button on the SYN Flood, UDP Flood and ICMP Flood tab pages.

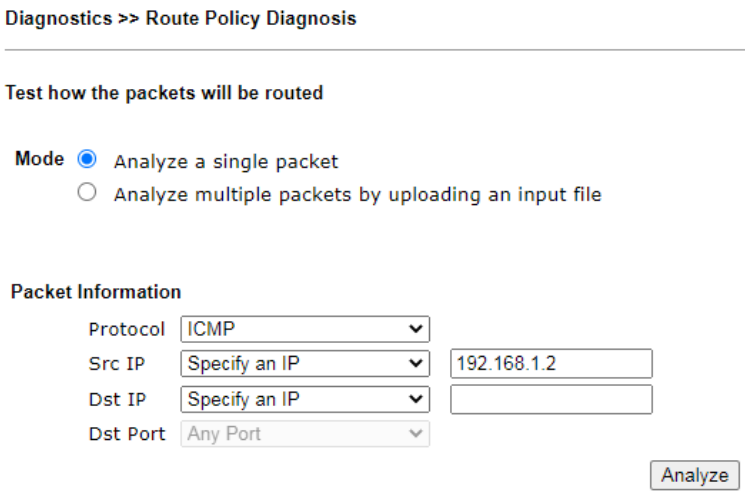


Info

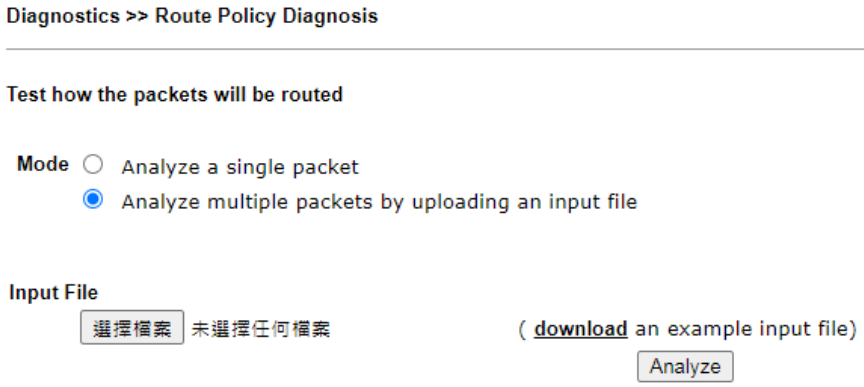
The icon - - means there is something wrong (e.g., attacking the system) with that IP address.

VIII-1-15 Route Policy Diagnosis

With the analysis done by such page, possible path (static route, routing table or policy route) of the packets sent out of the router can be traced.

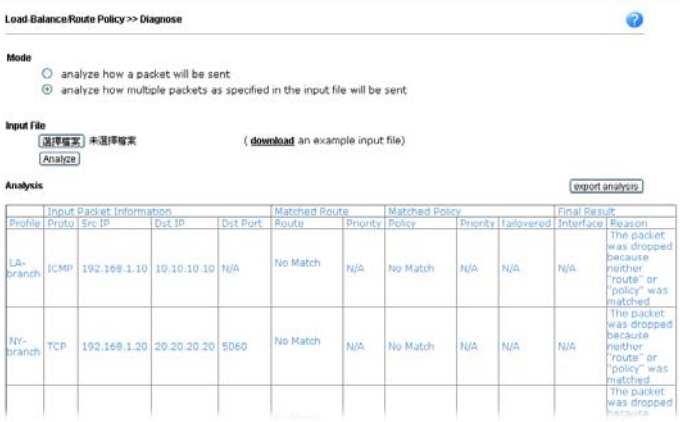


or



Available settings are explained as follows:

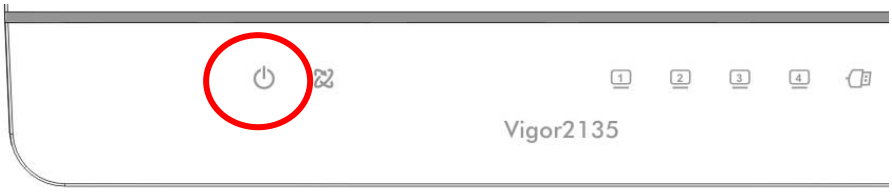
Item	Description
Mode	**Analyze a single packet** – Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy. **Analyze multiple packets**... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. **ICMP/UDP/TCP/ANY-** Specify a protocol for diagnosis. **Src IP** – Type an IP address as the source IP. **Dst IP** – Type an IP address as the destination IP. **Dst Port** – Use the drop down list to specify the destination

	port. **Analyze** – Click it to perform the job of analyzing. The analyzed result will be shown on the page..
Input File	It is available when Analyze multiple packets.. is selected as **Mode.** **Select** – Click the download link to get a blank example file. Then, click such button to select that blank ".csv" file for saving the result of analysis. **Analyze** – Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click **export analysis** 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.

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 **ACT 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

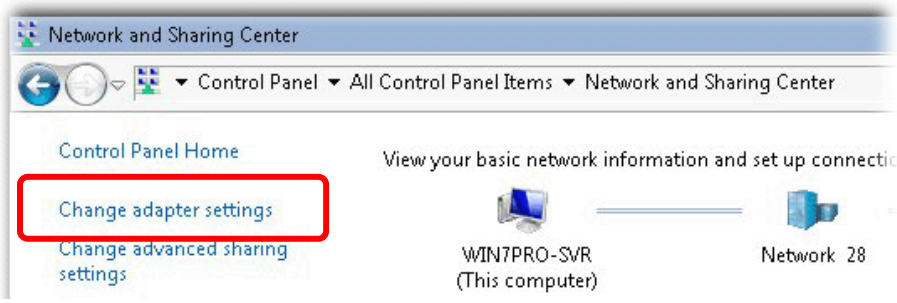
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

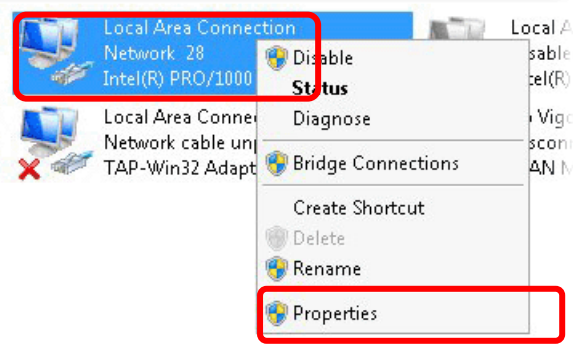
Info	The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

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

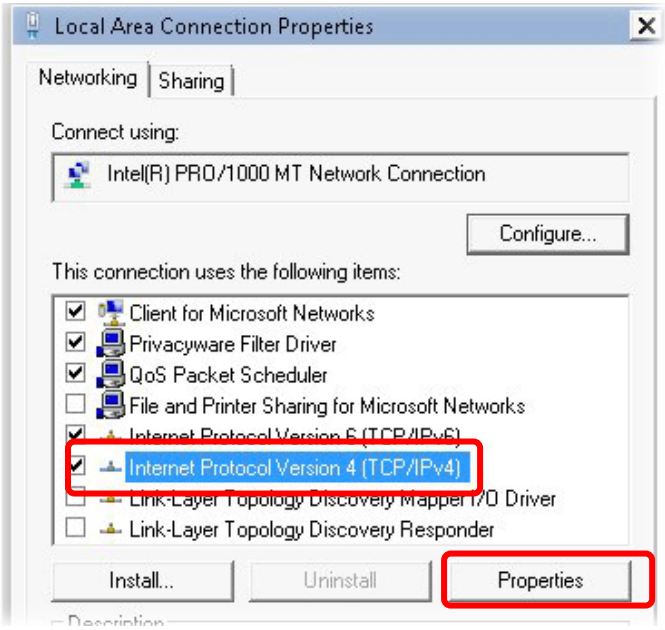
2. In the following window, click **Change adapter settings**.



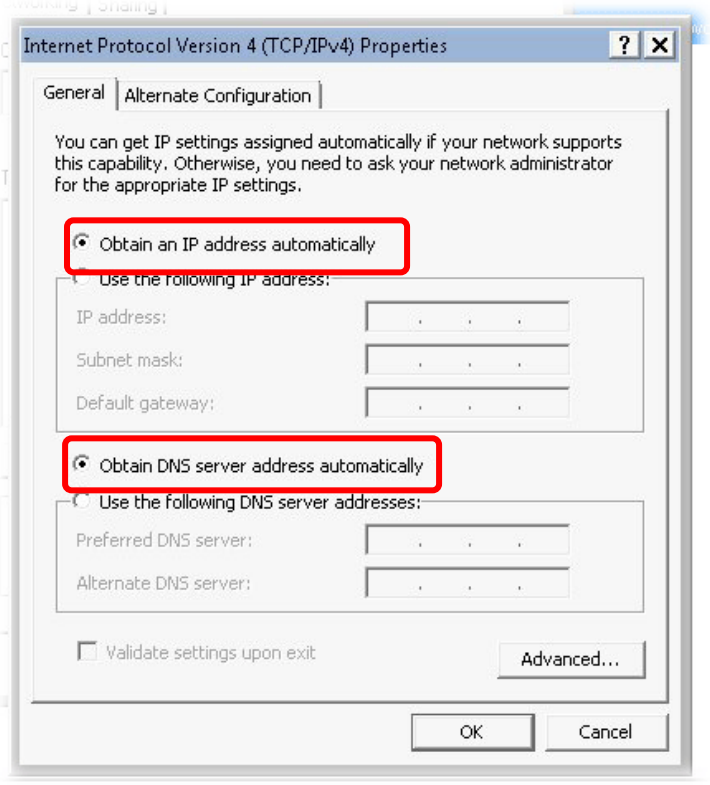
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

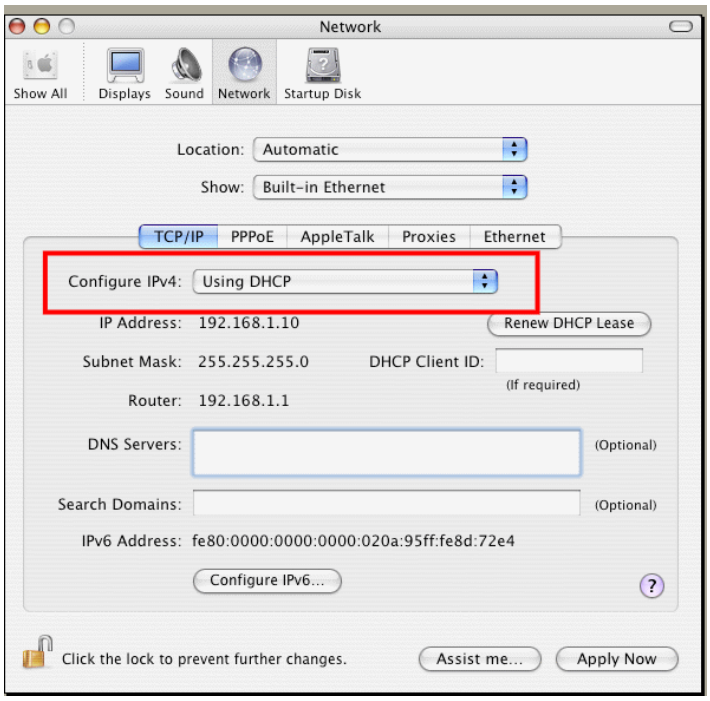


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



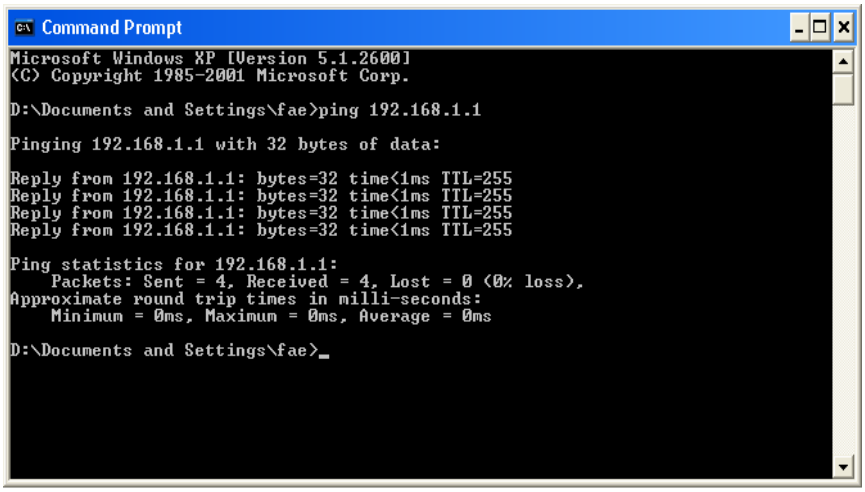
VIII-4 Pinging the Router from Your Computer

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 refer to the previous section IX-3)

Please follow the steps below to ping the router correctly.

For Windows

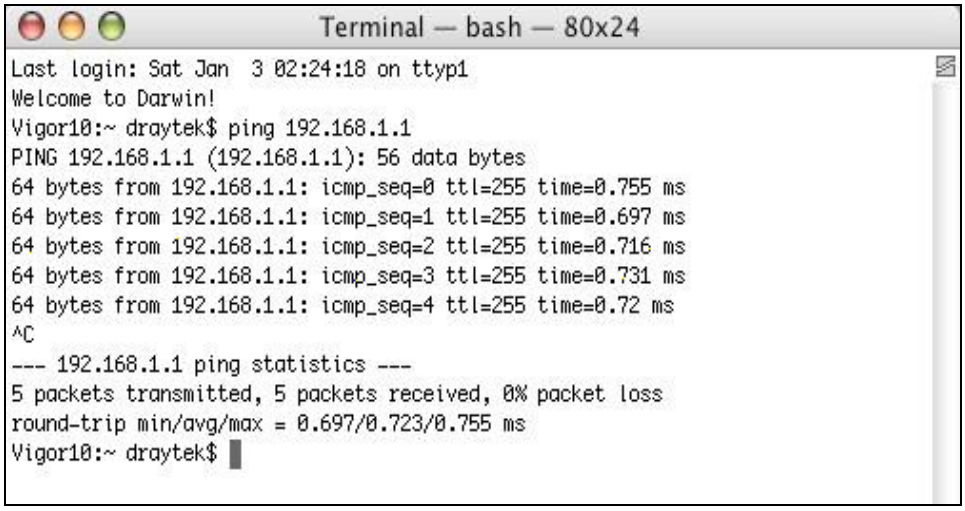
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Enter **cmd**. The DOS command dialog will appear.



3. Enter 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. Enter **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$

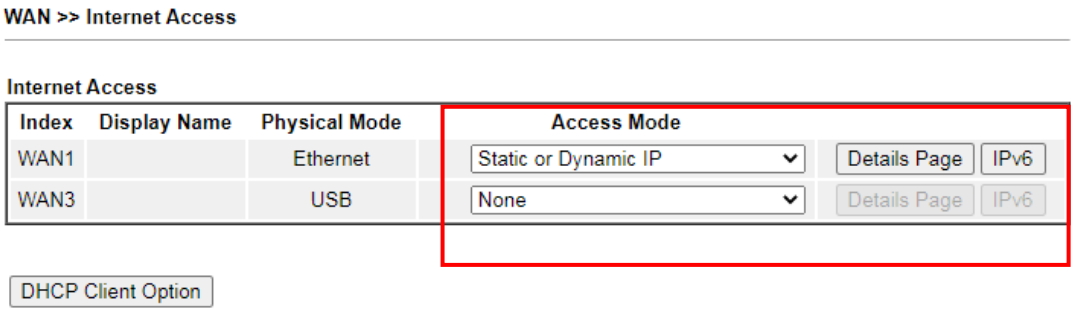
VIII-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section I-1-1, Indicators and Connectors) 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, change the physical type of modem (e.g., DSL/FTTX(GPON)/Cable modem) offered by ISP with the same value configured in Vigor router. 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~WAN6 to review the settings that you configured previously.



VIII-6 Problems for 3G/4G Network Connection

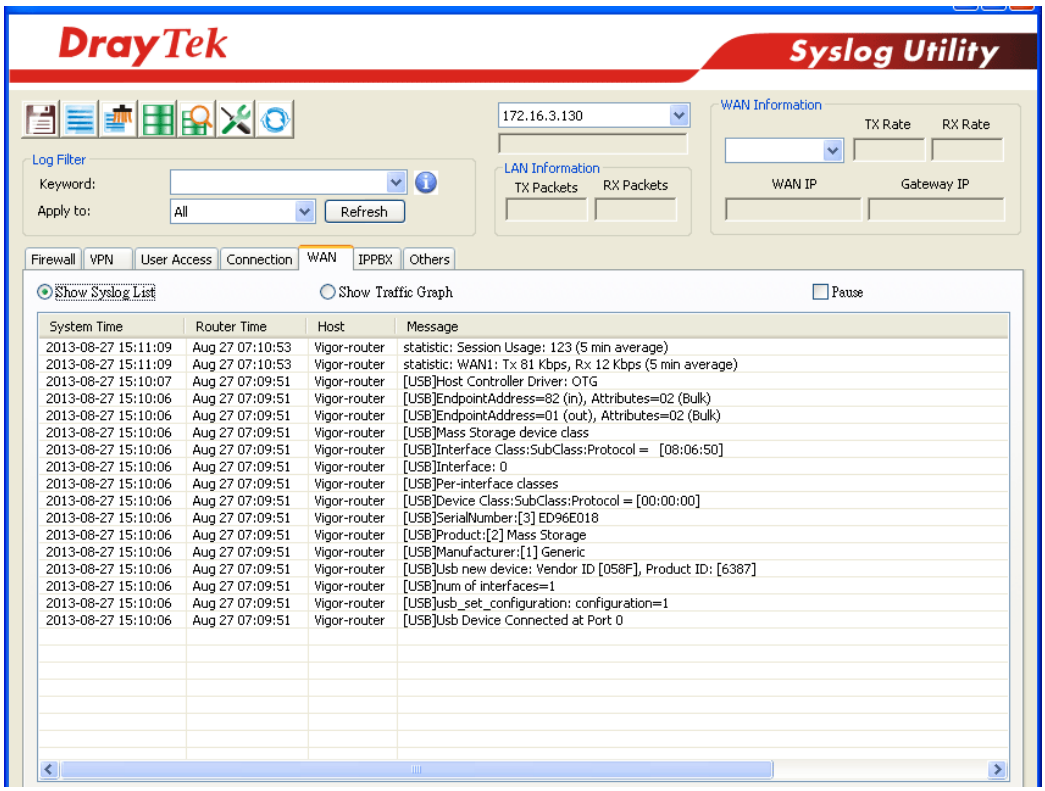
When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2135. Later, the USB LED will light on which means the installation of USB Modem is successful. If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2135.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G/4G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2135. In addition, please refer to the manual of 3G/4G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

VIII-7 Backing to Factory Default Setting If Necessary

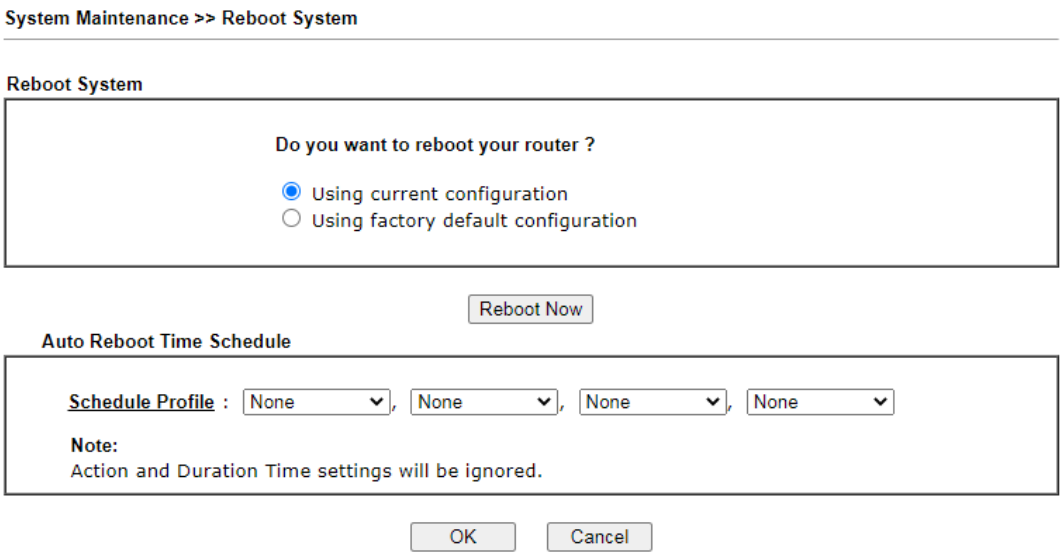
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

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

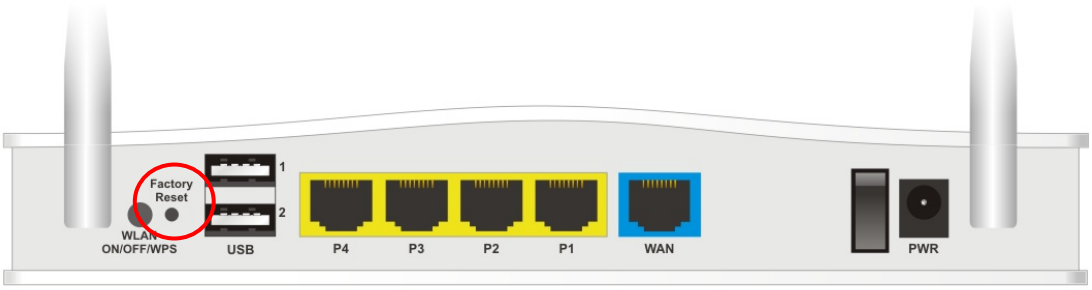
You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

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-8 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.

This page is left blank.

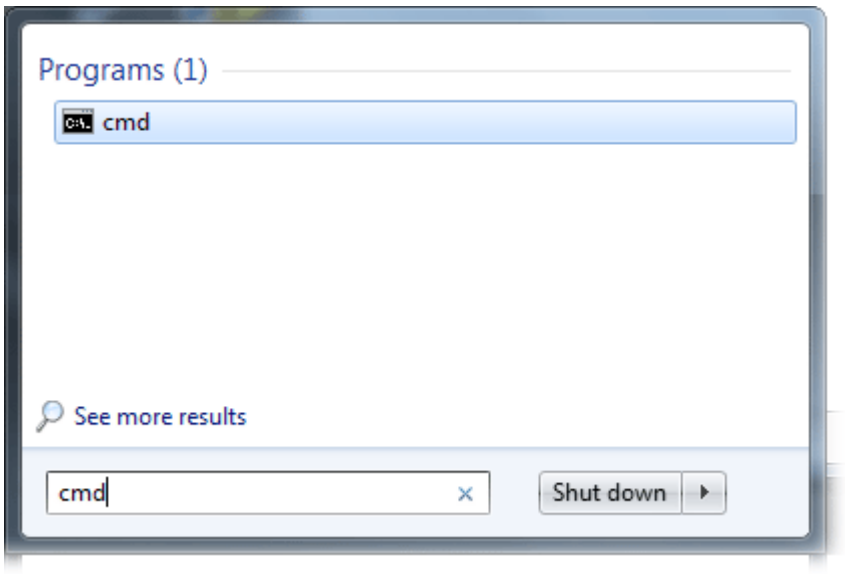
Part IX Telnet Commands

Accessing Telnet of Vigor2135

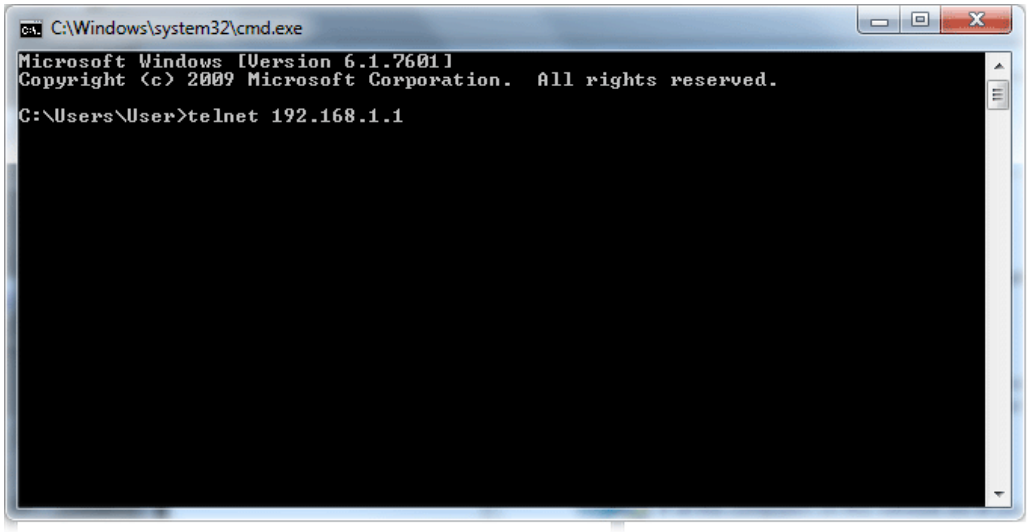
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.

Info	For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

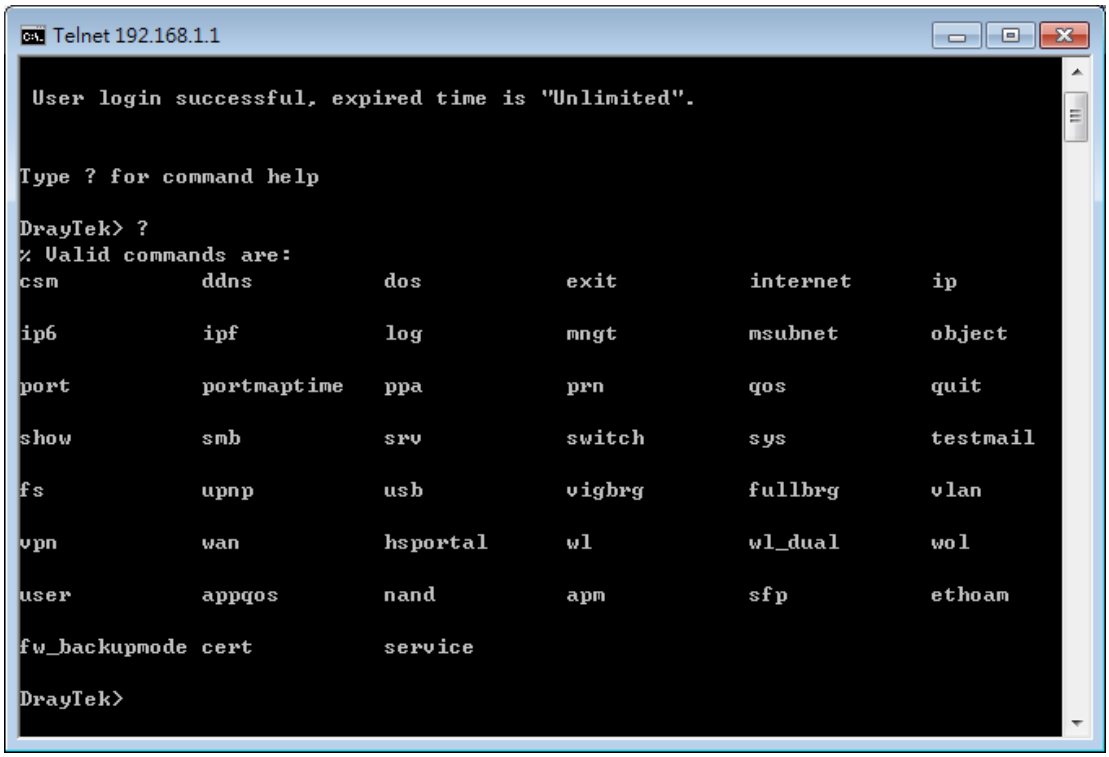
Enter **cmd** and press Enter. The Telnet terminal will be open later.



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, enter admin/admin for Account/Password. Then, enter **?**. You will see a list of valid/common commands depending on the router that your use.


Telnet 192.168.1.1
User login successful, expired time is "Unlimited".
Type ? for command help
DrayTek> ?
% Valid commands are:
csm ddns dos exit internet ip
ip6 ipf log mngt msubnet object
port portmaptime ppa prn qos quit
show smb srv switch sys testmail
fs upnp usb vigbrg fullbrg vlan
vpn wan hsportal wl wl_dual wol
user appqos nand apm sfp ethoam
fw_backupmode cert service
DrayTek>

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* | *-n NAME*|*setdefault*>

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- v	It means to view the configuration of the CSM profile.
- n	It means to set a name for the CSM profile.
NAME	It means to specify a name for the CSM profile, less then 15 characters.
setdefault	Reset to default settings.

Example

```
> csm appe prof -i 1 -n games
The name of APPE Profile 1 was setted.
```

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*| *-e AP_IDX* | *-d AP_IDX*>

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
- v	View the IM/P2P/Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
-a	Set the action of specific application
GROUP	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
AP_IDX	Each application has independent index number for identification in CLI command. Specify the index number of the application here. If you have no idea of the inex number, do the following (Take IM as an example): Type "csm appe set –I 1 –v IM", the system will list all of the index

	numbers of the applications categorized under IM.

Example

```
> csm appe set -i 3 -d 2
>
```

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	Specify the index number of CSM profile, from 1 to 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
-------------------------------------------------------------------------------
   OTHERS       Tunneling       73          CloudFlare       Disable
   OTHERS       Tunneling       74            DNSCrypt       Disable
   OTHERS       Tunneling       75            DynaPass       Disable
   OTHERS       Tunneling       76            FreeGate       Disable
   OTHERS       Tunneling       77       Hotspot Shield       Disable
   OTHERS       Tunneling       78           HTTP Proxy       Disable
   OTHERS       Tunneling       79         HTTP Tunnel       Disable
   OTHERS       Tunneling       80      LogMeIn Hamachi       Disable
   OTHERS       Tunneling       81            MS Teredo       Disable
   OTHERS       Tunneling       82              OpenDNS       Disable
   OTHERS       Tunneling       83              OpenVPN       Disable
   OTHERS       Tunneling       84               PGPNet       Disable
.
.
.
-------------------------------------------------------------------
Total 81 APPs
>
```

Telnet Command: csm appe interface

It is used to configure APPE signature download interface.

csm appe interface <*AUTO/WAN#*>

Syntax Description

Parameter	**Description**
AUTO	Vigor router specifies WAN interface automatically.
WAN	Specify the WAN interface for signature downloading.

Example

```
> csm appe interface wan1
Download interface is set as "WAN1" now.
> csm appe interface auto
Download interface is set as "auto-selected" now.
```

Telnet Command: csm appe email

It is used to set notification e-mail for APPE signature based on the settings configured in **System Maintenance>>SysLog/Mail Alert Setup (**in which, the box of **APPE Signature** is checkd under **Enable E-Mail Alert**).

csm appe email <*-e*|*-d*|*-s*>

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email -e
Enable APPE email.
```

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* | *-I [P*|*B*|*A*|*N]* | *uac* | *wf* >

csm ucf obj *INDEX -n <PROFILE_NAME>*

csm ucf obj *INDEX -p <VALUE>*

csm ucf obj *INDEX -I <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, from 1 to 8.

-n <PROFILE_NAME>	It means to set the profile name. PROFILE_NAME*:* specify the name of the profile (less than 16 characters.
-p <VALUE>	Set the priority (defined by the number specified in VALUE) for the profile. VALUE*:* Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 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]
> csm ucf show
URL Content Filter Profile Table:
Profile      Name        Profile       Name
-------------------------  -------------------------
[1]     [game        ]   [5]     [            ]
[2]     [            ]   [6]     [            ]
[3]     [            ]   [7]     [            ]
[4]     [            ]   [8]     [            ]
-------------------------  -------------------------

Administration Message (Max 255 characters):
-----------------------------------------------
<body><center><br><p>The requested Web page has been blocked by URL Content
Filt
er.<p>Please contact your system administrator for further
information.</center>
</body>
```

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, from 1 to 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:[block]
Priority Select : [Either : Url Access Control First]
-----------------------------------------------
URL Access Control
[ ]Enable URL Access Control   Action:[pass]
[v]Prevent web access from IP address.
  No  Obj NO.    Object 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, from 1 to 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. WEB_FEATURE: Features available for configuration are: c: Cookie p: Proxy u: Upload
-u < WEB_FEATURE>	It means to cancel the web feature configuration. WEB_FEATURE: Features available for configuration are: c: Cookie p: Proxy u: Upload
-f < File_Extension_Object_index>	It means to set the file extension object index number. File_Extension_Object_index: Enter the index number (1 to 8) for the file extension object.

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: Enter the content (less than 255 characters) of the message itself.
setdefault	It means to return to default settings for all of the profile.
Obj <INDEX>	It means to specify the object profile. INDEX: It means to specify the index number of web content filter profile, from 1 to 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>: specify 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 choose the items under CATEGORY or WEB_GROUP. *<CATEGORY >:* Child_Protection, Leisure, Business, Chating, Computer Internet, Other *<WEB_GROUP>:* 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. *<CATEGORY >:* Child_Protection, Leisure, Business, Chating, Computer Internet, Other *<WEB_GROUP>:* 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: csm dnsf

It means to configure the settings regarding to DNS filter.

csm dnsf enable <*ON|OFF***>**

csm dnsf syslog <*N|P|B|A***>**

csm dnsf wcf <*INDEX***>**

csm dnsf ucf <*INDEX***>**

csm dnsf cachetime *<CHACHE_TIME>*

csm dnsf blockpage *<value>*

csm dnsf profile_show

csm dnsf profile_edit *INDEX*

csm dnsf profile_edit *INDEX -n <PROFILE_NAME>*

csm dnsf profile_edit *INDEX -l <P|B|A>*

csm dnsf profile_edit *INDEX -w <WCF_PROFILE>*

csm dnsf profile_edit *INDEX -u <UCF_PROFILE>*

csm dnsf profile_edit *INDEX -c <CACHE_TIME>*

csm dnsf profile_setdefault

csm dnsf local_bw <*e/d/p/b/a/g/o/s/c***>**

Syntax Description

Parameter	Description
enable **<***ON|OFF***>**	Enable or disable DNS Filter. ON: enable. OFF: disable.
syslog **<***N|P|B|A***>**	Determine the content of records transmitting to Syslog. P: Pass. Records for the packets passing through DNS filter will be sent to Syslog. B: Block. Records for the packets blocked by DNS filter will be sent to Syslog. A: All. Records for the packets passing through or blocked by DNS filter will be sent to Syslog. N: None. No record will be sent to Syslog.
wcf <INDEX>	Specify a WCF profile (1 to 8) as the base of DNS filtering. Type a number to indicate the index number of WCF profile (1 is first profile, 2 is second profile, and so on ...).
Ucf <INDEX>	Specify a UCF profile (1 to 8) as the base of DNS filtering. Type a number to indicate the index number of UCF profile (1 is first profile, 2 is second profile, and so on ...).
cachetime <CACHE_TIME>	CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter. OFF is no cache ; AUTO is using TTL from pkt.
blockpage <value>	DNS sends block page for redirect port. When a web page is blocked by DNS filter, the router system will send a message page to describe that the page is not allowed to be visisted. Value includes on, off and show. ON: Enable the function of displaying message page. OFF: Disable the function of displaying message page. SHOW: Display the function of displaying message page is ON or OFF.
profile_show	Display the table of the DNS filter profile.
profile_edit	Modify the content of the DNS filter profile.
-n <PROFILE_NAME>	PROFILE_NAME: Enter the name of the DNS filter profile that you want to modify.
-l <P|B|A>	Specify the log type of the profile. P: Pass. B: Block. A: All.
-w <WCF_PROFILE>	WCF_PROFILE: Enter the index number of the WCF profile.
-u <UCF_PROFILE>	UCF_PROFILE: Enter the index number of the UCF profile.
-c <CACHE_TIME>	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
profile_setdefault	Reset to factory default setting.
local_bw e/d/p/b/s/c	Set the Black/White List of DNS Filter Local Setting. e: Enable the function of black/white list. d: Disable the function of black/white list. p: Set the action as "Pass". b: Set the action as "Block". s: Show the config setting. c: Clear the config setting and reset to factory default settings.
local_bw a <type index> <START_IP><END/MASK_IP>	Set the address type for Black/White List of DNS Filter. type index: Enter 0/1/2/3/4. In which, 0=mask, 1=single, 2=any, 3=range, 4=group and objects <START_IP>: Enter an IP address as a starting point. <END/MASK_IP>: Enter an IP address as an ending point.
local_bw g <item	Select the group index for Black/White List of DNS Filter.

number><group index>	item_number: 1 or 2 (group 1 or group 2) group_index: 1 to 192
local_bw o <item number><group index>	Select the object index for Black/White List of DNS Filter. item_number: 1 or 2 (object 1 or object 2) object_index: 1 to 32

Example

```
> csm dnsf enable on
DNS Filter enable!
> csm dnsf wcf 1
dns service set up!!!
> csm dnsf cachetime auto
use TTL from pkt!!!
> csm dnsf local_bw a 0 192.168.1.20 255.255.255.0
Address Type: 0:mask, 1:single, 2:any, 3:range, 4:object and group
Set the [MASK] Address type
> csm dnsf profile_edit 1 -n testformarket
Profile Index: 1
Profile Name:[testformarket]
Log:[block]
WCF Profile Index: 0
UCF Profile Index: 0
>
```

Telnet Command: ddns enable

Enable/disable the DDNS service.

Syntax Description

Parameter	Description
Enable <0/1>	Enable or disable DDNS service. 1: enable. 0: disable.

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 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 log

Displays the DDNS log.

Example

```
>ddns log
>
```

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. The range is from 1 to 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

>
```

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> | d <ATTACK_F><ATTACK_0>>*

dos *-o <LOG_TYPE>|p <LOG_TYPE> |l <LOG_TYPE>*

dos *-P <add4/remove4> <type> <value> |<add6/remove6> <type> <value> | <show> | remove4 all |remove6 all>*

dos *-B <add4/remove4> <type> <value> |<add6/remove6> <type> <value> | <show> | remove4 all |remove6 all>*

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 /- e <ATTACK_F><ATTACK_0>	It means to enable the defense function for all attacks or a specific attack listed in ATTACK_0. <ATTACK_F>: Specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan. <ATTACK_0>: It means to 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>: It means to specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-P <add4/remove4> <type> <value> |<add6/remove6> <type> <value> | <show> | remove4 all |remove6 all>	Add or remove the IPv4/IPv6 address in the white passing IP list. add4/remove4: Add /remove an IPv4/IPv6 address to/from the whitelist. add6/remove6: Add/remove an IPv6 address to/from the whitelist. Type: Two types, -i and -c. In which, "-i" means the IPv4 address and "-c" means the country object. Value: Enter the IP address for -i; enter the index number of the country object profile. Show: Display the whitelist.
-B <add4/remove4> <type> <value> |<add6/remove6> <type> <value> | <show> | remove4 all |remove6 all>	Add or remove the IPv4/IPv6 address in the black blocking IP list. add4/remove4: Add /remove an IPv4/IPv6 address to/from the blacklist. add6/remove6: Add/remove an IPv6 address to/from the blacklist. Type: Two types, -i and -c. In which, "-i" means the IPv4 address and "-c" means the country object. Value: Enter the IP address for -i; enter the index number of the country object profile. Show: Display the blacklist.
dos -o <LOG_TYPE>	Enable/Disable dos defense log. <LOG_TYPE>: Enter 0 or 1. 0: Disable 1: Enable
dos -p <LOG_TYPE>	Enable/Disable spoofing defense log. <LOG_TYPE>: Enter 0 or 1. 0: Disable 1: Enable
dos -l <LOG_TYPE>	Enable/Disable dos defense black/white list log. <LOG_TYPE>: Enter 0 to 3. 0: None 1: White list 2: Black List 3: All

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>
```

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 *-W n -M n [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
-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
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-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: Always-on n=1 ~ 999: Idle time for offline (default 180 seconds)
-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.
-s <server ip>	Set the PPTP/L2TP Server IP. <server ip>: Enter the IP address (e.g., ppp.qqq.rrr.sss) as the PPTP/L2TP server IP.
-A <idx>	Set current interface as Always On mode and specify the <idx> number as backup WAN#. <idx>: Enter the index number.
-B <mode>	Set current interface as Backup mode. <mode>: Enter 0 ro 1. 0: When any WAN disconnect; 1: When all WAN disconnect.
-V	It means to view Internet Access profile.

-C <sim pin code>	Set (PPP mode) SIM PIN code (max. 15 characters).
-O <init string>	Set (PPP mode) Modem Initial String (max. 47 characters).
-T <init string2>	Set (PPP mode) Modem Initial String2 (max. 47 characters)
-D <dial string>	Set (PPP mode) Modem Dial String (max. 31 characters).
-v <service name>	Set (PPP mode) Service Name (max. 23 characters).
-m <ppp username>	Set (PPP mode) PPP Username (max. 63 characters).
-o <ppp password>	Set (PPP mode) PPP Password (max. 62 characters).
-e n	Set (PPP mode) PPP Authentication Type. n= 0: PAP/CHAP (default), 1: PAP Only
-q n	(PPP mode) Index(1-15) in Schedule Setup-One
-x n	(PPP mode) Index(1-15) in Schedule Setup-Two
-y n	(PPP mode) Index(1-15) in Schedule Setup-Three
-z n	(PPP mode) Index(1-15) in Schedule Setup-Four
-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. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP
-L n	Set (PPP mode) WAN Connection Detection TTL (1-255) value.
-E <sim pin code>	Set (DHCP mode) SIM PIN code (max. 19 characters).
-G <mode>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
-N <apn name>	Set (DHCP mode) APN Name (max. 47 characters)
-U n	Set the MTU value for DHCP mode. n: 1000-1440.

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
```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the IP routing subnet for your router.

Syntax

ip 2ndsubnet <*Enable/Disable*>

Syntax Description

Parameter	Description
Enable	Enable the function.
Disable	Disable the function.

Example

```
> ip 2ndsubnet enable
2nd 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 an 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 an 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 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.

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.

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 or WAN*>

ip arp del <*IP address*> <*LAN or 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
IP address	It means the LAN IP address.
MAC address	It means the MAC address of your router.
LAN or WAN	It indicates the direction for the arp function.
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.
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       HOST ID             Interface  VLAN   Port
   1  192.168.1.9   60-A4-4C-E6-5A-4F                      LAN1       ---    P1
   2  192.168.1.11  00-1D-AA-0C-CD-08                      LAN1       ---    P3
>
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc *option*

ip dhcpc *option -h|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. -a: set option value by address list -c: set option number: 0~255 -d: delete custom dhcp client option by index number -e: enable/disable option feature, 1:enable, 0:disable -h: display usage -l: list all custom set DHCP options -u: update by idx number -v: set option value by string -w: set wan number -x: set option value by raw byte (hex) -r: remove all custom DHCP Client options
release <wan number>	It means to release current WAN IP address.

	<wan number>: 1 to 6.
renew <wan number>	It means to renew the WAN IP address and obtain another new one. <wan number>: 1 to 6.
status	It displays current status of DHCP client.

Example

```
>ip dhcpc status
====================================
WAN1:

DHCP Client Status: None active DHCP client!

====================================
WAN2:

DHCP Client Status: None active DHCP client!

====================================
WAN3:

DHCP Client Status: None active DHCP client!

====================================
WAN4:  <Virtual WAN>

DHCP Client Status: None active DHCP client!

====================================
WAN5:  <Virtual WAN>

DHCP Client Status: None active DHCP client!

====================================
WAN6:  <Virtual WAN>

DHCP Client Status: None active DHCP client!
```

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/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.

Example

```
>ip ping 172.16.3.229 WAN1
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
```

```
Receive reply from 172.16.3.229, time=0ms
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 <*Host/IP address*> <*WAN1/WAN3*> <*Udp/Icmp*>

Syntax Description

Parameter	Description
Host/IP address	It means the target IP address / host.
WAN1/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 LAN1. 2 means IP Routed.

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, 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
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
Now status:
WAN[1] 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
WAN[8] Rip Protocol enable
WAN[9] Rip Protocol enable
WAN[10] 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[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol enable
WAN[6] Rip Protocol enable
WAN[7] Rip Protocol enable
WAN[8] Rip Protocol enable
WAN[9] Rip Protocol enable
WAN[10] 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
dd <dst> <netmask> <gateway> <ifno> <rtype>	It means to add an IP address as static route. <dst>: Set the IP address of the destination. <netmask>: Set the netmask of the specified IP address. <gateway>: Set the gateway of the connected router. <ifno>: Enter the connection interface. In which, 3 means WAN1. <rtype>: Set the type (default or static) of the route. In which, default : default route; static: static route.
del <dst> <netmask> <rtype>	It means to delete specified IP address. <dst>: Set the IP address of the destination. <netmask>: Set the netmask of the specified IP address. <rtype>: Set the type (default or static) of the route. In which, default : default route; static: static route.
status	It means current status of static route.
cnc	It means current IP range for CNC Network.
default <off/?>	Set current default route.
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*

ip igmp_proxy *t_home <on/off/show/help>*

ip igmp_proxy *query*

ip igmp_proxy *ppp <0/1>*

ip igmp_proxy *status*

ip igmp_proxy *version <v2/v3/auto/show>*

ip igmp_proxy *syslog <0/1>*

Syntax Description

Parameter	Description
set	It means to enable proxy server.
reset	It means to disable proxy server.
wan	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	It means to set IGMP general query interval. The default value is 125000 ms.
ppp	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 set IGMP version fixed on v2 or v3.
syslog [0/1]	It means to set IGMP syslog. 0: disable 1: enable

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
>
```

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 hw_acc *<on/off/status>*

ip igmp_snoop txquery *<on/off> <v2/v3>*

ip igmp_snoop chkleave *<on/off>*

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.
hw_acc <on/off/status>	It means to set (on/off) or display the HW accleration setting for IGMP Snoop.
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
%% ip igmp_fl [enable|disable|status], IGMP Fast Leave is Enabled.
>
```

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> - Set the range of IP address specified for this command. <num> - Set the number of the session limits, e.g., 100. <p2pnum> - Set 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 *routing* <*on/off*>

ip bandwidth *schedule* <*s1*> <*s2*> <*s3*> <*s4*>

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*>	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.
routing <*on/off*>	It means to apply to IP Routed Subnet. On: apply to Off: not apply to
schedule <*s1*> <*s2*> <*s3*> <*s4*>	It means to set the scheduel profile(s) (0 to 16). Up to 4 profiles can be specified at one time.
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>: Set the range of IP address specified for this command. <tx>: Set transmission rate for bandwidth limit. <rx>: Set receiving rate for bandwidth limit. <shared>: S*et* 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 bandwidth routing on
```

```
> ip bandwidth schedule 1
```

Telnet Command: ip dataflowmonitor

This command allows users to set data flow monitor mechanism.

Syntax

ip dataflowmonitor on

ip dataflowmonitor off

ip dataflowmonitor status

Syntax Description

Parameter	Description
on	It means to enable the data flow monitor.
off	It means to disable the data flow monitor.
status	It means to show the status of data flow monitor.

Example

```
> ip dataflowmonitor on
Enable Data Flow Monitor.
>
```

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*

ip bindmac *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	It means that only those IP address in IP bindmac policy table can access into network.
strict_off	It means to turn off IP bindmac policy.
show	It means to display the IP address and MAC address of the pair of

	binded one.
add <IP> <MAC> <Comment>	It means to add one ip bindmac. <IP>: Enter the IP address for binding with specified MAC address. <MAC>: Enter the MAC address for binding with the IP address specified. <Comment>: En*ter* words as a brief description.
del <IP> <all>	It means to delete one ip bindmac. <IP>: Enter the IP address for binding with specified MAC address. <all>: 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>: Set all LAN subnets to bind strict mode. <set LAN_Index>: Enable the subnet setting by specify the index number of LAN subnet. <unset LAN_Index>: Disable the subnet setting by specify the index number of LAN subnet. Clear: Clear the settings. Show: Display the setting.

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 :
  Comment : just
>
```

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 policy_rt

This command is used to set the IP policy route profile.

Syntax

ip policy_rt *[-<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.
General Setup for Policy Route	
-i <value>	Specify an index number for setting policy route profile. Value: 1 to 60. "-1" means to get a free policy index automatically.
-e <0/1>	0: Disable the selected policy route profile. 1: Enable the selected policy route profile.
-o <value>	Determine the operation of the policy route. Value: add – Create a new policy rotue profile. del – Remove an existed policy route profile. edit – Modify an existed policy route profile. flush – Reset policy route to default setting.
-1 <any/range>	Specify the source IP mode. Range: Indicate a range of IP addresses. Any: It means any IP address will be treated as source IP address.
-2 <any/ip_range/ip_subnet/domain>	Specify the destination IP mode. Any: No need to specify an IP address for any IP address will be treated as destination IP address. ip_range: Indicates a range of IP addresses. ip_subnet: Indicates the IP subnet. domain: Indicates the domain name.

-3 <any/range>	Specify the destination port mode. Range: Indicate a range of port number. Any: It means any port number can be used as destination port.
-G <default/specific>	Specify the gateway mode.
-L <default/specific>	Specify the failover gateway mode.
-s <value>	Indicate the source IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.0)
-S <value>	Indicate the source IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.100)
-d <value>	Indicate the destination IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.0)
-D <value>	Indicate the destination IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.100)
-p <value>	Indicate the destination port start. Value: Type a number (1 ~ 65535) as the port start (e.g., 1000).
-P <value>	Indicate the destination port end. Value: Type a number (1 ~ 65535) as the port end (e.g., 2000).
-y <value>	Indicate the priority of the policy route profile. Value: Type a number (0 ~ 250). The default value is “150”.
-I <value>	Indicate the interface specified for the policy route profile. Value: Available interfaces include, LAN1 ~ LAN8, IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN3, VPN_PROFILE_1 ~ VPN_PROFILE_32, WAN_1_IP_ALIAS_1 ~ WAN_2_IP_ALIAS_8
-g <value>	Indicate the gateway IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.3.1)
-I <value>	Indicate the failover IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.4.1)
-t <value>	It means “protocol”. Value: Available settings include “TCP”, “UDP”, “TCP/UDP”, “ICMP” and “Any”.
-n <0/1>	Indicates the function of “Force NAT”. 0: Disable the function. 1: Enable the function.
-a <0/1>	Indicates to enable the function of failover. 0: Disable the function. 1: Enable the function.
-f <value>	It means to specify the interface for failover. Value: Avaialbe interfaces include, NO_FAILOVER, Default_WAN, Policy1 ~ Policy30 LAN1 ~ LAN8 IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN3,

	VPN_PROFILE_1 ~ VPN_PROFILE_32, WAN_1_IP_ALIAS_1 ~ WAN_2_IP_ALIAS_8
-b <value>	It means “failback”. Value: Available settings include, 0: Disable the function of “failback”. 1: Enable the function of “failback”.
-v	It means to display non-default settings.
Diagnose for Policy Route	
-s <value>	It means “source IP”. Value: Available settings include: Any: It indicates any IP address can be used as source IP address. “xxx.xxx.xxx.xxx”: The type format (e.g, 192.168.1.0).
-d <value>	It means “destination IP”. Value : Available settings include: Any: It indicates any IP address can be used as destination IP address. “xxx.xxx.xxx.xxx”: Specify an IP address.
-p <value>	It means “destination port”. Value: Specify a number or type Any (indicating any number).
-t <value>	It means “protocol”. Value: Available settings include “ICMP”, “TCP”, “UDP” and “Any”.

Example

```
> ip policy_rt diagnose -s 192.168.1.100 -d any -p any -t ICMP

   ------------------------------------------------
      Matched Route  (Priority)
   ------------------------------------------------
   * No_Match

   ------------------------------------------------
      Matched Policy (Priority)
   ------------------------------------------------
   * Policy_1 (200)

   * Conclusion:The packet was dropped because the send-to interface of the
matched policy "policy 1" was inactive and there was no failover setting
> ip policy_rt -i -1 -o add -1 range -s 192.168.1.10 -S 192.168.1.20 -2
ip_range –d 202.211.100.10 -D 202.211.100.20 -g 202.211.100.1 -I WAN2
```

Telnet Command: ip lanDNSRes

This command is used to set LAN DNS profiles. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.

Syntax

ip lanDNSRes *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-a <IP Address>	It is used to configure IP address mapping (IPv4/IPv6 Address or

	multiple subnet addresses). IP Address: type the IP address (e.g., 192.168.1.56).
-c <CNAME>	It is used to set CNAME. CNAME: Enter a string.
-d <address mapping index number>	It means to delete index number with address mapping configured. address mapping index number : type the index number which represents the address mapping profile.
-e <0/1>	It means to enable or disable the function of LAN DNS or DNS Forwarding Profile. 0: disable 1: enable
-i <profile setting index number>	It means to create LAN DNS profile with specified domain name. profile setting index number : type the index number which represents the profile with domain name configured.
-l	It means to list detailed information of profile configuration**.**
-n <domain name>	It means to specify a domain name to be accessed.
-p <profile name>	It means to set name of the LAN DNS profile.
-r	It means to clear specified domain name profile and the address mapping setting.
-R	It means to set to factory default setting.
-s <0/1>	It means to determine all subnet packets or only the packets with the same subnet will be replied for address mapping profile. 0: reply all subnet packets. 1: reply only same subnet packet.
-z	It means to update LAN DNS configuration to DNS cache.

Example

```
> ip lanDNSRes -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip lanDNSRes -i 1 -a 172.16.2.10 -s 1
% Configure Set1's IP:172.16.2.10
% Configure Set1's Idx:1 ReplyOnlySameSubnet:Yes
> ip lanDNSRes -i 1 -l
% Idx: 1
% State: Disable
% Profile:
% Domain Name: ftp.drayTek.com
% -------- Address Mapping Table --------
% Idx ReplyOnlySameSubnet IP Address
% 1   Yes             172.16.2.10
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

ip dnsforward *[-<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 <IP Address/Domain Name>	Set forwarded DNS server IP Address or domain name. <IP Address/Domain Name>: Enter an IP address or the domain name.
-d <DNS server mapping index number>	Delete the selected LAN DNS profile. <DNS server mapping index number>: Enter the index number.
-e <0/1>	0: disable this function. 1: enable this function.
-i <profile setting index number>	Type the index number of the profile. <profile setting index number>: Enter the index number.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.

Example

```
> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>
```

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/..LAN4/ WAN1/USB /VPN1/..VPN32>*

ip6 addr -d *<prefix> <prefix-length> <LAN1/..LAN4/ WAN1/USB /VPN1/..VPN32>*

ip6 addr -a *<LAN1/..LAN4/ WAN1 /USB /VPN1/..VPN32> -u*

ip6 addr -v *<LAN1/..LAN4/ WAN1/USB>*

ip6 addr -t *<old-prefix><old-prefix-length><new-prefix> <new-prefix-length> <LAN1/..LAN4/ WAN1/USB>*

ip6 addr -o *<1/2>*

ip6 addr -o 3 *<prefix> <prefix-length> <WAN1/USB>*

ip6 addr -l *<prefix> <prefix-length> <LAN1/..LAN4>*

ip6 addr <-*p/-b> <prefix> <prefix-length> <WAN1/USB>*

ip6 addr -x *<LAN1/..LAN4>*

ip6 addr -c *<LAN1/..LAN4>*

ip6 addr -e *<type> < LAN1/..LAN4>*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <LAN1/..LAN4/ WAN1/USB /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/..LAN4/ WAN1/USB /VPN1/..VPN32>: It means to specify LAN/WAN/USB/VPN interface for such address.
-d <prefix> <prefix-length> <LAN1/..LAN4/ WAN1/USB /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/..LAN4/ WAN1/USB /VPN1/..VPN32>: It means to specify LAN/WAN/USB/VPN interface for such address.
-a <LAN1/..LAN4/ WAN1 /USB /VPN1/..VPN32> -u	It means to show current address(es) status. <LAN1/..LAN4/ WAN1/USB /VPN1/..VPN32>: It means to specify LAN/WAN/USB/VPN interface. <-u>: It means to show unicast address only.
-v <LAN1/..LAN4/ WAN1/USB>	It means to show prefix list status.
-t <old-prefix><old-prefix-length><new-prefix> <new-prefix-length>	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.

<LAN1/..LAN4/ WAN1/USB>	<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/..LAN4/ WAN1/USB>: 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/USB>	<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/USB>: It means to specify a WAN/USB interface for such address.
-l <prefix> <prefix-length> < LAN1/..LAN8>	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/..LAN8>: It means to specify a LAN interface for such address.
-p/-b <prefix> <prefix-length> <WAN1 /USB>	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/ USB>: It means to specify a WAN/USB interface for such address.
-x <LAN1/..LAN4>	It means to generate a ULA automatically. <LAN1/..LAN4>: It means to specify a LAN interface.
-c <LAN1/..LAN4>	It means to delete a ULA . <LAN1/..LAN4>: It means to specify a LAN interface.
-e <type> <LAN1/..LAN4>	It means to set ULA type. <type>: 0, disable; 1, static; 2, auto <LAN1/..LAN4>: It means to specify a LAN interface.

Example

```
> ip6 addr -a
DMZ
Unicast Address:
 FE80::1F3A:8877:4D37:BAFD/64 (Link)
Multicast Address:
 FF02::1:FF00:0
 FF02::1:FF37:BAFD
 FF02::1
LAN4
Unicast Address:
 FE80::1F3A:8877:4D37:BAFD/64 (Link)
Multicast Address:
 FF02::1:FF00:0
 FF02::1:FF37:BAFD
 FF02::1
LAN3
```

```
Unicast Address:
 FE80::1F3A:8877:4D37:BAFD/64 (Link)
Multicast Address:
 FF02::1:FF00:0
 FF02::1:FF37:BAFD
 FF02::1
LAN2
Unicast Address:

 FE80::1F3A:8877:4D37:BAFD/64 (Link)
....
```

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|…|LAN4|WAN1|USB> [-<command> <parameter>| …]*

Syntax Description

Parameter	Description
req_opt	It means option-request.
<LAN1|LAN2|…|LAN4|WAN 1|USB>	It means to specify LAN or WAN 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 WAN1 -S 1
> ip6 dhcp req_opt WAN1 -r 1
> ip6 dhcp req_opt WAN1 -a
% Interface WAN2 is set to request following DHCPv6 options:
```

```
%    sip name
%    dns
%    refresh time
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

Syntax

ip6 dhcp *client <WAN1|USB> [-<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.
-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 WAN1 -d
 Client DUID = 000300011449bc0a8ab9
> ip6 dhcp client WAN1 –a
  Interface WAN1 has following DHCPv6 client settings:
       DHCPv6 client enabled
       request IA_PD 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.
-l	It means to clear the DHCPv6 table.
-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 pool name.
-c <parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-e <parameter>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable
-t <time>	It means to set prefer lifetime.
-y <time>	It means to set valid lifetime.
-u <time>	It means to set T1 time.
-o <time>	It means to set T2 time.
-i <pool_min_addr>	It means to set the start IPv6 address of the address pool.
-x <pool_max_addr>	It means to set the end IPv6 address of the address pool.
-R	It means to send reconfigure packet to the client.
-r <0/1>	It means to disable (0) or enable (1) the auto range.
-N <0/1>	It means to disable (0) or enable (1) the 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 <0/1>	It means to disable (0) or enable (1) the DHCP PD.
pdadd <suffix> <prefix_len> <client linklocal><client DUID>	It means to add PD node.
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 LAN1 pdadd 11:22:33 64 fe80::e202:1bff:fe65:4084
000100011d2ce39a00e06f25c839
%      Add to PD list success!
%% PD status : invalid, no prefix available.
>
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet *-W n -M n [-<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 1 -M 2 -u userid -p passwd -s broker.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 display IPv6 neighbour table.

Syntax

ip6 neigh *-s <inet6_addr> <eth_addr> <LAN1/..LAN4/ WAN1/ USB>*

ip6 neigh *-d <inet6_addr> <LAN1/..LAN4/ WAN1/ USB>*

ip6 neigh *-a <inet6_addr> <-N LAN1/..LAN4/ WAN1/ USB>*

Syntax Description

Parameter	Description
-s <inet6_addr> <eth_addr> <LAN1/..LAN4/ WAN1/ USB>	It means to add a neighbour. <inet6_addr>: Enter an IPv6 address. <eth_addr>: Enter a submask address. <LAN1/..LAN4/ WAN1/ USB>: Specify an interface for the neighbor.
-d <inet6_addr> <LAN1/..LAN4/ WAN1/ USB>	It means to delete a neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ USB>: Specify an interface for the neighbor.
-a <inet6_addr> <-N LAN1/..LAN4/ WAN1/ USB>	It means to show neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ USB>: 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                                 FAILED

 LAN1 ::                                                  NONE

>
```

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

Syntax

ip6 pneigh *-s <inet6_addr> < LAN1/..LAN4/ WAN1/ USB>*

ip6 pneigh *-d <inet6_addr> <LAN1/..LAN4/ WAN1/ USB>*

ip6 pneigh *-a <inet6_addr> <-N LAN1/..LAN4/ WAN1/ USB>*

Syntax Description

Parameter	Description
-s <inet6_addr> < LAN1/..LAN4/WAN1/ USB >	It means to add a proxy neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ USB>: Specify an interface for the proxy neighbor.
-d <inet6_addr> < LAN1/..LAN4/WAN1/USB >	It means to delete a proxy neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ USB>: Specify an interface for the proxy neighbor.
-a <inet6_addr> <-N LAN1/..LAN4/WAN1/USB >	It means to show proxy neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ USB>: 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 IPv6 route policy.

Syntax

ip6 route *-s <prefix> <prefix-length> <gateway> <LAN1/..LAN4/WAN1/ USB/VPN1/..VPN32> <-D>*

ip6 route *-d <prefix> <prefix-length>*

ip6 route *-a <LAN1/..LAN4/WAN1/ USB/VPN1/..VPN32>*

ip6 route *-l*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <gateway> < LAN1/..LAN4/WAN1/ USB/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/..LAN8/DMZ/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/..LAN4/WAN1/ USB/VPN1/..VPN32>	It means to show the route status. <LAN1/..LAN8/DMZ/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::1F3A:8877:4D37:BAFD/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|…|LAN4|WAN1|USB>] <send count> <data_ size(1~1452)>*

Syntax Description

Parameter	Description
IPv6 address/Host	It means to specify the IPv6 address or host for ping.
<iLAN1|LAN2|…|LAN4|WAN 1|USB>	It means to specify LAN or WAN interface for such address.

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|…|LAN4|WAN1|USB]]*

Syntax Description

Parameter	Description
IPV6 address/Host	It means to specify the IPv6 address or host for ping.
<LAN1/..LAN8/DMZ/WAN1/ WAN2/USB1/USB2>	It means to specify an 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) Info=2 (means WAN2)

Example

```
DrayTek> ip6 tspc 1
Tunnel Broker: broker.freenet6.net
Status: Idle
>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

Ip6 radvd <*LAN1/..LAN4*> <-<*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 -s 1
% [LAN1] setting !
%   Enable LAN1 radvd OK!
> ip6 radvd LAN1 -d 1800
% [LAN1] setting !
```

```
%   Set default lifetime ok: 1800 !
> ip6 radvd LAN1 -V
% [LAN1] setting !
%  Default Lifetime : 0 seconds
%  min interval time: 200 seconds
%  MAX interval time: 600 seconds
%  Hop limit        : 64
%  MTU              : 1280
%  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> <IPv6 Object Index> |remove <Index>|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.
add <Index> <IPv6 Object Index> |remove <index>|flush	It means to add an IPv6 address which can be used to execute management through Internet. <Index>: 1 to 10. Ten profiles can be set for IPv6 access list. <IPv6 Object index>: It means the index number of IP object (1 to 64) or keyword object (1 to 200) . remove <Index>: It means to remove (delete) the specified IP/Keyword object.
flush	It means to clear the IPv6 access table.
status	It means to show the status of IPv6 remote management.
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 1
%% Set OK.
> ip6 mngt list
DrayTek> ip6 mngt list
% IPv6 Access List :
[Index] [IPv6 Object Index]    [IPv6/Prefix Length or StartIPv6 ~ EndIPv6]
=========================================================================
  1           1            Please setting index=1 for IPv6 Object

> ip6 mngt status
```

```
internet access : off,  telnet : off,   http : off,    https : off,    ssh :
off,     ping : off,    enforce_https : off
```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

Syntax

ip6 online <*WAN1*|*USB*>

Syntax Description

Parameter	Description
<*WAN1*|*USB*>	It means the connection interface.

Example

```
> ip6 online WAN1
 % WAN1 online status :
 % IPv6 WAN1 TSPC
 % Default Gateway : ::
 % Interface : DOWN
 % UpTime : 00:00:00
 % 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 to 8: LAN1 to LAN4. n=9: DMZ.

Example

```
> ip6 lan -l 2 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
%   Set LAN2!

%   Set primary WAN1!

%  Set 1st DNS server 2001:4860:4860::8888

%   Set Other Option Enable!

%   [LAN2] 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    : Enable
%  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 for bandwidth control.

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-IP2> /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-IP2> /all	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. 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
>
```

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 *[OPTION]*

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-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
ipf: IP Filter: v3.3.1 (1852)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x6059749c = block, nomatch
Default: pass all, Logging: available
>
```

Telnet Command: ipf set

This command is used to set general rule, filter set and filter rule for firewall.

Syntax

ipf set *[Options]*

ipf set *<SET_NO><Options>*

ipf set *<SET_NO> rule <RULE_NO> <Options>*

Syntax Description

Parameter	Description
ipf set [options]	It means to set the firewall general setup and default rule.
ipf set <SET_NO><Options>	It means to set the firewall fiter set including comments and next fiter set.
ipf set <SET_NO> rule <RULE_NO> <Options>	It means to set the firewall rule in a filter set. For detailed information, refer to Telnet Command: ipf rule.
About ipf set [options]	
-v	It means to view the configuration of general set.
-d <p1>	It means to setup Data Filter. <p1>: Specify the index number (1 to 12) of the set profile. To disable the setting, enter "0".

- p <p1> <p2>	It means to setup actions for packet not matching any rule and whether record syslog. <p1>: Type “0” to let packets not matching any rule pass; Type “1” to block the packets not matching any rule. <p2>: "0" means the log related to rule matching will not be recorded on Syslog; "1" means the log related to rule matching will be recorded on Syslog. For example, to set pass for packet not matching any rule and enable syslog, *-p 0 1*.
-R <v4/v6> <Enable/Disable>	It means to accept routing packet from WAN. <v4/v6>: IPv4 or IPv6. <Enable/Disable>: Enter 0 (enable) or 1 (disable). Set Accept routing packet from WAN by IPv4, please enter *-R v4 0*.
-L <p1>	It means to enable or disable the Strict Security Firewall function. <p1>: Enter 1(enable) or 0 (disable).
-C <p1>	It means to setup Code Page. <p1>: Enter a code page number (0 to 20). For example, ipf set -C 20. 0. None 1. ANSI(1250)-Central Europe 2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/OEM(874)-Thai 17. ANSI/OEM(932)-Japanese Shift-JIS 18. ANSI/OEM(936)-Simplified Chinese GBK 19. ANSI/OEM(949)-Korean 20. ANSI/OEM(950)-Traditional Chinese Big5
-M <p1> <p2>	It means to setup APP Enforcement and Syslog. <p1>: Enter a number (0 to 32). In which, 0 means none; 1 to 32 mens the index number of the profile. <p2>: "0" means the log related to APP Enforcement will not be recorded on Syslog; "1" means the log related to APP Enforcement will be recorded on Syslog.
-U <p1> <p2>	It means to setup URL Content Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to URL Content Filter will not be recorded on Syslog; "1" means the log related to URL Content Filter will be recorded on Syslog.
-W <p1> <p2>	It means to setup Web Content Filter for packets not matching any rule.

	<p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to Web Content Filter will not be recorded on Syslog; "1" means the log related to Web Content Filter will be recorded on Syslog.
-D <p1> <p2>	It means to setup DNS Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to DNS Filter will not be recorded on Syslog; "1" means the log related to DNS Filter will be recorded on Syslog.
-a <p1>	It means to configure the advanced settings.
-f <p1>	It means to accept large incoming fragmented UDP or ICMP packets. <p1>: Enter 1(enable) or 0 (disable).
-t <p1>	It means to enable or disable the Transparent Mode. <p1>: Enter 1(enable) or 0 (disable).
-E <p1> <p2>	It means to set the maximum count for session limitation. <p1>: Enter a number (0 to 50000) <p2>: "0" means the log related to session control will not be recorded on Syslog; "1" means the log related to session control will be recorded on Syslog.
-Q <p1> <p2>	It means to set the QoS Class. <p1>: Enter a number (0 to 4). 0: None 1: Class 1 2: Class 2 3: Class 3 4: Default Class <p2>: "0" means the log related to QoS Class will not be recorded on Syslog; "1" means the log related to QoS Class will be recorded on Syslog.
-Y <p1> <p2>	It means to set the User Management. <p1>: Enter a number (-1 to 2). -1: None 0: All 1: user object 2: user group <p2>: 1 to 200(if p1 is set with 1, user object) or 1 to 32(if p1 is set with 2, user group)
-y <p1>	It means the log related to User Management will be or be not recorded on Syslog. <p1>: Enter 1(enable) or 0 (disable).
-w <p1>	It means to set the window size of TCP protocol. <p1>: Enter a value (0 to 65535).
-A <p1>	It means to enable or disable the function of packet capture. <p1>: Enter 1(enable) or 0 (disable).
About ipf set <SET_NO> <Options>	
-m <Comments>	It means to set comment for a filter set. <Comments>: Enter a description for the filter set.
-v	It means to view the comment and the next filter set.
-n <NEXT_SET_NO>	It means to specify the next filter set of current filter set.

	<NEXT_SET_NO>: Enter a number (1 to 12). For example, ipf set 1 -n 2.

Example

```
> ipf set -R "v4 1"
Setting saved.
> ipf set -R "v6 1"
Setting saved.
> ipf set -v

Data Filter: Enable (Start Filter Set = 1)
Log Flag   : Disable

Actions for packet not matching any rule:
  Pass or Block        : Pass
  CodePage             : ANSI(1252)-Latin I
  Max Sessions Limit   : 50000
  Current Sessions     : 0
  Mac Bind IP          : Non-Strict
  QOS Class            : None
  APP Enforcement      : None
  URL Content Filter   : None
  WEB Content Filter   : None
  DNS Filter           : None
  Load-Balance policy  : Auto-select
  ------------------------------------------------------------------
  CodePage             : ANSI(1252)-Latin I
  Window size          : 65535
  Session timeout      : 60
  DrayTek Banner       : Enable
  ------------------------------------------------------------------
  Accept large incoming fragmented UDP or ICMP packets: Enable
  Transparent Mode                                 : Disable
  ------------------------------------------------------------------
  Block routing packet from WAN:
    [v] IPv4
    [v] IPv6
  ------------------------------------------------------------------
  [v] Enable Strict Security Firewall
>
```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

Syntax

ipf rule *s r [-<command> <parameter> | …*

ipf rule s r -v

Syntax Description

Parameter	Description
s	It means the Filter Set.

	s: Enter a value (1 to 12).
r	It means Filter Rule r: Enter a value (1~7).
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-e <0/1>	It means to enable or disable the rule setting. 0: disable 1:enable
-v	It is used to show current filter rule settings.
-D <value>	It means to set the direction of packet flow. It is for **Data Filter** only. 0, LAN/RT/VPN -> WAN 1, WAN -> LAN/RT/VPN 2, LAN/RT/VPN -> LAN/RT/VPN
-I "<e/d> <para1, para2,…>"	It means to set incoming interface. e: Enable the function. d: Disable the function. Para1, para2,…: all, LAN1, LAN2, …, LAN4, DMZ, RT, VPN, WAN1, …, WAN6
-O "<e/d> <para1, para2,…>"	It means to set outgoing interface. e: Enable the function. d: Disable the function. Para1, para2,…: Available values include all, LAN1, LAN2,…LAN8, RT, VPN, WAN1, WAN2,…WAN7 Exampe: > ipf rule 3 1 -e 1 -O "e LAN2"
-s "o|o6|g|g6|c <field> <obj>"	It means to specify source IP object, IP group. o: Indicates “IPv4 object”. o6: Indicates IPv6 object". g: Indicates “IPv4 group”. g6: Indicates “IPv6 group”. c: Indicates country object. field: Indicates the quantity of objects/groups that can be set for this rule at one time. -2 object profiles are allowed for IPv4 -2 group profiles are allowed for IPv4 group -3 object profiles are allowed for IPv6 -1 group profiles is allowed for IPv6 group obj : indicates index number of object or index number of group. -Range for IPv4, from 1 to 192, 0 means none. -Range for IPv4 group, from 1 to 32, 0 means none. -Range for IPv6, from 1 to 64, 0 means none. -Range for IPv6 group, from 1 to 32, 0 means none. -Ranges for country object, from 1 to 32. For example, -s "o 1 2" means IPv4 object profile 1 and 2 are set as souce IP. Exampe: > ipf rule 3 1 -e 1 -s "o 1 2"
–s "u <Address Type> <Start IP Address> <End IP Address> | <Address Mask>"	It means to configure **source** IP address including address type, start IP address, end IP address and address mask. u : It means “user defined”. *Address Type* : Type the number (representing different address type). 0 : Subnet Address

	1 : Single Address 2 : Any Address 3 : Range Address Example: Set Subnet Address => -s "u 0 192.168.1.10 255.255.255.0" Set Single Address => -s "u 1 192.168.1.10 " Set Any Address => -s "u 2 " Set Range Address => -s "u 3 192.168.1.10 192.168.1.15"
-d "o|o6|g|g6|c <field> <obj>"	It means to specify destination IP object, IP group. o: Indicates “IPv4 object”. o6: Indicates IPv6 object". g: Indicates “IPv4 group”. g6: Indicates “IPv6 group”. c: Indicates country object. field: Indicates the quantity of objects/groups can be set for this rule at one time. -2 object profiles are allowed for IPv4 -2 group profiles are allowed for IPv4 group -3 object profiles are allowed for IPv6 -1 group profiles is allowed for IPv6 group obj : indicates index number of object or index number of group. -Range for IPv4, from 1 to 192, 0 means none. -Range for IPv4 group, from 1 to 32, 0 means none. -Range for IPv6, from 1 to 64, 0 means none. -Range for IPv6 group, from 1 to 32, 0 means none. -Ranges for country object, from 1 to 32. For example, -s "o 1 2" means IPv4 object profile 1 and 2 are set as destination IP. Exampe: > ipf rule 3 1 -e 1 -d "o 2 2"
–d "u <Address Type> <Start IP Address> <End IP Address> | <Address Mask>"	It means to configure **destination** IP address including address type, start IP address, end IP address and address mask. u : It means “user defined”. *Address Type* : Type the number (representing different address type). 0 : Subnet Address 1 : Single Address 2 : Any Address 3 : Range Address Example: Set Subnet Address => -d "u 0 192.168.1.10 255.255.255.0" Set Single Address => -d "u 1 192.168.1.10 " Set Any Address => -d "u 2 " Set Range Address => -d "u 3 192.168.1.10 192.168.1.15"
-S o|g <obj>	It means to specify Service Type object. o : indicates “object” profile. g: indicates “group” profile. <obj> : indicates index number of object or index number of group. Available settings range from 1-96. For example, -S "o 1" means the first service type object profile.
-S "u <protocol> <source_port_value> <destination_port_vale>"	It means to configure advanced settings for Service Type, such as protocol and port range. u : it means “user defined”. <protocol> : It means TCP(6),UDP(17), TCP/UDP(255), Any(0),

	ICMP(1), ICMPv6(58), Other(other) <source_port_value> : 1 : Port OP, range is 0-3. 0:= =, 1:!=, 2:>, 3:< 3 : Port range of the Start Port Number, range is 1-65535. 5 : Port range of the End Port Number, range is 1-65535. <destination_port_value>: 2 : Port OP, range is 0-3, 0:==, 1:!=, 2:>, 3:< 4 : Port range of the Start Port Number, range is 1-65535. 6: Port range of the End Port Number, range is 1-65535.
-f <value>	It means to set fragment type. 0 : Don't care. 1 : Unfragmented. 2 : Fragmented. 3 : Too Short
-F "<Param 0> <Param 1>"	It means the Filter action you can specify. <param 0>: Enter the number to set the filter action. 0 : Pass Immediately. 1 : Block Immediately. 2 : Pass if no further match. 3 : Block if no further match. <Param 1>: Let the log be recorded on Syslog. 0 : Disable Log. 1 : Enable Log.
-m "<Param 0> <Param 1>"	It means to set MAC Bind IP type and the Syslog. <param 0>: Enter the number to choose the type. 0 : Non-Strict. 1 : Strict. <Param 1>: Let the log be recorded on Syslog. 0 : Disable Log. 1 : Enable Log.
-Y <Param 0> <Param 1>	It means to set the User Management. <param 0>: Enter the number to choose the type. -1 : None. 0 : All. 1 : User Object 2 : User group <Param 1>: Let the log be recorded on Syslog if <param 0> is set with None/ALL. 0 : Disable. 1 : Enable. Enter the the user object number (1 to 200) / group number (1 to 32) if <param 0> is set with User Object.
-y <value>	It means the log related to User Management will be or be not recorded on Syslog. <value>: Enter 1(enable) or 0 (disable)
-L <Param 0> <Param 1>	It means to set the maximum count for the session limitation. <param 0>: Enter the number (0 to 50000) to choose the type. <Param 1>: Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.

-q <Param 0> <Param 1>	It means to set the classification for QoS. <Param 0>: 1– Class 1, 2 – Class 2, 3 – Class 3, 4 – Other <Param 1>: Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-l <Param 0> <Param 1>	It means load balance policy. Such function is used for "debug" only. <Param 0>: Enter 0, 1, 2, or 3. 0:Auto-Select, 1:WAN 1. 2:WAN 2. 3:WAN 3. <Param 1>: Enter 0 or 1. 0:Disable Log. 1:Enable Log.
-a "<Param 0> <Param 1>"	It means to specify which APP Enforcement profile will be applied. <Param 0> : Available settings range from 0 ~ 32. "0" means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-u <Param 0> <Param 1>	It means to specify which URL Content Filter profile will be applied. <Param 0> : Available settings range from 0 ~ 8. "0" means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-w "<Param 0> <Param 1>"	It means to specify which Web Content Filter profile will be applied. <Param 0> : Available settings range from 0 ~ 8. "0" means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-n "<Param 0> <Param 1>"	It means to specify which DNS Filter profile will be applied. <Param 0> : Available settings range from 0 ~ 8. "0" means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-N <value>	It means to set the Next Filter Set. <value> : Available settings range from 0 ~ 12. "0" means no profile will be applied. 0 : None 1 : Set#1; 2: Set#2, and so on.
-c <0~20>	It means to set code page. Different number represents different code page. 0. None 1. ANSI(1250)-Central Europe

	2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/OEM(874)-Thai 17. ANSI/OEM(932)-Japanese Shift-JIS 18. ANSI/OEM(936)-Simplified Chinese GBK 19. ANSI/OEM(949)-Korean 20. ANSI/OEM(950)-Traditional Chinese Big5
-C "<Windows Size> <Session_Timeout>"	It means to set Window size and Session timeout (Minute). <Windows Size> - Available settings range from 1 ~ 65535. <Session_Timeout> - Make the best utilization of network resources.
-b <value>	It means to enable or disable the DrayTek Banner. <value>: 0 : Disable; 1 : Enable.
-t "i <Param 0> <Param 1>"	It means to set schedule profile. Totally, there are four sets of schedule profiles can be specified. <param 0>: Enter the index number (1 to 4) for each set. <param 1>: Enter the index number (0 to 15) of the schedule profile for each set. 0 means none. For example, -t "i 1 3" means schedule profile #3 is configured for set #1. Exampe: > ipf rule 3 1 -e 1 -t "i 1 3"
-t "c <value>"	It means to enable or disable the function of clearing sessions when the schedule is ON. <value>: 0 : Disable; 1 : Enable.
-M <Your Comments>	It means to set comments for the fitler rule. <Your Comments>: Enter a brief description.
-U "<up/down>"	It means to move up or move down the order of a filter rule in the filter set. up: It indicates move the filter rule up. down: It indicates move the filter rule down.

Example

```
> ipf rule 2 1 -e 1 -M "Your Comments" -s "o 1" -d "o 2" -S "o 1" -F "1"
> ipf rule 2 1 -v
Filter Set 2 Rule 1:

Status  : Disable
Comments: <null>
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>
```

```
Clear sessions when schedule is ON: Disable

Direction         : LAN/RT/VPN -> WAN
Src Interface     : LAN1, LAN2, LAN3, LAN4, Routed, VPN
Dst Interface     : WAN1, WAN2, WAN3, WAN4, WAN5, WAN6
Source IP         : Any
Destination IP    : Any
Service Type      : Any
Fragments         : Don't Care

Pass or Block             : Pass Immediately
Branch to Other Filter Set: None
Max Sessions Limit        : 50000
Current Sessions          : 0
Mac Bind IP               : Non-Strict
Qos Class                 : None
APP Enforcement           : None
URL Content Filter        : None
WEB Content Filter        : None
DNS Filter                : None
Load-Balance policy       : Auto-select
Log                       : Disable
------------------------------------------------------------------------
CodePage                  : ANSI(1252)-Latin I
Window size               : 65535
Session timeout           : 60
DrayTek Banner            : Enable
  ------------------------------------------------------------------------
  Strict Security Checking
    [ ]APP Enforcement
DrayTek>
```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

Syntax

ipf flowtrack set *[-re]*

ipf flowtrack view *[-f]*

ipf flowtrack *-i<IP address> -p<value>-t<value>*

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.

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 flowtrack OFF
Refresh the flowstate ok
>
```

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 *[-cfhiptwx?] [-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.
-F	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
-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.

Example

```
> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
```

```
       Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

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	It means to Enter the number for 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	It means to enter the number for 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	It means to 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 sslvpnport

This command allows users to set SSL VPN port for management.

Syntax

mngt sslvpnport <*SSL VPN port***>**

Syntax Description

Parameter	Description
SSL VPN port	It means to type the number for SSL VPN port. The default setting is 443.

Example

```
> mngt sslvpnport 1010
% Set SSL VPN port to 1010 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	It means to 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	It means to 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.
del port	It means to delete a TCP port for block.
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/snmp*> <*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/snmp	It means to specify one of the servers/protocols for enabling or disabling.
on/off	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> -I <value>*

mngt lanaccess *–f*

mngt lanaccess *–d*

mngt lanaccess *–v*

mngt lanaccess *–h*

Syntax Description

Parameter	Description
-e <0/1>	It means to enable/disable the function. 0-disable the function. 1-enable the function.
-s <value>	It means to specify service offered. Available values include: FTP, HTTP, HTTPS, TELNET, SSH, None, All
-i<value>	It means the interface which is allowed to access. Available values include: LAN1~LAN8, IP Routed Subnet, None, All **Note**: LAN1 is always allowed for accessing into the router.
-I <value>	It means the IP object index allowed to access. Available values include: 1 to 192
-E <0/1>	It means to enable the function of specific IP allowed to be access. 0-disable the function. 1-enable the function.
-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.

Example

```
> mngt lanaccess -e 1
> mngt lanaccess -s FTP,TELNET
> mngt lanaccess -i LAN3
> mngt lanaccess -v
Current LAN Access Control Setting:
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 49: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 50: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 51: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 52: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 53: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 54: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 55: enabled
     - Specific IP(IP object:0) is disabled
   - LAN 56: enabled
     - Specific IP(IP object:0) is disabled
   - IP Routed Subnet 8: 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 Object Index*>

mngt accesslist *remove <index>*

mngt accesslist *flush*

Syntax Description

Parameter	Description
list	It can display current setting for your reference.
add <index> <IP Object Index>	It means adding a new entry. <index>: Specify the number (1 to 10) of the entry. <IP Object Index>: Specify the index number (1 to 192) of the IP object profile.
remove <index>	It means to delete the selected item. <index>: Specify the number (1 to 10) of the entry.
flush	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 1
%% Set OK.
> mngt accesslist list
%% Access list :
  [Index]      [IP Object Index]      [IP/CIDR or StartIP ~ EndIP]
=========================================================================
  1           1                    Please setting index=1 for IP Object
>
```

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.
-a <1/2>	1: Enable the SNMPV1 function. 2: Disable the SNMPV1 function.
-b <1/2>	1: Enable the SNMPV2C function. 2: Disable the SNMPV2C function.
-c <1/2>	1: Enable the SNMPV3 function. 2: Disable the SNMPV3 function.
-g <Community name>	It means to set the name for getting community by typing a proper character. (max. 23 characters)
-s <Community name>	It means to set community by typing a proper name. (max. 23 characters)
-m <IP address>	It means to set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.

	It allows to set 3 IPs, separated by ",".
-t <Community name>	It means to set trap community by typing a proper name. (max. 23 characters)
-n <IP address>	It means to set the notification host. It allows to set 2 IPs, separated by ",".
-T <seconds>	It means to set the trap timeout <0~999>.
-o <username>	It means to set a user account (maximum 23 characters) for user management.
-p <0/1/2>	It means to set the authentication algorithm. 0: No auth 1: MD5_AUTH 2: SHA_AUTH
-q <password>	It means to set the password (maximum 23 characters) for authentication.
-r <0,3/4/6>	It means to set privacy algorithm 0, 3: No_PRIV 4: DES_PRIV 6: AES_PRIV
-u <password>	It means to set the password (maximum 23 characters) for privacy.
-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: mngt bfp

This command allows you to configure brute force protect (BFP) for system management.

Syntax

mngt bfp *[<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 / disable the BFP function. 0 – Disable 1 – Enable

-s <service>	It means to enable different service. service - Available types are FTP, HTTP, HTTPS, TELNET, TR069, SSH, and All.
-l <failure>	It means to set login failure retry times. failure - Available number is from 1 to 255.
-p <penalty>	It means to set penalty time for BFP. The unit is sec.
-v	It means to view current settings.

Example

```
> mngt bfp -e 1
> mngt bfp -s FTP
> mngt bfp -l 10
> mngt bfp -v
Current Brute Force Protection Setting:
* Enable: yes
* Service:
 - FTP:        yes
 - HTTP:       no
 - HTTPS:      no
 - TELNET:     no
 - TR069:      no
 - SSH:        no
* Maximum login failures: 10
* Penalty period: 0
```

Telnet Command: mngt cert_import

This command allows you to import a certificate to Vigor router.

Syntax

mngt cert_import local_cert *<URL><password>*

mngt cert_import trusted_ca *<URL>*

Syntax Description

Parameter	Description
local_cert url <URL> <password>	URL - Enter a URL(http://....) for downloading the certificate. The file is encrypted with the file format of "xxxx.p12". Password - Enter the password for decrypting the .p12 certificate.
trusted_ca <URL>	URL - Enter a URL(http://....) for downloading the certificate. The file is encrypted with the file format of "xxxx.p12".

Telnet Command: mngt telnettimeout

This command allows you to configure the timeout for telnet connection.

Syntax

mngt telnettimeout <*value*>

Syntax Description

Parameter	Description
<*value*>	Range from 60 to 300. The default value is 300 (seconds).

Example

```
> mngt telnettimeout 100
% Telnet timeout : 100s
```

Telnet Command: mngt sshtimeout

This command allows you to configure the timeout for SSH connection.

Syntax

mngt sshtimeout <*value*>

Syntax Description

Parameter	Description
<*value*>	Range from 60 to 300. The default value is 180 (seconds).

Example

```
> mngt sshtimeout 200
% SSH timeout : 200s
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

Syntax

msubnet switch <*2/3/4*> <*On/Off*>

Syntax Description

Parameter	Description
<*2/3/4*>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<*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 *<2/3/4> <IP address>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 *<2/3/4> <IP address>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 *<2/3/4>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4

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 *<2/3/4>* *<On/Off>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 *<2/3/4> <On/Off>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 *<2/3/4> <Gateway IP>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3

	4=LAN4
<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 *<2/3/4> <IP counts>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 *<1/2/3/4> <1/2/3/4> <On/Off>*

Syntax Description

Parameter	Description
<1/2/3/4>	It means LAN interface. 1=LAN1

	2=LAN2 3=LAN3 4=LAN4
<*On/Off*>	On – It means Off **-** It means

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1 and LAN2!
> msubnet talk ?
% msubnet talk <1/2/3/4> <1/2/3/4> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4,
% Now:
%            LAN1   LAN2   LAN3   LAN4
% LAN1         V
% LAN2         V     V
% LAN3                     V
% LAN4                           V
>
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

msubnet startip <*2/3/4*> <*Gateway IP*>

Syntax Description

Parameter	Description
<*2/3/4*>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<*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
>
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

msubnet pppip *<2/3/4> <Start IP>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 <2/3/4> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200
>
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

msubnet nodetype *<2/3/4> <count>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 2
% Set LAN2 Dhcp Node Type done !!!
> msubnet nodetype ?
% msubnet nodetype <2/3/4> <count>
% Now: LAN2 2; LAN3 0; LAN4 0

% 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 *<2/3/4> <WINS IP>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<WINS IP>	Enter the IP address as the WINS IP.

Example

```
> msubnet primWINS 2 192.16.3.5

% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS

% msubnet primWINS <2/3/4> <WINS IP>

% Now: LAN2 192.16.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

Syntax

msubnet secWINS *<2/3/4> <WINS IP>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<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 <2/3/4> <WINS IP>
% Now: LAN2 192.168.3.89; LAN3 0.0.0.0; LAN4 0.0.0.0
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

Syntax

msubnet tftp *<2/3/4>* *<TFTP server name>*

Syntax Description

Parameter	Description
<2/3/4>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<TFTP server name>	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

> msubnet tftp
% msubnet tftp <2/3/4> <TFTP server name>
% Now: LAN2 publish
         LAN3
         LAN4
>
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/ IP Routed Subnet.

Syntax

msubnet mtu *<interface>* *<value>*

Syntax Description

Parameter	Description
<interface>	Available settings include LAN1~LAN4, and IP_Routed_Subnet.
<value>	1000 ~ 1500 (Bytes), default: 1500 (Bytes)

Example

```
> msubnet mtu LAN1 1492
Set LAN1 subnet mtu as 1492
> msubnet mtu
Usage:

  >msubnet mtu <interface> <value>

  <interface>: LAN1~LAN4,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)
   LAN3 MTU:           1500 (Bytes)
   LAN4 MTU:           1500 (Bytes)
   IP Routed Subnet MTU: 1500 (Bytes)

>
```

Telnet Command: msubnet leasetime

This command is used to set leasetime for multi-subnet.

Syntax

msubnet leasetime <*1/2/3/4*> <*Lease Time sec.*>

Syntax Description

Parameter	Description
<*1/2/3/4*>	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4
<*Lease Time sec.*>	Enter a value (range: 10 to 259200).

Example

```
> msubnet leasetime 1 18603
% Set LAN1 lease time: 18603

> msubnet leasetime ?
% msubnet leasetime <1/2/3/4> <Lease Time (sec.)>
% Now:LAN1 18603; LAN2 259200; LAN3 259200; LAN4 259200
>
```

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 *<INDEX> -a <TYPE> <START_IP> <END/MASK_IP>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
<INDEX>	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: *object ip obj 1 -v*
-n <NAME>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object ip obj 9 -n bruce*
-i <INTERFACE>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: *object ip obj 8 -i 0*
-s <INVERT>	It means to set invert seletion for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: *object ip obj 3 -s 1*
-a <TYPE>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Range TYPE=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. Type an IP address.
<END/MASK_IP>	Type 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*>	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object ip grp 1 -v*
-n <NAME>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: *object ip grp 8 -n bruce*
-i <INTERFACE>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: *object ip grp 3 -i 0*
-a <IP_OBJ_INDEX>	It means to specify IP object profiles for the group profile. 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]

Set ok!
> object ip grp 2 -i 1
IP Group Profile 2
 Name   :[First]
 Interface:[Lan]
 Included ip object index:
 [0:][1]
 [1:][2]
 [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 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 *<INDEX> -a <TYPE> <START_IP> <END/MASK_IP>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
<INDEX>	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: *object ip obj 1 -v*
-n <NAME>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object ip obj 9 -n bruce*
-i <INTERFACE>	It means to define an interface for the IP object.

	INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: *object ip obj 8 -i 0*
-s <INVERT>	It means to set invert seletion for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: *object ip obj 3 -s 1*
-a <TYPE>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang 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. Type an IP address.
<END/MASK_IP>	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ipv6 obj 3 -n marketing
Setting saved.
> object ipv6 obj 3 -a 0 2607:f0d0:1002:51::4 128
Setting saved.
> object ipv6 obj 3 -v
 IPv6 Object Profile 3
 Name   :[marketing]
 Address Type:[mask]
 Start IPv6 Address:[2607:F0D0:1002:51::4]
 End IPv6 Address:[::]
 Prefix Length:[128]
 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 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>	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object ip grp 1 -v*
-n <NAME>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: *object ip grp 8 -n bruce*
-i <INTERFACE>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: *object ip grp 3 -i 0*
-a <IP_OBJ_INDEX>	It means to specify IP object profiles for the group profile. 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 ipv6 grp 3 -a 1 2 3 4 5
 IP Group Profile 3
 Name   :[]
Included ip object index:
[0:][1]
[1:][2]
[2:][3]
[3:][4]
[4:][5]
[5:][0]
[6:][0]
[7:][0]
> object ipv6 grp 3 -n marketing
 IPv6 Group Profile 3
 Name   :[marketing]
 Included ip object index:
 [0:][1]
 [1:][2]
 [2:][3]
 [3:][4]
 [4:][5]
 [5:][0]
 [6:][0]
 [7:][0]
```

Telnet Command: object country obj

This command is used to create country object profile.

Syntax

object country set *<INDEX> -v*

object country set *<INDEX> -n <NAME>*
object country set *<INDEX>-a <COUNTRY_INDEX>*
object country activate
object country setdefault
object country list

Syntax Description

Parameter	Description
<INDEX>	It means the index number of the specified country object profile (1 to 32).
<name>	It means to set a name of the object.
<COUNTRY_INDEX>	It means the code number of a country. To get the detailed information of the code number, use "object country list" to get the one you need.oj
activate	It means to activate the country object profile.
setdefault	It means to return to default settings for all profiles.
list	Displays a list of country with code number. For example, "222" means "Taiwan"; "241" means "United States".

Example

```
> object country set 1 -n Best
Country object Profile 1
 Name   :[Best]
 Included country index:

Set ok!
> object country set 1 -a 222
> object country set 1 -a 222
 Country object Profile 1
 Name   :[Best]
 Included country index:
 [0:][222] Taiwan

Set ok!
```

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>	It means the index number of the specified service object profile.
-v	It means to view the information of the specified service object profile. Example: *object service obj 1 -v*
-n <NAME>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object service obj 9 -n bruce*
-i <PROTOCOL>	It means to define a PROTOCOL for the service object profile. PROTOCOL =0, means any PROTOCOL =1, means ICMP PROTOCOL =2, means IGMP PROTOCOL =6, means TCP PROTOCOL =17, means UDP PROTOCOL =255, means TCP/UDP Other values mean other protocols. Example: *object service obj 8 -i 0*
<CHK>	It means the check action for the port setting. 0=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=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=larger**(>)**, the port number greater than this value is available.. 3=less**(<)**, the port number less than this value is available for this profile.
-s <CHK> <START_P> <END_P>	It means to set source port check and configure port range (1~65565) for TCP/UDP. START_P: Enter a port number as a starting port. END_P, type a port number as an ending port. Example: *object service obj 3 -s 0 100 200*
-d <CHK> <START_P> <END_P>	It means to set destination port check and configure port range (1~65565) for TCP/UDP. START_P: Enter a port number as a starting port. END_P: Enter a port number as an ending point. 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:[255]
 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>	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object service grp 1 -v*
-n <NAME>	It means to define a name for the service group. NAME: Type a name with less than 15 characters. Example: *object service grp 8 -n bruce*
-a <SER_OBJ_INDEX>	It means to specify service object profiles for the group 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 Grope_1
 Service Group Profile 1
 Name   :[Grope_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 PAGE

object kw obj *<INDEX> -v*

object kw obj *<INDEX> -n <NAME>*

object kw obj *<INDEX> -a <CONTENTS>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
show PAGE	It means to show the contents of the specified profile. PAGE: Enter the page number.
show	It means to show the contents for all of the profiles.
<INDEX>	It means the index number of the specified keyword profile.
-v	It means to view the information of the specified keyword profile.
-n <NAME>	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
-a <CONTENTS>	It means to set the contents for the keyword profile. Example: *object kw obj 40 -a test*

Example

```
> object kw obj 1 -n children
 Profile 1
 Name   :[children]
 Type   :[Normal]
 Content:[]
> object kw obj 1 -a gambling
 Profile 1
 Name   :[children]
 Type   :[Normal]
 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>	It means the index number (from 1 to 8) of the specified file extension object profile.
-v	It means to view the information of the specified file extension object profile.
-n <NAME>	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
-e	It means to enable the specific CATEGORY or FILE_EXTENSION.
-d	It means to disable the specific CATEGORY or FILE_EXTENSION
<CATEGORY><FILE_EXTENSION>	CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Executation, P2P, Document Example: *object fe obj 1 -e Image* FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".ico", ".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", ".doc", ".docx", ".odp", ".ods", ".odt", ".pdf", ".ppt", ".pptx", ".xls", ".xlsx" 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
-------------------------------------------------------------------------
P2P category:
 [ ].torrent
-------------------------------------------------------------------------
Document category:
 [ ].doc   [ ].docx  [ ].odp   [ ].ods   [ ].odt   [ ].pdf   [ ].ppt   [ ].pptx
 [ ].xls   [ ].xlsx
```

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>	It means the index number (from 1 to 10) of the specified SMS object profile.
-v	It means to view the information of the specified SMS object profile.
-n <NAME>	It means to define a name for the SMS object profile. NAME: Type a name with less than 15 characters.
-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. 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)
-u <Username>	It means to define a user name for the SMS object profile. Type a user name that the sender can use to register to selected SMS provider.
-p <Password>	It means to define a password for the SMS object profile. Type a password that the sender can use to register to selected SMS provider.
-q <Quota>	Enter the number of the credit that you purchase from the service provider. Note that one credit equals to one SMS text message on the standard route.
-I <Interval>	It means to set the sending interval for the SMS to be delivered. Enter the shortest time interval for the system to send SMS.
-l <URL>	It means to set the URL for Custom 1 and Custom 2 profiles. The profile name for Custom 1 and Custom 2 are defined in default and can not be changed.

Example

```
> object sms obj 1 -n TW
> 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:[TW]
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***> -***l*** <*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*>	It means the index number (from 1 to 10) of the specified mail object profile.
-v	It means to view the information of the specified mail object profile.
-n <Profile Name>	It means to define a name for the mail object profile. *Profile Name*: Type a name with less than 15 characters.
-s <SMTP Server>	It means to set the IP address of the mail server.
-l <Use SSL<	It means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. 0 – disable 1 – enable to use the port number.
-m <SMTP Port>	It means to set the port number for SMTP server.
-a <Sender Address>	It means to set the e-mail address (e.g., johnwash@abc.com.tw) of the sender.
-t <Authentication>	The mail server must be authenticated with the correct username and password to have the right of sending message out. 0 – disable 1 – enable to use the port number.
-u <Username>	Type a name for authentication. The maximum length of the name you can set is 31 characters.
-p <Password>	Type a password for authentication. The maximum length of the password you can set is 31 characters.
-i <Sending Interval>	Define the interval for the system to send the SMS out. The unit is second.

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:[0(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>	It means the index number (from 1 to 8) of the specified notification object profile.
-v	It means to view the information of the specified notification object profile.
-n <Profile Name>	It means to define a name for the notification object profile. *Profile Name*: Type a name with less than 15 characters.
–e	It means to enable the status of specified category.
-d	It means to disable the status of specified category.
Category	Available categories are: 1: WAN; 2: VPN Tunnel; 3: Temperature Alert; 4: WAN Budget; 5: CVM; 6: High Availability
status	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. For High Availability – 1: Failover Occurred, Config Sync Fail, and Router Unstable

Example

```
> object noti obj 1 –n market
> object noti obj 1 -e 2 1
> object noti obj 1 -v
Profile Index: 1
Profile Name:[market]
```

```
   Category                  Status
WAN                  [v]Disconnected     [v]Reconnected
VPN Tunnel           [v]Disconnected     [ ]Reconnected
Temperature Alert    [ ]USB Temperature Out of Range
WAN Budget Alert     [ ]Limit Reached
Security             [ ]Web Log-in event occurs
                     [ ]Telnet Log-in event occurs
                     [ ]SSH Log-in event occurs
                     [ ]TR069 Log-in event occurs
                     [ ]FTP User Log-in event occurs
                     [ ]Config-Changed event occurs
```

Telnet Command: object schedule

This command is used to create schedule object profile.

Syntax

object schedule set *INDEX option*
object schedule view
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	Available options for schedule.
-e <value>	It means to enable the schedule setup. 0 – disable 1 – enable
-c <comment>	It means to set brief description for the specified profile. The length range of the comment: 0 ~ 32 characters.
-D <year><month><day>	It means to set the starting date of the profile. [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"*
-T <hour><minute>	It means to set the starting time of the profile. [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"*
-d <hour><minute>	It means to set the duration time of the profile. [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"*
-a <value>	It means to set the action used for the profile. [value] – 0:Force On, 1:Force Down, 2:Enable Dial-On-Demand, 3:Disable Dial-On-Demand
-I <value>	It means to set idle time. [value] – Must be between 0-255(minute). The default is 0.
-h <option> <day/date/cycle_days>	Set how often the schedule will be applied. [option] – Enter 0 to 3.

	0: Once, 1: Weekdays 2: Monthly 3: Cycle days [day] – Enter Sun, Mon, Tue, Wed, Thu, Fri, Sat. If the [option] set as 1(Weekdays), then select which days of a Week. [date] : 1-28 If the [option] set as 2(Monthly), then select which date of a Month. [cycle_days] : 1-30 If the [option] set as 3 (cycle days), then select which days to do the cycle schedule. example: To select Sunday, Monday, Thursday, type *> object schedule set 1 -h "1 Sun Mon Thu"*
view <INDEX>	It means to show the content of the profile.
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 "2020 11 8"
> 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)  [ 2020 ]-[ 11 ]-[  8 ]
      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, 3, 4, all> <AN, 1G, 100F, 100H, 10F, 10H, status>*

port *<wan2> <AN, 1000F, 100F, 100H, 10F, 10H, status>*

port *<enable, disable> <1, 2, 3, 4, all>*

port status

port sniff *<on,off,port,txrx,restart,status>*

port 8021x *<enable,disable,status,addport,delport>*

port jumbo *<on/off>*

port jumbo *size <value>*

port wanfc *<INDEX> <on/off/status>*

Syntax Description

Parameter	Description
<1, 2, 3, 4, all> <AN, 1G, 100F, 100H, 10F, 10H, status>	It means to set the LAN port and the physical type for the specific port. <1, 2, 3, 4, all>: Select an interface. <AN, 1G, 100F, 100H, 10F, 10H, status>: Select 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 to set the WAN port and the physical type for the specific port. <wan2>: Select an interface. <AN, 1000F, 100H, 10F, 10H, status>: Select 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.
<enable, disable> <1, 2, 3, 4, all>	It means to enable or disable the LAN port(s). <enable, disable>: Enter enable or disable. <1,2,3,4, all>: Enter the number to select a LAN port. Or, enter "all" to select all ports.
status	It means to view the Ethernet port status.
sniff <on,off,port,txrx,restart,status>	It means to set settings for sniffer. <on,off,port,txrx,restart,status>: See the following, on - Turn on the sniffer. off - Turn off the sniffer. port - Specify a LAN port (p1, p2, p3 or p4). restart - Restart the system to activate the settings. status - Display current settings. rxrx - Set the transmission and receiving rates for a LAN/WAN port. e.g., > port sniff txrx 30000 p2
802.1x <enable,disable,status,addport,delport>	It means to set settings for 802.1x. <enable,disable,status,addport,delport>: See the following, enable - Enable the function. disable - Disable the function. status - Display current settings. addport - Add a port number (1 to 4). delport - Delete a port number (1 to 4).
Jumbo <on/off>	It means to enable or disable the Jumbo function. <on/off>:If enabled, set a value for the jumbo frame.

jumbo size <value>	If jumbo is enabled, set a jumbo size. <value>: 1537 to 9022. Set a number.
wanfc <INDEX> <on/off/status>	It means to set WAN flow control. <INDEX>: Enter the index number (1 to 2) of the WAN interface. <on/off/status>: Enter "on" to enable the function; enter "off" to disable the function; enter "status" to view current settings.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
> port wanfc 1 status
% WAN1 local node flow control support: ON
```

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: ppa

This command allows you to configure PPA mode.

ppa *[-<command> <parameter> | …]*

ppa n *[-<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.
-z <1/0>	Enable or disable the PPA Hardware Acceleration. <1/0>: Enter 1(enable) or 0 (disable).
-m <mode>	Specify a mode. 1=auto 2=manual(traffic) 3=manual(qos) 0=disable
-p <proto>	Specify a protocol. <proto> - 1-TCP; 2-UDP; 3-Both.
-b <1/0>	Enable/disable TWO-way hardware acceleration. <1/0>: Enter 1(enable) or 0 (disable).
-M enable/disable	Enable/disable the multicast hardware acceleration.
-S	Show multicast table in HW accleration
-v	Show PPA_WAN_Table and PPA_LAN_Table for reference.
-c	Clean all settings.
-x	Show hardware acceleration information.
-k	Clean the PPA table.
ppa n – used in QoS or specific host	
-l <rule>	Specify an index number of rule profile for QoS mode.
-x	Show hardware acceleration information.
-k	Clean the PPA table.

Example

```
> ppa -m 1 -p 1 -b 0
 Set ok! The PPA mode is Auto
% You need to set the Manual mode first !

> ppa –v
%PPA is enabled
%PPA NAT is enabled
% PPA mode is Auto
%PPA Protocol TCP 1, UDP 0
%PPA Multicast is enabled
%PPA two way enable
%PPA time  is 10
%PPA range is 8000
%PAE range is 2048
%MPE range is 5952
%PPA LAN entries 0, working 0
%PPA WAN entries 0, working 0
%PPA statistics interval: 5 sec
>
```

Telnet Command: prn

This command allows you to view current status (interface and driver) of USB printer.

Syntax

prn status

prn debug

prn enable <0/1>

Example

```
> prn status
Interface: USB bus 2.0
Printer: NotReady

> prn debug
conn[0] :
none
conn[1] :
none
conn[2] :
none
conn[3] :
none
LPD_data_total=0

usblp_ptr=0
UsbPrintReady=0, UsbIsPrinting=0
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup *[-<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.
-W <1~3>	It means to select an interface. <1~3>: 1 is WAN1; 2 is WAN2; 3 is WAN3. The default is WAN1.
-m <mode>	It means to define which traffic the QoS control settings will apply to and eable QoS control. 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. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only) The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.

-r <index:ratio>	It means to set ratio for class index, in %.
-u <mode>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.
-p <ratio>	It means to enable bandwidth limit ratio for UDP.
-t <mode>	It means to enable/disable Outbound TCP ACK Prioritize. 0: disable 1: enable
-V	Show all the settings.
-I <bandwidth>	It means the minimum available non-VoIP Inbound Bandwidth when VoIP is detected (Kbps). <bandwidth>: Enter a value. Default value: half of WAN inbound bandwidth.
-O <bandwidth>	It means the minimum available non-VoIP Outbound Bandwidth when VoIP is detected (Kbps). <bandwidth>: Enter a value. Default value: half of WAN outbound bandwidth.
-v <0/1>	It means to adjust to minimum In/Out bandwidth setting (or half QoS bandwidth). 0: Auto bandwidth adjustment. 1: When VoIP detected, QoS In/Out bandwidth will be adjusted to minimum values.
-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
 inbound bandwidth set to 9500
 outbound bandwidth set to 8500
 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.

	Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-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. 0: disable, 1: enable
-I <addr>	Set the local address. *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. *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.
-s <Service type>	Specify the predefined service type by typing the number. The available types are listed as below: 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
-u <Service type>	Specify the user defined service type by typing the number (1 to 40).
-S <d/s>	Show the content for specified DSCP ID/Service type.
-V <1/2/3>	Show the rule in the specified class.

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>]***.**

Syntax Description

Parameter	Description
-a <name>	It means to add rule.
-e <no>	It means to edit user defined service type. “no” means the index number. Available numbers are 1~40.
-d <no>	It means to delete user defined service type. “no” means the index number. Available numbers are 1~40.
-n <name>	It means the name of the service.
-t <type>	It means protocol type. 6: tcp(default) 17: udp 0: tcp/udp <1~254>: other
-p <port>	It means service port. 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 voip

This command allows user to enable or disable the QoS for VoIP and RTP.

Syntax

qos voip *<on/off>*

Syntax Description

Parameter	Description
on/off	On – Enable the QoS for VoIP. Off – Disable th QoS for VoIP.

Example

```
> qos voip off
QoS for VoIP: Disable; SIP Port: 5060
>
```

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
[V]LAN2  192.168.5.1    255.255.255.0   V   192.168.2.90   15   192.168.2.1
[X]LAN3  192.168.3.1    255.255.255.0   V   192.168.3.10   100  192.168.3.1
[X]LAN4  192.168.4.1    255.255.255.0   V   192.168.4.10   100  192.168.4.1
[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

```
%     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]

%  LAN3  Primary DNS: [Not set]
%  LAN3  Secondary DNS: [Not set]
```

```
%  LAN4  Primary DNS: [Not set]
%  LAN4  Secondary DNS: [Not set]

%  LAN5  Primary DNS: [Not set]
%  LAN5  Secondary DNS: [Not set]

%  LAN6  Primary DNS: [Not set]
%  LAN6  Secondary DNS: [Not set]

%  LAN7  Primary DNS: [Not set]
%  LAN7  Secondary DNS: [Not set]

%  LAN8  Primary DNS: [Not set]
%  LAN8  Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
%%     Openport settings:
Index   Status  Comment       Local IP Address
*******************************************************
                No data entry.
```

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
--- 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 [Timeout/Protocol/Flag]
------------------------------------------------------------------------------
```

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: 50000
% Maximum Session Usage: 0
% Current Session Usage: 0
% Current Session Used(include waiting for free): 15
```

```
% WAN1 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:46:20:29
LAN Status
Primary DNS:8.8.8.8         Secondary DNS:8.8.4.4
IP Address:192.168.1.1       Tx Rate:265153    Rx Rate:234251

WAN 1 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:tcom
Mode:PPPoE      Up Time:00:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate(bps):0   RX Packets:0         RX Rate(bps):0


WAN 3 Status: Disconnected
Enable:Yes      Line:USB        Name:
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: show voip

This command displays current status of voip.

Example

```
> show status
Idx    LAN_IP  PeerIP  via    Delay(ms)      Jitter(ms)     Loss(%) Time
Duration(sec)   Status
[11] 0.0.0.0   0.0.0.0 ----    0      0      0      --------       -----
---
[10] 0.0.0.0   0.0.0.0 ----    0      0      0      --------       -----
---
[9] 0.0.0.0    0.0.0.0 ----    0      0      0      --------       -----
---
[8] 0.0.0.0    0.0.0.0 ----    0      0      0      --------       -----
---
[7] 0.0.0.0    0.0.0.0 ----    0      0      0      --------       -----
---
[6] 0.0.0.0    0.0.0.0 ----    0      0      0      --------       -----
---
[5] 0.0.0.0    0.0.0.0 ----    0      0      0      --------       -----
---
[4] 0.0.0.0    0.0.0.0 ----    0      0      0      --------       -----
---
[3] 0.0.0.0    0.0.0.0 ----    0      0      0      --------       -----
---
```

```
[2] 0.0.0.0    0.0.0.0 ----   0      0      0      --------       -----
---
[1] 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 traffic

This comman can display traffic graph for WAN1 to WAN4, transmitted bytes, receivied bytes and sessions.

Syntax

show traffic *[wan1/wan2/wan3/wan4] [tx/rx] [weekly]*

show traffic *[ipaddr] [tx/rx]*

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 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9
 ,10 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,10
 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,
9 ,9 ,9 ,9 ,9 ,9 ,10 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9 ,9
 >
```

Telnet Command: show clienttraffic

This command displays packet information for specified external device.

Syntax

show clienttraffic <*device index*> <*wan# or lan#*> <*tx/rx*> <*weekly*>

Syntax Description

Parameter	Description
<*device index*>	Enter the device index (01 – 30) in double-digit (ex: 01, 02) for external device. Use “switch list” to check which VigorSwitch connects to this router. Then, Enter the index number of this VigorSwitch in this field.
<*wan# or lan#*>	wan# - Specify WAN interface (WAN1 to WAN2) for Vigor router. lan#- Specify LAN interface (LANA / LANB) for Vigor router.
<*tx/rx*>	Tx – Inidcate transmitted data.

	Rx – Indicate receivied data.
<*weekly*>	Display the transmitted data or receivied data collected weekly.

Example

```
> show clienttraffic 01 wan1 tx weekly
> show clienttraffic ?
% clienttraffic [device index] [wan# or lan#] [tx/rx] [weekly]
The external devices index must be between 01 and 30.
Do the command "switch list" to check the device index and device type.
Enter the device index in double-digit. ex: 01, 02, ...
```

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 ~WAN5 (including multi-PVC) interface for displaying related statistics.

Example

```
> 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
 >
```

Telnet Command: smb setting

This command is used to configure file sharing settings for SMB server.

Syntax

smb setting *<enable/disable>*

smb setting *show status*

smb setting *set workgroup <Workgroup name>*

smb setting *set host <host name>*

smb setting *set access <LAN / LANWAN>*

smb setting *set version <v1v2/v2>*

Syntax Description

Parameter	Description
<enable/disable>	Enable or disable the SMB service.
show status	Displays current status of SMB service.
Set workgroup <Workgroup name>	It means to set a name of workgroup for SMB service.
set host <host name>	It means to set a name of the host for SMB service.
set access <LAN / LANWAN>	It means to set the access into SMB server by LAN or borth LAN and WAN.
set version <v1v2/v2>	It means to set SMB server version.

Example

```
> smb setting enable
SMB service is enabled.

> smb setting set access LAN
Allow SMB access from LAN only.
> smb setting set version v1v2
SMB version: v1 and v2.
>
```

Telnet Command: srv dhcp dhcp2

This command is used for configuring which method (LAN interface or MAC address) that the DHCP server on IP routed LAN shall use for assigning an IP address to the IP routed LAN clients.

Syntax

srv dhcp dhcp2 *-l <enable>*

srv dhcp dhcp2 *-m <enable>*

srv dhcp dhcp2 *-e <id>*

srv dhcp dhcp2 *-d <id>*

srv dhcp dhcp2 *-v*

Syntax Description

Parameter	Description

-l <enable>	The DHCP server assigns the IP addresses to the clients via LAN port. <enable> : Enter 0 (disable) or 1 (enable).
-m <enable>	The DHCP server assigns the IP addresses to the clients via MAC address configuration. <enable> : Enter 0 (disable) or 1 (enable).
-e <id>	Turn on the flag of LAN 1 or LAN 2 if LAN port is enabled. <id>: Enter 1 or 2.
-d <id>	Turn off the flag of LAN port 1 or LAN port 2. <id>: Enter 1 or 2.
-v	View current status.

Example

```
> srv dhcp dhcp2 -l 1 -e 1,2
> 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/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>:* Specify 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 XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host.
del <MAC Addr XX-XX-XX-XX-XX-XX/all/ALL>	It means removing the selected MAC address. <MAC Addr XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host. all/ALL: It means all of the MAC addresses.

Example

```
> srv dhcp public start 192.168.1.100
```

```
%% You must enable IP routing !!!
> 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/lan3/lan4> <DNS IP address>*

Syntax Description

Parameter	Description
<lan1/lan2/lan3/lan4>	It means to sepcify the LAN interface for setting the DNS server.
<DNS IP address>	It means the IP address that you want to use as DNS1. **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 <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/lan3/lan4> <DNS IP address>*

Syntax Description

Parameter	Description
<lan1/lan2/lan3/lan4>	It means to sepcify the LAN interface for setting the DNS server.
<DNS IP address>	It means the IP address that you want to use as DNS2. **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 lan2 10.1.1.1
% srv dhcp dns2 lan2 <DNS IP address>
% Now: 10.1.1.1
>
```

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
?	It means to display the current status.
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.

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.

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 2nd_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.
<*index*>	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

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.

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.

Syntax

srv dhcp status <*LAN1/2/3/4/ip_routed_subnet>*

Syntax Description

Parameter	Description
<*LAN1/2/3/4/ip_routed_subnet>*	It means to display current status for the selected interface.

Example

```
> srv dhcp status lan1
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
-------------------------------------------------------------------------
1      192.168.1.11   00-1D-AA-0C-CD-08      3:43:46
>
```

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.

Example

```
> srv dhcp leasetime 1500
>
```

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. 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.
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.
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.

Example

```
Vigor> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 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.

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 dhcp option

This command can set the custom option for the DHCP server.

Syntax

srv dhcp option *-h*

srv dhcp option *-l*

srv dhcp option *-d <idx>*

srv dhcp option *-e <1 or 0> -i <lan number> -s <Next Server IP Address>*

srv dhcp option *-e <1 or 0> -i <lan number> -c <option number> -v <option value>*

srv dhcp option *-e <1 or 0> -i <lan number> -c <option number> -x <option value>*

srv dhcp option -*e <1 or 0> -i <lan number> -c <option number> -a <option value>*

srv dhcp option *-u <idx unmber>*

Syntax Description

Parameter	Description
-h	It means to display usage of this command.
-l	It means to display all the user defined DHCP options.
-d <idx>	It means to delete the option number by specifying its index number.
-e <1 or 0>	It means to enable/disable custom option feature. 1:enable 0:disable
-i <lan number>	<lan number> *:* It means to specify the LAN interface. 1: lan1 a: all LAN r: routed subnet
-s <Next Server IP Address>	It means to set the next server IP address. Next Server IP Address: Enter an IP address.
-c <option number>	It means to set option number. Available number ranges from 0 to 255. option number: Enter a number.
-v <option value>	It means to set option number by typing string. option value: Enter a string.
-x <option value>	It means to set option number with the format of Hexadecimal characters. option value: Enter a number (hex).
-a <option value>	It means to set the option value by specifying the IP address. option value: Enter an IP address.
-u <idx number>	It means to update the option value of the sepecified index. idx number: Enter the index number of the option value.
-r	Remove all the DHCP server options.

Example

```
> srv dhcp option -e 1 -i 1 -s 8.8.8.8
> srv dhcp option -l
% state   idx interface        opt type    data
% enable  1   ALL LAN          18  ASCII   /path
```

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 *[-<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.
n	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
m	It means the index number (1 to 8) of the DMZ host. Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 ~ 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
-e	It means to enable/disable such feature. 1:enable 0:disable
-i	It means to specify the private IP address of the DMZ host.
-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
> srv nat dmz -v
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP    Private IP
-----------------------------------------------------
   1    Disable 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 *[options]*

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
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
n	It means the index number for the profiles. The range is from 1 to 40.
m	It means to specify the sub-item number for this profile. The range is from 1 to 10.
-a <enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment>	It means to Enter the description (less than 23 characters) for the defined network service.
-I <source ip idx>	It means to set source IP object. 1 to 192: for IP object 1 to 32: for IP group 0: Any

	For example: srv nat openport 1 1 -l 1 -g 0
-g <source ip type>	It means to set IP type. 0: IP object 1: IP group For example: srv nat openport 1 1 -l 1 -g 0
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <widx><ipidx>	widx: Specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, …and so on. ipidx: Specify the index number of an alias IP (1 to 32).
-p <protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.
-s <start port>	It means to specify the starting port number of the service offered by the local host. The range is from 0 to 65535.
-e <end port>	It means to specify the ending port number of the service offered by the local host. The range is from 0 to 65535.
-v	It means to display current settings.
-r <remove>	It means to delete the specified open port setting. remove: Enter the index number of the profile.
-f <flush>	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.100 -w 1 -p TCP -s 23 -e 83
          Set WAN Port ok!!
> srv nat openport -v
%% Status: Enable
%% Comment: games
%% WAN Interface: WAN1
%% Private IP address: 192.168.1.55
Index   Protocal      Start Port     End Port
************************************************************
  1.    TCP           56             83
>
```

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 type> <src ip idx> <pri ip> <pri port> <wan idx> <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*

srv nat portmap *view*

Syntax Description

Parameter	Description
add <idx>	It means to add a new port redirection table with an index number. Available index number is from 1 to 40.
<serv name>	It means to type one name as service name.
<proto>	It means to specify TCP or UDP as the protocol.
<pub port>	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
<src ip type>	It means to specify the IP type (object or group). ip type: 0 means IP object; 1 means IP group.
<src ip idx>	It means to specify the index number of the object profile. ip idx: 1 to 192 for IP object profile; 1 to 32 for IP group profile. 0 means any object or group.
<pri ip>	It means to specify the private IP address of the internal host providing the service.
<pri port>	It means to specify the private port number of the service offered by the internal host.
<wan idx>	It means to specify WAN interface for the port redirection. Idx: wan1 to wan4, all
<alias IP>	It means to specify an alias IP by entering the index number (1 to 32). ip: 1 to 32.
del <idx>	It means to remove the selected port redirection setting.
disable <idx>	It means to inactivate the selected port redirection setting.
enable <idx>	It means to activate the selected port redirection setting.
flush	It means to clear all the port mapping settings.
table	It means to display Port Redirection Configuration Table.
view	It means to display the setting for the selected profile.

Example

```
> srv nat portmap add 1 floor tcp 1500 1 1 192.168.1.1 3000 wan1 1
> srv nat portmap table
```

```
NAT Port Redirection Configuration Table:

Index  Service Name    Protocol  Public Port  Private IP      Private Port ifno
 1     floor           TCP        1500   192.168.1.11        3000     -1
 2                     0          0                     0     -2
 3                     0          0                     0     -2
 4                     0          0                     0     -2
 5                     0          0                     0     -2
 6                     0          0                     0     -2
 7                     0          0                     0     -2
 8                     0          0                     0     -2
 9                     0          0                     0     -2
10                     0          0                     0     -2
11                     0          0                     0     -2
12                     0          0                     0     -2
13                     0          0                     0     -2
14                     0          0                     0     -2
15                     0          0                     0     -2
16                     0          0                     0     -2
17                     0          0                     0     -2
18                     0          0                     0     -2

19                     0          0                     0     -2

20                     0          0                     0     -2

....
```

Telnet Command: srv nat trigger

This command allows users to configure port triggering settings for NAT.

Syntax

srv nat trigger setdefault

srv nat trigger view

srv nat trigger *n [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
setdefault	Set to factory default settings.
view	Dispaly all of the port triggering settings.
n <command><parameter>|…]	"n" means the rule number. The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-c <XXX>	Type a comment for such rule if required.
-e <0/1>	Enable (1) or disable (0) a rule (specified with rule number).
-p <1/2/3>	Specify the protocol for such trigger rule. 1 – TCP 2 – UDP

	3 - All
-t	Specify the port number (0~65535) for trigger.
-P <1/2/3>	Specify the incoming protocol for such trigger rule. 1 – TCP 2 – UDP 3 - All
-i	Specify the port number (0~65535) for incoming protocol.
-d	Delete the selected trigger rule.
-v	Display the port trigger settings for specified rule.

Example

```
>  srv nat trigger 1 -c after_dinner
DrayTek> srv nat trigger 1 -v

Port Trigger Rule Index:1

Status:Disable
Comment:after_dinner
Triggering Protocol:
Triggering Port:
Incoming Protocol:
Incoming Port:

DrayTek>
```

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         1500   192.168.1.11           3000
 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
...
Protocol: 0 = Disable, 6 = TCP, 17 = UDP
>
```

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     0.0.0.0:1500             192.168.1.1:3000         Y

O01     TCP     0.0.0.0:56~83            192.168.1.55:56~83        Y

D01     All     0.0.0.0                   192.168.1.96            Y

R:Port Redirection, O:Open Ports, D:DMZ
```

Telnet Command: srv nat pseudoctl

This command allows users to check the pseudo port number to prevent from port conflict.

Syntax

srv nat pseudoctl *session <value>*

srv nat pseudoctl *function <0-3>*

Syntax Description

Parameter	Description
session <value>	Set the threshold of the session. <value>: o to 2147483647.
function <0-3>	0: It means "Auto". Check the created pseudo port number automatically when the session number is over the threshold. 1: It means "Not". Create a pseudo port number based on subnet setting. No verification. 2: It means "Must". Check the created pseudo port number if it is used by other client. 3: Create a pseudo port number. No verification.

Example

```
> srv nat pseudoctl function 2
 pesudo port: get hash pseudo port + subnet.
 pseudo port search: check pseudo port(Must).
```

```
> srv nat pseudoctl function 3
 pesudo port: get hash pseudo port.

> srv nat pseudoctl function 0
 pesudo port: get hash pseudo port + subnet.
 pseudo port search: check pseudo port(Auto).
```

Telnet Command: srv nat RSTTimeout

This command is used for forwarding RST out via TCP after a period of time.

Syntax

srv nat RSTTimeout <*value*>

Syntax Description

Parameter	Description
<*value*>	Set the timeout value. <value>: 0 to 10 (one unit is 10msec).

Example

```
> srv nat RSTTimeout 2
 Set timeout 2 unit

> %% srv RSTtimeout <value> (unit is 10msec). (0<=value<=10)
--------------------------
now timeout set 2 unit
>
```

Telnet Command: switch -i

This command is used to obtain the TX (transmitted) or RX (received) data for each connected switch.

Syntax

switch -i <*switch idx_no*> <*option*>

Syntax Description

Parameter	Description
<*switch idx_no*>	It means the index number of the switch profile.
option	The available commands with parameters are listed below. *cmd* *acc* *traffic* <*on/off/status/tx/rx*>
cmd	It means to send command to the client.
acc	It means to set the client authentication account and password.
traffic <*on/off/status/tx/rx*>	It means to turn on/off or display the data transmission from the client.

Example

```
>  switch -i 1 traffic on

External Device NO. 1 traffic statistic function is enable
```

Telnet Command: switch status

This command is used to check the status for the auto discovery of external devices.

Example

```
>  switch -i 1 traffic on

External Device auto discovery status : Enable

No Respond to External Device : Enable

Display External Device syslog  : Enable
```

Telnet Command: switch not_respond

This command is used to detect the external device automatically and display on this page.

Syntax

switch not_respond 0

switch not_respond 1

Syntax Description

Parameter	Description

0	Disable the option of "No Respond to External Device packets".
1	Enable the option of "No Respond to External Device packets".

Example

```
>  switch not_respond 1
slave not respond!
>
```

Telnet Command: switch on

This command is used to turn on the auto discovery for external devices.

Example

```
>  switch on
Enable Extrnal Device auto discovery!
```

Telnet Command: switch off

This command is used to turn off the auto discovery for external devices.

Example

```
>  switch off
Disable External Device auto discovery!
```

Telnet Command: switch list

This command is used to display the connection status of the switch.

Example

```
> switch list?
No.      Mac             IP         status   Dur Time   CWMP   ACS_CTL   Mod
el_Name   firmware_version
-------------------------------------------------------------------------------
------------------------------
[1]  00-1d-aa-0c-cd-08  192.168.1.11    On-Line   00:44:35    -1       -1
G2280
```

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

Syntax

switch clear *[idx]*

Syntax Description

Parameter	Description
idx	It means the index number of each item shown on the table. The range is from 1 to 8.
-f	It means to clear all of the data.

Example

```
> switch clear 1
Switch Data clear successful

> switch clear -f
Switch Data clear successful
```

Telnet Command: switch query

This command is used to enable or disable the switch query.

Example

```
> switch query on
Extern Device status query is Enable
> switch query off
Extern Device status query is Disable
```

Telnet Command: switch syslog

This command is used to enable or disable the external device syslog.

Example

```
> switch syslog on
Extern Device status is Enable
> switch syslog off
Extern Device status is Disable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account and specify LDAP server. The server will authenticate the local user who wants to access into the web user interface of Vigor router.

Syntax

sys adminuser *[option]*

sys adminuser edit *[index] username password*

Syntax Description

Parameter	Description
option	Available options includes: Local [0-1] LDAP [0-1] edit [INDEX] delete [INDEX] view [INDEX]
Local [0-1]	0 – Disable the local user. 1 – Enable the local user.
LDAP [0-1]	0 – Disable the LDAP. 1 – Enable the LDAP.
edit [INDEX] username password	Edit an existed user account or create a new local user account. [INDEX] – 1 ~8. There are eight profiles to be added / edited. Username – Type a new name for local user. Password – Type a password for local user.
delete [INDEX]	Delete a local user account.
view [INDEX]	Show the user account/password detail information.

Example

```
> sys adminuser Local 1
Local User has enabled!
> sys adminuser LDAP 1
LDAP has enabled!
> sys adminuser edit 1 carrie test123
Updated!
> sys adminuser view 1

Index:1
User Name:carrie
User Password:test123
```

Telnet Command: sys board

This command is used to disable/enable and configure the panel control.

Syntax

sys board button def <*on/off*>

sys board button wlan <*on/off*>

sys board led control <*on/off*>

sys board led sleepMode <*on/off*>

sys board led sleepMode time <*minute*>

sys board usb <*p1/p2*> <*on/off*>

Syntax Description

Parameter	Description

button def <on/off>	The default reset button will be invalid if turn it off. On - The button is valid. Off - The button is invalid.
Button wlan <on/off>	The wireless button will be invalid if turn it off. On - The button is valid. Off - The button is invalid.
led control <on/off>	All LEDs on the front panel will be invalid if turn it off. On - The LEDs are valid. Off - The LEDs are invalid.
led sleepMode <on/off>	All LEDs on the front panel will be set in sleep mode. On - The sleep mode is on. Off - The sleep mode is off. If the sleep mode is on, push the "wireless button" and the "factory reset button" to turn the LED on (even the buttons are disabled).
led sleepMode time [minutes]	After enableing the sleep mode for all LEDs, they will sleep after the minutes configured here. Minutes: Enter the number of the time.
usb <p1/p2> <on/off>	The USB port *<p1/p2>* will be invalid if turn it off. On - The port is valid. Off - The port is invalid.

Example

```
> sys board usb p2 off
 USB port2 power is off now.

> sys board usb p2 on
 USB port2 power is on now.
```

Telnet Command: sys bonjour

This command is used to disable/enable and configure the Bonjour service.

Syntax

sys bonjour *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-e <enable>	It is used to disable/enable bonjour service (0: disable, 1: enable).
-h <enable>	It is used to disable/enable http (web) service (0: disable, 1: enable).
-t <enable>	It is used to disable/enable telnet service (0: disable, 1: enable).
-f <enable>	It is used to disable/enable FTP service (0: disable, 1: enable).
-s <enable>	It is used to disable/enable SSH service (0: disable, 1: enable).
-p <enable>	It is used to disable/enable printer service (0: disable, 1: enable).
-6 <enable>	It is used to disable/enable IPv6 (0: disable, 1: enable).

Example

```
> sys bonjour -s 1
>
```

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: 4.0.0   Status: 1 (0x9df515cf)
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
   [1] sys board ?
   [2] sys board button ?
   [3] sys led ?
   [4] sys board led ?
   [5] sys board led sleepMode ?
   [6] sys board usb ?
   [7] sys board usb p2 off
   [8] sys board usb p2 on
   [9] sys ?
   [10] sys bonjour ?
   [11] sys cfg ?
   [12] sys cfg status
   [13] sys cmdlog ?
   [14] sys cmdlog
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
on	It means to turn on the FTP server of the system.
off	It means to 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*> <*Domain Name Suffix*>

sys domainname <*wan1*> *clear*

Syntax Description

Parameter	Description
<wan1>	It means to specify WAN interface for assigning a name for it.
<Domain Name Suffix>	It means the name for the domain of the system. The maximum number of characters that you can set is 39.
clear	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever

> DrayTek> sys domainname ?

% sys domainname <wan1> <Domain Name Suffix (max. 39 characters)>

% sys domainname <wan1> clear

% Now: wan1 == clever

>
```

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: 14-49-BC-0A-8A-B8
Interface 3 PPPoE:
Status: UP
IP Address: ---         Netmask: 0xFFFFFFFF
MAC: 14-49-BC-0A-8A-B9
Interface 4 Ethernet:
Status: UP
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 14-49-BC-0A-8A-BA
Interface 5 Ethernet:
Status: UP
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 14-49-BC-0A-8A-BB
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 14-49-BC-0A-8A-BD
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 14-49-BC-0A-8A-BE
--- 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*> <*ASCII string*>

sys name <*wan1*> *clear*

Syntax Description

Parameter	Description
<*wan1*>	It means to specify WAN interface for assigning a name for it.
ASCII string>	It means the name for router. The maximum character that you can set is 39.

Example

```
> sys name wan1 drayrouter

> sys name ?

% sys name <wan1/wan2> <ASCII string (max. 20 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*>

Syntax Description

Parameter	Description
old password	Enter the old password.
new password	Enter a string as the new password for administrator. The maximum character that you can set is 83.

Example

```
> sys passwd admin admin123
Password change successful !!!
```

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 cc

This command can display current country code and wireless region of this device.

Example

```
> sys cc
Country Code       : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor2135ac   Version: 4.2.1.2_STD English
Profile version: 4.0.0   Status: 1 (0x9df515cf)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Nov 25 2020 14:24:25
Router Name: DrayTek
Revision: 94071 V421
Router serial no: None
>
```

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#: 1647, cached#:   30
Buf KMC4088  (4088B), used#:    0, cached#:    8
Buf KMC2552  (2552B), used#: 1641, cached#:   42
Buf KMC1016  (1016B), used#:    7, cached#:    1
Buf KMC504   ( 504B), used#:    8, cached#:    8
Buf KMC248   ( 248B), used#:   26, cached#:   22
Buf KMC120   ( 120B), used#:   67, cached#:   61
Buf KMC56    (  56B), used#:   20, cached#:   44
Buf KMC24    (  24B), used#:   58, cached#:   70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2 cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# 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	It means to turn on pulling buffer.
off	It means to 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	It means to turn on the bridge task for improving the triple play quality.
off	It means to 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 <*parm*> <*option*>

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 inform <*event code*>

sys tr069 port <*port num*>

sys tr069 cert_auth<*on/off*>

sys tr069 only_standard_parm <*on/off*>

sys tr069 notify -S

sys tr069 notify -n <*on/off*>

sys tr069 notify -l <*on/off*>

sys tr069 notify -c <*on/off*>

sys tr069 notify -b <*on/off*>

sys tr069 notify -B *"<WAN number> <Medium threthold> <High threthold> <TX Speed>Mb <RX Speed>Mb"*

Syntax Description

Parameter	Description
get <parm> <option>	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
set <parm> <value>	It means to set parameters for tr-069.
getnoti <parm>	It means to get parameter notification value.

setnoti <parm> <value>	It means to set parameter notification value.
log	It means to display the TR-069 log.
debug <on/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] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC", 3-"3 SCHEDULED", 4-"4 VALUE CHANGE", 5-"5 KICKED", 6-"6 CONNECTION REQUEST", 7-"7 TRANSFER COMPLETE", 8-"8 DIAGNOSTICS COMPLETE", 9-"M Reboot"
port <port num>	It means to change tr069 listen port number.
cert_auth <on/off>	on: turn on certificate-based authentication. off: turn off certificate-based authentication.
only_standard_parm <on/off>	It means to turn on or off to exclude all the Vendor-Specific ("X_") parameters, and only send out standard parameters.
notify -n <on/off>	It means to set CPE notification settings. It means to / not to record the CPE notify log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
notify -l <on/off>	It means to / not to record the web login log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
notify -c <on/off>	It means to / not to record the web changed log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
notify -b <on/off>	It means to / not to record the bandwidth utilization log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
notify -B "<WAN number> <Medium threthold> <High threthold> <TX Speed>Mb <RX Speed>Mb"	It means to set bandwidth utilization setting. <WAN number>: Enter the index number of WAN interface(s). <Medium threthold>: Enter a value. <High threthold>: Enter a value. <TX Speed>Mb: Enter a value. <RX Speed>Mb: Enter a value.
-S	Show the CPE notification settings.

Example

```
> sys tr069 get InternetGatewayDevice.ManagementServer.
Total number of parameter is 49
Total content length of parameter is 3196
```

```
InternetGatewayDevice.ManagementServer.URL=
InternetGatewayDevice.ManagementServer.Username=
InternetGatewayDevice.ManagementServer.Password=
InternetGatewayDevice.ManagementServer.PeriodicInformEnable= 0
InternetGatewayDevice.ManagementServer.PeriodicInformInterval= 900
InternetGatewayDevice.ManagementServer.PeriodicInformTime=
1970-01-01T00:00:00
InternetGatewayDevice.ManagementServer.ParameterKey=
InternetGatewayDevice.ManagementServer.ConnectionRequestURL=
InternetGatewayDevice.ManagementServer.ConnectionRequestUsername= vigor
InternetGatewayDevice.ManagementServer.ConnectionRequestPassword=
InternetGatewayDevice.ManagementServer.UpgradesManaged= 0
InternetGatewayDevice.ManagementServer.UDPConnectionRequestAddress=
InternetGatewayDevice.ManagementServer.UDPConnectionRequestAddressNotific
ation-L
imit= 0
InternetGatewayDevice.ManagementServer.STUNEnable= 0
InternetGatewayDevice.ManagementServer.STUNServerAddress=
InternetGatewayDevice.ManagementServer.STUNServerPort= 3478
InternetGatewayDevice.ManagementServer.STUNUsername=
InternetGatewayDevice.ManagementServer.STUNPassword=
InternetGatewayDevice.ManagementServer.STUNMaximumKeepAlivePeriod= -1
InternetGatewayDevice.ManagementServer.STUNMinimumKeepAlivePeriod= 60
InternetGatewayDevice.ManagementServer.NATDetected= 0
InternetGatewayDevice.ManagementServer.ManageableDeviceNumberOfEntries= 0
InternetGatewayDevice.ManagementServer.CPEEnable= 0
InternetGatewayDevice.ManagementServer.ApplyApEnable= 0
InternetGatewayDevice.ManagementServer.ApplyApPassword=
InternetGatewayDevice.ManagementServer.BWUNEnable= 0
InternetGatewayDevice.ManagementServer.BWUNPeriodic= 3
InternetGatewayDevice.ManagementServer.BWUNWANNumberOfEntries= 2
InternetGatewayDevice.ManagementServer.BWUNWAN.1.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.1.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.1.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.1.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.1.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.2.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.2.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.2.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.2.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.2.RX= 0
InternetGatewayDevice.ManagementServer.HWAcceler.Enable= 1
InternetGatewayDevice.ManagementServer.HttpsTriggerEnable= 0
InternetGatewayDevice.ManagementServer.ApplyApSTUNEnable= 0
InternetGatewayDevice.ManagementServer.ApSTUNEnable= 0
InternetGatewayDevice.ManagementServer.ApSTUNServerAddress=
InternetGatewayDevice.ManagementServer.ApSTUNServerPort= 3478
InternetGatewayDevice.ManagementServer.ApSTUNMaximumKeepAlivePeriod= -1
InternetGatewayDevice.ManagementServer.ApSTUNMinimumKeepAlivePeriod= 60
InternetGatewayDevice.ManagementServer.AcquireURLEnable= 0
InternetGatewayDevice.ManagementServer.CPEPort= 8069
InternetGatewayDevice.ManagementServer.CPEClear=
> sys tr069 notify -B "1 30 60 100 100"
Please enable the CPE notify log.
```

```
> sys tr069 notify -b on
Please enable the CPE notify log.
> sys tr069 notify -n on
> sys tr069 notify -B "1 30 60 100 100"
Please enable the bandwidth utilization notify log.
> sys tr069 notify -b on
set OK
> sys tr069 notify -B "1 30 60 100 100"
> sys tr069 notify -S
CPE Notify Settings:
 CPE Notify           Enable
 -Web Login           Disable
 -Web Changed         Disable
 -Bandwidth Utilization Enable
      Threshold(
  WAN1 Med: 30 High: 60 TX:  100 RX:  100
  WAN2 Med:  0 High:  0 TX:    0 RX:    0
  WAN3 Med:  0 High:  0 TX:    0 RX:    0
>
```

Telnet Command: sys alg

This command can enable or disable ALG (Application Layer Gateway) master switch.

Syntax

sys alg <*1/0*>

Syntax Description

Parameter	Description
1	It means to enable ALG master switch.
0	It means to disable ALG master switch.

Example

```
> sys alg -e 1
 Enable ALG

> sys alg
Usage: sys alg <command> <parameter>
 -e: enable ALG (0:disable, 1:enable)

Current ALG status
 -ALG Master Switch: Enabled
```

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

Syntax

sys sip_alg *[<command> <parameter>|…]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-e <0/1>	0: Disable the function of SIP ALG. 1: Enable the function of SIP ALG.
-p <parameter>	It means to set the listening port for SIP ALG. <parameter> : Ranges from 1 to 65535.
-u	It means to enable or disable the listen along UDP path setting. 0: Disable 1: Enable
-t	It means to enable or disable the listen along TCP path setting. 0: Disable 1: Enable

Example

```
> sys sip_alg -e 1
 Enable SIP ALG

> sys sip_alg -p 65535
 Current listening port: 65535

DrayTek> sys sip_alg ?
Usage: sys sip_alg <command> <parameter>
 -e: enable SIP ALG (0:disable, 1:enable)
 -p: set your listening port for SIP ALG
 -u: enable listen along UDP path (0:disable, 1:enable)
 -t: enable listen along TCP path (0:disable, 1:enable)

Current SIP ALG status
 -ALG Master Switch: Enabled
 -SIP ALG: Enabled
 -Listen along UDP path: Yes
 -Listen along TCP path: Yes
 -Listening Port: 65535
 -Max sipalg session num: 256
 -Remain sipalg session num: 256
```

Telnet Command: sys rtsp_alg

This command can turn on/off RTSP ALG (Application Layer Gateway) for traversal.

Syntax

sys rtsp_alg *[<command> <parameter>|…]*

Syntax Description

Parameter	Description
[<command>	The available commands with parameters are listed below.

<parameter>|…]	*[…]* means that you can type in several commands in one line.
-e <0/1>	0: Disable the function of RTSP ALG. 1: Enable the function of RTSP ALG.
-p <parameter>	It means to set the listening port for RTSP ALG. <parameter> : Ranges from 1 to 65535.
-u	It means to enable or disable the listen along UDP path setting. 0: Disable 1: Enable
-t	It means to enable or disable the listen along TCP path setting. 0: Disable 1: Enable
-v	It displays RTP and RTCP portmap information of RTSP ALG.

Example

```
> sys rtsp_alg -e 1
 Enable RTSP ALG

> sys rtsp_alg -p 60000
 Current listening RTSP Port: 60000

> sys rtsp_alg -v
 Current Open PortMap Number of RTSP ALG: 0

> 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: 60000
 -Max RTSP session num: 256
 -Remain RTSP session num: 256
```

Telnet Command: sys license

This command can process the system license.

Syntax

sys license *reset_regser*

sys license *licera*

sys license *licifno <AUTO/WAN#>*

sys license *licalias <index>*

sys license *lic_trigger*

sys license *licelog*

Syntax Description

Parameter	Description
reset_regser	It means the license register server setting. or register service in portal??
licera	It means to erase license setting.
licifno <AUTO/WAN#>	It means license and signature download interface setting.
licalias <index>	It means to specify an IP alias by entering the index number of the IP alias profile.
lic_trigger	It means to trigger the license.
licelog	It means to show the authentication log.

Example

```
> sys license licifno wan1

Download interface is set as "WAN1" now.
```

Telnet Command: sys diag_log

This command is used for RD debug.

Syntax

sys diag_log <*status*| *enable*| *disable*| *flush*| *lineno* <*w*> | *level* <*x*> | *feature* <*on*|*off*><*y*>| *voip_feature* <*on*|*off*> <*vf_name*>| *log*>

Syntax Description

Parameter	Description
status	It means to show the status of diagnostic log.
enable	It means to enable the function of diag_log.
disable	It means to disenable the function of diag_log.
flush	It means the flush log buffer.
lineno <*w*>	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
level <*x*>	It determines the level of data displayed. x – Available value ranges from 0 to 12. The larger the number is, the detailed the data is displayed.
feature <*on*|*off*> <*y*>	It is used to specify the function of the log. Supported features include SYS and DSL (Case-Insensitive). Default setting is “on” for “DSL”.
voip_feature <*on*|*off*> <*vf_name*>	It means VoIP feature. Type on to enable the feature or type off to disable the feature. vf_name: available settings include DRVTAPI, DRVVMMC, DRVMPS, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN, DTMFPSER, CALLERID (Case-Insensitive).
log	It means the dump log buffer.

Example

```
> sys diag_log status
 Status:
 diag_log is Enabled.
 lineno : 10000.
 level : 3.
 Enabled feature: SYS DSL
> sys diag_log log
0:00:02   [DSL] Current modem firmware: AnnexA_548006_544401
0:00:02   [DSL] Modem firmware feature: 5, ADSL_A, VDSL2
0:00:02   [DSL] xtseCfg=04 00 04 00 0c 01 00 07
0:00:02   [DSL] don't have last showtime mode!! set next mode to VDSL!!
0:00:02   [DSL] Status has changed: Stopped(0) -> FwWait(3)
0:00:02   [DSL] Status has changed: FwWait(3) -> Starting(1)
0:00:02   [DSL] Status has changed: Starting(1) -> Running(2)
0:00:02   [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:02   [DSL] Status was switched: Init(5) to Restart(10)
0:00:02   [DSL] Status was switched: Restart(10) to FirmwareRequest(1)
0:00:02   [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02   [DSL] Entering VDSL2 mode
0:00:03   [DSL] modem code: [05-04-08-00-00-06]
0:00:05   [DSL] Status was switched: FirmwareRequest(1) to firmwareReady(3)
```

```
0:00:05    [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:05    [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05    [DSL] >> nHsToneGroupMode=0, nHsToneGroup=106, nToneSet=43,
nCamState
=2
0:00:05    [DSL] Line state has changed: 000000FF -> 00000100
0:00:05    [DSL] Line state has changed: 00000100 -> 00000200
0:00:05    [DSL] Status was switched: Init(5) to Train(6)
```

Telnet Command: sys arp_AutoReq

This command is used to enable / disable the function that Vigor router sends ARP request to the connected device(s) periodically.

Syntax

sys arp_AutoReq -d <*value*>

Syntax Description

Parameter	Description
-d [value]	Disable the function of ARP auto request. 0 – Enable 1 – Disable

Example

```
> sys arp_AutoReq -d 1
  Arp auto-request disable.
```

Telnet Command: sys daylightsave

This command is used to conifgure day light saving.

Syntax

sys daylightsave *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
[<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-v	Display the daylight saving settings.
-r	Set to factory default setting.
-e [1/0]	Enable (1) / disable (0) daylight saving.
-t [0/1/2]	Specify the saving type for daylight setting. 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 – must be the year after 2013. month - 1 ~ 12 day – 1 ~ 31 hour – 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 – After 2013. month - 1 ~ 12 day – 1 ~ 31 hour – 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 - 1 ~ 12 th weekday – 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour – 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 - 1 ~ 12 th weekday – 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour – 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 type in several commands in one line.
-l	It means to show DNS IPv4 entry in DNS cache table.
-s	It means to show DNS IPv6 entry in DNS cache table.
-v	It means to show TTL limit value in DNS cache table.
-t <ttl>	It means to set TTL limit value. <ttl>: 0(no limit) or an number greater than 5.
-c	It means to clear the DNS cache table.

Example

```
> sys daylightsave -y 9 1 0 14
% Start: Yearly on Sep 1th Sun 14:00
DrayTek> sys dnsCacheTbl -t 50
% Set TTL limit: 50 seconds.
% When TTL larger than 50s , delete the DNS entry in the router's DNS cache
tabl
```

```
e.
> sys dnsCacheTbl -v
% TTL limit: 50 seconds
% When TTL larger than 50s , delete the DNS entry in the router's DNS cache
tabl
>
```

Telnet Command: sys syslog

This command is used to conifgure day light saving.

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 type in several commands in one line.
-a <1/0>	Enable (1) or disable (0) Syslog Access Setup.
-s <1/0>	Enable (1) or disable (0) Syslog Save to Syslog Server.
-i <IP address>	Define the IP address of the Syslog server.
-d <port number>	Define the port number (1 ~ 65535) as the destination port.
-u <1/0>	Enable (1) or disable (0) Syslog Save to USB Disk.
-m <1/0>	Enable (1) or disable (0) Mail Syslog.
-f <1/0>	Enable (1) or disable (0) Filewall Log.
-v <1/0>	Enable (1) or disable (0) VPN Log.
-e <1/0>	Enable (1) or disable (0) User Access Log.
-c <1/0>	Enable (1) or disable (0) Call Log.
-w <1/0>	Enable (1) or disable (0) WAN Log.
-r <1/0>	Enable (1) or disable (0) Router/DSL Information.
-t <1/0>	Enable (1) or disable (0) AlertLog Setup.
-o <port number>	Define the port number (1 ~ 65535) for AlertLog.

Example

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
>
```

Telnet Command: sys mailalert

This command is used to configure settings for syslog mail alert.

Syntax

sys mailalert *[-<command> <parameter>]*

Syntax Description

Parameter	Description
[<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.

-e <0/1>	Enable/disable Mail Alert. 0 – Disable. 1 – Enable.
-w <0/1/2/...>	Set Interface (Physical) Any/WAN1/WAN2/WAN... and etc.
-x <WAN IP Alias index>	Set WAN IP Alias. Index 1 is reserved and must set an interface first.
-i <SMTP Server IP>	Set IP Address for SMTP server.
-o <SMTP Server Port>	Set port number for SMTP server..
-a <Mail Address>	Set E-maiil address for alert mail reciver.
-r <Mail Address>	Set E-mail Address for mail return.
-s <0/1>	Enable/disable the function of Use SSL. 0 – Disable. 1 – Enable.
-h <0/1>	Enable/disable SMTP Authentication. 0 – Disable. 1 – Enable.
-u <Username>	Set username for SMTP Authentication.
-p <Password>	Set password for SMTP Authentication.
-l <type><0/1>	Enable / disable mail alert for different types. Number 0 ~ 6 represent different types. "0 <0/1>" : Enable/Disable Mail Alert of the DoS Attack. "1 <0/1>" : Enable/Disable Mail Alert of the APPE. "2 <0/1>" : nable/Disable Mail Alert of the VPN Log. "3 <0/1>" : Enable/Disable Mail Alert of the APPE Signature. "6 <0/1>" : Enable/Disable Mail Alert of the Reboot Debug Log. In which, 0 – Disable. 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: Limited Mode 1: Unlimited Mode.

Example

```
> sys mailalert -e 1
Set Enable Mail Alert.
> sys mailalert -v
------ Current setting for Mail Alert ------
Mail Alert: Enable
SMTP Server IP Address: 0.0.0.0
SMTP Server Port: 25
Alert Mail Reciver E-maiil Address:
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 APPE Signature: Disable.
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 zone <*index*>

Syntax Description

Parameter	Description
domain	Enter the domain name of the time server. The maximum length is 39 characters.
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 01 Sat 21:28:36]
  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 / hide items (such as System Information, Interface…) on dashboard.

Syntax

sys dashboard *[-<command> <value> | …]*

sys dashboard show

Syntax Description

Parameter	Description

[<command> <value>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several parameters in one line. <command> "0 ~ 9" and "a" represent different sections to be displayed on the dashboard. 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> 1 : Enable 0 : Disable
show	Display current status (enabled /disabled) for each item.

Example

```
> sys dashboard -0 1
  Front Panel enabled
> sys dashboard show
  Front Panel enabled
  System Information enabled
  IPv4 LAN Information enabled
  IPv4 Internet Access enabled
  IPv6 Internet Access enabled
  Interface enabled
  Security enabled
  System Resource enabled
  LTE Status enabled
  Quick Access enabled
  VoIP enabled
>
```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
 Mail Alert:[Enable]
 Interface :Any
 WAN_Alias index:[0]
 SMTP_Server:[0.0.0.0]
 SMTP_Port:[25]
 Mail to:[]
 Return-Path:[]
 Connection Security:[Plaintext]
```

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 >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >>(null)<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
<NULL>

((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<<
<NULL>

((2))
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<<
<NULL>

--- 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:f6c9fedc-6c5d-41f4-992e-1449bc0a8ab8

>>>>> 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:6cdf7eae-9a99-40d9-8f53-83d97e143364

>>>>> SERVICE TABLE3 <<<<<
  serviceType urn:schemas-upnp-org:service:WANPOTSLinkConfig:1
  serviceId   urn:upnp-org:serviceId:WANPOTSLinkC1
  SCPDURL     /upnp/WANPOTSL.xml
  controlURL  /upnp?control=WANPOTSLinkC1
  eventURL
  UDN        uuid:2b84726d-d351-43ab-b96a-f601ff9818b3.
...
```

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 (0 to 3) to apply UPnP. n=0, it means to auto-select WAN interface. n=1, WAN1 n=2, WAN2 …….

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is use to display the information about the brand name and model name of the USB modems which are supported by Vigor router.

Example

```
> usb list ?
Brand        Module                Standard
-----------------------            --------
4G system    XSPlug P3             3.5G             Y
Aiko         Aiko 76E              3.5G             Y
Alcatel      Alcatel X500          3.5G             Y
Alfa         ALFA Flyppp           3.5G             Y
Amoi         Amoi H01              3.5G             Y
BandRich     Bandluxe C321         3.5G             Y
BandRich     Bandluxe C330         3.5G             Y
BandRich     Bandluxe C331         3.5G             Y
BandRich     Bandluxe C502         3.5G             Y
BigPond      BigPond Next G Wir    3.5G             Y
BigPond      Broadband USB Mobi    3.5G             Y
Huawei       Huawei E150           3.5G             Y
Huawei       Huawei E153           3.5G             Y
Huawei       Huawei E172           3.5G             Y
Huawei       Huawei E176c          3.5G             M
Huawei       Huawei E270           3.5G             Y
Huawei       Huawei E3131          3.5G             Y
Huawei       Huawei E3272          3.5G             Y
Huawei       Huawei E3276s         LTE              Y
Huawei       Huawei E367           3.5G             Y
Huawei       Huawei E398           LTE              Y
Huawei       Huawei EC228          3.5G             Y
Huawei       Huawei K4505          3.5G             M
Huawei       Huawei K4511          3.5G             Y
MOMODESIGN   MD-@                  3.5G             Y
QP           QP QLD310             LTE              Y
Royal        Royal R220            3.5G             Y
Sierra       Sierra 308            3.5G             Y
Telstra      Telstra TurBO / Ne    3.5G             Y
TP-LINK      TP-LINK MA180         3.5G             Y
TP-LINK      TP-LINK MA260         3.5G             Y
Vodafone     Vodafone K3520-Z      3.5G             Y
XS Stick     XS Stick W12          3.5G             Y
ZadaCOM      ZadaCOM ppp+ 7.2      3.5G             Y
ZTE          ZTE MF627 plus        3.5G             Y
ZTE          ZTE MF636             3.5G             Y
ZTE          ZTE MF636DB           3.5G             Y
ZTE          ZTE MF637             3.5G             Y
Alcatel      Alcatel L100V         LTE              Y
Alcatel      Alcatel L800          LTE              Y
Alcatel      Alcatel W800          LTE              Y
Alcatel      Alcatel Y855          LTE              Y
D-Link       D_LINK DWM156         3.5G             M
Huawei       Huawei E303           3.5G             M
```

```
Huawei        Huawei E3131          3.5G              Y
Huawei        Huawei E3272          LTE               Y
Huawei        Huawei E3276s         LTE               Y
Huawei        Huawei E3372          LTE               Y
Huawei        Huawei E3531          3.5G              Y
Huawei        Huawei E392           LTE               Y
Huawei        Huawei E398           LTE               Y
LG            LG VL600              LTE               Y
Novatel Wi    Novatel 551L          LTE               Y
Novatel Wi    Novatel UML290VW      LTE               M
Samsung       Samsung GT-B3730      LTE               M
Vodafone      Vodafone K4201        3.5G              M
Vodafone      Vodafone K4203        3.5G              M
Vodafone      Vodafone K5150        LTE               Y
Vodafone      Vodafone K5160        LTE               Y
ZTE           ZTE  MF823           LTE               Y
ZTE           ZTE D6601S            3.5G              Y
ZTE           ZTE MF667             3.5G              M
ZTE           ZTE MF820D            LTE               M
ZTE           ZTE MF821D            LTE               Y
ZTE           ZTE MF880D            LTE               Y
Samsung       swc-u200              WiMAX             M

------------------------

Y: tested and is supported.
M: has not been tested but might be supported.

total 66 records
```

Telnet Command: usb user

This command is used to set profiles for FTP/SMB users.

Syntax Description

usb user add <*Index*> <*Username*> <*Password*> <*Permission*> <*Home path*>

usb user rm <*Index*>

usb user enable <*Index*>

usb user disable <*Index*>

usb user list

Syntax Description

Parameter	Description
add <*Index*> <*Username*> <*Password*> <*Permission*> <*Home path*>	Add a new user profile. <Index>: It means the index number of the user profile. There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16. <Username>: Enter a text (maximum 131 characters) as the username for the user profile. <Password>: Enter a text (maximum 131 characters) as the password for the user profile. <Permission>: Specify the action (RWDLCR) permitted. If one of the actions is not allowed, simple type "-" instead.

	R – Read File. W – Write File. D – Delete File. L – List directory. C – Create directory. R – Remove selected directory. <Home path>: Set the path (maximum 159 characters) for the USB user profile.
rm <Index>	Delete an existed user profile. <Index>: It means the index number of the user profile.
enable <Index>	Enable a user profile. <Index>: It means the index number of the user profile.
disable <Index>	Disable a user profile. <Index>: It means the index number of the user profile.
list	Display all of the user profile.

Example

```
> usb user add 1 root 1234 R-DLCR /usr
> No usb storage is available!!
```

Telnet Command: usb temp

This command is to configure USB temperature.

Syntax Description

usb temp set <*-c*|*-f*|*-a*|*-b*|*-m*|*-u*|*-l*|*-r*>

usb temp show

usb temp all_data

Syntax Description

Parameter	Description
set -c	Set the temperature unit (Celsius).
set -f	Set the temperature unit (Fahrenheit).
set -a	Set the temperature sensor by using a probe or the built-in sensor automatically. The probe will be detected and used first, and fall back to the built-in sensor if the probe is not detected.
set -b	Set to use the built-in sensor.
set -m	Enable or disable the Alarm Setting. 1: Enable 0: Disable
set -u <value>	Set the upper temperature limit. <value>: Enter a value, e.g., 30.35.
set -l <value>	Set the lower temperature limit. <value>: Enter a value, e.g., 10.35.
set -r	Shows the setting of temperature unit and sensor type.
show	Displays current temperature.

all_data	Displays all temperature data.

Example

```
> usb temp set -r
Show setting:temp set -r

Alarm Settings: 0 (0:Disable, 1: Enable.)
upper temperature limit: 30.0 C
lower temperature limit: 18.0 C
unit: 0 (0:Celsius, 1: Fahrenheit.)
sensor: 0 (0:Auto select, 1: built-in.)
```

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>	Indicate the IP version for the IP address. 4 – IPv4. 6 – IPv6.
-w <WAN_idx>	WAN_idx – Indicate the WAN interface. 1 – WAN1 2 – WAN2 3 – WAN3 4 – WAN4 5 - WAN5
-l <LAN_idx>	LAN_idx – Indicate the LAN interface. 1 – LAN1 2 – LAN2 3 – LAN3 4 – LAN4 5 - LAN5 6 - LAN6 …. 15 - LAN15
e <0/1>	Enable (1) or disable (0) the Vigor Bridge for WAN or/and LAN.
f <0/1>	Enable (1) or disable (0) the firewall functions.

Example

```
> vigbrg set -v 4 -w 3 -l 1 -e 1

[WAN3] IPv4 bridge is enable. Set subnet[LAN1]
```

Telnet Command: vigbrg closeall

This command can disable vigor bridge function.

Example

```
> vigbrg closeall
Close all bridge and bridge firewall

[WAN3] 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
```

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.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wanstatus

This command can display the existed WAN connection status for the modem (change from ADSL router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function..

Example

```
> vigbrg wanstatus
Vigor Bridge: Stop
WAN mac table:
Index   MAC Address           Stamp Time     PVC    VLan Port
```

Telnet Command: vigbrg wlanstatus

This command can display the existed WLAN connection status for the modem (change from router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wlanstatus
Vigor Bridge: Stop
WAN mac table:
Index   MAC Address           Stamp Time     PVC    VLan Port
```

Telnet Command: fullbrg

The command is used to enable Full Bridge Mode so that the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.

Syntax

fullbrg status

fullbrg set -i <*WAN index*> **-n** <*Subnet index*> **-b** <*Bridge mode*>

Syntax Description

Parameter	Description
-i <WAN index>	At present, only WAN1 is available. <WAN index>: 1.
-n <Subnet index>	Subnet index: Ranges from 1 to 8. 1: Subnet 1, 2: Subnet 2, ...etc.
-b <Bridge mode>	It means to enable / disable Bridge mode. 0: OFF 1: ON

Example

```
> fullbrg status
Show gConfig setting of full bridge
WAN 1 full bridge to LAN 1, mode=OFF.
> fullbrg set -i 1 -n 2 -b 1
Configure OK! Please reboot device to make it effective.
>
```

Telnet Command: voip debug

This command can display debug message on the screen.

Syntax

voip debug *[flush]*

voip debug *[showmsg]*

Syntax Description

Parameter	Description
flush	It means to clear current log.
showmsg	It means to show current log.

Example

```
> voip debug showmsg
-->Send Message to 192.168.1.2:5060 <02:35:16>
INVITE sip:192.168.1.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.1:5060;branch=z9hG4bK-YMa-3630;rport
From:  <sip:change_me@192.168.1.1>;tag=WLJ-11782
To: <sip:192.168.1.2>
Call-ID: PbU-25312@192.168.1.1
CSeq: 1 INVITE
Contact: <sip:change_me@192.168.1.1>
Max-Forwards: 70
supported: 100rel, replaces
User-Agent: DrayTek UA-1.2.3 DrayTek Vigor2910
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, REFER, NOTIFY, PRACK
Content-Type: application/sdp
Content-Length:   264

v=0
o=change_me 5972727 56415 IN IP4 192.168.1.1
```

Telnet Command: voip dialplan

This command allows users to set phone book settings.

Syntax

voip dialplan block *n [-<command><parameter>]*

voip dialplan phonebook *n [-<command><parameter>]*

voip dialplan region *[-<command><parameter>]*

voip dialplan local *[1/0]*

Syntax Description

Parameter	Description
voip dialplan block	
n	It means the index number of the VoIP settings. n=1 ~ 20
-<command><parameter>	The available commands with parameters are listed below.

-m 0/1	It means to enable or disable the block mode. 0 – Disable 1 - Enable
-p <path>	Determines the block path. 1:in_url, 2:in_number 3:out_url, 4:out_number 5:(in & out)_url, 6:(in & out)_number))
-n <number>	Determines the block number (maximum 29 characters).
-d <domain>	Block the specified domain.
-i <inf>	Block the specified interface(s) or All interfaces.
-s <Schedule>	Specify schedule profiles by indicating the index number of the schedule profile. Four schedule profiles can be used at one time.
-w	Delete the selected entry. N=null (clear all)
-v	List current settings.
voip dialplan phonebook	
n	It means the index number of the VoIP settings. n=1 ~ 60
-<command><parameter>	The available commands with parameters are listed below.
-d <number>	Specify the speed dial number.
-c <url>	Contact SIP URL l(max. 59 characters)
-n <name>	Contact name (max. 23 characters)
-a <enable>	Enable/disable the specify entry.
-m <mode>	Specify backup number mode. 0 – none 2 - PSTN
-b <number>	Spedify the backup number.
-o <acc num>	Specify the dial out account. 0 – default 1 - acc1, 2 - acc2... ~ 12:=acc12
-z <enable>	Enable/disable ZRTP/SRTP VoIP security. 1 – enable 0 - disable
-l	Delete the specify entry.
-V	List current VoIP settings.
voip dialplan region	
-e	Dnable or disable the regional function. 1 – enable 0 - disable
-m <number>	Return the last miss call.
-l <number>	Return the last incoming call.
-o <number>	Return the last outgoing call.
-F <number>	Hotkey to enable call forwarding (all) function.

-f <number>	Hotkey to enable call forwarding (busy) function.
-C <number>	Hotkey to enable call forwarding (no answer) function.
-c <number>	Hotkey to disable call forwarding function.
-W <number>	Hotkey to enable call waiting function.
-w <number>	Hotkey to disable call waiting function.
-H <number>	Hotkey to enable hide caller ID function.
-h <number>	Hotkey to disable hide caller ID function.
-D <number>	Hotkey to enable DND function.
-d <number>	Hotkey to disable DND function.
-A <number>	Hotkey to enable block anonymous calls function.
-a <number>	Hotkey to disable block anonymous calls function.
-U <number>	Hotkey to enable block unknow domain calls function.
-u <number>	Hotkey to disable block unknow domain calls function.
-P <number>	Hotkey to disable block IP calls function.
-p <number>	Hotkey to disable block IP calls function.
-l <number>	Hotkey to block last incoming call.
-v	List current status for Regional settings.
voip dialplan local	
enable/disable	Enable or disable the local calls. 1 – enable 0 - disable

Example

```
> voip dialplan phonebook 1 -d 1125
> voip dialplan region -l 8
> voip dialplan region -v
 Your Setting for Regional
 Regional Function is: Enable
 Return the Last Miss Call: 20
 Return the Last Incoming Call: *12
 Return the Last Outgoing Call: 1
 Hotkey to enable call forwarding (all) function: 0
 Hotkey to enable call forwarding (busy) function: *90
 Hotkey to enable call forwarding (no answer) function: *92
 Hotkey to disable call forwarding function: 12
 Hotkey to Enable Call Waiting Function: *56
 Hotkey to Disable Call Waiting Function: *57
 Hotkey to Enable Hide Caller ID Function: *67
 Hotkey to Disable Hide Caller ID Function: *68
 Hotkey to Enable DND Function: *78
 Hotkey to Disable DND Function: *79
 Hotkey to Enable Block Anonymous Calls Function: *77
 Hotkey to Disable Block Anonymous Calls Function: *87
 Hotkey to Enable Block Unknow Domain Calls Function: *40
 Hotkey to Disable Block Unknow Domain Calls Function: *04
 Hotkey to Enable Block IP Calls Function: *50
 Hotkey to Disable Block IP Calls Function: *05
```

```
Hotkey to Disable Block The Last Incoming Call Function: 8
```

Telnet Command: voip dsp

Syntax

voip dsp countrytone *[channel] [value]*

voip dsp dialtonepwr *[channel] [AbsoluteValue]*

voip dsp EchoCanceller *[type] [w_size] [nlp]*

voip dsp cidtype *[channel] [value]*

voip dsp micgain *[channel] [value/(1~10)]*

voip dsp spkgain *[channel] [value/(1~10)]*

voip dsp jitterBuffer *[port] [mode] [value]*

voip dsp dtmfDetset *[nLevel] [nTwist]*

voip dsp dtmftonepwr *[Level]*

voip dsp cwtonepwr *[ch] [value]*

voip dsp pstnringfxs *[1|2] [on|off]*

voip dsp relaydbounce *[on|off]*

voip dsp setRingPat *[ring_pattern_index] [patten_num]*

voip dsp setDtmfCidlevel –l [value]

voip dsp setDtmfCidlevel –h [value]

voip dsp setDtmfCidlevel –r 0

voip dsp cidplusdigit [1/0] [channel] [value]

Syntax Description

Parameter	Description
voip dsp countrytone	
[channel] [value]	This command allows users to set the region for the tone settings. Different regions usually need different tone settings. Channel – 1 or 2. Value – displayed as follows: [2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany, [7] Netherlands, [8] Portugal, [9] Sweden, [10] Australia, [11] Slovenia, [12] Czech, [13] Slovakia, [14] Hungary, [15] Switzerland , [16] France , [17] Malta
voip dsp dialtonepwr	
channel	This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting. Channel - Available channel number: 1 – 2
AbsoluteValue	AbsoluteValue - In -1 dB increments, with 1 corresponding to 6 dBm. Range - 1 to 30
voip dsp EchoCanceler	
type	This command is used to set the type of echo reduction. 0 - Disable the LEC processing.

	1 - Cancel using the fixed window. 2 - Cancel using the fixed and moving window. 3 - Cancel using fixed window + Echo Suppressor.
w_size	The Line Echo Canceller (LEC) window size is 4, 6, 8 or 16 (ms).
nlp	Nlp - Non-linear processing (NLP) for more smooth transitions. 1 - disable 0 - enable
voip dsp cidtype	
channel	Set the caller ID type for FXS 1 (Channel 1) or FXS 2 (Channel 2). 1 – FXS 1 2 – FXS 2
value	Each number (1 to 6) represents different type. 1 – FSK_ETSI 2 - FSK_ETSI(UK) 3 - FSK_BELLCORE(US/AU) 4 - DTMF 5 - DTMF(Dk) 6 - DTMF(SE,NL,FIN) For example : Vigor> voip dsp cidtype 2 6 channel=2, current cidType: 6 That means the caller ID type for FXS2 (Channel2) is DTMF (SE, NL, FIN).
voip dsp micgain	
channel	Adjust the volume of microphone by entering number from 1- 10 for FXS 1 or FXS 2. 1 – FXS 1 2 – FXS 2
value/(1~10)	The larger the number is, the louder the volume will be.
voip dsp spkgain	
channel	Adjust the volume of speaker by entering number from 1- 10 for FXS 1 or FXS 2. 1 – FXS 1 2 – FXS 2
value/(1~10)	The larger the number is, the louder the volume will be.
voip dsp jb	
port	Set the size of jitter buffer. Available settings are 0 (FXS1) and 1 (FXS2).
mode	Available settings are **Fixed** and **Adaptive** (default setting).
value	Available settings are 1 ~ 180 (unit: msec). e.g., Vigor> voip dsp jb 1 FIXED 100
voip dsp timer	
[Timer]	Set the waiting time for dialing out. It means to set the timer settings. The unit is mini-second. The range is from 1 to 255. Value “1” is corresponding to 500ms. That is to say, Value “6” is corresponding 3000ms (i.e., 3 seconds) Timer: 1 ~ 20. Vigor> voip dsp timer 20

	Set the timer:20
Voip dsp debugMsg	
?	Avaible settings include: clrev - clear phone hook status. getev - get phone hook status. clrfskcid - clear fsk data for caller-ID from PSTN line. getfskcid - get fsk data for caller-ID from PSTN line. clrdtmfcid - clear dtmf data for caller-ID from PSTN line. getdtmfcid - get dtmf data for caller-ID from PSTN line. voicebuf - get message for available voice buffer pool. clrint - clear status for interrupt. getint - get status for interrupt. Vigor> voip dsp debugMsg getint the interrupt status for ad0 = 21 the interrupt status for ad1 = 0 the interrupt status for vc = 0
voip dsp dtmfDetset	
nLevel	Set minimal signal level in dB, for DTMF detection. Range – (-96 ~ -1)
nTwist	Maximum allowed signal twist in dB, for DTMF detection. Range – (0 ~ 12)
voip dsp dtmftonepwr	
Level	Set power level for DTMF frequency. Level – 0 ~ 100. Power level for dtmf frequency in 0.3 dB steps. 0 map to 0dB 1 map to -0.3dB .... 100 map to -30dB
voip dsp cwtonepwr	
ch	Set the call waiting tone power level. 1 – FXS 1 2 – FXS 2.
value	1 ~ 30, in -1 dB increments, with 1 corresponding to 8 dBm.
voip dsp pstnringfxs	
1|2	Enable or disable PSTN ring on FXS 1/FXS 2. 1 meansFXS1; 2 means FXS2.
on|off	On means enable; off means disable.
voip dsp relaydbounce	
on|off	on: Enable relay filter noise. But it maybe ignore the caller-id!!! off: Disable relay filter noise. But the noise will cause the relay to switch to PSTN!!!
voip dsp setRingPat	
ring_pattern_index	This command can change the ring pattern at Index(2)~Index(6). ring_pattern_index – Index (1) was locked for your country.
patten_num	It's the ring pattern number (1~12) for a country. ---------- *patten_num=1 Australia Ring Pattern:* *cadenceOneOn=400, cadenceOneOff=200* *cadenceTwoOn=400, cadenceTwoOff=2000* *patten_num=2 Denmark Ring Pattern:*

	cadenceOneOn=1000, cadenceOneOff=4000 ……
voip dsp setFaxECmode -s	
ch	Set the FAX error correction mode. ch : range (0 ~ 1)
mode	mode : EC(error correction) ch(x) mode(0) : REDUNDANCY EC(error correction) ch(x) mode(1) : FEC
voip dsp setDtmfCidlevel –l / voip dsp setDtmfCidlevel –h [value] *voip dsp setDtmfCidlevel –r 0*	
value	"setDtmfCidLevel" is used to configure the signal strength for transferring to FXS DTMF caller ID. value - 0 ~ 64 voip dsp setDtmfCidLevel -l [value] voip dsp setDtmfCidLevel -h [value] voip dsp setDtmfCidLevel -r 0/1 r - reset low/high DTNF level to default setting. 0 means Disable; 1 means Enable. Note: This function is supported only by special mode.
voip dsp setfxoCY	
value	It is used to apply FXO country settings. 0: "use system country" 1: "Taiwan" 2: "Germany" 3: "Sweden" 4: "France" 5: "Switzerland" 6: "Holland" 7: "Finland" 8: "Denmark" 9: "UK" 10: "Australia" 12: "Italy" 14: "Red_China" 15: "Singapore" 17: "Spain" 18: "Portugal" 20: "Poland" 21: "Czech" 22: "Hungary" 23: "Slovenia" 25: "Slovakia" 37: "Brasil" 61: "US"
voip dsp setfxoringl	
value	It is used to configure detection ring voltage threshold to apply to FXO. Available setting include: 0 : use driver default value 1 : Minimum voltage threshold: 25V 2 : Minimum voltage threshold: 35V 3 : Minimum voltage threshold: 45V Note: This function is supported only by special mode.
voip dsp setfxoCid	

value	Set FXO detect caller ID type. It is available only for the model with FXO port.
voip dsp cidplusdigit	
[1/0] [channel] [value]	Set the substitution (0~9) for '+' digit in caller ID. 1 – enable the substitution. 0 – disable the substitution. channel – 0 (FXS 1) -1 (FXS 2) value – 0 – 9
voip dsp setRingThres	
port	Set the threshold for ring signal. Port setting is “0” only.
value	Available settings 0-250. Unit is ms. The time is an approximate value.
voip dsp setCidDetGain	
tx|rx gain	Set the gain value of caller ID detected. Tx gain – Available settings -24 ~ 12. Default is 0. Rx gain – Available settings -24 ~ 12. Default is -6.

Example

```
> voip dsp countrytone ?
VoIP has been disable. Please enable VoIP first.
> voip sip misc –D 0
System reboot now!
> voip dsp countrytone ?
> Vigor> voip dsp countrytone?
usage:
 voip dsp countrytone [channel][value]
 [channel]: 1-2
 [value]: ( [2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany, [7] Netherland
s, [8] Portugal, [9] Sweden, [10] Australia, [11] Slovenia, [12] Czech, [13]
Slovakia, [14] Hungary, [15] Switzerland , [16] France , [17] Malta)
============  Channel=1  ===================
 current country tone: user defined

----------- ( Dial tone ) --------------------
 Feq1=425, Feq2=0, OneOn=0, Off=0, TwoOn=0, TwoOff=0
----------- ( Ringing tone ) -----------------
 Feq1=425, Feq2=0, OneOn=1500, OneOff=3000, TwoOn=0, TwoOff=0
----------- ( Busy tone ) --------------------
 Feq1=425, Feq2=0, OneOn=200, OneOff=200, TwoOn=0, TwoOff=0

============  Channel=2  ===================
 current country tone: user defined
> voip dsp dialtonepwr 1 20
Current power level of dialtone:20 (-13 db), channel=1
> voip dsp setCidDetGain tx 1
 Current CID Detect Tx Gain [1], Rx Gain [-6]
> voip dsp setCidDetGain rx 3
 Current CID Detect Tx Gain [1], Rx Gain [3]
```

Telnet Command: voip rtp

Syntax

voip rtp codec *[sip acc index][type|size|vad|one][value]*

voip rtp dtmf *[index] [mode|payloadtype][value]*

voip rtp port *[start|end] [value]*

voip rtp symmetric *[value]*

voip rtp tos ?

Syntax Description

Parameter	Description
voip rtp codec	
[sip acc index][type|size|vad|one][value]	Set the voice coding. sip acc index –SIP account index number. Available number, 1 ~ 12. type – Available settings include 0. G.711MU 1. G.711A 2. G.729A/B 3. G.723 4. G.726_32 size - Five options, 0 means 10ms 1 means 20ms 2 means 30ms 3 means 40ms 5 means 60ms Vad - 0 means to Disable the function of Voice Active Detector (vad); 1 means to Enable the function of Voice Active Detector (vad). One – 0 means to Disable the function of single codec; 1 means to Enable the function of single codec.
voip rtp dtmf	
[index] [mode | payloadtype][value]	Set the DTMF mode and Payload type for DTMF. Index – SIP account index number. Available number, 1 ~ 12. Mode – Four options to be selected. 0. Inband 1. Outband 2. SIP INFO (cisco) 3. SIP INFO (nortel) Payloadtype – Available settings 96~127. Value – Type 0~3 or 96~127 based on the mode specified. For example, > voip rtp dtmf 1 mode 1
voip rtp port	
start|end	Specifies the start/end port for RTP stream.
value	The default value is 10050/15000.
voip rtp symmetric	
value	Make the data transmission going through on both ends of local router and remote router not misleading due to IP lost.

	1 – Enable 0 - Disable
voip rtp tos	
value	Set the type of service (TOS) setting for RTP packets. For example, > voip rtp tos 0x899 Set TOS: 0x899

Example

```
> voip rtp codec 1 type 3
> voip rtp dtmf 2 mode 3
> voip rtp port start 10070 end 14400
Set start port: 10070
> voip rtp port end 14400
Set end port: 14400
> voip rtp symmetric 1
Set symmetric rtp to Enable
```

Telnet Command: voip sip

This command allows users to set SIP account.

Syntax

voip sip acc n *[-<command> <parameter> | ...]*

voip sip calllog

voip sip ep n *[-<command> <parameter> | ...]*

voip sip misc*[-<command> <parameter> | ...]*

voip sip nat *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
voip sip acc - Allows users to set SIP account.	
n	n = 1 to 12 It means the index number of the VoIP settings.
-P [profile]	It means the name of the account profile (maximum 11 characters).
-r [reg mode]	Set registration mode for SIP account. 0 – none 1 – auto 2 - wan1 only 3 - wan2 only 4 - lan/vpn 5 – PVC 6 - wan3 only 7 - wan4 only 8 - wan1 first 9 - wan2 first 10 - wan3 first 11 - wan4 first
-o [port]	Set the port number for sending/receiving SIP message for building

	a session. The default value is 5060.
-d [domain]	Set the domain name or IP address of the SIP Registrar server. The maximum is 63 characters.
-y [proxy]	Set domain name or IP address of SIP proxy server. The maximum is 63 characters.
-b [enable]	Enable / disable outbound proxy by SIP account. 0 – disable 1 - enable
-s [enable]	Enable / disable to locate SIP server (rfc 3263). 0 – disable 1 - enable
-N [name]	Set SIP account display name. Name - max. 23 characters.
-n [number]	Set SIP account number. Number - max. 63 characters.
-a [id]	Set SIP authentication ID. Id - max. 63 characters.
-A [enable]	Enable /disable to use SIP authentication ID. 0 – disable 1 - enable
-p [passwd]	Set SIP account password (max. 63 characters).
-e [sec]	Set expiry time (default 3600) for SIP account.
-w [enable]	Enable to make phone call without registering.
-m [mode]	Set NAT traversal mode. 0 – disable 1 – stun 2 – manual 3 - nortel
-F [mode]	Set call forwarding mode. 0 – disable 1 – always 2 – busy 3 - no answer 4 - busy or no answer
-u [url]	Set SIP URL for call forwarding (max. 63 characters).
-t [sec]	Set call forwarding timer. For example, voip sip acc 1 –t 30
-g [port]	Set the ring port for incoming call. For example, Port - r1 means FXS1; r2 means FXS2.
-z [pattern]	Set account ring pattern (1 ~ 6).
-i [enable]	Remove all bindings while they are un-registered. 0 means Disable; and 1 means Enable.
-B <enable>	Enable / disable the function of Broadsoft Call Control. 0 – disable 1 - enable
-S [idx]	Enable and use alias IP to register. idx - 1 to 31. If 0 is used, such function will be disabled.
-k [num1 num2…]	Set backup wan list (first wan, second wan…).

	range: 1 to 4.
-v	View current status for account settings.
Voip sip calllog	Display current status for SIP call log.
voip sip ep	
n	The index number of the VoIP settings. n – 1, 2.
-o [acc]	Available dial out account (1 ~ 12).
-L [url]	Set SIP URL (max. 63 characters) for hot line.
-l [enable]	Enable / disable the function of hot line. 0 – disable 1 - enable
-W [enable]	Enable / disable the function of warm line. 0 – disable 1 - enable
-w [enable]	Enable / disable the function of call waiting enable. 0 – disable 1 - enable
-E [enable]	Enable / disable the function of call waiting enable but only remind one time. 0 – disable 1 - enable
-x <enable>	Enable / disable the function of call transfer. 0 – disable 1 - enable
-d [enable]	Enable / disable the function of DND (Do Not Disturb) 0 – disable 1 - enable
-s [id]	Indicate DND schedule. Id - s1, s2, s3, s4 (max. 4 schedule)
-h [enable]	Enable / disable the function of calling line identification restriction (CLIR). 0 – disable 1 - enable
-u [mode]	Set CLIR mode. 0 - means “draft-ietf-sip-privacy” 1 – means “rfc 3323/3325)”
-z [enable]	Enable / disable playing dial tone when registered on sip server. 0 – disable 1 - enable
-n [enable]	Enable / disable session timer. 0 – disable 1 - enable
-m [sec]	Set the value for session timer (unit: sec).
-R [min,max]	Set the flash hook time range 100~2000 (unit: ms).
-8 [enable]	Enable or disable T.38 fax relay feature. 0 – disable 1 - enable

-v	View current settings.
voip sip misc - Allows users to set miscellaneous settings for the device.	
-c [enable]	Enable compact header to shorten the packet (0: disable, 1: enable).
-s [enable]	Change “#” into digit number. 0 - disable 1 - enable
-e [enable]	Enable Europe style flash hook operation mode. 0 - disable 1 - enable
-h [enable]	Enable/disable call hold mode based on protocol RFC2543 (0: disable, 1:enable).
-i [enable]	Enable CODEC change without Re-INVITE. 0 - disable 1 - enable
-p [enable]	Enable PRACK message. 0 – Not support PRACK. 1 – Support PRACK.
-P [enable]	Enable IP Call. 0 – Disable IP call. 1 – Enable IP call.
-H [enable]	SIP INFO packet will be sent out when encounting hook flash event. 0 - disable 1 - enable
-t [val]	Set the mode of User-Agent (e.g., phone, software, and device) for SIP packet. 0 - Hide SIP header "User-Agent". 1 - Show SIP header "User-Agent". 2 - Use default "User-Agent" value. 3 - Use user-defined "User-Agent" value.
-u UAValue	For every SIP user agent identifies itself with a string, this command allows you to set the value (e.g, IP address, phone number, e-mail address) of User-Agent. The length of the string must be less than 64 characters.
-D [disable]	Disable VoIP Service. 1 – disable VoIP service. 0 – enable VoIP service. System will automatic reboot to activate voip service
-v	View current status for miscellaneous settings.
voip sip nat - Allows users to set NAT Traversal Setting.	
-s [server]	Set the IP address for STUN server.
-t [sec]	Set ping interval for SIP account. Sec – 6 ~ 600
-i [ip]	Indicate external IP address.
-v	View current settings for SIP NAT.

Example

```
> voip sip misc -t 1
```

```
includes User-Agent header

> voip sip misc -u 91704688carrie
user-defined User-Agent:91704688carrie
> voip sip acc 1 -P carrie_1 -r 1 -d 172.16.3.133
> voip sip acc 1 -t 30
> voip sip misc -h 1
> voip sip acc 1 -v
index        :  1
profile      :  carrie_1
reg mode     :  1 | reg. [No]
alias_ip_idx      :  0
backup list       :
domain       :  172.16.3.133
proxy        :   | outbound [No] | DNS-SRV [No]
noreg call   :  No
disp. Name   :
acc number   :  ---
auth. ID     :   | [disable]
expiry       :  3600
NAT mode     :  0
ring ports   :  0
ring pat.    :  1
call fwd mode     :  0
call fwd url      :
call fwd timer    :  30
Broadsoft    :  disable
Italian ITSP modification: disable
```

Telnet Command: voip secure

This command allows users to enable or disable secure phone feature, and SAS voice prompt.

Syntax

voip secure general *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
voip secure general -e	Enable / disable secure phone feature. 0 - disable 1 - enable
voip secure general -p	Enable /disable SAS voice prompt. 0 - disable 1 - enable
voip secure general -v	view only secure phone general settings

Example

```
> voip secure general -v
secure phone feature is disabled
SAS voice prompt is enabled
```

```
> voip secure general -p  0
SAS voice prompt is disabled
```

Telnet Command: vlan

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	It means the group 0 to 7 for VLAN.
set	It indicates each port can join more than one VLAN group.
set_ex	It indicates each port can join one VLAN group at one time.
p1/p2/p3/p4	It indicates LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please type the port number(s) you want.
s1/s2/s3/s4	It is only available for WALN models.

Example

```
> vlan group 3 set p1 s3 s4 5gs3 5gs4
VLAN   p1   p2   p3   p4   s1   s2   s3   s4  5gs1  5gs2  5gs3  5gs4

-------------------------------------------------------------------------
  3    V                         V    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 LAN2/3/4/5/6/7/8 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	It means VLAN ID number. n=VLAN ID number (from 0 to 7).
pri_no	It means the priority of VLAN profile. pri_no=0 ~7 (from none to highest priority).

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 5gs1 5gs2 5gs3 5gs4  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            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/s4/5gs1/5gs2/5gs3/5gs4, 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 <*1/2/3/4*>

Syntax Description

Parameter	Description
<*1/2/3/4*>	It means interfaces, LAN1 ~ LAN4.

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.
```

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	It means to enable the promiscuous mode.
off	It means to enable the normal mode.
status	It 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.
```

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*>	It means VLAN number. The ranage is from 0 to 15.
<*on/off*>	It means to enable/disable the tagged VLAN.
<*unlimited*> <*on/off*>	unlimited on: It allows the incoming of untagged packets even all VLAN are tagged. unlimited off: It does not allows the incoming of untagged packets.
<*p1_untag*> <*on/off*>	P1_untag on: It allows the incoming of untagged packets form LAN port 1. P1_untag off: It does not allow the incoming of untagged packets from LAN port 1.

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*>	It means VLAN channel. The ranage is from 0 to 7.
<*vid_no*>	It means the value of VLAN ID. Type the value as the VLAN ID number. The range is form 0 to 4095.

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	It means the value to be set as VLAN ID. The range is from 0 to 4018.

Example

```
> vlan sysvid 100
 You have set system VLAN ID to range: 100 ~ 177,
 We recommend that you reboot the system now.
>
```

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/aesg5/aesg14*>

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*>

vpn l2lset <*list index*> **compress** <*0/1/2/3*>

Syntax Description

Parameter	Description
<*list index*>	It means the index number of L2L (LAN to LAN) profile.
peerid <*peerid*>	It means the peer identity for aggressive mode.
localid <*localid*>	It means the local identity for aggressive mode.
main <*auto/proposal index*>	It means to choose proposal for main mode.

	<auto>: Choose default proposals. <proposal index>: choose specified proposal.
aggressive <desg1/desg2/aesg1/aesg2/ aesg5/aesg14>	It means the chosen DH group for aggressive mode.
pfs <on/off>	It means “perfect forward secrete”. <on/off>: Turn on or off the PFS function.
phase1 <lifetime> / *phase2 <lifetime>*	It means phase 1 or 2 of IKE. <lifetime>: Set the lifetime value (in second) for phase 1 and phase 2.
x509localid <0/1>	It means to enable (1) or disable (0) the X509 local ID.
compress <0/1/2/3>	It means to set the compress setting. <0/1/2/3>: Enter a number. 0: Disable 1: No 2: LZ4 3: LZO

Example

```
> vpn l2lset 1 peerid 10226
>
```

Telnet Command: vpn l2lDrop

This command allows users to terminate current LAN to LAN VPN connection.

Syntax

vpn l2lDrop *l2lname <name>*

vpn l2lDrop *l2lidx <idx>*

vpn l2lDrop *h2lname <name>*

vpn l2lDrop *h2idx <idx>*

vpn l2lDrop *<ifno>*

vpn l2lDrop

Syntax Description

Parameter	Description
l2lname <name>	It means to drop VPN connection by specifying the name of the LAN to LAN profile.
l2lidx <idx>	It means to drop VPN connection by specifying the index number of LAN to LAN profile.
h2lname <name>	It means to drop VPN connection by specifying the name of the remote dial-in user profile.
h2idx <idx>	It means to drop VPN connection by specifying the index number of the remote dial-in user profile.
<ifno>	It means to drop VPN connection by using VPN ifno.
l2lDrop	It means to drop all VPN connections.

Example

```
> vpn l2lDrop l2lidx 2
% Drop 0 VPN with idx : 2
>
```

Telnet Command: vpn l2lDialout

This command allows users to terminate current LAN to LAN VPN connection (dial-out).

Syntax

vpn l2lDialout <*idx*>

vpn l2lDialout *list*

Syntax Description

Parameter	Description
l2lDialout <idx>	It means to build VPN connection by specifying the index number of dial-out LAN to LAN profile. <idx>: Enter an index number (1 to 32).
list	It means to display LAN to LAN profiles (enabled).

Example

```
> vpn l2lDialout 1
 Profile Index: 1 not enable!!!
> vpn l2lDialout list
List LAN to LAN profiles of the status as Enable
Index   Profile      Active    Status
% Drop 0 VPN with idx : 2
>
```

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*> **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*>	It means the index number of the profile.
<*list index*> <*on/off*>	It means to enable or disable the profile. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<*list index*> *motp* <*on/off*>	It means to enable or disable the authentication with mOTP function. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<*list index*> *pin_secret*<*pin*> <*secret*>	It means to set PIN code with secret. <list index> - Enter the index number of the VPN profile. <pin> **-** Type 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 idle timeout. The default is 300 (seconds). <list index> - Enter the index number of the VPN profile. <0~9999> - Enter a value.
<*list index*> *dintype* <*Type*> <*on/off*>	It means to enable/disable the allowed dial-in type. <list index> - Enter the index number of the VPN profile. <Type> - 0 to 3. In which, 0 means PPTP; 1 means IPsec Tunnel; 2 means L2TP with IPsec Policy; 3 means SSL Tunnel. <on/off> - on: Enable; off: Disable.
vpn dinset <*list index*> *subnet* <*0~4*>	It means to set the LAN subnet for the selected VPN profile. <list index> - Enter the index number of the VPN profile. <0~4> - Enter a number to specify the LAN subnet. In which, 0:LAN1 1:LAN2 2:LAN3 3:LAN4 4:DMZ
vpn dinset <*list index*> *assignip* <*on/off*>	It means to enable or disable the function of assigning the static IP address. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
vpn dinset <*list index*>	It means to enable or disable the function of specifying the remote

srnode <on/off>	node. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> remoteip <Remote_Client_IP_Address >	It means to enable or disable the function of assigning remote client IP. <list index> - Enter the index number of the VPN profile. <Remote_Client_IP_Address> - Set the IP address of the remote client.
vpn dinset <list index> peer <Peer_ID>	It means to assign the peer ID. <list index> - Enter the index number of the VPN profile. <Peer_ID> - Enter the string of the peer ID.
vpn dinset <list index> naming <pass/block>	It means to set the Netbiod Naming Packet for the VPN profile. <list index> - Enter the index number of the VPN profile. <pass/block> - Let the packet pass or block the packet.
vpn dinset <list index> multicastvpn <pass/block>	It means to set the multicast via VPN for IGMP, IP-CAM, DHCP relay, and etc. <list index> - Enter the index number of the VPN profile. <pass/block> - Let the packet pass or block the packet.
vpn dinset <list index> prekey <on/off>	It means to enable/disable the Pre-Shared Key setting for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> assignkey <Pre_Shared_Key>	It means to set the Pre-Shared Key for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <Pre_Shared_Key> - Enter a string as PSK.
vpn dinset <list index> digsig <on/off>	It means to enable/disable the digital signature (X.509) for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> ipsec <Method> <on/off>	It means to enable / disable and set the protocol for IPsec security method. <list index> - Enter the index number of the VPN profile. <Method> - Enter a number (0 to 3) to specify the protocol. 0 means Medium(AH) High(ESP), 1 means DES 2 means 3DES 3 means AES <on/off> - on: Enable; off: Disable.
vpn dinset <list index> localid <Local_ID>	It means to set local ID (optional) for IPsec Security Method. <list index> - Enter the index number of the VPN profile. <local_ID> - Enter the string of local ID.

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*> <*1/2/3/4*>

Syntax Description

Parameter	Description
<*index*>	It means the index number of the VPN profile.
<*1/2/3/4*>	1 – it means LAN1 2 – it means LAN2. 3 – it means LAN3 4 – it means LAN4.

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*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address to dial to.
<*usr*> <*pwd*>	It means the user and the password required for the PPTP connection.
<*nip*> <*nmask*>	It means the remote network IP and the mask. 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*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address to dial to.
<*key*>	It means the value of IPsec Pre-Shared Key.
<*nip*> <*nmask*>	It means the remote network IP and the mask. 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*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address to dial to.
<*usr*> <*pwd*>	It means the user and the password required for the L2TP connection.
<*nip*> <*nmask*>	It means the remote network IP and the mask. 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*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address allowed to dial in.
<*usr*> <*pwd*>	It means the user and the password required for the PPTP/L2TP connection.
<*key*>	It means the value of IPsec Pre-Shared Key.
<*nip*> <*nmask*>	It means the remote network IP and the mask. 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*> | *…]*

Syntax Description

Parameter	Description
<*index*>	It means the index number of the profile. Available index numbers: 1 ~ 32
For Common Settings	
<*index*>	It means the index number of the profile.
pname	It means the name of the profile.
ena	It means to enable or disable the profile. on – Enable off - Disable
thr	It means the way that VPN connection passes through. Available settings are wlf, wlo, w2f, and w2o.

	w1f – WAN1 First. w1o – WAN1 Only. w2f – WAN2 First. w2o – WAN2 Only.
nnpkt	It means the NetBios Naming Packet. on – Enable the function to pass the packet. off – Disable the function to block the packet.
dir	It means the call direction. Available settings are b, o and i. b – Both o – Dial-Out i – Dial-In.
idle=[value]	It means Always on and Idle Time out. Available values include: -1 – it means always on for dial-out. 0 – it 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	It means to enable PING to keep alive. -1 – disable the function. 1,2,3,4 – Enable the function and PING IP 1.2.3.4 to keep alive.
For Dial-Out Settings	
ctype	It means “Type of Server I am calling”. “ctype=t” means PPTP. “ctype=s” means IPSec. “ctype= l” means L2TP(IPSec Policy None). “ctype= l1” means L2TP(IPSec Policy Nice to Have). “ctype= l2” means L2TP(IPSec Policy Must).
dialto	It means Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89).
ltype	It means Link Type. “ltype=0” means “Disable”. “ltype=1” means “64kbps”. “ltype=2” means “128kbps”. “ltype=3” means “BOD”.
oname	It means Dial-Out Username. “oname=admin” means to set Username = admin.
opwd	It means Dial-Out Password “opwd=1234” means to set Password = 1234.
pauth	It means PPP Authentication. “pauth=pc” means to set PPP Authentication = PAP&CHAP. “pauth=p” means to set PPP Authentication = PAP Only
ovj	It means VJ Compression. “ovj=on/off” means to enable/disable VJ Compression.
okey	It means IKE Pre-Shared Key. “okey=abcd” means to set IKE Pre-Shared Key = abcd.
ometh	It means IPSec Security Method. “ometh=ah/” means AH. “ometh=espd/espda/” means ESP DES without/with Authentication. “ometh=esp3/esp3a/” means ESP 3DES without/with

	Authentication. “ometh=espa/espaa” means ESP AES without/with Authentication.
sch	It means Index(1-15) in Schedule Setup. sch=1,3,5,7 Set schedule 1->3->5->7
rcallb	It means Require Remote to Callback. “rcallb=on/off” means to enable/disable Set Require Remote to Callback.
ikeid	It means IKE Local ID. “ikeid=vigor” means Set Local ID = vigor.
For Dial-In Settings	
itype	It means Allowed Dial-In Type. Available settings include: “itype=t” means PPTP. “itype=s” means IPSec. “itype=L1”means L2TP (None). “itype=L1” means L2TP(Nice to Have). “itype=l2” means L2TP(Must).
peer	It means specify Peer VPN Server IP for Remote VPN Gateway. Type “203.12.23.48” means to allow VPN dial-in with IP address of 203.12.23.48. Type “off” means any remote IP is allowed to dial in.
peerid	It means the peer ID for Remote VPN Gateway. Type “draytek” means the word is used as local ID.
iname	It means Dial-in Username. “iname=admin” means to set username as “admin”.
ipwd	It means Dial-in Password. “ipwd=1234” means to set password as “1234”.
ivj	It means VJ Compression. “ivj=on/off” means to enable /disable VJ Compression.
ikey	It means IKE Pre-Shared Key. “ikey=abcd” means to set IKE Pre-Shared Key = abcd.
imeth	It means IPSec Security Method “imeth=h” means “Allow AH”. “imeth=d” means “Allow DES”. “imeth=3” means “Allow 3DES”. “imeth=a” means “Allow AES.
For TCP/IP Settings	
mywip	It means My WAN IP. “mywip=1.2.3.4” means to set My WAN IP as “1.2.3.4”.
rgip	It means Remote Gateway IP. “rgip=1.2.3.4” means to set Remote Gateway IP as “1.2.3.4”.
rnip	It means Remote Network IP. “rnip=1.2.3.0” means to set Remote Network IP as “1.2.3.0”.
rnmask	It means Remote Network Mask. “rnmask=255.255.255.0” means to set Remote Network Mask as “255.255.255.0”.
rip	It means RIP Direction. “rip=d” means to set RIP Direction as “Disable”. “rip=t” means to set RIP Direction as “TX”.

	"rip=r" means to set RIP Direction as "RX". "rip=b" means to set RIP Direction as "Both".
mode	It means the option of "From first subnet to remote network, you have to do". "mode=r" means to set Route mode. "mode=n" means to set NAT mode.
droute	It means to Change default route to this VPN tunnel (Only single WAN supports this). droute=on/off means to enable/disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
>
```

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
list	It means to display all of the route settings.
add	It means to add a new route.
del	It means to delete specified route.
<*index*>	It means the index number of the profile. Available index numbers: 1 ~ 32
<*network ip*>/<*mask*>	Enter the IP address with the network mask address.

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
all	It means to list configuration of the specified profile.
com	It means to list common settings of the specified profile.
out	It means to list dial-out settings of the specified profile.
in	It means to list dial-in settings of the specified profile.
net	It means to list Network Settings of the specified profile.
<*index*>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```
> vpn list 32 all
% Common Settings

% Profile Name            : ???
% Profile Status          : Disable
% Dialout WAN IP Alias Index  : None
% Netbios Naming Packet   : Pass
% Call Direction          : Both
% Idle Timeout            : 300
% PING to keep alive      : off
% OVPN Compress           : Disable
% OVPN tls_auth option    : off

% Dial-out Settings

% Type of Server          : PPTP
% Link Type:              : 64k bps
% Username                : ???
% Password                :
% PPP Authentication      : PAP/CHAP
% VJ Compression          : on
% Pre-Shared Key          :
% IPsec Security Method   : AES with Authentication
% Schedule                : 0,0,0,0
% Remote Callback         : off
% Provide ISDN Number     : off
```

```
% IKE phase 1 mode         : Main mode
% IKE Local ID             :

% Dial-In Settings

% Allow Dial-in Type    : ISDN IPsec L2TP (IPsec Policy None) --- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> vpn list 1 com
% Common Settings

% Profile Name             : ???
% Profile Status           : Disable
% Netbios Naming Packet    : Pass
% Call Direction           : Both
% Idle Timeout             : 300
% PING to keep alive       : off
>
```

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>	There are four types to be selected.
<on/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 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>	H2I means Remote Access User Accounts.

	L2l means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<*index*>	The index number of the profile.
<*Block/Pass*>	**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*>	1~4 represent various type. 1 – PPTP 2 – L2TP 3 – IPSec 4 – L2TP over IPSec 5 - SSL Tunnel
<*TCP maximum segment size range*>	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  = 1260
> vpn mss show
% VPN TCP maximum segment size (MSS) :
  PPTP  = 1400
  L2TP  = 1360
  IPsec = 1360
  L2TP over IPsec  = 1360
  SSL Tunnel  = 1260
>
```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

Syntax

vpn ike -q

vpn ike -s

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*>	H2L means Host to LAN (Remote Access User Accounts). L2L means LAN-to-LAN Profile.
<*index*>	The index number of the profile.
<*Block/Pass*>	Set Block/Pass the Multicast Packets. The default is Block.

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 – the packets can pass through NAT. off – the packets cannot pass through NAT.

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 – 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 passAPM

This command is used for configuring the APM broadcast allowed to pass the VPN tunnel.

Syntax

vpn passAPM <*on/off***>**

Syntax Description

Parameter	Description
<*on/off***>**	on – the packets can pass through NAT. off – the packets cannot pass through NAT.

Example

```
> vpn passAPM on
% APM broadcast is allowed to pass VPN tunnel!
>
```

Telnet Command: vpn sameSubnet

This command allows users to build VPN between clients via virtual subnet.

Syntax

vpn sameSubnet *-i <value>*

vpn sameSubnet *–E <0/1>*

vpn sameSubnet *–e <value>*

vpn sameSubnet *-I <Virtual Subnet>*

vpn sameSubnet *-o <add/del>*

vpn sameSubnet *-v*

vpn sameSubnet *-m <1/2>*

Syntax Description

Parameter	Description
-i <value>	Specify the index number of VPN profile.
–E <0/1>	Enable or disable the IPsec with the same subnet. 1 – enable. 0 – disable.
–e <value>	Translate specified LAN to virtual subnet. 1 – LAN1 2 – LAN2 3 – LAN3 **...**
-I <Virtual Subnet>	Set the virtual subnet (e.g., 172.16.3.250).
-o <add/del>	Set the operation.
-v	Display current status of virtual subnet.
-m <1/2>	Set the translated type. <1/2>: Enter a number. 1 means the Whole Subnet; 2 means Specific IP.

Example

```
> vpn sameS  -i 1 -e 1 -E 1 -e 1 -I 10.10.10.0 -o add
 Enable IPsec with Same Subnet !!

 Add entry Succcess!!
> vpn sameS -v
IPsec with the same subnet:
VPN profile 1 enable,
  Whole Subnet:
    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*>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<*MRU size* >	It means the number of PPP LCP MRU. The available range is from 1400 to 1600.

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 WAN.

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 users to configure primary and / or secondary DNS server.

Syntax

wan dns <*wan_no*> <*dns_select*> <*ipv4_addr*>

Syntax Description

Parameter	Description
<*wan_no*>	Select WAN interface. 1 - WAN1
<*dns_select*>	Specify primary and / or secondary DNS server. pri – It means primary DNS server. sec – It means secondary DNS server.
<*ipv4_addr*>	Enter the IP address of DNS server.

Example

```
> wan dns 1 pri 168.95.1.1
% Set WAN1 primary DNS done.
% Now: 168.95.1.1
```

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*>	It means to enable or 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*>	It means to enable or 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=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

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 TX Packets=0, TX
Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: wan modem

This command, wan modem, allows you to configure 3G/4G USB Modem (PPP mode) of WAN3.

Syntax

wan modem <*init/dial/pin*> <*string*>

wan modem dial <*string*>

wan modem pin <*1/0*>

wan modem paponly <*on/off*>

wan modem backup_wait <*value*>

wan modem pipe <*Int*><*Din*><*Dout*> *(for USB WAN3 only)*

wan modem wakeup <*on/off/value*> *(for USB WAN3 only)*

wan modem status

Syntax Description

Parameter	Description
init	Set initial modem AT command (default value is

	"AT&FE0V1X1&D2&C1S0=0").
dial <string>	Set dial modem AT command. <string>: Enter a string. (default value is "ATDT*99#").
pin <0>	Set PIN code for SIM card. "0":disable
paponly <on/off>	It means PAP Only. Set the PPP authentication of the USB WAN. on: None. off: PAP or CHAP.
backup_wait <value>	Set waiting time after boot if USB WAN is in backup mode. This waiting time is reserved for the dial of main WANs so that the backup USB WAN will not go up first. Available setting is from 1 to 255. Unit is second.
pipe	It is for RD debug only. Please don't use it without our advice.
wakeup [on/off]	It is for RD debug only. Please don't use it without our advice.
status	Display current status of USB modem.

Example

```
> wan modem pin 0
> wan modem status
 Modem Link Speed=0
 Current Signal Strength=0
 Last Fail Message:
 Current Connect Stage:
```

Telnet Command: wan lte

This command allows you to configure LTE WAN (for L model only).

Syntax

wan lte auth *<0/1>*

wan lte band

wan lte del <*index #/all***>**

wan lte pass *<string>*

wan lte quota *[-<command><parameter>|...]*

wan lte read <*index #/all***>**

wan lte reboot *[-<command><parameter>|...]*

wan lte reply *[-<command><parameter>|...]*

wan lte send *<number><message>*

wan lte stus

wan lte tag <*index #/all***>**

wan lte user *<string>*

wan lte wms *send <cdma/gwpp> / recv <cdma/gwgw>*

wan lte wms *setting*

Syntax Description

Parameter	Description
auth <0/1>	Set PPP authentication of LTE WAN. 0: None. 1: PAP or CHAP.
band	Display working band information for LTE network connection.
del <index #/all>	Delete an SMS from the LTE SIM card by specifying the index number. Use “all” to delete all.
pass <string>	Set the password of LTE WAN.
quota [-<command><parameter>|...]	Set settings of SMS Quota Limit function. Available commands with parameter are listed below: [...] means that you can Enter several commands in one line. -a <0/1>: Set whether to send an e-mail alert when SMS quota exceeded. (0: no 1: yes) -c <cycle>: Set the order of today in refresh cycle. -d <day>: Set the refresh day. -e <0/1>: Enable or disable SMS Quota Limit function. (0: disable 1: enable) -h <hour>: Set the refresh hour. -m <0/1/2>: Set SMS quota refresh mode. (0: None 1: monthly 2: periodically) -n <number>: Set SMS quota. The avaible number is between 1 and 1000000. -s <0/1>: Set whether to stop sending SMS after SMS quota exceeded. (0: no 1: yes)
read <index #/all>	Display information of an SMS in the LTE SIM card by specifying the index number. Use "all" to display all.

reboot	Set settings of Reboot on SMS Message function. <command> <parameter> | ... The available commands with parameters are listed below. [...] means that you can Enter several commands in one line. -a <0/1>: Enable or disable Access Control List. (0: disable 1: enable) -e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable) -p <password>: Set the Password / PIN. This setting is necessary if this function is enabled. -x <number>: Set the first phone number in Access Control List. -y <number>: Set the second phone number in Access Control List. -z <number>: Set the third phone number in Access Control List.
reply	Set settings of Reply with Router Status Message function. <command> <parameter> | ... The available commands with parameters are listed below. [...] means that you can Enter several commands in one line. -a <0/1>: Enable or disable Access Control List. (0: disable 1: enable) -c <0/1>: Set whether to reply with MAC address. (0: no 1: yes) -e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable) -f <0/1>: Set whether to reply with WAN1 IP address. (0: no 1: yes) -g <0/1>: Set whether to reply with WAN2 IP address. (0: no 1: yes) -h <0/1>: Set whether to reply with LTE WAN IP address. (0: no 1: yes) -i <0/1>: Set whether to reply with WAN4 IP address. (0: no 1: yes) -j <0/1>: Set whether to reply with WAN1 data usage. (0: no 1: yes) -k <0/1>: Set whether to reply with WAN2 data usage. (0: no 1: yes) -l <0/1>: Set whether to reply with LTE WAN data usage. (0: no 1: yes) -m <0/1>: Set whether to reply with WAN4 data usage. (0: no 1: yes) -n <0/1>: Set whether to reply with Router name. (0: no 1: yes) -p <password>: Set the Password / PIN. This setting is necessary if this function is enabled. -u <0/1>: Set whether to reply with Router system uptime. (0: no 1: yes) -v <0/1>: Set whether to reply with Router firmware version. (0: no 1: yes) -x <number>: Set the first phone number in Access Control List. -y <number>: Set the second phone number in Access Control List. -z <number>: Set the third phone number in Access Control List.
send <number><message>	Send an SMS message to the specified phone number through the LTE SIM card.
stus	Display status of LTE connection.
tag <index #/all>	Set an SMS in the LTE SIM card as read state by specifying the index number. Use "all" to set all SMS as read state.
user <string>	Set the UserName of LTE WAN.
wms send <cdma/gwpp>/ *wms recv <cdma/gwgw>* *wms setting*	This command is for RD debug only. We use it to test new USB modems. Please don't use it without our advice.

Example

```
> wan lte band

Access technology : LTE
Access band information : E-UTRA Op Band 3
Interfere with 2.4G WLAN : NO
Active channel: 1725
>wan lte stus
Status: Operational. (Online)
Access Tech: LTE
Band: E-UTRA Op Band 3
ISP: Chunghwa
MCC: 466, MNC: 92, LAC: 65534, Cell ID: 81023501
Max Channel TX Rate: 50000000 bps
Max Channel RX Rate: 100000000 bps
IMEI: 356318040749422
IMSI: 466924200859808
RSSI: -61 dBm
Unread SMS: 4
SMSC address: +886932400821
SMS service status : Ready
Number of SMS sent : 0
```

Telnet Command: wan detect

This command allows you to configure WAN connection detection. When Ping Detection is enabled (for Static IP or DHCP or PPPoE mode), Router pings specified IP addresses to detect the WAN connection.

Syntax

wan detect <*wan1*> <*on/off/strict/always_on*>

wan detect <*wan1*> <*on/off*> *-t* <*time*>

wan detect <*wan1*> <*on/off*> *-i* <*interval*>

wan detect <*wan1*> **target** <*ip addr*>

wan detect <*wan1*> **target2** <*ip addr*>

wan detect <*wan1*> **target_gw** <*1/0*>

wan detect <*wan1*> **ttl** <*value*>

wan detect <*wan1*> **interval** <*interval*>

wan detect <*wan1*> **retry** <*retry*>

wan detect status

Syntax Description

Parameter	Description
<*on/off/strict/always_on*>	On: Enable ping detection. The IP address of the target shall be set. Off: Enable ARP detection (default). Time and interval should be set. strict: Enable the strict ARP detection. Time and interval should be set. always_on: Disable link detect, always connected(only support static IP)

-t <time>	Set the time for ARP detect or strict ARP detection.
-i <interval>	Set the interval for ARP detect or strict ARP detection.
target <ip addr>	Set the ping target. <ip addr>: It means the IP address used for detection. Type an IP address (e.g., 192.168.1.10) in this field.
target2<ip addr>	Set the secondary ping target. <ip addr>: It means the IP address used for detection. Type an IP address (e.g., 192.168.1.10) in this field.
target_gw <1/0>	Set whether to use gateway as ping target. 1: yes 0: no Note that USB WAN (PPP mode) cannot support PING gateway
ttl <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.
interval <interval>	Set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second. <*interval*>*:* Type a value.
retry <retry>	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. <retry>: Type a number.
status	It means to show the current status.

Example

```
> wan detect status
 WAN1: arp detect, send time=30, Interval = 5
 WAN2: arp detect, send time=30, Interval = 5
 WAN3: arp detect, send time=30, Interval = 5
 WAN4: arp detect, send time=30, Interval = 5
 WAN5: arp detect, send time=30, Interval = 5
 WAN6: arp detect, send time=30, Interval = 5
> wan detect wan1 target 192.168.1.78
 Set OK
> wan detect wan1 on
 Set OK

> wan detect status
 WAN1: ping detect, Target=192.168.1.78, TTL=255, Target2=0.0.0.0,
 TargetGW=off,
 Interval=1, Retry=10
 WAN2: arp detect, send time=30, Interval = 5
 WAN3: arp detect, send time=30, Interval = 5
 WAN4: arp detect, send time=30, Interval = 5
 WAN5: arp detect, send time=30, Interval = 5
 WAN6: arp detect, 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	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, bridge mode can be set on PVC number 2 to 9.
status	It means to display the whole Bridge status.
save	It means to save the configuration into flash of Vigor router.
enable/disable	It means to enable/disable the Multi-VLAN function.
on/off	It means to turn on/off bridge mode for the specific channel.
clear	It means to turn off/clear the port.
tag tag_no	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
service type	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
vlan priority	It means to specify the priority for the VALN setting. Range is from 0 to 7.
px	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

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> wan mvlan 7 on p2 p3 p4

PVC  Bridge  p1 p2 p3 p4 p5 p6   Service Type    Tag     Priority    Keep Tag
 ---------------------------------------------------------------------
   7  ON     0  0  1  1  0  0     Normal      0(OFF)     0       OFF

>
```

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 #*>	There are several channels for bridge connection. Available settings are: 4=Channel 4 5=Channel 5 … 10=Channel 10
<*WAN interface #*>	Type a number to indicate the WAN interface. *1=WAN1*
status	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
% Channel 8 uplink ifno: 3
% Channel 9 uplink ifno: 3
>
```

Telnet Command: wan vlan

This command allows you to configure the VLAN tag of WAN1 or WAN2.

Syntax

wan vlan wan <*#*> **tag <***value*>

wan vlan wan <*#*> <*enable/disable*>

wan vlan stat

Syntax Description

Parameter	Description
wan <*#*>	Specify which WAN interface will be tagged.
tag **<***value*>	Type a number for tagging on WAN interface.
<*enable/disable*>	Enable: Specified WAN interface will be tagged. Disable: Disable the function of tagging on WAN interface.

stat	Display current VLAN status.

Example

```
> wan vlan stat
% Interface       Pri   Tag    Enabled
% ====================================
% WAN1            0      0
% WAN2            0      0
```

Telnet Command: wan phyvlan

This command is used to set VLAN tag insertion for outer tag (service) for WAN interface. WAN interfaces must be configured first before setting VLAN encapsulation.

Syntax

wan phyvlan wan <#> **tag <***value***>**

wan phyvlan wan <#> **pri <***value***>**

wan phyvlan wan <#> <*enable/disable*>

wan phyvlan stat

Syntax Description

Parameter	Description
<#>	It means WAN interface. 1 – WAN1 2 – WAN2
tag **<***value***>**	It means to tag a value (1 to 4095) onto the selected WAN interface.
pri **<***value***>**	It means to set value (0 to 7) for priority for such VLAN tag.
<*enable/disable*>	It means to enable / disable the VLAN tag.
stat	Display the setting status.

Example

```
> wan phyvlan wan 1 tag 22
% Set physical port tag to 22 for WAN1
% Set physical port tag to 22 for WAN1
% You need to reboot router making config effective
> wan phyvlan stat ?
% Interface    Pri     Tag    Enabled
% ====================================
% WAN1         0       22
% WAN2         0        0
>
```

Telnet Command: wan budget

This command allows you determine the data *traffic volume* for each WAN interface respectively to prevent from overcharges for data transmission by the ISP.

Syntax

wan budget wan <#> *rdate <day><hour>*

wan budget wan <#> <*enable*|*disable*>

wan budget wan <#> **thres** <*budget limit (MB)*>

wan budget wan <#> **gthres** <*budget limit (GB)*>

wan budget wan <#> **mode** <*monthly*|*periodic*|*none*>

wan budget wan <#> **psday** <*th day in periodic*>

wan budget wan <#> *custom_mode <0/1>*

wan budget wan <#> *custom_mode_reset_hour <hour>*

wan budget wan <#> **action** <*action bitmap*>

wan budget status

Syntax Description

Parameter	Description
wan <#> rdate <day><hour>	wan <#>: Specify the WAN interface. *rdate <day><hour>:* Specify the WAN budget refresh time. day – Available settings are from 1 to 30. hour – Available settings are from 1 to 23. E.g., `wan budget wan 1 rdate 5 10` If monthy mode is selected: WAN budget will be refreshed on 5th day at 10:00 in each month. If periodic mode is selected: WAN budget will be refreshed every 5 days and 10 hours.
<*enable*|*disable*>	enable - Enable the function of wan budget. disable - Disable the function of wan budget.
thres <budget limit (MB)>	Specify the maximum value for WAN budget limit. (Unit: MB) budget limit – Type a number.
gthres <budget limit (GB)>	Specify the maximum value of wan budget limit. (Unit: GB) budget limit – Type a number.
mode <*monthly*|*periodic*|*none*>	Specify the calculation mode (monthly, periodically, or none) for WAN budget.
psday <th day in periodic>	It is used only when mode is set with "periodic". Specify the order of "today" in the cycle. E.g., `wan budget wan 5 psday` → It means "today" is the 5th day in the billing cycle.
custom_mode <0/1>	Set the custom mode (cycle in hours or in days). 0: cycle_in_hours 1: cycle_in_days
custom_mode_reset_hour <hour>	Set the reset hour value. hour: Enter 1 to 23.
action <action bitmap>	Determine the action to be performed when it reaches the WAN budget limit. *action bitmap* – Type a total number of actions to be executed. Different numbers represent different actions. 1: shotdown wan

	2: send mail alert 4: send sms alert For example, if you type “5” (5=1+4), the system will send SMS alert when WAN shotdown is detected.
status	Display current configuration status of WAN budget.

Example

```
> wan budget wan 1 action 5
% WAN 1 budget action set to 5
> wan budget wan 1 gthres 10
% WAN 1 budget limit set to 10 GB
> wan budget status
% WAN1 budget configuration:
% Status = Disabled
% Mode = No Refreshing
% Action = Shutdown WAN  Send SMS
% Budget Limit = 10 GB
% WAN2 budget configuration:
% Status = Disabled
% Mode = No Refreshing
% Action = None
% Budget Limit = 0 MB
% WAN3 budget configuration:
% Status = Disabled
% Mode = No Refreshing
% Action = None
% Budget Limit = 0 MB
>
```

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 <#> -c <count>*

Syntax Description

Parameter	Description
-I <Host/IP address>	Specify the IPv4 target to detect. If can be an IPv4 address or domain name. Host/IP address: Enter the IP address/domain name of the target.
-s <mtu_size>	Set the MTU size base for Discovery. mtu_size: Available setting is 1000 ~ 1500.
-d <decrease size>	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.
-c <count>	Set the maximum times of ping failure during a Discovery. count: Available settings are 1 ~ 10. Default value is 3.

Example

```
> wan detect_mtu -w 2 -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 <#>*

Syntax Description

Parameter	Description
-I <Host/IP address>	Specify the IPv6 target to detect. It must be an IPv6 IP address. IPv6 address: Enter the IPv6 address of the target.
-s <mtu_size>	Specify the size of MTU. mtu_size: Available setting is 1280 ~ 1500.
-w <#>	Specify the WAN interface. number: Enter the number of WAN interface. 1: WAN1.

Example

```
> wan detect_mtu6 -w 1 -i 2404:6800:4008:c06::5e -s 1500
>
```

Telnet Command: wan failover

This command is used to configure failover WAN.

Syntax

wan failover off *<index>*

wan failover on *<1><2><3><4><5><6>*

wan failover show *<index>*

Syntax Description

Parameter	Description
failover off <index>	Set specified WAN interface to always on. index – Ranges from 1 to 3.
failover on <1><2><3><4><5><6>	There are six fields which represent different options. Field 1 – Specify WAN interface as failover WAN by typing 1 to 3. Field 2 – Enable / disable the action for the failover WAN. Such action is “Active When selected WAN [disconnect/reached traffic

	threshold]". 0 – Disable 1 - Enable Field 3 - Enable / disable the action for the failover WAN. Such action is "Active When [any/all] of selected WAN disconnect or reached traffic threshold". 0 – Disable 1 - Enable Field 4 – Specify main WAN by typing 1 to 3. The main WAN will be set to always on. Field 5 – Specify traffic threshold [Download threshold(Kbps)]. Field 6 - Specify traffic threshold [Upload threshold (Kbps)]. For example, WAN 2 will be set as failover, and will be active when any of selected WANs has reached traffic threshold. WAN 3 is the selected WAN. Download threshold : 50 Kbpsl; Upload threshold : 20 Kbps. You can type as follows: *wan failover on 2 1 0 3 50 20*
show <index>	Display parameters settings for WAN interface. index – Ranges from 1 to 4.

Example

```
> wan failover on 2 1 0 3 50 20
> wan failover show 2
  wan2 Active Mode : Failover
       Active when : Any of the selected WANs reached the Traffic Threshold
       Traffic Download Threshold : 50 Kbps
       Traffic Upload Threshold   : 20 Kbps
>
```

Telnet Command: hsportal

This command is used to configure a profile (Hotspot Web Portal) with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router.

Syntax

hsportal setup -p *<profile> [-l <lan>] [-s <ssid>] …*

hsportal setup -p *<profile> -c*

Syntax Description

Parameter	Description
-p <profile>	Indicate available profile to be configured. <profile>: Enter the index number (1 to 4) of the profile.

-l	Apply to LAN interfaces (1 to 8). For example: hsportal setup -p 1 -l 1, 2 (apply LAN1 and LAN2)
-s	Apply to WLAN interfaces (1 to 4). For example: hsportal setup -p 1 -s 1, 2 (apply SSID1 and SSID2)
-a	Apply to WLAN5G interfaces (1 to 4). For example: hsportal setup -p 1 -a 1, 2 (apply SSID1 and SSID2)
-m	Select login mode. 0: skip 1: click 2: social 3: pin 4: social or pin For example: hsportal setup -p 1 -m 0
-f <0/1>	It menas to enable or disable the function of Configure facebook login. 0: disable. 1: enable.
-g <0/1>	It menas to enable or disable the function of Configure google login. 0: disable. 1: enable.
-h <0/1>	It menas to enable or disable the function of HTTPS redirection. 0: disable. 1: enable.
-v <0/1>	It menas to enable or disable the function of portal detection. 0: disable. 1: enable.
-i <string>	It means to set APP ID. <string>: Enter a string as APP ID. For example, to configure facebook APP id, you can type: > hsportal set -p 1 -f 1 -i this_is_app_id Profile 1 set facebook login enabled … [OK] Profile 1 set API ID … [OK]
-k <string>	It means to set APP key. <string>: Enter a string as APP key. For example, to configure google APP key, you can type: > hsportal set -p 1 -g 1 -k keyforapp Profile 1 set google login enabled … [OK] Profile 1 set API KEY … [OK]
-r <0/1/2>	It means to set landing page mode. 0: fixed URL. 1: user request. 2: bulletin. For example, > hsportal set -p 1 -r 0 Profile 1 set landing page mode 0 … [OK]
-e	It means to enable the specified profile.
-d	It means to disable the specified profile.
-c <1/2/3/4>	Reset the specified profile. <1/2/3/4>: Enter the index number of profile.

	For example, > hsportal set -p 1 -c Reset profile 1 ... [OK]
-o	Clear profiles for all clients.
-t <value>	Set the expire time for the specified profile. <value>: Enter a number of time period (unit: minutes). For example, k> hsportal setup -p 1 -t 300 Profile 1 set expire time 300 mins ... [OK]

Example

```
> hsportal setup -p 1 -c
Reset profile 1 ... [OK]
> hsportal setup -p 1 -r 0
Profile 1 set landing page mode 0 ... [OK]
> hsportal setup -p 2 -g 1 -k app_key_google
Profile 2 set google login enabled ... [OK]
Profile 2 set API KEY  ... [OK]
>
```

Telnet Command: hsportal level

This command allows the user to configure bandwidth and sessions quota which is only applicable to the web portal clients.

Syntax

hsportal level *-p <index> [-e <enable>] [-t <mins>] …*

Syntax Description

Parameter	Description
-p <index>	It means to specify (add) a quota policy profile. <index>: Enter the index number (1 to 20) of the quota policy profile.
-e <0/1>	It means to enable or disable the quota policy profile. 0: disable. 1: enable.
-t <value>	It means to set expired time for quota policy. <value>: Enter a number (unit:minutes).
-i <0/1> -o <value>	It means to enable or disable the function of idle timeout 0: disable. 1: enable. If enabled, -o <value>: Set the idle timeout (unit:minutes) if idle timeout is enabled. For example: hsportal level -p 1 -e 1 -i 1 -o 300
-d <value>	It means to set the maximum number of devices that can be connected to the network using the same account. <value>: Enter a number (0 to 100). "0" means unlimited. For example: hsportal level -p 1 -e 1 -d 0

-b <0/1>	It means to enable or disable the function of bandwidth limit. 0: disable. 1: enable.
-ru <0/1>	It means to specify the bandwidth limit download unit. 0: kbps 1: mbps
-tu <0/1>	It means to specify the bandwidth limit upload unit. 0: kbps. 1: mbps.
-s <0/1>	It means to enable or disable the session limit. 0:disable. 1:enable.
-n <value>	It means to set a maximum session limit. <value>: Enter a value (0 to 6000). For example: hsportal level -p 1 -s 1 -n
-U <kbps/mbps>	It means to specify the bandwidth upload limit. kbps mbps
-D <kbps/mbps>	It means to specify the bandwidth download limit. kbps mbps
-c <index>	It means to delete a quota policy profile. <index>: Enter the index number (1 to 20) of the quota policy profile.
-r <0/1>	It means to enable or disable the function of reconnection time restriction. 0:disable. 1:enable.
-f <value>	It means to set a period of time to block the same user reconnecting to the network. <value>: Enter a number (1 to 1439 minutes). For example: hsportal level -p 1 -e 1 -r 1 -f 300
-g <value>	It means to set a reconnection time to block the same user from reconnecting before the set time. <value>: Enter the hour (01 to 23) and the minutes (0~59) (unit: minutes). For example: hsportal level -p 1 -e 1 -r 1 -f 23:15 (The same user can reconnect after 23:15 every day)

Example

```
> hsportal level -p 1 -e 1 -r 1 -f 30000
>
```

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*> <*isolate*>

wl acl del <*MAC*>

wl acl mode <*ssid1 ssid2 ssid3 ssid4*> <*white/black*>

wl acl show

wl acl showmode

wl acl clean

Syntax Description

Parameter	Description
enable <ssid1 ssid2 ssid3 ssid4>	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable <ssid1 ssid2 ssid3 ssid4>	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add <MAC> <ssid1 ssid2 ssid3 ssid4> <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
del <MAC>	It means to delete a MAC address entry defined in the access control list.
mode <ssid1 ssid2 ssid3 ssid4> <white/black>	It means to set white/black list for each SSID.
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 showmode
 SSID1: None
 SSID2: None
 SSID3: None
 SSID4: None
> wl acl add 00-50-70-ff-12-70 ssid1 ssid2 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          14:49:bc:0a:8a:b8   SSID1 SSID2

 s: Isolate the station from LAN
>
```

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 channel show

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*>/ *show*

wl config beaconperiod <*value*> / *show*

wl config radio <*1/0*>/*show*

wl config frag <*value*>/ *show*

wl config rts <*value*> / *show*

wl config rate_alg <*value*> / *show*

wl config country <*value*> / *show*

Syntax Description

Parameter	Description
mode <value>	It means to select connection mode for wireless connection. Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
mode show	It means to display what the current wireless mode is.
channel <number>	It means the channel of frequency of the wireless LAN. The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13. number=0, means Auto number=1, means Channel 1 …. number=13, means Channel 13.
channel show	It means to display what the current channel is.
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. 0: disable to use long preamble. 1: enable to use long preamble.
preamble show	It means to display if the current preamble is enabled or not.
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. 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:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *ssid_name*: Give a name for the specified SSID. *hidden_ssid*: Type 0 to hide the SSID or 1 to display the SSID
security <SSID_NUMBER><mode><key ><index>	It means to configure security settings for the wirelesss connection. *SSID_NUMBER*: Type 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, index*: Moreover, 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.
ratectl <ssid_num enable upload download>	It means to set the rate control for the specified SSID. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. *upload*: It means to configure the rate control (from 1kbps to 300 kbps) for data upload. The unit is kbps. *download*: It means to configure the rate control (from 1kbps to 300 kbps) 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:* Choose 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> / show	Set the DTIM value. value: 1 to 255 show: Display the DTIM setting.
beaconperiod <value> / show	Set the beaconperiod value. value: 20 to 1023 (milli-second) show: Display the beaconperiod etting.
radio <1/0>/show	Enble or disable the wireless radio. 1/0: Type 1 to enable; 0 to disable. show: Display the radio setting.
frag<value>/ show	Set the fragment value. value: 256 to 2346 show: Display the fragment setting.
rts <value> / show	Set the RTS value. value: 1 to 2347

	show: Display the RTS setting.
rate_alg <value>/ show	Set the algorithm for ALG rate. value: 0 for old algorithm; 1 for new algorithm. show: Display the ALG rate setting.
country <value>/ show	Set the country code for a country. value: two capital letters, e.g., TW, UK show: Display the country cod setting.

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)
```

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>	It means to Enter the SSID for the router. The maximum character that you can use is 32.
<CHAN<En>	It means to specify required channel for the router. *CHAN:* The range for the number is between 1 ~ 13. *En*: type *on* to enable the function; type *off* to 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. 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. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl stamgt

This command is used to configure connection time and reconnection time for each SSID that wireless client used for accessing into Internet.

Syntax

wl stamgt *<enable/disable> <ssid_num>*

wl stamgt *show <ssid_num>*

wl stamgt *set <ssid_num> <c> <r>*

wl stamgt *reset <ssid_num>*

Syntax Description

Parameter	Description
<enable/disable>	It means to enable/disable the station management control.
<ssid_num>	It means channel selection. Available channel for 2.4G: 0/1/2/3 Available channel for 5G: 4/5/6/7.
show	It means to display status or configuration of the selected channel.
c	It means connection time. The unit is minute.
r	It means reconnection time. The unit is minute.

Example

```
> wl stamgt enable 1
% Station Management Status: enabled
> wl stamgt set 1 60 60
> wl stamgt show 1
NO. SSID           BSSID            Connect time  Reconnect time
1.  Draytek      00:11:22:aa:bb:cc  0d:0:58:26      0d:0:0
```

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	It means the number of SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
En	It means 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	It means to set WMM for access point.
bss	It means to set WMM for wireless clients.
ack	It means to map to the Ack policy settings of AP WMM.
enable	It means to enable the WMM for each SSID. 0: disable 1: enable
Apsd [value]	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable
show	It displays current status of WMM.
QueIdx	It 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	It controls how long the client waits for each data transmission.
Cwmin/ Cwmax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Specify the value ranging from 1 to 15.
Txop	It means transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```
> wl wmm ap 0 3 4 6 0 0
 QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm enable 1 0 1 0
 WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
 Enable WMM: SSID0 =1, SSID1 =0,SSID2 =1,SSID3 =0
 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
wl ht bw value	The value you can type is 0 (for BW_20), 1 (for BW_20_40) and 2 (BW_40).
wl ht gi value	The value you can type is 0 (for GI_800) and 1 (for GI_400)
wl ht badecline value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht autoba value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht rdg value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht msdu value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht txpower value	The value you can type ranges from 1 – 6 (level).
wl ht antenna value	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
wl ht greenfield value	The value you can type is 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 <*value*>

wl wds flush

Syntax Description

Parameter	Description
mode <*value*>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeapter
security <*value*>	It means to configure security mode with encrypted keys for WDS. *mode*: 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: 1 – enable the function. 0 – disable the function.

hello <value>	It means to send hello message to remote end (peer). Value: 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 <ndex addr>	add *[index addr]* – Add the peer MAC entry in Repeater/Bridge WDS MAC table.
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*>	0: disable 1: enable

Example

```
> wl btnctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

Telnet Command: wl iwpriv / wl efuse

This command is reserved for RD debug. Do not use them.

Telnet Command: wl stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

wl stalist

wl stalist num

wl stalist neighbor

wl stalist validtime <*time*>

wl stalist maxnum <*num*>

Syntax Description

Parameter	Description
num	Display the wireless station list.
neighbor	Diplay the number of the wireless stations.
valildtime <*time*>	Set the valid time (0 to 300000) of neighbor station list.
maxnum <*num*>	Set the maximum number (10 to 512) of neighbor station list.

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: wl bndstrg

This command allows users to configure settings for Band Steering (2.4GHz).

Syntax

wl bndstrg show

wl bndstrg enable <*1/0*>

wl bndstrg chk_time <*value*>

Syntax Description

Parameter	Description
show	Display current status for Band Steering function.
enable <*1/0*>	It means to enable wireless 2.4GHz AP client mode. 1 – enable 0 – disable

chk_time <value>	If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for Vigor router to detect the wireless client. *<value>– 1 to 60 seconds.*

Example

```
> wl bndstrg show
band steering: disable
chk_time: 15 sec
> wl bndstrg chk_time 50 30
argv[0]:chk_time, argv[1]:50, argv[2]:30

%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

Telnet Command: wl artfns

This command allows users to configure airtime fairness function for wireless (2.4GHz) connection.

Syntax

wl artfns enable *<value>*

wl artfns trg_num *<value>*

wl artfns show

Syntax Description

Parameter	Description
enable <value>	It means to enable wireless airtime fairness function. 1 – enable 0 – disable
trg_num <value>	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
show	Display current status (enable or disable) and triggering client number for airtime fairness function.

Example

```
> wl artfns enable 1
> wl artfns trg_num 3
> wl artfns show
airtime fairness: enable
trg_num: 3
>
```

Telnet Command: wl drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl drayrs *set <mode><rs_low><rs_low_security><delta>*

wl drayrs *restart*

wl drayrs *show*

Syntax Description

Parameter	Description
set <mode> <rs_low> <rs_low_security> <delta>	Select a mode for roaming. 0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI rs_low – Set a value of Strictly Minimum RSSI (62~86). rs_low_security – Set a value of Minimum RSSI (62~86). delta – Set a value of Adjacent AP RSSI (1~20).
restart	Restart to activate roaming function.
show	Dispaly current configuration of roaming function.

Example

```
> wl drayrs show
% Mode : Disable
%  rs_low         : -73
%  rs_low_secure  : -66
%  delta          : 5
>
```

Telnet Command: wl_dual acl

This command allows the user to configure wireless (5GHz) access control settings.

Syntax

wl_dual acl enable *<ssid1 ssid2 ssid3 ssid4>*

wl_dual acl disable *<ssid1 ssid2 ssid3 ssid4>*

wl_dual acl add <*MAC><ssid1 ssid2 ssid3 ssid4><isolate>*

wl_dual acl del <*MAC>*

wl_dual acl mode *<ssid1 ssid2 ssid3 ssid4> <white/black>*

wl_dual acl show

wl_dual acl showmode

wl_dual acl clear

Syntax Description

Parameter	Description
enable <ssid1 ssid2 ssid3 ssid4>	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable <ssid1 ssid2 ssid3 ssid4>	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add <MAC><ssid1 ssid2 ssid3 ssid4><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 *isolate*: It means to isolate the wireless connection of the wireless client (identified with the MAC address) from LAN.
del **<***MAC***>**	It means to delete a MAC address entry defined in the access control list. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
mode <ssid1 ssid2 ssid3 ssid4> <white/black>	It means to set white/black list for each SSID.
show	It means to display current status of access control.
showmode	It means to show the mode for each SSID.
clear	It means to clear all of the access control settings.

Example

```
> wl_dual acl showmode
 SSID1: None
 SSID2: None
 SSID3: None
 SSID4: None
> wl_dual acl add 14-49-BC-0A-8A-B8 ssid1 ssid2 isolate
 Set Done !!
> wl_dual acl show
 ----------Enable Mac Address Filter---------
 SSID1: Disable SSID2: Disable SSID3: Disable SSID4: Disable
 ----------MAC Address Filter----------
 Index   Attribute      MAC Address        Associated SSIDs
   1       s          14:49:bc:0a:8a:b8   SSID1 SSID2

 s: Isolate the station from LAN
```

Telnet Command: wl_dual apscan

This command is used to scan Access Point installed near the location of Vigor router.

Syntax

wl_dual apscan *start*

wl_dual apscan *show*

Syntax Description

Parameter	Description
start	It means to execute the AP scanning.
show	It means to display the content of the AP list.

Example

```
> wl_dual apscan start
> wl_dual apscan show
 AP scan is ongoing.
> wl_dual apscan ?
% wl_dual apscan [start/show]
% start: do AP scan
% show: show AP list

> wl_dual apscan show
5G Access Point List :
BSSID            Channel   SSID
```

Telnet Command: wl_dual config

This command allows users to configure general settings and security settings for wireless connection (5GHz).

wl_dual config enable <*value*>

wl dual config enable show

wl_dual config mode <*value*>

wl_dual config mode show

wl_dual config channel <*number*>

wl_dual config channel show

wl_dual config preamble <*enable*>

wl_dual config preamble show

wl_dual config ssid <*ssid_num enable ssid_name*>

wl_dual config ssid hide <*ssid_num enable*>

wl_dual config ssid show

wl_dual config ratectl <*ssid_num enable upload download*>

wl_dual config ratectl show

wl_dual config isolate lan <*ssid_num enable*>

wl_dual config isolate member <*ssid_num enable*>

wl_dual config isolate vpn <*ssid_num enable*>

wl_dual config isolate show

wl_dual config frag <*value*>

wl_dual config frag show

wl_dual config rts <*value*>

wl_dual config rts show

wl_dual config country <*value*>

wl_dual config txpower <*value*>

wl_dual config nss <*value*>

Syntax Description

Parameter	Description
enable <value>	It means to enable/disable the 5GHz wireless function. 1: enable 0: disable
show	It means to display if 5G wireless function is enabled or not.
mode <value>	It means to select connection mode for wireless connection. Available settings are: "11a", "11n_5g", "11n" and "11an".
mode show	It means to display what the current wireless mode is.
channel <number>	It means the channel of frequency of the wireless LAN. The available settings are: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140. number=0, means Auto number=36, means Channel 36 ….

	Number=52, means Channel 52.
channel show	It means to display what the current channel is.
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. 0: disable to use long preamble. 1: enable to use long preamble.
preamble show	It means to display if preamble is enabled or not.
ssid <ssid_num enable ssid_name>	It means to set the name of the SSID, hide the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *ssid_name*: Give a name for the specified SSID.
ssid hide <ssid_num enable>	It means to hide the name of the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. enable: Type 0 to hide the SSID or 1 to display the SSID.
ssid show	It means to display a table of SSID configuration.
ratectl <ssid_num enable upload download>	It means to set the rate control for the specified SSID. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. *upload*: It means to configure the rate control for data upload. The unit is kbps. *download*: It means to configure the rate control for data download. The unit is kbps. (example: *`wl dual config ratectl 1 1 25 25`*)
ratectl show	It means to display the data transmission rate (upload and download) for SSID1, SSID2, SSID3 and SSID4.
isolate lan <ssid_num enable>	It means to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable
isolate member <ssid_num enable>	It means to isolate the wireless connection from Member. It can make the wireless clients (stations) with the same SSID not accessing for each other. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable.
isolate vpn <ssid_num enable>	It means to isolate the wireless connection from VPN. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable.
isolate show	It means to display the status of wireless isolation.
frag <value>	It means to set the fragment threshold. value: Enter a number (256 to 2346).
frag show	It means to display current value of fragment threshold.
rts <value>	It means to set the RTS threshold. value: Enter a number (1 to 2347).
rts show	It means to display current value of RTS threshold.

country <*value*>	It means to set the country code. Each country will be represented with two digits. value: Enter two capital letters (e.g., TW, UK, CN..)
txpower <*value*>	It means to set TX power. Value: Enter a number (1 to 6).
nss <*value*>	It means to set NSS. Value: Enter a number (0 to 4).

Example

```
> wl_dual config mode 11a
 Current mode is 11a
% <Note> Please restart 5G wireless after you set the channel
> wl_dual config channel 60
 Current channel is 60
% <Note> Please restart 5G wireless after you set the channel.
> wl_dual config preamble 1
Long preamble is enabled
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual config ssid 1 enable dray
SSID  Enable  Hide_SSID  Name
 1    1      0         dray
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual config ssid show
 SSID  Enable  Hide_SSID  Name
 1    1      0         dray
 2    0      0         DrayTek_5G_Guest
 3    0      0
 4    0      0
>
```

Telnet Command: wl_dual restart

This command allows you to restart wireless setting (5GHz).

Example

```
> wl_dual restart

 5G wireless restart.................
```

Telnet Command: wl_dual security

This command allows users to configure security settings for the wireless connection (5GHz).

Syntax

wl_dual security <*SSID_NUMBER*> <*mode*> <*key*> <*index*>

wl_dual security show

Syntax Description

Parameter	Description
Security <*SSID_NUMBER*> <*mode*> <*key*> <*index*>	*SSID_NUMBER*: Type 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, index: Moreover, 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.	
show	It means to display current mode selection for each SSID.	

Example

```
> wl_dual security 1 wpa2psk 123456789e
% <Note> Please restart 5G wireless after you set the parameters.

> wl_dual security show
%% 5G Wireless LAN Security Settings:
% SSID1
%%  Mode: WPA2/PSK
% SSID2
%%  Mode: Disable
% SSID3
%%  Mode: Disable
% SSID4
%%  Mode: Disable
```

Telnet Command: wl_dual stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

wl_dual stalist

wl_dual stalist num

wl_dual stalist neighbor

wl_dual stalist validtime <*time*>

wl_dual stalist maxnum <*num*>

Syntax Description

Parameter	Description
num	Display the wireless station list.
neighbor	Diplay the number of the wireless stations.
valildtime <*time*>	Set the valid time (0 to 300000) of neighbor station list.

maxnum <num>	Set the maximum number (10 to 512) of neighbor station list.

Example

```
> wl_dual stalist
5G 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: wl_dual wds

This command allows users to configure WDS for wireless connection (5GHz).

Syntax

wl_dual wds mode <*value*>

wl_dual wds security <*value*>

wl_dual wds ap <*value*>

wl_dual wds hello <*value*>

wl_dual wds status

wl_dual wds show

wl_dual wds mac add <*index addr*>

wl_dual wds mac clear/disable/enable <*index/all*>

wl_dual wds flush

Syntax Description

Parameter	Description
mode <*value*>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeapter
security <*value*>	It means to configure security mode with encrypted keys for WDS. *mode*: 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: 1 – enable the function. 0 – disable the function.
hello <*value*>	It means to send hello message to remote end (peer). Value: 1 – enable the function. 0 – disable the function.
status	It means to display WDS link status for 5GHz connection.
show	It means to display current WDS settings.
mac add <*index addr*>	**add** <*index addr*> – Add the peer MAC entry in Repeater/Bridge WDS MAC table.
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_dual wds status
Please enable WDS hello function first.

> wl_dual wds hello 1
% <Note> Please restart router after you set the parameters.
> wl_dual wds security wep
% Please configure WEP key set in Security Settings.
% <Note> Please restart router after you set the parameters.
> wl_dual wds show
Mode : Disable
Security : WEP
> wl_dual wds wep 12345
% <Note> Please restart router after you set the parameters.
```

Telnet Command: wl_dual wps

This command allows users to configure WPS for wireless connection (5GHz).

Syntax

wl_dual wps enable <*value*>

wl dual wps pbc

wl_dual wps pin <*code*>

wl_dual wps show

Syntax Description

Parameter	Description
enable <value>	It means to enable WPS. 1 – enable

	0 – disable
pbc	It means to start WPS by pressing the WLAN ON/OFF WPS button on Vigor router.
pin <code>	It means to start WPS by using client PIN code. code: Client PIN code (digit number).
show	It means to display current WPS settings.

Example

```
> wl_dual wps enable 1
 WPS is enabled.
> wl_dual wps pin 88563337
 WPS has triggered by PIN code.
 The AP will wait for WPS request from your client for 2 minutes...
```

Telnet Command: wl_dual artfns

This command allows users to configure airtime fairness function for wireless (5GHz) connection.

Syntax

wl_dual artfns enable *<value>*

wl_dual artfns trg_num <*value***>**

wl_dual artfns show

wl_dual artfns status

Syntax Description

Parameter	Description
enable **<***value***>**	It means to enable wireless airtime fairness function. 1 – enable 0 – disable
trg_num **<***value***>**	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
show	Display current status (enable or disable) and triggering client number for airtime fairness function.
status	Display whether the function of airtime fairness is enabled or disabled.

Example

```
> wl_dual artfns show
airtime fairness for 5G: disable
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!

> wl_dual artfns enable 0
> wl_dual artfns trg_num 2
> wl_dual artfns show
airtime fairness for 5G: disable
```

```
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!
```

Telnet Command: wl_dual drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl_dual drayrs *set <mode><rs_low><s_low_security><delta>*

wl_dual drayrs *restart*

wl_dual drayrs *show*

Syntax Description

Parameter	Description
Set <mode> <rs_low> <s_low_security> <delta>	Select a mode for roaming. 0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI rs_low – Set a value of Strictly Minimum RSSI (62~86). rs_low_security – Set a value of Minimum RSSI (62~86). delta – Set a value of Adjacent AP RSSI (1~20).
restart	Restart to activate roaming function.
show	Dispaly current configuration of roaming function.

Example

```
> wl_dual drayrs show
% Mode : Disable
%  rs_low         : -73
%  rs_low_secure  : -66
%  delta          : 5
> wl_dual drayrs set 1 68 66 2
> wl_dual drayrs show
% Mode : Strictly Minimun RSSI
%  rs_low        : -68
%  rs_low_secure  : -66
%  delta         : 2
```

Telnet Command: wol

This command allows Administrator to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

wol up *<MAC Address>*

wol fromWan *<on/off/any>*

wol fromWan_Setting *<idx><ip address><mask>*

Syntax Description

Parameter	Description

<MAC Address>	It means the MAC address of the host.
<on/off/any>	It means to enable or disable the function of WOL from WAN. on: enable off: disable any: It means any source IP address can pass through NAT and wake up the LAN client. This command will allow the user to choose whether WoL packets can be passed from the Internet to the LAN network from a specific WAN interface.
<idx><ip address><mask>	It means the index number (from 1 to 4). These commands will allow the user to configure the LAN clients that the user may wake up from the Internet through the use of the WoL packet. *ip address* - It means the WAN IP address. *mask* - It means the mask of the IP address.

Example

```
> wol fromWan on
% wol fromWan: on
> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
% wol fromWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Telnet Command: user

The command is used to create new user account profiles.

Syntax

user set <*-a*|*-b*|*-c*|*-d*|*-e*|*-l*|*-o*|*-q*|*-r*|*-s*|*-u*>

user edit <*PROFILE_IDX*>
<*-a*|*-d*|*-e*|*-f*|*-i*|*-o*|*-m*|*-n*|*-p*|*-q*|*-r*|*-s*|*-t*|*-u*|*-v*|*-w*|*-x*|*-A*|*-H*|*-T*|*-P*|*-l*|*-L*|*-D*>

user account <*USER_NAME*><*-t*|*-d*|*-q*|*-r*|*-w*>

user setdefault

Syntax Description

Parameter	Description
set	It means to configure general setup for the user management.
edit	It means to modify the selected user profile.
account	It means to set time and data quota for specified user account.
User Set	
-a <Profile idx> <User name><IP_Address>	It means to pass an IP Address. Profile idx- type the index number of the selected profile. User name- type the user name that you want it to pass. IP_Address- type the IP address that you want it to pass.
-b <user name> *-b ip <ip address>*	Block specifies user or IP address. *user name* – type the user name that you want to block. *ip address* — type the IP address that you want to block.
-c <user name> *-c all*	Clear the user record. *user name* – type the user name that you want to get clear corresponding record. *all* – all of the records will be removed.
-d	Enable the User management in Rule-Based mode.
-e	Enable the User management in User-Based mode.
-l all *-l user* *-l ip*	Show online user. *all* – all of the users will be displayed on the screen. *user name* – type the user name that you want to view on the screen. *ip* – type the IP address that you want to view on the screen.
-o	It means to show user account information. e.g.,*-o*
-q	It means to trigger the alert tool to do authentication.
-r <user name | all>	Remove the user record. *user name* – type the name of the user profile. *all* – all of the user profile settings will be removed.
-s <0/1>	It means to set login service. 0:HTTPS 1:HTTP e.g.,*-s 1*
-u user <user name> *-u ip <ip address>*	Unblock specifies user or IP address. *user name* – type the user name that you want to unblock. *ip address* — type the IP address that you want to unblock.

User edit	
PROFILE_IDX	Type the index number of the profile that you want to edit.
-a <0/1>	Enable(1) or disable(0) the internal RADIUS.
-d	Disable User profile function.
-e	Enable User profile function.
-f <0/1>	Enable(1) or disable(0) the local 802.1x user.
-i <0-255>	It means to set idle time (from 0 to 255, 0 means unlimited). e.g., *-i 60*
-o <0-65535>	It means to set auto-logout (from 0 to 65535, 0 means unlimited).
-m <0-2000>	It means to set the maximum (from 0 to 2000) login user number. e.g., *-m 200*
-n <param>	It means to set a user name for a profile. Param: Enter a string, e.g.,*-n fortest.*
-p <param>	It means to configure user password. Param: Enter a string, e.g., *-p 60fortest.*
-q <param>	It means to set time quota (0-65535) of the user profile. Param: Enter a value, e.g., *-q 200.*
-r <param>	It means to set data quota. Param: Enter a value, e.g., *-r 1000.*
-s <sch_idx1,sch_idx2,sch_idx3 , and sch_idx4>	It means to set schedule index. Available settings are" sch_idx1,sch_idx2,sch_idx3, and sch_idx4.
-t <0/1>	It means to enable /disable time quota limitation for user profile 0:Disable 1:Enable
-u <0/1>	It means to enable /disable data quota limitation for user profile 0:Disable 1:Enable
-v	It means to view user profile(s).
-w <MB/GB>	It means to specify the data quota unit (MB/GB). e.g., -w MB
-x <0-3>	It means to set external server authentication 0: None 1: LDAP 2: Radius 3: TACAS e.g., *-x 2*
-l <0-3>	It means to set log type. 0:None 1:Login 2:Event 3:All
-P <0/1>	It means to enable /disable pop browser tracking window for user profile 0:Disable 1:Enable
-T <0/1>	It means to enable /disable authentication by telnet.

	0:Disable 1:Enable
-H <0/1>	It means to enable /disable authentication by web page. 0:Disable 1:Enable
-A <0/1>	It means to enable /disable authentication by alert tool. 0:Disable 1:Enable
-L <index>	It means to set active directory / LDAP profiles. Index: Specify the index number (profile_idx1 to profile_idx8) of the profile.
-D	It means to list all active directory / LDAP profiles.
-O <0/1>	It means to reset the quota automatically. 0:Disable 1:Enable
-Q <param>	It means to set the default time quota. param: Enter a number (1 to 65535).
-R <param>	It means to set the default data quota. param: Enter a number (1 to 65535).
-M <param>	It means to set the default quota type. 0: when login permission schedule expired. 1: at the start time of schedule.
I <param>	It means to specify the default quota schedule index to perform the job at the start time.
-S	It means to display the reset default quota type and the schedule index.
User account	
USER_NAME	It means to type a name of the user account.
-d<0/1>	It means to enable /disable data quota limitation for user account. 0:Disable 1:Enable
-q	It means to set account time quota. e.g., *-q 200*
-r	It means to set account data quota. e.g., *-r 1000*
-t <0/1>	It means to enable /disable time quota limitation for user account. 0:Disable 1:Enable
-w	It means to set data quota unit (MB/GB).

Example

```
> user account admin -d 1

 Enable the [admin] data quota limited
```

Telnet Command: appqos

The command is used to configure QoS for APP.

Syntax

appqos view

appqos enable <*0/1***>**

appqos traceable <*-v | -e AP_INDEX CLASS | -d AP_INDEX***>**

appqos untraceable <*[-v | -e AP_INDEX CLASS | -d AP_INDEX***>**

Syntax Description

Parameter	Description
view	It means to display current status of APP QoS.
enable **<***0/1***>**	It means to enable or disable the function of APP QoS.
traceable/ untraceable	The APPs are divided into traceable and untraceable based on their properties.
-v	It means to view the content of all traceable APs. Use "appqos traceable –v" to display all of the traceable APS with speficed index number. Use "appqos untraceable –v" to display all of the untraceable APS with speficed index number.
-e	It menas to enable QoS for application(s) and assign QoS class.
AP_INDEX	Each index number represents one application. Index number: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 are used for 13 traceabel APPs. Index number: 0~49, 55~59, 61, 67, 69, and 70~123 are used for 125 untraceable AP.
CLASS	Specifies the QoS class of the application, from 1 to 4 1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class
-d	It means to disable QoS for application(s).

Example

```
> appqos enable 1

APP QoS set to Enable.
> appqos traceable -e 68 2

TELNET: ENABLED, QoS Class 2.
```

Telnet Command: nand bad /nand usage

"NAND usage" is used to display NAND Flash usage; "nand bad" is used to display NAND Flash bad blocks.

Syntax

nand bad

nand usage

Example

```
>nand usage
Show NAND Flash Usage:
Partition   Total         Used          Available      Usecfg        419
4304       16768         4177536         0bin_web     33554432      181
20754      15433678       54cfg-bak     4194304       16768         417
7536         0bin_web-bak  33554432      18120754      15433678       54
> nand bad
Show NAND Flash Bad Blocks:
Block   Address        Partition
1020    0x07f80000     unused
1021    0x07fa0000     unused
1022    0x07fc0000     unused
1023    0x07fe0000     unused
```

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 Vigor2135.

Syntax

apm enable

apm disable

apm show

apm clear

apm discover

apm query

Syntax Description

Parameter	Description
enable	It means to enable APM function.
disable	It means to disable APM function.
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 Vigor2135. Information related to the registered AP will be send back to Vigor2135 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	It is used to copy the same parameters settings from one profile to another APM profile.
del	It is used to delete a specified APM profile. The default (index #1) should not be deleted.
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	It is used to display specified APM profile.
apply	It is used to apply the selected APM profile onto specified VigorAP.
<*from index*>	Type an index number in this field. It is the original APM profile to be cloned to other APM profile.
<*to index*>	Type an index number in this file. It is the target profile which will clone the parameters settings from an existed APM profile.
<*new name*>	Type a name for a new APM profile.
<*profile index*>	Enter the index number of existed profile.
client index1/2/3/4/5	It is useful for applying the selected APM profile 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          - /     -
>
```

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 Vigor2135.
clear	It means to remove the information related to VigorAP registered Vigor2135.

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*>	It means to set the load balance configuration file for APM.
show	It shows the configuration value.
<*value*>	You need to type 10 numbers in this field. Each number represents different setting value. [1] – The first number means the load balance function. Type 1 – enable load balance, 0 – disable load balance. [2] – The second number means the station limit function. Type 1 –enable station limit, 0 – disable station limit. [3] – The third number means the traffic limit function. Type 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. Type 1 – enable upload limit, 0 – disable upload limit. [6] – The sixth number means the download limit function. Type 1 – enable download limit, 0 – disable download limit. [7] – The seventh number means disassociation by idle time. Type 1 – enable disassociation, 0 – disable disassociation. [8] – The eighth number means to enable or disable disassociation by signal strength. Type 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] - The 11th number means to set the RSSI threshold (from -200 to -50 dbm).

Example

```
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 0
2. Enable station limit : 0
3. Enable traffic limit : 0
4. limit Number : 64
5. Upload limit : 0
6. Download limit : 0
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength : 0
9. Traffic limit unit (upload)   : 0
10.Traffic limit unit (download) : 0
flag : 0
> apm lbcfg set 1 1 0 15 0 0 0 0 1 1
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 1
2. Enable station limit : 1
3. Enable traffic limit : 0
4. limit Number : 15
5. Upload limit : 0
6. Download limit : 0
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength : 0
9. Traffic limit unit (upload)   : 1
```

```
10.Traffic limit unit (download) : 1
flag : 49
```

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: fw_backupmode

This command is used to backup the firmware to the router. The firmware will be retrieved for rebooting Vigor router after it crashes over three times.

Syntax

backupmode *[<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 n	Set the backup time. n : 1 ~ 168 hours
-m n	Set the firmware backup mode. n= 0 or 1. 1: Backup after timeout. 0: Backup after upgrade.
-b	Backup the firmware manually and immediately.
-r n	Set the firmware recovery mode. n= 0 or 1. 1: the firemware will be recovered when the system crash. 0: No recovery.

Example

```
> fw_backupmode -b

 Do Firmware backup now!!!.
```

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
> 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   : Vigor2135 Series
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 []
```

Index

3

3G/4G USB Modem, 65

3G/4G USB Modem (DHCP mode), 57

3G/4G USB Modem (PPP mode), 56

6

6rd Mode, 120

6rd Prefix, 120

6rd Prefix Length, 120

8

802.1x ports, 169

A

Access Control, 292

Access List, 468

Access Mode, 79

Access Mode-ADSL/VDSL2, 78

Access Mode-Etherenet / USB, 79

Access Tech, 277

Active Directory/LDAP, 205

Active Mode, 68, 71, 72, 75, 77

Active-Standby, 218

Additional Filter, 207

Address Mapping, 244, 261

ADSL/VDSL2, 70

Advance Mode, 396

Advanced Mode, 272

Advanced Setting, 299

Aggregation MSDU, 300

Airtime Fairness, 306

ake on LAN, 211

Always On, 99, 104, 111, 113, 114, 116, 117, 119, 120, 125

Analyze, 410

Anonymous, 205

Antenna, 301

AP Discovery, 105, 305

AP Maintenance, 572, 580

AP Map, 572, 581

APN Name, 56, 107, 109

APP Enforcement, 393, 402

APP Enforcement Filter, 415

APP Enforcement Profile, 416

APP QoS, 491

APPE Module Version, 418

APPE Signature Upgrade, 418

Applications, 183

APSD Capable, 301

ARP Cache Table, 667

ARP Detect, 82, 84, 89, 92, 96, 99, 104, 107, 109, 124

ARP Table, 166

ATM QoS, 124

Authentication, 203

Authentication Information, 683

Authentication Key, 219

Authentication Mode, 296

Authentication Port, 202

Authentication Type, 169

Auto Adjustment, 304

Auto detect, 35

Auto Logout, 20

Auto-Update interval, 186

Aux. WAN IP, 178

B

Backup, 166

Band Steering, 308

Bandwidth Limit, 481

Bandwidth Management, 304, 481

Base Distinguished Name, 207

Beacon Period, 588

Bind IP to MAC, 165

Bind to WAN, 338

Bind Type, 205

Bogus DNS Reply, 195

Bonjour, 214

Bridge Mode, 85, 93, 100, 116, 118

Bridge Subnet, 93, 100, 116, 118

Brute Force Protection, 466

C

Cache, 425

Call Direction, 354

Call Filter, 388

Certificate Backup, 385

Change the TTL value, 97, 101

Channel, 284, 289

Channel Bandwidth, 300

Choose IP, 176

Comment, 166, 178

Common Name Identifier, 207

Config Backup, 29

Config Sync, 220

Configuration Backup, 456

Connection Management, 366

Connectivity, 64

Country Code, 302

CPE Management, 554

CSV file, 644

Current System Time, 197

D

Dashboard, 23, 573

Data Coding Scheme, 274

Data Filter, 388

Data Flow Monitor, 673

Data Quota, 498

DataType, 79

Daylight Saving, 462

Days in a week, 198

Default Lifetime, 158

Default MAC Address, 82, 86, 90, 101

Default Preference, 158

Default Rule, 392

Destination IP, 252

Details - PPPoE/PPPoA, 88

Details Page, 79

Details-3G/4G USB Mdem(PPP mode), 106

Details-3G/4G USB Modem(DHCP mode), 108

Details-IP Routed Subnet, 154

Details-IPv6-6in4 Static Tunnel, 118

Details-IPv6-6rd, 120

Details-IPv6-AICCU, 114

Details-IPv6-DHCPv6 Client, 115

Details-IPv6-Offline, 110

Details-IPv6-PPP, 111

Details-IPv6-Static IPv6, 117

Details-IPv6-TSPC, 112

Details-LAN IPv6, 156

Details-LAN-DMZ, 152

Details-LAN-Ethernet, 148

Details-MPoA/Static or Dynamic IP, 84, 91

Details-PPPoE, 81, 96

Details-PPTP/L2TP, 102

Details-Static IP or Dynamic IP, 98

Details-Static or Dynamic IP, 104

Determine Real WAN IP, 188

DFS Restrictions, 282

DHCP, 47

DHCP Client Identifier, 86, 94

DHCP Server Configuration, 149, 152, 154

DHCP Server IP Address, 149, 152

DHCP Table, 669

DHCPv6 (Stateful), 156

DHCPv6 Server, 157

Diagnose, 196, 256

Diagnostic, 665

Dial-out Triggering, 665

Digital Signature, 350

Display Name, 72, 74, 76, 79

DMZ Host, 175

DNS Cache Table, 671

DNS Filter, 393

DNS Filter Profile, 428

DNS Security, 195

DNS Server, 196

DNS Server IP Address, 87, 95, 101, 150, 153

DNS Server IPv6 Address, 157

Domain, 196

Domain Diagnose, 196

Domain Name, 101, 255

DoS Defense, 389, 405, 408

DoS Flood Table, 685, 686

Download Limit, 304

DrayTek Banner, 403

DSL Mode, 70

DSL Modem Code, 70

DSL Status, 681

Dynamic DNS, 183, 185

Dynamic DNS Account, 187, 189

Dynamic IP, 104

E

Enable PING to keep alive, 99

Encapsulating, 92

Encapsulating Type, 88

Encapsulation, 124, 127

End IPv6 Address, 157

End Port, 179

ESP, 339

Event Code, 446

Event Log, 590

Extension WAN, 158

External Devices, 611

External RADIUS, 200

External TACACS+, 204

F

Failover, 71, 72, 75, 77

Failover to/Failback, 244

File Explorer, 653

File Extension Object, 631

Filter Setup, 395

Firewall, 388

Firmware Upgrade, 477

Fixed IP, 82, 90, 98, 103, 125

Force NAT /Force Routing, 253

Force Update, 185

Fragment Length, 301

G

Gateway IP Address, 86, 94, 101, 104, 149, 152

General Setup, 67

Google Map, 560

GRE, 357

Group ID, 210, 219

Guard Interval, 300

GUI Map, 27

H

Hardware Installation, 10

Hide SSID, 289

High Availability, 217

High Availability Status, 681

Host Name, 48

Hot-Standby, 218

I

Idle Timeout, 98, 103, 125

IGMP, 209

IGMP Proxy, 209

IGMP Snooping, 209

Incoming Port, 182

Incoming Protocol, 182

Indicators and Connectors, 2, 8

Installation, i

Interface, 253

Inter-LAN Routing, 148

Internal RADIUS, 201

Internal Service User List, 479

Internet Access, 78

IP (Internet Protocol), 65

IP address, 104

IP Address, 86, 94, 101, 103, 148, 152, 154

IP Address Assignment Method(IPCP), 103

IP Address List, 193

IP Based, 68

IP Bind List, 166

IP Filters, 388

IP Group, 618

IP Object, 615

IP Pool Counts, 149, 152, 154

IPsec General Setup, 338, 339

IPsec Peer Identity, 341

IPv4 Border Relay, 120

IPv4 Mask Length, 120

IPv6 Address, 117

IPv6 Gateway Address, 117

IPv6 Group, 622

IPv6 Neighbour Table, 668

IPv6 Object, 620

IPv6 TSPC Status, 680

Isolate, 289

ISP Access Setup, 82, 90, 96, 102

ISP Name, 125

K

Keep WAN Connection, 99

Keyword Group, 630

Keyword Object, 628

L

LAN, 144

LAN DNS / DNS Forwarding, 183, 191

LAN Port Mirror, 168

LAN to LAN, 352

Landing Page, 494

LAN-General Setup, 146

LDAP /Active Directory Setup, 183

Lease Time, 149, 152, 154

Line Speed, 67, 70, 72, 75, 76

Load Balance, 592

Load Balance for AP, 572

Load Balance Mode, 68

Load-Balance, 251, 259

Load-Balance /Route Policy, 251

Local 802.1X, 479

Local 802.1X General Setup, 222

Local Certificate, 323, 377

Local IP Address, 178

Log, 421

Log & Alert, 562

Login, 61

Login Page Greeting, 454

Logout, 29

Long Preamble, 300

LTE, 268

LTE Status, 277

M

Mail Alert, 213

Mail Extender, 188

Mail Service, 213

Main Screen, 20

Maintenance, 605

Management, 465

Management Interface, 219

MBS, 129

Min/Max Interval Time, 158

Minimum Keep Alive Period, 446

Mirror Port, 168

Mode, 284, 291

Modem Code Upgrade, 478

Modem Dial String, 107

Modem Initial String, 56, 107

Modem Initial String2, 107

Modem Setting (for ADSL only), 81, 84

Modem Settings, 88

Modem Settings (for ADSL only), 92

Modem Support List, 106, 108

Modulation, 88, 92

MPoA / Static or Dynamic IP, 38

MPPE, 336

MTU, 82, 85, 89, 93, 97, 100, 102, 105, 110, 158

Multiple SSID, 280

multiple-WAN, 67

Multi-PVC channel, 88, 92

Multi-PVC/VLAN, 122

MyVigor, 58

N

Name Link, 25

NAT, 170

NAT Sessions Table, 670

Neighbor AP Detection, 588

Network Configuration, 148, 152, 154

Network Interface, 250

Network Mode, 109

Notification Object, 639

NS Detect, 116

O

Objects Settings, 614

Online Statistics, 487

Open Ports, 178

Option Number, 79

P

Packet-OVERDRIVE, 300

PAP, 336

Pass Phrase, 105

Password, 82, 90, 96, 101, 102, 113, 114, 125

Password Strength, 291, 451

Path MTU Discovery, 82, 85, 89, 93, 97, 100, 102, 110

PCR, 129

Peer ID, 330, 333

Per Station Limit, 304

Physical Connection, 30

Physical Members, 124, 128

Physical Mode, 67, 70, 72, 74, 76, 79

Physical Type, 40, 67

PinCode, 296

Ping Detect, 82, 84, 89, 92, 96, 99, 104, 107, 109, 111, 113, 114, 116, 117, 119, 120, 124

Ping Diagnosis, 672

Ping Gateway IP, 82, 84, 89, 92, 96, 99, 104, 107, 109, 124

Ping Interval, 82, 84, 89, 92, 96, 99, 107, 109, 124

PING Interval, 99

Ping IP/Hostname, 111, 113, 114, 116, 117, 119, 120

Ping Retry, 82, 84, 89, 92, 96, 99, 107, 109, 124

Port Redirection, 171

Port Triggering, 180, 182

Port-Based VLAN, 161

PPP Authentication, 82, 90, 98, 103, 107, 125

PPP General Setup, 336

PPP Password, 107

PPP Setup, 103

PPP Username, 107

PPPoE, 41

PPPoE Pass-through, 81, 89

PPPoE/PPPoA, 35

PPTP/L2TP, 44

Prefix Len, 250

Prefix Length, 117

Pre-shared Key, 298

Pre-Shared Key (PSK), 291

Primary DNS Sever, 157

Primary IP Address, 150, 153

Primary/Secondary Ping IP, 82, 84, 89, 92, 96, 99, 107, 109, 124

Printer Server, 651

Priority, 34, 71, 73, 162, 244, 256

Priority ID, 219

Private IP, 173

Private IP Address, 65

Private Port, 173

Production Registration, 61

Protocol, 88, 219

Public IP Address, 65

Public Port, 173

Push Button, 296

PVC to PVC Binding, 129

Q

QoS Type, 124, 128, 129

Quality of Service, 481, 486

Query Server, 425

Quick Access, 26

Quick Start Wizard, 33

Quota Limit, 131

R

RADIUS/TACACS+, 183, 200

Rate Adaptation Algorithm, 301

Rate Control, 145

Reboot System, 476

Recipient, 212

Recipient Number, 274

Redundancy Method, 218

Registering Vigor Router, 61

Regular DN, 206

Regular Mode, 205

Regular Password, 206

Relay Agent, 149, 152

Remote Access Control, 335

Remote Dial-in User, 343, 348

Remote Endpoint IPv4 Address, 118

Repeater, 298

Restore, 166

RIP Protocol, 85, 93, 100

RIPng Protocol, 111, 116, 118, 158

Rogue AP, 589

Rogue AP Detection, 587

Root CA, 383

Route Policy, 244

Router Advertisement Configuration, 158

Router Commands, 275

Router Name, 101, 459

Routing, 244

Routing Information Protocol, 145

Routing Table, 666

RTS Threshold, 302

S

Scan, 305

Schedule, 107, 109, 183, 197, 289

SCR, 129

Secondary DNS Server, 157

Secondary IP Address, 150, 153

Security, 290

Security Key, 284

Self-Signed Certificate, 386, 474

Send SMS, 274

Sensor, 655

Server Address, 102

Server Certificate, 338

Service, 181

Service Activation Wizard, 58

Service Name, 36, 96, 107, 173

Service Provider, 187, 189, 634

Service Type Group, 626

Service Type Object, 624

Sesseion Based, 68

Sessions Control, 392

Sessions Limit, 481, 482

Set to Factory Default, 185, 197, 246

Shared Secret, 202, 204

SIM card, 268

SIM Pin code, 56

SIM PIN code, 107, 109

Simple Mode, 205, 271

SLAAC(stateless), 156

Smart Bandwidth Limit, 485

SMB, 652

SMS / Mail Alert Service, 212

SMS Alert, 212

SMS Inbox, 271

SMS Provider, 212

SMS Quota Limit, 269

SMS/Mail Service Object, 633

Source IP, 173, 179, 182, 252

Specify an IP address, 86

SPI, 389

SSL VPN, 338

Start IP Address, 149, 152, 154

Start IPv6 Address, 157

Start Port, 179

Static IP, 46, 50, 53

Static Route, 145, 245

Static Route for IPv6, 249

Station Control, 303

Station List, 282, 313, 314

Station Number, 591

Stations (STA), 280

Status, 574

Strict Bind, 165

Strict Security Firewall, 391

String Object, 640, 641

STUN Settings, 446

Subnet, 162

Subnet Mask, 86, 94, 101, 103, 104, 148, 152, 154

Subnet Prefix, 114

Support List, 606, 609, 610

Switch, 594

Switch Group, 603

Switch Hierarchy, 597, 598

Switch Status, 595

Sync User Profile, 222

Syslog Alarm, 656

Syslog Explorer, 679

Syslog/Mail Alert, 459

System Maintenance, 442

System time set, 197

T

Tag value, 34, 71, 73

Tagged VLAN, 161

Temperature Sensor, 587, 655

Time and Date, 462

Time Quota, 497

Time Schedule, 485

Time Server, 462

Time Zone, 462

Total Traffic, 591

Trace Route, 678

Traceable, 491

Traffic Graph, 586, 676

Traffic Threshold, 71, 72, 75, 77

Triggering Port, 182

Triggering Protocol, 182

Trusted CA Certificate, 382

TSPC, 112

TTL (Time to Live), 82, 84, 89, 92, 96, 99, 104, 107, 109, 111, 113, 114, 116, 117, 119, 120, 124

Tunnel Broker, 113, 114

Tunnel ID, 114

TX Power, 301

U

Unique Local Address (ULA), 157

Update DDNS, 219

Upload Limit, 304

UPnP, 184, 207

URL Access Control, 421

URL Content Filter, 393, 402, 415

URL Content Filter Profile, 420

USB, 50, 56

USB General Settings, 650

USB User Management, 651

User Group, 499

User Password, 451

User Profile, 203, 222, 495

Username, 82, 90, 96, 101, 102, 113, 114, 125

V

VCI, 92

VID, 162

View SMS Outbox Cache, 274

Virtual LAN, 145

Virtual Panel, 24

Virtual WAN, 32

VLAN, 161

VLAN Configuration, 163

VLAN Tag, 124, 127, 162

VLAN Tag insertion, 34, 40, 71, 73

VPI, 92

VPN, 317, 551

VPN and Remote Access, 318

VPN Client Wizard, 319

VPN Dial-Out Through, 323

VPN Graph, 677

VPN Management, 561

VPN Server Wizard, 326

VPN Trunk Management, 361

W

Wake by IP Address, 211

Wake on LAN, 184

WAN, 65

WAN Application-**IPTV**, 124

WAN Application-Management, 124

WAN Budget, 130

WAN Budget-Status, 133

WAN Connection Detection, 82, 84, 89, 92, 96, 99, 104, 107, 109, 111, 113, 114, 116, 117, 119, 120, 124

WAN Failure, 71, 72, 75, 77

WAN Interface, 178, 187, 189

WAN IP, 173

WAN IP Alias, 82, 86, 94, 98, 101, 103

WAN IP Network Settings, 86, 94, 101, 103

WAN Type, 123, 127

WAN-USB, 76

WDS, 297

Web Console, 28

Web Content Filter, 393, 402, 415

Web Content Filter Profile, 424

Web Feature, 422

Weight, 68

WEP, 105, 281, 292

Wildcard, 188

Wired 802.1x, 169

Wireless 2.4/5G, 71

Wireless LAN, 279

Wireless Wizard, 283

Wizard Mode, 396

WLAN Isolation, 281

WLAN Profile, 575

WMM Capable, 301

WPA, 281, 291

WPS, 282, 294