DrayTek

Vigor3910 Series

Multi-WAN Security Router

USER'S GUIDE

V1.61

Vigor3910 Series
Multi-WAN Security Router

User's Guide

Version: 1.61

Firmware Version: V4.3.2.5

(For future update, please visit DrayTek web site)

Date: January 29, 2024

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, 11 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Do not power off the device when saving configurations or firmware upgrades. It may damage the data in a flash. Please disconnect the Internet connection on the device before powering it off when a TR-069/ ACS server manages the device.
- 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.

Table of Contents

Part I Installation 1

I-1 Introduction 2

I-1-1 Indicators and Connectors 3

I-2 Hardware Installation 5

I-2-1 Installing Vigor Router 5

I-2-2 Rack-Mounted Installation 6

I-3 Accessing Web Page 7

I-4 Changing Password 9

I-5 Dashboard 10

I-5-1 Virtual Panel 11

I-5-2 Quick Access for Common Used Menu 12

I-5-3 GUI Map 13

I-5-4 Web Console 14

I-5-5 Config Backup 14

I-5-6 Manual Download 15

I-5-7 Logout 15

I-5-8 Online Status 16

I-5-8-1 Physical Connection 16

I-5-8-2 Virtual WAN 18

I-6 Quick Start Wizard 19

I-6-1 For WAN1 (Fiber) 20

I-6-2 For WAN3 (Ethernet - 2.5G) 27

I-6-3 For WAN5~WAN8 (Etherent) 34

I-7 Service Activation Wizard 41

I-8 Registering Vigor Router 43

I-9 VPN Client Wizard 46

I-10 VPN Server Wizard 53

Part II Connectivity 63

II-1 Port Setup 64

II-2 WAN 65

Web User Interface 66

II-2-1 General Setup 66

II-2-2 Internet Access 71

II-2-2-1 Details Page for PPPoE 73

II-2-2-2 Details Page for Static or Dynamic IP 76

II-2-2-3 Details Page for IPv6 – Offline in Ethernet WAN 80

II-2-2-4 Details Page for IPv6 – PPP 80

II-2-2-5 Details Page for IPv6 – TSPC 81

II-2-2-6 Details Page for IPv6 – AICCU 83

II-2-2-7 Details Page for IPv6 – DHCPv6 Client 85

II-2-2-8 Details Page for IPv6 – Static IPv6 86

II-2-2-9 Details Page for IPv6 – 6in4 Static Tunnel 87
II-2-2-10 Details Page for IPv6 – 6rd 90
II-2-3 Multi-VLAN 92
II-2-4 WAN Budget 96
II-2-4-1 General Setup 96
II-2-4-2 Status 99
II-3 LAN 100
Web User Interface 102
II-3-1 General Setup 102
II-3-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup 103
II-3-1-2 Details Page for IP Routed Subnet 106
II-3-1-3 Details Page for LAN1 – IPv6 Setup 108
II-3-1-4 DHCP Server Option 112
II-3-2 VLAN 113
II-3-3 Bind IP to MAC 115
II-3-4 Port Mirror/Packet Capture 118
II-3-5 Wired 802.1x 120
II-3-6 PPPoE Server 122
II-4 NAT 123
Web User Interface 124
II-4-1 Port Redirection 124
II-4-2 DMZ Host 128
II-4-3 Open Ports 131
II-4-4 Port Triggering 133
II-4-5 Fast NAT 137
II-4-6 ALG 138
II-5 Applications 139
Web User Interface 141
II-5-1 Dynamic DNS 141
II-5-2 LAN DNS / DNS Forwarding 146
II-5-3 DNS Security 150
II-5-3-1 General Setup 150
II-5-3-2 Domain Diagnose 151
II-5-4 Schedule 152
II-5-5 RADIUS/TACACS+ 155
II-5-5-1 External RADIUS 155
II-5-5-2 Internal RADIUS 157
II-5-5-3 External TACACS+ 160
II-5-6 Active Directory/ LDAP 161
II-5-6-1 General Setup 161
II-5-6-2 Active Directory / LDAP Profiles 162
II-5-7 UPnP 163
II-5-8 IGMP 165
II-5-8-1 General Setting 165
II-5-8-2 Working Status 166

II-5-9 Wake on LAN 167
II-5-10 SMS / Mail Alert Service 168
II-5-10-1 SMS Alert 168
II-5-10-2 Mail Alert 169
II-5-11 Bonjour 170
II-5-12 High Availability 173
II-5-12-1 General Setup 173
II-5-12-2 Config Sync 175
II-5-13 Local 802.1X General Setup 177
II-5-14 Smart Action 179
Application Notes 181
A-1 How to Implement the LDAP/AD Authentication for User Management? 181
A-2 How to use DrayDDNS? 184
II-6 Routing 189
Web User Interface 190
II-6-1 Static Route 190
II-6-2 Load-Balance /Route Policy 195
II-6-2-1 General Setup 195
II-6-2-2 Diagnose for Route Policy 201
II-6-3 Fast Routing 205
II-6-4 OSPF 206
II-6-5 BGP 208
II-6-4-1 Basic Settings 209
II-6-4-2 Static Network 210
Application Notes 211
A-1 How to Customize a Secure Route between VPN Router and Remote Router by Using Route Policy 211

Part III VPN 215

III-1 VPN and Remote Access 216
Web User Interface 216
III-1-1 Remote Access Control 217
III-1-1-1 Remote Access Control Setup 217
III-1-2 Bind to WAN 218
III-1-2 PPP General Setup 219
III-1-3 SSL General Setup 221
III-1-4 IPsec General Setup 222
III-1-5 IPsec Peer Identity 225
III-1-6 VPN Matcher Setup 227
III-1-7 OpenVPN 229
III-1-7-1 OpenVPN Server Setup 229
III-1-7-2 Client Config 232
III-1-7-3 Import Certificate 233
III-1-8 WireGuard 234
III-1-9 Remote Dial-in User 235

III-1-10 LAN to LAN 242
III-1-11 VPN Trunk Management 252
III-1-12 Connection Management 257
Application Notes 259
A-1 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tunnel (Main Mode) *259*
III-2 Certificate Management 264
Web User Interface 265
III-2-1 Local Certificate 265
III-2-2 Trusted CA Certificate 270
III-2-3 Certificate Backup 273
III-2-4 Self-Signed Certificate 274

Part IV Security 275

IV-1 Firewall 276
Web User Interface 278
IV-1-1 General Setup 278
IV-1-2 Filter Setup 283
IV-1-3 Defense Setup 293
IV-1-3-1 DoS Defense *293*
IV-1-3-2 Spoofing Defense *296*
IV-1-4 Diagnose 296
Application Notes 299
A-1 How to Configure Certain Computers Accessing to Internet *299*
IV-2 CSM (Central Security Management) 302
Web User Interface 303
IV-2-1 APP Enforcement Profile 303
IV-2-2 URL Content Filter Profile 305
IV-2-3 Web Content Filter Profile 309
IV-2-4 DNS Filter Profile 312
Application Notes 314
A-1 How to Create an Account for MyVigor *314*
A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter *318*
A-3 How to use APP Enforcement to block application like Facebook, YouTube or TeamViewer? *323*

Part V Management 327

V-1 System Maintenance 328
Web User Interface 329
V-1-1 System Status 329
V-1-2 TR-069 331
V-1-2-1 ACS and CPE Settings *331*
V-1-2-2 Reporting Configuration *333*
V-1-2-3 Export Parameters *335*

V-1-3 Administrator Password 336
V-1-4 User Password 339
V-1-5 Login Page Greeting 342
V-1-6 Configuration Backup 344
V-1-7 Configuration Export 346
V-1-8 Webhook 347
V-1-9 Syslog/Mail Alert 348
V-1-10 Time and Date 351
V-1-11 SNMP 352
V-1-12 Management 354
V-1-13 Self-Signed Certificate 359
V-1-14 Reboot System 361
V-1-15 Firmware Upgrade 362
V-1-16 Internal Service User List 363
V-1-17 Dashboard Control 364
V-1-18 Max Connection 364
V-2 Bandwidth Management 365
Web User Interface 366
V-2-1 Sessions Limit 366
V-2-2 Bandwidth Limit 368
V-2-3 Quality of Service 370
V-2-4 APP QoS 376
V-3 User Management 377
Web User Interface 378
V-3-1 General Setup 378
V-3-2 User Profile 380
V-3-3 User Group 385
V-3-4 User Online Status 386
V-3-5 PPPoE User Online Status 387
Application Notes 388
A-1 How to authenticate clients via User Management 388
A-2 How to use Landing Page Feature 397
V-4 Hotspot Web Portal 401
Web User Interface 401
V-4-1 Profile Setup 401
V-4-1-1 Login Method 402
V-4-1-2 Steps for Configuring a Web Portal Profile 403
V-4-2 Users Information 419
V-4-2-1 User Info 419
V-4-2-2 Database Setup 421
V-4-3 Quota Management 423
V-4-4 PIN Generator 426

V-4-4-1 PIN Status *426*
V-4-4-2 PIN Generator *427*
V-4-4-3 PIN Voucher *428*
Application Notes 430
A-1 How to allow users login to Vigor's Hotspot with their social media accounts (e.g., Facebook & Google) *430*
A-2 How to allow hotspot clients to get login PIN code via SMS? *438*
V-5 Central Management (AP) 446
Web User Interface 447
V-5-1 Dashboard 447
V-5-2 Status 448
V-5-3 WLAN Profile 449
V-5-4 AP Maintenance 454
V-5-5 Traffic Graph 455
V-5-6 Event Log 456
V-5-7 Total Traffic 457
V-5-8 Station Number 457
V-5-9 Load Balance 458
V-6 Central Management (Switch) 460
Web User Interface 461
V-6-1 Status 461
V-6-1-1 Switch Status *461*
V-6-1-2 Switch Hierarchy *463*
V-6-1-3 Detailed Info *464*
V-6-1-4 TR069 Setting *465*
V-6-2 Profile 466
V-6-3 Group 469
V-6-4 Maintenance 471
V-6-5 Alert and Log 472
V-6-5-1 Alert Setup *472*
V-6-5-2 Switch and Port Setup *473*
V-6-6 Database Setup 475
V-6-7 Support List 476
V-7 Central Management (External Devices) 477
Part VI Others 479
VI-1 Objects Settings 480
Web User Interface 481
VI-1-1 IP Object 481
VI-1-2 IP Group 484
VI-1-3 IPv6 Object 485
VI-1-4 IPv6 Group 487
VI-1-5 Service Type Object 488
VI-1-6 Service Type Group 490

VI-1-7 Keyword Object 492
VI-1-8 Keyword Group 494
VI-1-9 File Extension Object 495
VI-1-10 SMS/Mail Service Object 497
VI-1-11 Notification Object 502
VI-1-12 String Object 504
VI-1-13 Country Object 505
VI-1-14 Objects Backup/Restore 507
Application Notes 508
A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection 508
VI-2 USB Application 512
Web User Interface 513
VI-2-1 USB General Settings 513
VI-2-2 USB User Management 513
VI-2-3 File Explorer 515
VI-2-4 USB Device Status 517
VI-2-5 Temperature Sensor 519
Part VII Troubleshooting 521
VII-1 Diagnostics 522
Web User Interface 523
VII-1-1 Dial-out Triggering 523
VII-1-2 Routing Table 524
VII-1-3 ARP Cache Table 525
VII-1-4 IPv6 Neighbour Table 526
VII-1-5 DHCP Table 527
VII-1-6 NAT Sessions Table 528
VII-1-7 DNS Cache Table 529
VII-1-8 Ping Diagnosis 530
VII-1-9 Data Flow Monitor 532
VII-1-10 Port Mirror/Packet Capture 534
VII-1-11 Traffic Graph 537
VII-1-12 VPN Graph 538
VII-1-13 Trace Route 540
VII-1-14 Syslog Explorer 541
VII-1-15 IPv6 TSPC Status 542
VII-1-16 High Availability Status 543
VII-1-17 Authentication Information 545
VII-1-18 DoS Flood Table 546
VII-1-19 Route Policy Diagnosis 547
VII-1-20 Debug Logs 549

VII-2 Checking If the Hardware Status Is OK or Not 550
VII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not 551
VII-4 Pinging the Router from Your Computer 554
VII-5 Checking If the ISP Settings are OK or Not 556
VII-6 Backing to Factory Default Setting If Necessary 557
VII-7 Contacting DrayTek 559

Part VIII DrayTek Tools 561

VIII-1 SmartVPN Client 562
VIII-1-1 DrayTek Android-based SmartVPN APP for the establishment of SSL VPN connection 562
VIII-1-2 How to Use SmartVPN Android APP to Establish SSL VPN Tunnel? 563

Part IX Telnet Commands 567

Accessing Telnet of Vigor3910 568

Part I Installation

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

I-1 Introduction

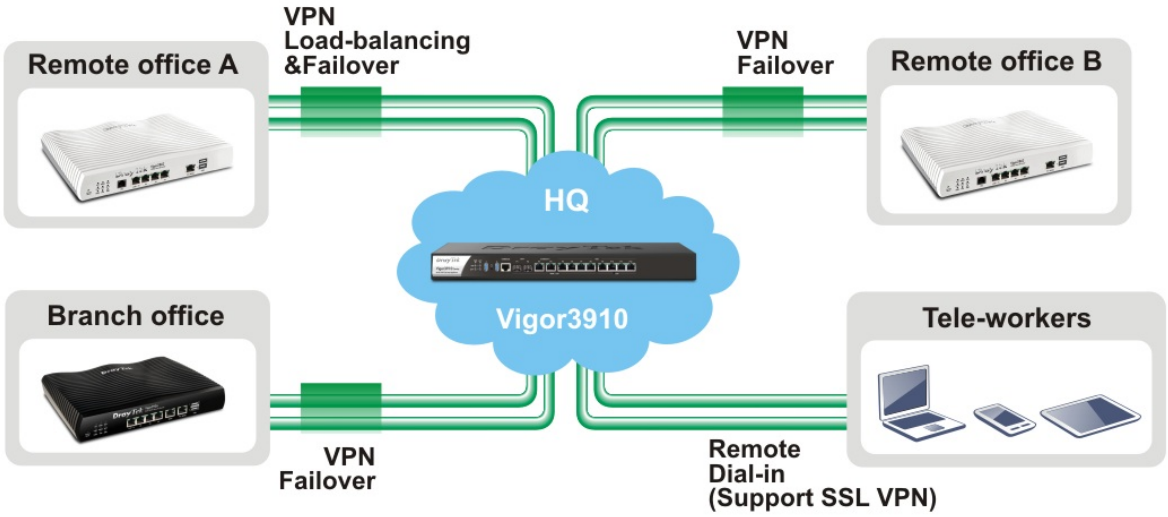
This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

Vigor3910 Series, a broadband router, integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly and offers several protocols (such as IPSec/PPTP/L2TP) with up to **100** VPN tunnels.

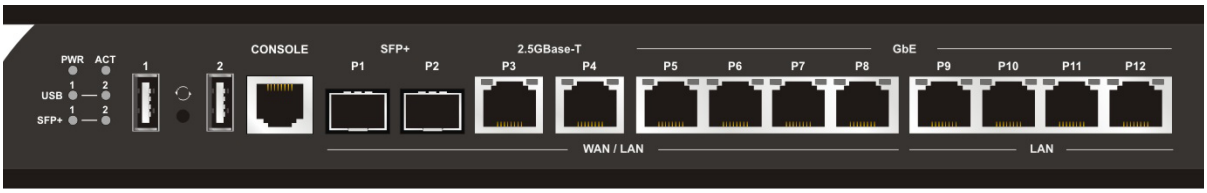
The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy easily. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention and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

Object-based firewall is flexible and allows your network be safe.

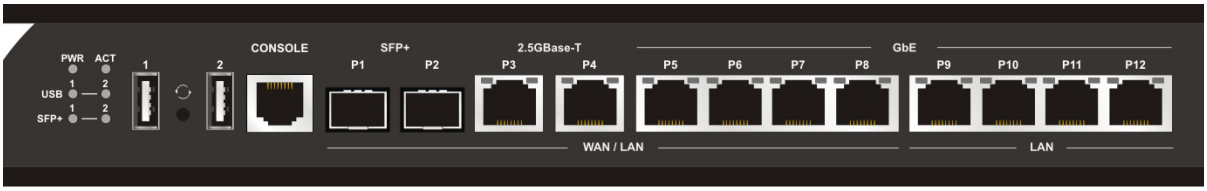


I-1-1 Indicators and Connectors

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



LED		Status	Explanation
PWR		On	The router is powered on.
		Off	The router is powered off.
ACT		Blinking	The system is active.
		Off	The system is hanged.
USB		On	The USB device is installed and ready.
		Off	No USB device is installed.
SFP+		On	The fiber connection is established.
		Blinking	The data is transmitting.
		Off	No fiber connection is established or the system is hanged.
P3~P12		On (Left)	The Ethernet link is established on corresponding port.
		Off (Left)	No Ethernet link is established.
		Blinking (L)	The data is transmitting.
		On (Right)	The Ethernet link is established on corresponding port with 1G Mbps or above.
		Off (Right)	The Ethernet link is established on corresponding port with less than 1G Mbps.
LED on Connector			
DMZ	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps.
LAN	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
WAN1~ WAN4	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps



Interface	Description
USB1 / USB2	Connecter for the USB device.
Console	Provided for technician use.
SFP+ (P1~P2)	Connecter for SFP module with the rate of 10G/1G bps.
2.5GBase-T (P3~P4)	Connector for remote network devices or local network devices (WAN/LAN) with the rate of 2.5G/1G/100M/10M bps.
GbE P5~P8	Connectors for remote network devices or local network devices (WAN/LAN) with the rate of 1G/100M/10M bps.
GbE P9~P12	Connecter for local network devices (LAN) with the rate of 1G/100M/10M bps.
	The Factory Reset button is used to restore the default settings. 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.
	Connecter for a power cord. ON/OFF - Power switch.

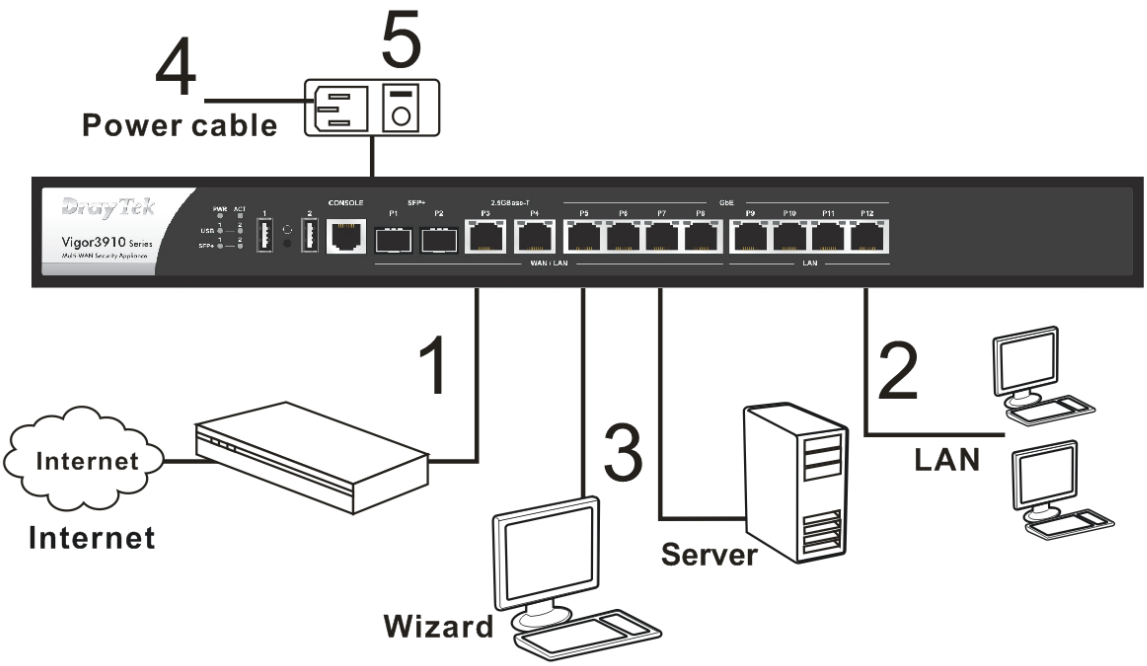
I-2 Hardware Installation

I-2-1 Installing Vigor Router

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

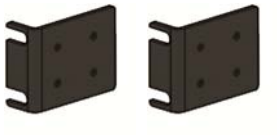
1. Connect a modem to any WAN port of Vigor3910 with Ethernet cable (RJ-45) to access Internet.
2. Connect the other end of the cable (RJ-45) to the Ethernet port on your computer (that device also can connect to other computers to form a small area network). The LAN LED for that port on the front panel will light up.
3. Connect a server/router (depends on your requirement) to any WAN port of Vigor3910 with Ethernet cable (RJ-45). The WAN LED will light up.
4. Connect the power cord to Vigor3910's power port on the rear panel, and the other side into a wall outlet.
5. Power on the device by pressing down the power switch on the rear panel. The PWR LED should be ON.
6. The system starts to initiate. After completing the system test, the ACT LED will light up and start blinking.

Below shows an outline of the hardware installation for your reference.

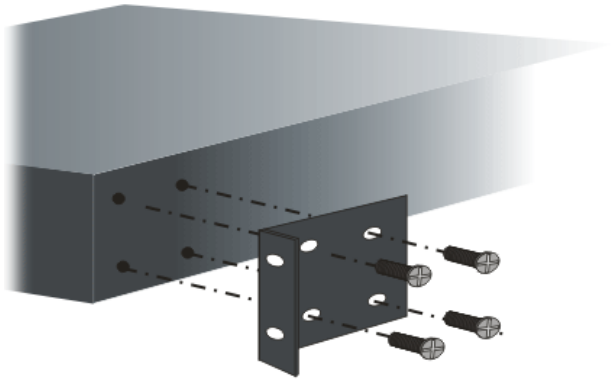


I-2-2 Rack-Mounted Installation

The Vigor3910 Series can be mounted on the wall by using standard brackets shown below.



Attach the brackets to the chassis of a rack. The second bracket attaches the other side of the chassis.



After the bracket installation, the Vigor3910 Series chassis can be installed in a rack by using four screws for each side of the rack.

Desktop Type Installation

Rubber pads are included with the Vigor3910 Series. These rubber pads improve the air circulation and decrease unnecessary rubbing on the desktop.

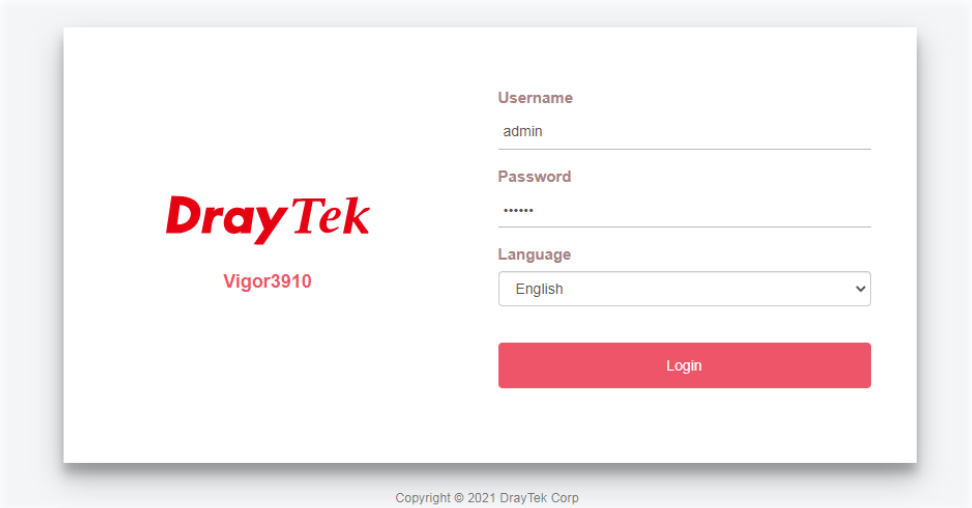
.

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.

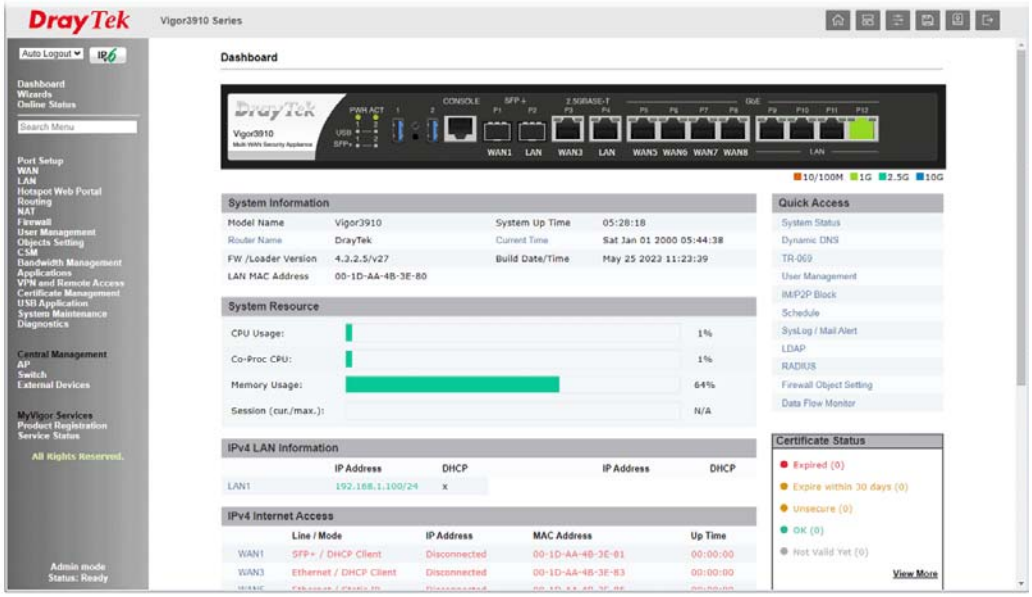


3. Please type “admin/admin” as the Username/Password and click **Login**.

Info

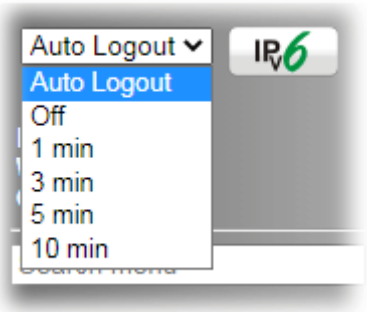
If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

4. Now, the **Main Screen** will appear.



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

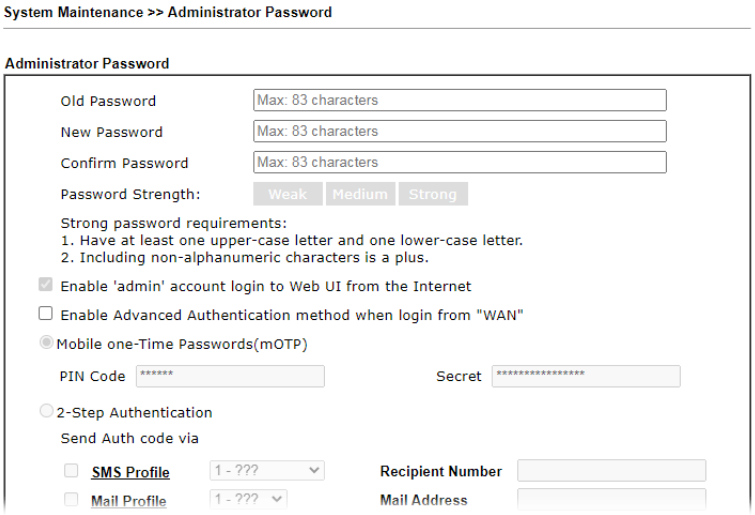
5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



I-4 Changing Password

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

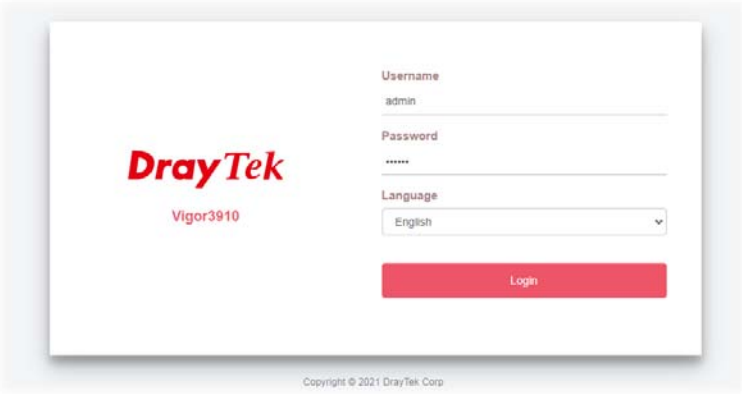
1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.
2. Please type “admin/admin” as Username/Password for accessing into the web user interface with admin mode.
3. Go to **System Maintenance** page and choose **Administrator Password**.



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

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

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

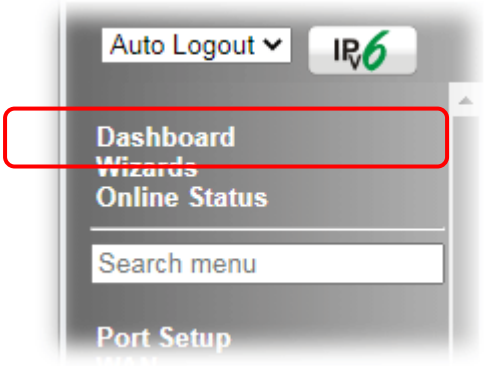


Info	Even the password is changed, the Username for logging onto the web user interface is still “admin”.

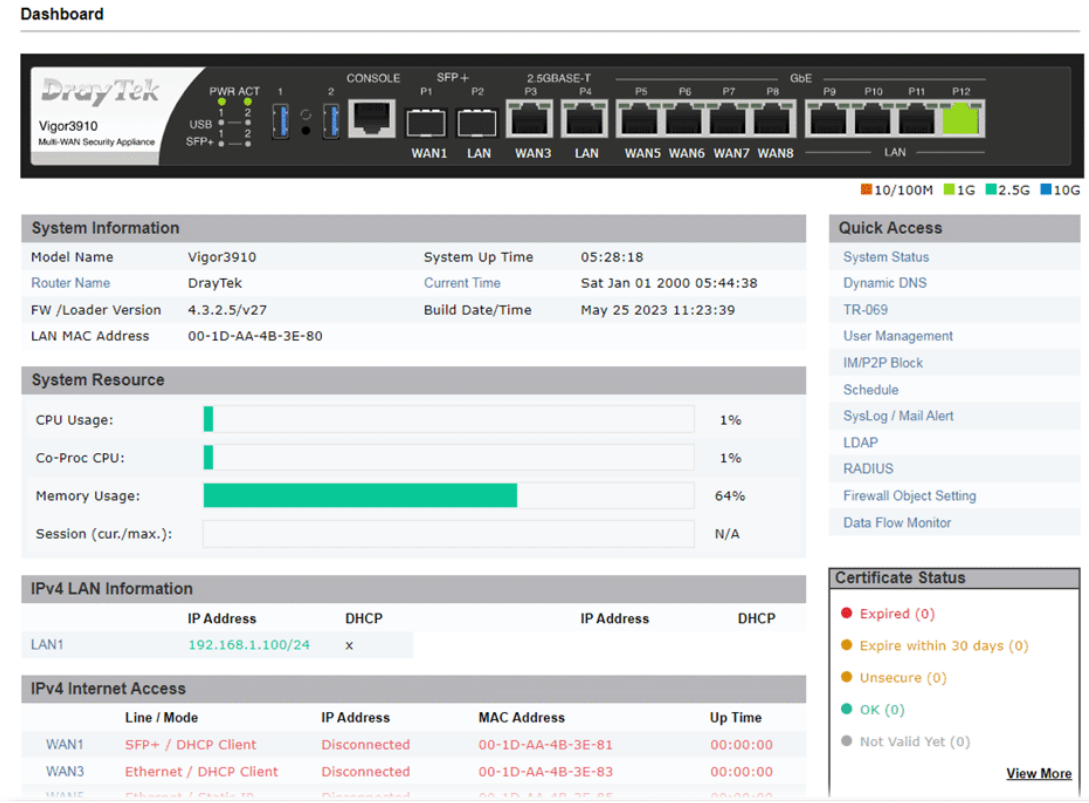
I-5 Dashboard

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

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



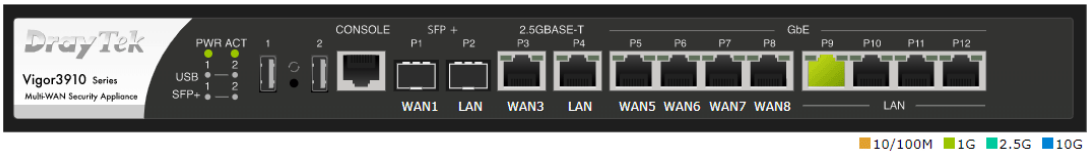
A web page with default selections will be displayed on the screen. Refer to the following figure:



I-5-1 Virtual Panel

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

Dashboard



Port	Color	Description
LAN	Black	LAN port is disconnected.
	Orange	LAN port is connected at 10/100 Mbps.
	Green	LAN port is connected at 1 Gbps.
WAN	Black	WAN port is disconnected.
	Orange	WAN port is connected at 10/100 Mbps.
	Green	WAN port is connected at 1 Gbps.

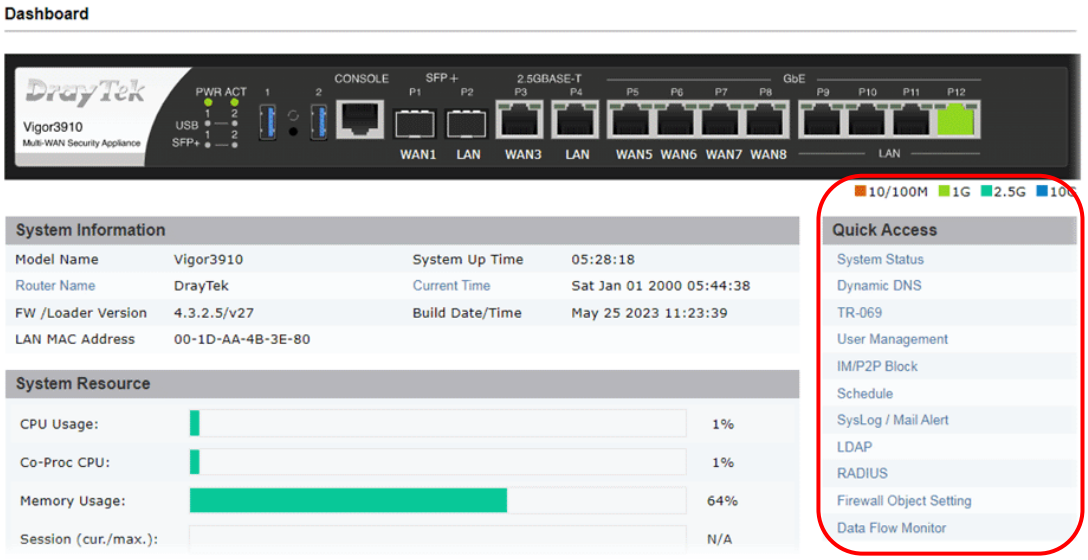
For detailed information about the LED display, refer to **I-1-1 LED Indicators and Connectors**.

I-5-2 Quick Access for Common Used Menu

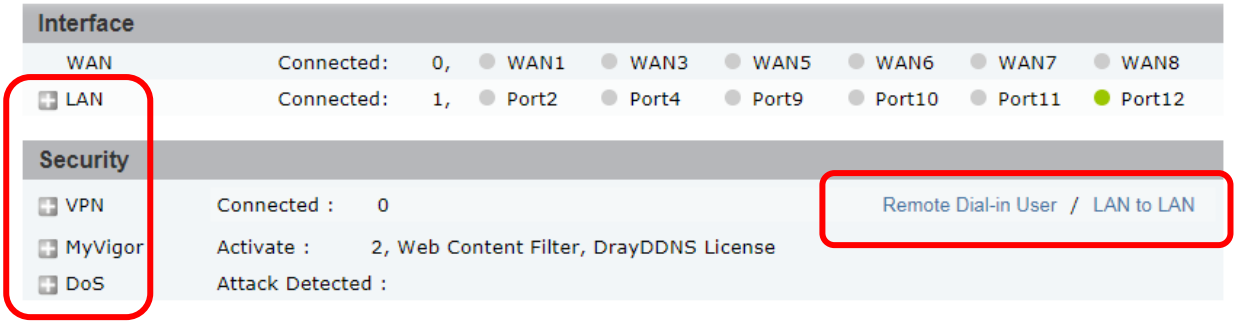
All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

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

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



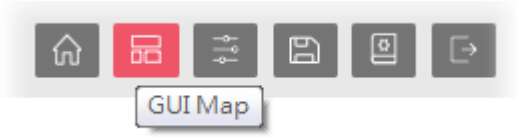
Besides, LAN, IP Routed Subnet, WAN interfaces, VPN security settings such as Remote Dial-in User and LAN to LAN also can be accessed on this page easily. Scroll down the page to find them and move your mouse cursor on the item to open the configuration web page.



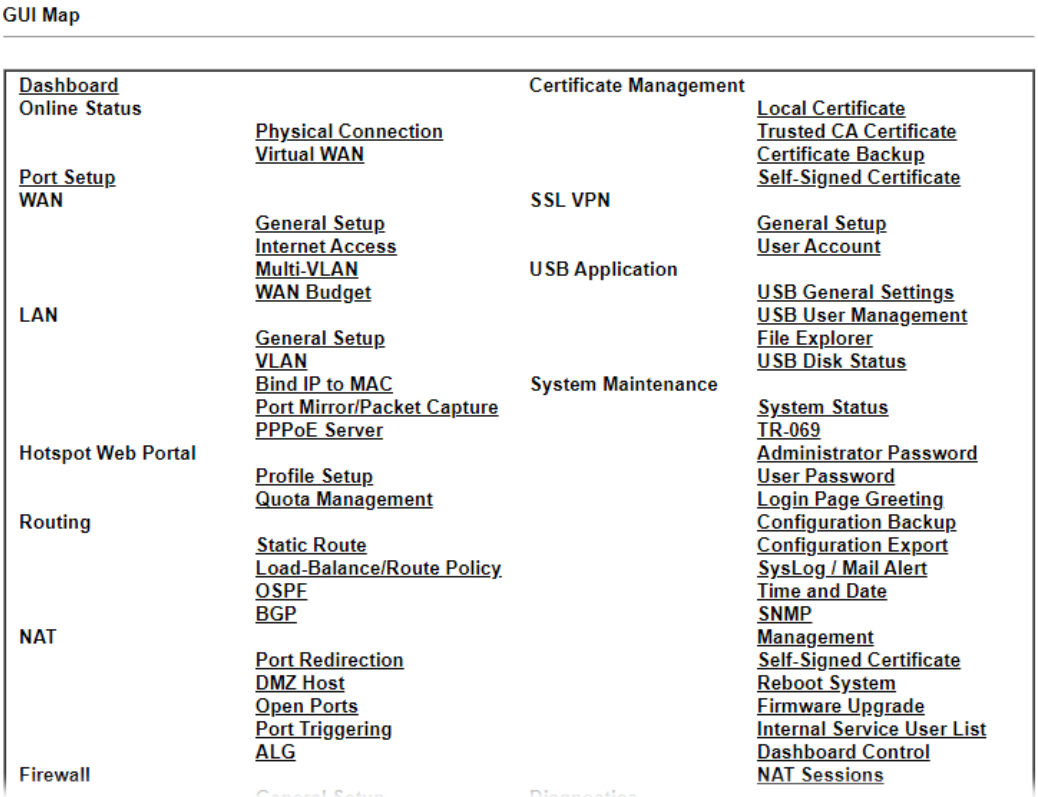
Note that there is a plus ( ) icon located on the left side of VPN/LAN. Click it to review the LAN connection(s) used presently.

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-5-3 GUI Map



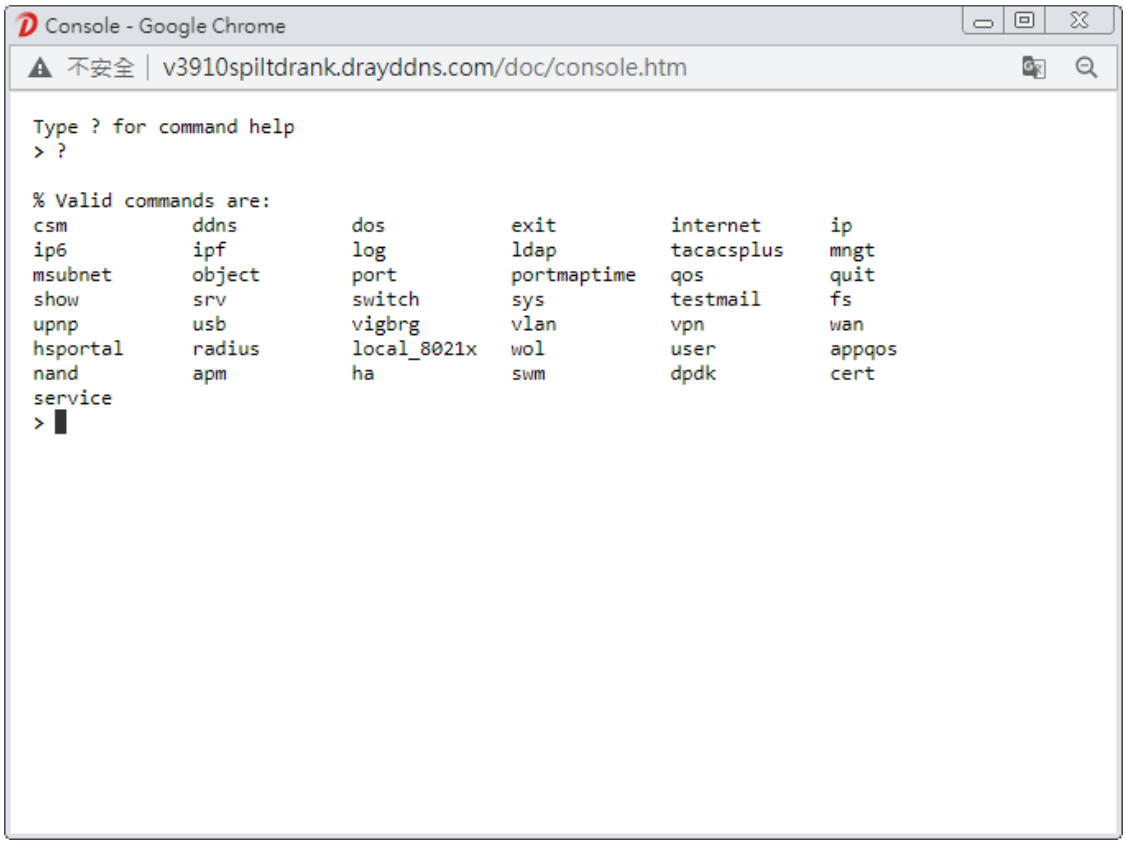
All the functions the router supports are listed with table clearly in this page. Users can click the function link to access into the setting page of the function for detailed configuration. Click the icon on the top of the main screen to display all the functions.



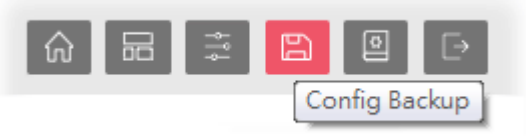
I-5-4 Web Console

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.



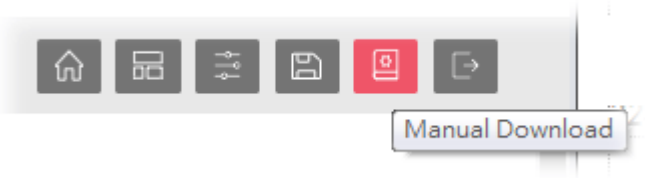
I-5-5 Config Backup



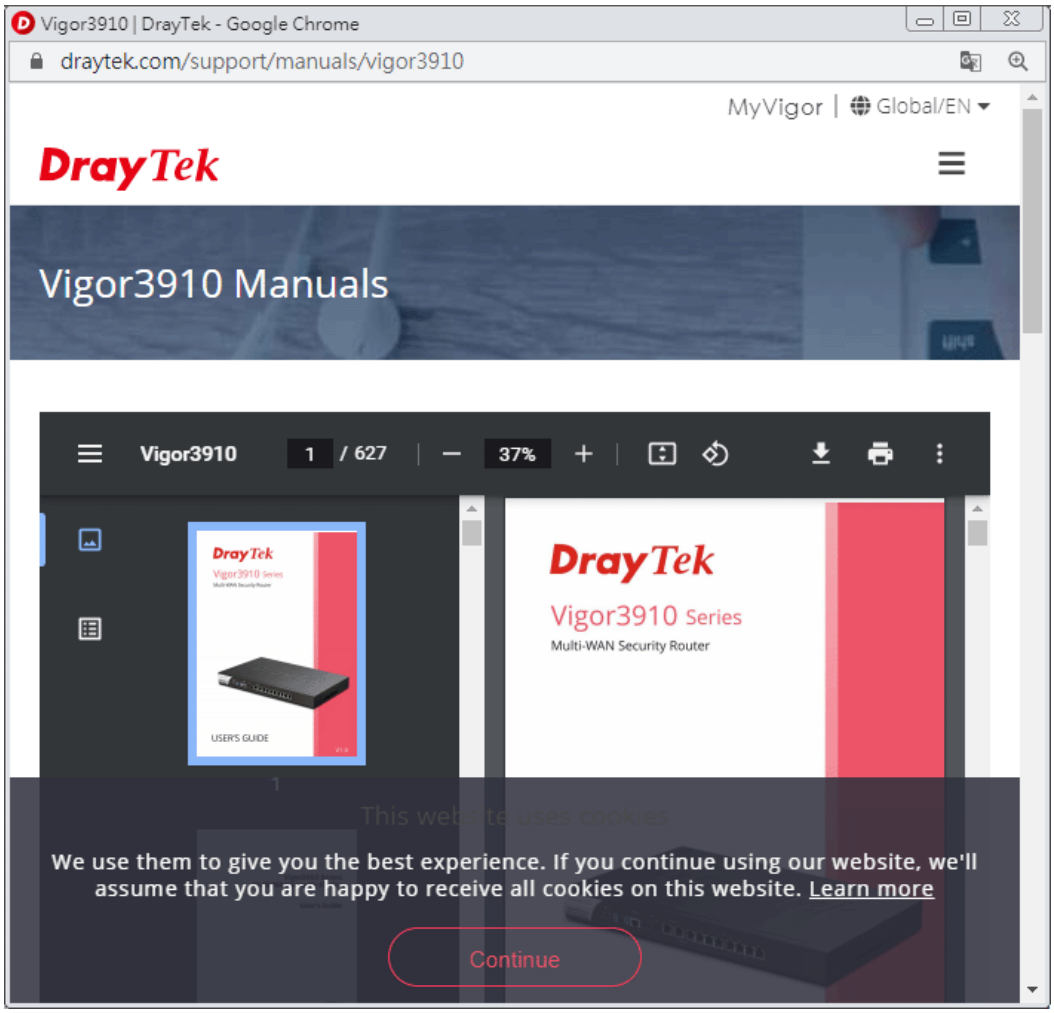
There is one way to store current used settings quickly by clicking the **Config Backup** icon. It allows you to backup current settings as a file. Such configuration file can be restored by using **System Maintenance>>Configuration Backup**.

Simply click the icon on the top of the main screen.

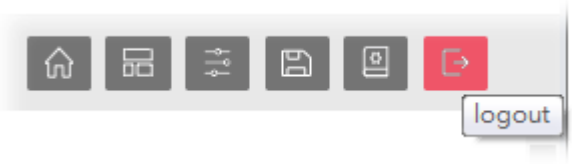
I-5-6 Manual Download



Click this icon to open online user's guide of Vigor router. This document offers detailed information for the settings on web user interface.

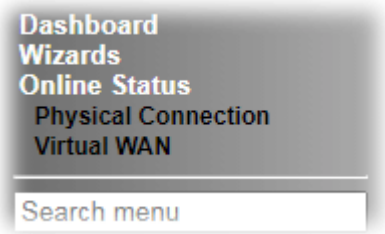


I-5-7 Logout



Click this icon to exit the web user interface.

I-5-8 Online Status



I-5-8-1 Physical Connection

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

Physical Connection for IPv4 Protocol

Online Status

Physical Connection — System Uptime: 6days 7:14:11

IPv4 | IPv6

LAN Status

IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:
192.168.1.1	260,444	128,959	8.8.8.8	8.8.4.4

WAN 1 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

WAN 3 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

WAN 5 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

WAN 6 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

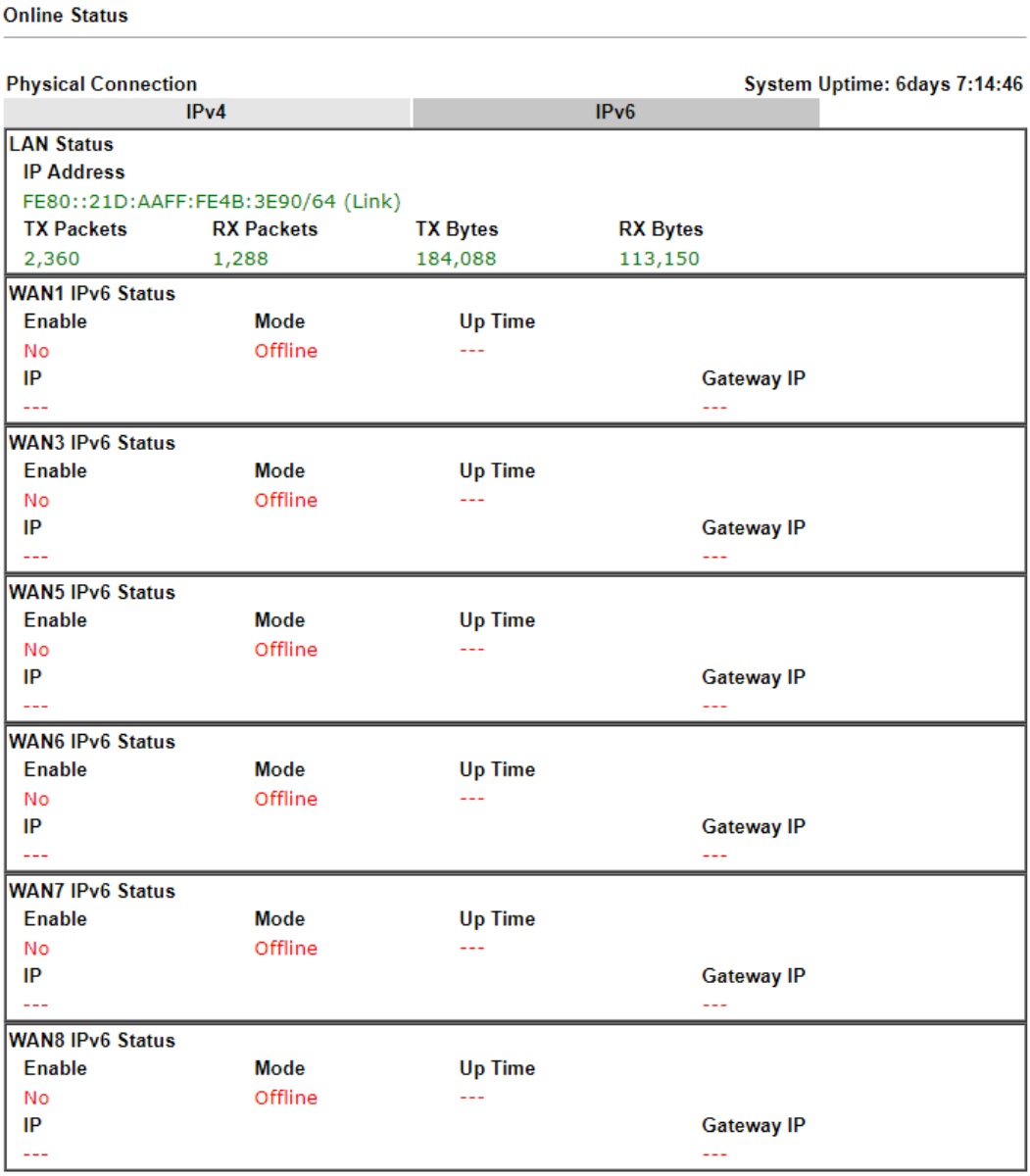
WAN 7 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

WAN 8 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0

Physical Connection for IPv6 Protocol



Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	**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.
WAN1 to WAN8 Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. **Line** – Displays the physical connection (VDSL, ADSL, or Ethernet) of this interface. **Name** – Display the name of the router.

Item	Description
	Mode - Displays the type of WAN connection (e.g., PPPoE). **Up Time** - Displays the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **GW IP** - Displays the IP address of the default gateway. **TX Packets** - Displays the total transmitted packets at the WAN interface. **TX Rate** - Displays the speed of transmitted octets at the WAN interface. **RX Packets** - Displays the total number of received packets at the WAN interface. **RX Rate** - Displays the speed of received octets at the WAN interface.

Detailed explanation (for IPv6) is shown below:

Item	Description
LAN Status	**IP Address**- Displays the IPv6 address of the LAN interface. **TX Packets**-Displays the total transmitted packets at the LAN 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.
WAN1 to WAN8 IPv6 Status	**Enable – No** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. No in red means such interface is not available. **Mode** - Displays the type of WAN connection (e.g., TSPC). **Up Time** - Displays the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **Gateway IP** - Displays the IP address of the default gateway.

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

I-5-8-2 Virtual WAN

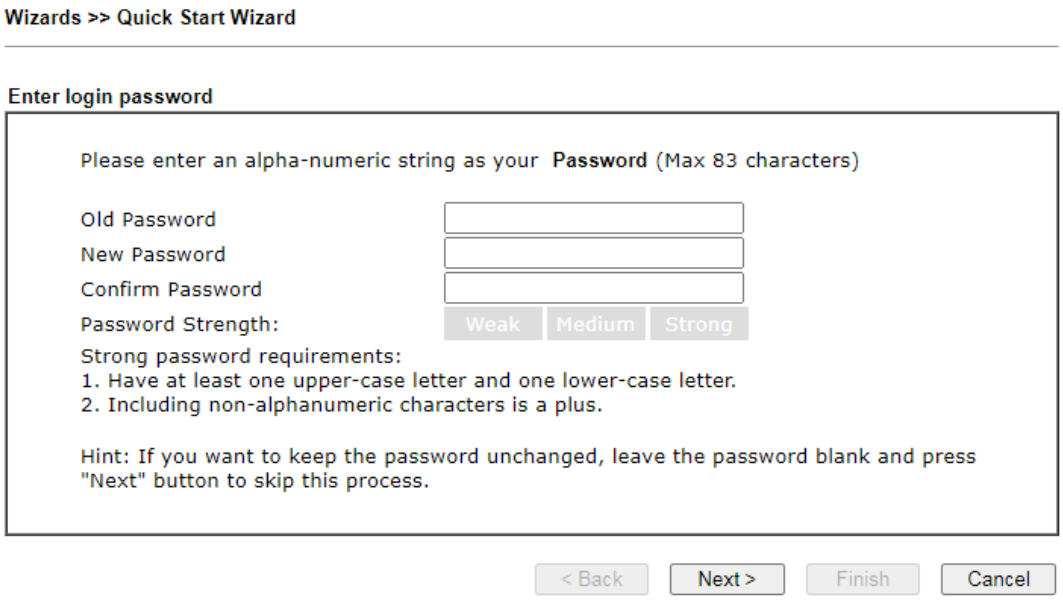
Such page displays the virtual WAN connection information.

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

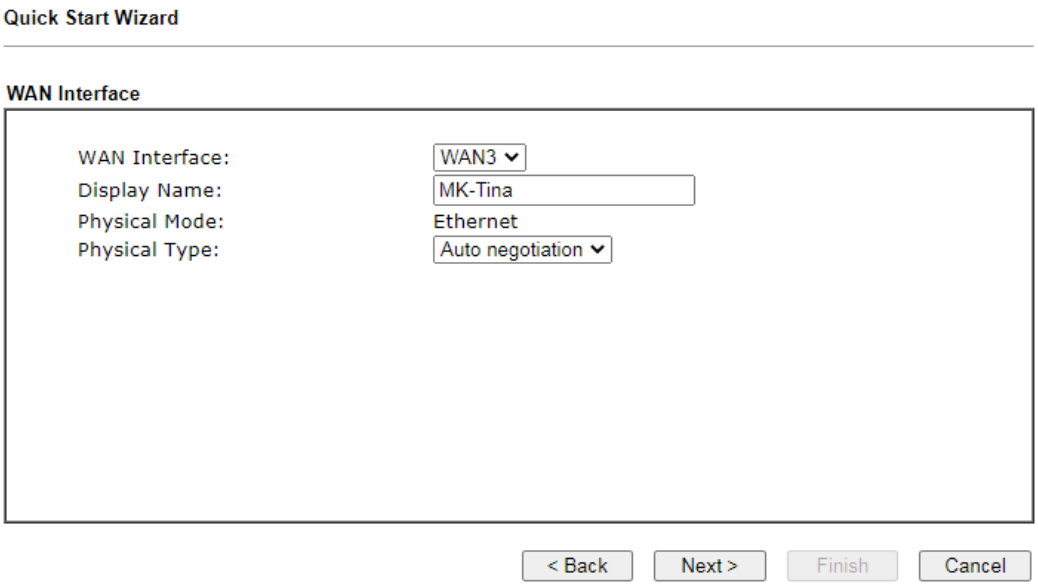
The field of Application will list i-9the purpose of such WAN connection.

I-6 Quick Start Wizard

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



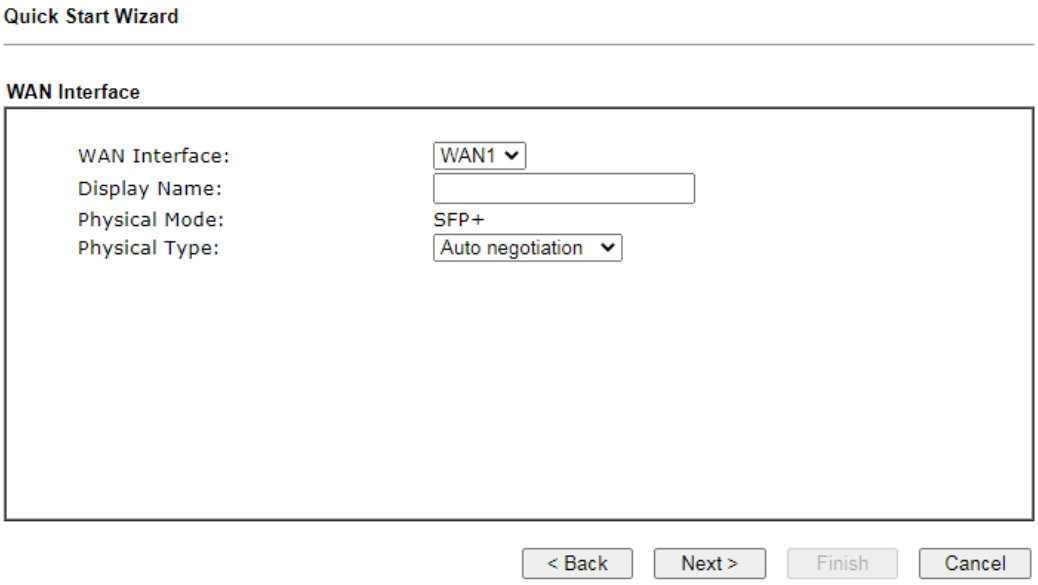
On the next page as shown below, please select the WAN interface that you use. If fiber is used, please choose WAN1/WAN2; if Ethernet is used, please choose WAN3 ~WANx. Then click **Next** for next step.



Fiber WAN and Etherent WAN will bring up different configuration page. Refer to the following for detailed information.

I-6-1 For WAN1 (Fiber)

WAN1 can be configured for physical mode of SFP+ (Fiber connection).



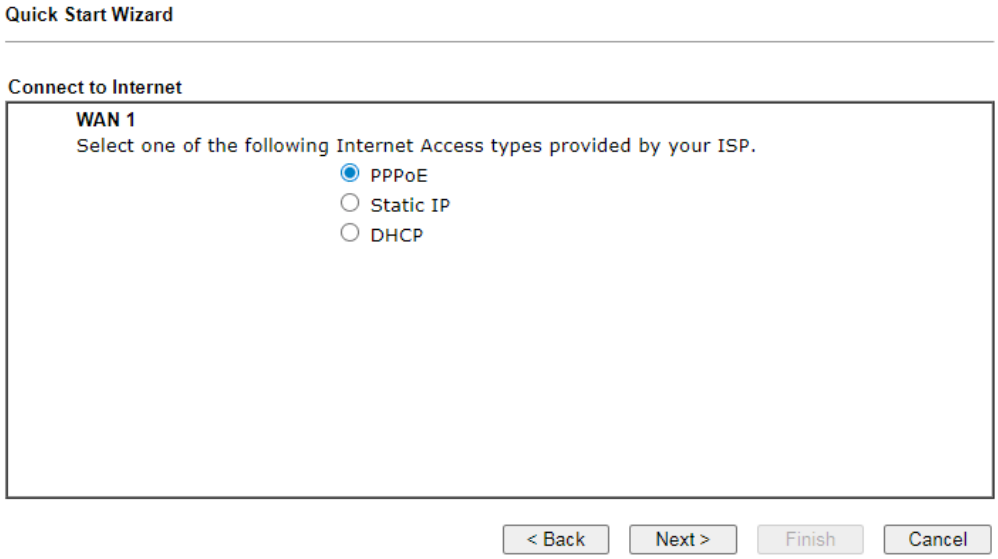
Available settings are explained as follows:

Item	Description
Display Name	Enter a name for the router.
Physical Type	This setting will vary based on the Physical Mode. In general, **Auto negotiation** is suggested.

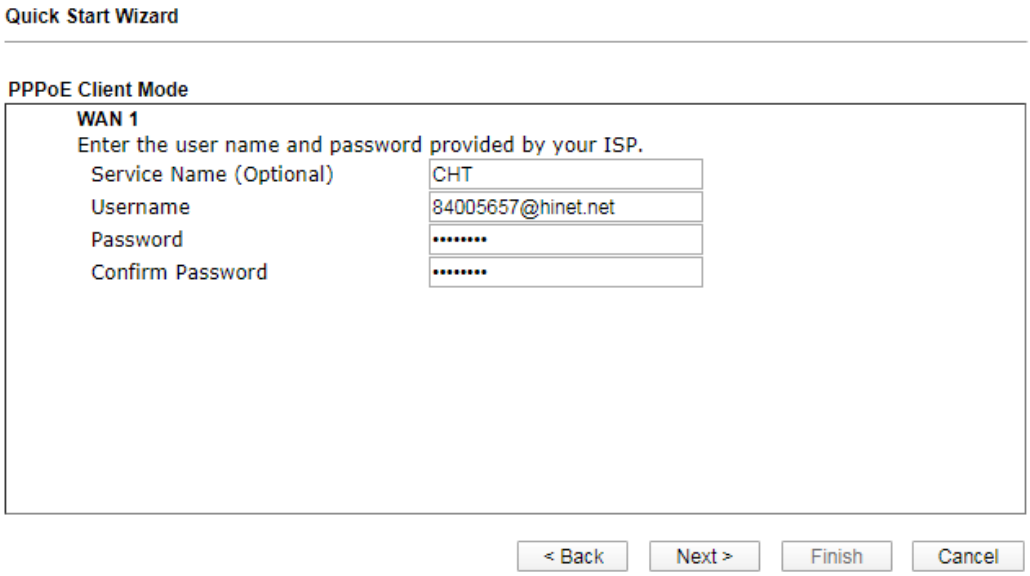
On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

Ethernet WAN1 - PPPoE

1. Choose **WAN1** as the WAN Interface. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



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



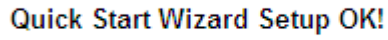
Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
Username	Assign a specific valid user name provided by the ISP. **Note:** The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. **Note:** The maximum length of the password you can set is 62 characters.

Item	Description
Confirm Password	Re-enter the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

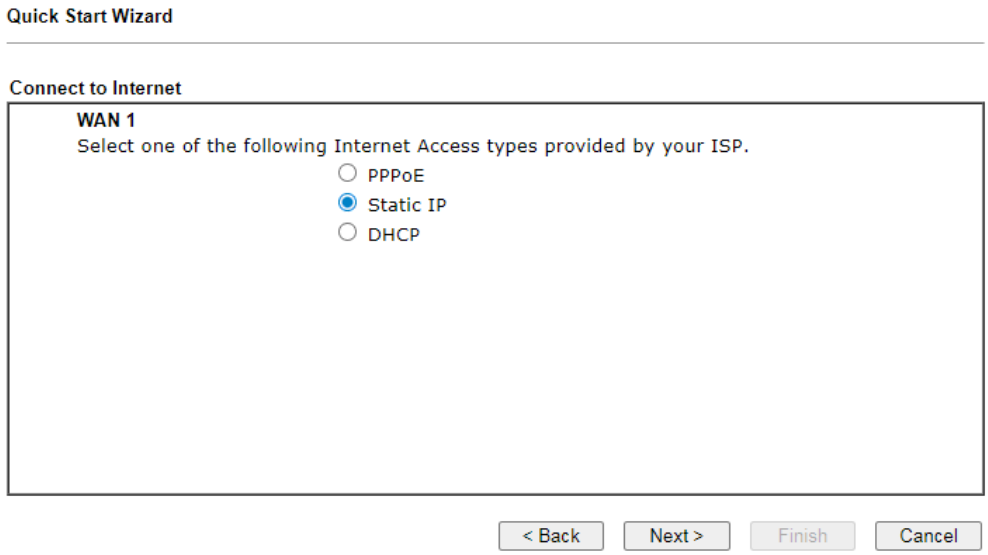
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



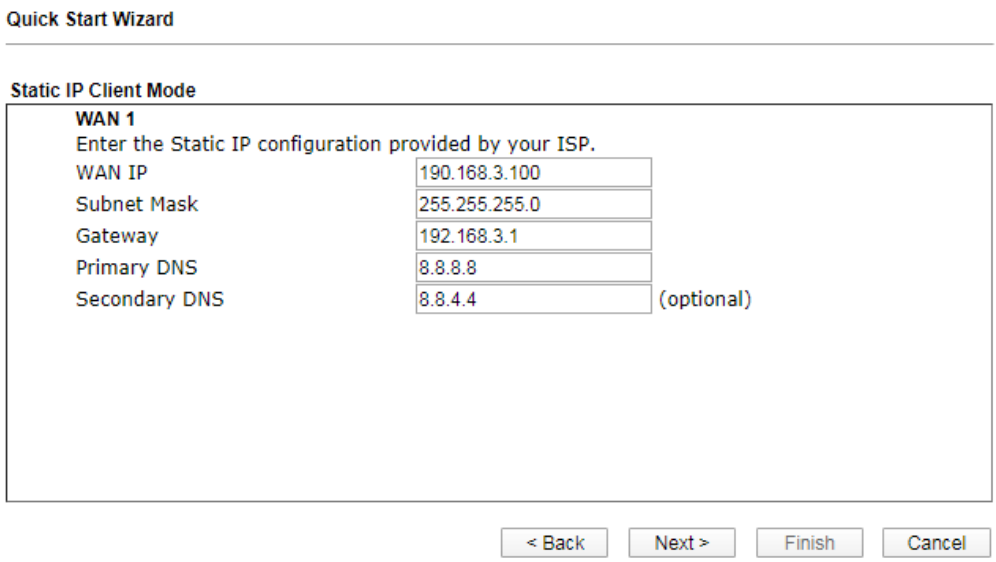
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN1 - Static IP

1. Choose **WAN1** as the WAN Interface. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **Static IP** as the Internet Access type to get the following page.



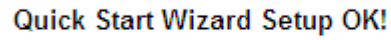
Available settings are explained as follows:

Item	Description
WAN IP	Enter the IP address.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the IP address of gateway.
Primary DNS	Enter the primary IP address for the router.
Secondary DNS	Enter the secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.

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

3. Please Enter the IP address information originally provided by your ISP. Then click **Next** for next step.

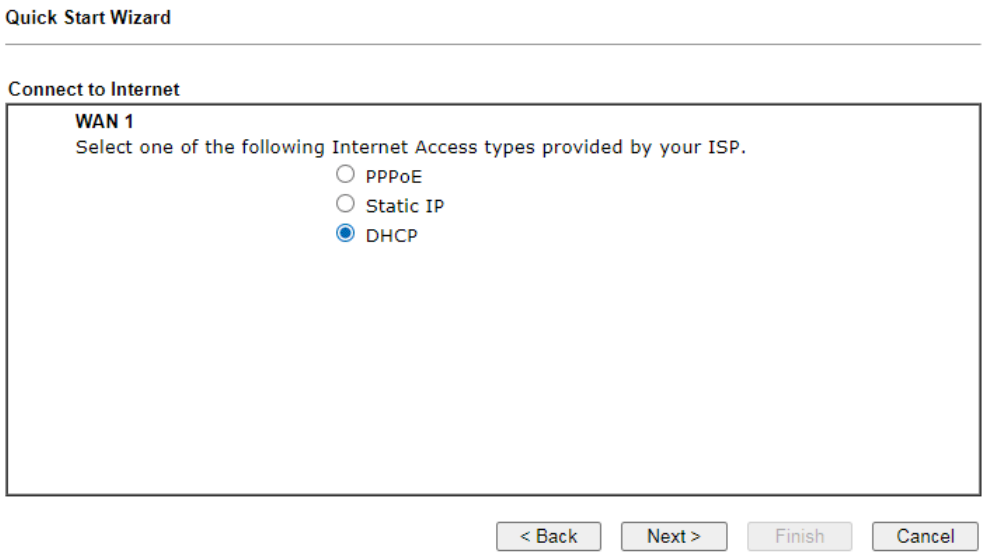
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



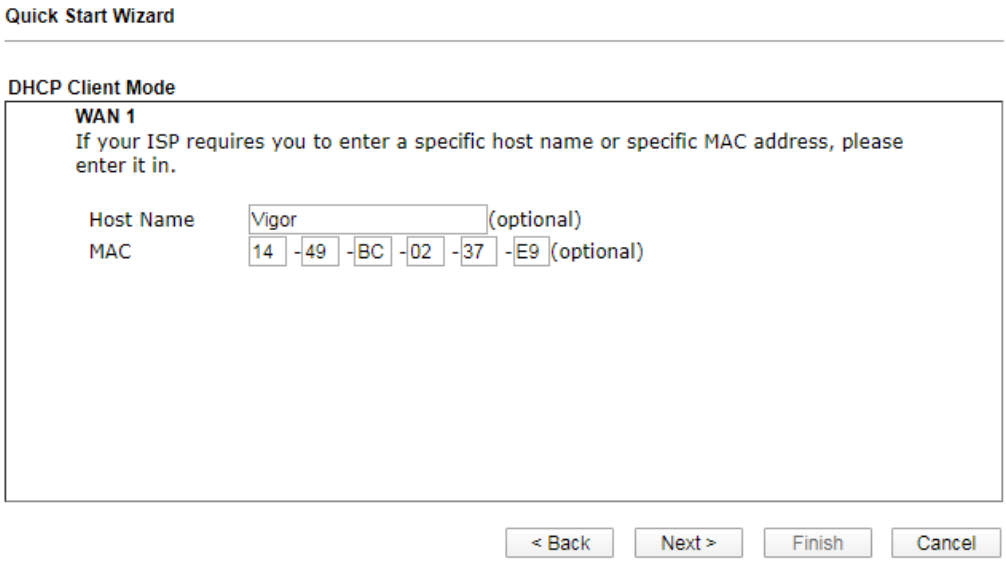
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN1 - DHCP

1. Choose **WAN1** as the WAN Interface. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **DHCP** as the Internet Access type to get the following page.



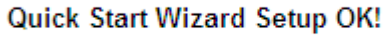
Available settings are explained as follows:

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

Cancel	Click it to give up the quick start wizard.

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

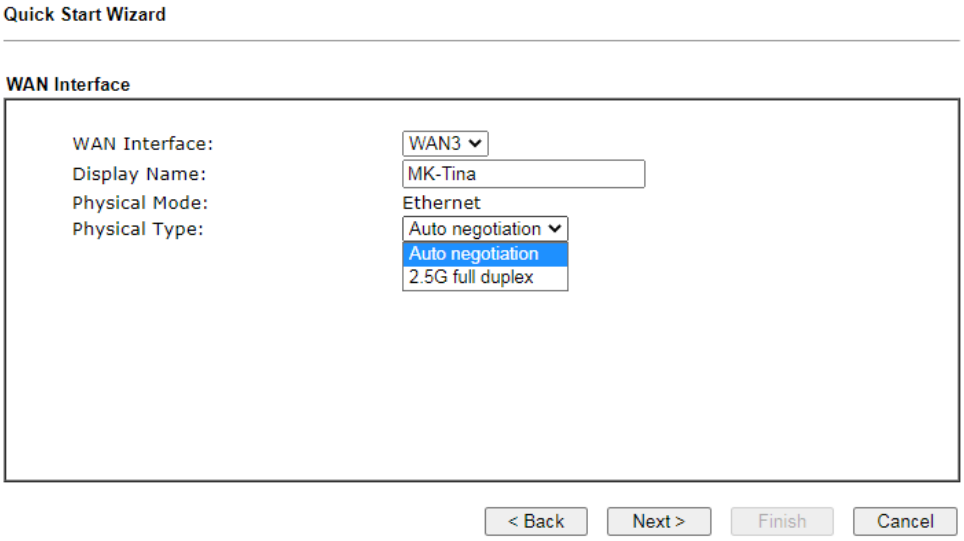
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



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

I-6-2 For WAN3 (Ethernet - 2.5G)

WAN3 shall be used for connection with rate 2.5G.



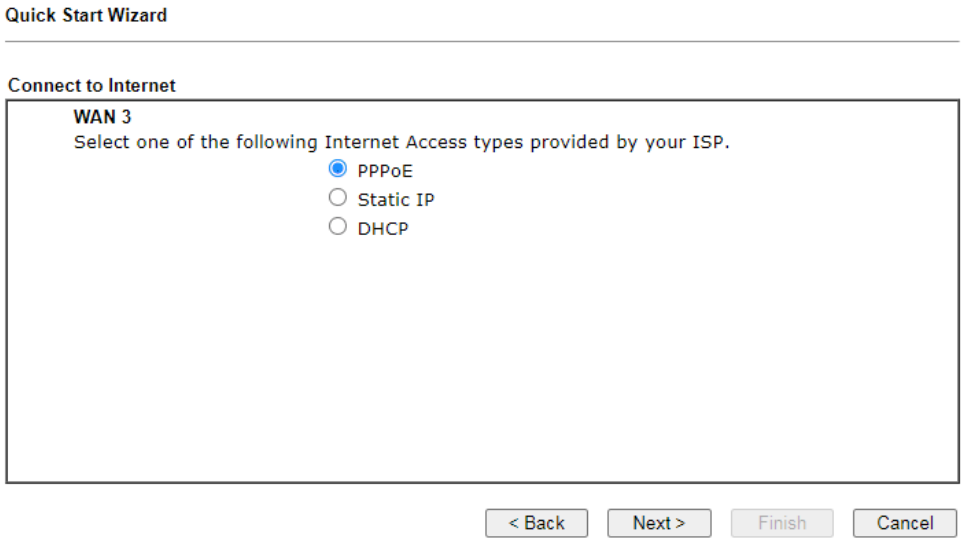
Available settings are explained as follows:

Item	Description
Display Name	Enter a name for the router.
Physical Type	This setting will vary based on the Physical Mode. In general, **Auto negotiation** is suggested.

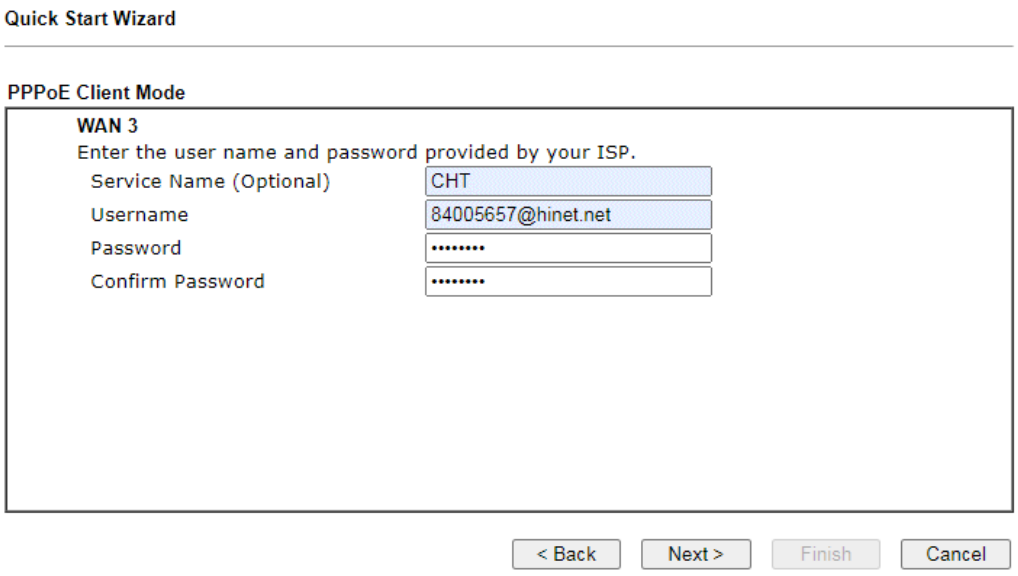
On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

Ethernet WAN3 - PPPoE

1. Choose **WAN3** as the WAN Interface. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



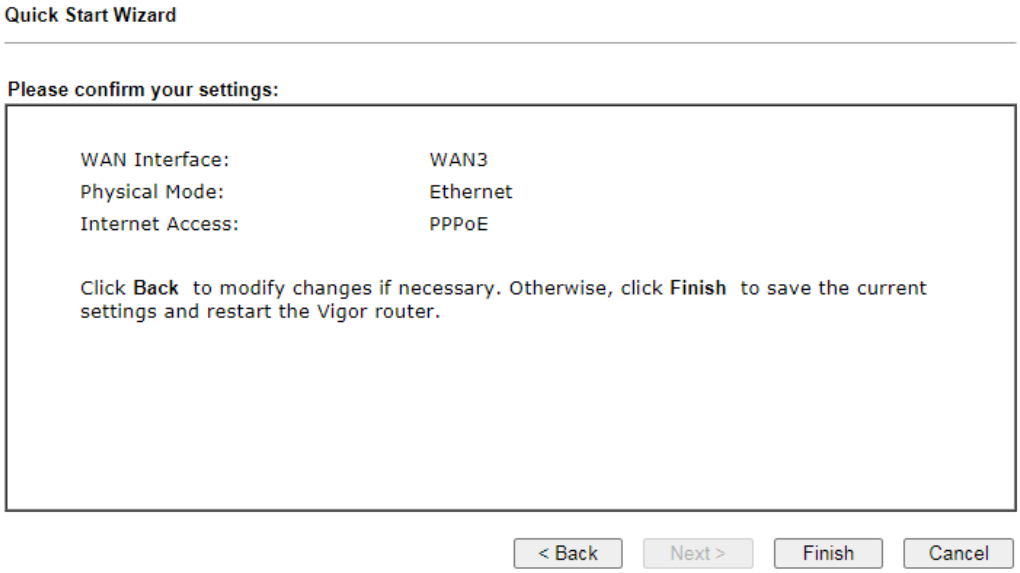
2. Click **PPPoE** as the Internet Access Type to get the following page.



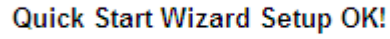
Available settings are explained as follows:

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

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



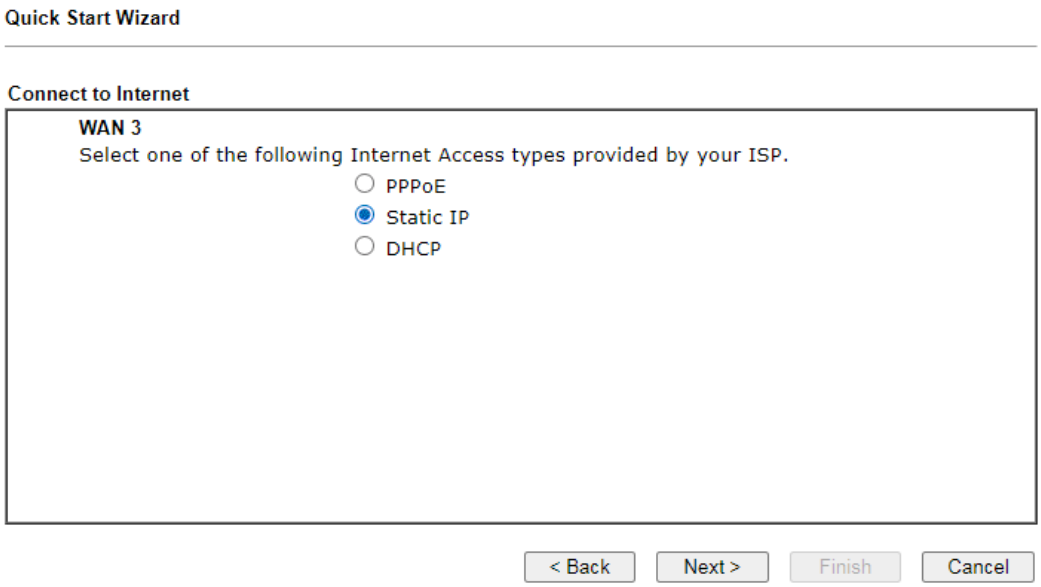
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



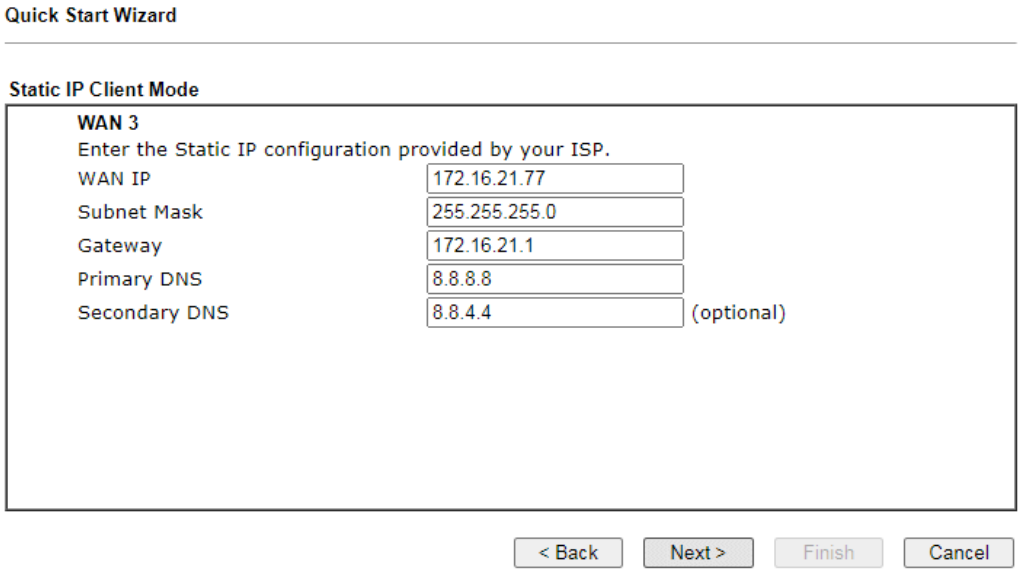
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN3 - Static IP

1. Choose **WAN3** as the WAN Interface. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **Static IP** as the Internet Access type to get the following page.

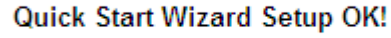


Available settings are explained as follows:

Item	Description
WAN IP	Enter the IP address.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the IP address of gateway.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Please enter the IP address information originally provided by your ISP. Then click **Next** for next step.

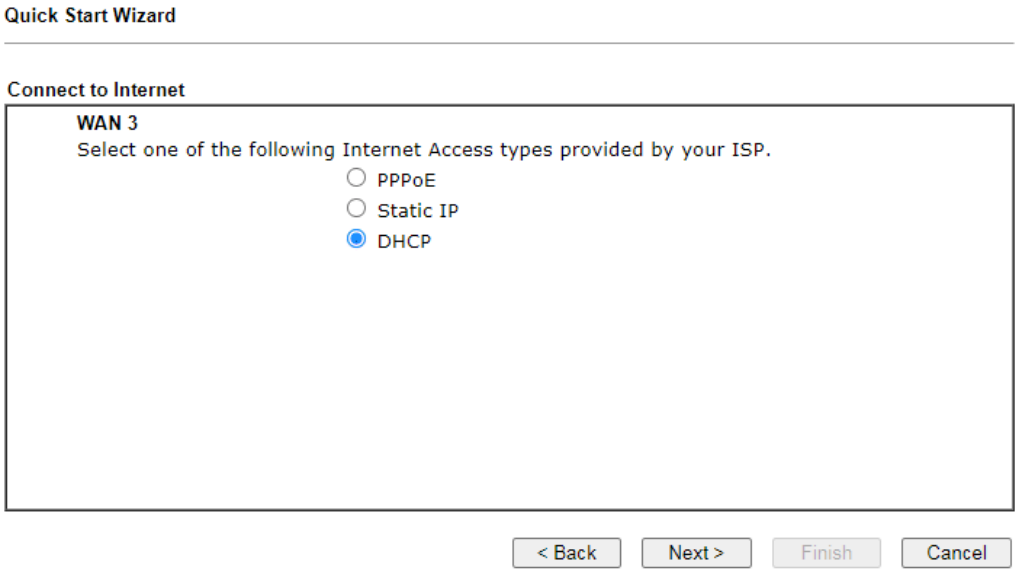
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



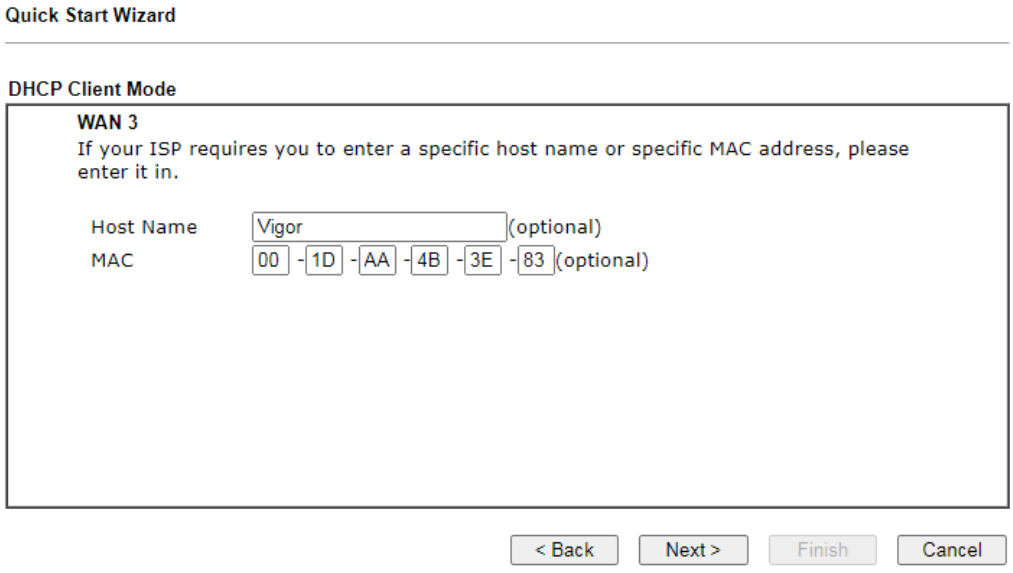
5. Now, you can enjoy surfing on the Internet.

Wireless WAN3 - DHCP

1. Choose **WAN3** as the WAN Interfac. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **DHCP** as the Internet Access type to get the following page.

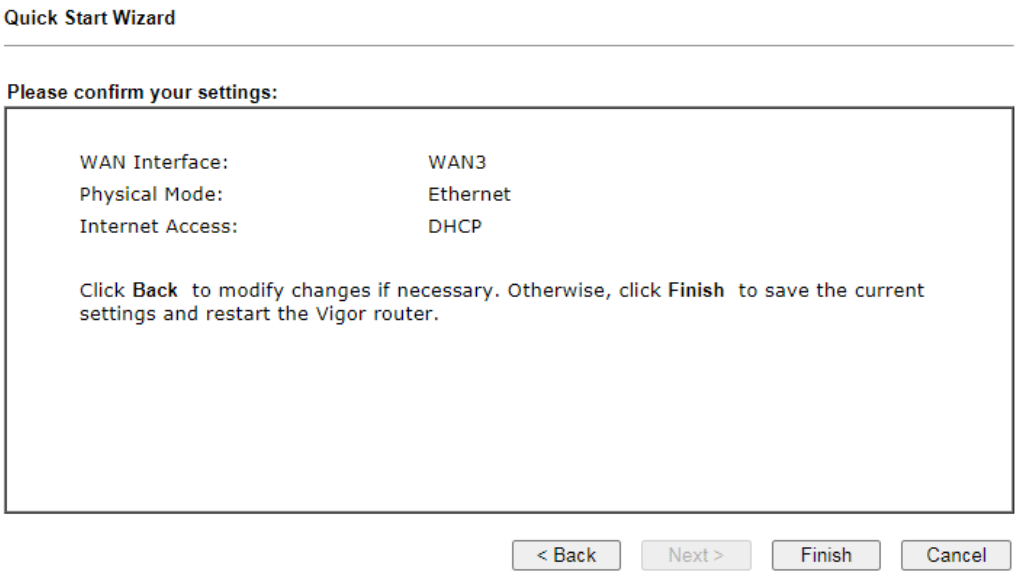


Available settings are explained as follows:

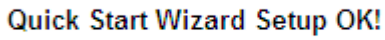
Item	Description
Host Name	Enter the name of the host. **Note:** The maximum length of the host name you can set is 39 characters.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
Back	Click it to return to previous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

Cancel	Click it to give up the quick start wizard.

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



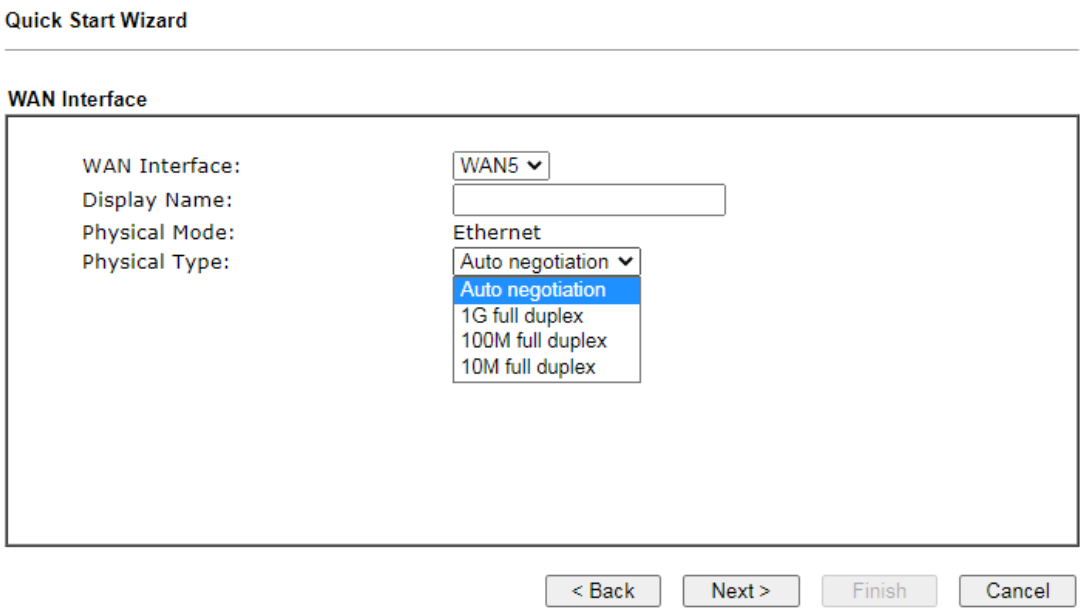
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



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

I-6-3 For WAN5~WAN8 (Etherent)

WAN5~WAN8 can be configured for physical mode of Ethernet.



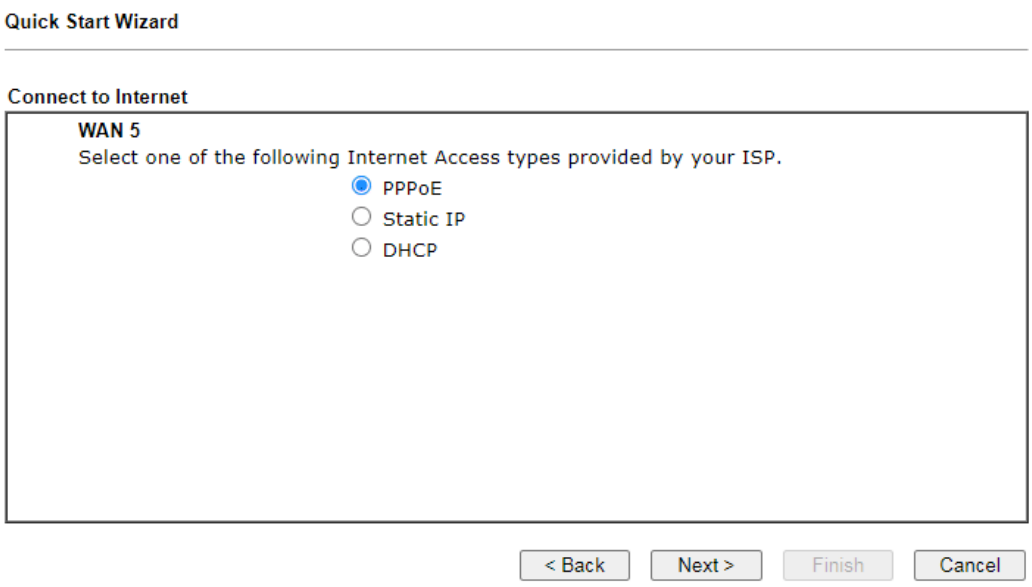
Available settings are explained as follows:

Item	Description
Display Name	Enter a name for the router.
Physical Type	This setting will vary based on the Physical Mode. In general, **Auto negotiation** is suggested.

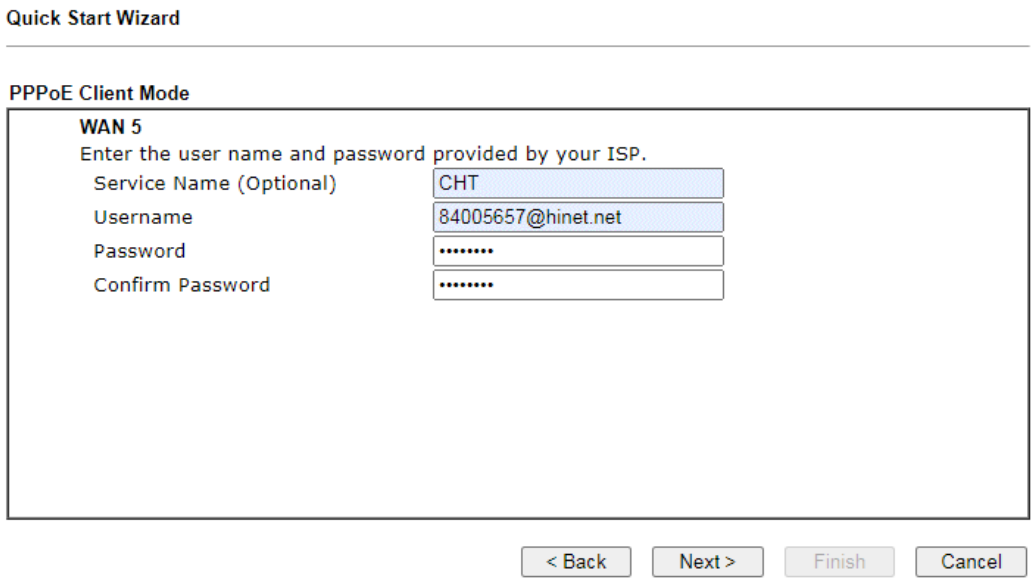
On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

Ethernet WAN5 - PPPoE

1. Choose **WAN5** as the WAN Interface. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



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



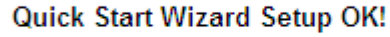
Available settings are explained as follows:

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

Item	Description
Cancel	Click it to give up the quick start wizard.

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

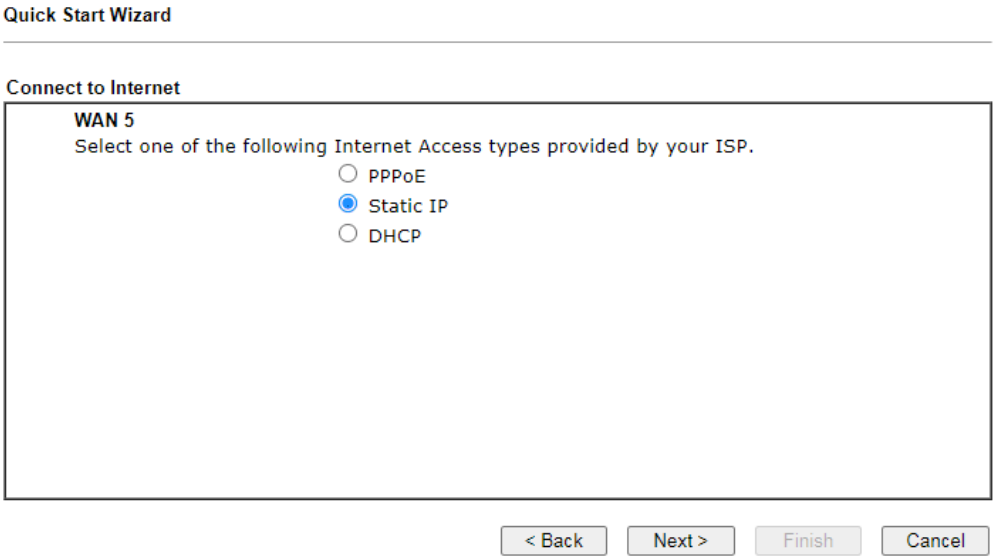
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



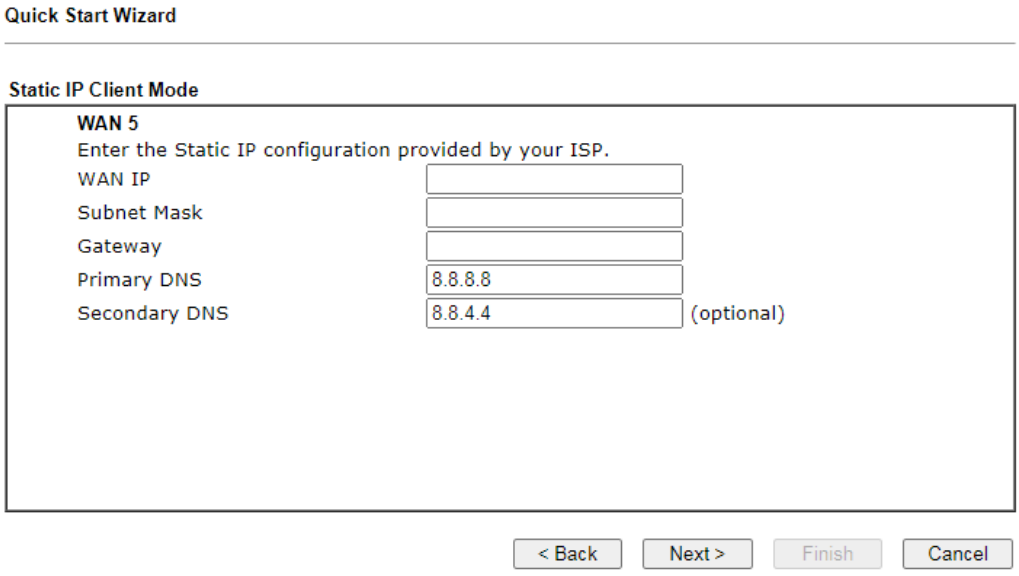
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN5 - Static IP

1. Choose **WAN5** as the WAN Interface. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **Static IP** as the Internet Access type to get the following page.

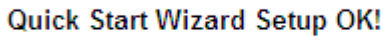


Available settings are explained as follows:

Item	Description
WAN IP	Enter the IP address.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the IP address of gateway.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Please enter the IP address information originally provided by your ISP. Then click **Next** for next step.

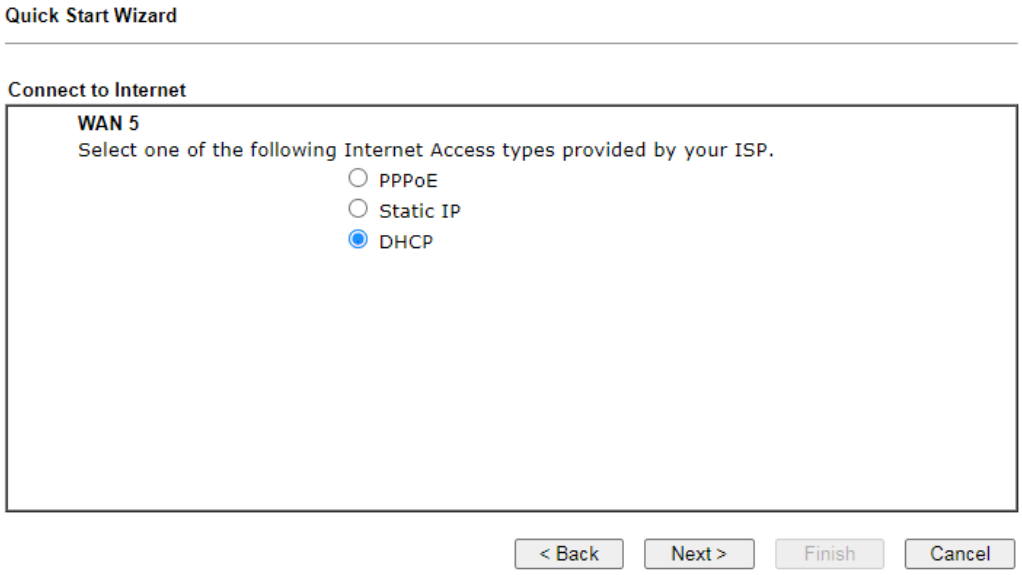
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



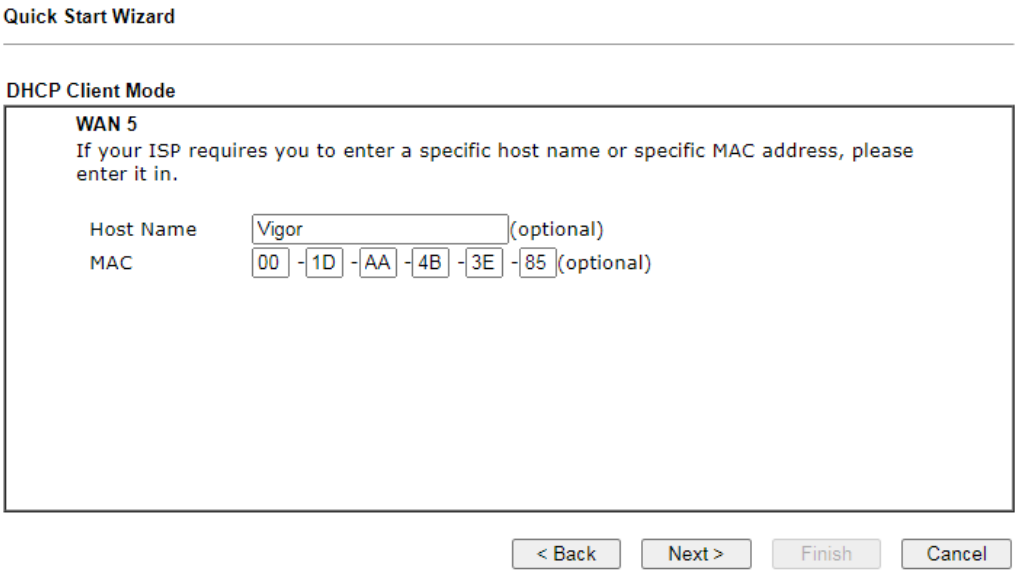
5. Now, you can enjoy surfing on the Internet.

Wireless WAN5 - DHCP

1. Choose **WAN5** as the WAN Interfac. Click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **DHCP** as the Internet Access type to get the following page.

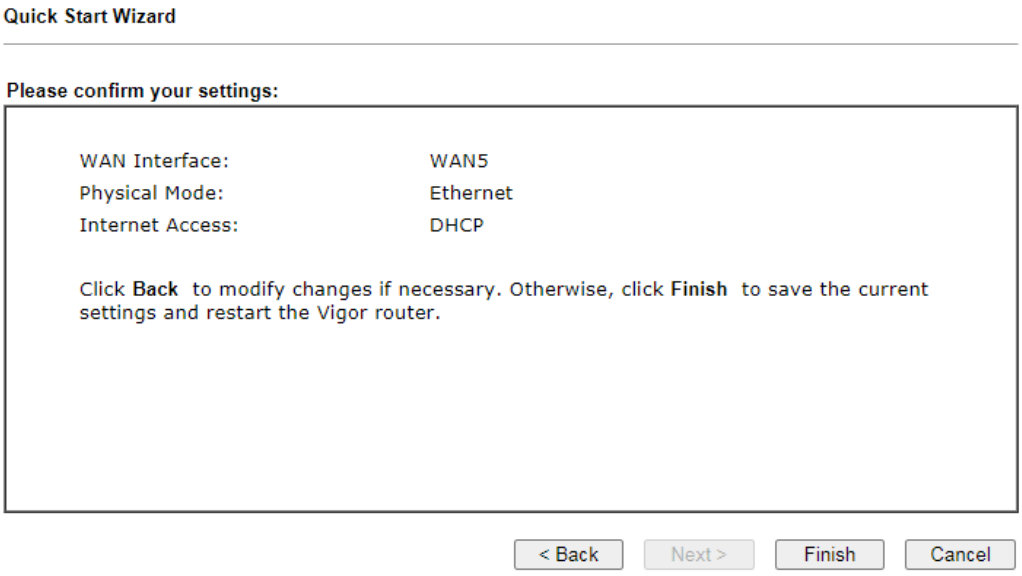


Available settings are explained as follows:

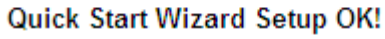
Item	Description
Host Name	Enter the name of the host. **Note:** The maximum length of the host name you can set is 39 characters.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
Back	Click it to return to previous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

Cancel	Click it to give up the quick start wizard.

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



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



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

I-7 Service Activation Wizard

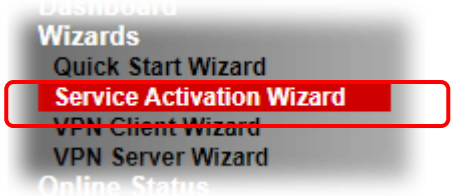
Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, therefore, please type "admin/admin" on Username/Password while Logging into the web user interface.**

Service Activation Wizard is a tool which allows you to use trial version of WCF directly without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com. For using Web Content Filter Profile, please refer to later section **Web Content Filter Profile** for detailed information.

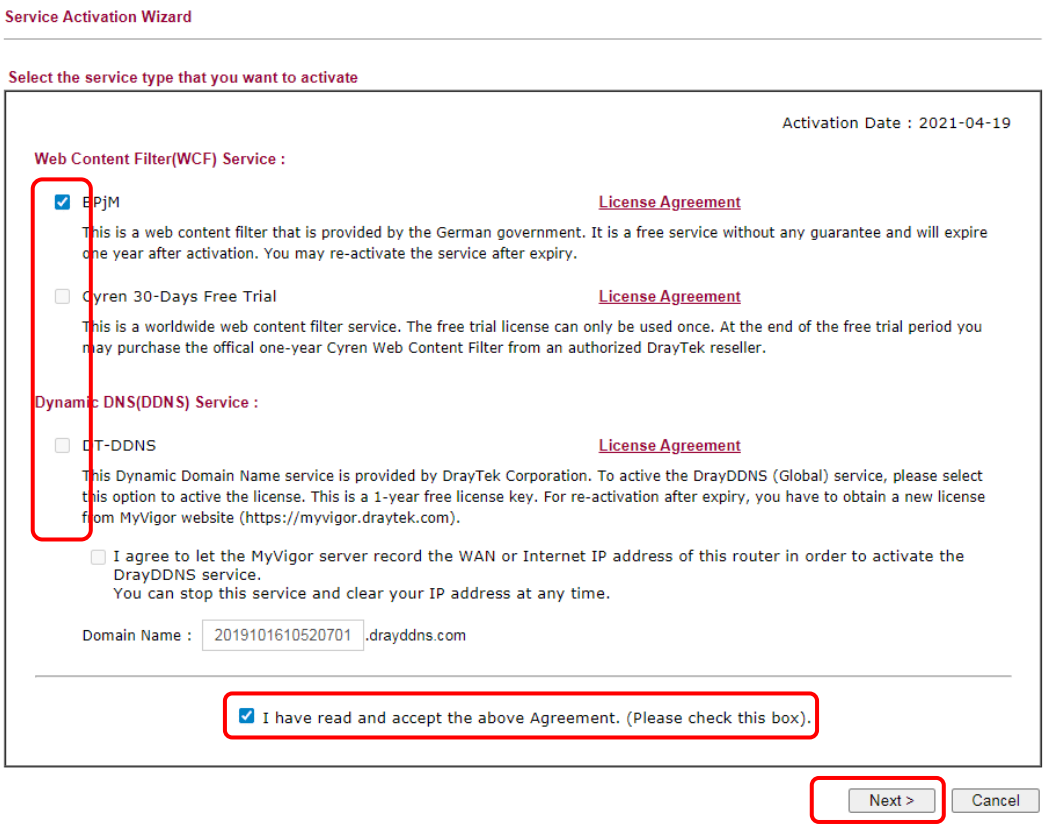
Now, follow the steps listed below to activate WCF feature for your router.

Info	Such function is available only for Admin Mode.

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



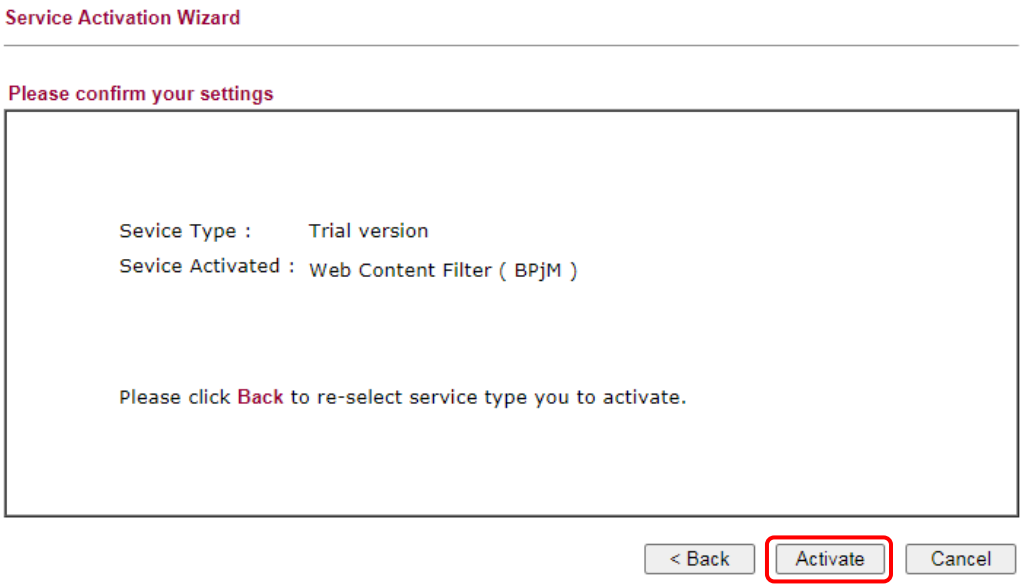
2. The screen of **Service Activation Wizard** will be shown as follows. You can activate the Web content filter services and/or DDNS service at the same time or individually. When you finish the selection, please click **Next**.



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

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



Info

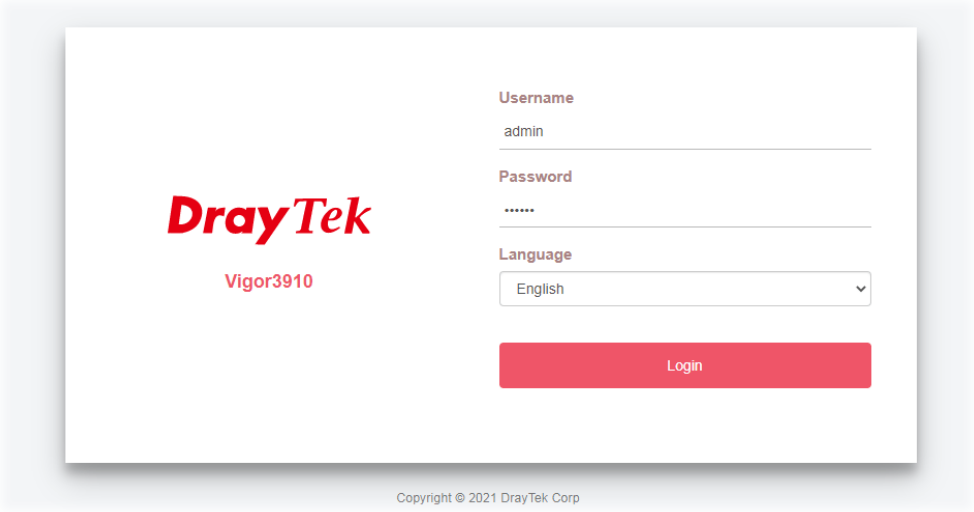
The service will be activated and applied as the default rule configured in Firewall>>General Setup.

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

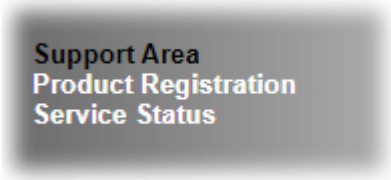
I-8 Registering Vigor Router

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.

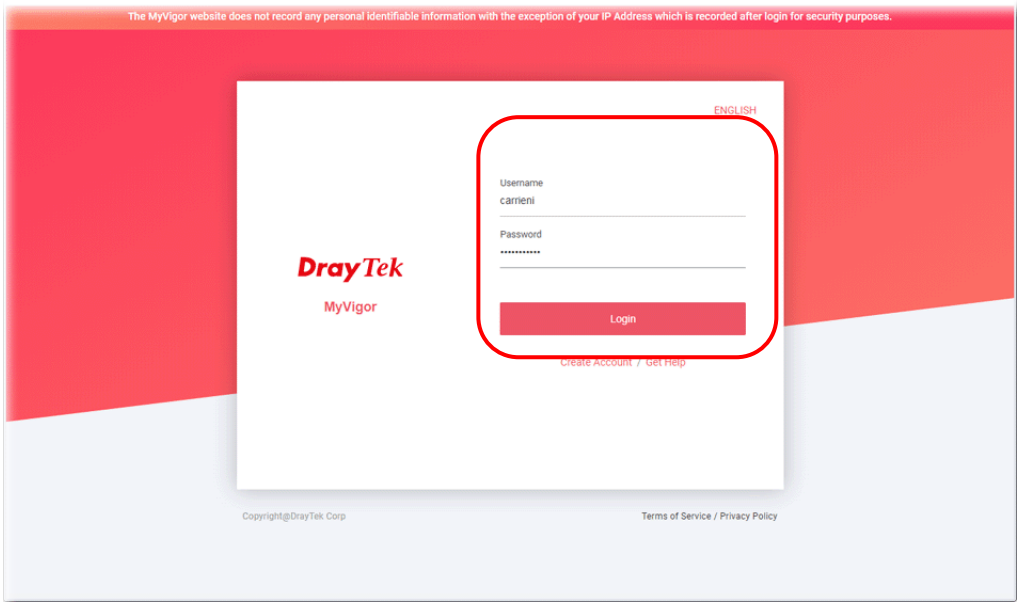
1 Please login the web configuration interface of Vigor router by typing "**admin/admin**" as User Name / Password.



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



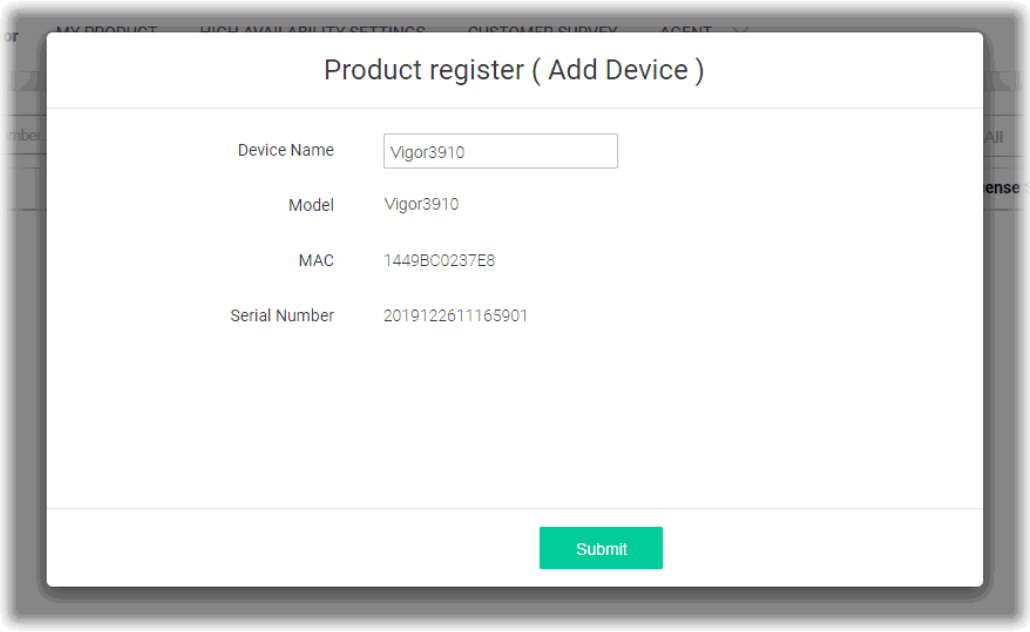
3 A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



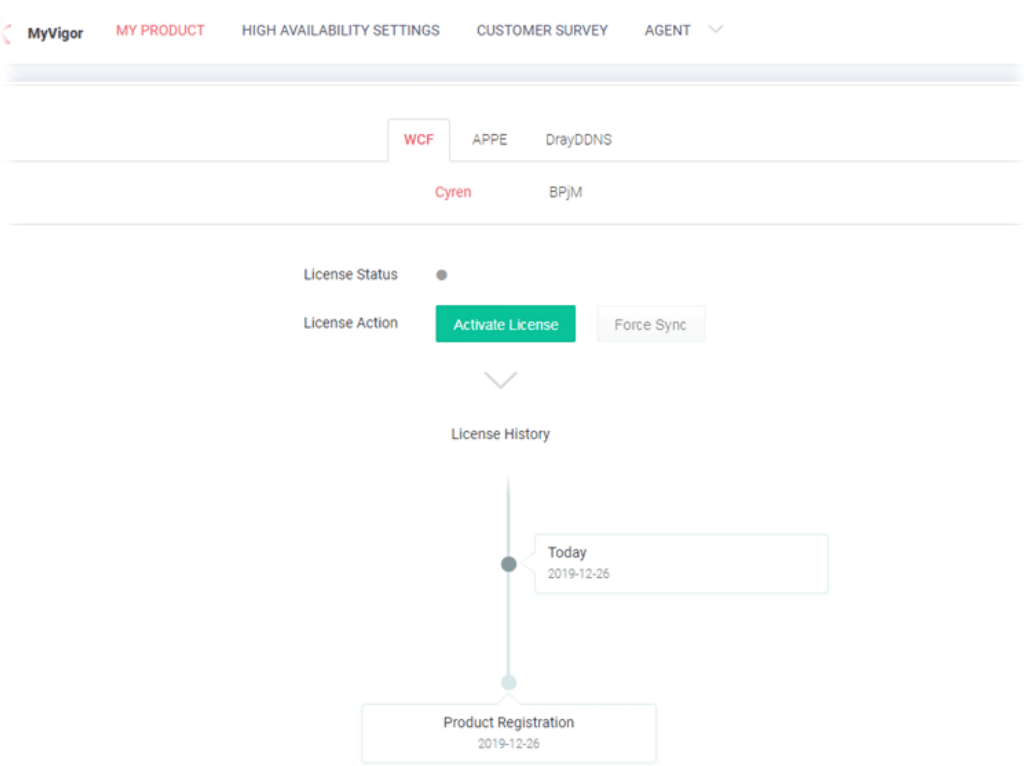
Info

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

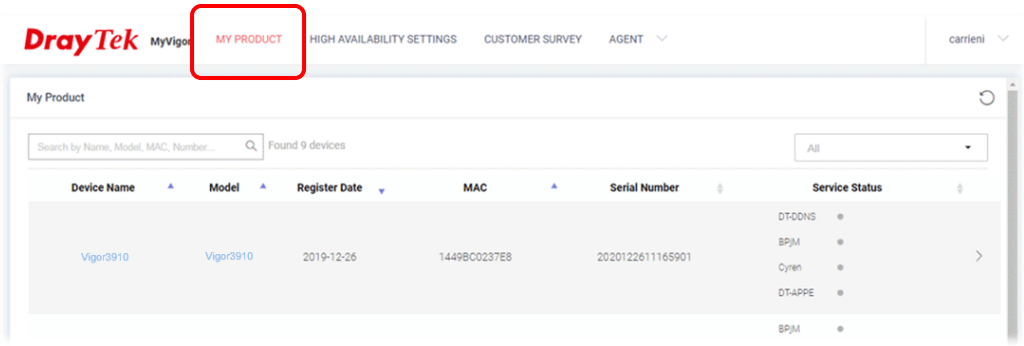
4 The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click **Submit**.



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



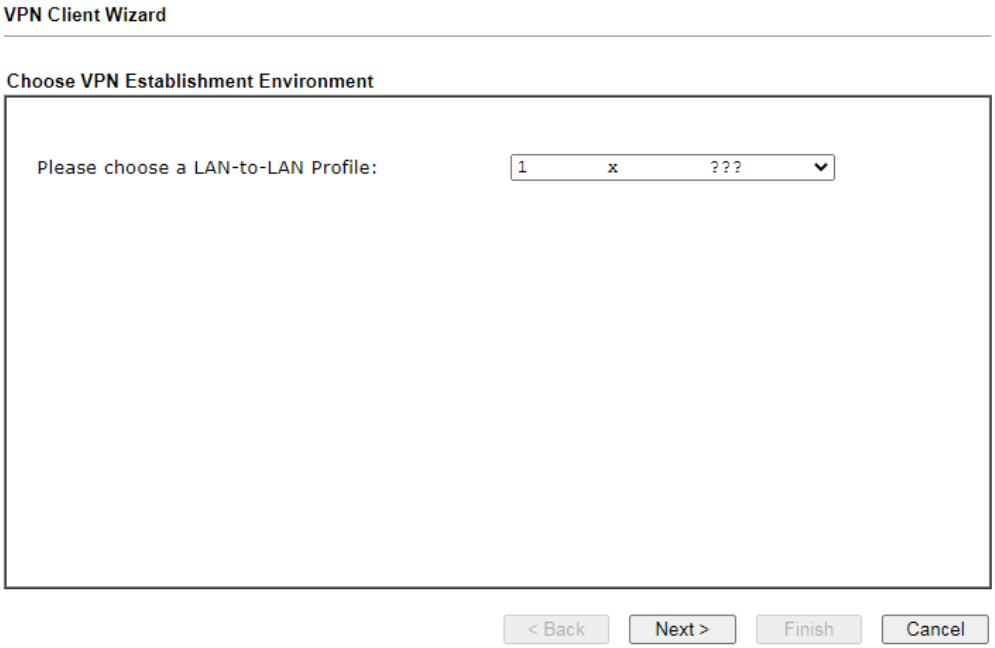
6 Clicking **MYPRODUCT** for viewing the general information of the registered router on MyVigor website.



I-9 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.

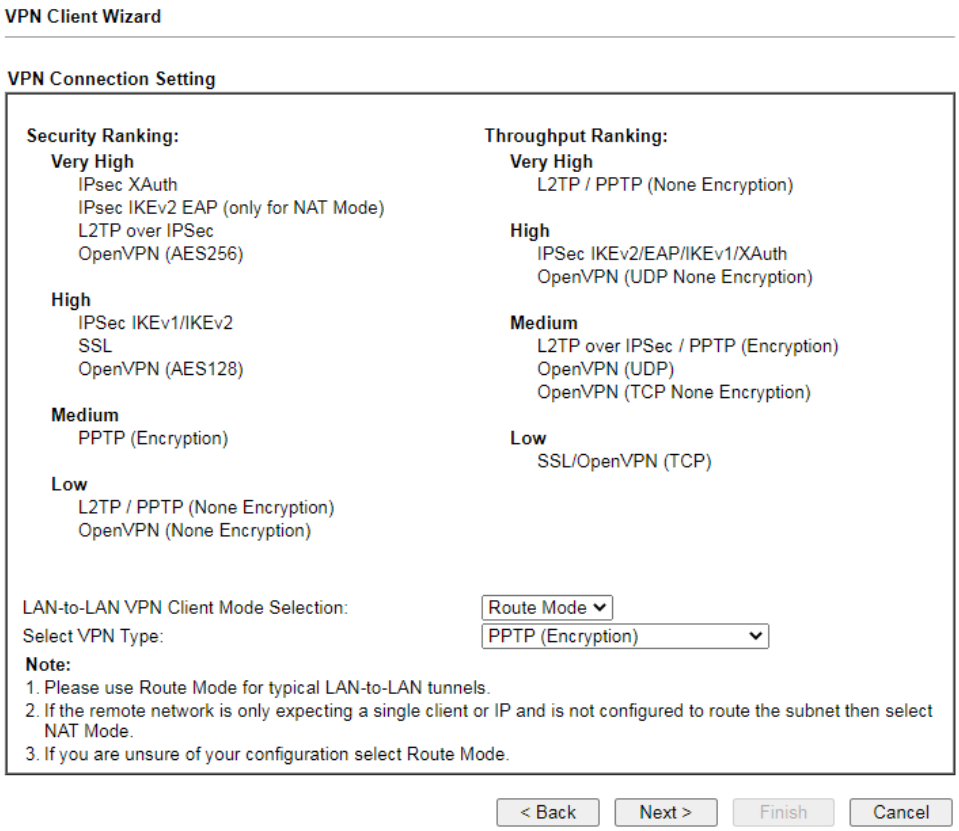
1. On the menu bar, click on **Wizards,** and then **VPN Client Wizard**.



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.

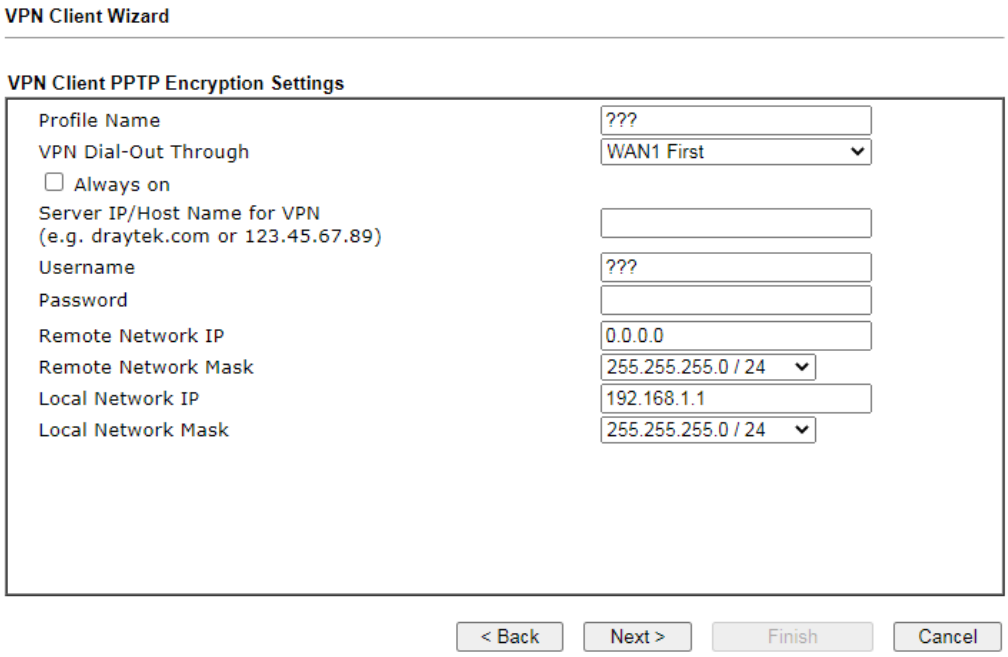


Available settings are explained as follows:

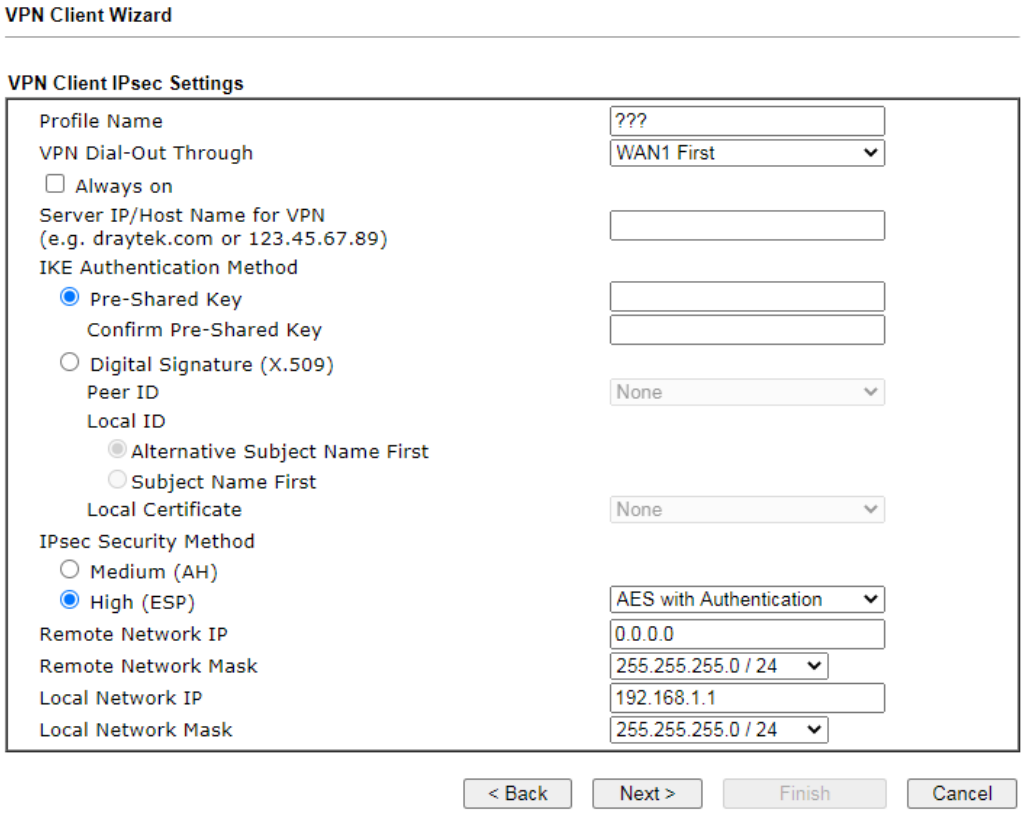
Item	Description
LAN-to-LAN Client Mode Selection	**Route Mode –** All traffic between the local network and the remote network bear the originating IP addresses. Select this if the VPN server can establish routes to handle inter-LAN traffic routing. **NAT Mode –** The VPN client (local router) uses 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.

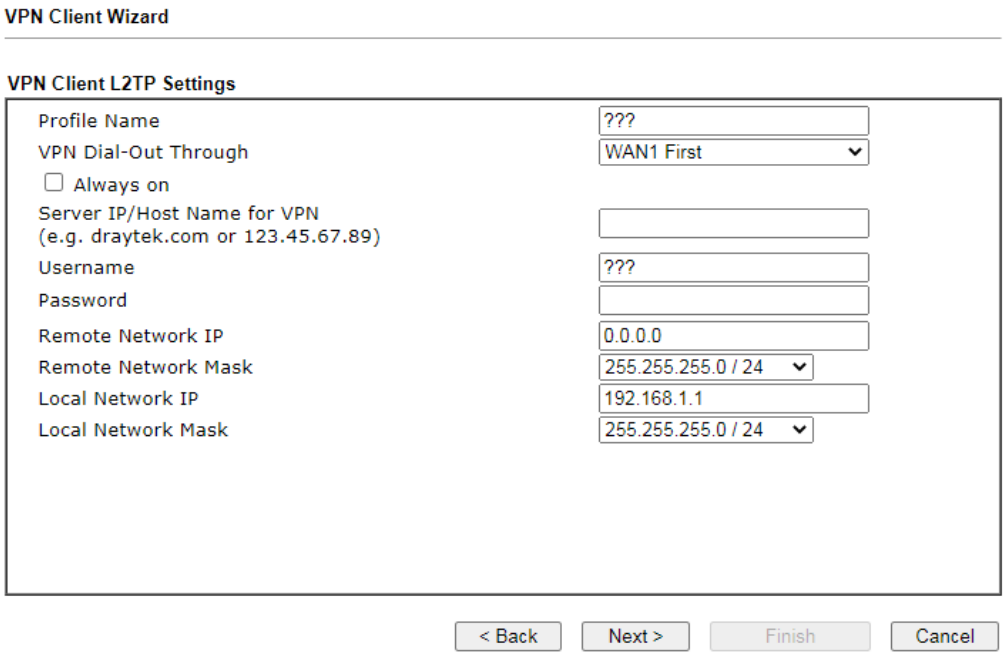
If you have selected **PPTP (None Encryption)** or **PPTP (Encryption)**, the following configuration screen appears.



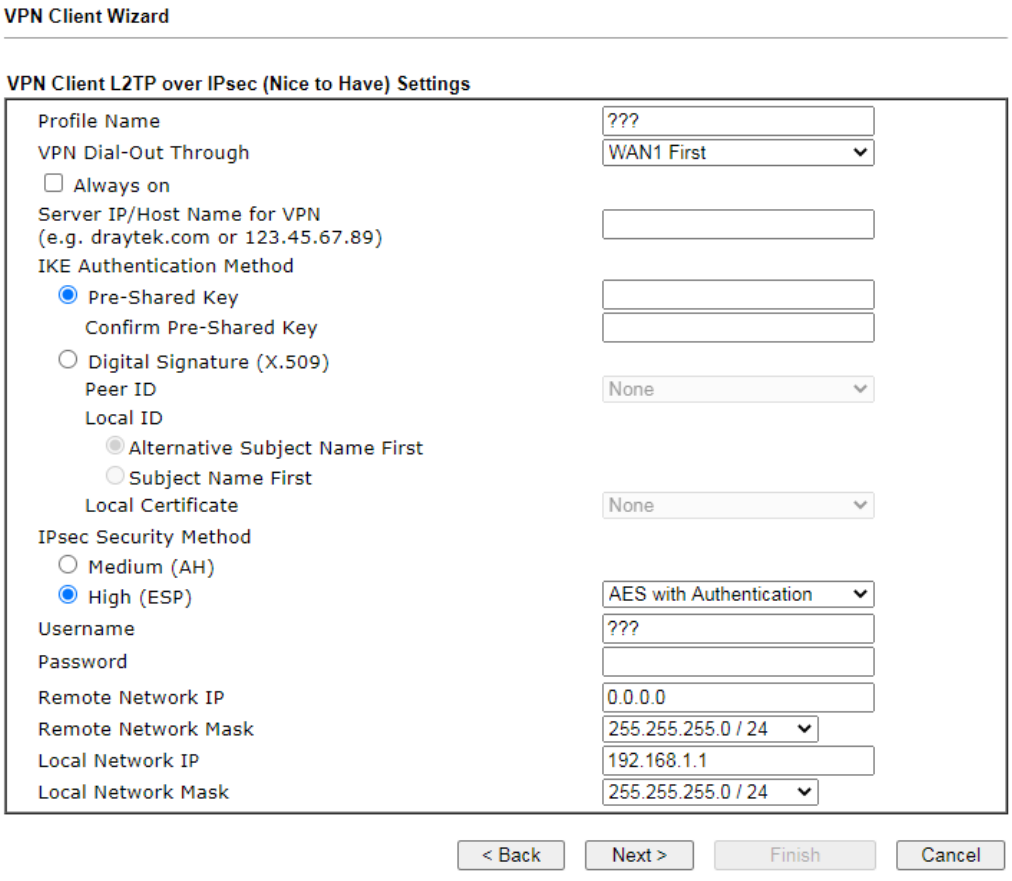
If you have selected **IPsec**, the following configuration screen appears.



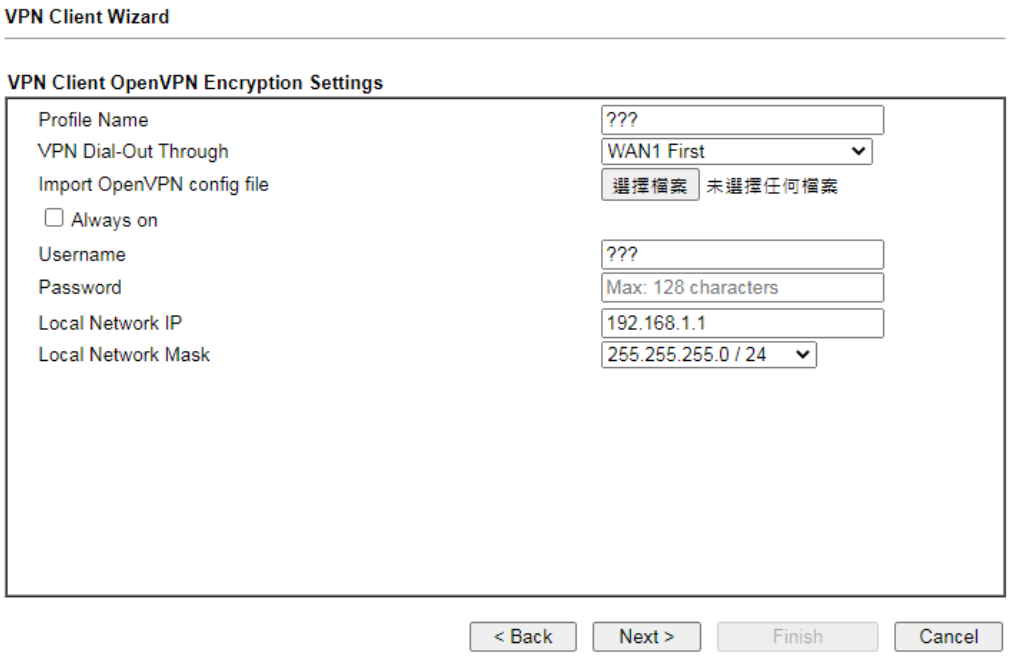
If you have selected **SSL/L2TP**, the following configuration screen appears.



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



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

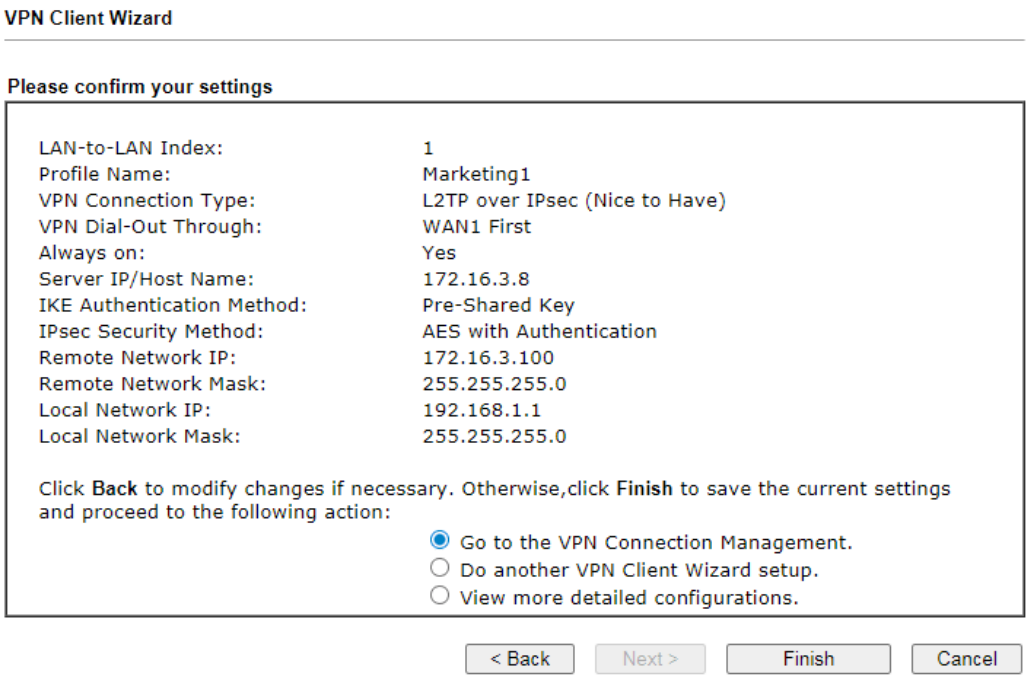


Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. The maximum length of the Profile Name is 10 characters.
VPN Dial-Out Through	The WAN interface to be used for dialing out to establish the VPN tunnel. **WANx First** - The Router first attempts to establish the VPN tunnel using this WAN interface. When that is unsuccessful, it will attempt to use other WAN interfaces. **WANx Only** - The Router will establish the VPN tunnel using this WAN interface only.
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.
Import OpenVPN config file	Select to import an OpenVPN configuration file from a specified OpenVPN server (e.g., Vigor router, PC, other VPN provider and etc.) onto to Vigor router. Later, as a VPN client, this router can access into VPN server via the username and password.
Username	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:

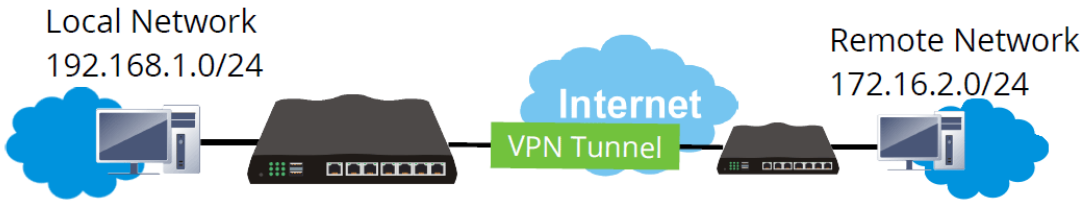
Item	Description
Go to the VPN Connection Management	Proceed to **VPN and Remote Access>>Connection Management** to manage VPN sessions.
Do another VPN Client Wizard Setup	Rerun the VPN Client Wizard to configure another LAN-to-LAN VPN profile.
View more detailed configuration	Open this profile in **VPN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

I-10 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.

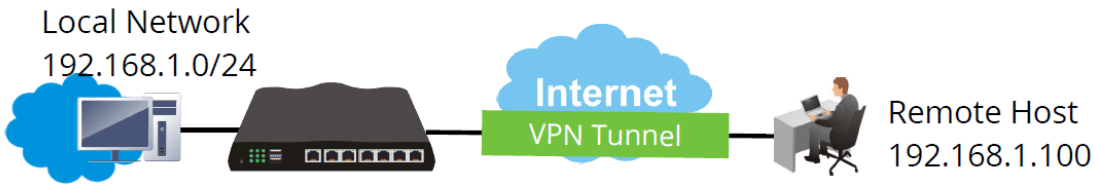
Site-to-Site (LAN-to-LAN)

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



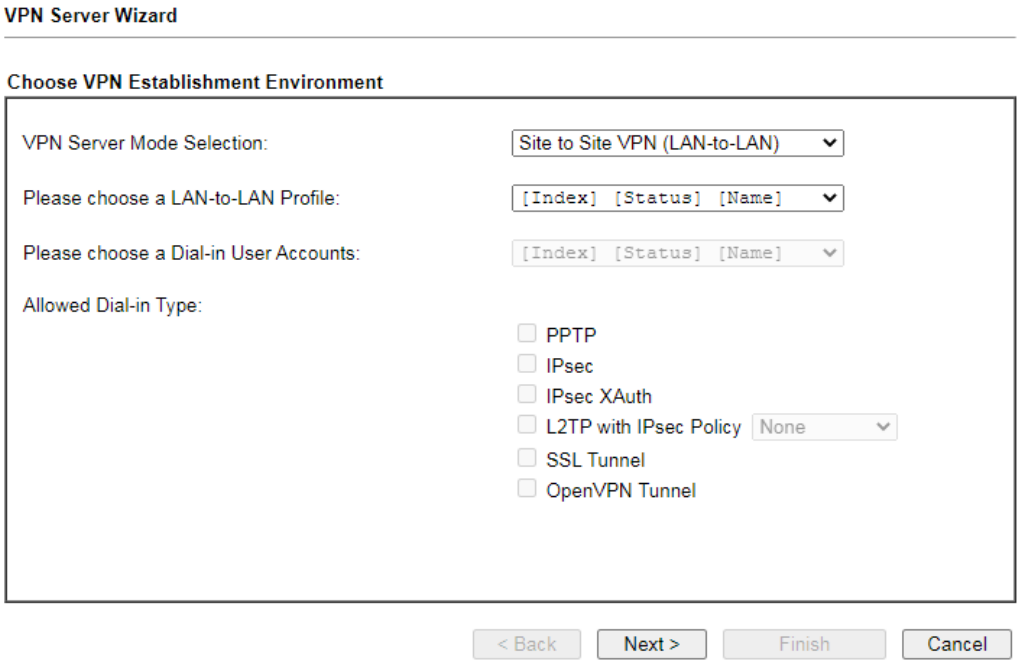
Remote Access (Remote Dial-in)

- 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**.

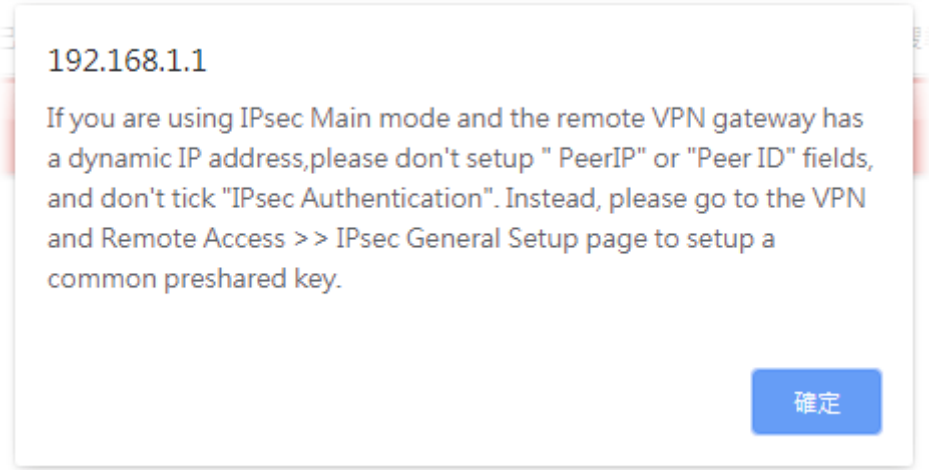


Available settings are explained as follows:

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.

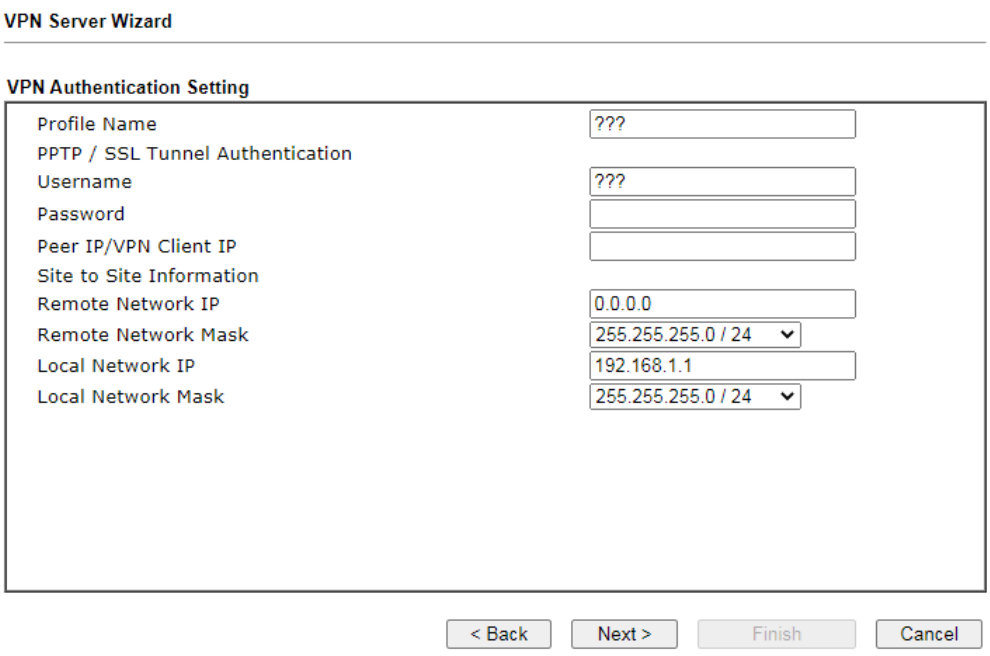


Click **OK** to dismiss the dialog box and proceed to the next page.

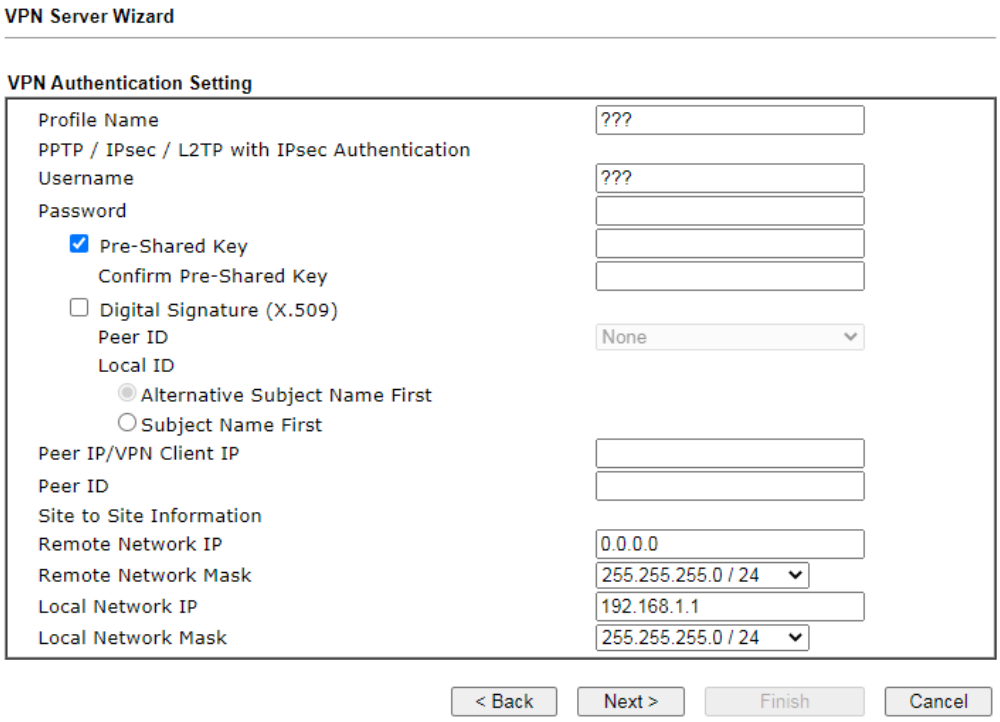
If you have chosen to configure a LAN-to-LAN VPN profile, proceed to step 4.

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

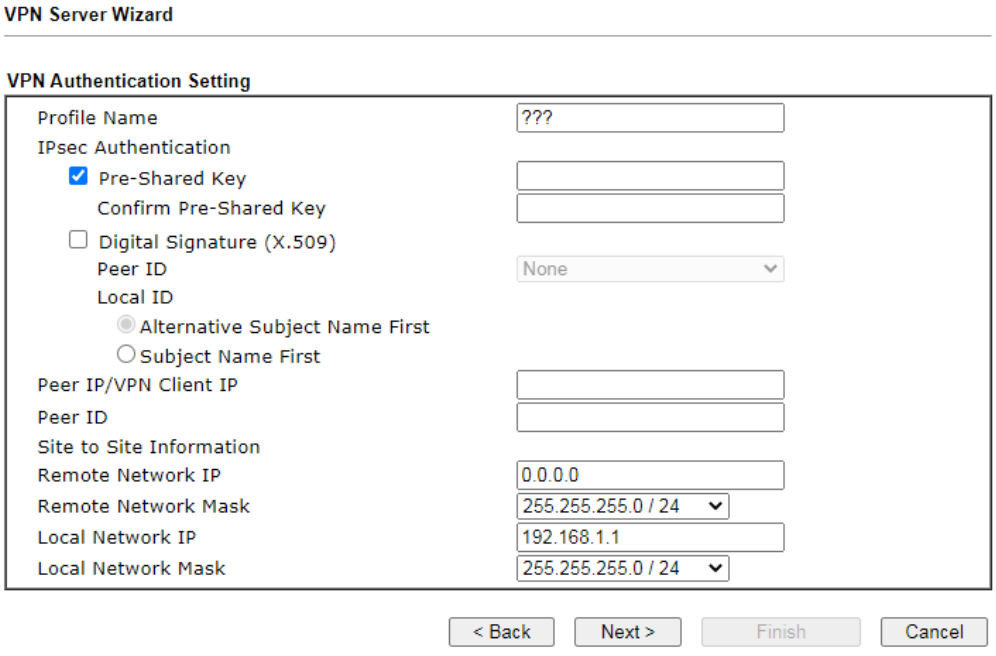
4. The **Site to Site VPN (LAN-to-LAN)** configuration page appears as follows if you have selected **PPTP/SSL**.



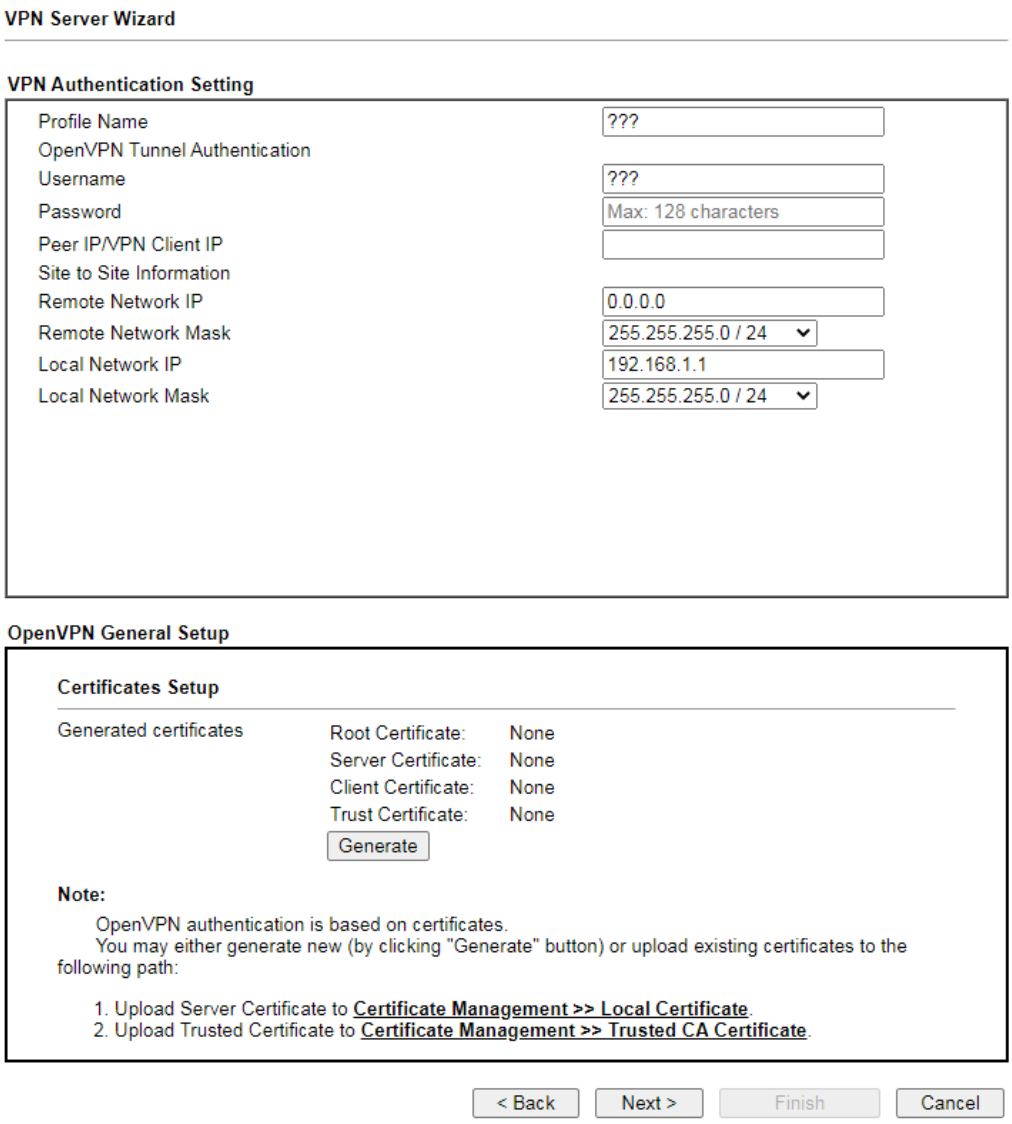
If you have selected **PPTP & IPsec & L2TP** (three types) or **PPTP & IPsec** (two types) or **L2TP with Policy (Nice to Have/Must),** the following configuration screen appears.



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



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

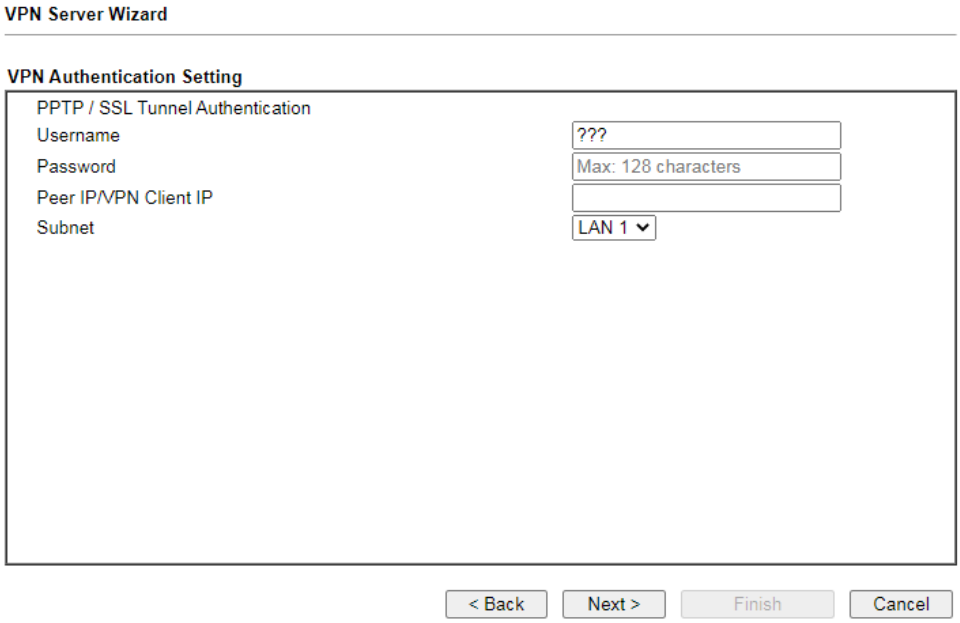


Available settings are explained as follows:

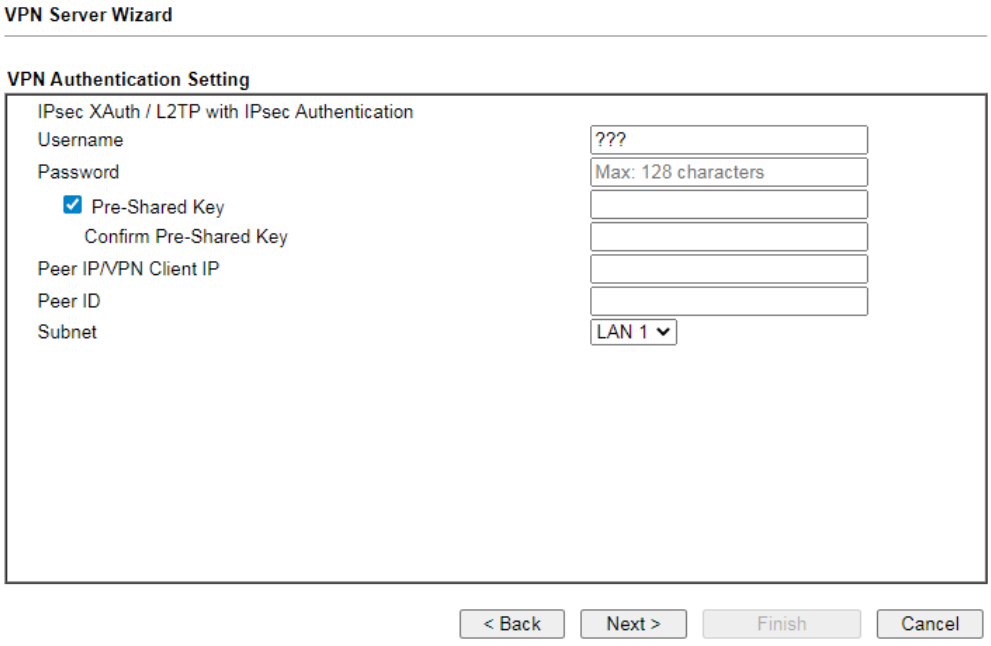
Item	Description
Profile Name	Name to identify this VPN profile.
User Name	Used by the remote LAN to establish a VPN connection. The length of the user name is limited to 11 characters.
Password	Used by the remote LAN to establish a VPN connection. The length of the password is limited to 11 characters.
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.
OpenVPN General Setup	**Generate** - Click to generate certificate for OpenVPN authentication. Or upload an existing certificate from **Local Certificate** or **Trusted CA Certificate** page.

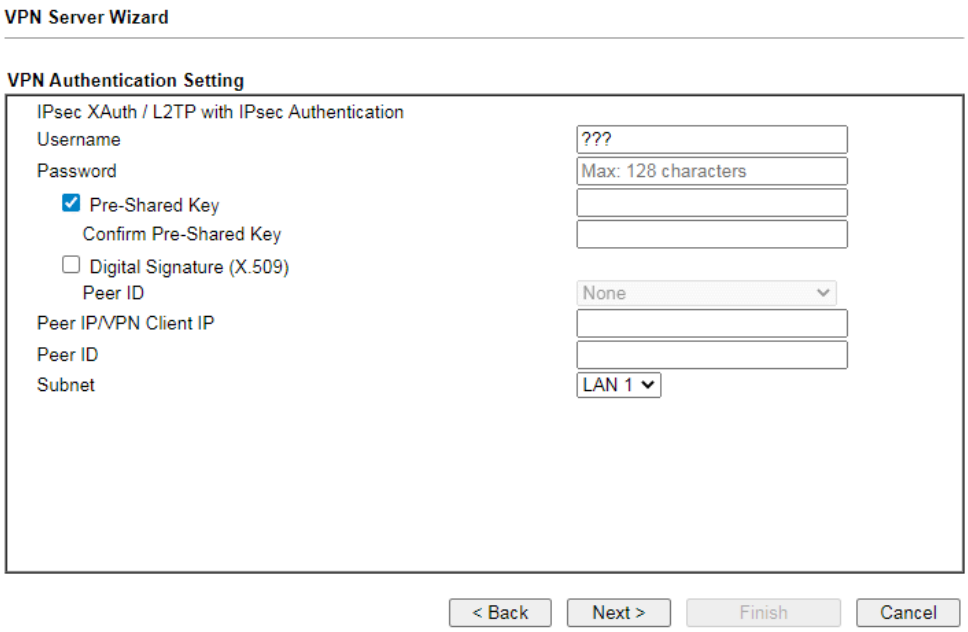
5. The **Remote Dial-in User (Teleworker)** VPN configuration page appears as follows if you have selected **PPTP/SSL**.



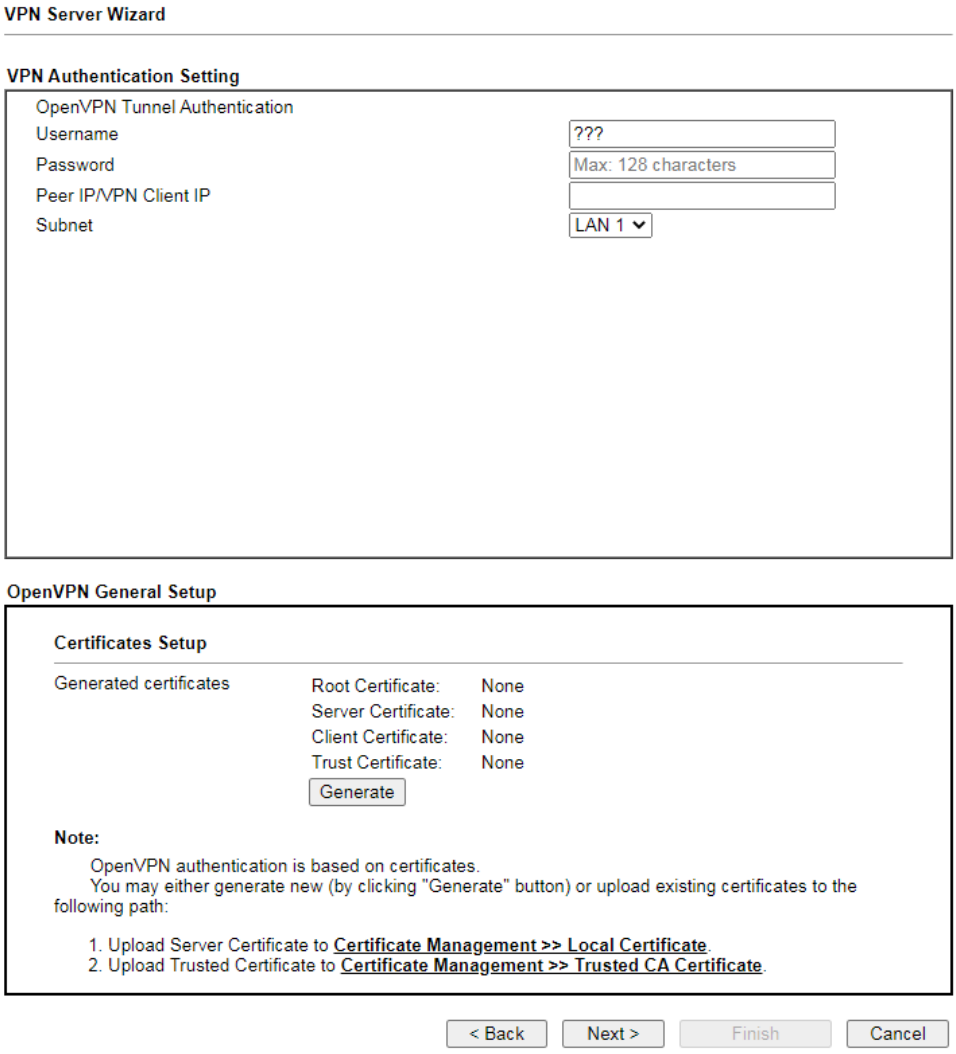
If you have selected **IPsec XAuth/L2TP with IPsec Policy (None),** the following configuration screen appears.



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



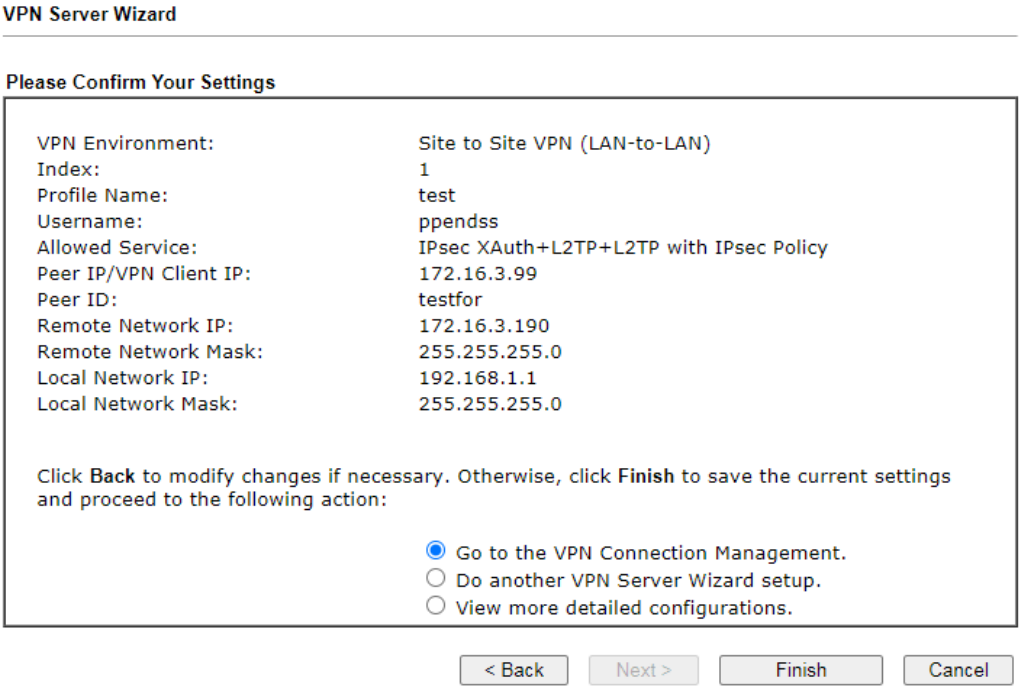
If you have selected **OpenVPN Tunnel,** the following configuration screen appears.



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.
Subnet	Select an interface.
OpenVPN General Setup	**Generate** - Click to generate certificate for OpenVPN authentication. Or upload existing certificates from **Local Certificate** or **Trusted CA Certificate** page.

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.

Part II Connectivity

WAN

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

LAN

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.

NAT

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.

Applications

DNS, LAN DNS, IGMP, WOL, RADIUS, ...

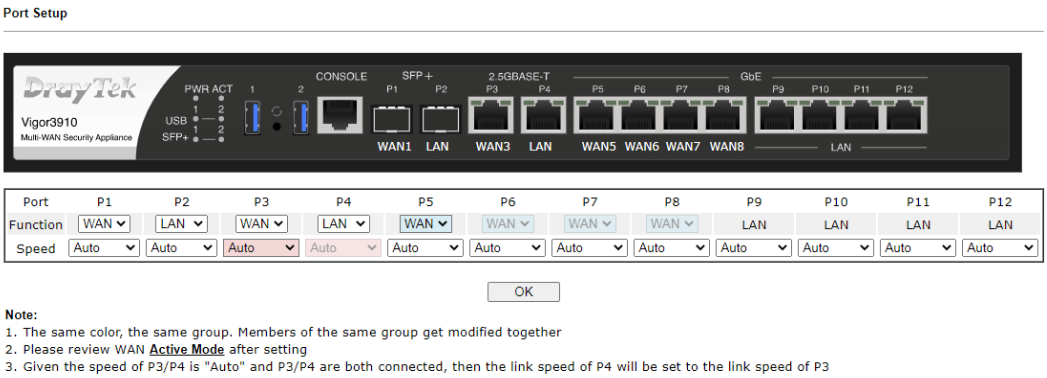
Routing

Static Route, Load-Balance/Route Policy, OSPF, BGP

II-1 Port Setup

This page is used for configuring tranmission rate for LAN and WAN ports respectively.

Due to hardware restriction, the speed of P3 is the same as the speed of P4. So whenever P3 is changed, P4 is changed too and vice versa.



Available settings are explained as follows:

Item	Description
Port	Display the physical ports on Vigor router.
Function	P1 ~ P8 - These ports are switchable between WAN and LAN ports.
Speed	P1 ~ P2 - Available options include Auto, 10G FD, 2.5G FD, 1G FD and 1G AN. P3 ~ P4 - Available options include Auto, 2.5G AN, 1G AN and 100M AN. Due to the hardware limitation, the speed for P4 is the same as P3. P5 ~ P12- Available options include Auto, 1G AN, 100M AN, and 10M AN.

II-2 WAN

It allows users to access Internet.

Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

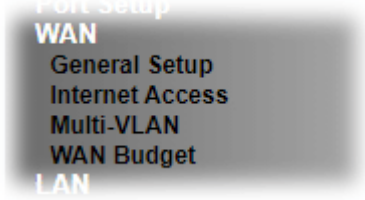
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the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

Get Your Public IP Address from ISP

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

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

Web User Interface

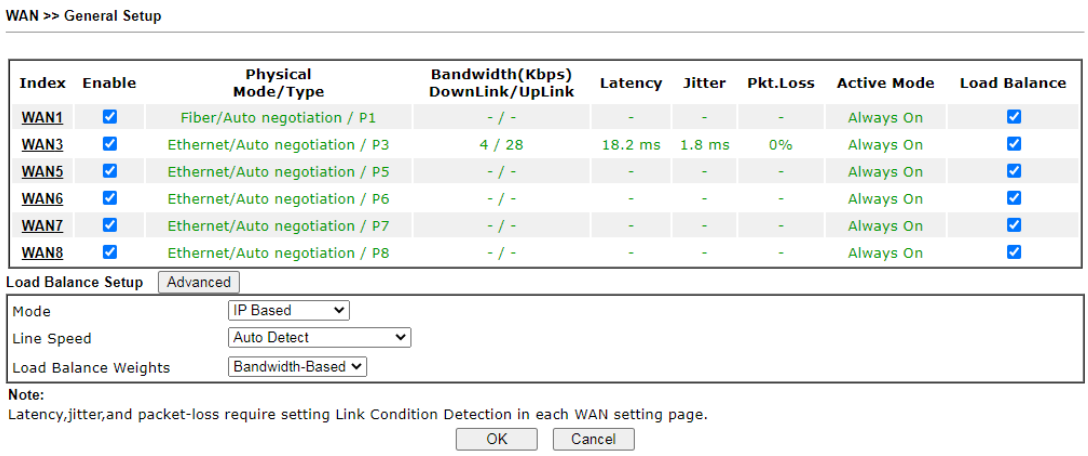


II-2-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1~WAN8 in details.

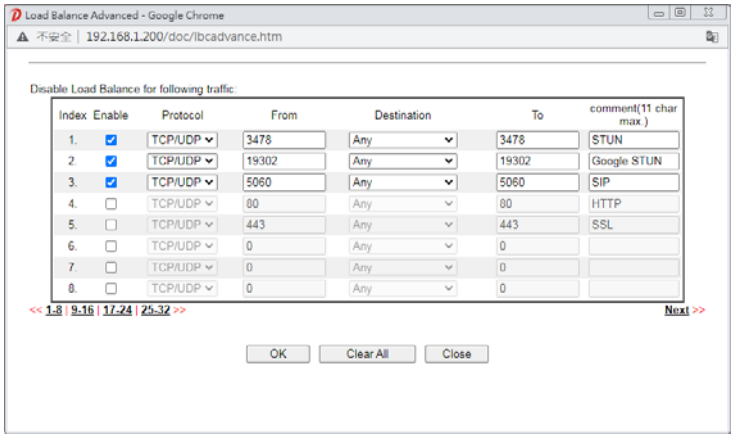
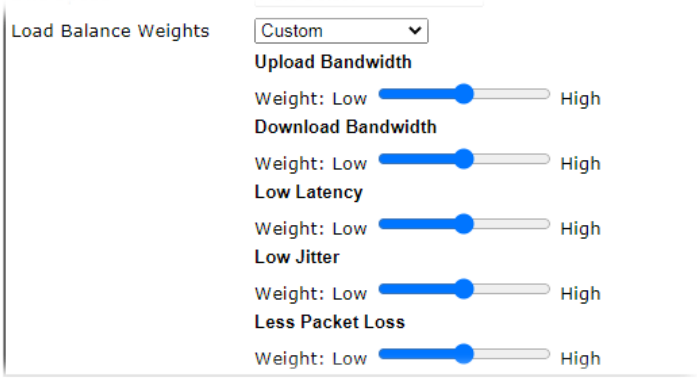
This router supports multiple-WAN function. It allows users to access Internet and combine the bandwidth of the multiple WANs to speed up the transmission through the network. Each WAN port can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such 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 WAN# settings.

This webpage allows you to set general setup for WAN# respectively.



Available settings are explained as follows:

Item	Description
Index (WAN1 ~WAN8)	Click the WAN interface link under Index to access into the WAN configuration page.
Enable	Check the box to enable this WAN interface.
Physical Mode / Type	Display the physical mode, physical type, and LAN port of this WAN interface.
Line Speed(Kbps) DownLink/UpLink	Display the downstream and upstream rate of this WAN interface.
Active Mode	Display whether this WAN interface is Active device or backup device. **Always On** - WAN is always enabled.

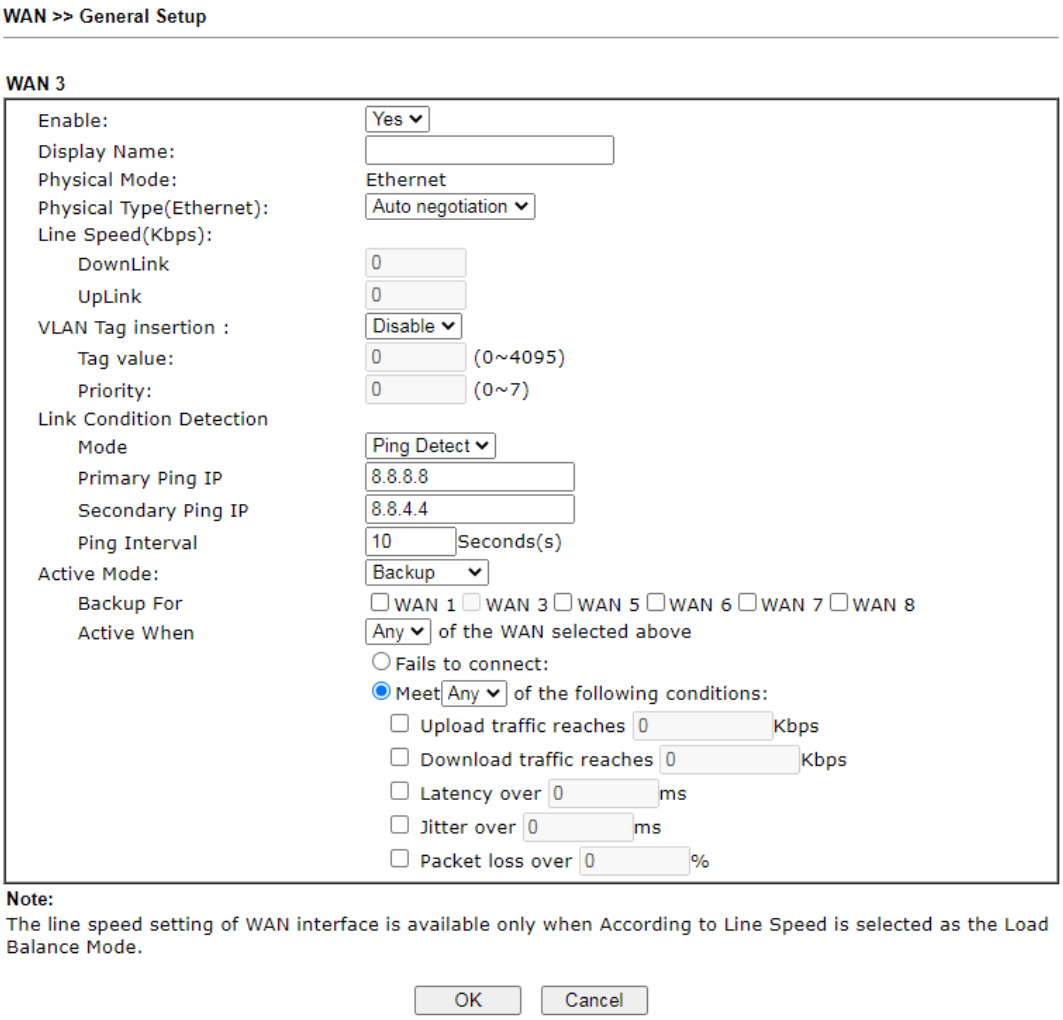
	Backup (WAN#)- Display the backup WAN interface for this WAN when it is disabled.
Load Balance	**V** means the function of load balance for such WAN interface is enabled.
Load Balance Setup	**Advanced** - Load Balance for the traffic of STUN, google STUN, and SIP are disabled in default to prevent from conflict. The following dialog allows you to define protocol, port and name for the traffic not to be applied with load balance. That is, when an item is enabled (checked), it might not be affected by load balance. 
Mode	**IP Based** - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting. **Session Based**- All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP. If you have no strong demand about speed test result, keep default settings as IP based.
Line Speed	This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of **According to Line Speed**. Otherwise, please choose **Auto Detect** to let the router reach the best load balance.
Load Balance Weights	There are four weight types for choosing to meet your request. **Custom** - You can distribute the usage ratio for each WAN interface by setting weights for bandwidth, latency, jitter, and packet loss respectively. 

	• **Upload / Download Bandwidth** - The higher the weight is, the WAN interface with higher bandwidth will get higher usage. • **Low Latency** - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower latency will get higher usage. • **Low Jitter** - It defines the change rate of latency. For stable session, small jitter value will be better. The higher the weight is, the WAN interface with lower jitter will get higher usage. • **Less Packet Loss** - It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower packet loss will get higher usage. **Bandwidth-Based** - The load balance weight for each WAN will be executed according to line speed setting (DownLink/UpLink Rate). This is default setting. **Quality-Based** - The load balance weight for each WAN will be executed according to the transmission rate, latency time and the jitter time. **Reliabiltiy-Based** - The load balance weight for each WAN will be executed according to line speed and packet loss value. Usually, the WAN interface with low packet loss will have the higher ratio to be used.

Info	In default, each WAN port is enabled.

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

To configure WAN interface settings, click the WAN# link to open the following page.



Available settings are explained as follows:

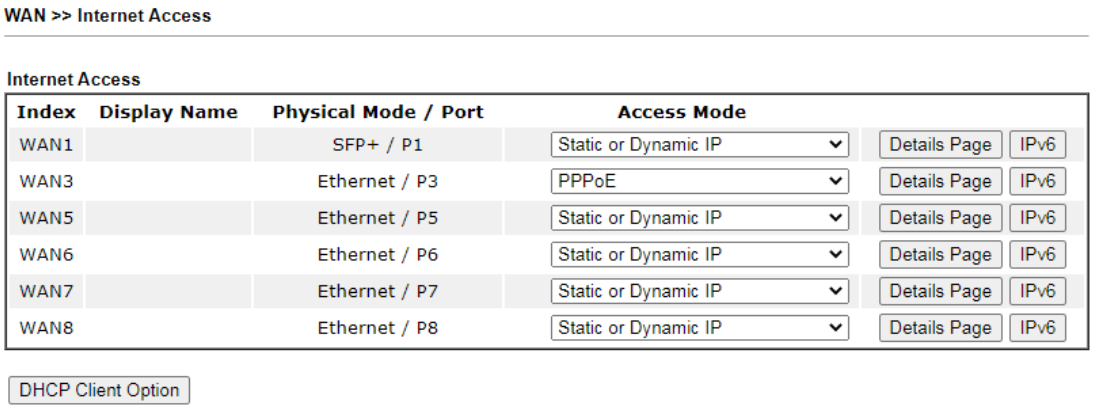
Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Physical Type	You can change the physical type for WAN or choose **Auto negotiation** for determined by the system.
Line Speed	If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.
VLAN Tag insertion	Such feature is offered to the user with the environment supporting IEEE_802.1ad. In which, service is used for outer tag; customer is used for inner tag. It is available only when **Ethernet** is selected as **Physical Mode**. **Disable** – Disable the function of VLAN with tag. **Enable** –Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please Enter the tag value and specify the priority for the

	packets sending by WAN1. • **Tag value** – Enter the value as the VLAN ID number. The range is form 0 to 4095. • **Priority** – Enter the packet priority number for such VLAN. The range is from 0 to 7.
Link Condition Detection	In order for the system to detect the latency, jitter, and packet-loss status for each WAN interface, you have to specify the IP transmitting data through the interface. **Mode** - Choose Ping Detect, Http Detect, or Disable as detection mode. If Ping Detect or Http Detect is selected, you have to configure the following option. • **Primary Ping IP** - Enter an IP address. • **Secondary Ping IP** - Enter an IP address. • **Ping Interval** - Set a time interval (unit:second) for the system to ping the IP address specified above.
Active Mode	**Always On** - Choose **Always On** to make this WAN connection being activated always. **Backup** – Choose it to make this WAN connection as a backup connection. **Backup For** - Specify the WAN interface by checking the WAN box. This WAN will be the backup WAN for the selected WAN interface(s). **Active When** - Set the condition for backup connection. **Any/All** – This WAN will be activated when any/all master WAN interface(s), • **Fails to connect** • **Meet All/Any of the following conditions** – When the upload traffic, download traffic, latency, jitter and/or packet loss of active WAN reaches the traffic threshold (specified here), the backup WAN will be enabled automatically to share the overloaded data traffic.

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

II-2-2 Internet Access

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



Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1 ~ WAN8 that entered in general setup.
Physical Mode / Port	It shows the physical connection for WAN(Ethernet) /port number according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface. Note that **Details Page** will be changed slightly based on physical mode.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.
DHCP Client Option	This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.

Enable – Check the box to enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example,

Option number:100

Data: abcd

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

Interface – Specify the WAN interface(s) that will be overwritten by this function. WAN13 ~ WAN52 can be located under **WAN>>Multi-VLAN**.

Option Number – Type a number for such function.

DataType – Choose the type (ASCII or Hex) for the data to be stored.

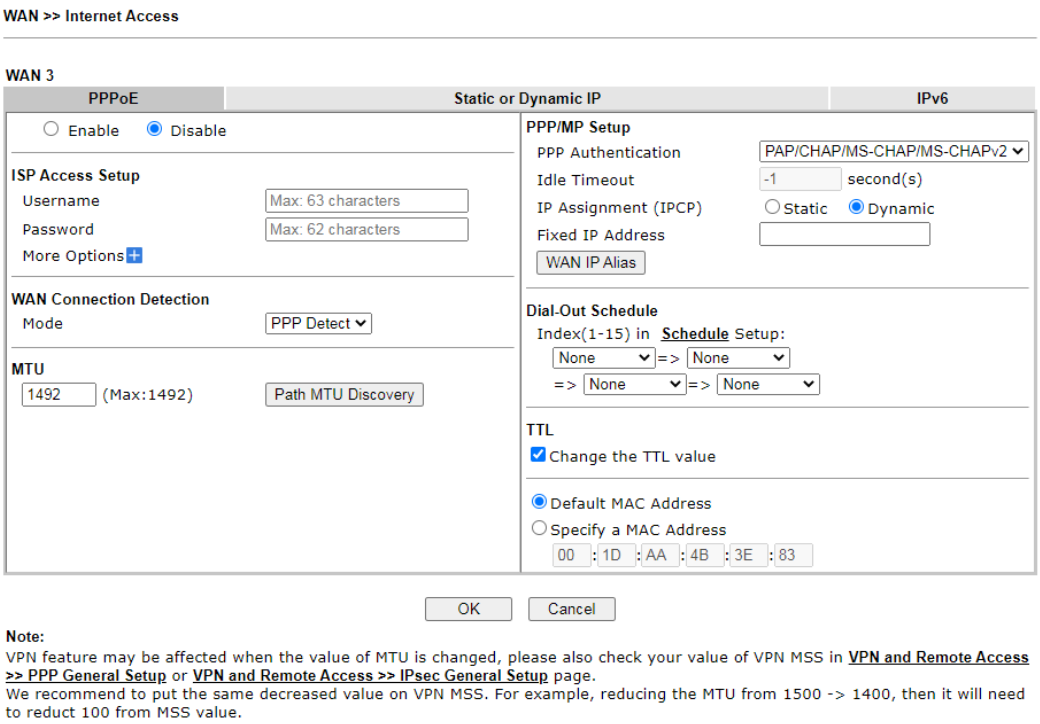
Data – Type the content of the data to be processed by the function of DHCP option.

Info

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

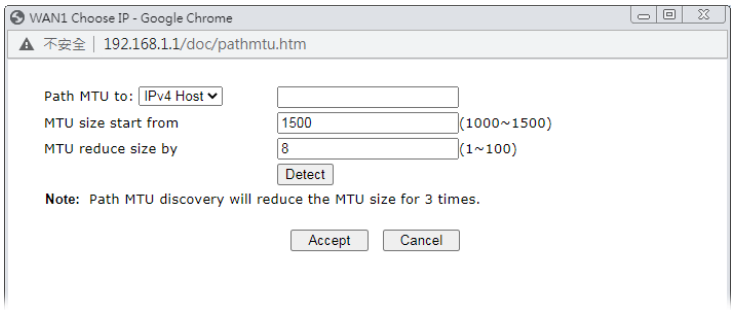
II-2-2-1 Details Page for PPPoE

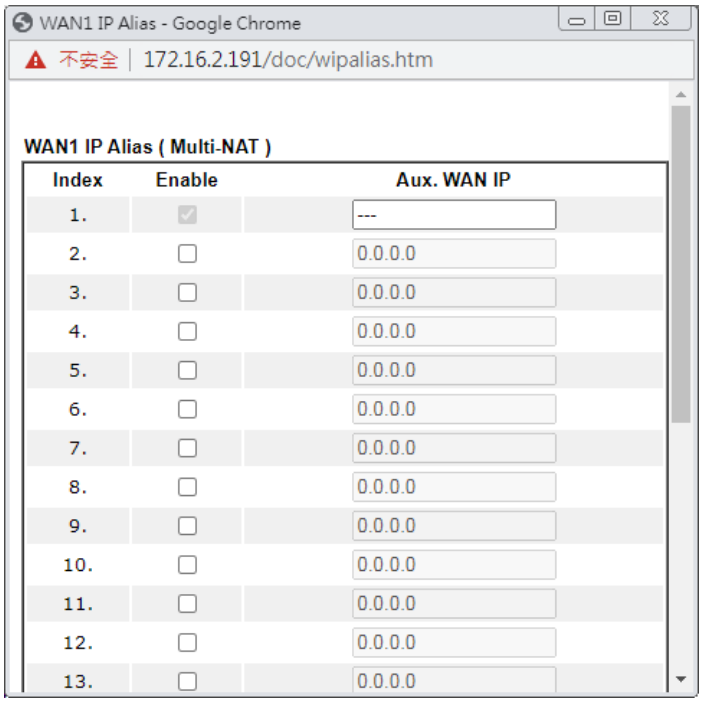
To choose PPPoE as the accessing protocol of the Internet, please select **PPPoE** from the **WAN>>Internet Access >>WAN3** page. The following web page will be shown.



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 -** ● **Service Name (Optional) -** Sets the PPP service name tag. Required by some ISPs. Leave blank unless instructed otherwise by your ISP**.**
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 **Path MTU Discovery** 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-CHAPv2** - 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. **Assignment (IPCP)** - Configure the router according to how your ISP allocates WAN IP address(es) to you. • **Static** - ISP has assigned a fixed WAN IP address, which is to be entered below in Fixed IP Address. • **Dynamic** - WAN IP address is dynamically allocated. **Fixed IP Address** – Enter a fixed IP address. **WAN IP Alias** - Click to enter multiple WAN IP addresses assigned by your ISP. 
Dial-Out Schedule	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.
MAC	**Default MAC Address –** Use the default MAC address for the WAN Ethernet port. **Specify a MAC Address –** Specify a MAC address for the WAN

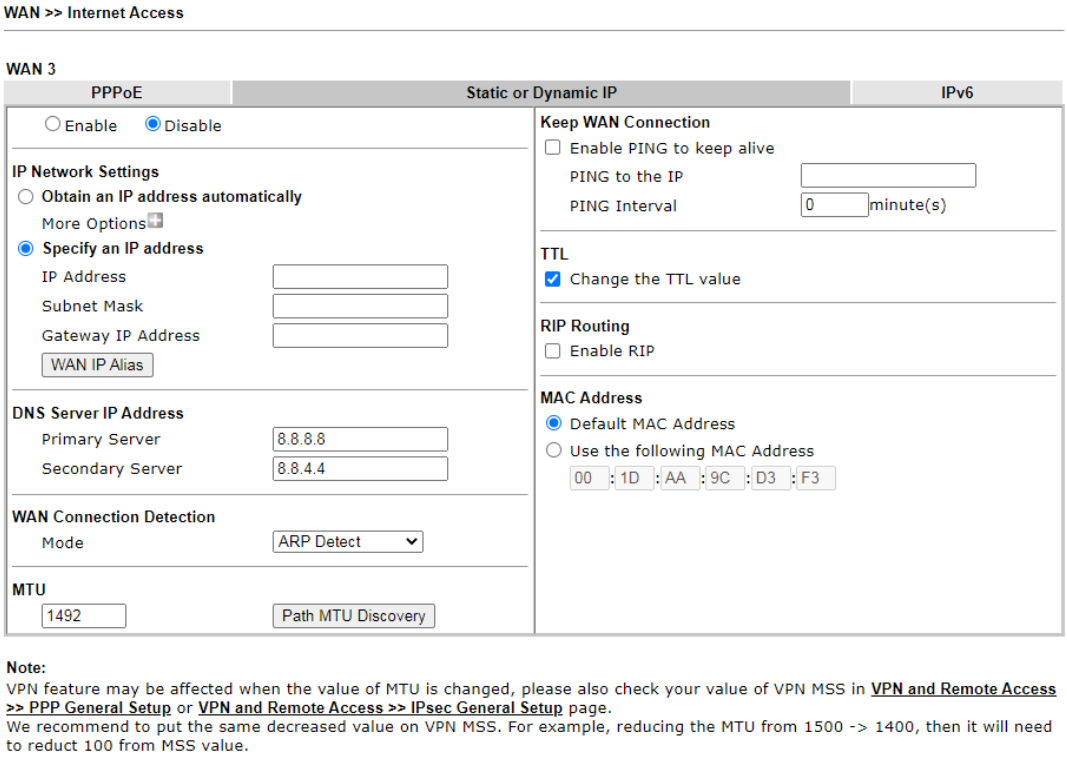
	Ethernet port. Select this option if your ISP authenticates by MAC addresses.

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

II-2-2-2 Details Page for Static or Dynamic IP

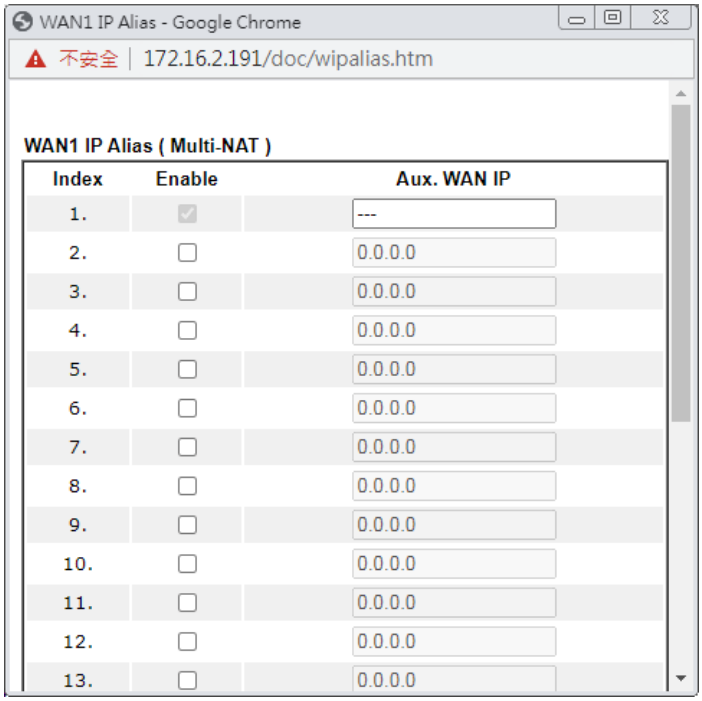
For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you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

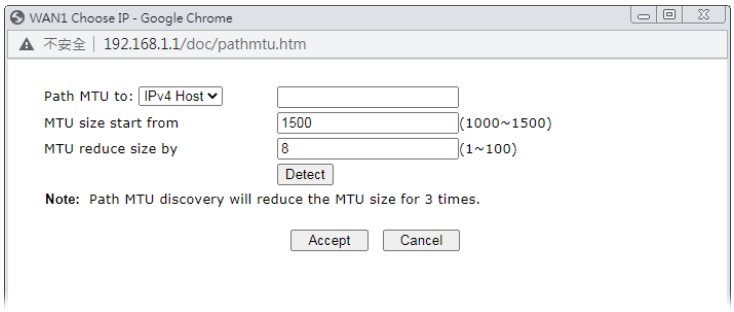
To use **Static or Dynamic IP** as the accessing protocol of the internet, please click the **Static or Dynamic IP** tab. The following web page will be shown.



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 set 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. ● **Enable 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

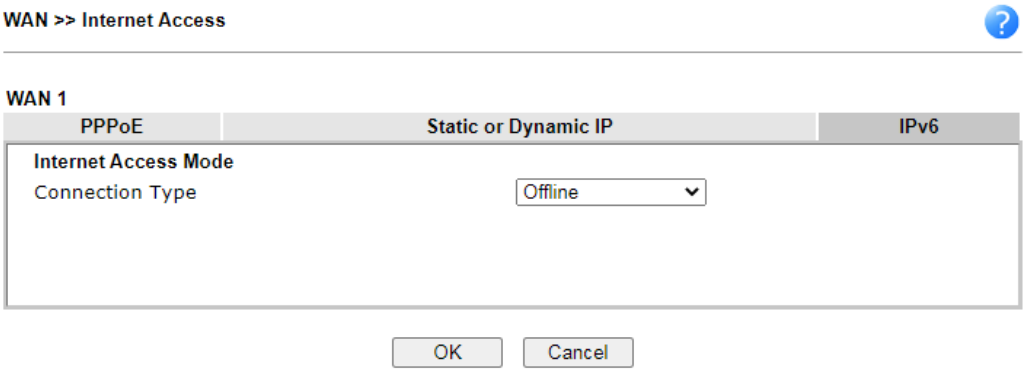
	if the WAN connection is on or off. ● **TTL (Time to Live)** – Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255. ● **Ping Interval –** Enter the interval for the system to execute the PING operation. ● **Ping Retry –** Enter the number of times 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 **Path MTU Discovery** 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 –** Check the box to enable 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 Routing	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.

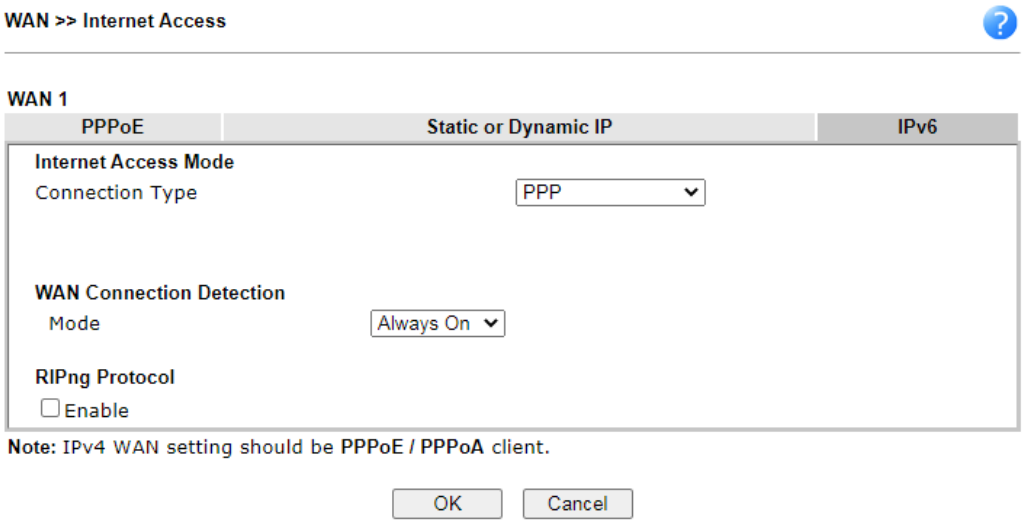
II-2-2-3 Details Page for IPv6 – Offline in Ethernet WAN

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



II-2-2-4 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.

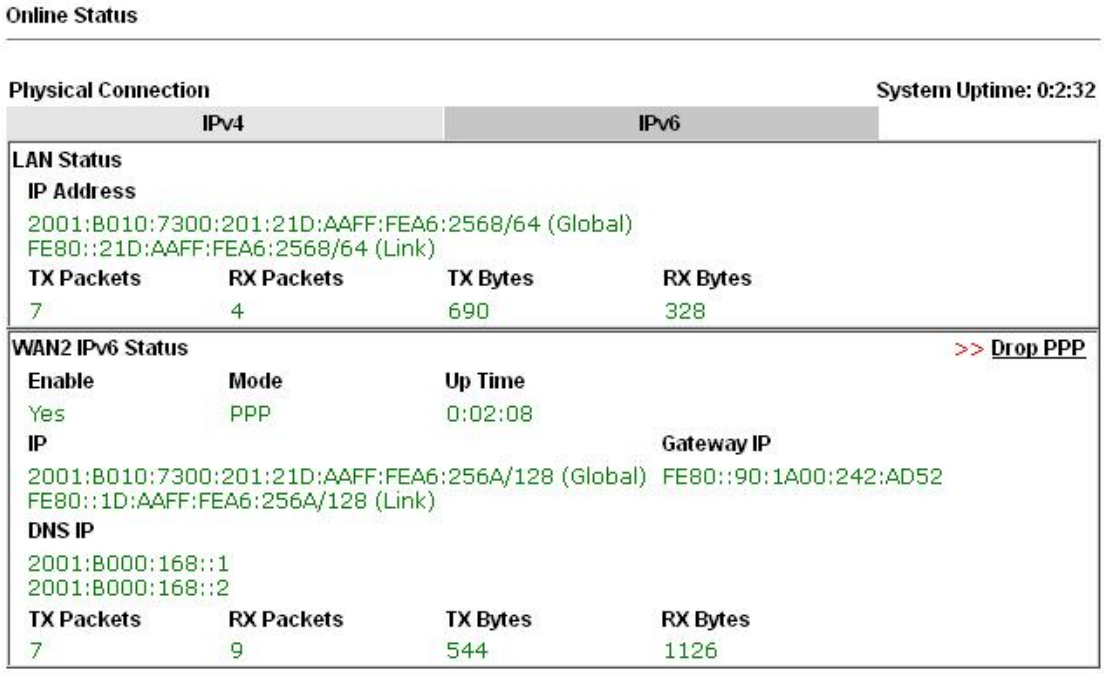


Available settings are explained as follows:

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.



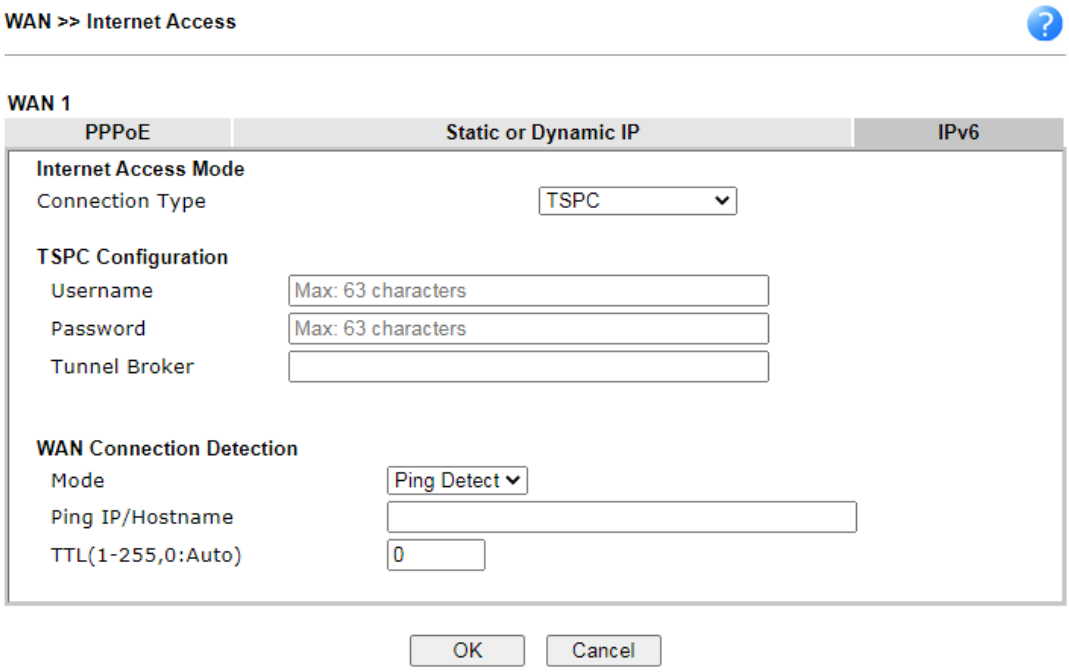
Info	At present, the IPv6 prefix can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

II-2-2-5 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.

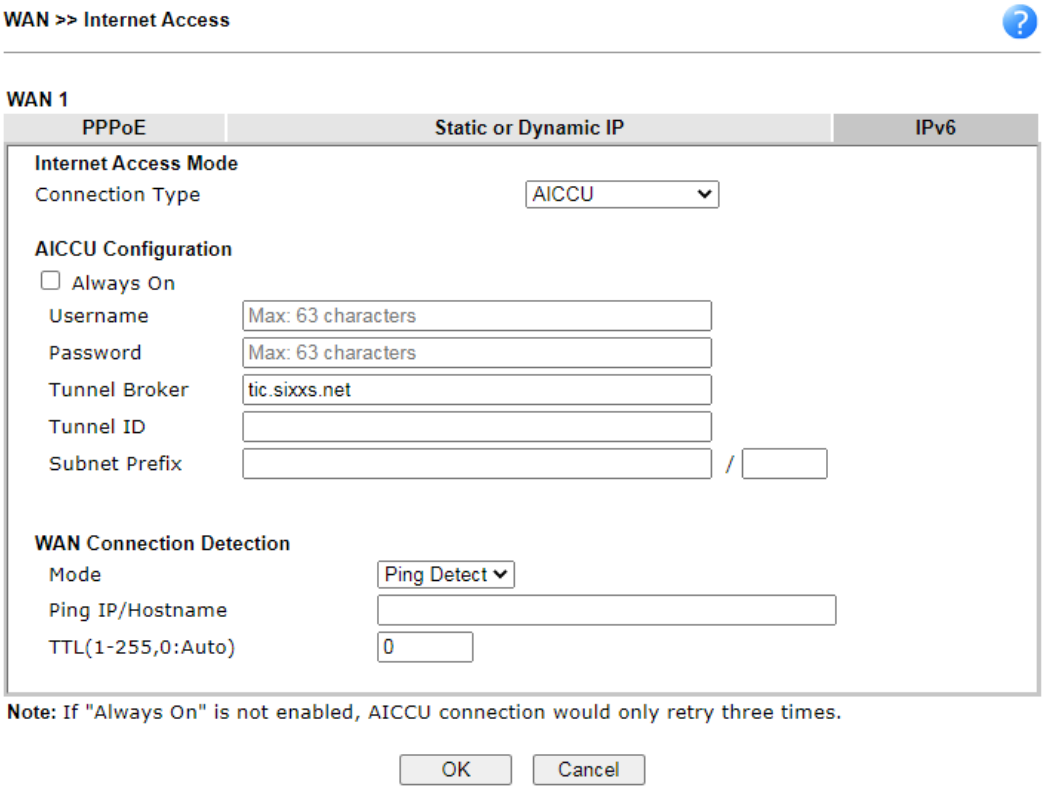


Available settings are explained as follows:

Item	Description
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account. The maximum length of the name you can set is 63 characters.
Password	Enter the password assigned with the user name.
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-2-2-6 Details Page for IPv6 – AICCU



Available settings are explained as follows:

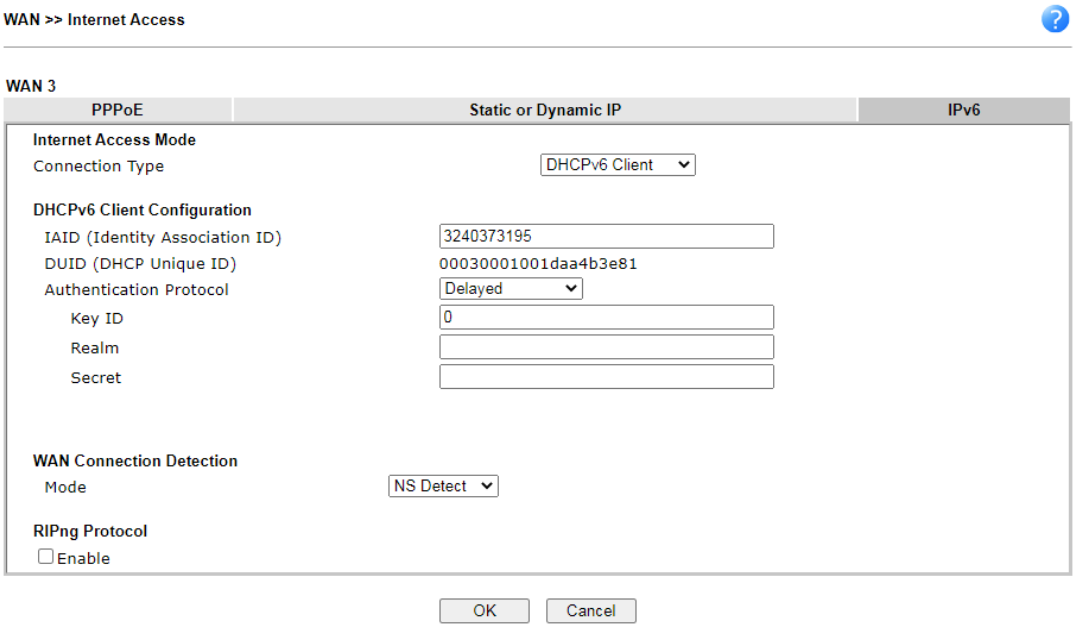
Item	Description
Always On	If selected, always attempt to reconnect if connection is lost. If unselected, reconnect up to 3 times if connection is lost.
Username	Login Username. Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply 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). Type the ID offered by Tunnel Broker.
Subnet Prefix	Type 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-2-2-7 Details Page for IPv6 – DHCPv6 Client

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



Available settings are explained as follows:

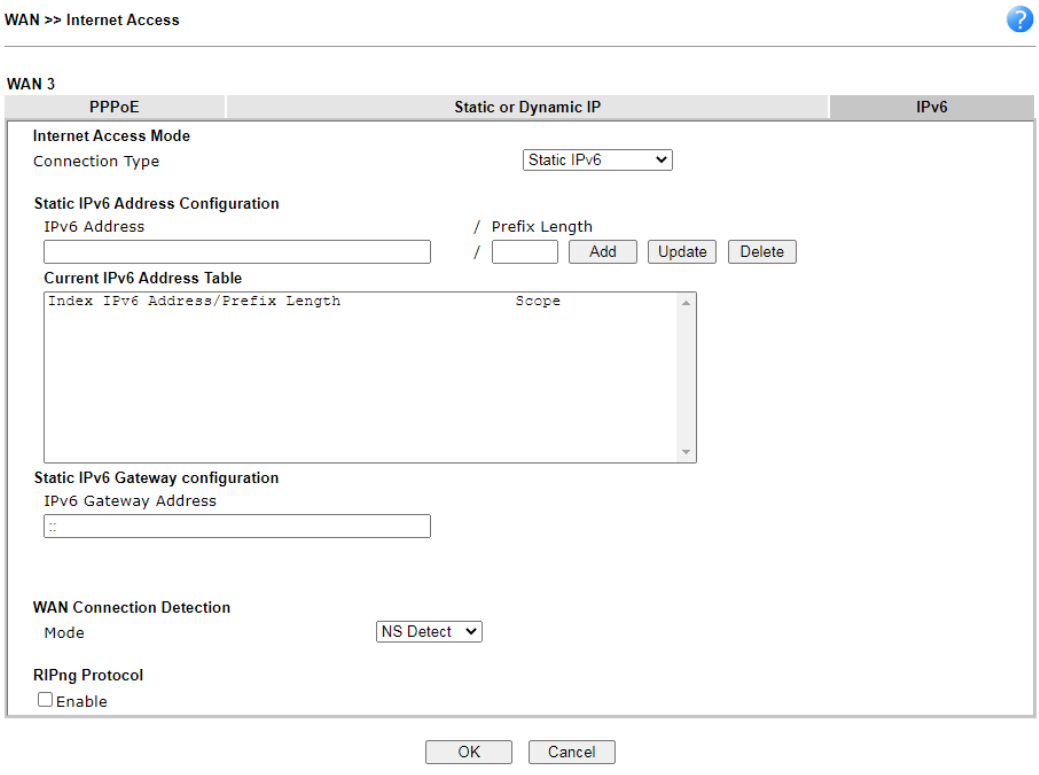
Item	Description
DHCPv6 Client Configuration	**IAID** - Type a number as IAID. **DUID** – Display the DHCP unique ID used by such WAN interface. **Authentication Protocol** – Such protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three 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.

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

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

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



Available settings are explained as follows:

Item	Description
Static IPv6 Address Configuration	**IPv6 Address** – 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 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.

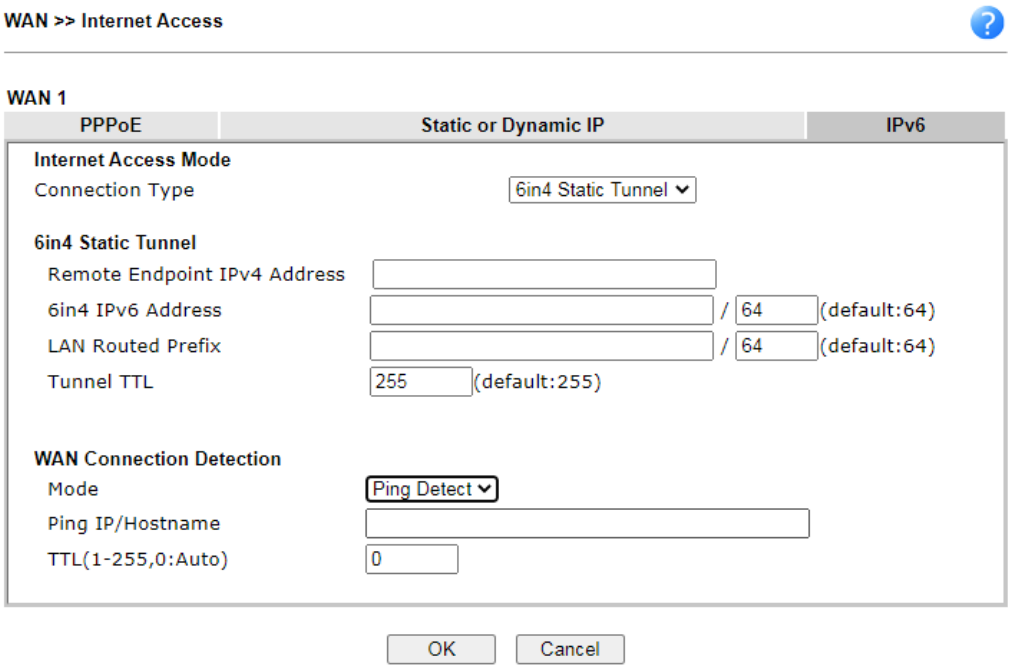
After finished the above settings, click **OK** to save the settings.

II-2-2-9 Details Page for IPv6 – 6in4 Static Tunnel

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

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

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



Available settings are explained as follows:

Item	Description
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)

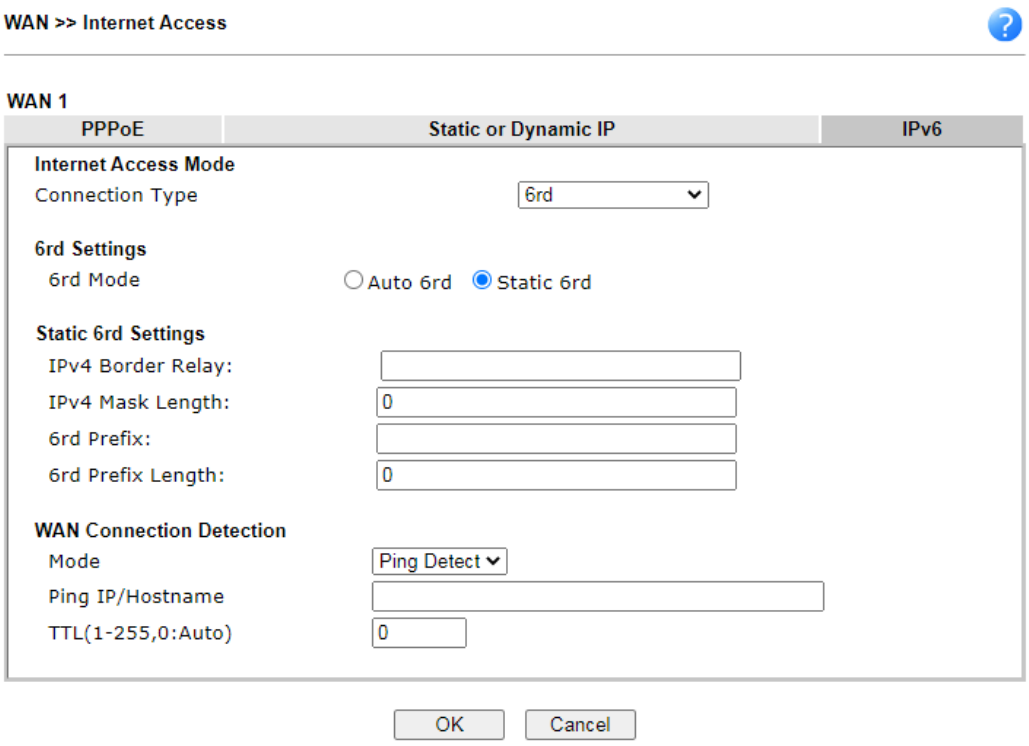
TX Packets	RX Packets	TX Bytes	RX Bytes
14	80	1244	6815

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-2-2-10 Details Page for IPv6 – 6rd

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



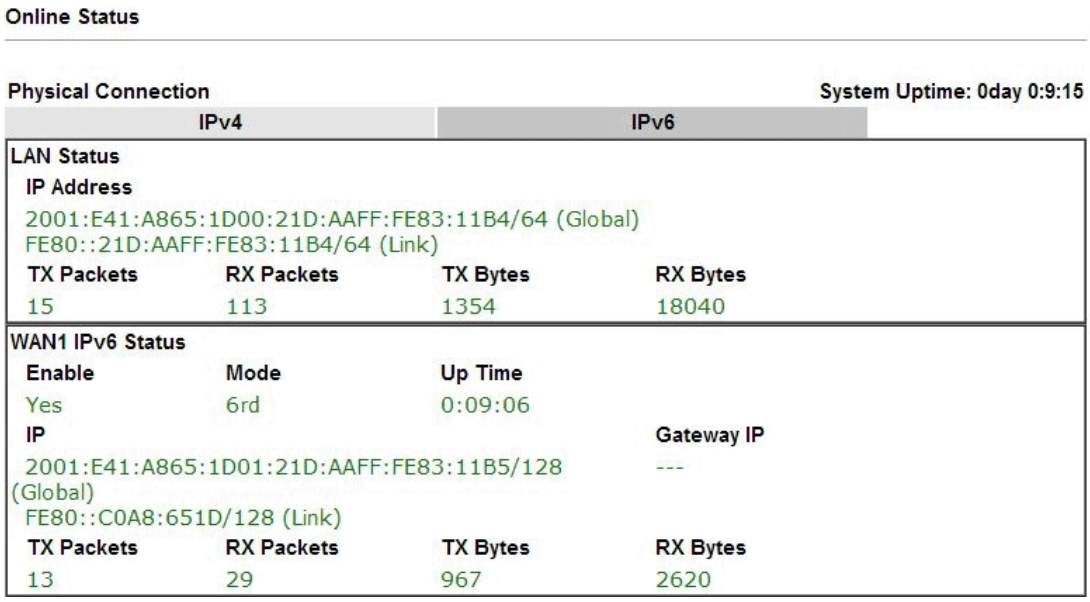
Available settings are explained as follows:

Item	Description
6rd Settings	**Auto 6rd** - Used in conjunction with DHCPv4, the router automatically provisions IPv6 using option 212. **Static 6rd** - IPv6 configuration information is manually entered.
Static 6rd Settings	**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.



II-2-3 Multi-VLAN

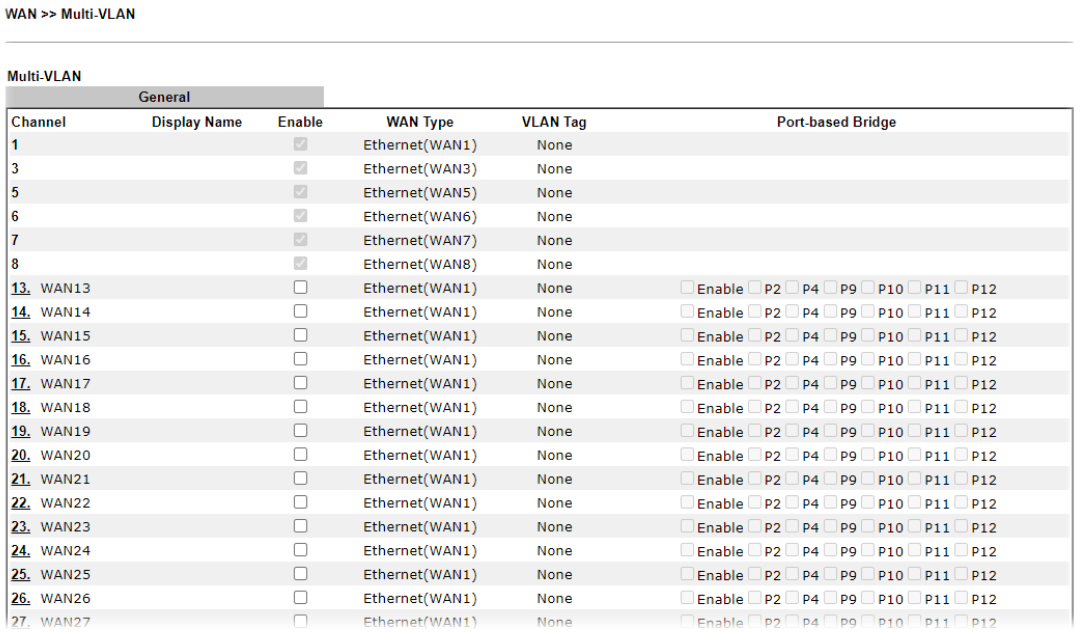
Multi-VLAN lets you configure multiple VLAN groups.

Channel 1 to 8 have the following fixed assignments and cannot be altered.

Channels 13 through **52** can be configured as virtual WANs.

General

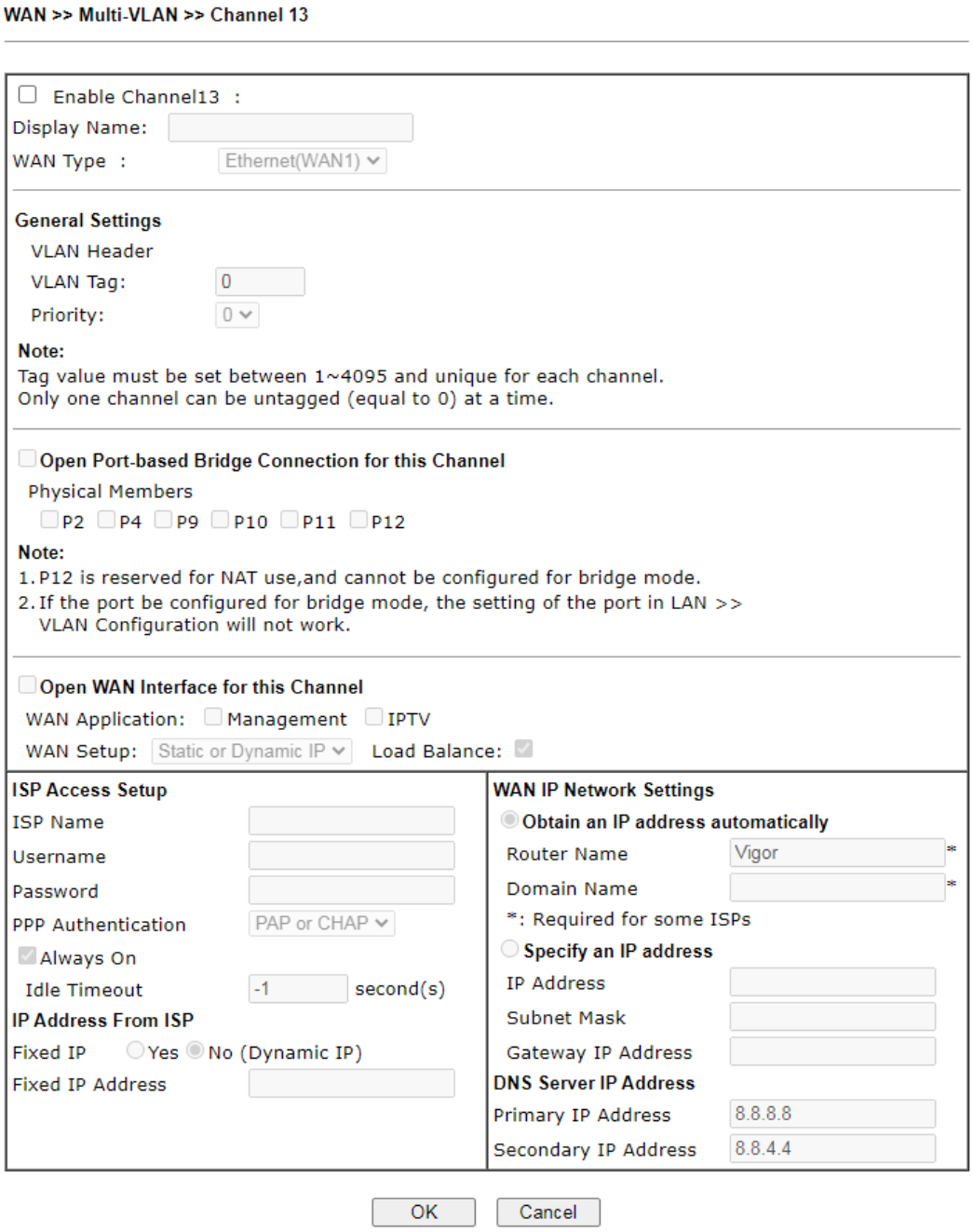
The system allows you to set up to eight channels used as multi-VLAN.



Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1~8 are used by the Internet Access web user interface and can not be configured here. Channels 13 ~ 52 are configurable.
Enable	Display whether the settings in this channel are enabled (checked) or not (unchecked).
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. **P2 ~ P12** – Check the box(es) to build bridge connection on LAN.

Click any index (13~52) to get the following web page:



Available settings are explained as follows:

Item	Description
Enable Channel 13~52	**Enable –** Click it to enable the configuration of this channel. **Disable –**Click it to disable the configuration of this channel.
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.
General Settings	**VLAN Tag –** Type 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. **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.

	• **Fixed IP Adderss** - Enter an IP address.
WAN IP Network Settings	**Obtain an IP address automatically** – Select this option if the router is to receive IP configuration information from a DHCP server. • **Router Name** – Sets the value of DHCP Option 12, which is used by some ISPs. • **Domain Name** – Sets the value of DHCP Option 15, which is used by some ISPs. **Specify an IP address** – Select this option to manually enter the IP address. • **IP Address** – 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.

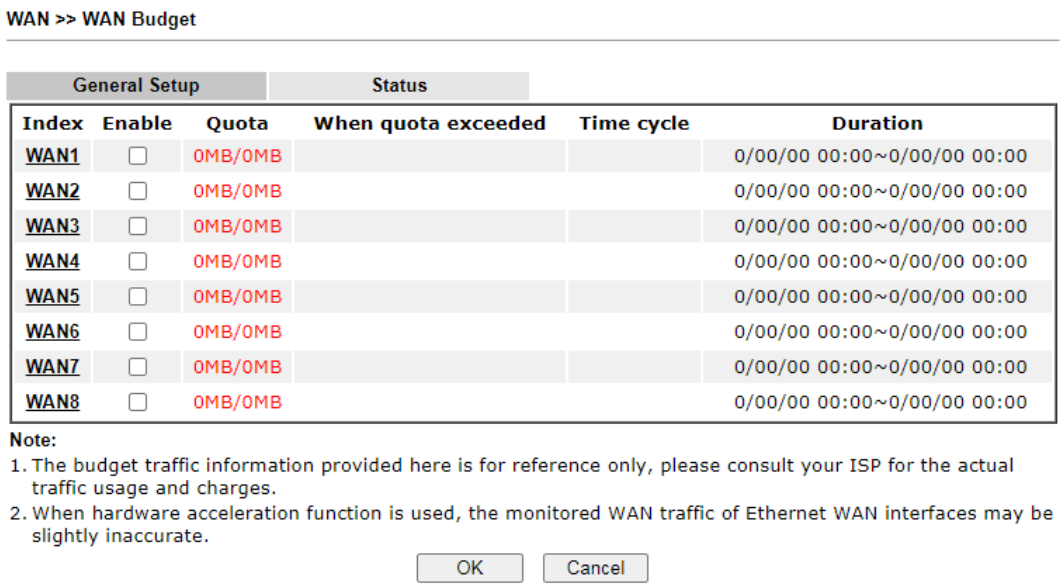
II-2-4 WAN Budget

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

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

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

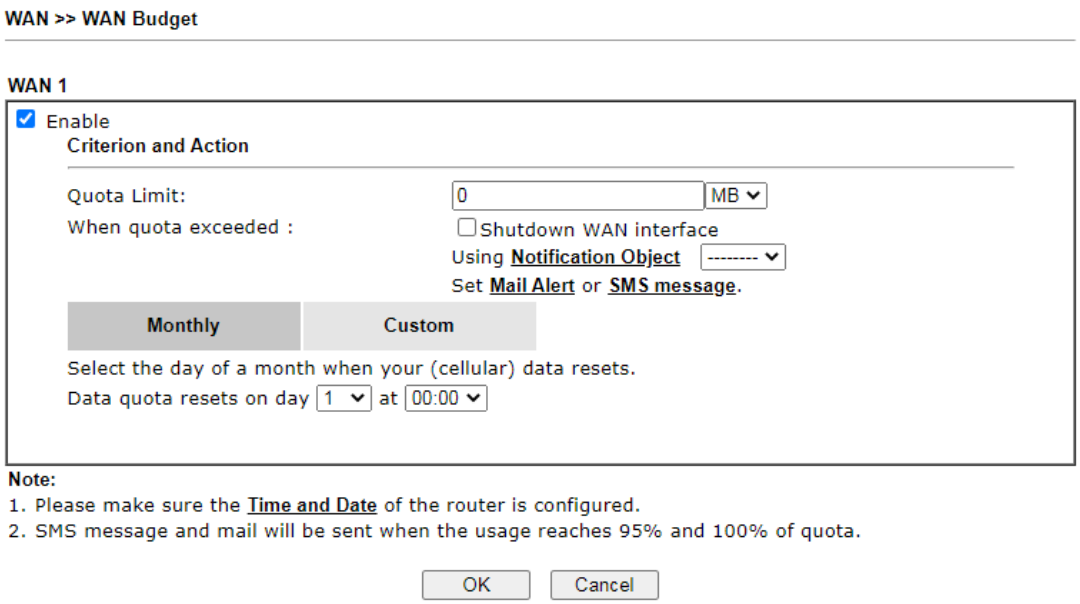
II-2-4-1 General Setup



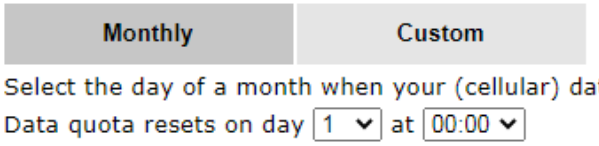
Item	Description
Index	The WAN port. Click to configure WAN Budget for a particular WAN.
Enable	**v -** WAN Budget is enabled on this WAN. **x -** WAN Budget is disabled on this WAN.
Quota	The current cycle's Internet usage is expressed as *x/y* where *x* is the cumulative usage and *y* is the upper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

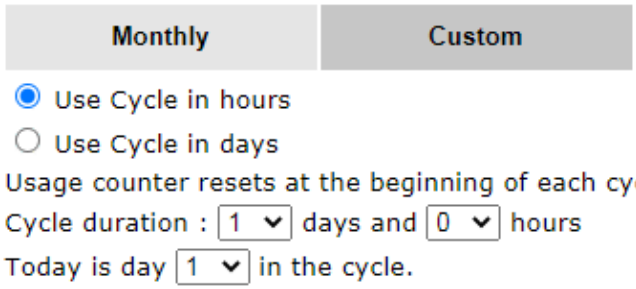
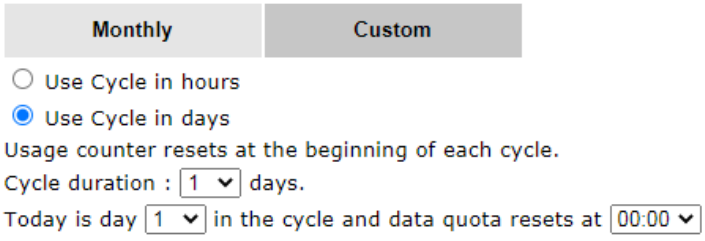
Duration	Start and end timestamps of the current cycle.

Click WAN1 (to WAN8) link to open the following web page.



Available settings are explained as follows:

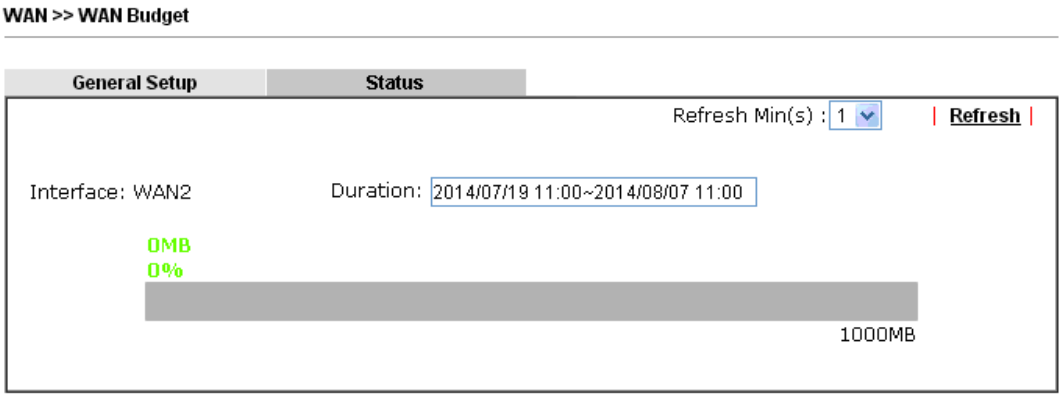
Item	Description
Enable	When selected, WAN Budget is enabled for this WAN.
Quota Limit	Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify.
When quota exceeded	Check the box(es) as the condition(s) for the system to perform when the traffic 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.

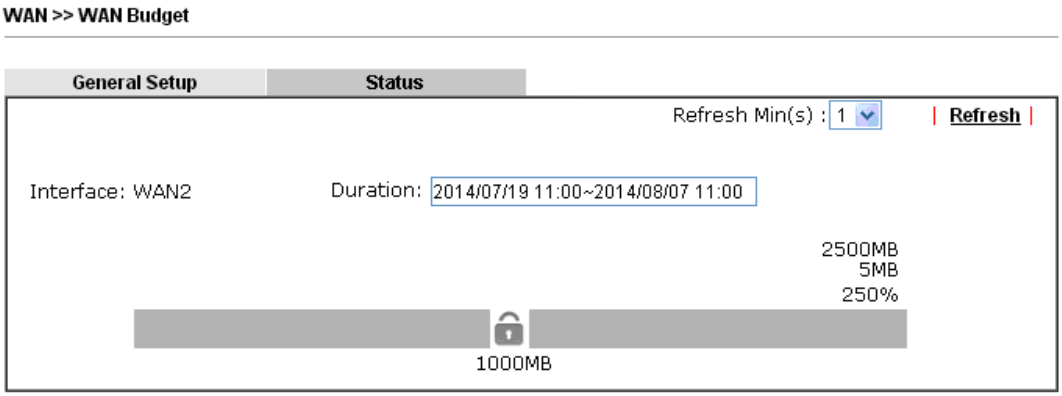
After finished the above settings, click **OK** to save the settings.

II-2-4-2 Status

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



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



II-3 LAN

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

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

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

IP Address

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

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

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

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

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

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

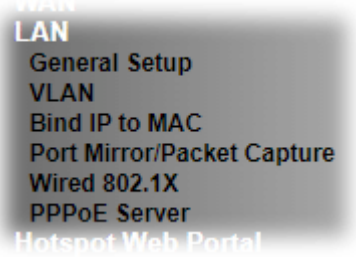
In most cases, the default IP address block should work satisfactorily. However, there are situations where you need to select a different address block, such as when you need to communicate with other LANs that already use the same address block.

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

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

Web User Interface

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



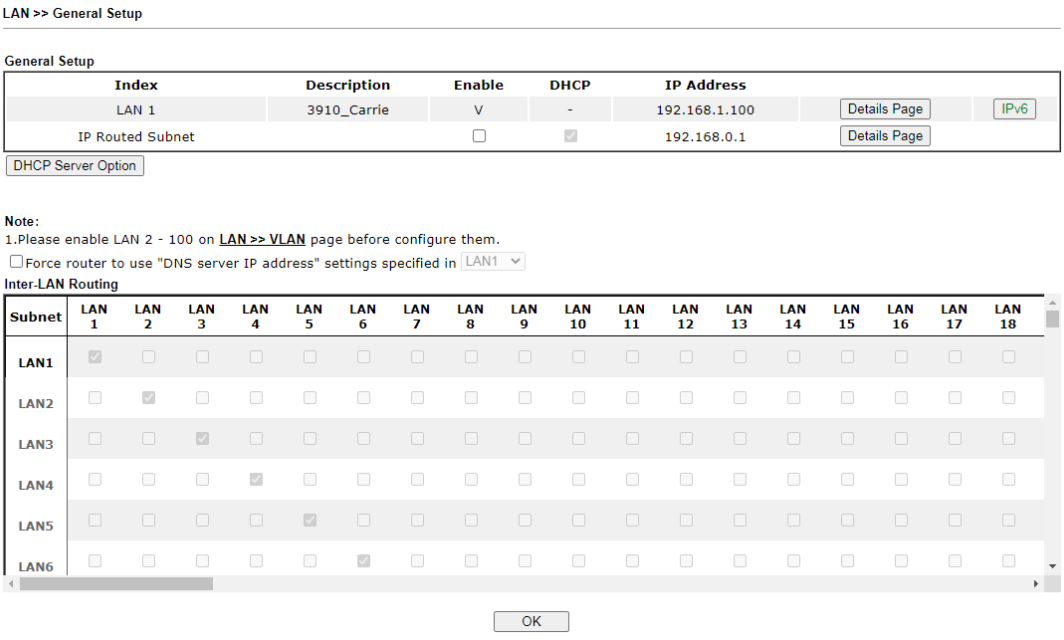
II-3-1 General Setup

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

There are several subnets provided by the router which allow users to divide groups into different subnets (LAN2 – LAN100). 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 – LAN50 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 100 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.

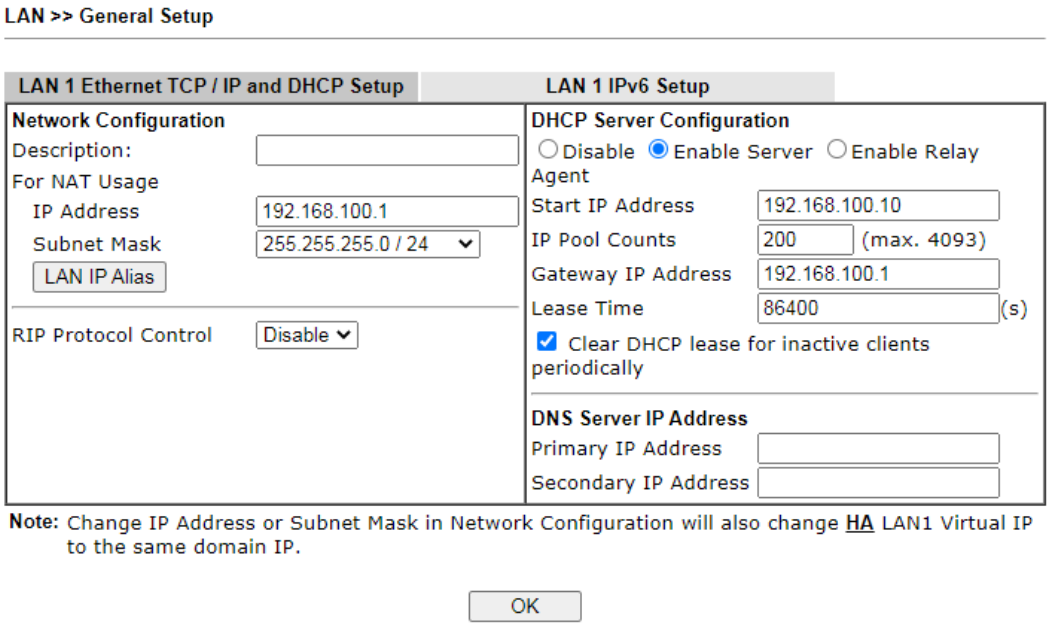
	Index - Display all of the LAN items. **Enable** - Basically, LAN1 status is enabled in default. LAN2 –LAN50 and IP Routed Subnet can be configured after enabling via LAN>>VLAN. **DHCP-** LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN. **IP Address -** Display the IP address for each LAN item. Such information is set in default and you can not modify it. **Details Page -** Click it to access into the setting page. Each LAN will have different LAN configuration page. **Each LAN must be configured in different subnet.** **IPv6 –** Click it to access into the settings page of IPv6.
DHCP Server Options	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 LAN port 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-3-2 VLAN on how to set up VLANs. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

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

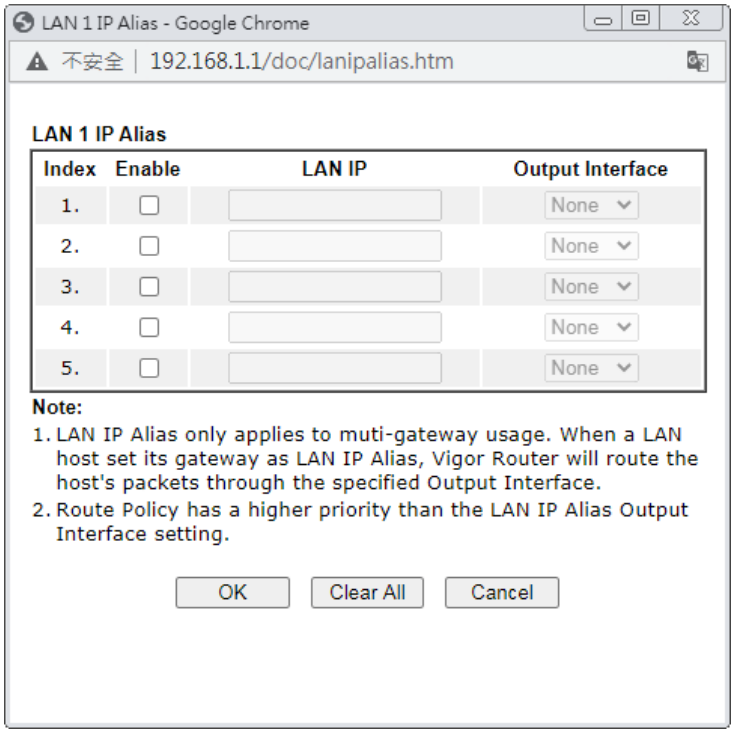
Info	To configure a subnet, select its Detials Page button to bring up the LAN **Details Page**.

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

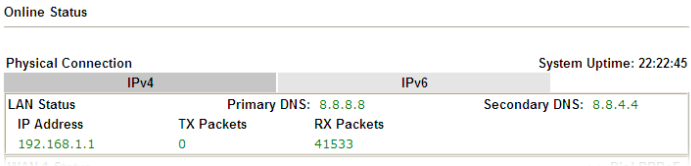
This page has two tabs, LAN Ethernet TCP/IP and DHCP Setup, which sets up the IPv4 LAN environment, and LAN IPv6 Setup, which sets up the IPv6 environment.



Available settings are explained as follows:

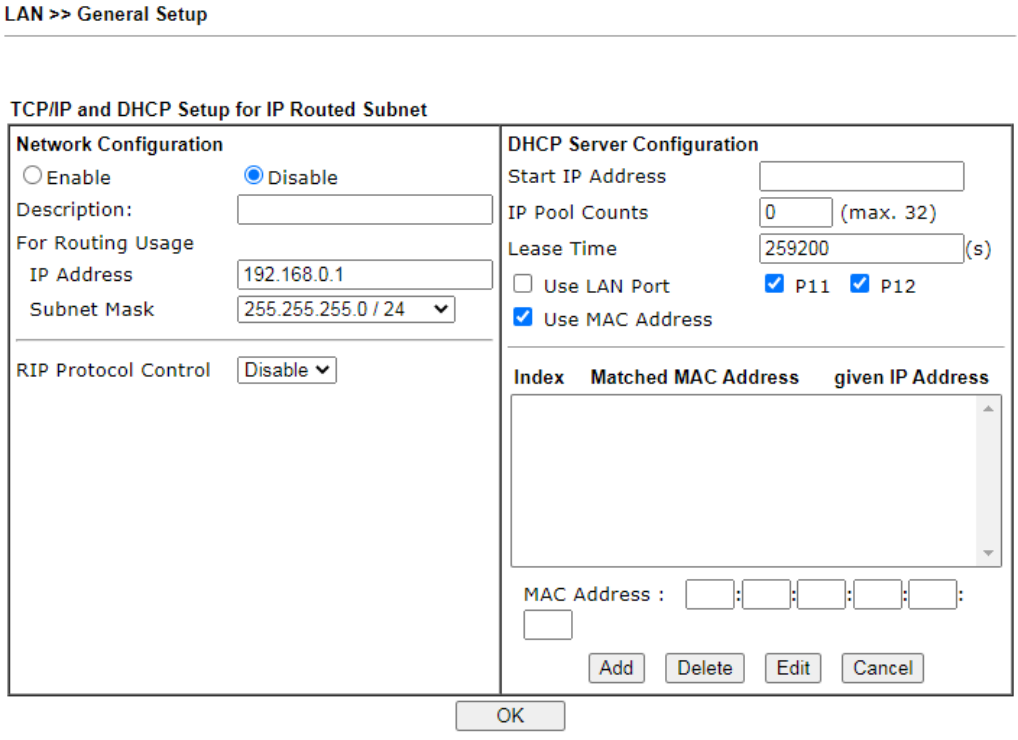
Item	Description
Network Configuration	**For NAT Usage,** **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24). **LAN IP Alias** –Such feature allows specifying multiple gateways (under a switch) with different WAN interfaces for accessing the Internet via the Vigor router.  **RIP Protocol Control,** **Enable** –When Enabled, the router will attempt to exchange

	routing information with neighbouring routers using the Routing Information Protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. **Disable** – 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 its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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

II-3-1-2 Details Page for IP Routed Subnet



Available settings are explained as follows:

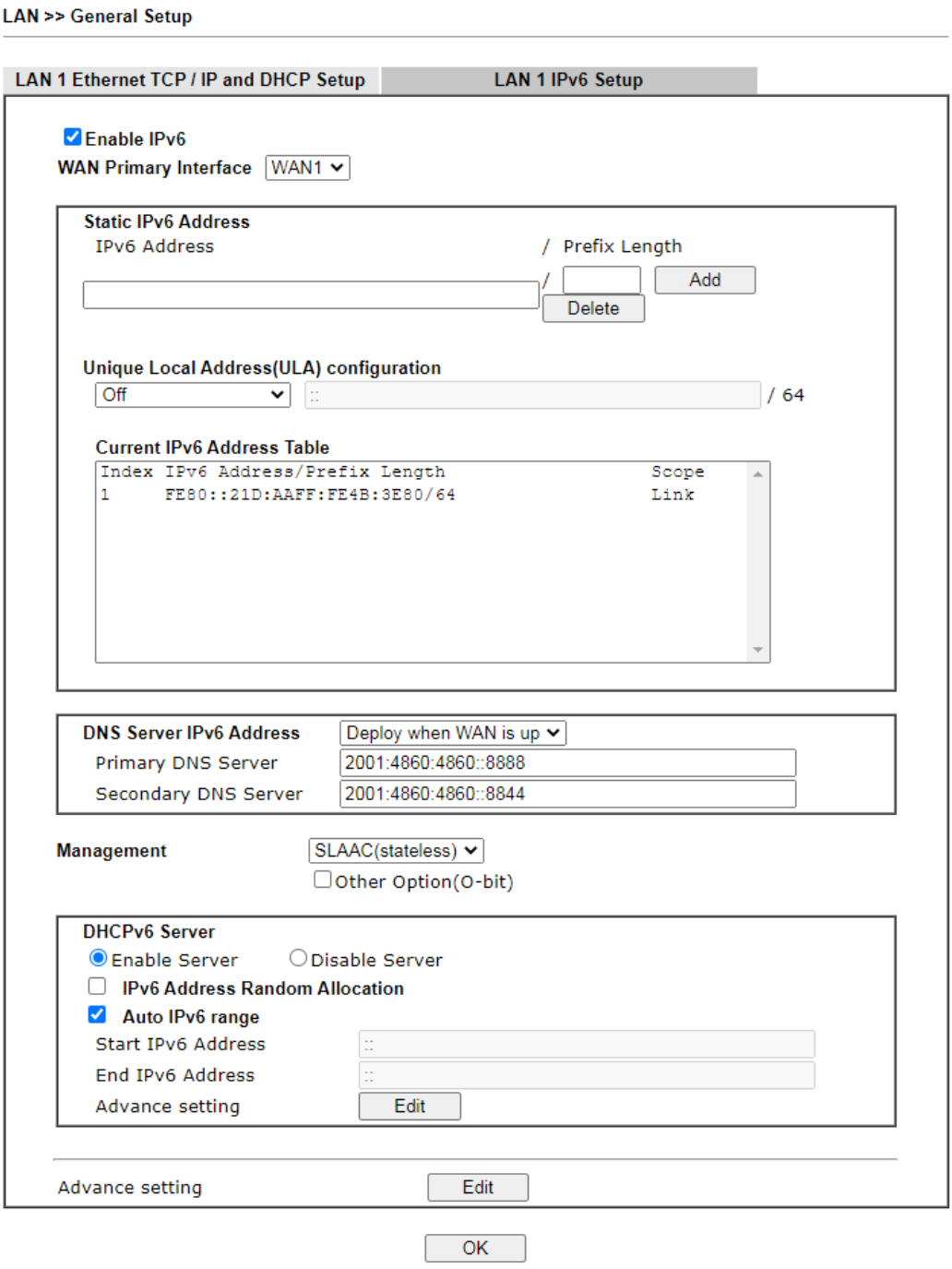
Item	Description
Network Configuration	**Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration. **For Routing Usage,**

	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 P11 and/or P12. Please check the box of P11 and P12. **Use MAC Address -** Check such box to specify MAC address. **MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts which can be assigned, deleted or edited from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet. **Add –** Enter the MAC address in the boxes and click this button to add. **Delete** – Click it to delete the selected MAC address. **Edit** – Click it to edit the selected MAC address. **Cancel** – Click it to cancel the job of adding, deleting and editing.

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

II-3-1-3 Details Page for LAN1 – IPv6 Setup

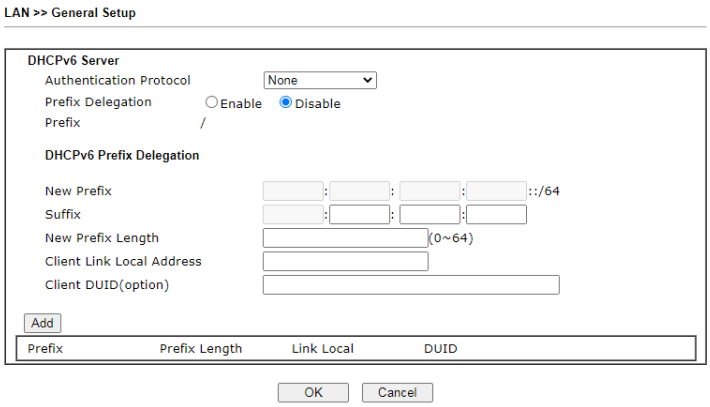
There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.

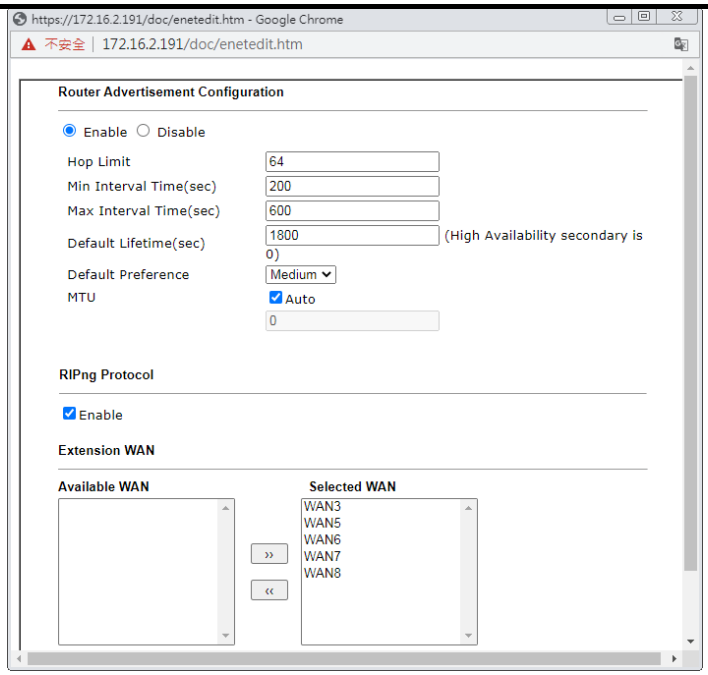


It provides 2 daemons for LAN side IPv6 address configuration. One is **SLAAC**(stateless) and the other is **DHCPv6 Server** (Stateful).

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.

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.

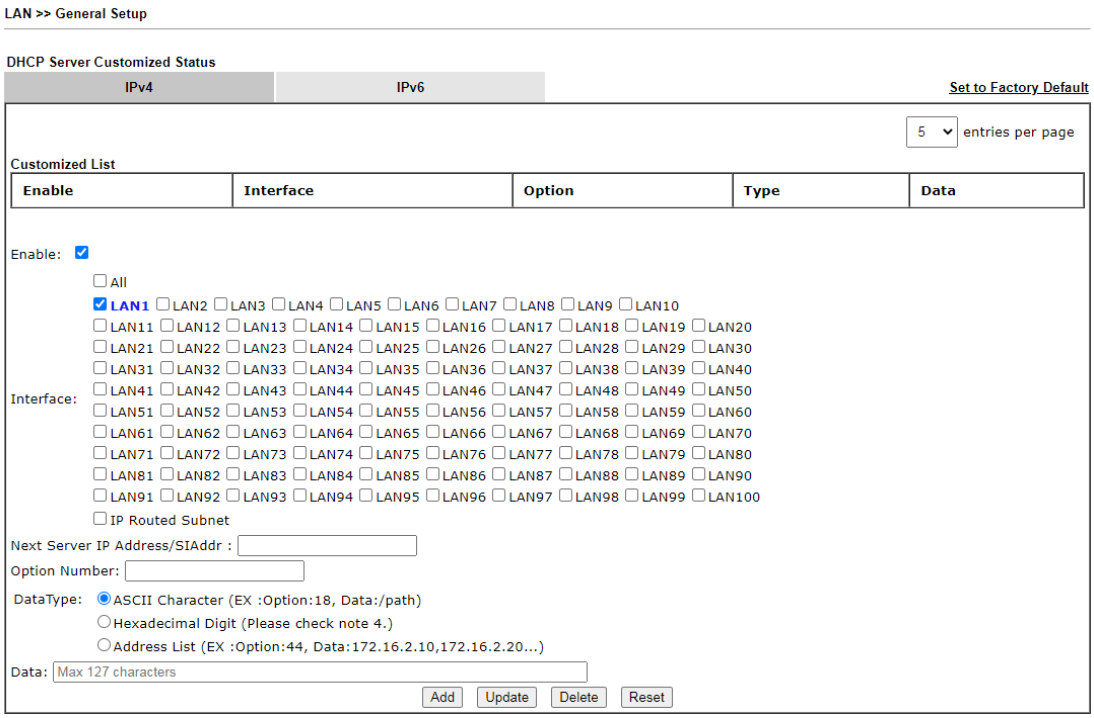
Available WAN – Additional WANs available but not currently selected to carry IPv6 traffic.

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-3-1-4 DHCP Server Option

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



Available settings are explained as follows:

Item	Description
Customized List	Shows all the DHCP options that have been configured in the system.
Enable	If selected, DHCP option entry is enabled. If unselected, DHCP option entry is disabled.
Interface	LAN interface(s) to which this entry is applicable.
Next Server IP Address/SIAddr	Overrides the DHCP Next Server IP address (DHCP Option 66) supplied by the DHCP server.
Option Number	DHCP option number (e.g., 100).
DataType	Type of data in the Data field: **ASCII Character** - A text string. Example: /path. **Hexadecimal Digit -** A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468. **Address List -** One or more IPv4 addresses, delimited by commas.
Data	Data of this DHCP option.
Add	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.
Update	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.
Delete	To delete a DHCP option entry, click on it in **Customized List**, and then click **Delete**.
Reset	Clear the current settings.

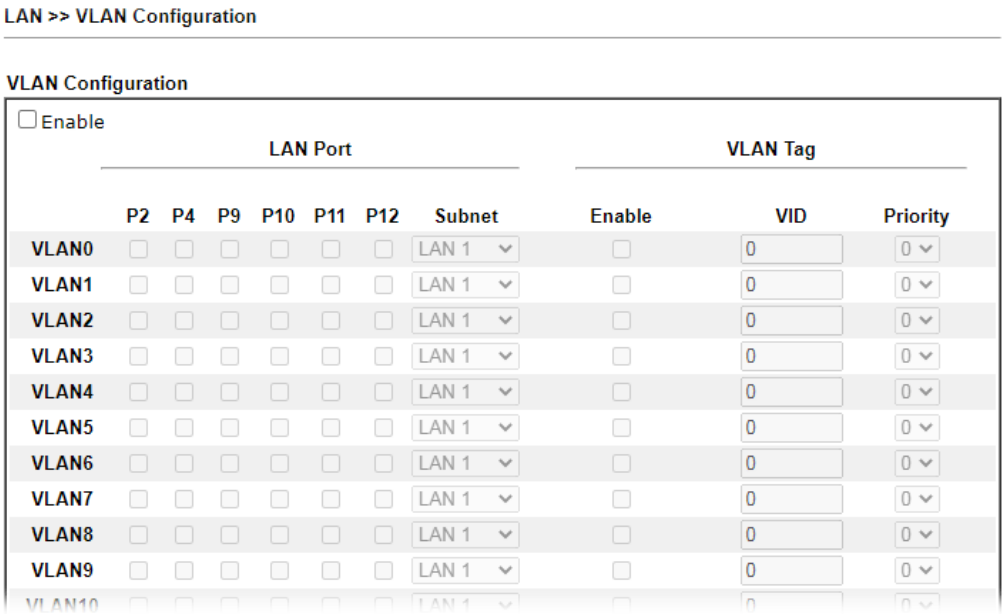
II-3-2 VLAN

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

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

Tagged VLAN

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



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

Available settings are explained as follows:

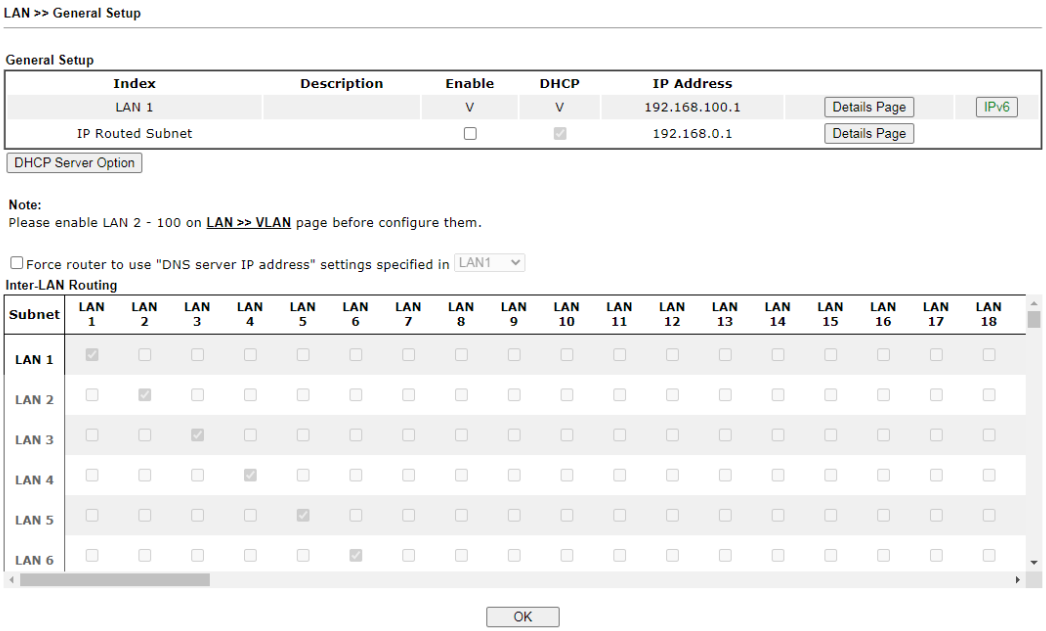
Item	Description
Enable	Enables or disables VLAN functionality.
VLAN#	Virtual LANs.
LAN Port	**P2 - P12** – Physical Ethernet ports on the router. Select the LAN port(s) to group them under the selected VLAN.

Subnet	Select a LAN subnet from LAN 1 to LAN 100 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 P12 to access router	Select to allow untagged hosts connected to LAN port P12 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.

Inter-LAN Routing

The Vigor router supports up to 99 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).



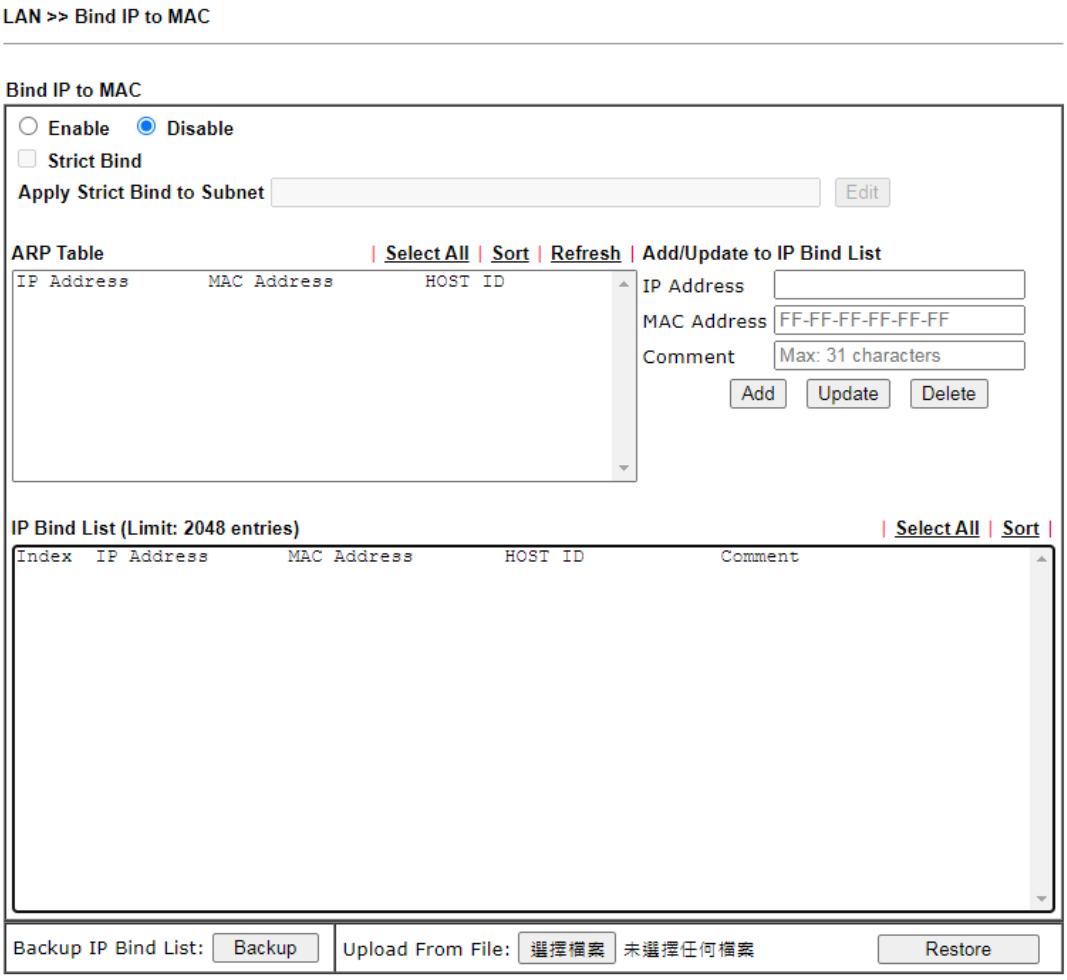
Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

Vigor router 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.

II-3-3 Bind IP to MAC

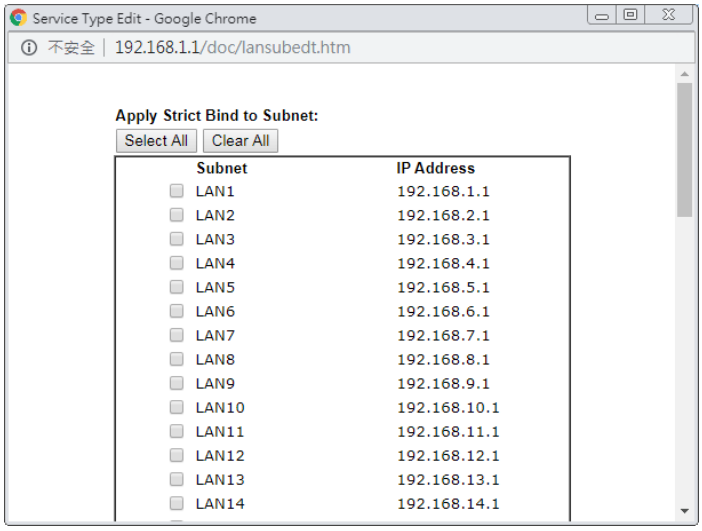
This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

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



Available settings are explained as follows:

Item	Description
Enable	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	Check the box to block the connection of the IP/MAC which is not listed in IP Bind List. LAN clients will be assigned IP addresses according to the MAC-to-IP address associations on this page. LAN client whose MAC address has not been bound to an IP address will be denied network access.

	Note: Before selecting **Strict Bind**, make sure at least one valid MAC address has been bound to an IP address. Otherwise no LAN clients will have network access, and it will not be possible to connect to the router to make changes to its configuration. **Apply Strict Bind to Subnet** – Choose the subnet(s) for applying the rules of Bind IP to MAC. 
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.
Select All	Select all entries in the ARP Table for manipulation.
Sort	Sort the entries in the ARP Table by IP address.
Refresh	Refresh the screen to reflect the current state of the ARP table.
Add / Update to IP Bind List	**IP Address** – Enter the IP address to be associated with a MAC address. **Mac Address** – Enter the MAC address of the LAN client's network interface. **Comment** – 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.

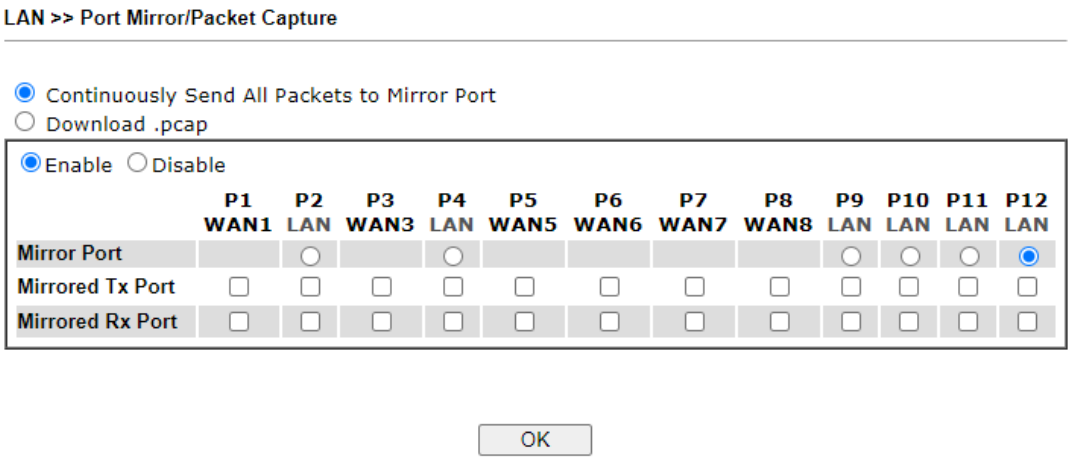
When you finish the configuration, click **OK** to save the settings.

II-3-4 Port Mirror/Packet Capture

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.

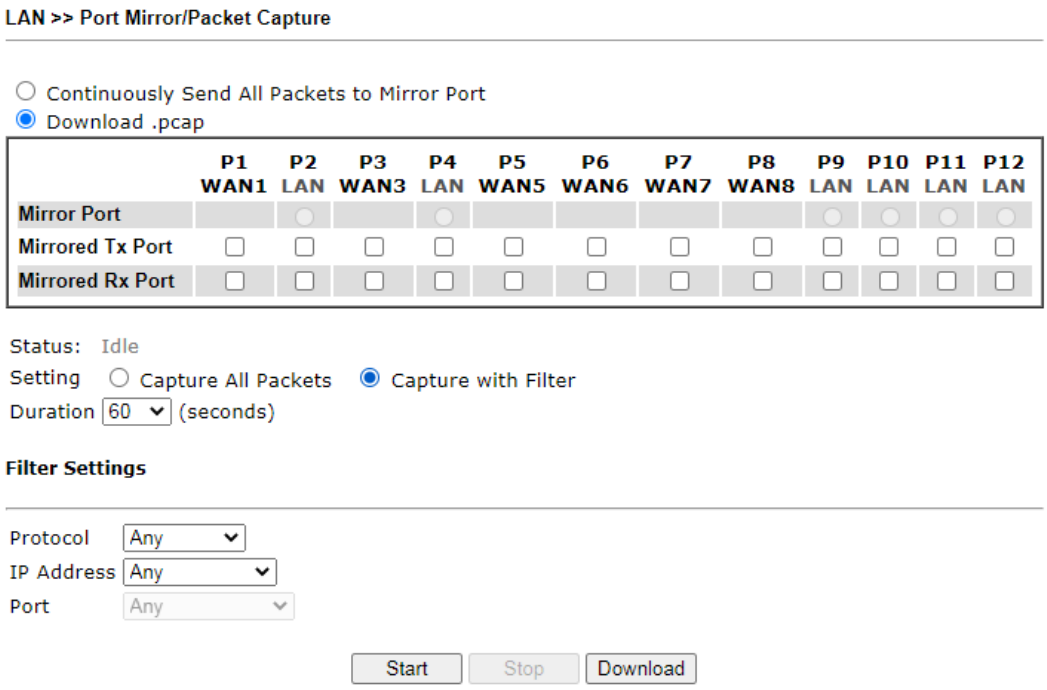
If selecing "Continuously Send All Packets to Mirror Port", the setting page will be shown as follows:



Available settings are explained as follows:

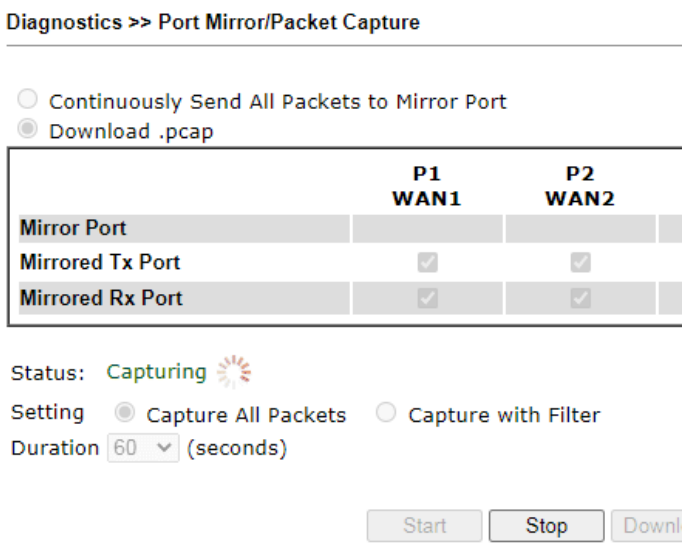
Item	Description
Continuously Send All Packets to Mirror Port	Select to send all packets to mirror port.
Enable/Disable	Select Enable to activate the function. Select Disable to cancel the function.
Mirror Port	One and only one port is selected as the mirror port, to which traffic is to be forwarded.
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.
OK	Save the settings.

If selecing "Download .pcap", the setting page will be shown as follows:



Available settings are explained as follows:

Item	Description
Download .pcap	If it is selected, the packets from the specified mirror port can be downloaded for analysis.
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.
Setting	**Capture All Packets** - All packets will be captured for analysis. **Capture with Filter** - Only the packets filtered by ICMP, TCP, UDP, or TCP/UDP will be captured for analysis.
Duration	Set a period of time for Vigor router to capture the packets.
Filter Settings	It is available only when Capture with Filter is selected. **Protocol** - Filter the packet by using Any, ICMP, TCP, UDP, and TCP/UDP. **IP Address** - Filter the packet by IP address. If Customized IP is selected, please enter an IP address in the entry box. **Port** - It is available when TCP, UDP, or TCP/UDP is selected as the Protocol. Select Any or Customize Port. If Customize Port is selected, please enter a port number in the entry box.
Start	Click to begin the packet capturing.

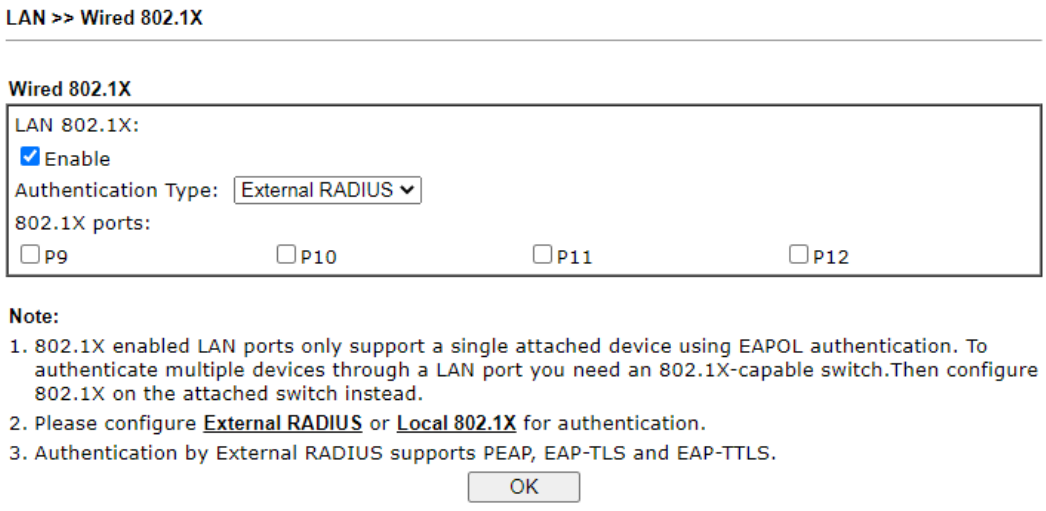
	
Stop	Click to terminate the scanning job.
Download	Click to download the packet capture result as a file with the file format,.pcap.

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

II-3-5 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:

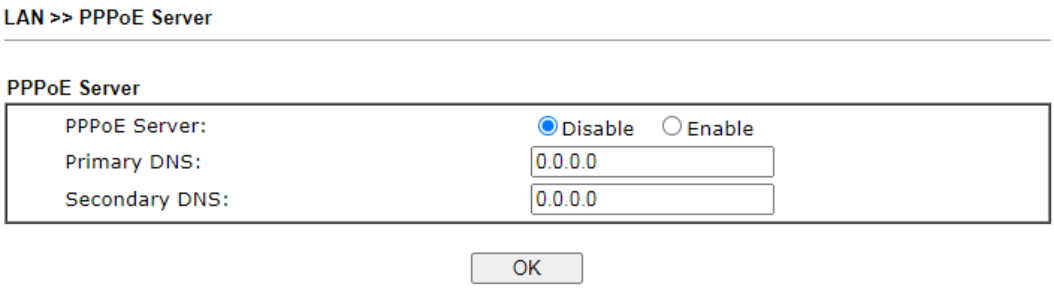
Item	Description
Enable	Check the box to enable LAN 802.1x function.
Authentication Type	**External RADIUS -** An external RADIUS server is to be used for 802.1X authentication. Go to **Applications >> RADIUS / TACACS+>>External RADIUS** to specify the RADIUS server. **Local 802.1X** - Use the user database on the router to

	authenticate clients. Go to **User Management >> User Profile** to set up users by entering user names, passwords and ensure that Local 802.1X service is enabled for the profiles.
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-3-6 PPPoE Server

LAN users can access into Internet through built-in PPPoE server on Vigor router. PPPoE server is a mechanism which can authenticate LAN users (configured in **User Management>>User Profile**) and prevent ARP attack completely.



Available settings are explained as follows:

Item	Description
PPPoE Server	Enable – Activate the built-in PPPoE Server. Disable – Disable the built-in PPPoE Server.
Primary DNS / Secondary DNS	Type the IP address(es) of Primary /Secondary DNS server for PPPoE Client(s) in LAN.

II-4 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.

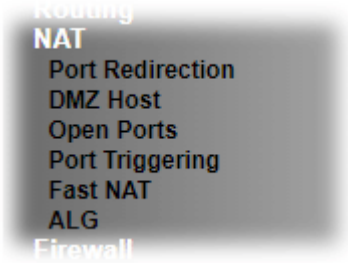
The benefit of the NAT includes:

- **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.

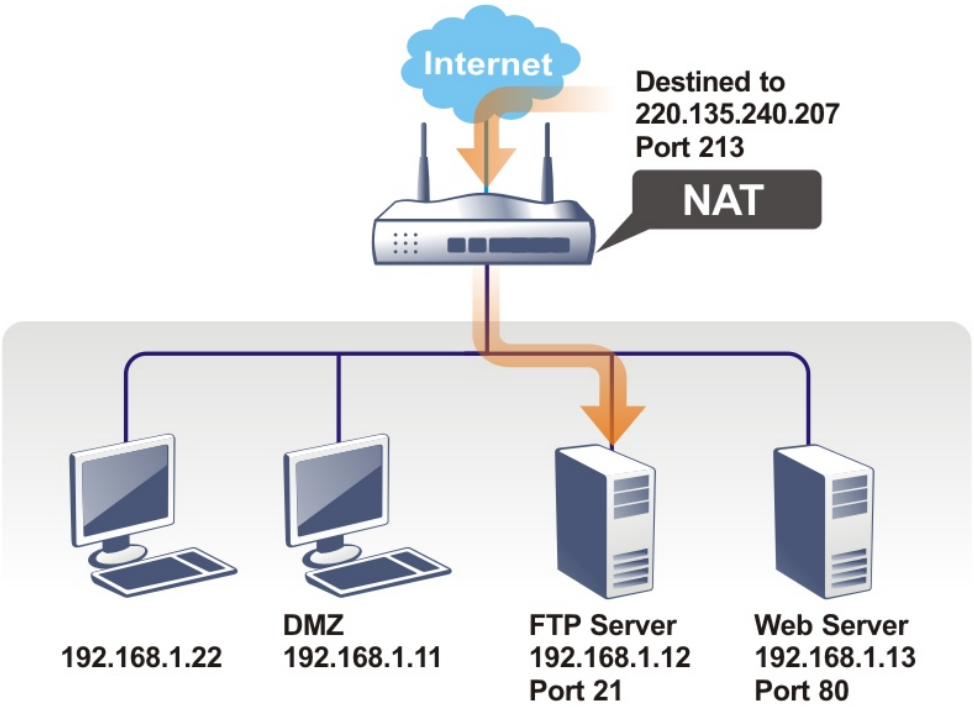
Web User Interface



II-4-1 Port Redirection

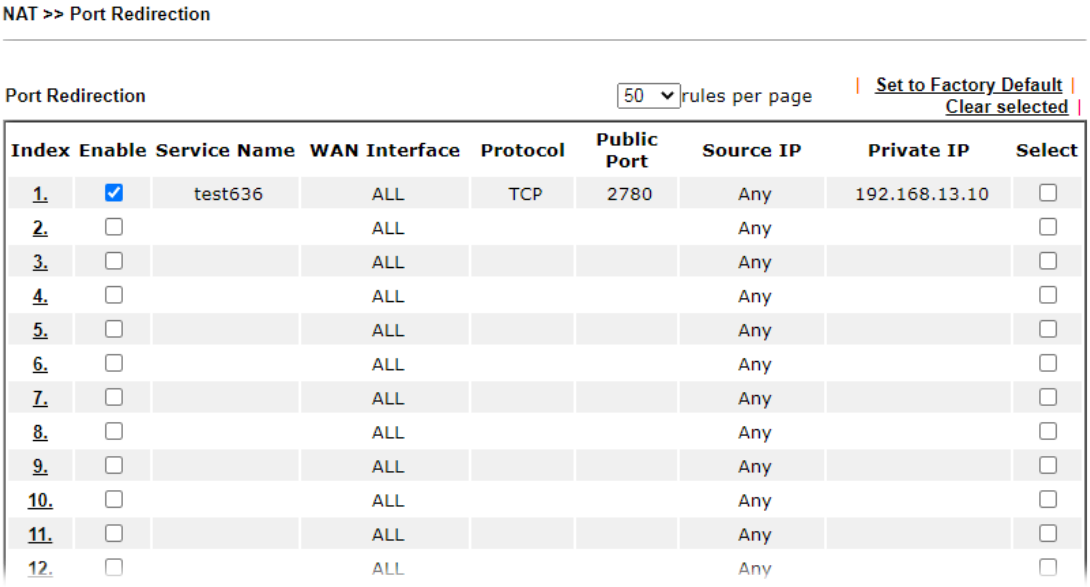
Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually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

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.



The port redirection can only apply to incoming traffic.

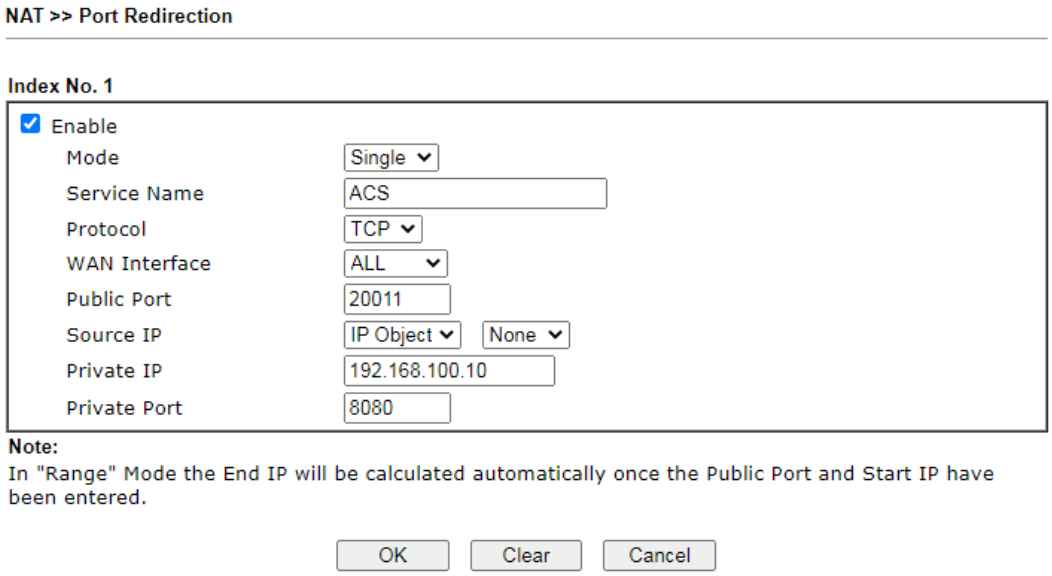
To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 520 port-mapping entries for the internal hosts.



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.



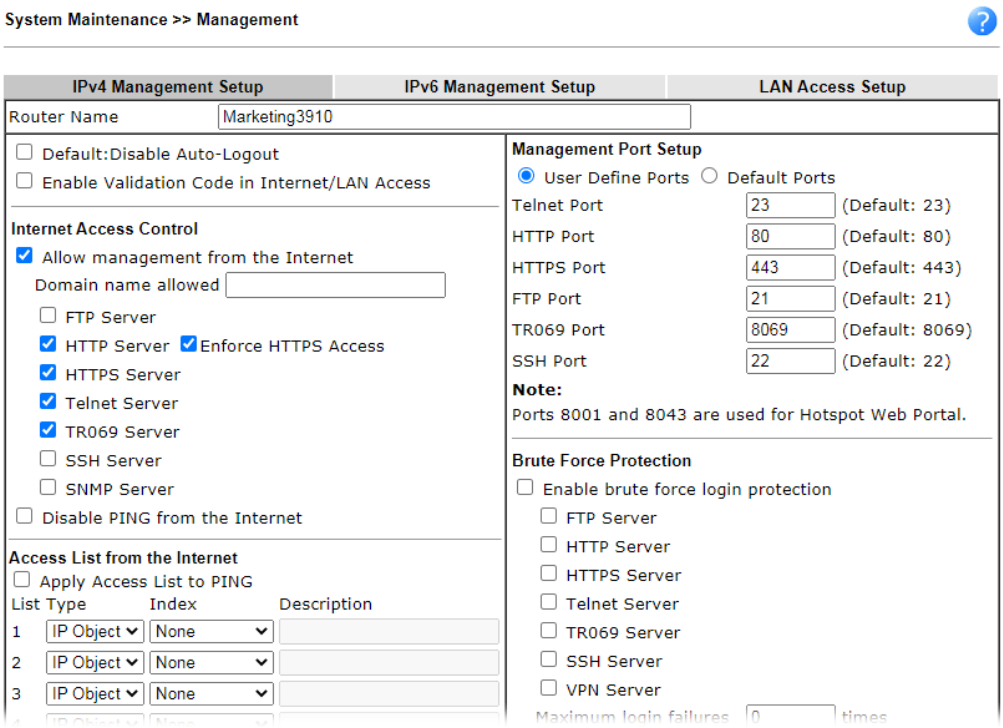
Available settings are explained as follows:

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.

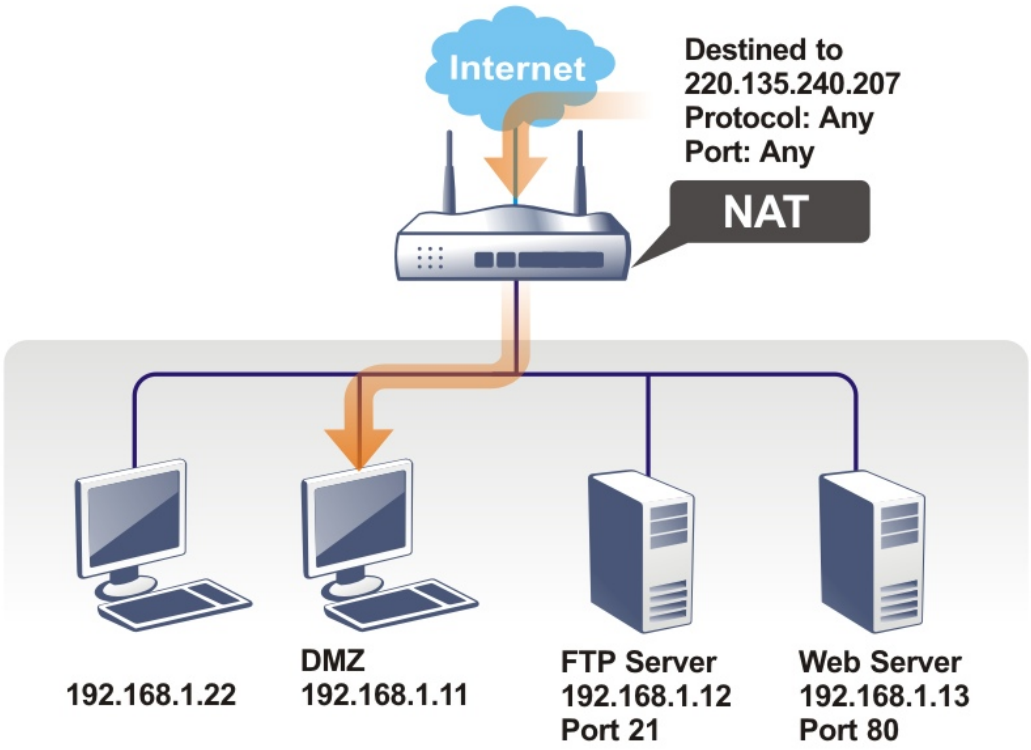
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

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.



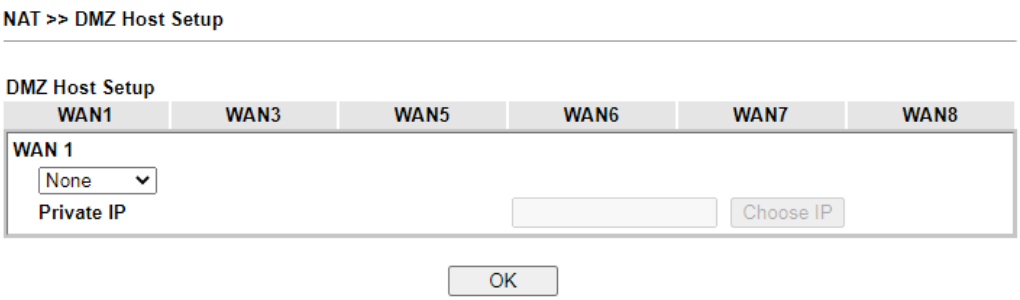
II-4-2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.

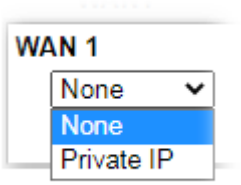
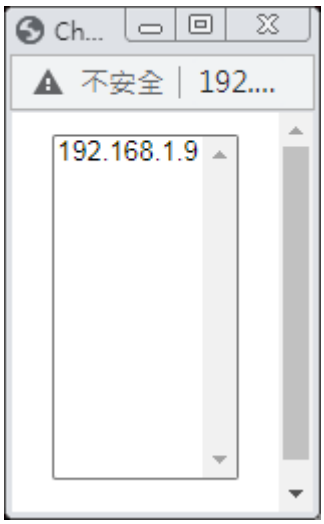


The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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

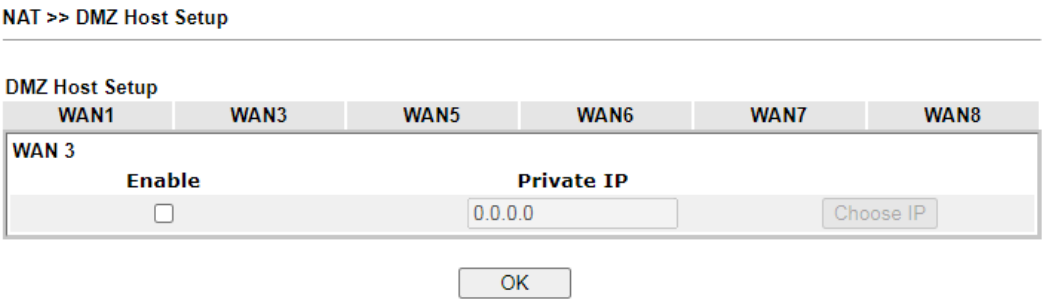


Available settings are explained as follows:

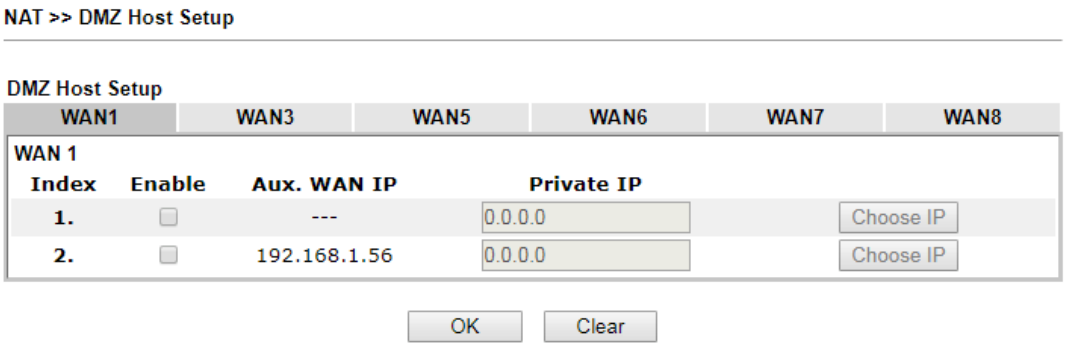
Item	Description
	Enables or disables DMZ host. **None** - Disables DMZ host function. **Private IP** - Allows WAN traffic to be sent to a specific LAN IP address.
Private IP	If Private IP mode has been selected, click the **Choose IP** button to select a LAN IP address.
Choose IP	Click this button and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

DMZ Host for other WAN interface is slightly different with WAN1. **Active True IP** selection is available for WAN1 only.

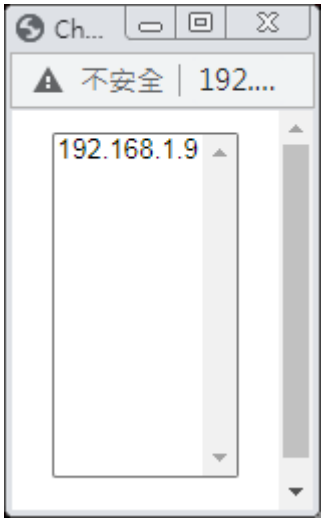
See the following figure.



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.

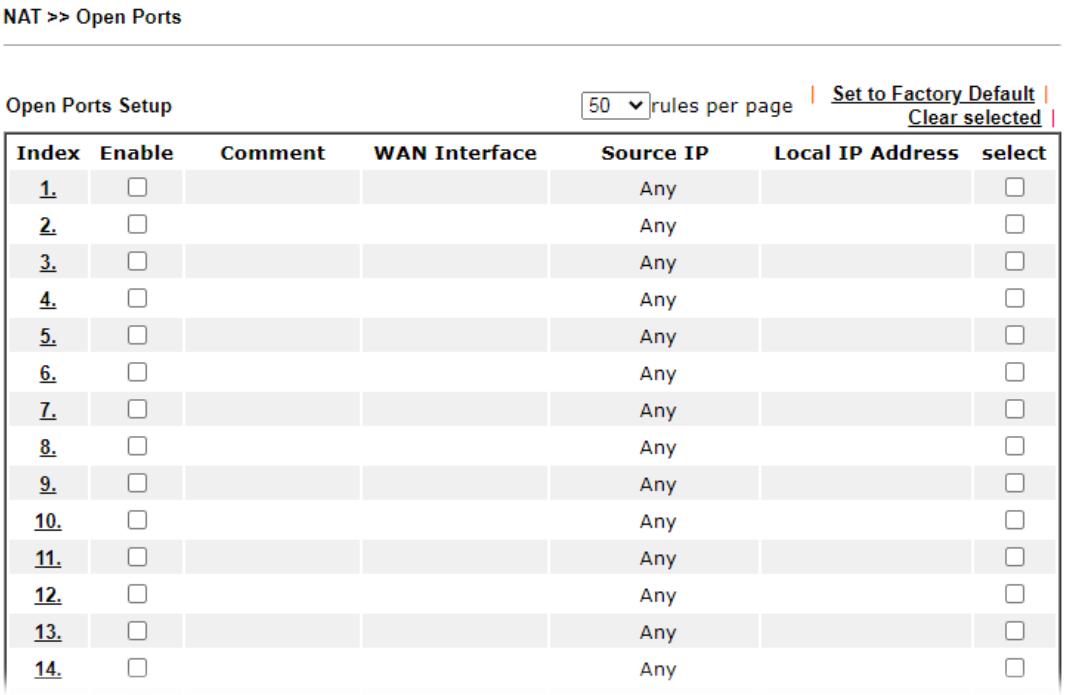
After finishing all the settings here, please click **OK** to save the configuration.

II-4-3 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.

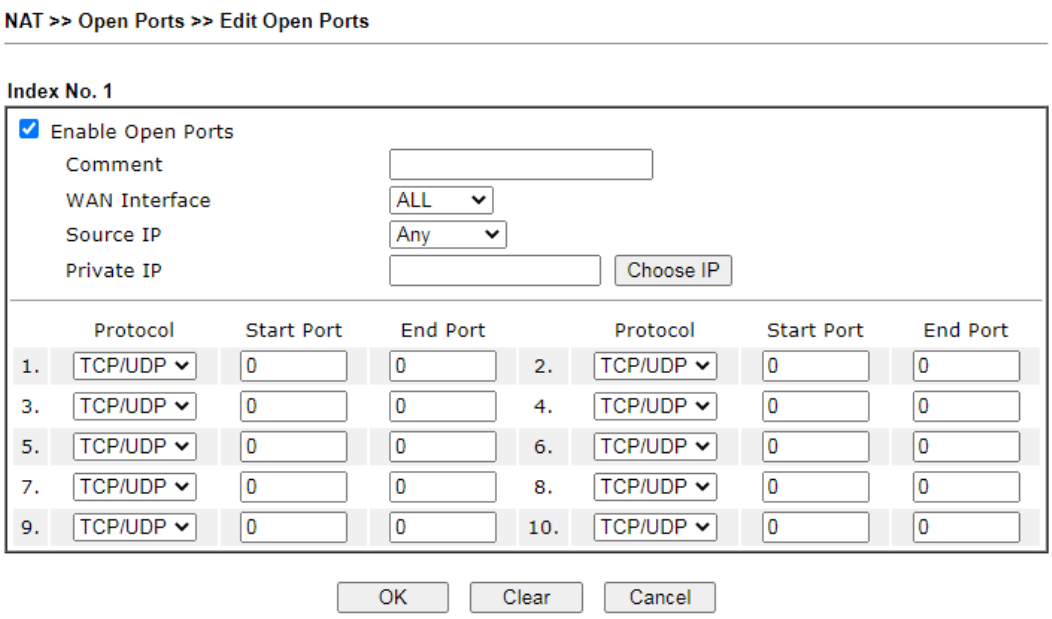
The common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule, and others), Internet Camera, etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.



Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry (1 to 260) that you want to offer service in a local host. 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.

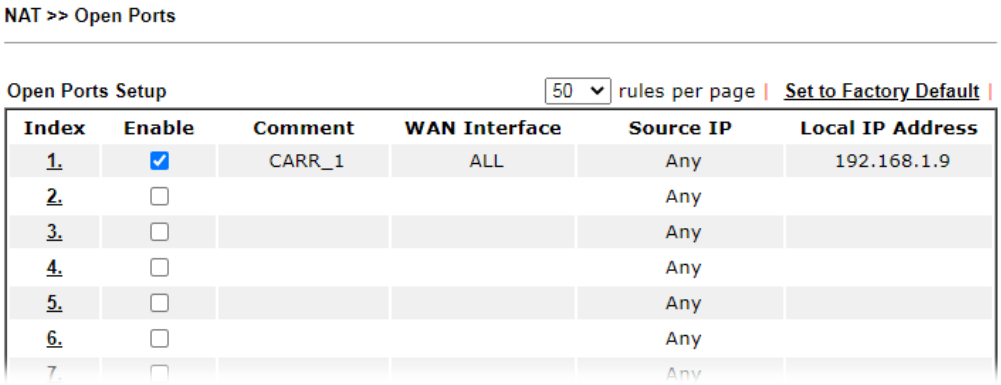
To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.



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-4-4 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.

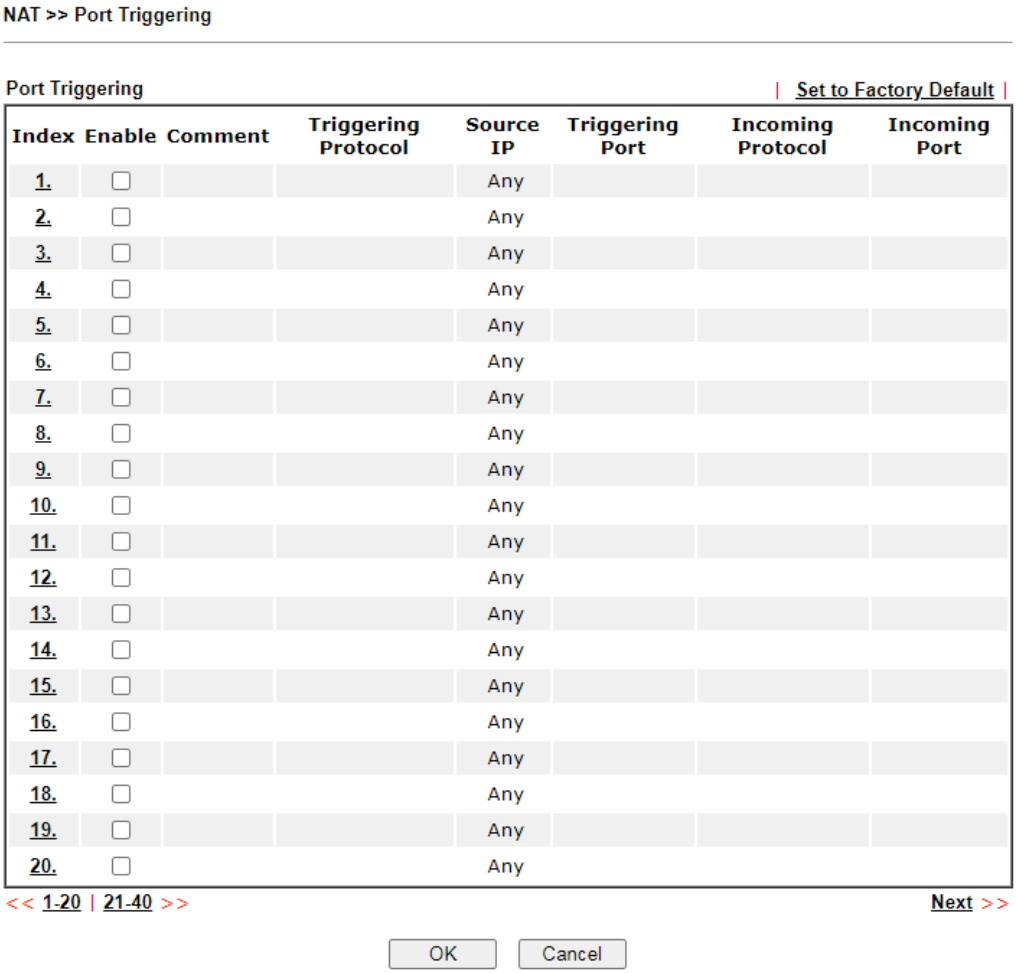
  TCP: 86400 sec.

  UDP: 180 sec.

  IGMP: 10 sec.

  TCP WWW: 60 sec.

  TCP SYN: 60 sec.

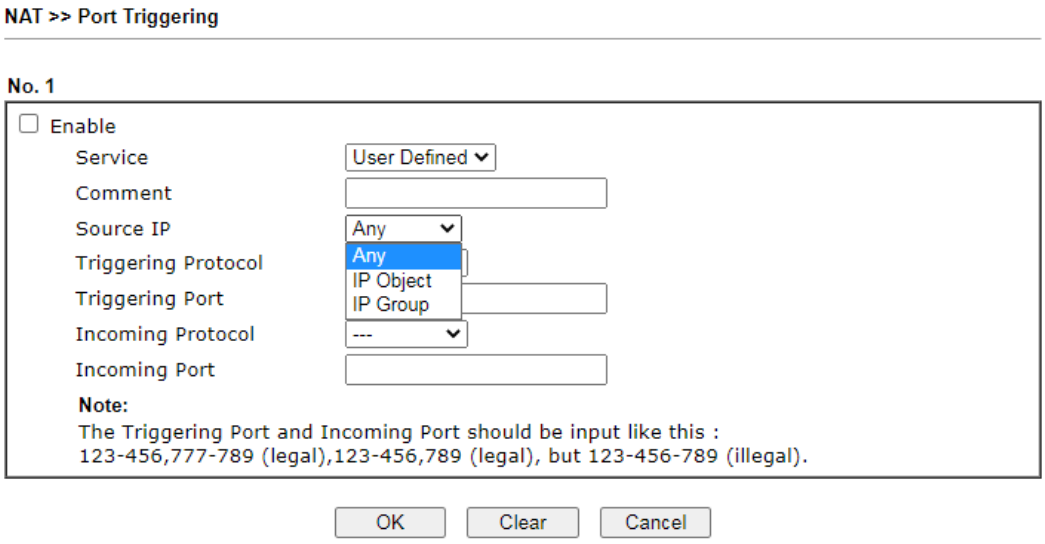


Available settings are explained as follows:

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.

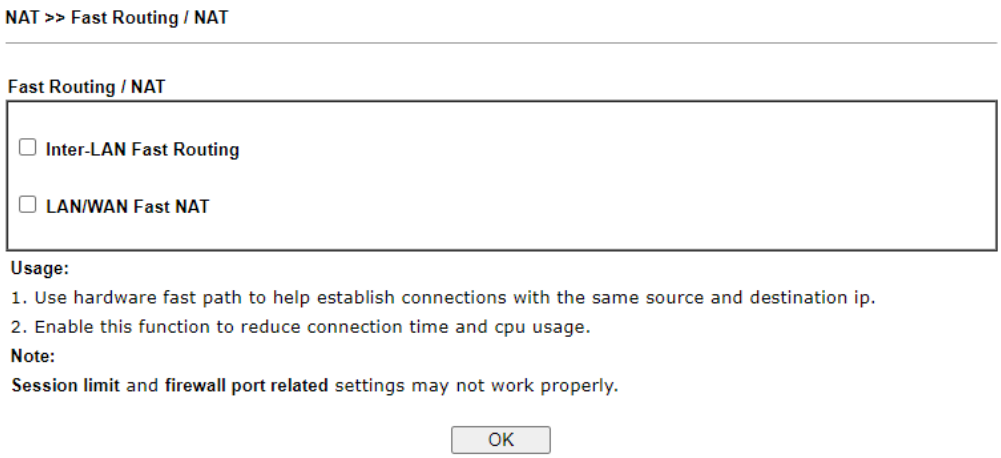
After finishing all the settings here, please click **OK** to save the configuration.

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-4-5 Fast NAT

This function allows for establishing a network connection with a built-in acceleration engine. Time can be saved and CPU usage can be reduced.



Available settings are explained as follows:

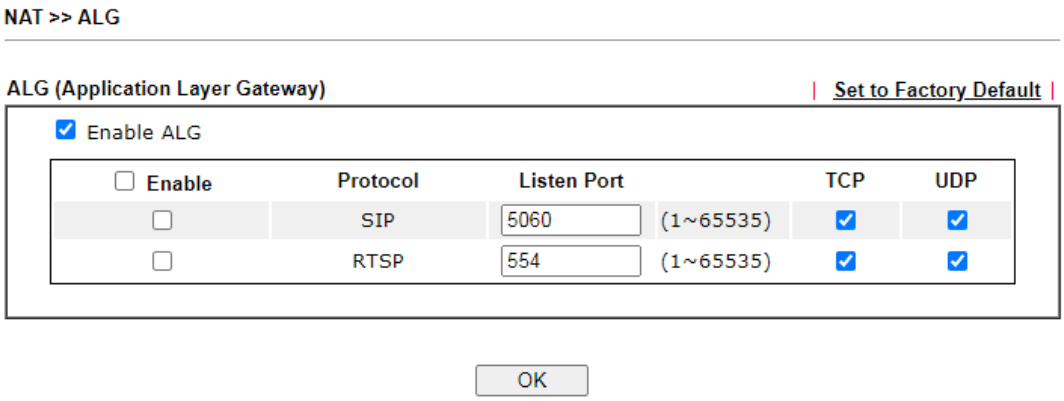
Item	Description
Inter-LAN Fast Routing	If enabled, the routing connection will be accelerated.
LAN/WAN Fast NAT	If enabled, the NAT connection will be accelerated.

II-4-6 ALG

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

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

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



Available settings are explained as follows:

Item	Description
Enable ALG	Check to enable such function.
Listen Port	Type a port number for SIP or RTSP protocol.
TCP	Check the box to make correspond protocol message packet from TCP transmit and receive via NAT.
UDP	Check the box to make correspond protocol message packet from UDP transmit and receive via NAT.

II-5 Applications

Dynamic DNS

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.

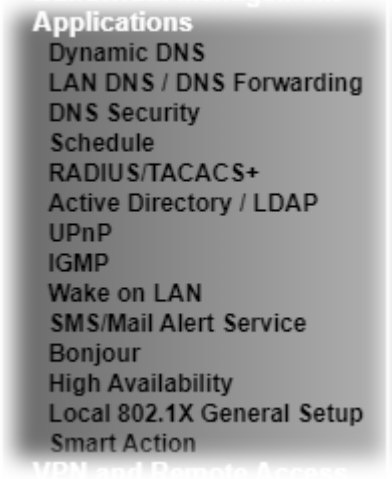
Examples of applications and devices that support UPnP include file-sharing applications such as uTorrent, Vuze and eMule, gaming consoles such as the Sony PlayStations 3 and 4 Xbox 360 and Xbox One, media streaming applications such as Plex and XBMC, and messaging and calling applications such as Skype. 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.

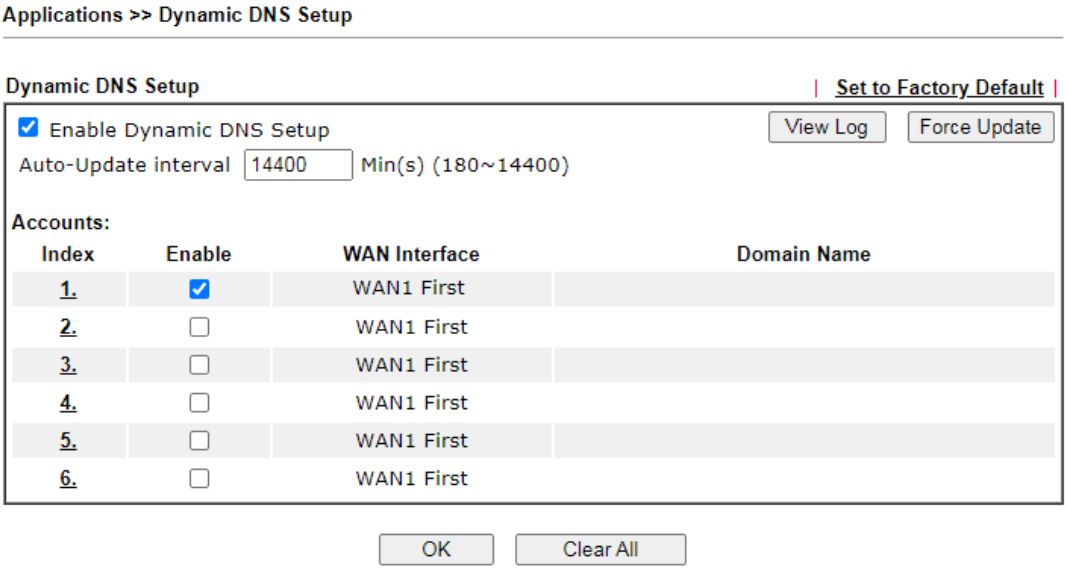
Web User Interface



II-5-1 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:

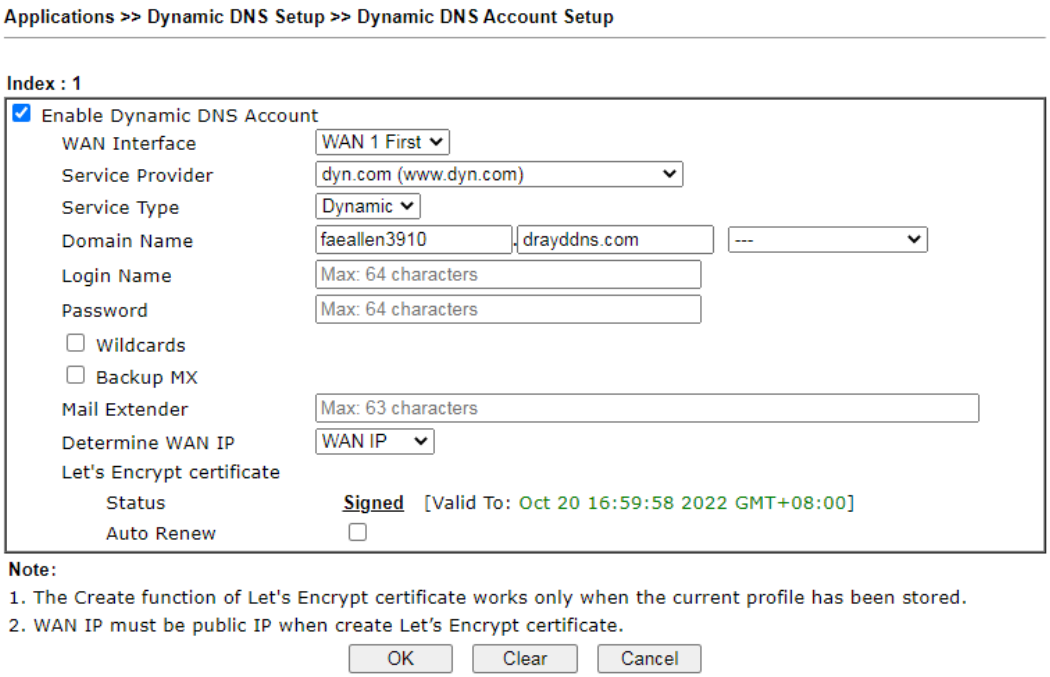


Available settings are explained as follows:

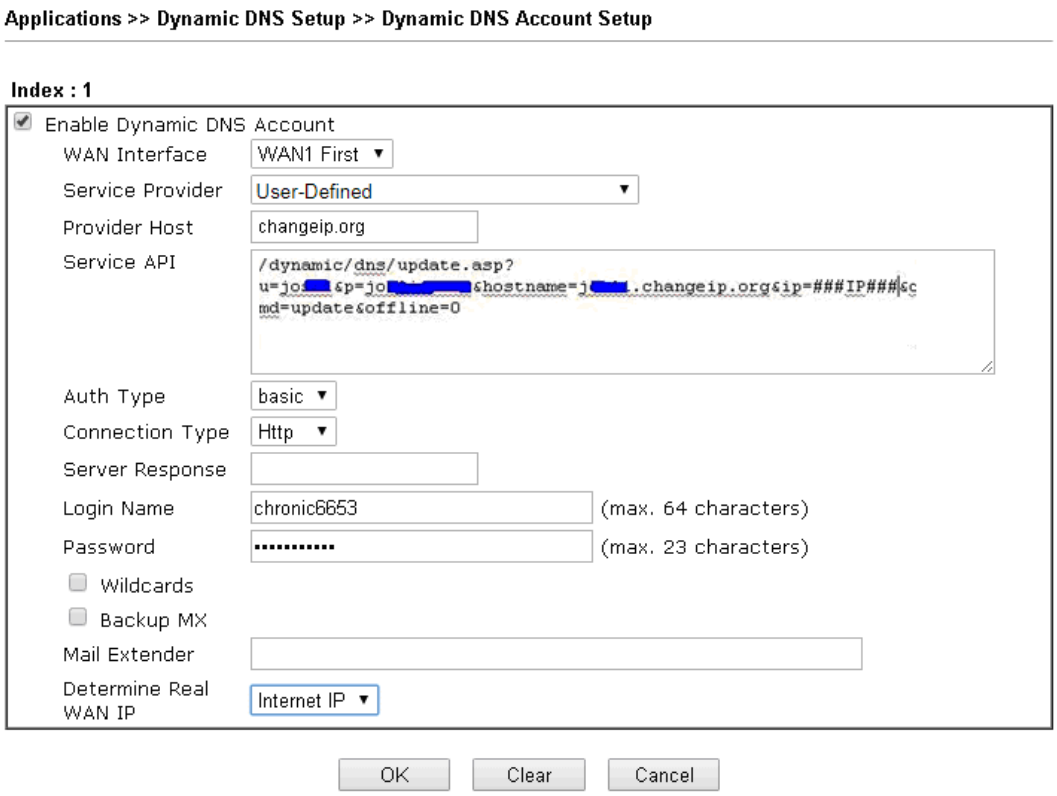
Item	Description
Enable Dynamic DNS Setup	Select to enable DDNS function.
Set to Factory Default	Click to clear all profiles to factory settings.
View Log	Select to display the most recent DDNS update messages.
Force Update	Click to connect immediately to DDNS servers to update IP address information.

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.
WAN Interface	Shows the WAN interface associated with the DDNS profile.
Domain Name	Shows the domain name with which the profile is associated.

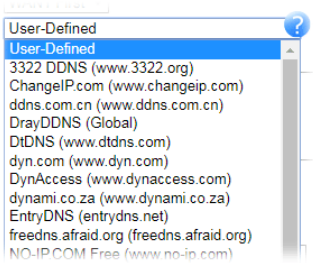
After clicking on the index number, the detail configuration screen for the DDNS profile appears:



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.
Let's Encrypt certificate	**Create –** Click it to generate a certificate issued by Let's Encrypt for applying to such DDNS account. **Auto Renew**– Check the box to make the system update the

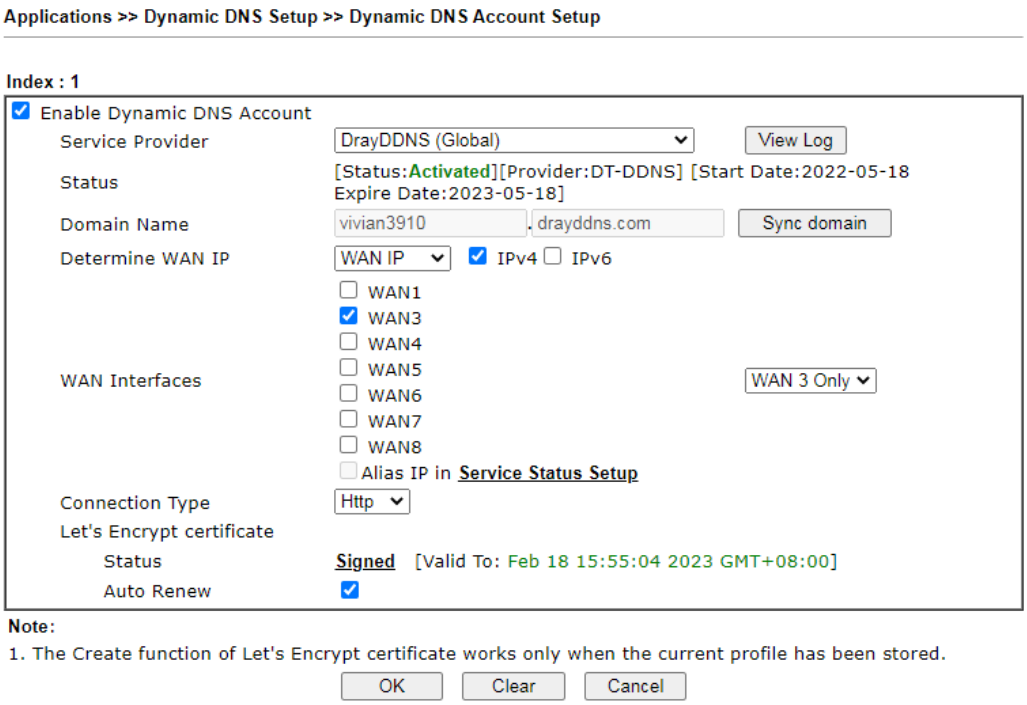
	certificate automatically.

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.
Status	Display if the license is actvtaed or not.
Domain Name	The domain and subdomain to be updated.
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	**Auto Renew** – Check the box to make the system update the certificate automatically.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

DDNS updates take place when:

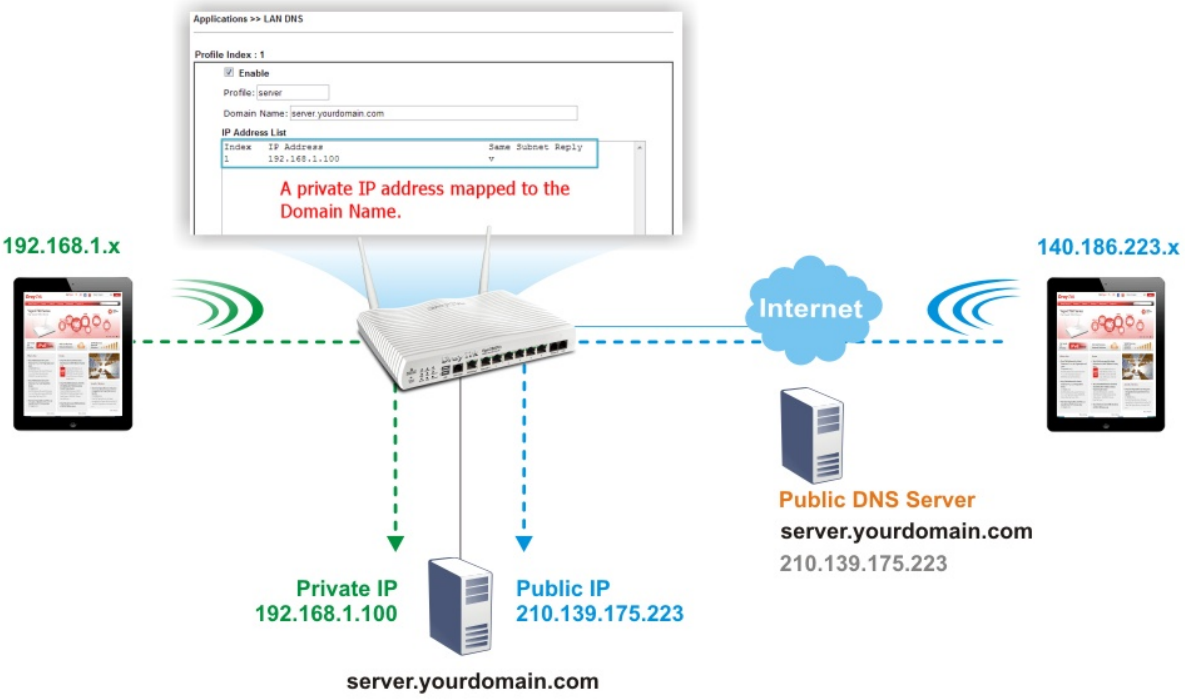
- The router is powered on or rebooted.
- The public IP address of any WAN interface changes.
- The online status of a WAN interface changes (going from online to offline or vice versa).
- The DDNS function is changed from disabled to enabled.
- A DDNS entry is modified and enabled.
- The Auto-Update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

Procedures for Setting up a Dynamic DNS Entry

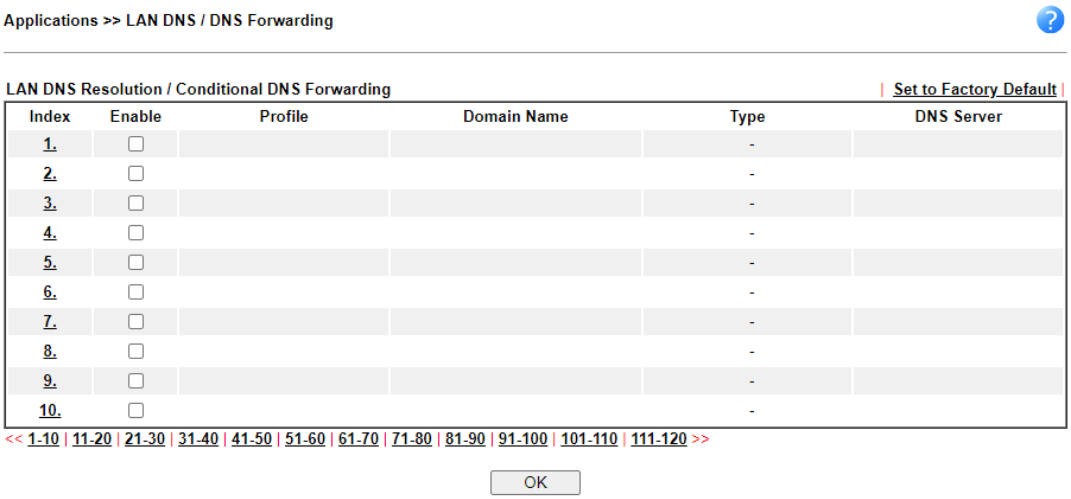
1. Contact the dynamic DNS provider of your choice and have service set up. Most DDNS providers accept signups on their websites. Service could be provided free of charge or for a fee.
2. Create a DDNS entry on the router by selecting the appropriate DDNS provider and enter the account information.
3. 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-5-2 LAN DNS / DNS Forwarding

The 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 Vigor3910 Series will respond the specified private IP address.



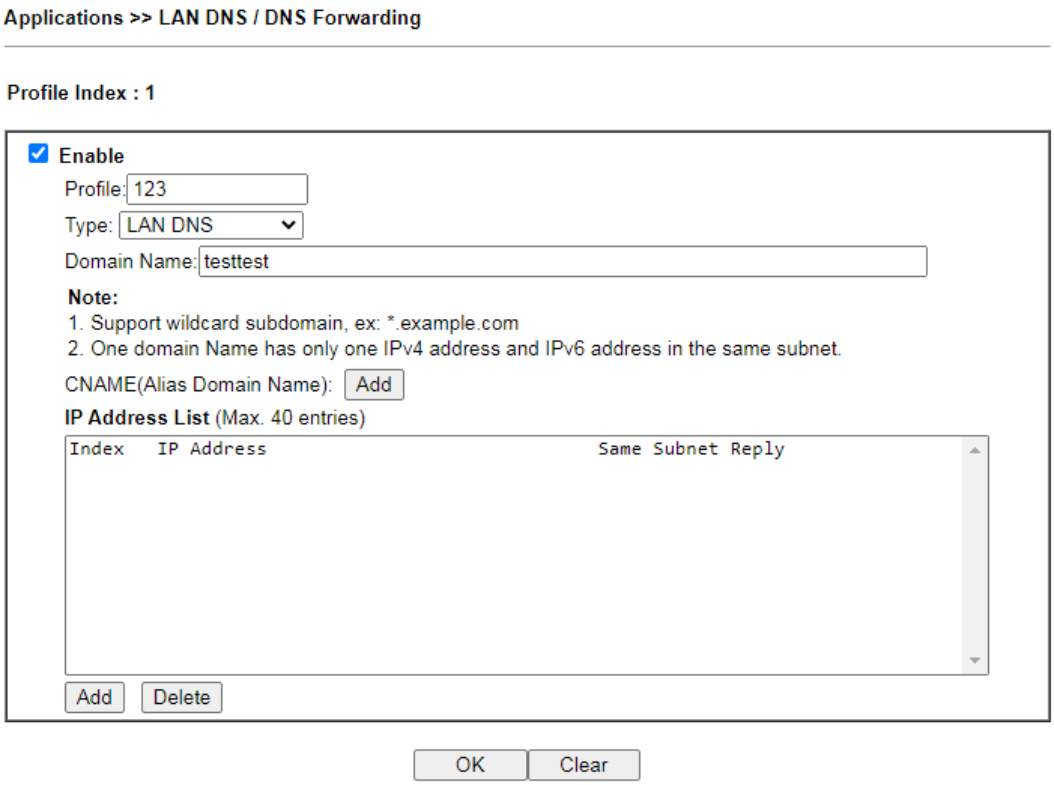
To start configuring LAN DNS or DNS Forwarding, from the main menu, click **Applications**, followed by **LAN DNS / DNS Forwarding**.



Each item is explained as follows:

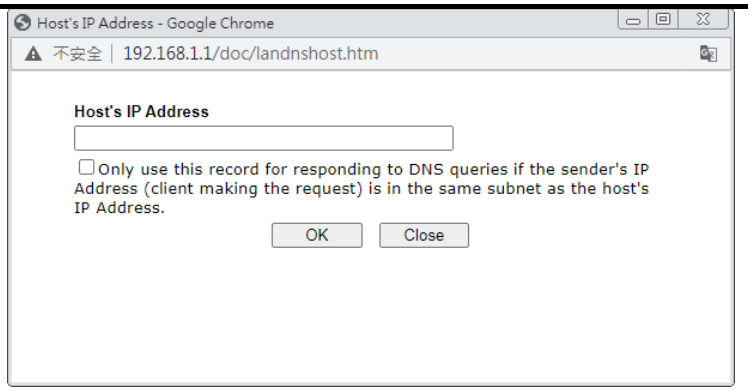
Item	Description
Set to Factory Default	Click to clear all profiles to factory settings.
Index	Click to bring up the configuration page for the profile.
Enable	Select to enable this profile.
Profile	Shows the name of the profile.
Domain Name	Shows the domain name configured for the profile.
Type	Display the type (LAN DNS or DNS Forwarding) of the profile.
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.
Type	Choose LAN DNS or LAN Forwarding.
If LAN DNS is selected	**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.
If DNS Forwarding is selected	**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. **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-5-3 DNS Security

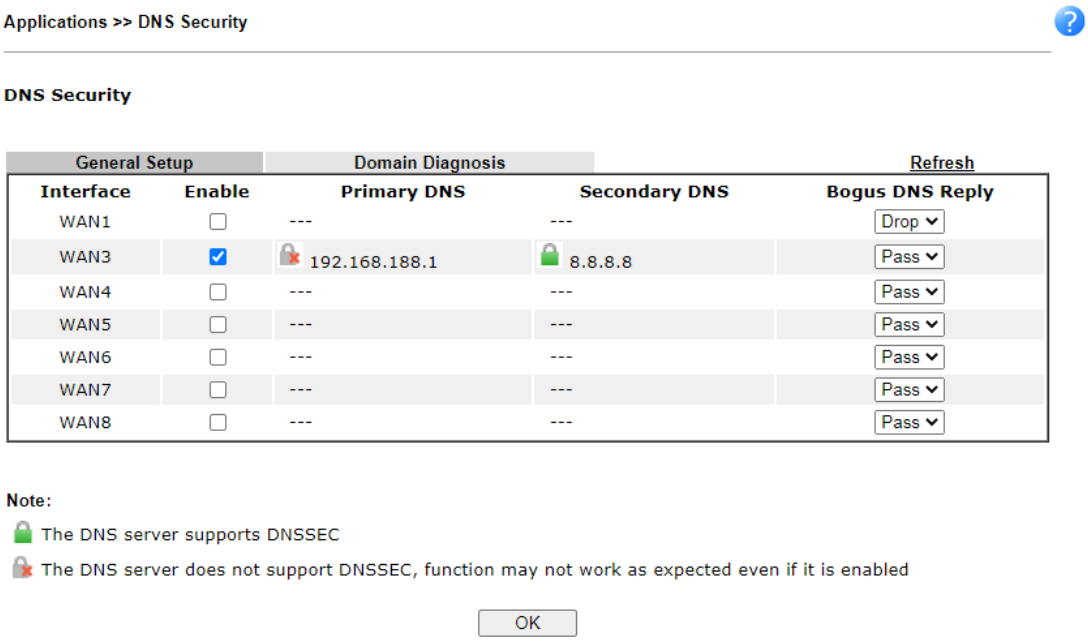
Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.

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-5-3-1 General Setup

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



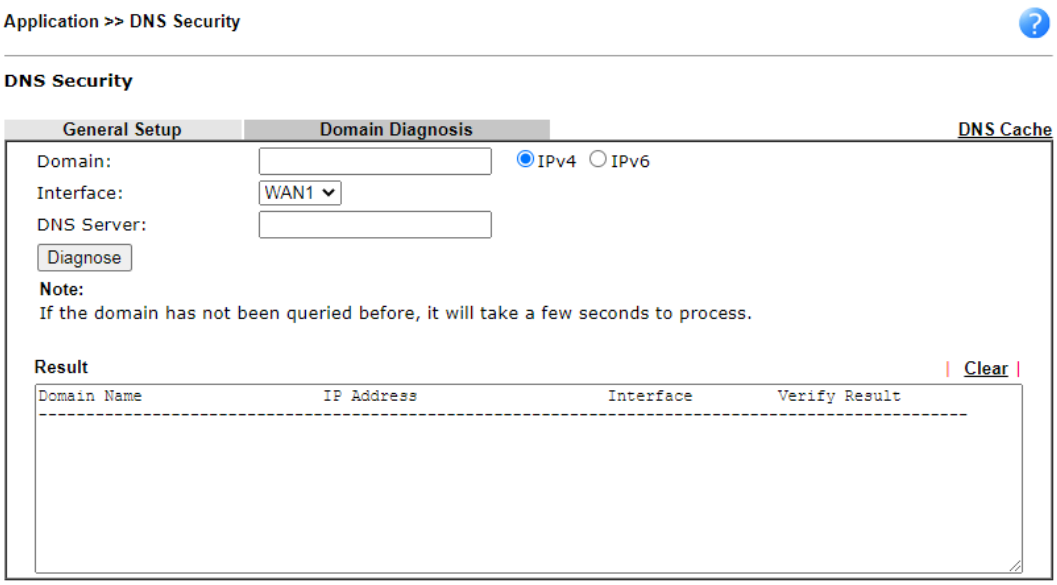
Available settings are explained as follows:

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-5-3-2 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-5-4 Schedule

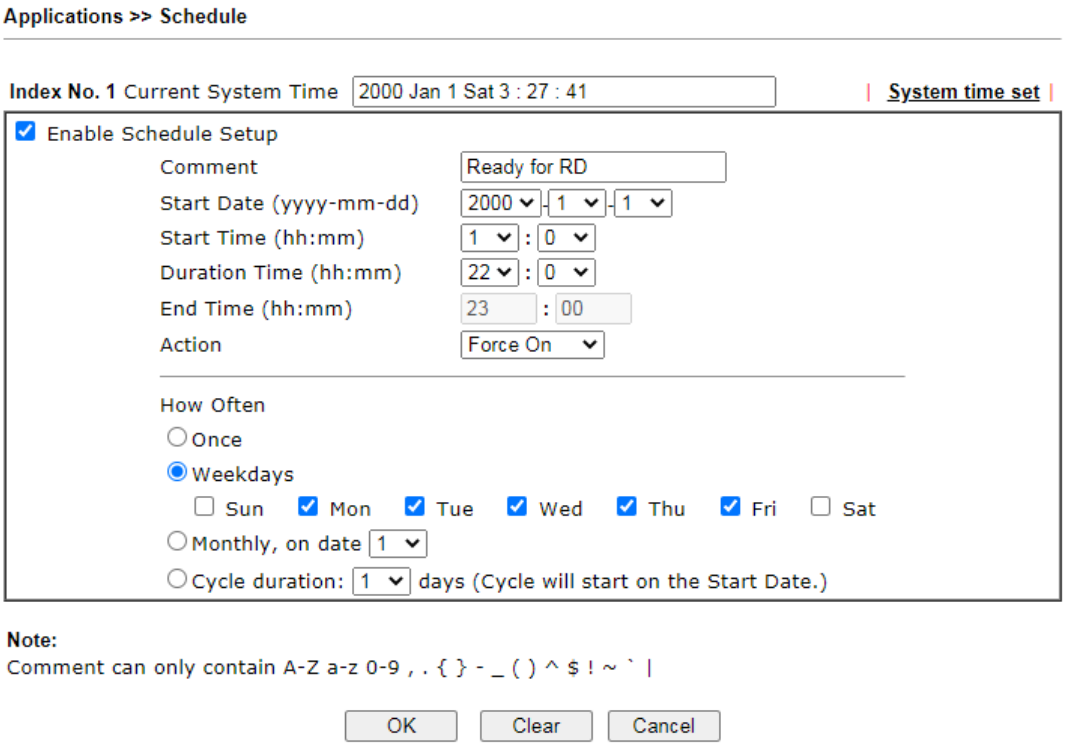
Time schedules can be created and used with router features that support them, so that those features can be turned on and off automatically at preconfigured times.

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-5-5 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 in enterprise networks. It is the most common authentication method to manage the clients' access to the wireless network, the Internet and the VPN.

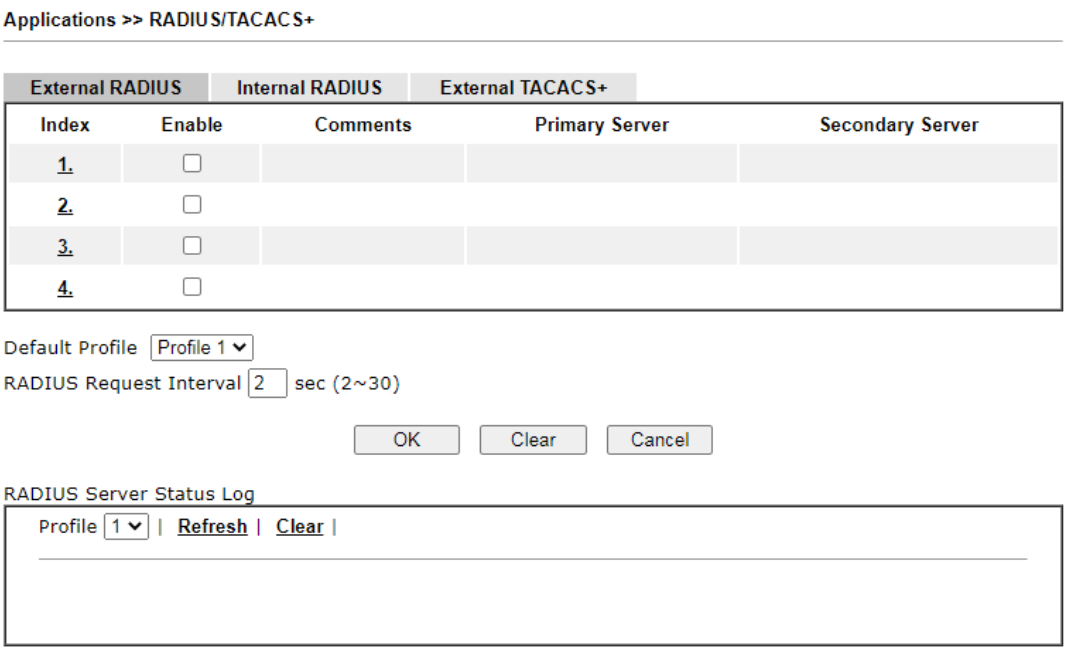
The router supports external TACACS+ and internal and external RADIUS servers for user authentication. To configure TACACS+ or RADIUS servers, from the Main Menu select **Applications >> RADIUS/TACACS+**.

II-5-5-1 External RADIUS

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

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

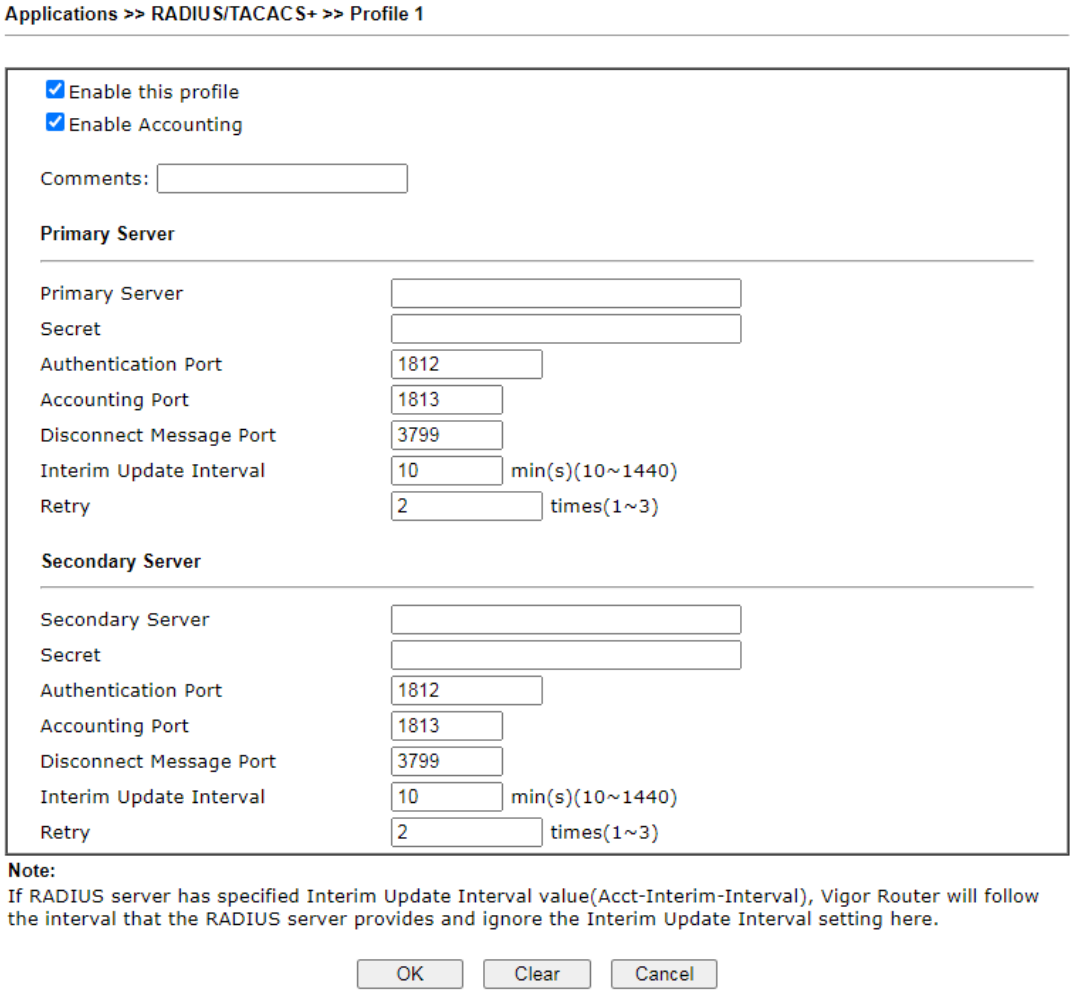
Select External RADIUS to configure the router to use an external RADIUS server for user authentication.



Item	Description
Enable	Select to enable the profile.
Comment	Displays the comment of the profile.
Primary Server	Displays the IP address of the primary server.
Secondary Server	Display the IP address of the secondary server.
Default Profile	Select one of the profiles as the default profile for user authentication.
RADIUS Request Interval	Set a timeout value for the router waiting for a response from the RADIUS server. If no response, Vigor router will send the authentication request again.

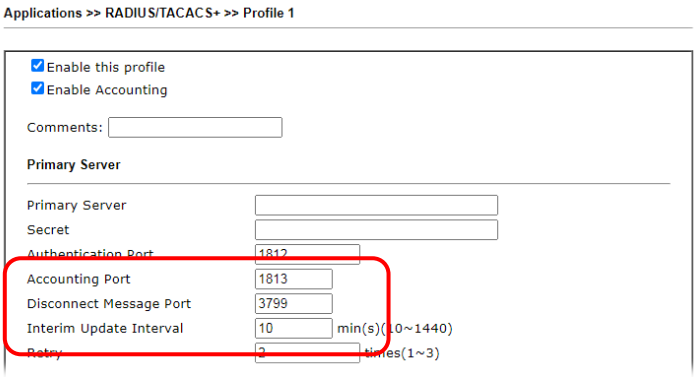
RADIUS Server Status Log	Display the record of current status of RADIUS server.

Click any index number to open the following page. It is used to configure settings for external RADIUS server. Then users of the Vigor router will be authenticated by this server for the network application.



Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable RADIUS client profile. **Comment** - Enter a brief description for this profile.
Enable Accounting	After checking it, Vigor router supports the accounting feature (available seconds for using, quantity of RX/TX data) for external RADIUS server. Any client tries to access the Internet shall be authenticated and accounted by an external RADIUS server. **Accounting Port** –The UDP port number that the RADIUS server is using. The default value is 1813, based on RFC 2138. **Disconnect Message Port** – Set a port number for listenning the RADIUS disconnection message. **Interim Update Interval** – Set a time interval for sending the accounting request to the RADIUS server.

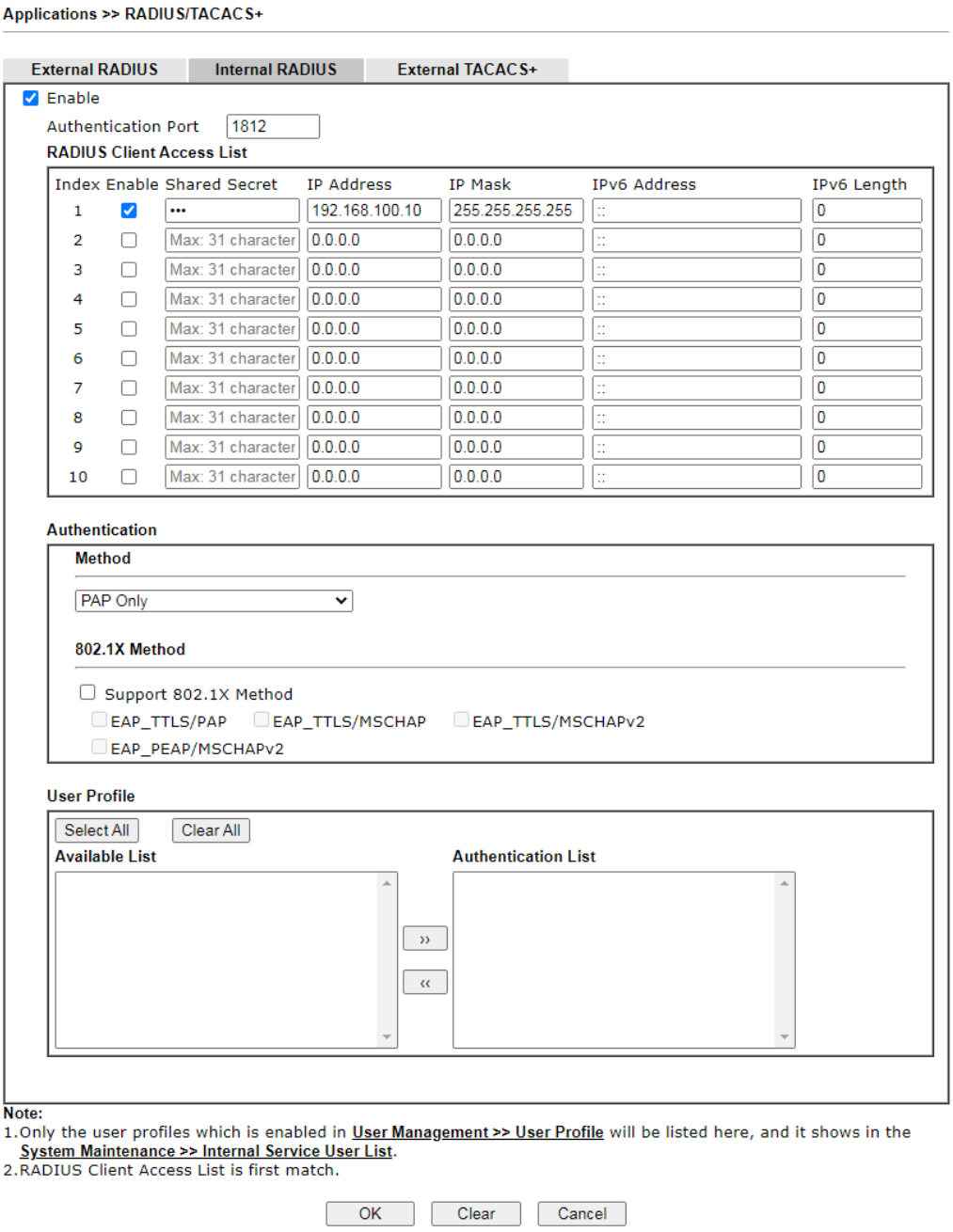
	
Primary Server	**Primary Server** - Enter the IP address of RADIUS server. **Secret** - The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can 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".

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

II-5-5-2 Internal RADIUS

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

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



Available settings are explained as follows:

Item	Description
Enable	Select to enable the router's internal RADIUS server.
Authentication Port	The UDP port for authentication message.
RADIUS Client Access List	Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server. **Index** - The index number of the client entry. **Enable** - Select to enable this client entry. **Shared Secret** - A text string that is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them. Maximum length is 36 characters. **IP Address** – Enter the base address of the IP block.

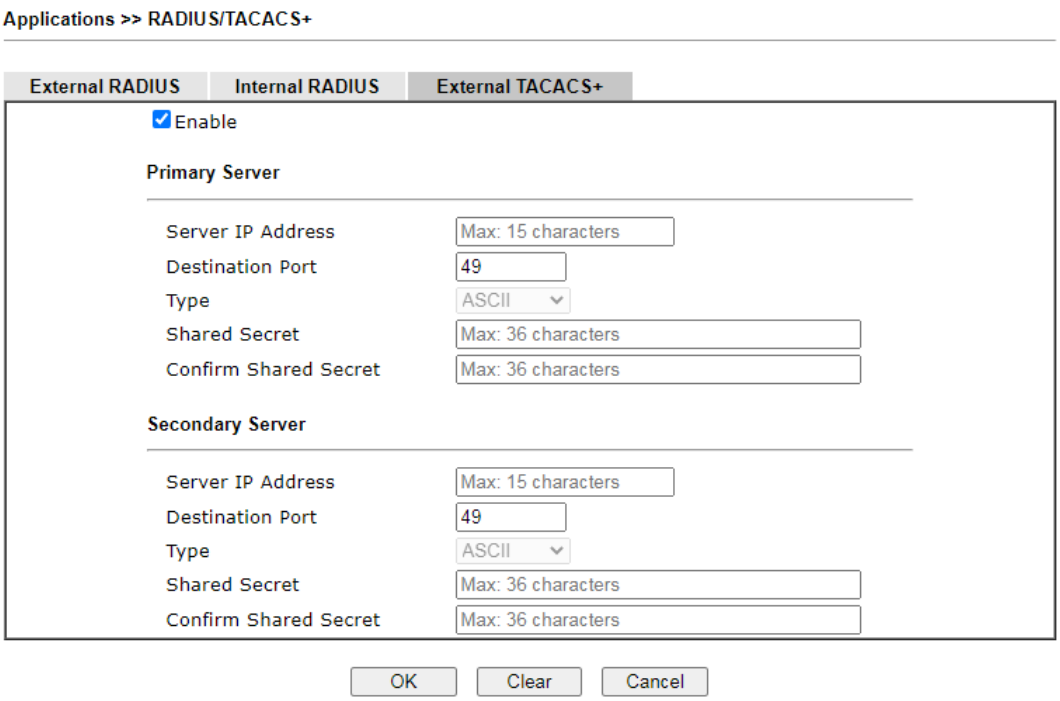
	IP Mask – Enter the IP mask to configure the size of the IP block. **IPv6 Address** – Enter the base address of the IPv6 block. **IPv6 Length** - Enter the prefix length of the IPv6 block.
Authentication	Configures the authentication settings. Specify the way to authenticate the client. **PAP –** Only the Password Authentication Protocol will be used to validate users. **PAP/CHAP/MS-CHAP/MS-CHAPv2 –** PAP, CHAP (Challenge-Handshake Authentication Protocol), and Microsoft versions of CHAP can be used to validate users. **Support 802.1X Method** – The built in RADIUS server offered by Vigor router can act as the AAA server. Select to enable 802.1X support.
User Profile	During the process of security authentication, user account and user password will be required for identity authentication. Before configuring such page, create at least one user profile in **User Management>>User Profile** first. **Select All** – Click to move all user profiles under the Available List to the Authentication List. **Clear All**- Click to remove all user profiles from the Authentication List. **Available List** – User profiles (created in **User Management >> User Profile**) that have not been added to the authentication list. **Authentication List** – User profiles (created in **User Management >> User Profile**) that have been added to the authentication list. Users can log in using these profiles.

To add a User Profile to the RADIUS server, select it under Available List, then click the >> button. To remove a User Profile from the RADIUS server, select it under Selected Authentication List, then click the << button.

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

II-5-5-3 External TACACS+

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



Available settings are explained as follows:

Item	Description
Enable	Select to enable the use of an external TACACS+ server.
Primary Server / Secondary Server	Two external TACACS+ servers are allowed to set in this page. The secondary TACACS+ server will be used as a backup server when the primary TACACS+ server is down.
Server IP Address	The IP address of the TACACS+ server.
Destination Port	The port used by the TACACS+ server. Port 49 is most common.
Shared Secret	A text string that is known to both the TACACS+ server and client (the router) that is used to authenticate messages sent between them. Maximum length is 36 characters.
Confirm Shared Secret	Enter the shared secret again for verification.

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

II-5-6 Active Directory/ LDAP

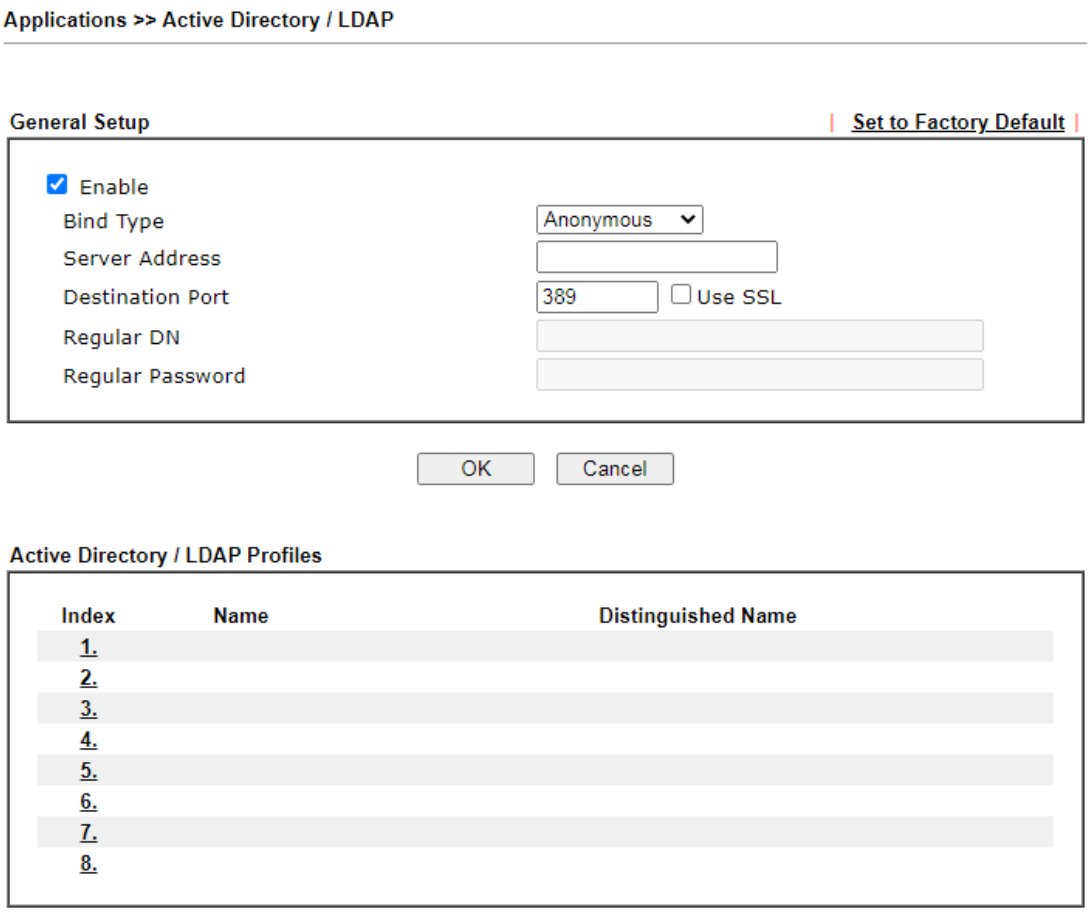
Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol for maintaining and accessing directory information on a network. When used in conjunction with a Vigor router, LDAP can be used to authenticate VPN connection attempts.

Active Directory (AD) is a directory service from Microsoft that supports LDAP queries.

To configure Active Directory or LDAP settings, from the Main Menu select **Applications >> Active Directory /LDAP**.

II-5-6-1 General Setup

To configure the settings for the LDAP server, select **General Setup**.



Available settings are explained as follows:

Item	Description
Enable	Select to enable LDAP client. If enabled, the LDAP profiles will be available for configuration.
Bind Type	Select from one of 3 bind types: ● **Simple Mode** – Initiate bind operation (authentication) without performing user search. This mode can be used when all users belong to the same branch in the LDAP structure. ● **Anonymous** – Bind anonymously, without supplying the distinguished name (DN) and password, and perform user

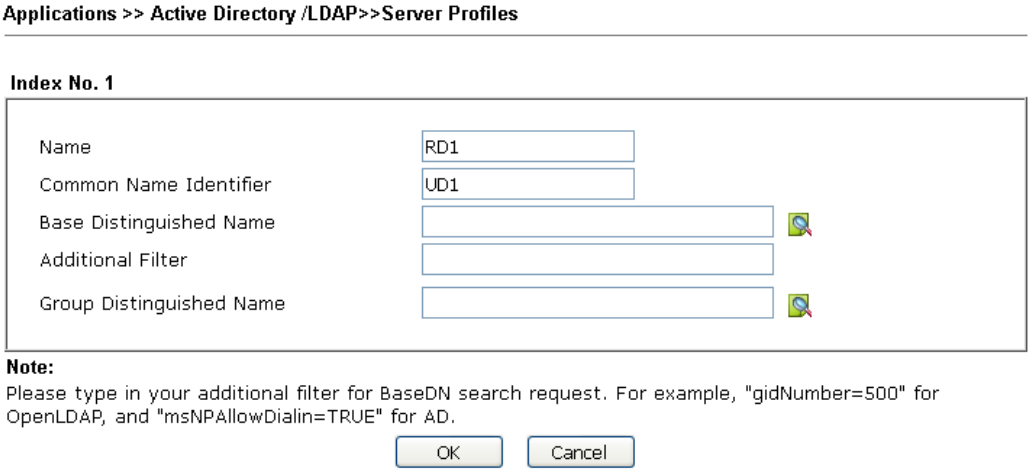
	search. This mode can be used when not all users belong to the same branch and the server allows anonymous searches. ● **Regular Mode** – Same as Anonymous mode, except that the DN and password are sent to the server. This mode can be used when not all users belong to the same branch and the server does not allow anonymous searches. For the regular mode, you'll need to Enter the **Regular DN** and **Regular Password**.
Server Address	The network address of the LDAP server.
Destination Port	The network port that the LDAP server listens on. The default ports are 389 for unsecured connections and 636 for LDAPS (LDAP over SSL) connections.
Use SSL	Select to use Secure Sockets Layer (SSL) for LDAP traffic.
Regular DN	Enter the LDAP Distinguished Name for authentication if **Bind Type** is set to **Regular Mode**.
Regular Password	Enter the LDAP Password for authentication if **Bind Type** is set to **Regular Mode**.
Active Directory / LDAP Profiles	Up to 8 LDAP profiles can be created. These profiles would be used with User Management for different purposes in management.

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

II-5-6-2 Active Directory / LDAP Profiles

Up to 8 LDAP profiles can be created. These profiles would be used with User Management for different purposes in management.

To configure an LDAP profile, click on its index to show the following settings page.



Available settings are explained as follows:

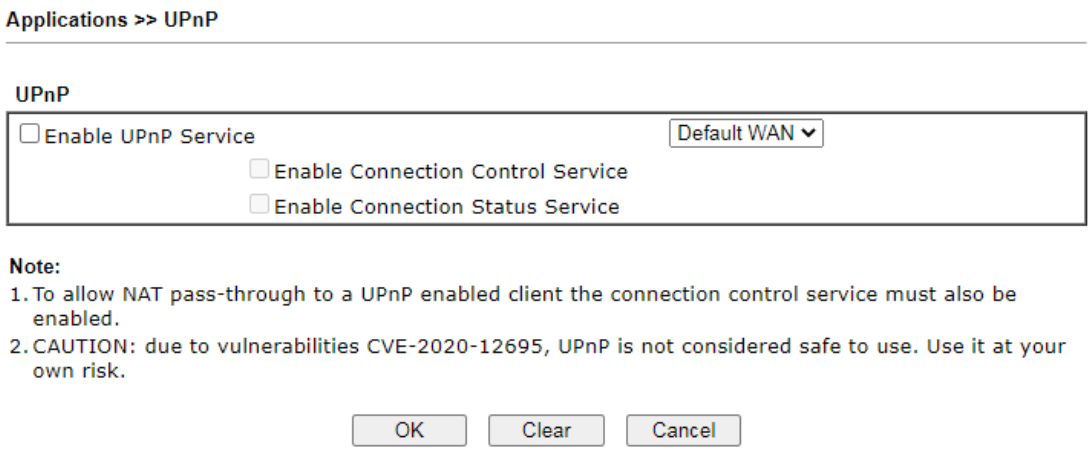
Item	Description
Name	Name that identifies this profile. Maximum length is 19 characters.
Common Name Identifier	The common name attribute, which is typically "cn" in most LDAP configurations.

Base Distinguished Name	The starting point of user search in the LDAP directory, for example, dc=draytek,dc=com. – click this icon to display a list of valid DNs in the LDAP directory.
Additional Filter	Additional filter to be applied to the search request to identify eligible users. For example, – "OpenLDAP: (gidNumber=500)" Here group ID 500 is the group of dial-in users. – "ActiveDirectory: (msNPAllowDialin=TRUE)" The msNPAllowDialin attribute indicates that the user has permission to dial in remotely.
Group Distinguished Name	The base DN of the tree in the LDAP directory that contains groups, for example, ou=groups,dc=draytek,dc=com. - click this icon to display a list of valid DNs in the LDAP directory.

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

II-5-7 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

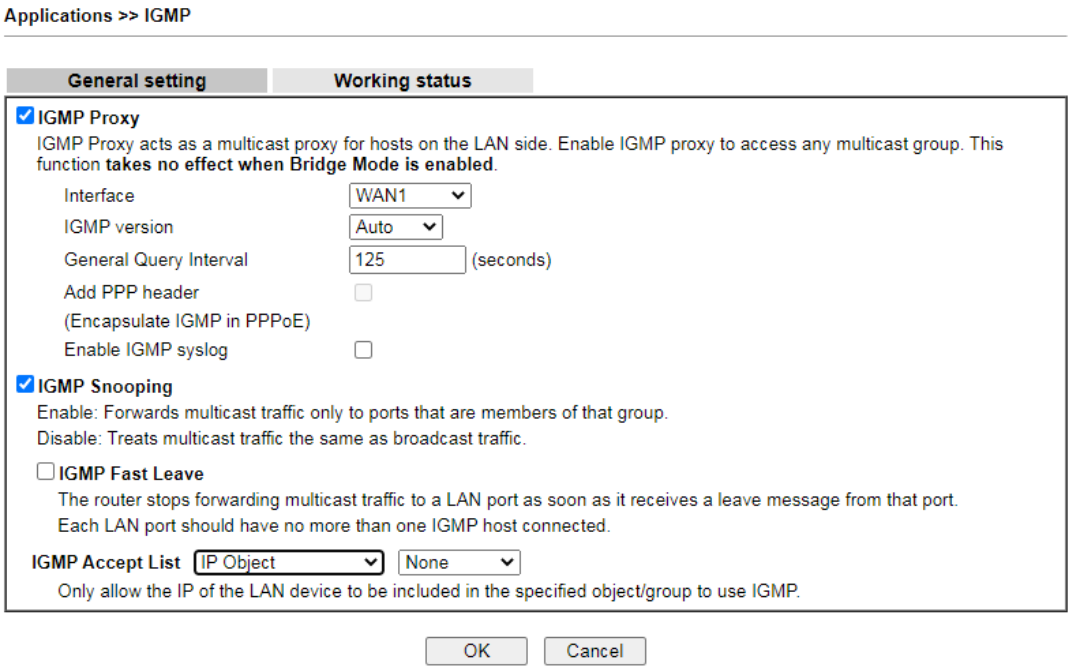
UPnP is required for some applications such as PPS, Skype, eMule...and etc. If you are not familiar with UPnP, it is suggested to turn off this function for security.

II-5-8 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-5-8-1 General Setting



Available settings are explained as follows:

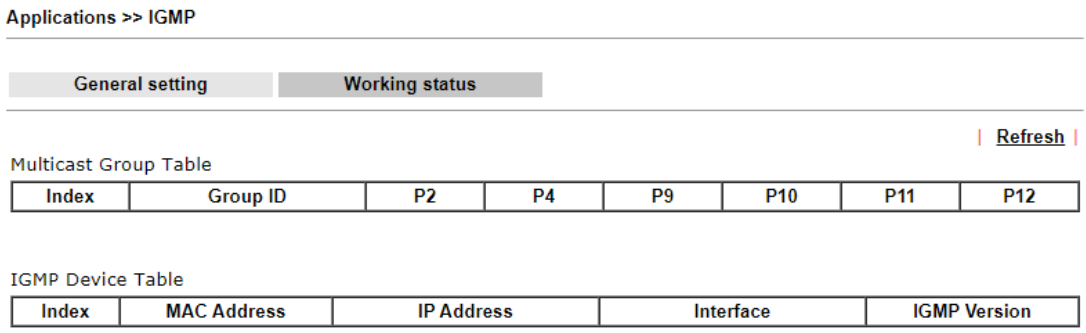
Item	Description
IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode. **Interface** – Specify an interface for packets passing through. **IGMP version** – At present, two versions (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 ontot 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	Select IP Object or IP Group. Only the IP of the LAN device within the IP object / IP group will be allowed to use IGMP.

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

II-5-8-2 Working Status

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.
P2 to P12	LAN ports that have IGMP hosts joined to this multicast group.

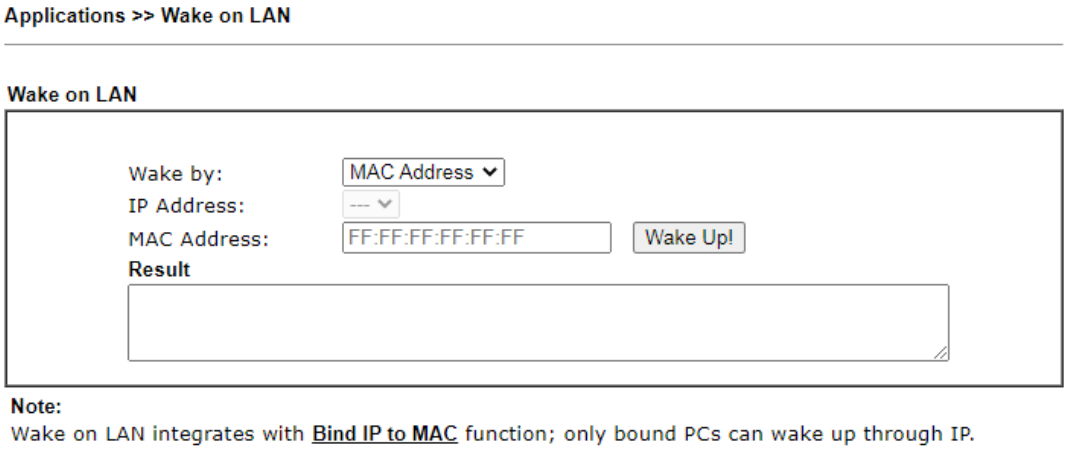
II-5-9 Wake on LAN

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:

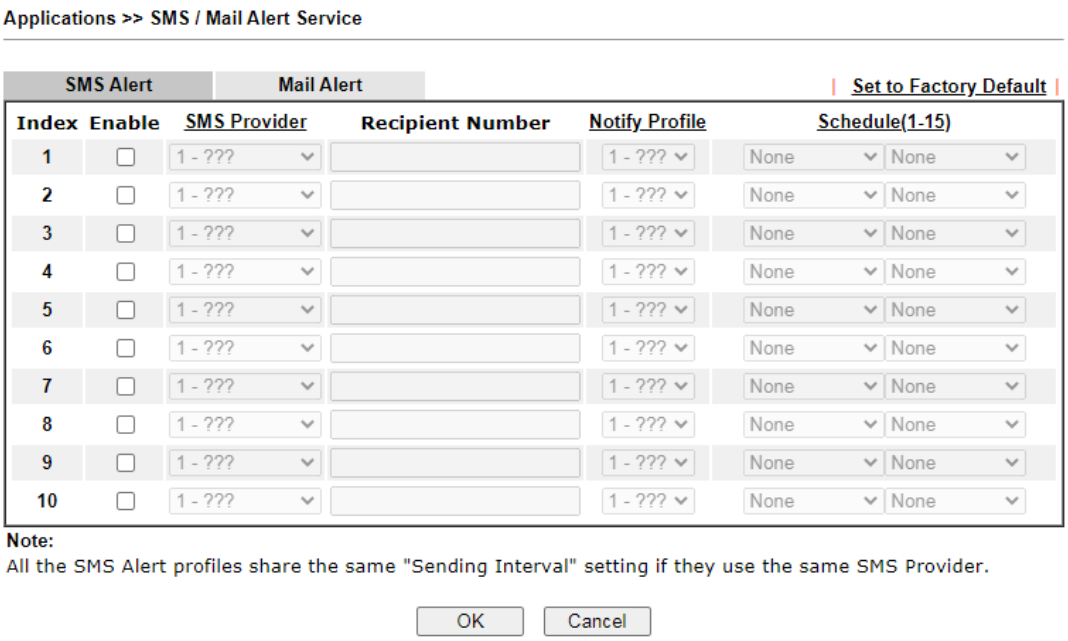
Item	Description
Wake by	The type of address of the LAN client to be woken up. ● If you choose Wake by **MAC Address**, you have to Enter the correct MAC address of the host in MAC Address boxes. ● If you choose Wake by **IP Address**, you have to choose the correct IP address.
IP Address	The IP addresses 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-5-10 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-5-10-1 SMS Alert

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



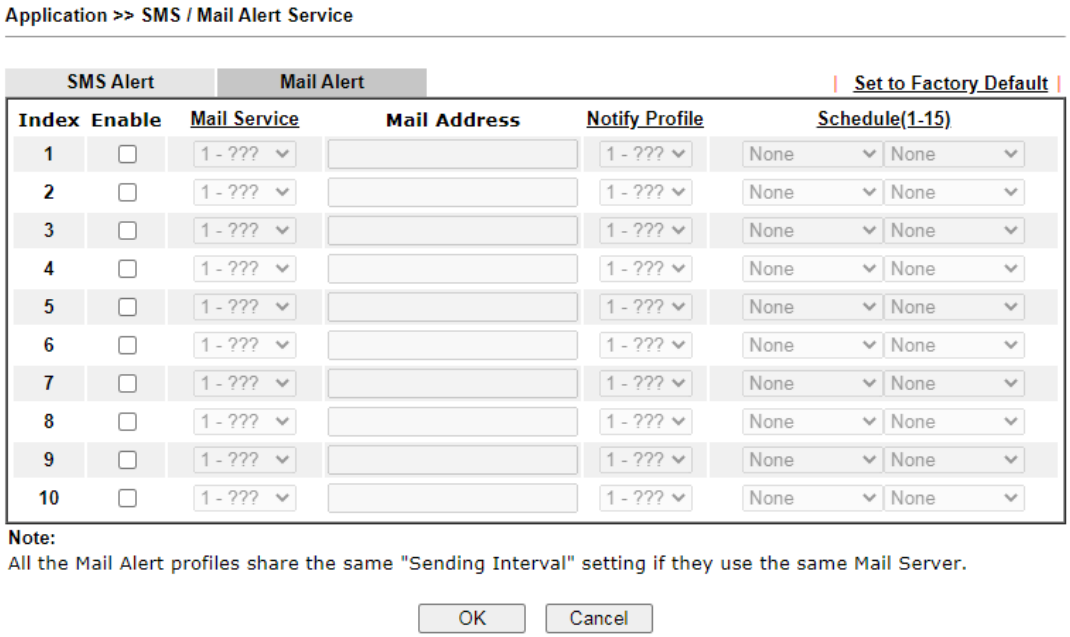
Available settings are explained as follows:

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-5-10-2 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.

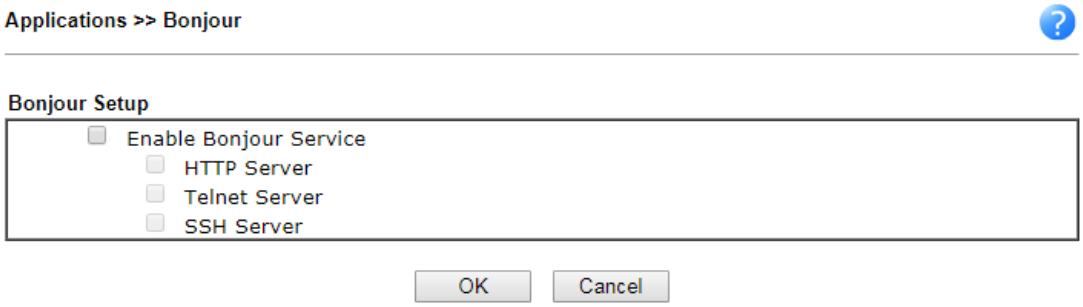
After finishing all the settings here, please click **OK** to save the configuration.

II-5-11 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.

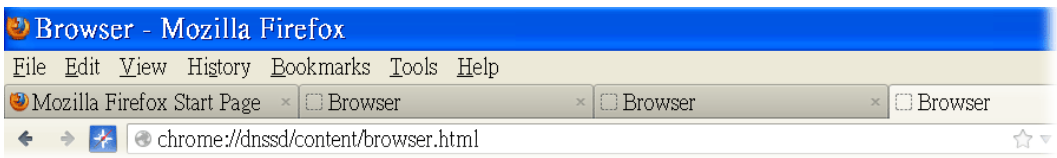


Available settings are explained as follows:

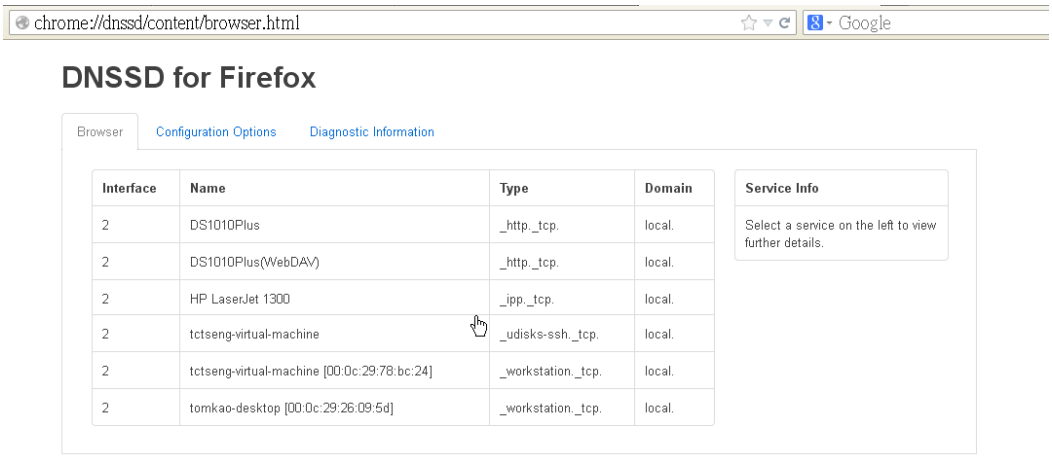
Item	Description
Enable Bonjour Service	Select to enable the Bonjour service on the router. The rest of the checkboxes will be enabled for selection when this checkbox has been selected.
HTTP Server	Select to allow the router's HTTP server to be discovered via Bonjour.
Telnet Server	Select to allow the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

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

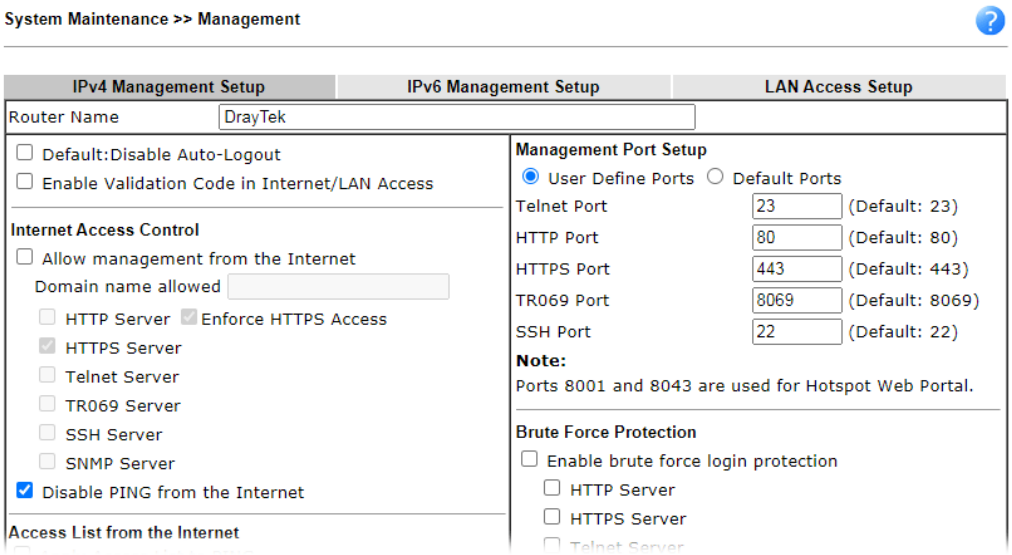
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



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.

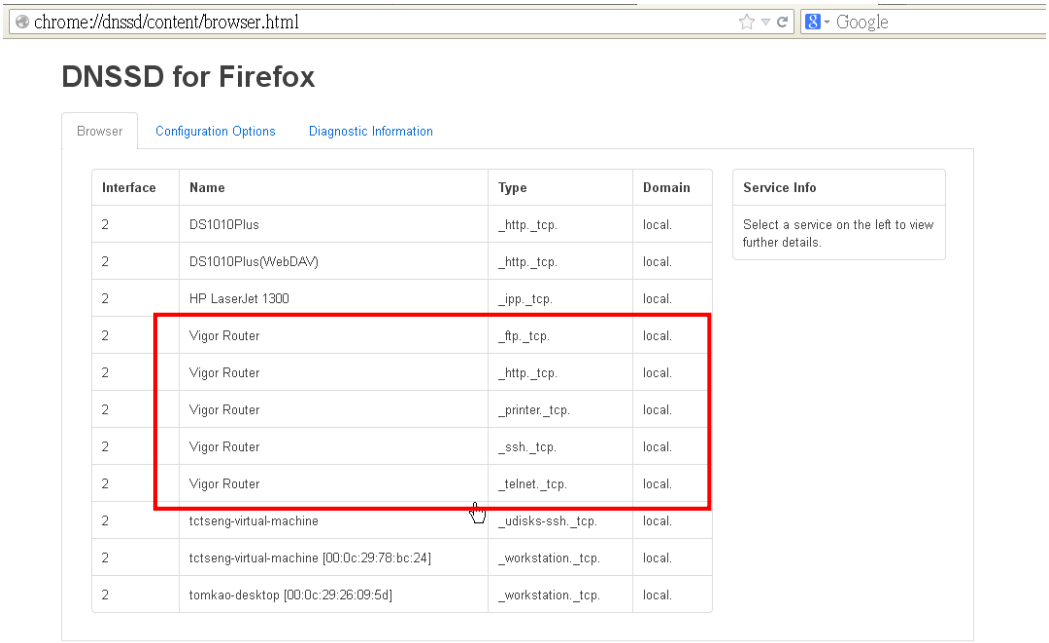


3. Open **System Maintenance>>Management**. Type a name (e.g., DrayTek) as the Router Name and click **OK**.

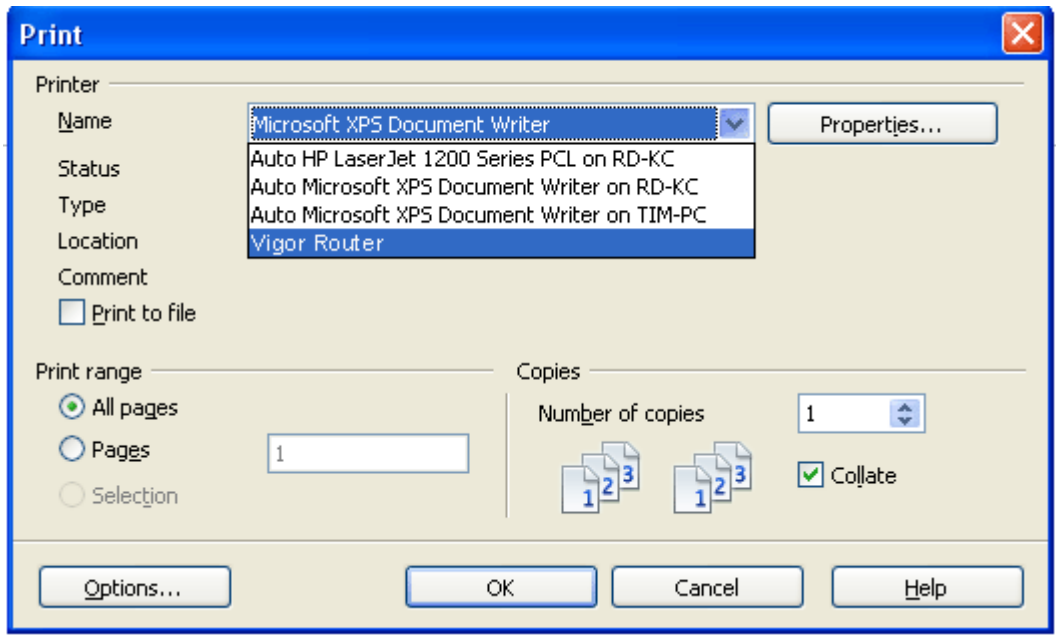


4. Next, open **Applications>>Bonjour**. Check the service that you want to use via Bonjour.

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).



II-5-12 High Availability

The High Availability (HA) feature of the router provides redundancy of network resources, and reduces downtime in case of component failure. The level of sophistication of HA is determined by availability requirements and tolerance of system interruptions. Systems that provide near full-time availability typically have redundant hardware and software.

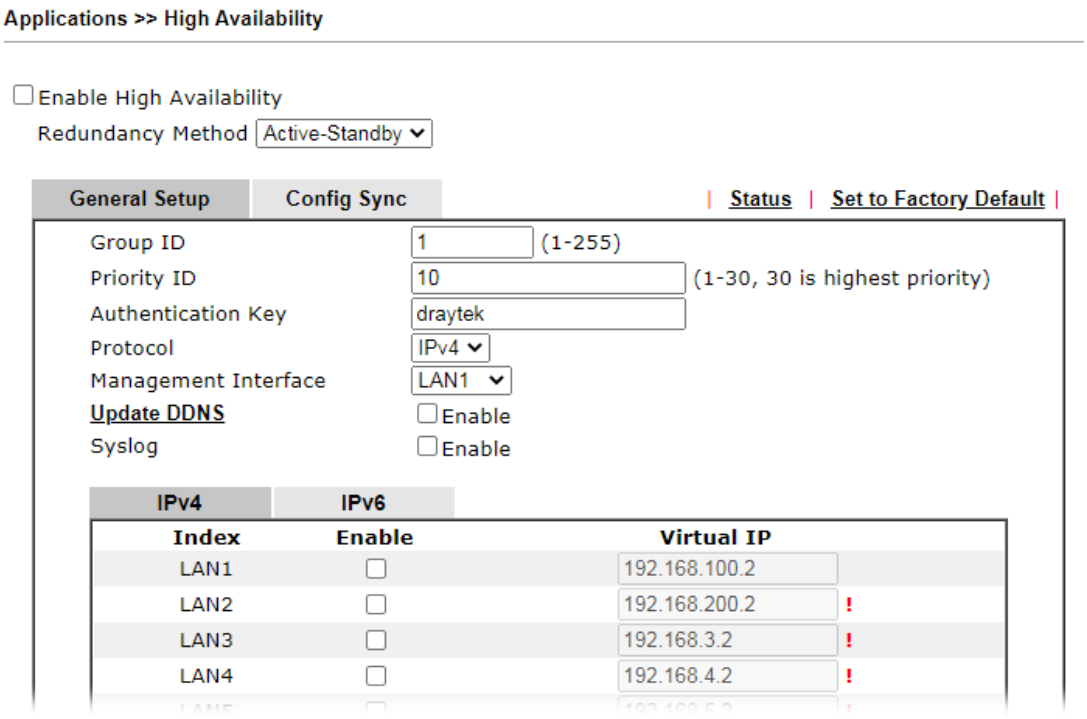
The HA of the Vigor3910 Series is designed to avoid single points-of-failure. When failures occur, the failover process transfers the network load handled by the failed component (the primary router) to the backup component (the secondary router), and the availability of network resources are preserved and partially failed transactions are recovered. In a matter of seconds the system returns to normal operation.

In order to set up High Availability, at least 2 DrayTek routers have to be configured in the following manner:

- Enable High Availability on both the primary and secondary routers.
- Set a high priority ID on the primary router, and a lower priority ID on the secondary router.
- Configure identical redundancy methods, group IDs, and authentication keys on both routers.
- Set the management interface of both routers to the same subnet.
- Enable virtual IP on both routers for each subnet in use. Make sure the virtual IPs are identical on both routers.

II-5-12-1 General Setup

Open **Applications>>High Availability** to bring up the configuration page to configure High Availability.



Available settings are explained as follows:

Item	Description

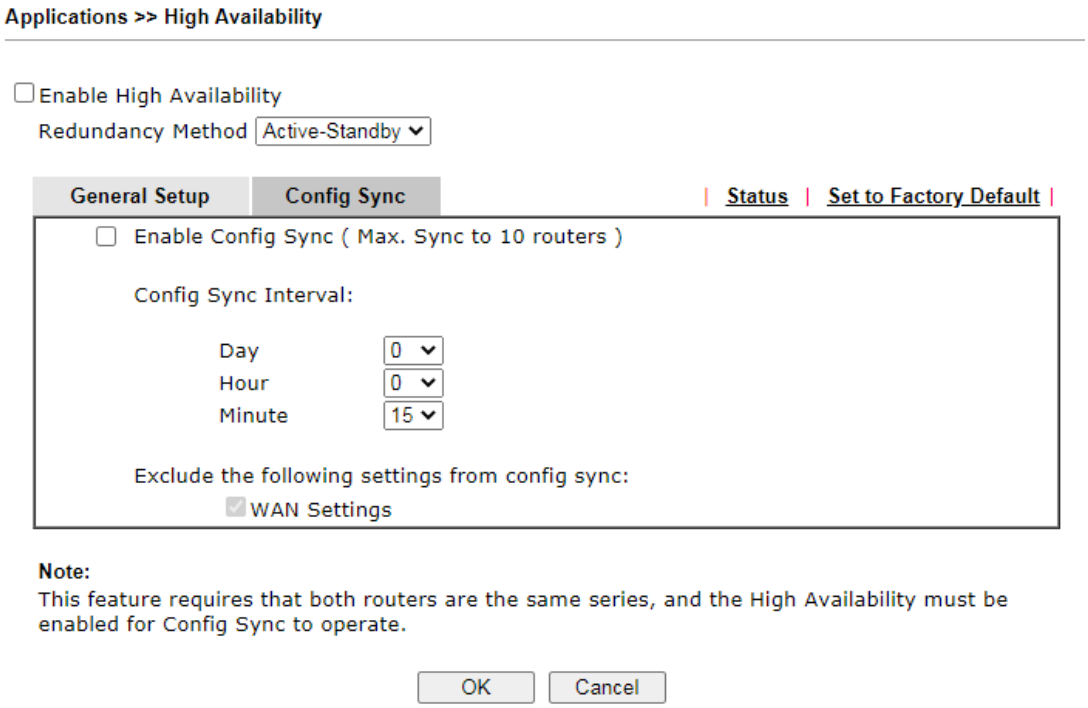
Enable High Abailablity	Select to enable HA function.
Redundancy Method	Select the redundancy method for high availability. **Hot-Standby -** Such method is suitable when there is only one ISP account. When this method is selected, ● During normal operation the secondary router will be idling. When the primary router fails to operate normally, the secondary router(s) will take over. ● WAN settings of the primary and secondary routers are identical. **Note**: When Hot-Standby is used, the wireless LAN function on secondary router will be "disabled" directlly. Clients can not connect to the secondary router any more. **Active-Standby -** This method is suitable when there are multiple simultaneously active ISP connections. When this method is selected, ● All WANs on the secondary routers can be up at the same time. LANs that are not configured under high availability can be routed to secondary routers. ● WAN settings of primary and secondary routers are independently configured. ● Config Sync may be enabled to synchronize most configuration settings between the primary and secondary routers. ● All routers must be set to the same redundancy method.
Group ID	Enter a value (1~255). All routers having the same group ID belong to the same group.
Priority ID	Enter a value (1~30). Different routers must be configured with different IDs. All routers within a group must be assigned a priority ID. Within a group, the router with the largest priority ID (i.e., the highest priority) will be the primary router. When multiple routers in a group are assigned the same priority ID, routers with lower LAN IP addresses (configured on the LAN >> General Setup page) have higher priority.
Authentication Key	Enter an authentication key up to 31 characters long. This is used to encrypt the DARP (DrayTek Address Redundancy Protocol) traffic to guard against malicious attacks.
Protocol	Select the IP protocol to be used for DARP.
Management Interface	Select the interface to be used for DARP negotiation between routers. Only interfaces which are enabled in **LAN>>General Setup** are available for selection. However, LAN1 is always enabled.
Update DDNS	Select **Enable** to update the DDNS server for secondary devices when the primary router fails.
Syslog	Select **Enable** to have syslog record HA activity.
LAN1 ~ LAN50	**Enable –** Check the box to enable the interface.

	Virtual IP - Display the default IP address for each LAN. If rquired, modify the IP address for the LAN port device.

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

II-5-12-2 Config Sync

The synchronization of configuration between high availability routers is configured here.



Available settings are explained as follows:

Item	Description
Enable Config Sync (Max. Sync to 10 routers)	Select to enable configuration synchronization. All routers to be synchronized must have this checkbox selected. Note that config sync can be enabled by **Hot-Standby** redundancy method only.
Config Sync Interval	**Day / Hour / Minute** - The primary router will synchronize its configuration with secondary routers at every specified time interval.
Exclude the following settings from config sync	This setting is available when the Redundancy Method is set to **Hot Standby**. Select the configuration settings to be excluded from synchronization.

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

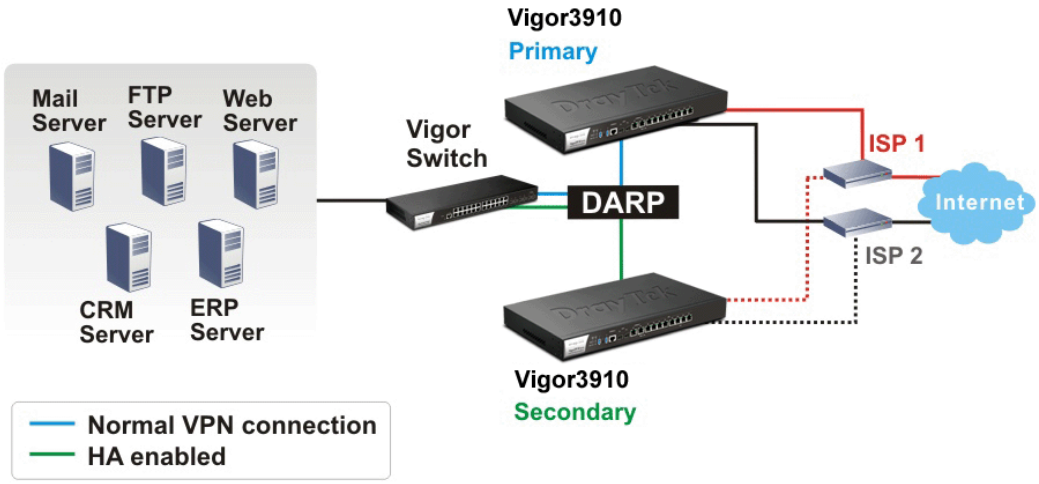
When the configuration method is set to “Hot Standby”, the following settings will not be synchronized:

- WAN (user selectable)
- LAN
- LAN IPv6

- router name
- admin and user passwords.

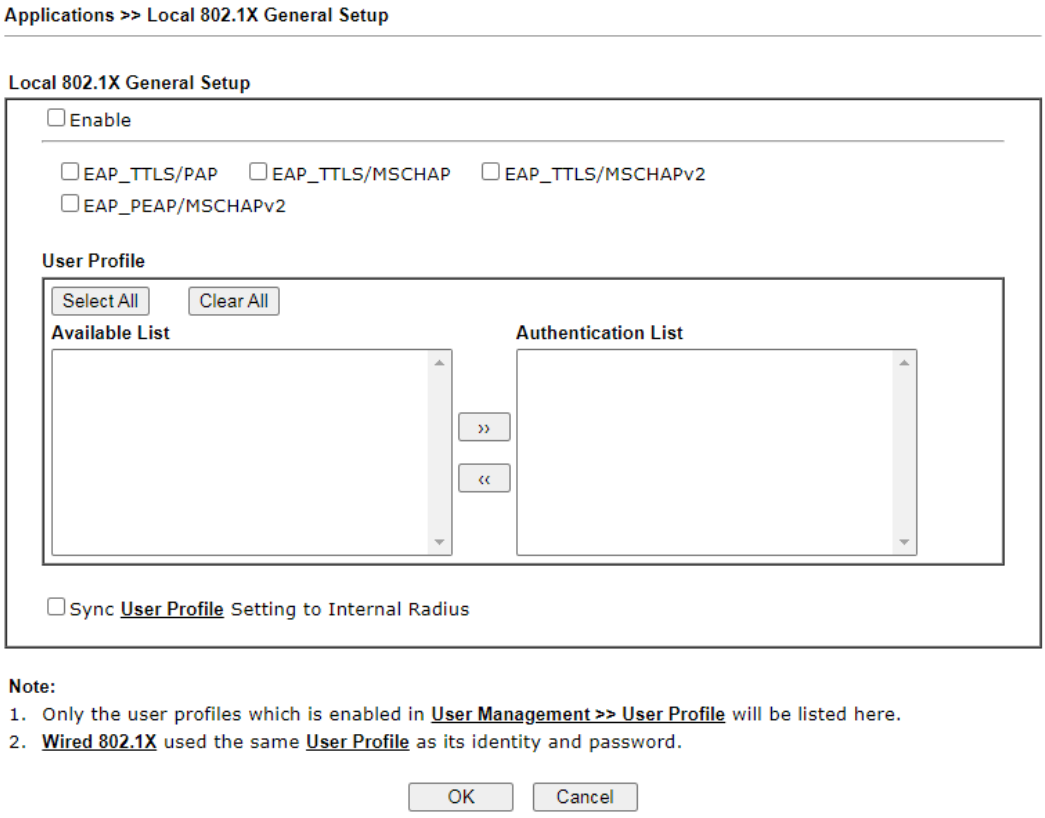
Example:

Take the following picture as an example. The upper Vigor3910 is regarded as primary device, the lower Vigor3910 is regarded as secondary device. When primary Vigor3910 Series is broken down, the secondary device could replace the primary role to take over all jobs as soon as possible. However, once the primary device is working again, the secondary device would be changed to original role to stand by.



II-5-13 Local 802.1X General Setup

You may configure the built-in 802.1X server here. The local 802.X server can be used to authenticate wired and wireless LAN clients.



Available settings are explained as follows:

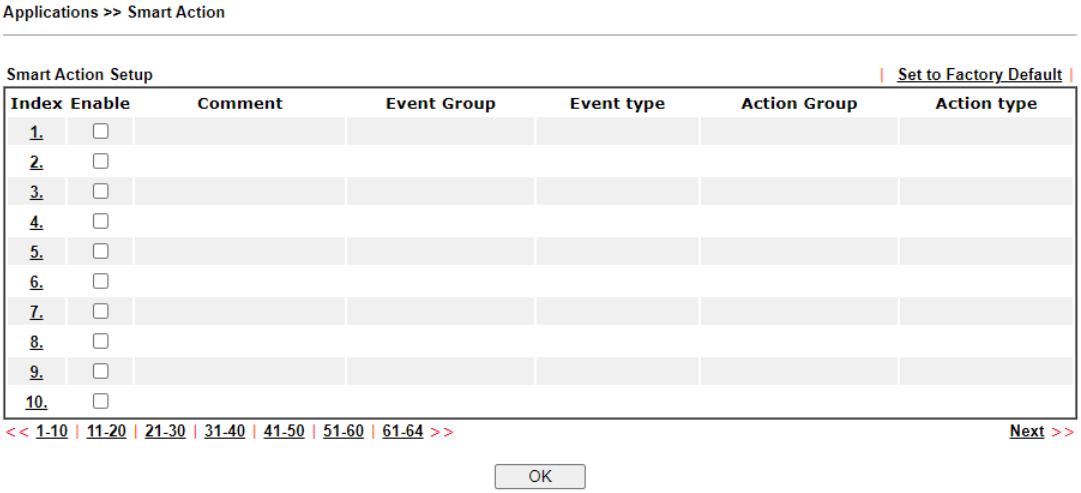
Item	Description
Enable	Select it to enable the built-in 802.1X server. At present, such feature can be used for wireless and wired 802.1x authentication.
User Profile	**Select All** – Click to add all User Profiles to the 802.1X server. All profiles will appear under the Authentication List. **Clear All** – Remove all user profiles from the 802.1X server. All profiles will appear under Available List.
Sync User Profile ….	Make the enabling/disabling setting for both Internal RADIUS and Local 802.1X synchronize for all of the user profiles (**User Management>>User Profile**). For example, if Local 802.1x is configured as Enabled (checked), the Internal RADIUS will be configured as Enabled too. If Local 802.1X is configured as Disabled (unchecked), the

	Internal RADIUS will be changed as Disabled too, even if it is enabled previously.
OK	Click it to save the settings.
Cancel	Click it to give up all settings configuration.

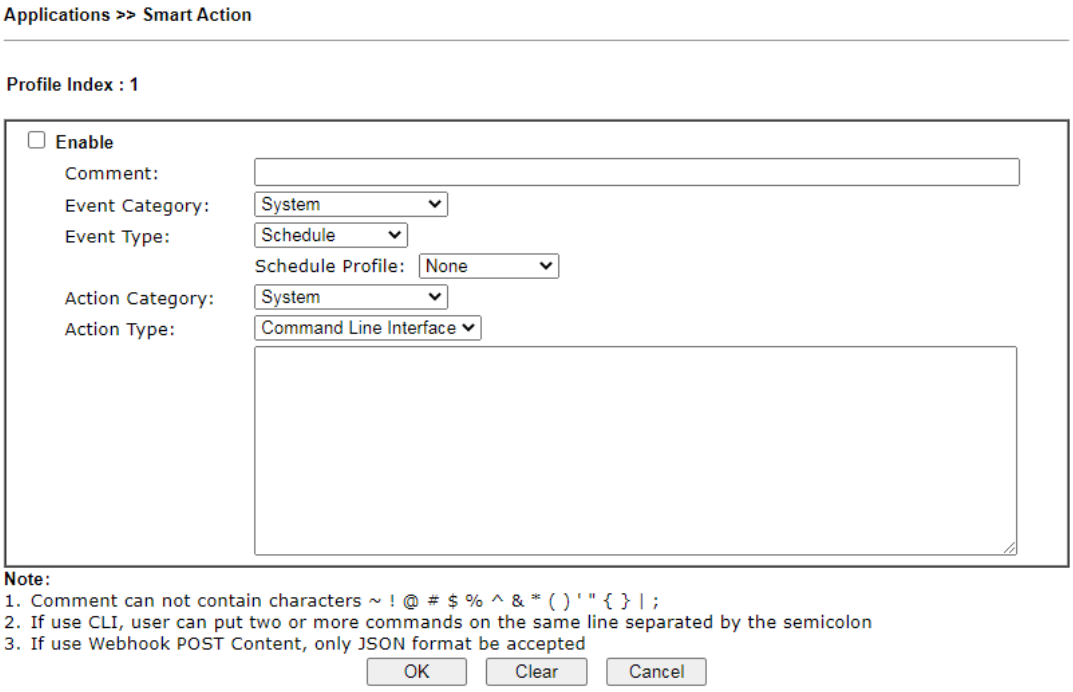
When you finish the configuration, please click **OK** to save and exit this page.

II-5-14 Smart Action

Smart Action allows you to run some tasks (e.g., sending alerts, mails, or removing a VPN profile) automatically at a specified date, a cycle time, or a specified situation. Vigor user can pre-configure up to 64 profiles to manage different tasks.



To configure a profile, click on its index to show the following settings page.



Available settings are explained as follows:

Item	Description
Enable	Select to enable this function.
Comment	Describe the name/focus of this profile.
Event Category	Select an event (e.g., System).
Event Type	Select an event type. **Schedule** - Specify an schedule profile to perform the job based on conditions determined by the action category and

	action type. ● **Schedule Profile** - Use the drop-down list to select a profile. If there is no schedule defined previously, click [Create New] to set a new schedule. **Date and Time** - Set the year, month, day, hour and minute to perform the job. **CPU Usage** - When the usage of the CPU reaches the threshold, a job based on the conditions set below will be performed. ● **Usage threshold** - Select a value. **Memory Usage** - When the usage of the memory reaches the threshold, a job based on the conditions set below will be performed. ● **Usage threshold** - Select a value.
Action Category	Select an action category to set the corresponding action type**.** ● **System** ● **Remote Dial-in User** ● **Lan-to-Lan**
Action Type	Available settings vary based on the selected action category. To perform a CLI or send out an e-mail, select **System** as the Action Category. ● **Command Lint Interface** - Put two or more commands on the same line separated by a semicolon. ● **Mail Alert** -Send an alert mail to a recipient. - **Email Notification Object** - Select an object. - **Recipient** - Enter the e-mail address of the recipient. - **Subject** - Enter the title of the e-mail. To enable, disable or terminate the VPN connection by the remote dial-in user, select **Remote Dial-in User** as the Action Category. ● **Enable Profile** - Enable the remote dial-in user profile. ● **Disable Profile** - Disable the selected remote dial-in user profile. ● **Drop Connection** - Terminate VPN connection for the selected remote dial-in user profile. To enable, disable or terminate the VPN connection by the LAN to LAN profile, select **Lan-to-Lan** as the Action Category, ● **Enable Profile** - Enable the LAN to LAN profile. ● **Disable Profile** - Disable the selected LAN to LAN profile. ● **Drop Connection** - Terminate VPN connection for the selected LAN to LAN profile.

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

Application Notes

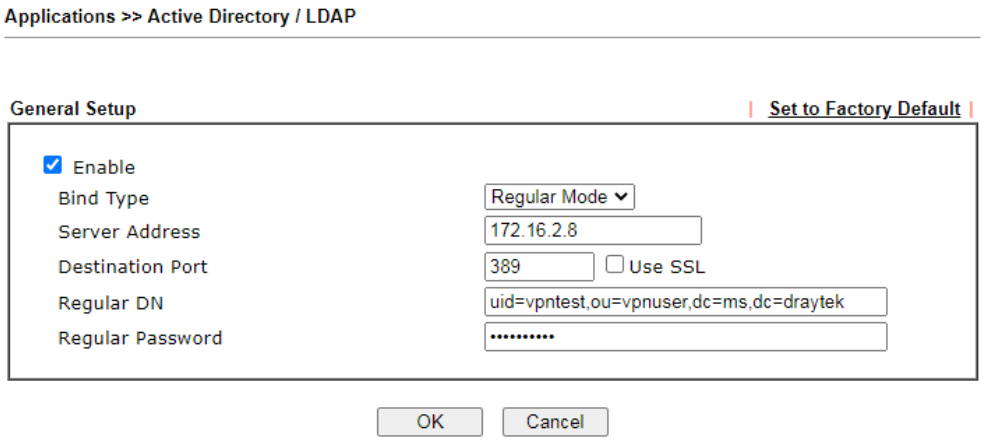
A-1 How to Implement the LDAP/AD Authentication for User Management?

For simplifying the configuration of LDAP authentication for User Access Management, we implement "Group" feature.

There is no need to pre-configure user profile for each user on Vigor router anymore. We only need to configure the Groups DN, then the Vigor router (e.g., Vigor 2860 series) can pass the authentication to LDAP server with the pre-defined Group path.

Below shows the configuration steps:

1. Access into the web user interface of the Vigor router.
2. Open **Applications>>Active Directory /LDAP** to get the following page for configuring LDAP related settings.

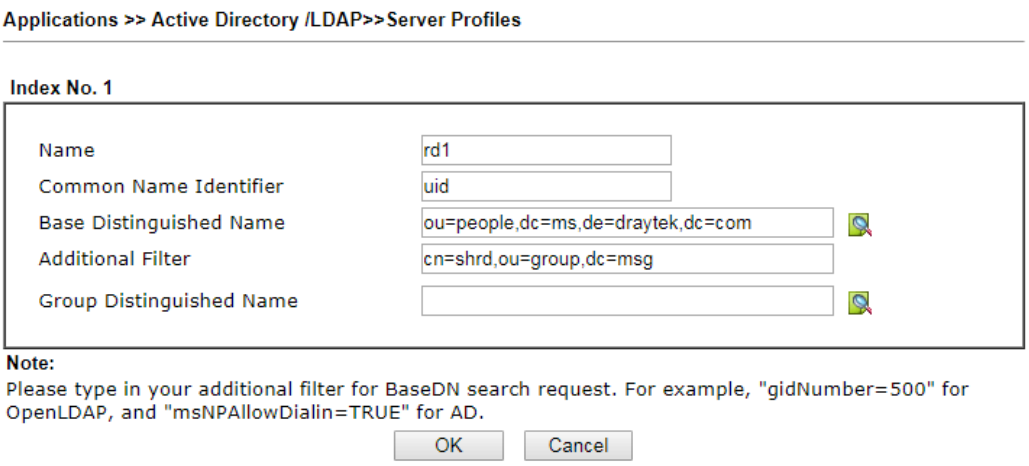


There are three types of bind type supported:

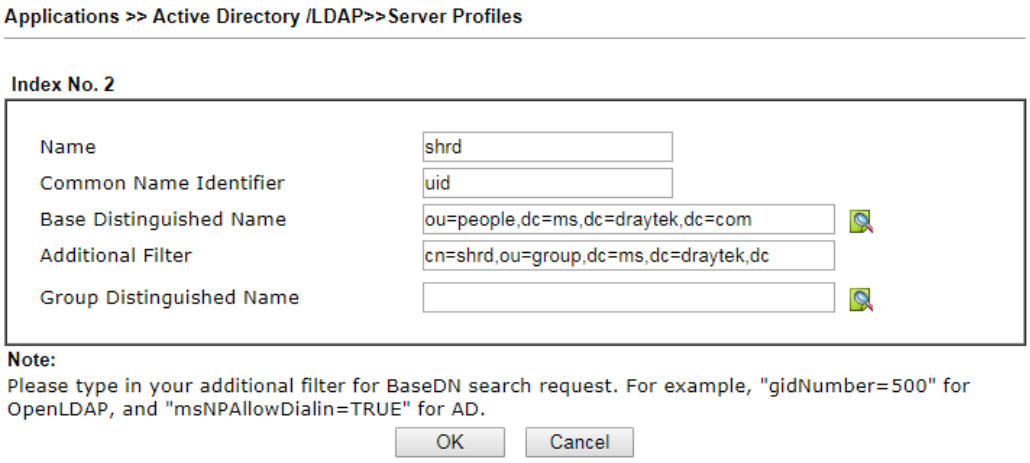
- **Simple Mode** – Just simply do the bind authentication without any search action.
- **Anonymous** – Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode**– Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority.
  For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.

3. Create LDAP server profiles. Click the **Active Directory /LDAP** tab to open the profile web page and click any one of the index number link.

   If we have two groups "**RD1**" and "**SHRD**" on LDAP server, we can configure two LDAP server profiles with different Group Distinguished Name.

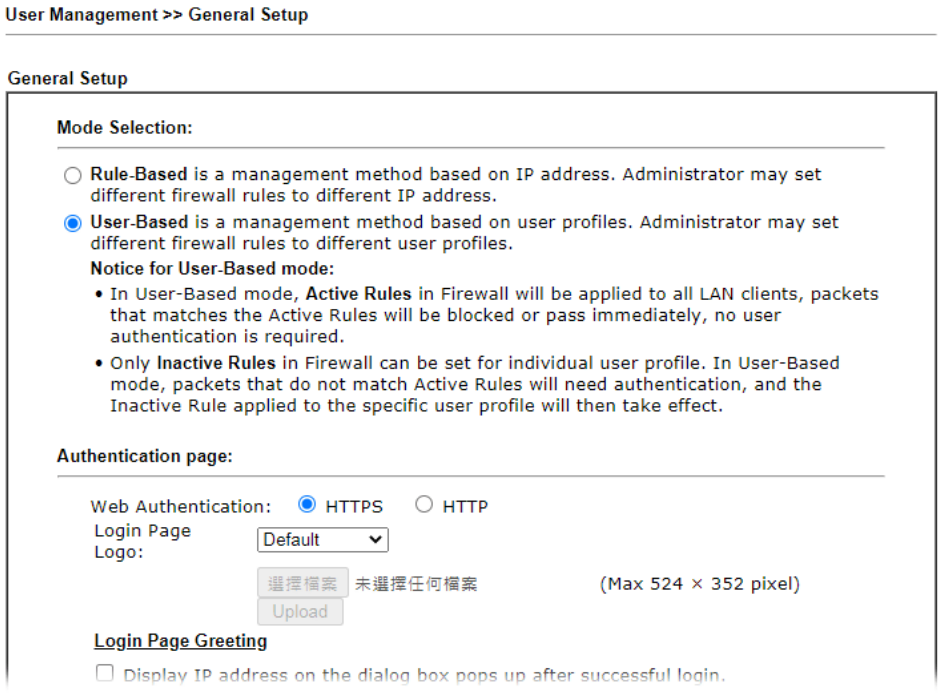


and

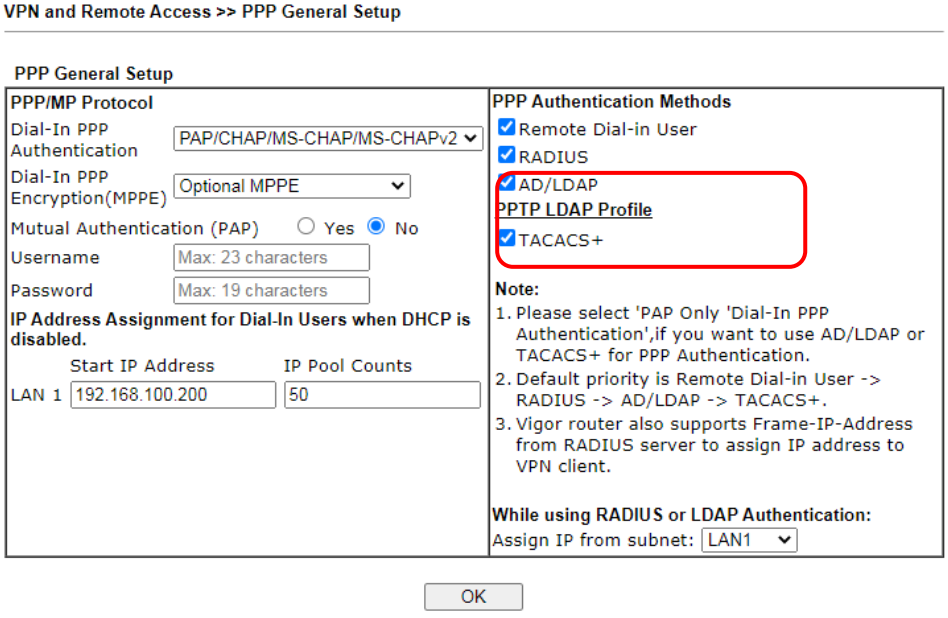


4. Click **OK** to save the settings above.

5. Open **User Management>>General Setup.** Select **User-Based** as the **Mode** option.



6. Then open **VPN and Remote Access>>PPP General Setup** to **check** the profile(s) that will be authenticated with LDAP server.



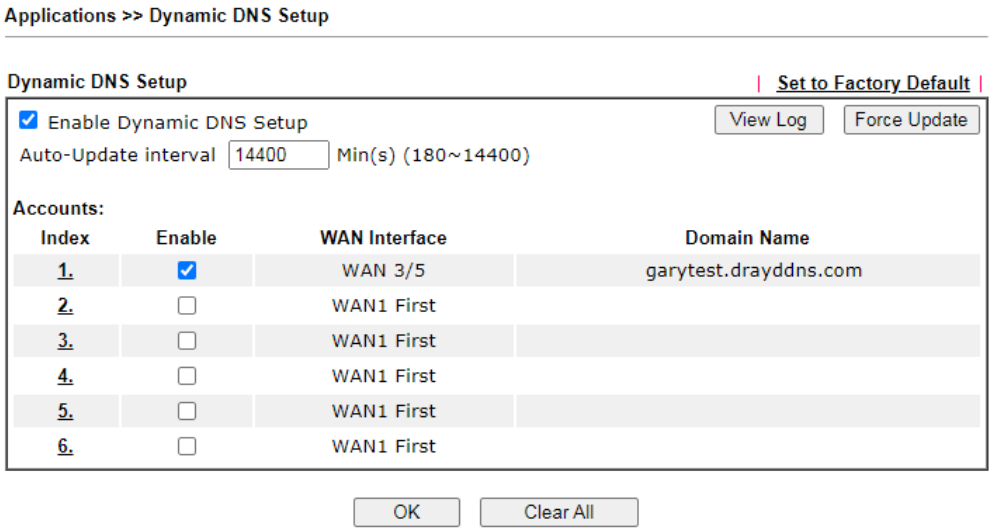
After above configurations, users belong to either “rd1” or “shrd” group can access Internet after inputting their credentials on LDAP server.

A-2 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.

Set up DrayDDNS on DrayOS Router

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

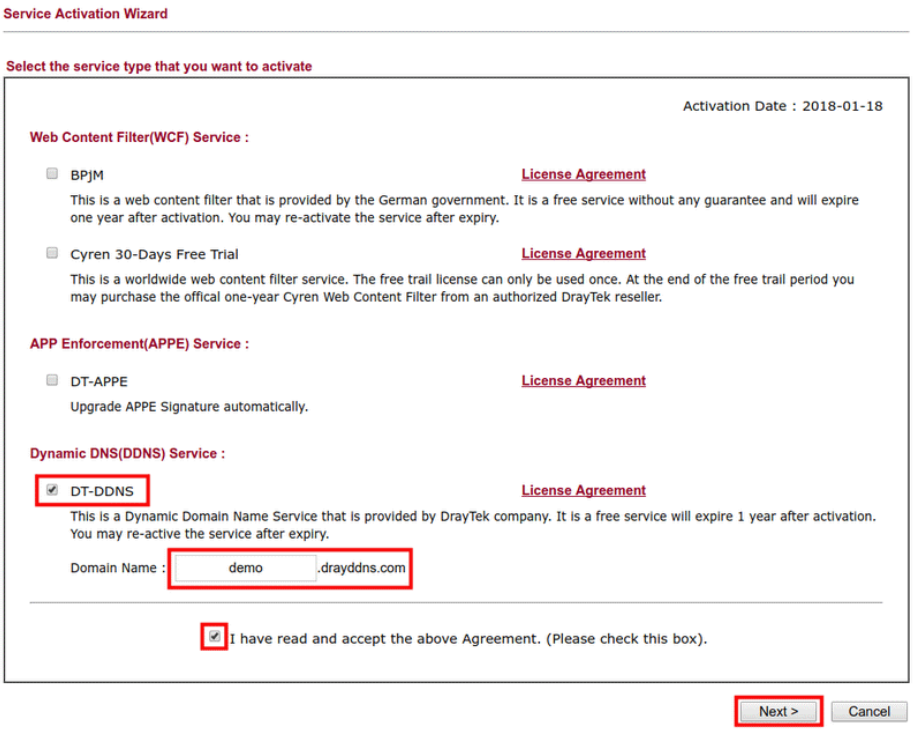


2. Go to **Wizards >> Service Activation Wizard** page, wait for the router to connect to MyVigor server, then:

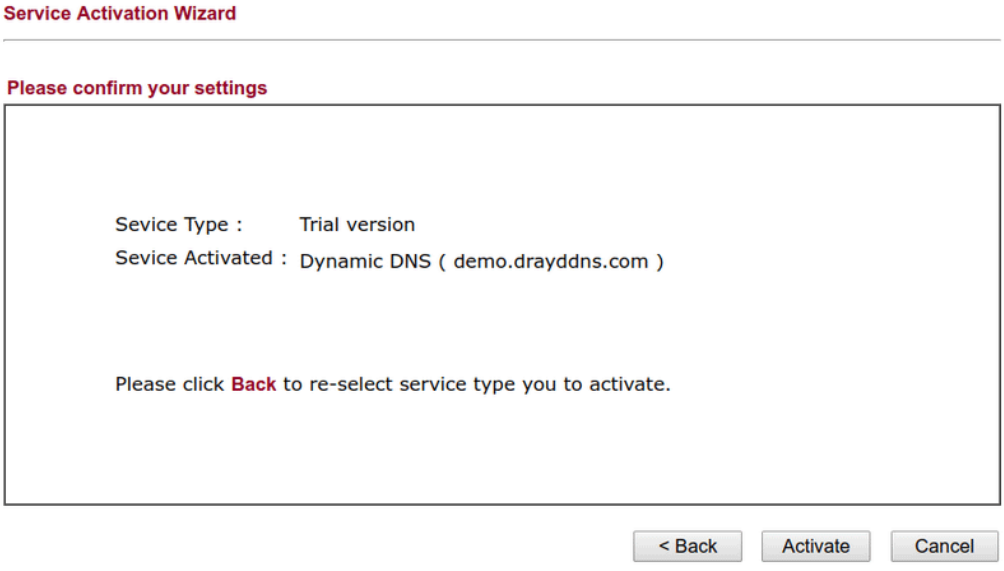
   (a) Select **DT-DDNS**.

   (b) Enter the desired Domain Name.

   (c) Make sure you have read the License Agreement. Check **I have read and accept the above Agreement**, then click **Next**.



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



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

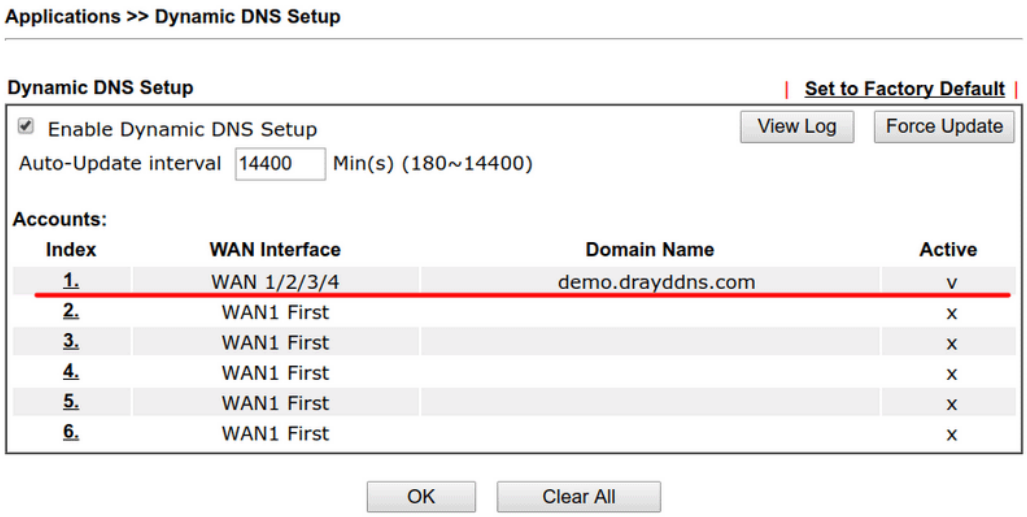
DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	---	---	Not Activated
APP Enforcement	---	---	Not Activated
DDNS	2018-01-18	2019-01-18	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.

Copyright © DrayTek Corp. All Rights Reserved.

5. Vigor router will contact with MyVigor server, then get the DrayDDNS license as well as the domain name back, and create the DDNS profile automatically. Please go to **Applications >> Dynamic DNS Setup** page to make sure the router has created the DDNS profile.

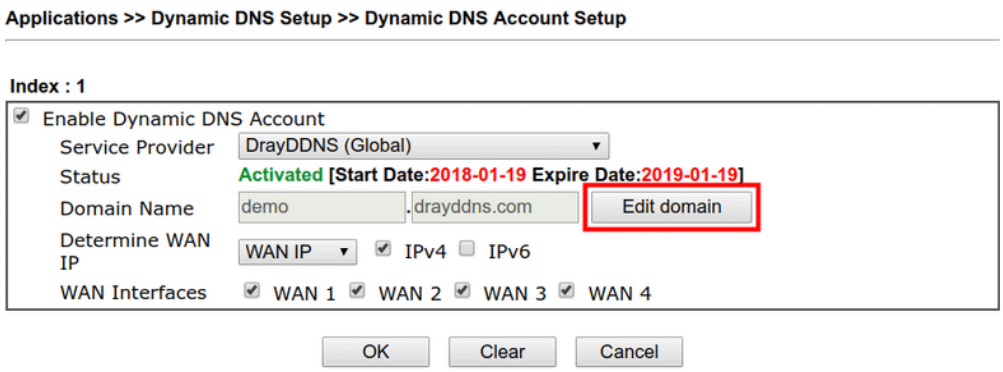


Note that, if your router does not get the domain after you activating the license, it may due to the router does not trigger the process, which to connect and get the license from MyVigor server. You may reboot the router to trigger the process.

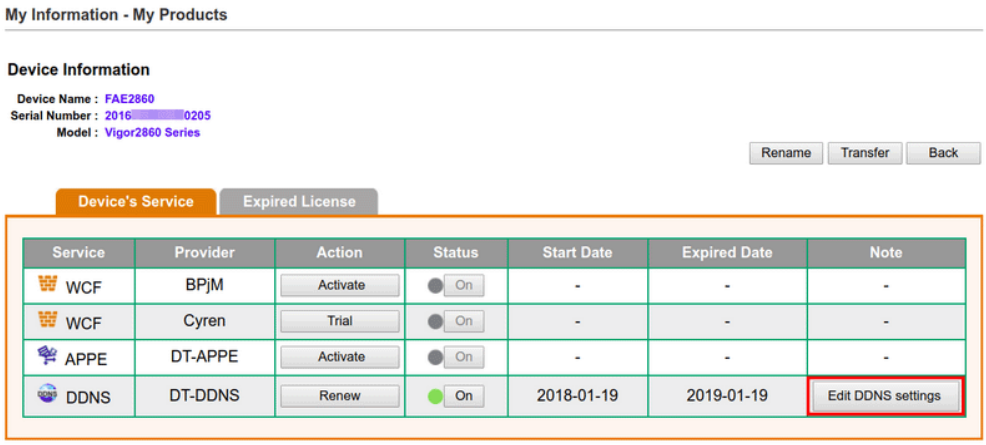
Modify DrayDDNS Domain Name

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.

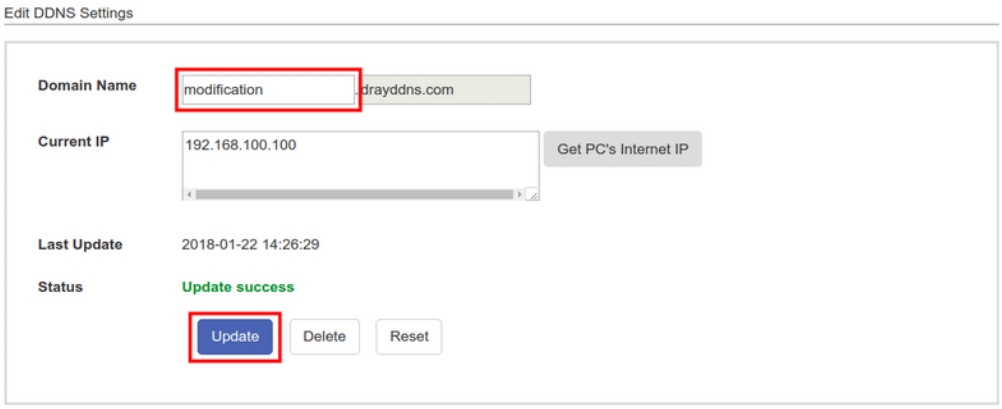
1. Please visit https://myvigor.draytek.com/ or go to **Applications >> Dynamic DNS Setup >> DrayDDNS** profile and click **Edit domain**.



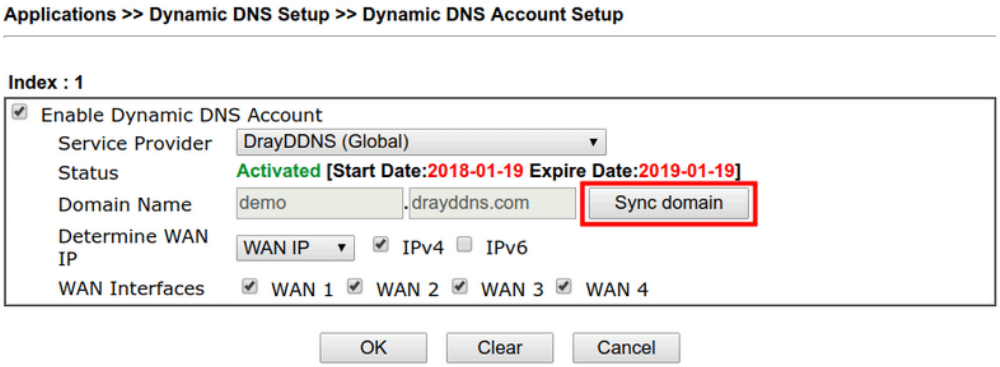
2. Log in to MyVigor Website, choose the profile, then click **Edit DDNS settings**.



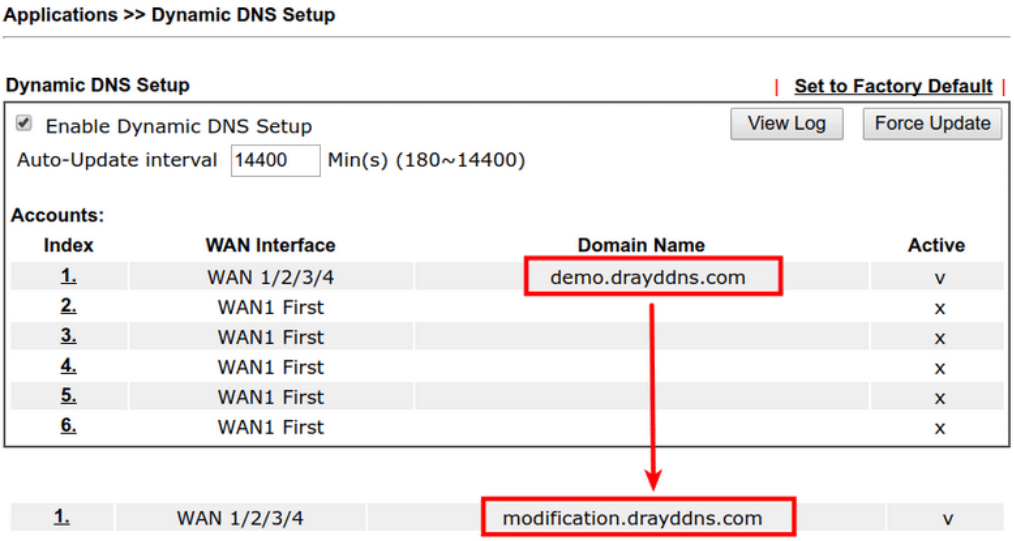
3. Input the desired **Domain name** and click **Update.**



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.



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



II-6 Routing

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

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

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

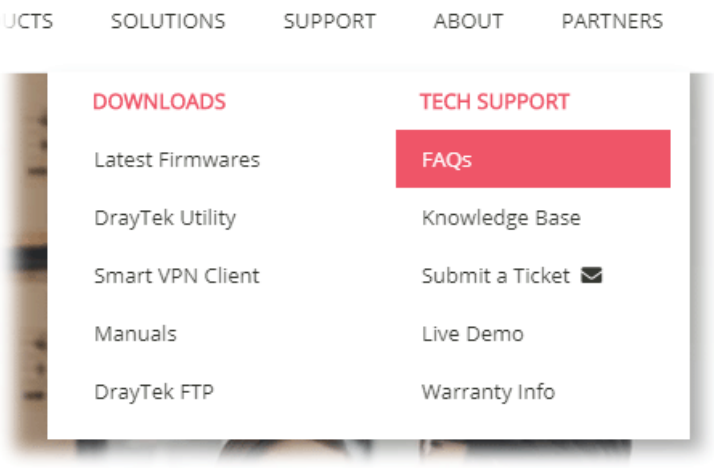
Packets will be sent through another Interface or follow another Policy when the original interface goes down (**Failover to**). Once the original interface resumes service (**Failback**), the packets will be returned to it immediately.

Other routing

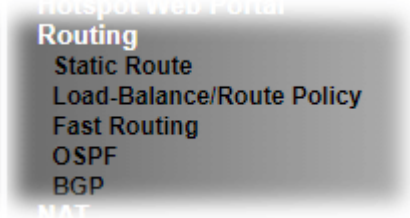
Specify routing policy to determine the direction of the data transmission.

Info

For more detailed information about using policy route, refer to SUPPORT >> TECH SUPPORT >>FAQs on www.draytek.com.



Web User Interface

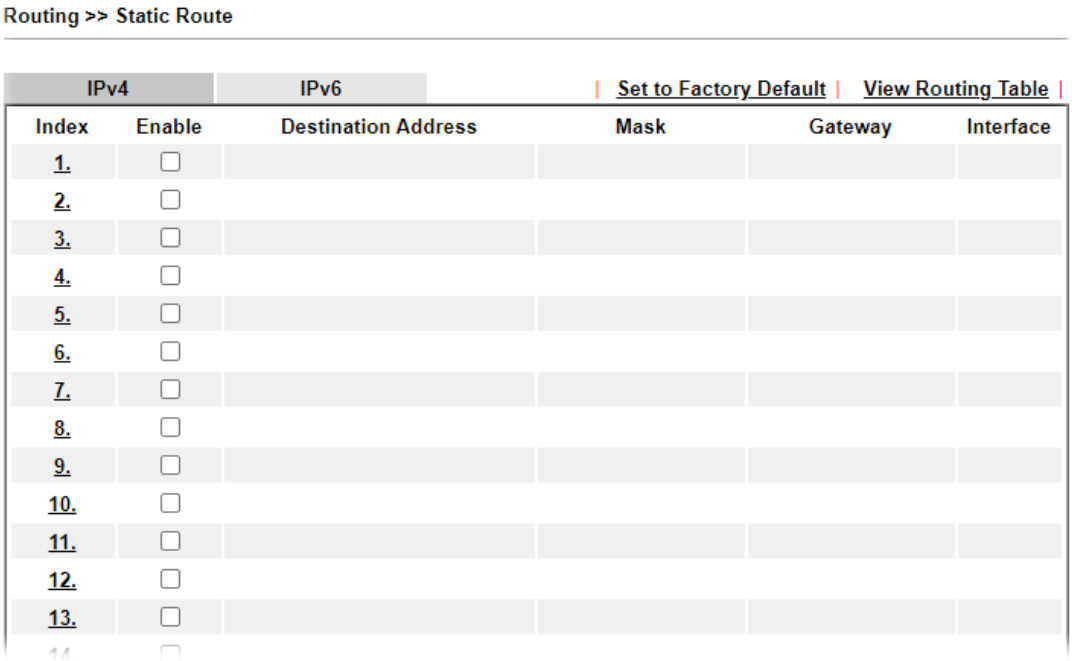


II-6-1 Static Route

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

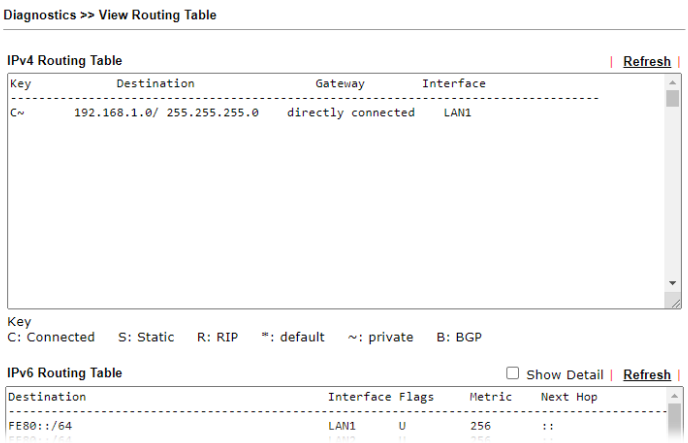
The Static Route Setup screen has separate tabs for IPv4 and IPv6. Select the appropriate tab to begin.

II-6-1-1 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.

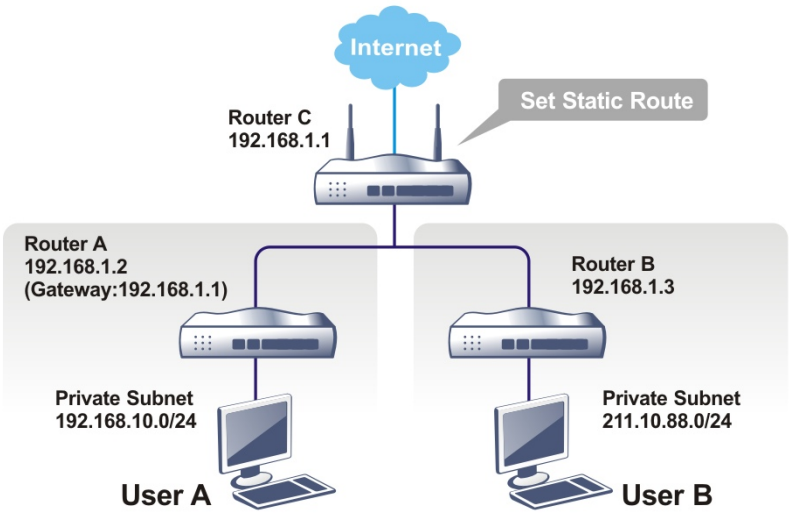
Viewing Routing Table	Displays the routing table for your reference. 
Index	The number (1 to 300) under Index allows you to open next page to set up static route.
Enable	Enables or disables the static route.
Destination Address	Beginning destination address.
Mask	Subnet mask of the destination address.
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.

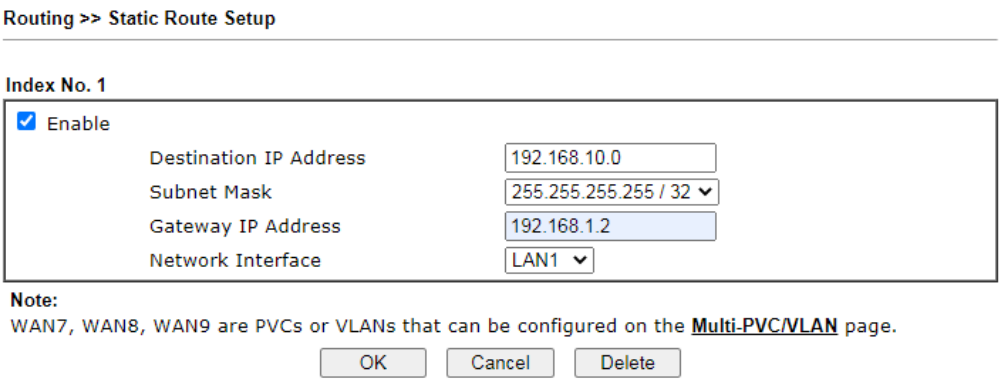


1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

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**.

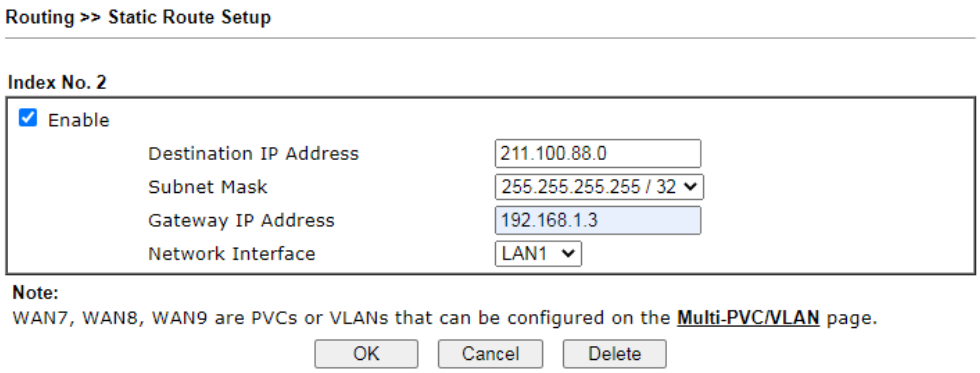


Available settings are explained as follows:

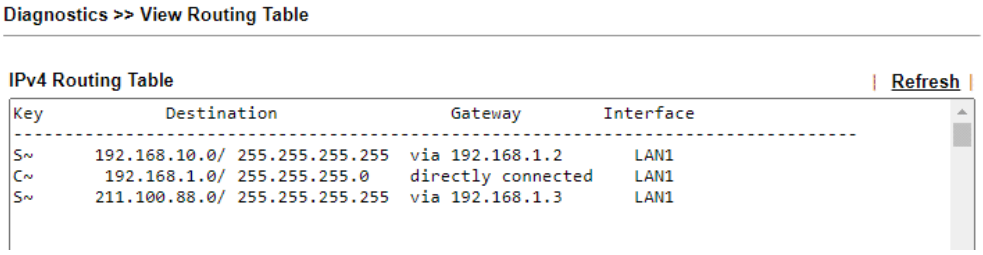
Item	Description
Enable	Enables or disables the static route.
Destination IP Address	Beginning destination address. Enter an IP address as the destination of the static route.
Subnet Mask	Subnet mask of the destination address. Enter the subnet mask for the static route.

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**.

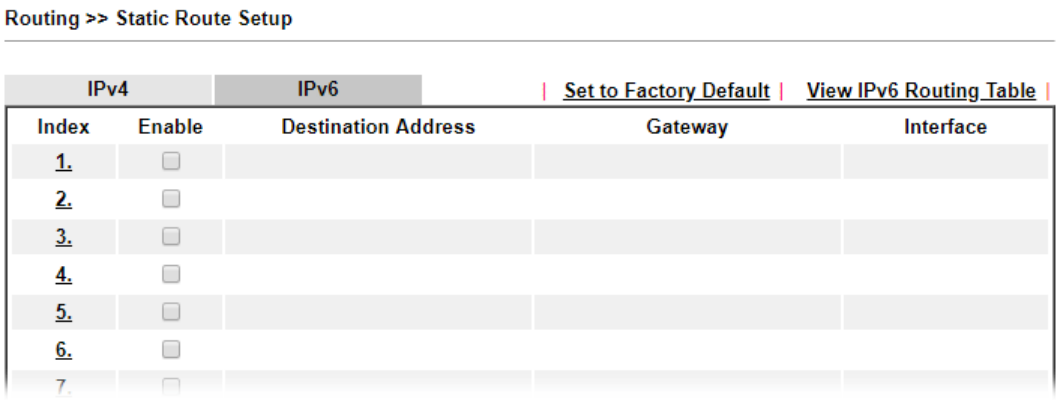


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



II-6-1-2 Static Route for IPv6

You can set up to 300 profiles for IPv6 static route. Click on a route index on the IPv6 tab to configure an IPv6 static route.

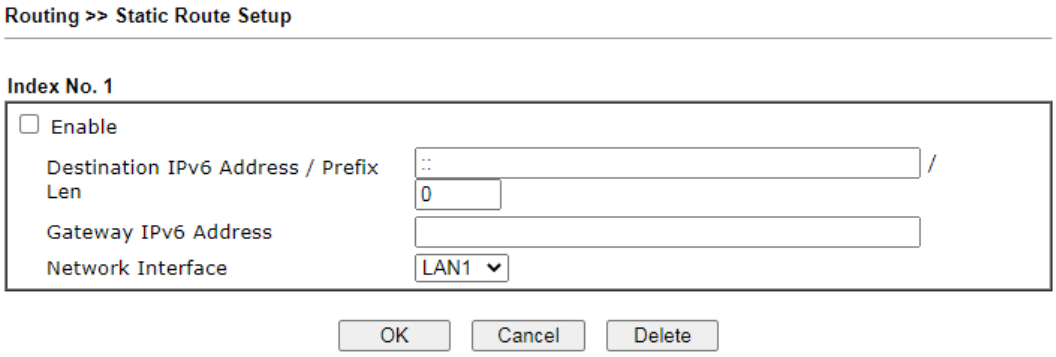


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.

Viewing IPv6 Routing Table	Displays the routing table for your reference.
Index	The number (1 to 300) 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.

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.

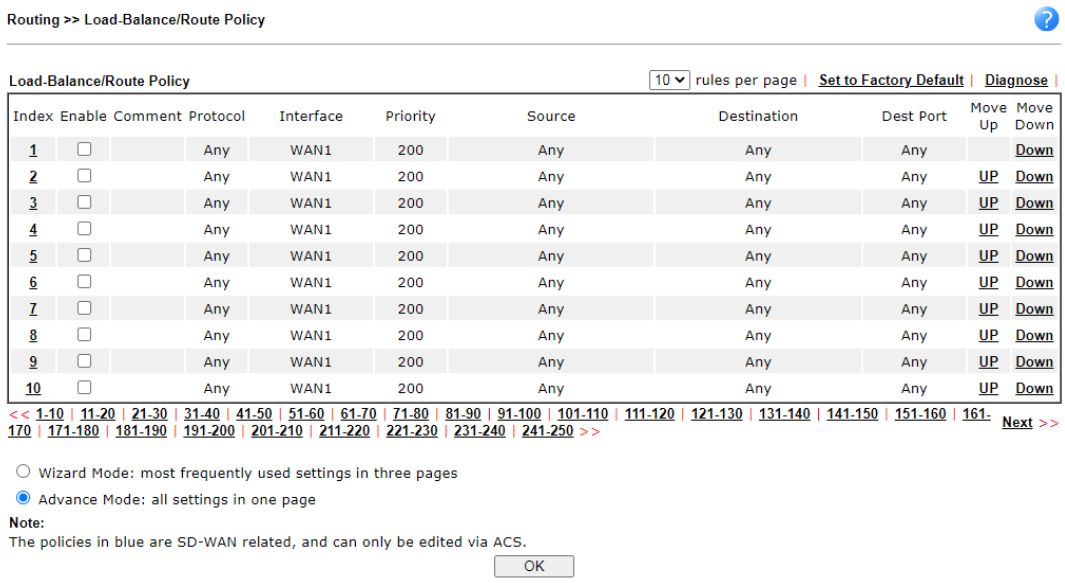
When you finish the configuration, please click **OK** to save and exit this page.

II-6-2 Load-Balance /Route Policy

The Load-Balance/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 Load-Balance/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.

II-6-2-1 General Setup

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



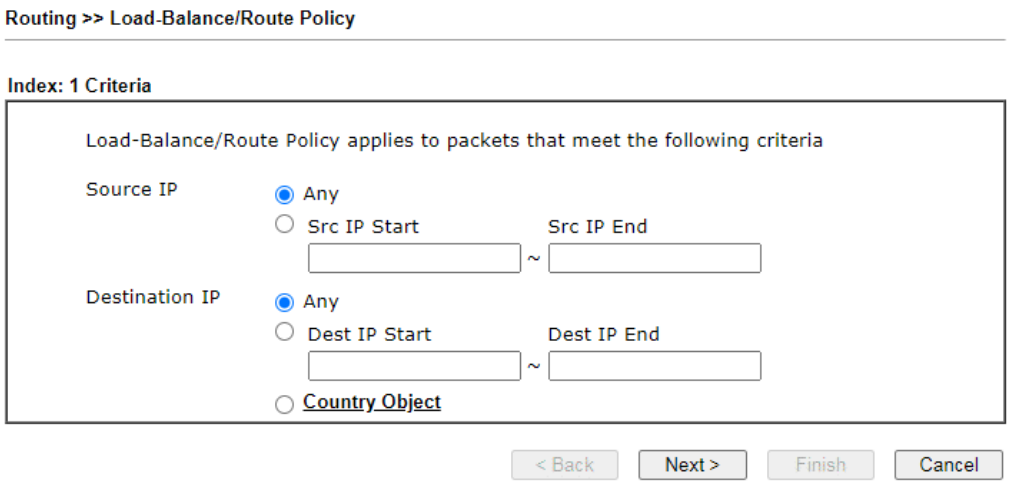
Available settings are explained as follows:

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 addresses.
Destination	The beginning and ending destination IP addresses.
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.

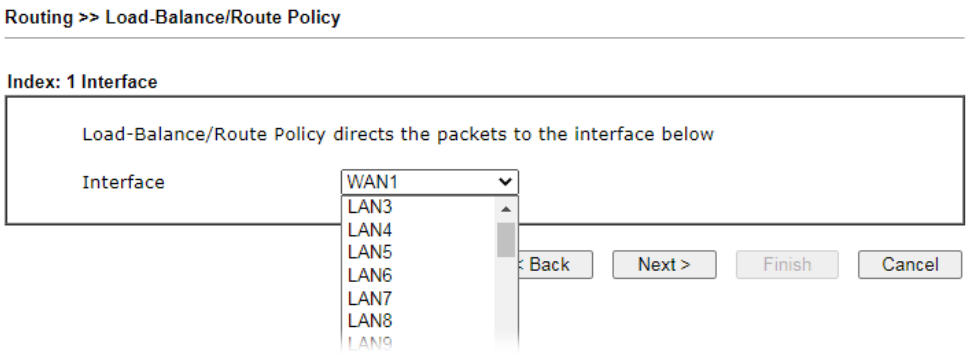
1. Click the **Wizard Mode** radio button.
2. Click **Index 1**. The setting page will appear as follows:



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, and IP Routed 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:

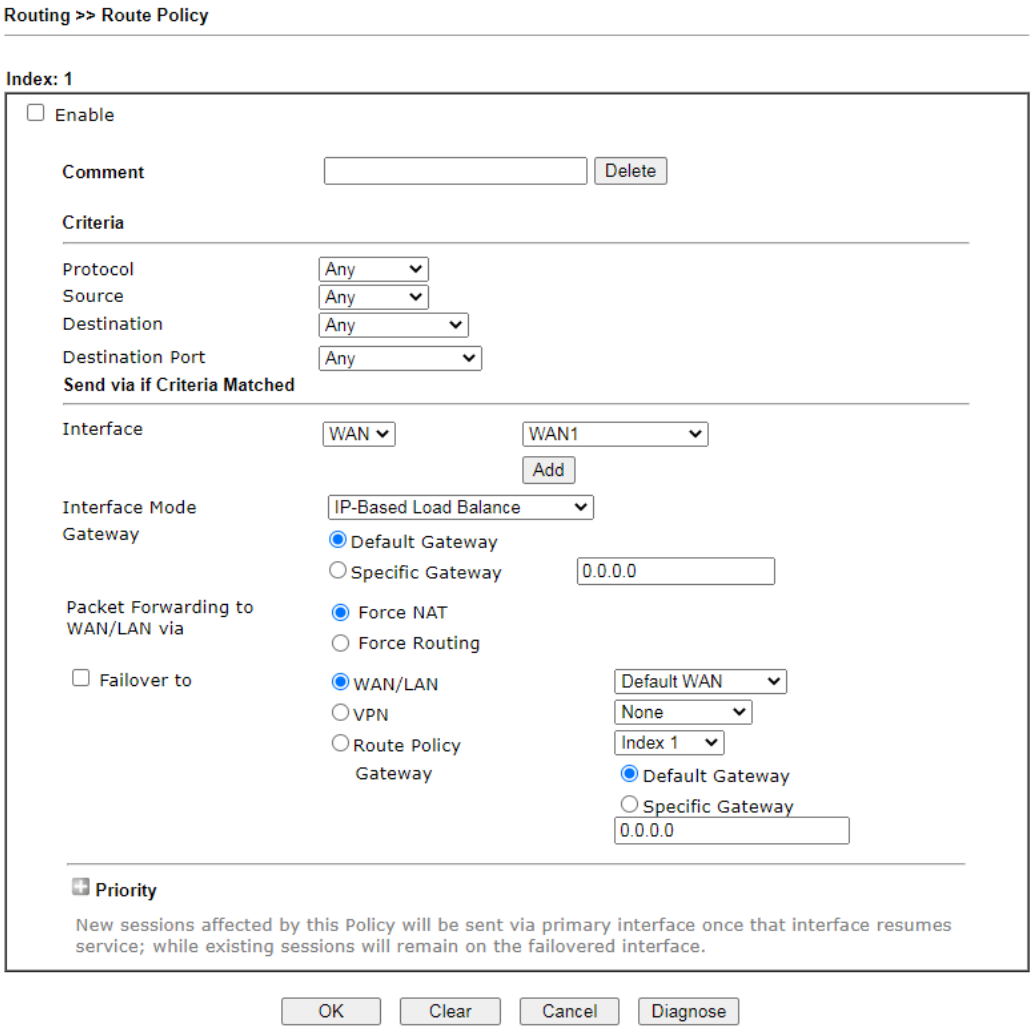
Item	Description
Force NAT /Force Routing	It determines which mechanism that the router will use to forward the packet to WAN.

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 2** to access into the following page.



Available settings are explained as follows:

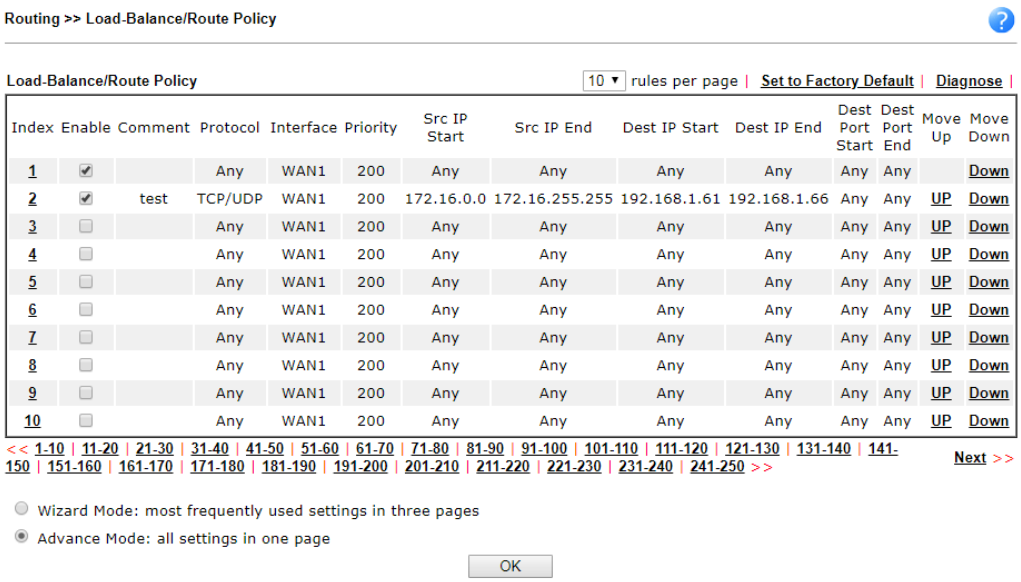
Item	Description
Enable	Select to enable rule and unlock all fields for configuration.
Comment	Type a brief explanation for such profile.
Criteria	Router examines outgoing LAN traffic to find the first rule whose criteria are satisfied. **Protocol -** Use the drop-down menu to choose a proper protocol 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). **Interface Mode** - It is available if WAN is selected as the Interface. ● **IP Based Load Balance** - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.

	• **Session Based Load Balance** - All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP. If you have no strong demand about speed test result, keep default settings as IP based. **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** – 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

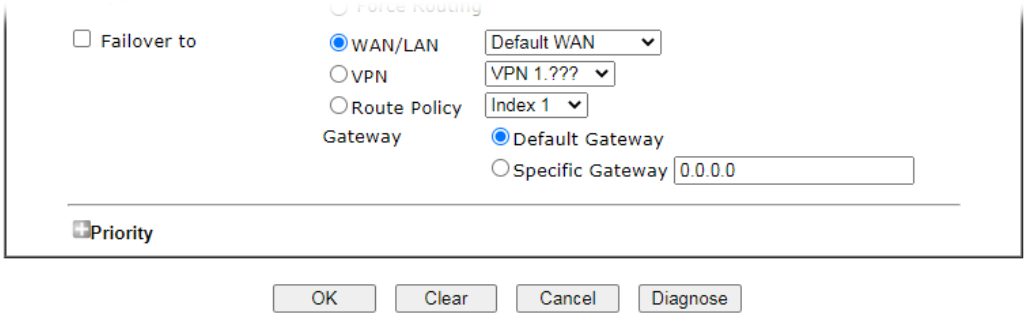
	value.

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



II-6-2-2 Diagnose for Route Policy

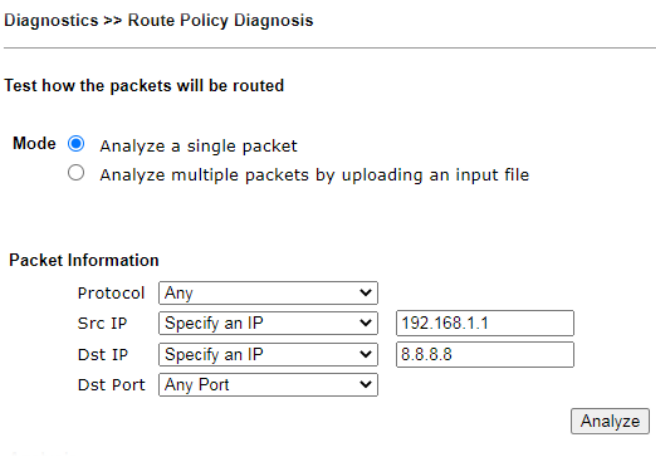
The Diagnose function allows you to determine how a specific type of traffic from a host to a destination will be routed, and which routes, route policies and load balance rules match the criteria of the traffic.



Click **Diagnose**.

Analyze a single packet

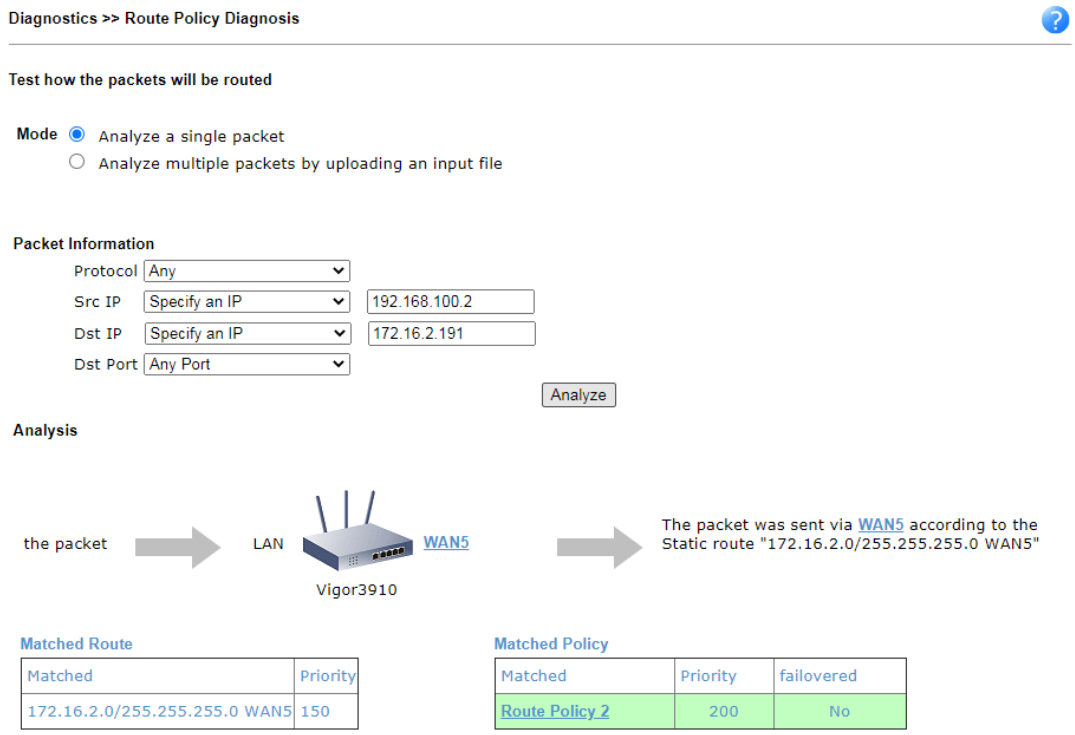
Select this mode to make Vigor router analyze how a single packet will be sent by a route policy.



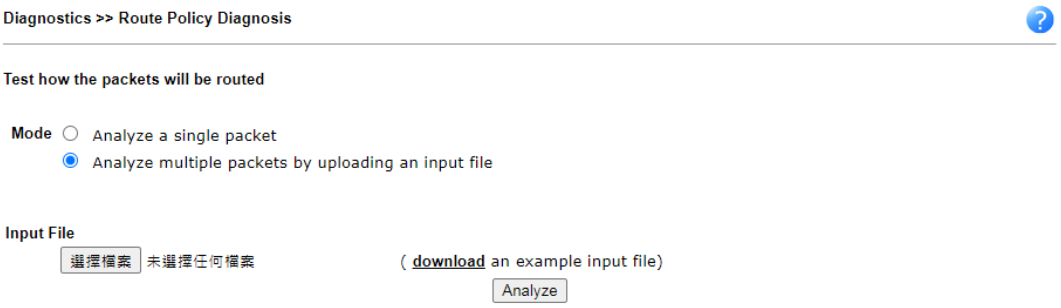
Available settings are explained as follows:

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. ● **Subnet/IP Routed Subnet** - Any source IP address on the specified subnet. **Dst IP** – IP address of the destination host. ● **Specify an IP** - One destination IP address. ● **Any IP** - Destination IP address is not specified. **Dst Port** – Number of port to which the traffic is sent. This setting is only applicable to UDP and TCP protocols. Use the drop down list to specify the destination port. **Analyze** – Click to analyze and display routes, route policies and load balance rules with matching criteria. If required, click **export analysis** to export the result as a file.

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



Analyze multiple packets by uploading an input file



Available settings are explained as follows:

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

Analyze – After selecting input file, click to start the analysis process. Click the **export** button to export the result as a file.

Note that the analysis was based on the current "load-balance/route policy" settings, we do not guarantee it will be 100% the same as the real case.

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

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

Mode: Analyze a single packet / Analyze multiple packets by uploading an input file

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

Analyze

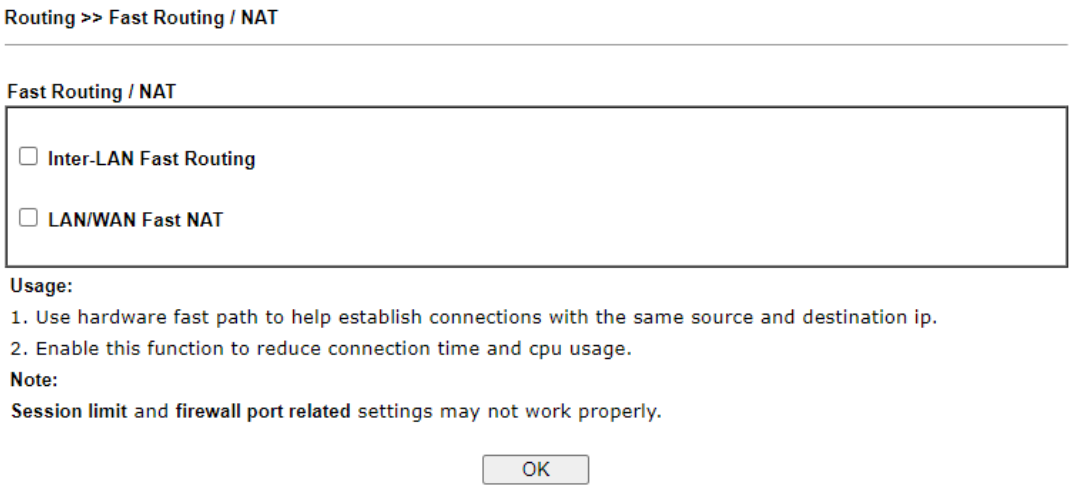
Analysis — export

	Input Packet Information				Matched Route		Matched Policy			Final Result	
Profile	Proto	Src IP	Dst IP	Dst Port	Route	Priority	Policy	Priority	failovered	Interface	Reason
LA-branch	ICMP	192.168.1.10	10.10.10.10	Any	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because neither "route" or "policy" was matched
NY-branch	TCP	192.168.1.20	20.20.20.20	5060	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because neither "route" or "policy" was matched
NZ	UDP	192.168.1.30	30.30.30.30	5060	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because

II-6-3 Fast Routing

This function allows for establishing a network connection with a built-in acceleration engine. Time can be saved and CPU usage can be reduced.

Available settings are explained as follows:



Item	Description
Inter-LAN Fast Routing	If enabled, the routing connection will be accelerated.
LAN/WAN Fast NAT	If enabled, the NAT connection will be accelerated.

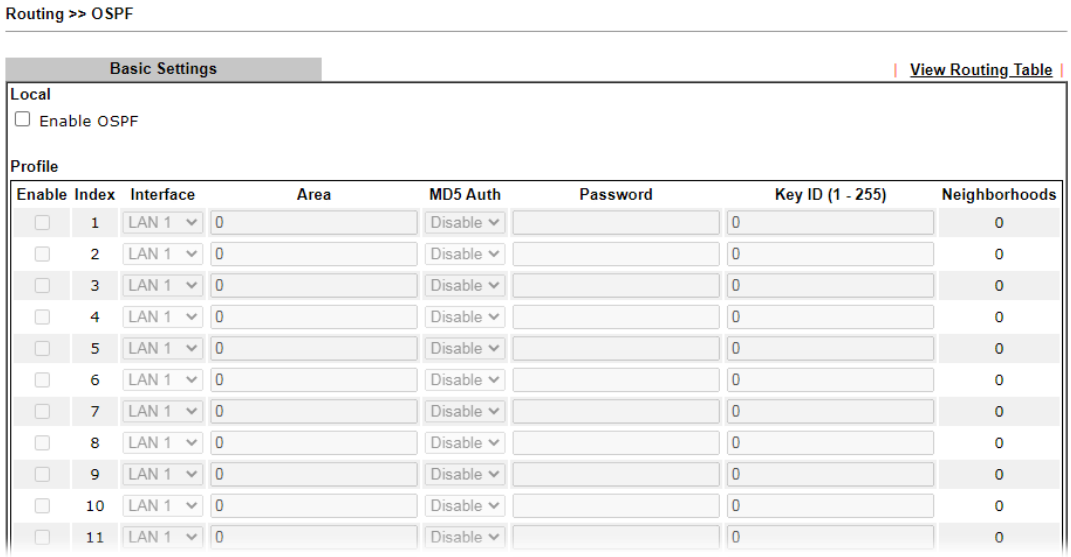
II-6-4 OSPF

OSPF(Open Shortest Path First), running within the AS, is a routing protocol based on IP protocol. It uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange. Vigor3910 supports up to OSPF version 2(only for IPv4).

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

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

Open **Routing >> OSPF** to get the following page.



Available settings are explained as follows:

Item	Description
Local	
Enable OSPF	Check the box to enable the function.
Profile	
Enable	Check it to enable and configure an OSPF profile.
Index	1 to 64 indicates profile 1 to profile 64.
Interface	Choose a LAN / WAN interface to apply the settings configured for this profile.
Area	An AS will be divided into several areas. Each area must be assigned with a dedicated number.
MD5 Auth	Enable/disable the MD5 authentication mechanism for such profile.
Password	Enter characters as the password for MD5 authentication.
Key ID (1-255)	Specify the IP address of such Vigor router. Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified,

	then an IP address of the active interface will be used by system automatically.
Neighborhoods	Displays current neighbors status in BGP routing environment.

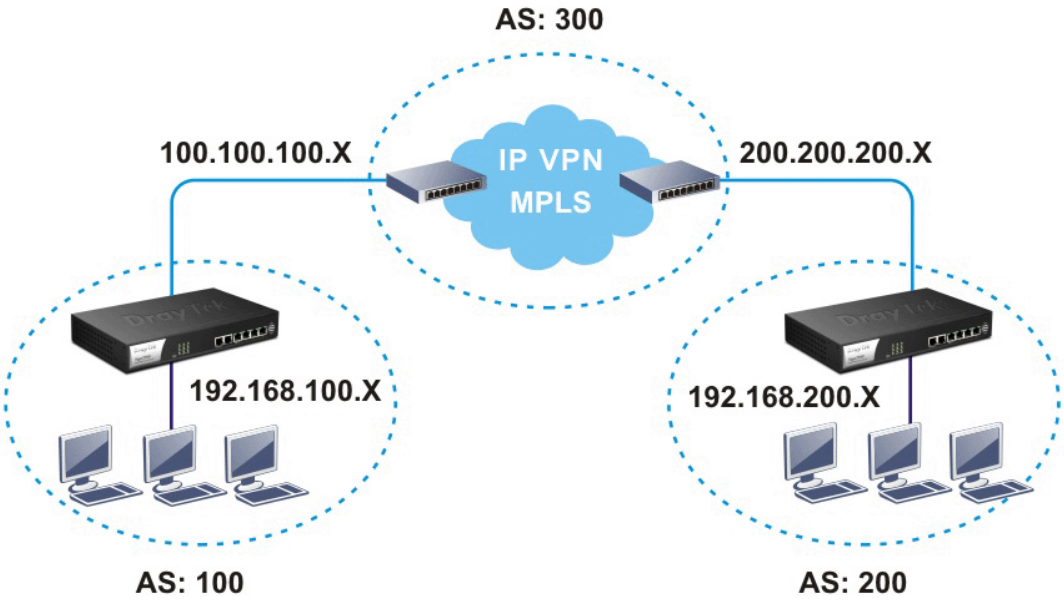
When you finish the configuration, please click **OK** to save and exit this page.

II-6-5 BGP

BGP means Border Gateway Protocol. It is a standardized exterior gateway protocol which can exchange routing and reachability information between autonomous systems (AS) on Internet.

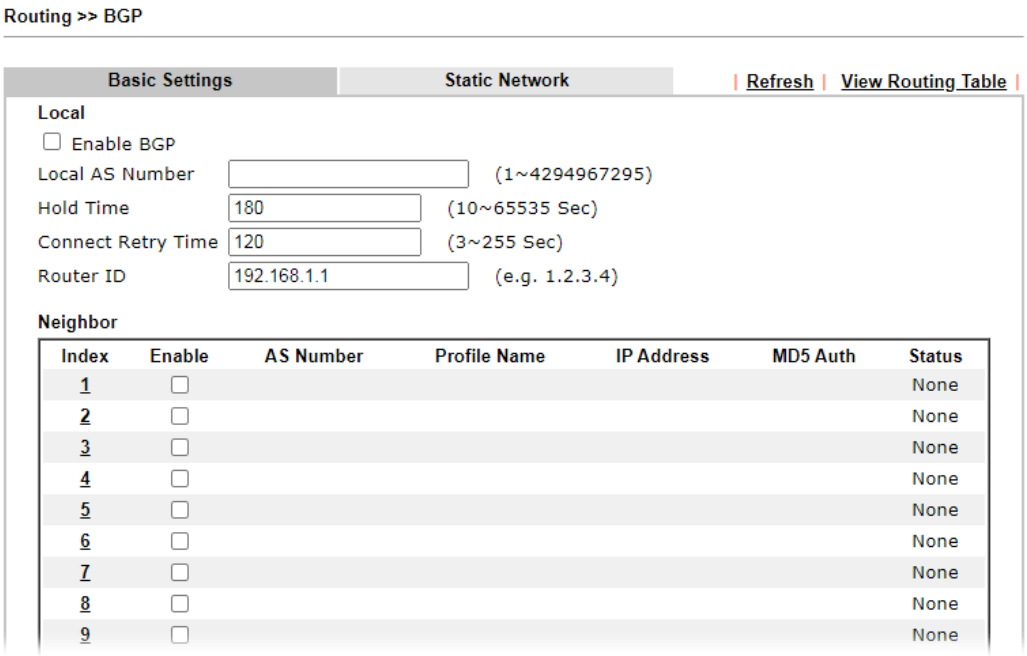
The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the "neighbor" of other BGP routers. Define the IP address, AS number for the router is essential for TCP connection of BGP routing information exchange.

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



II-6-4-1 Basic Settings

Set general settings for for local router and neighboring routers.



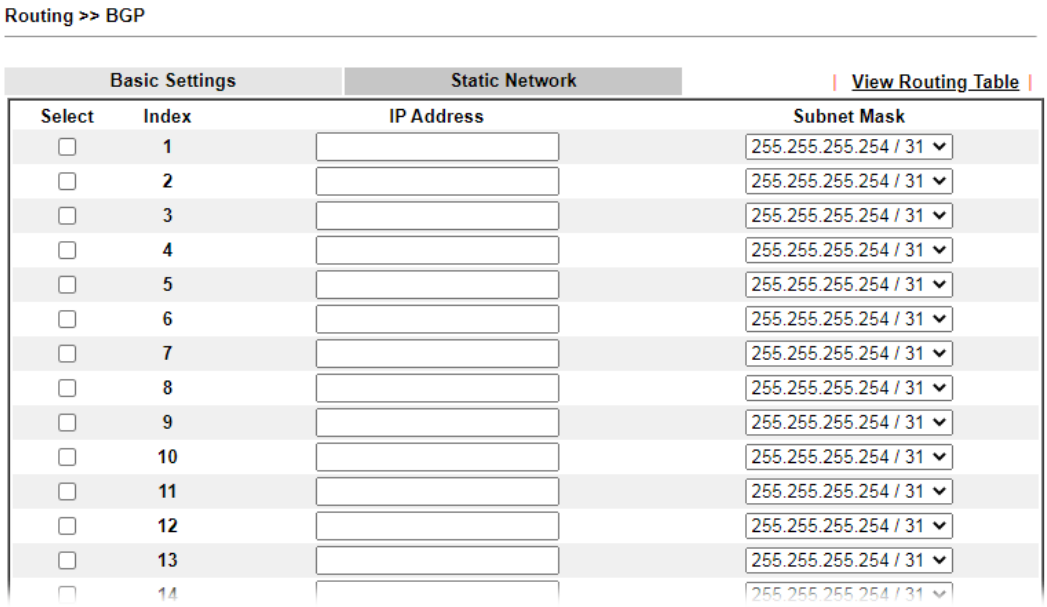
Available settings are explained as follows:

Item	Description
Local	
Enable BGP	Check the box to enable basic BGP function for local router.
Local AS Number	Set the AS number for local router.
Hold Time	Set the time interval (in seconds) to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time.
Connect Retry Time	If the router fails to connect to neighboring router, it requires a period of time to reconnect. Set the time interval to do reconnection.
Router ID	Specify the LAN subnet for the router.
Neighbor	
Index	Click the index number link to configure neighbor profile.
Enable	Check the box to enable the basic BGP function for neighboring router.
AS Number	Display the AS Number for neighboring router.
Profile Name	Display the name of the neighboring profile.
IP Address	Display the IP address specified for the neighboring profile.
MD5 Auth	Display the status (enable or disable) of MD5 Auth.
Status	Display the connection status for local router and neighboring router.

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

II-6-4-2 Static Network

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



Available settings are explained as follows:

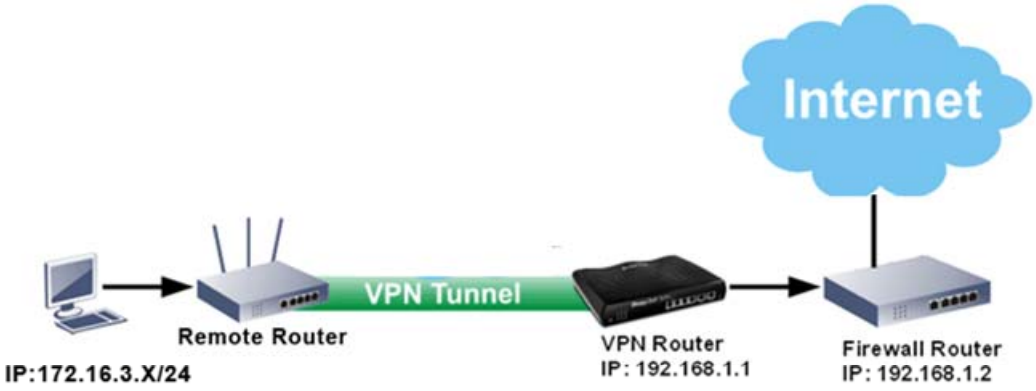
Item	Description
Select	Check the box to enable the configuration for the selected index entry.
IP Address	Enter the IP address for a router.
Subnet Mask	Choose the mask value for the IP address.

Application Notes

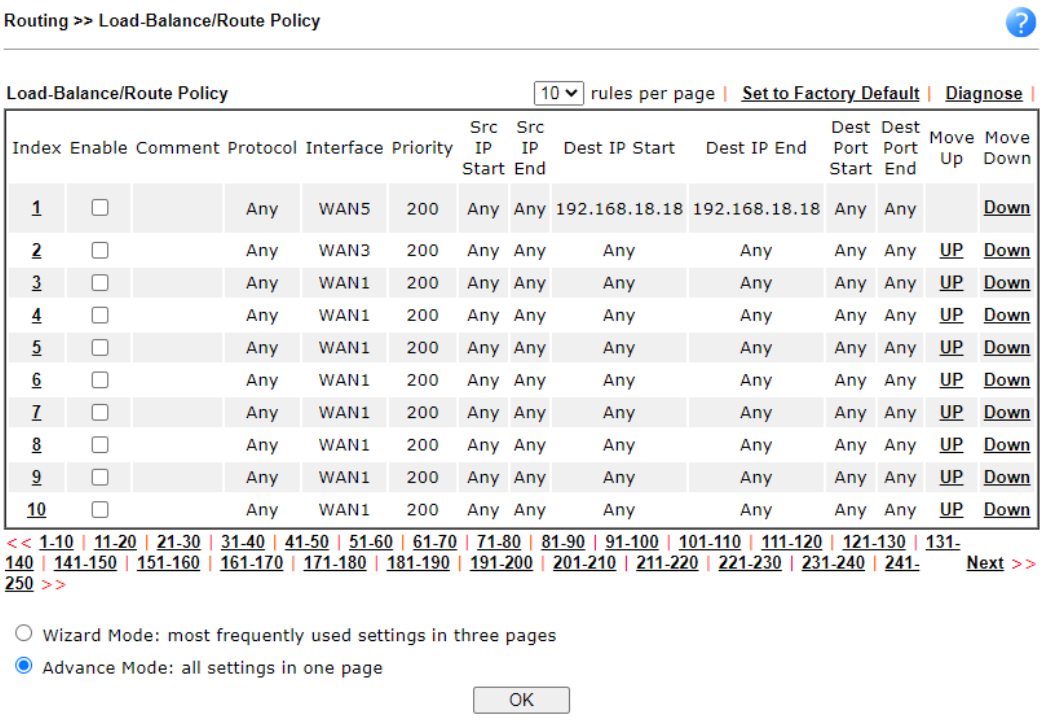
A-1 How to Customize a Secure Route between VPN Router and Remote Router by Using Route Policy

Example 1:

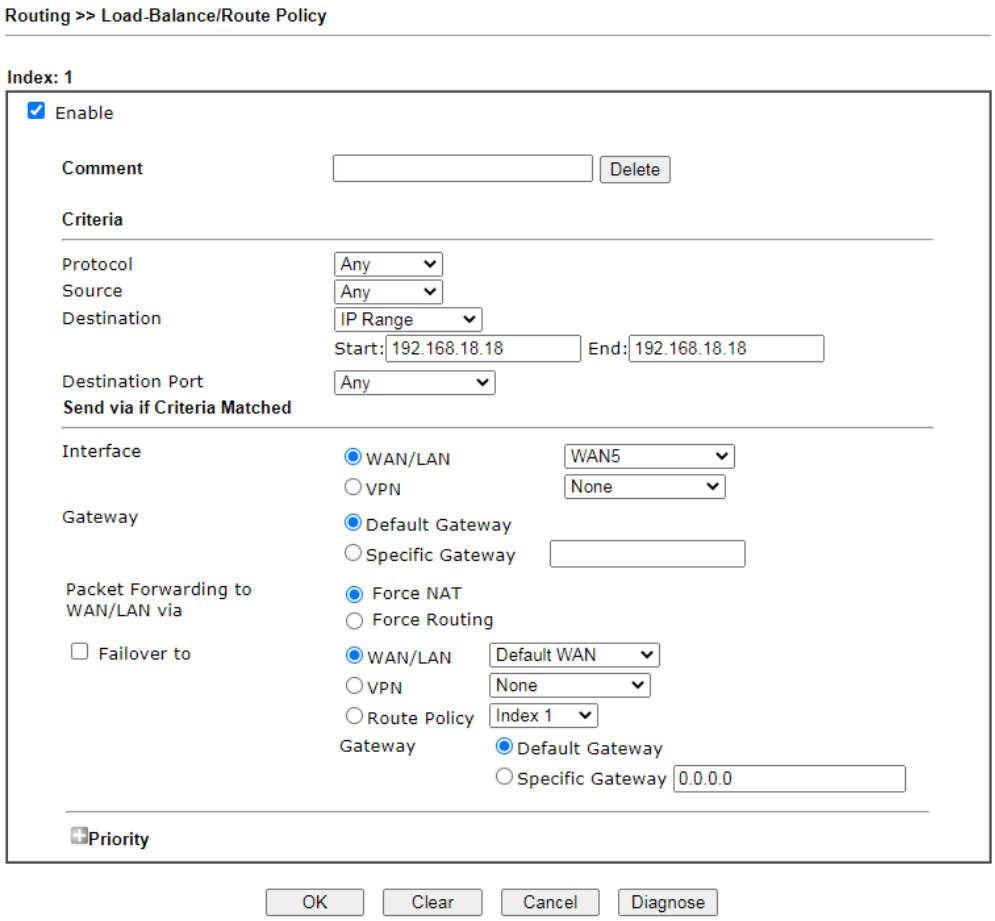
In the following figure, a LAN to LAN VPN tunnel is built between DrayTek VPN router (e.g., Vigor3910 Series) and the remote router. Firewall Router can receive all of the traffic coming from remote PC which wants to access into Internet; and send back the packets to Remote Router through VPN Router.



1. Establish a **VPN tunnel** between VPN Router and the Remote Router.
2. Change to default route for the router located in Remote Router.
3. Access into the web user interface of the router in VPN Router. Then, open **Routing >> Load-Balance / Route Policy** and click **Advance Mode.**

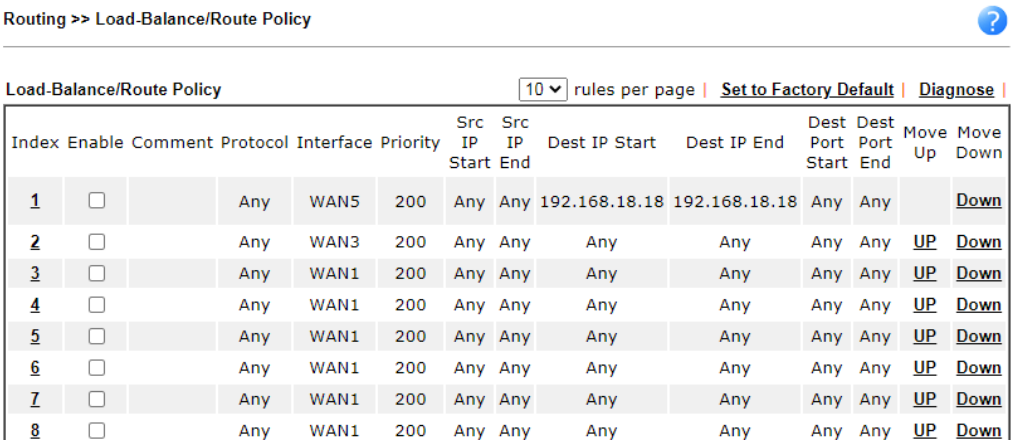


4. Click any **Index** number link (e.g., 1 in this case). Configure the settings as follows.



Now, if you want such route policy will be applied by Vigor router with higher priority, please adjust the value of **Priority** for such route policy. In general, default route is specified with the lowest priority for it value is fixed as "250". And Routes in Routing Table are fixed as "150". You can adjust the value for such route policy with lower value, e.g., 100 to ensure it will be applied to packets transmission with the highest priority.

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

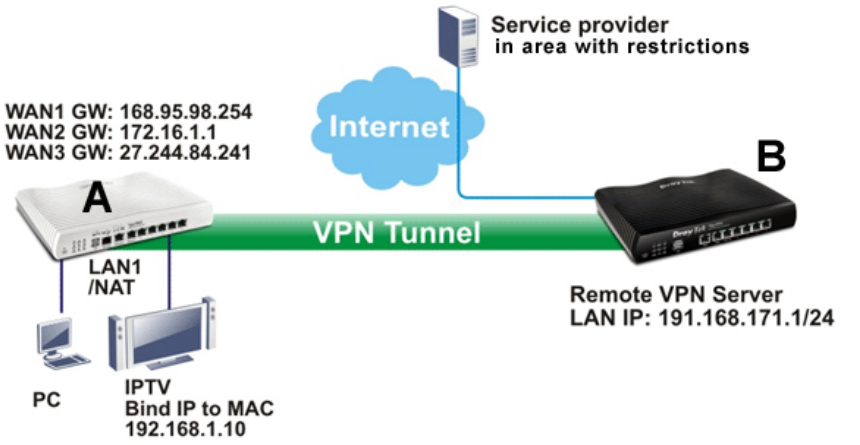


Index	Enable	Comment	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	☐		Any	WAN5	200	Any	Any	192.168.18.18	192.168.18.18	Any	Any		Down
2	☐		Any	WAN3	200	Any	Any	Any	Any	Any	Any	UP	Down
3	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
4	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
5	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
6	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
7	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
8	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down

6. To route the packets coming from the Firewall Router back to the remote router, access into the web user interface of the Firewall Router. Then, set "192.168.1.1/24" as the gateway IP address and set "172.16.3.0/24" as the destination IP address.

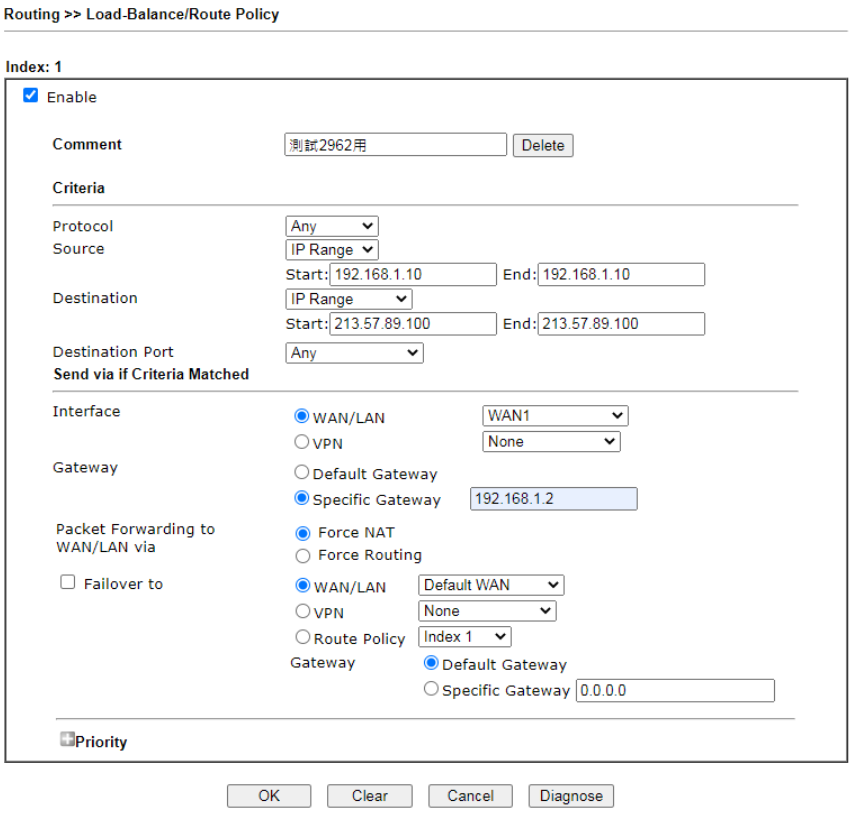
Example 2:

Below shows a scenario that local users behind Vigor router A want to access into a remote service (e.g., YouTube) which is blocked or restricted by local Service Provider in area with restrictions. A policy route can be created by the side of Router A to break through the Internet censorship circumvention.



A VPN tunnel has been established between Router A and router B.

1. Access into the web user interface of Router A.
2. Open **Routing >> Load-Balance/Route Policy** and click **Advance Mode.**
3. Click any index number (e.g., #1 in this case).
4. In the following web page, check **Enable**; type “192.168.1.10” as **Src IP Range**; type “213.57.89.100” as the **Destination IP** for the remote VPN server; and choose VPN as the **Interface** setting.



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

This page is left blank.

Part III 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.

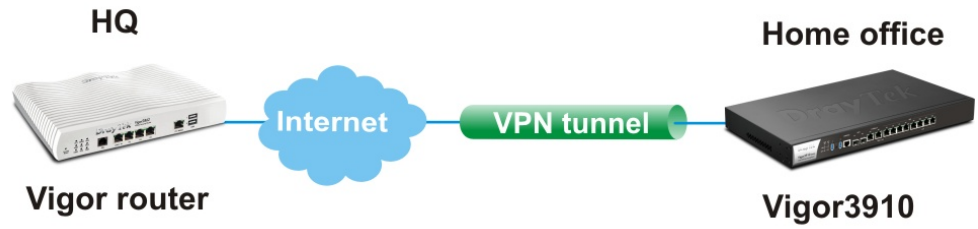
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is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

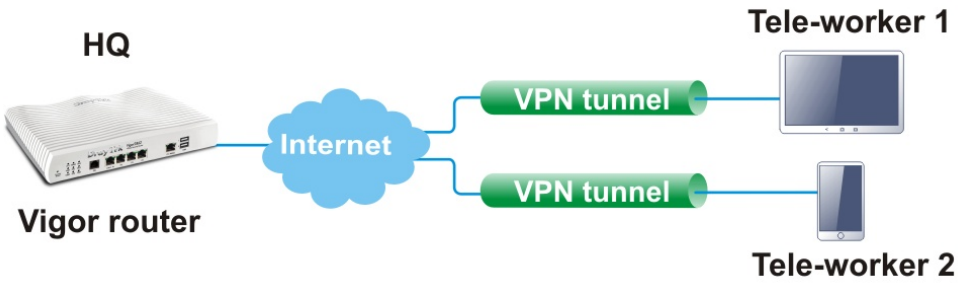
III-1 VPN and Remote Access

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

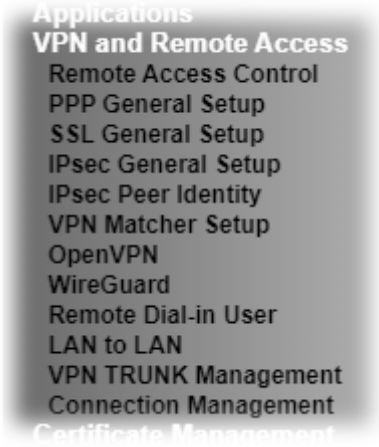
The VPN built is suitable for:

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





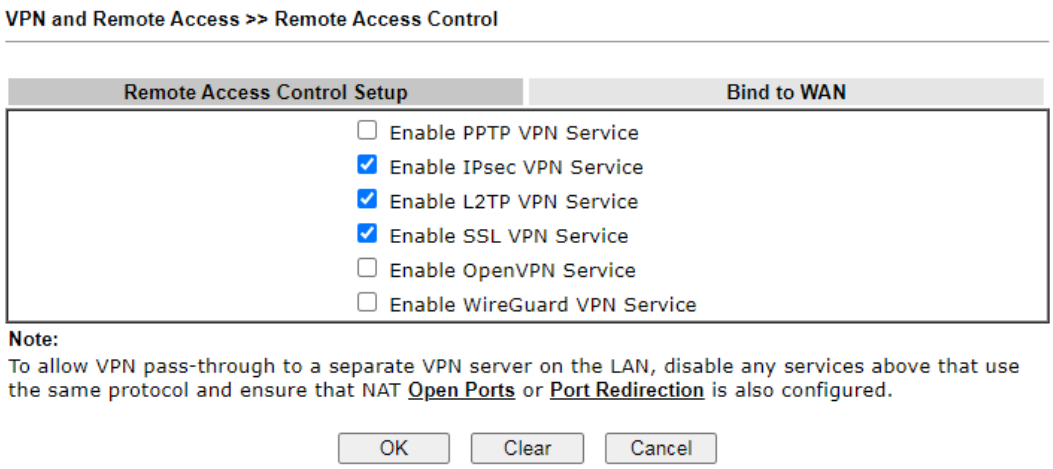
Web User Interface



III-1-1 Remote Access Control

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

III-1-1-1 Remote Access Control Setup

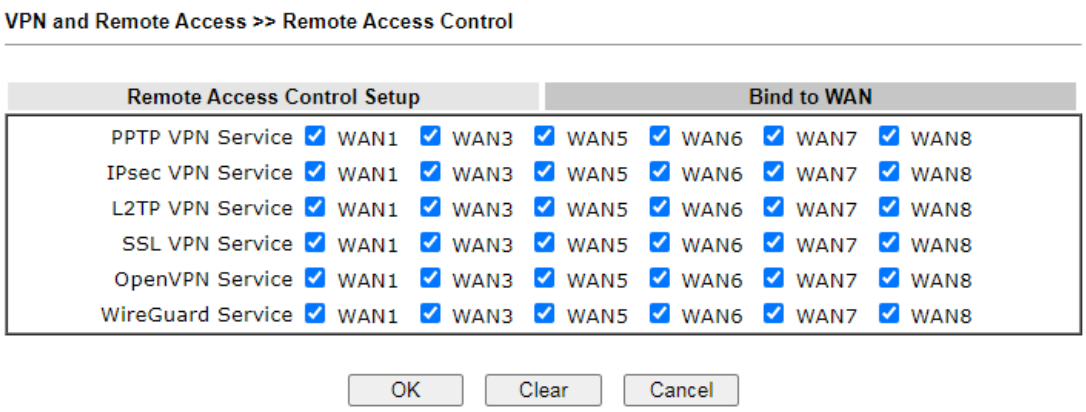


Item	Description
Enable PPTP VPN Service	This is the one of the earliest VPN protocols and is natively supported by all Microsoft Windows versions since Windows 95, all Android devices, iOS devices before version 10, and Mac OS X before version 10.12. It is easy to set up, has low overhead, and moderately 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	OpenVPN is an open-source VPN technique and could authenticate each other using pre-shared secret keys, certificates, or username/password.
Enable WireGuard VPN Service	WireGuard is a secure, fast, and modern open-source VPN Protocol. This type of VPN connection is made by exchanging public keys and intends to be considerably more performant than OpenVPN.

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**.

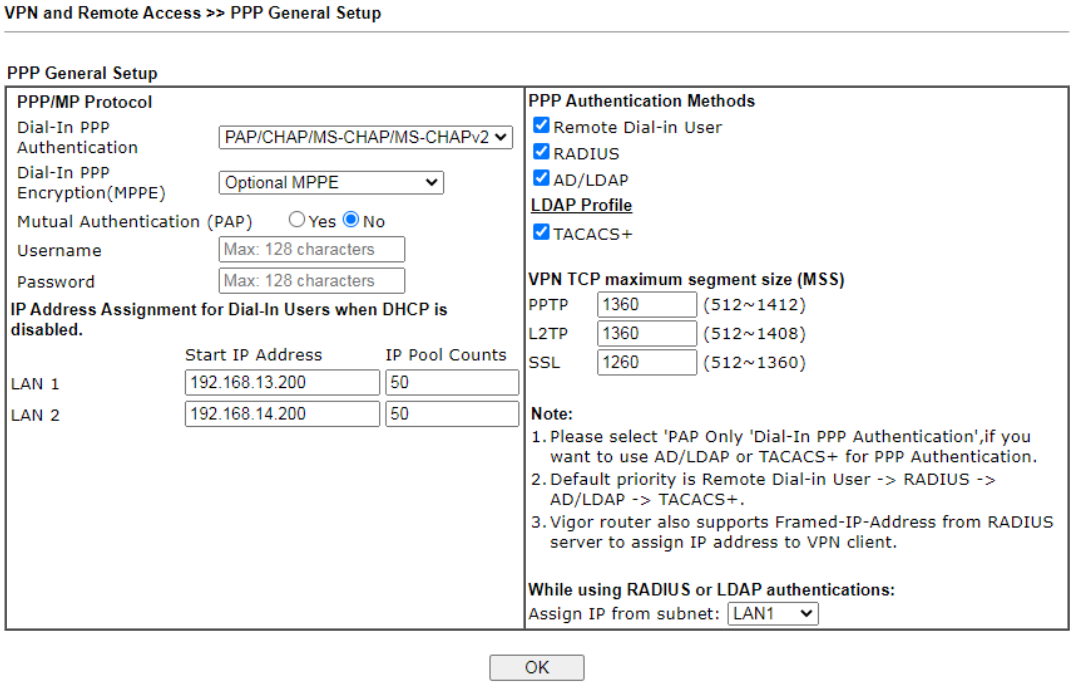
III-1-2 Bind to WAN

Select the WAN interfaces to accept PPTP VPN, IPsec VPN, L2TP VPN, inbound SSL VPN, OpenVPN and WireGuard connections.



III-1-2 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	**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. LAN# 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. **AD/LDAP** – An Active Directory/LDAP server is to be used for authentication. Please be sure to configure AD and LDAP settings in Applications >> Active Directory/LDAP. **TACACS+** – A TACACS+ server is to be used for authentication. Please be sure to set up the RADIUS server in Applications >> RADIUS/TACACS+ section.
PPTP LDAP Profile	Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles. However, if there is no profile listed, simply click the link of **PPTP LDAP Profile** to create/add some new LDAP profiles you want.
VPN TCP maximum segment size (MSS)	Set the maximum segment size (MSS) for different VPN types. Please specify the MSS values for each type to avoid packets cut by MTU during the data transmission period via the IPsec VPN connection.
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, AD, TACACS+), the assigned IP address will be drawn from the address pool of the LAN specified here.

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

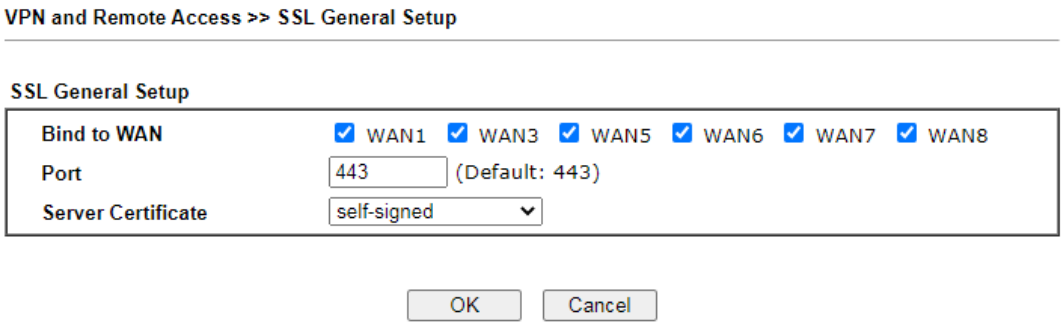
III-1-3 SSL General Setup

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**.

III-1-4 IPsec General Setup

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

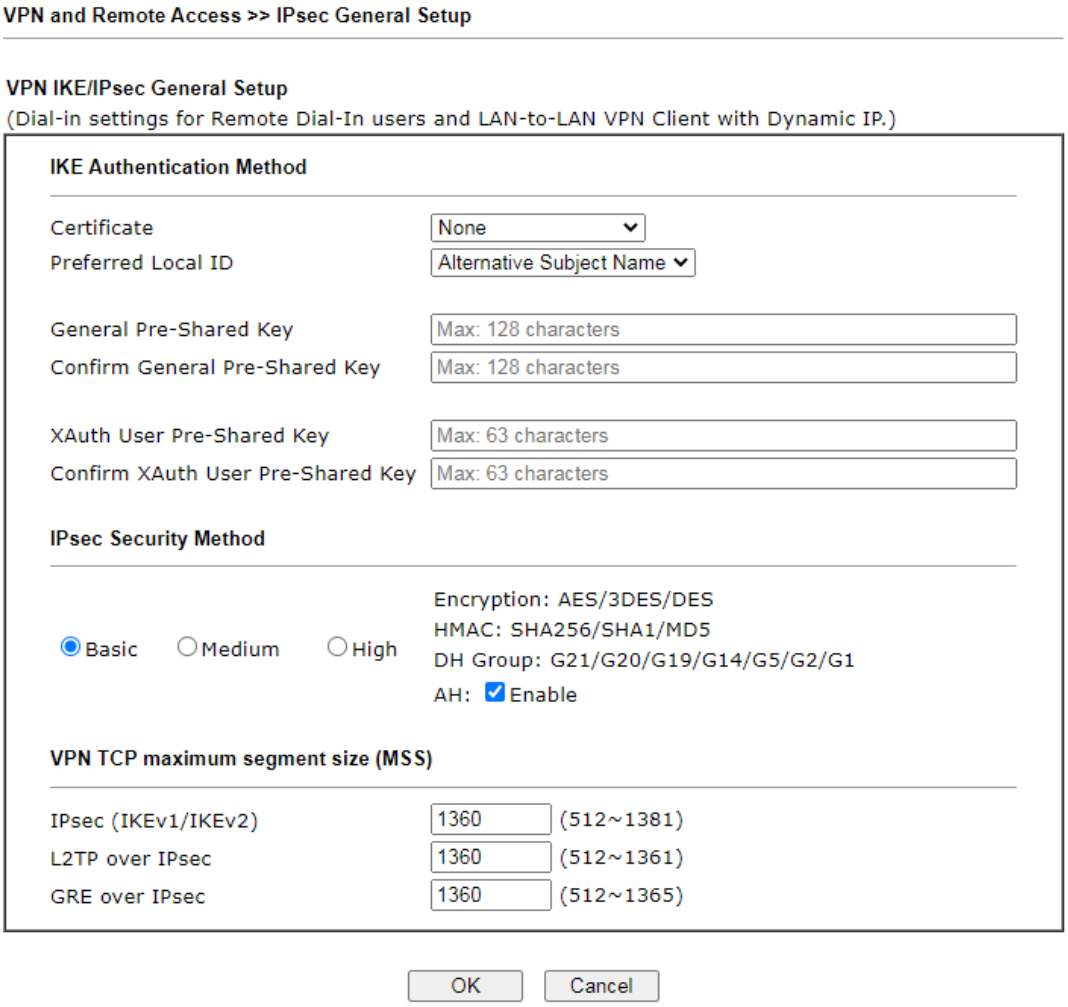
There are two phases of IPsec.

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

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

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

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



Available settings are explained as follows:

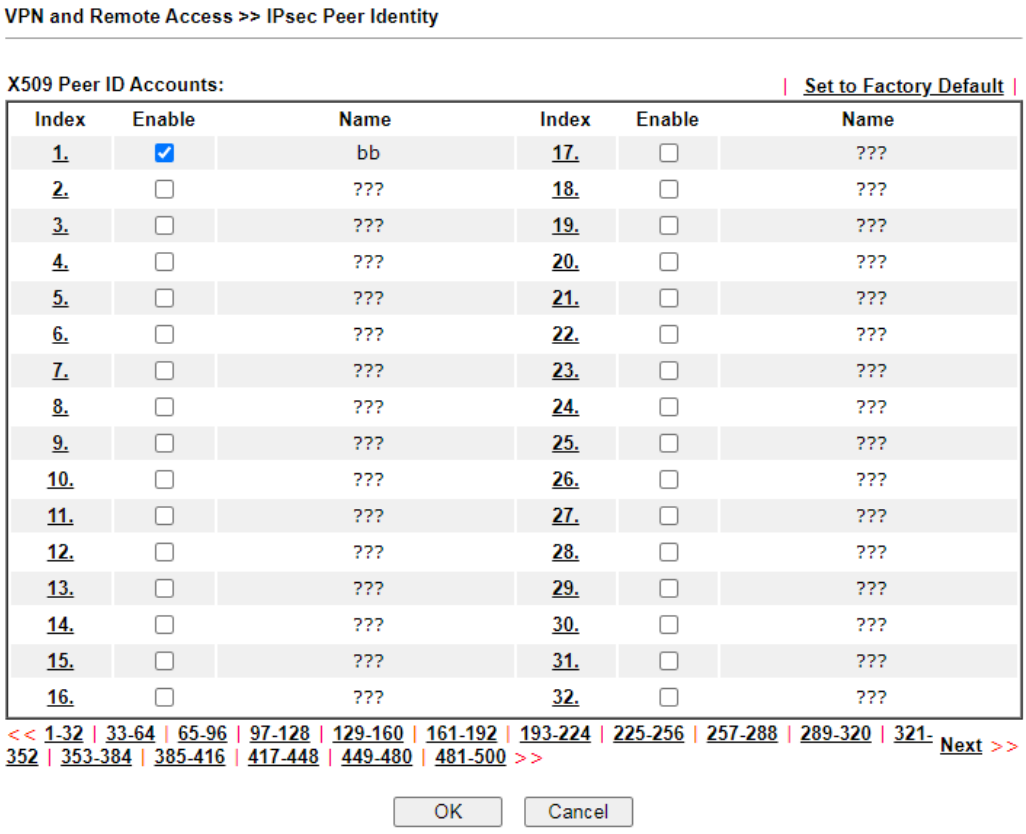
Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, **Certificate (X.509)** and **Pre-Shared Key**. **Certificate** – X.509 certificates can be used for IKE authentication. To set up certificates on the router, go to the Certificate Management section. **Preferred Local ID** - Specify the preferred local ID information **(Alternative Subject Name First** or **Subject Name First**) for IPsec authentication while the client is using the general setting (without a specific Peer IP or ID in the VPN profile). **General Pre-Shared Key-** Define the PSK key for general authentication. **Confirm General Pre-Shared Key-** Re-enter the characters to confirm the pre-shared key. **XAuth User Pre-Shared Key -** Define the PSK key for IPsec XAuth authentication. **Confirm XAuth User Pre-Shared Key-** Re-enter the

	characters to confirm the pre-shared key for IPsec XAuth authentication. **Note**: Any packets from the remote dial-in user which does not match the rule defined in **VPN and Remote Access>>Remote Dial-In User** will be applied with the method specified here.
IPsec Security Method	Available mthods include **Basic, Medium** and **High**. Each method offers different encryption, HMAC and DH Group. **Basic** - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **Medium** - When this option is selected, the Authentication Header (AH) protocol can be used to provide authentication to IPsec traffic. **High** - When this option is selected, the Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security.
VPN TCP maximum segment size (MSS)	Set the maximum segment size (MSS) for different VPN types. Please specify the MSS values for each type to avoid packets cut by MTU during the data transmission period via the IPsec VPN connection.

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

III-1-5 IPsec Peer Identity

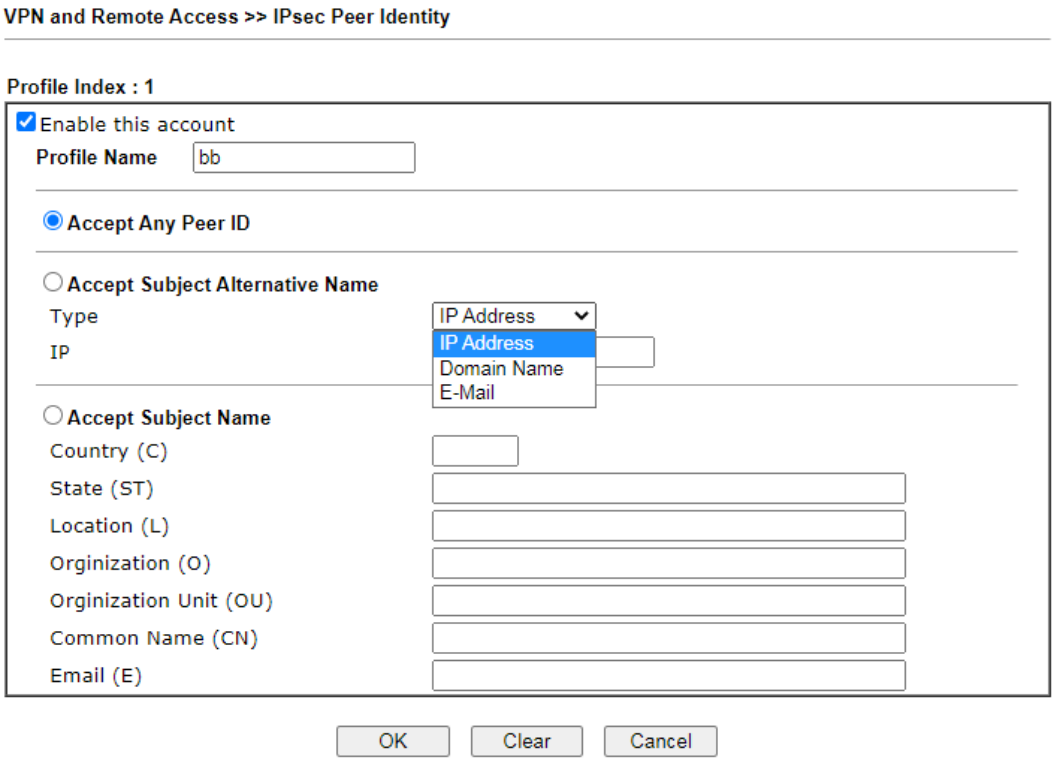
This screen allows creating profiles of subject alternative names (SANs) and distinguished names/subject names that can be used for IPsec peer authentication in LAN-to-LAN or remote user dial-in VPN connections.



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.



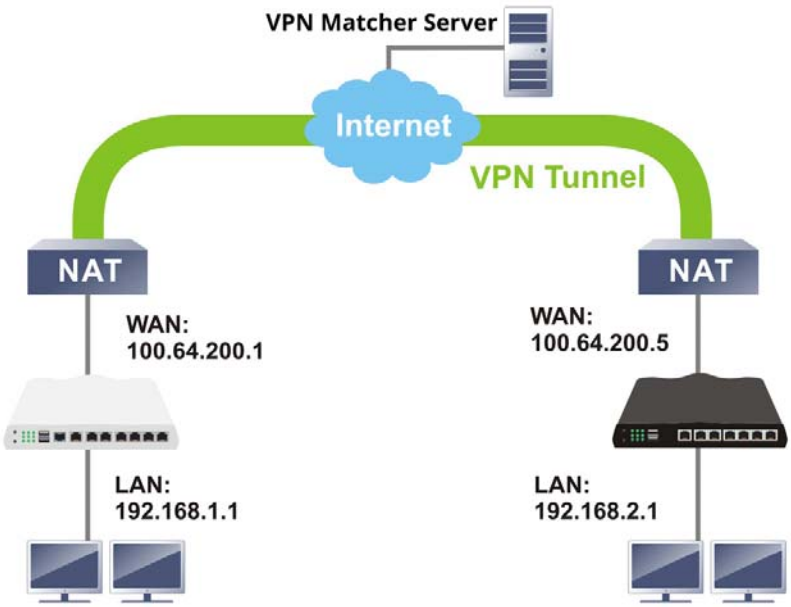
Available settings are explained as follows:

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**.

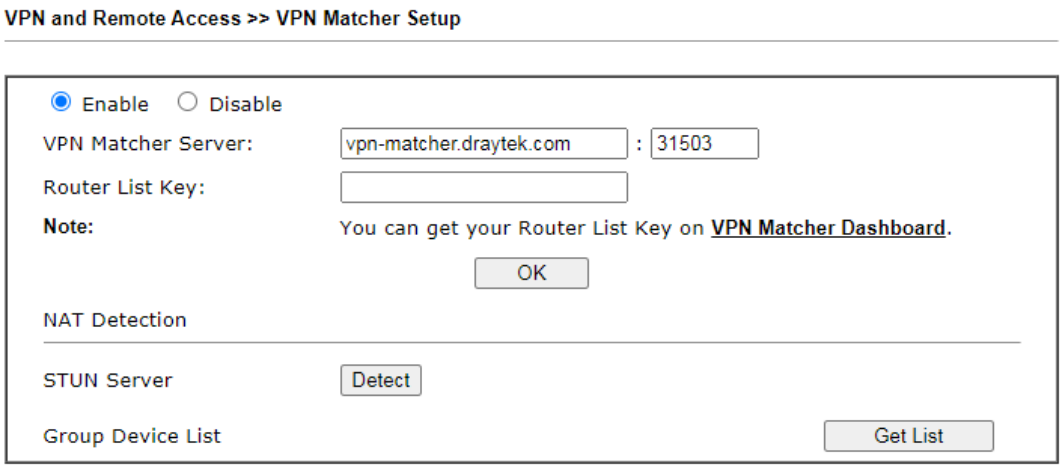
III-1-6 VPN Matcher Setup

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



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

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



Available settings are explained as follows:

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

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

III-1-7 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.

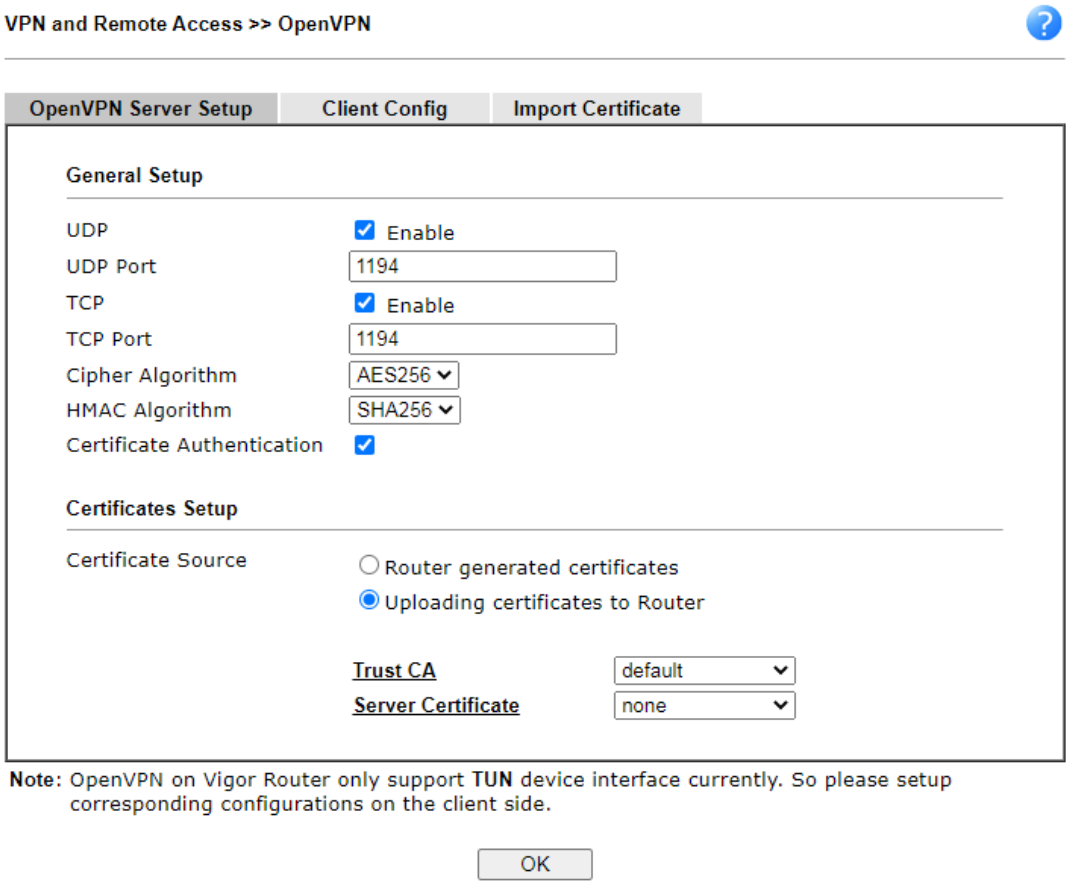
OpenVPN offers a convenient way for users to build a VPN between the local end and the remote end. There are two advantages of OpenVPN:

- 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.

III-1-7-1 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:

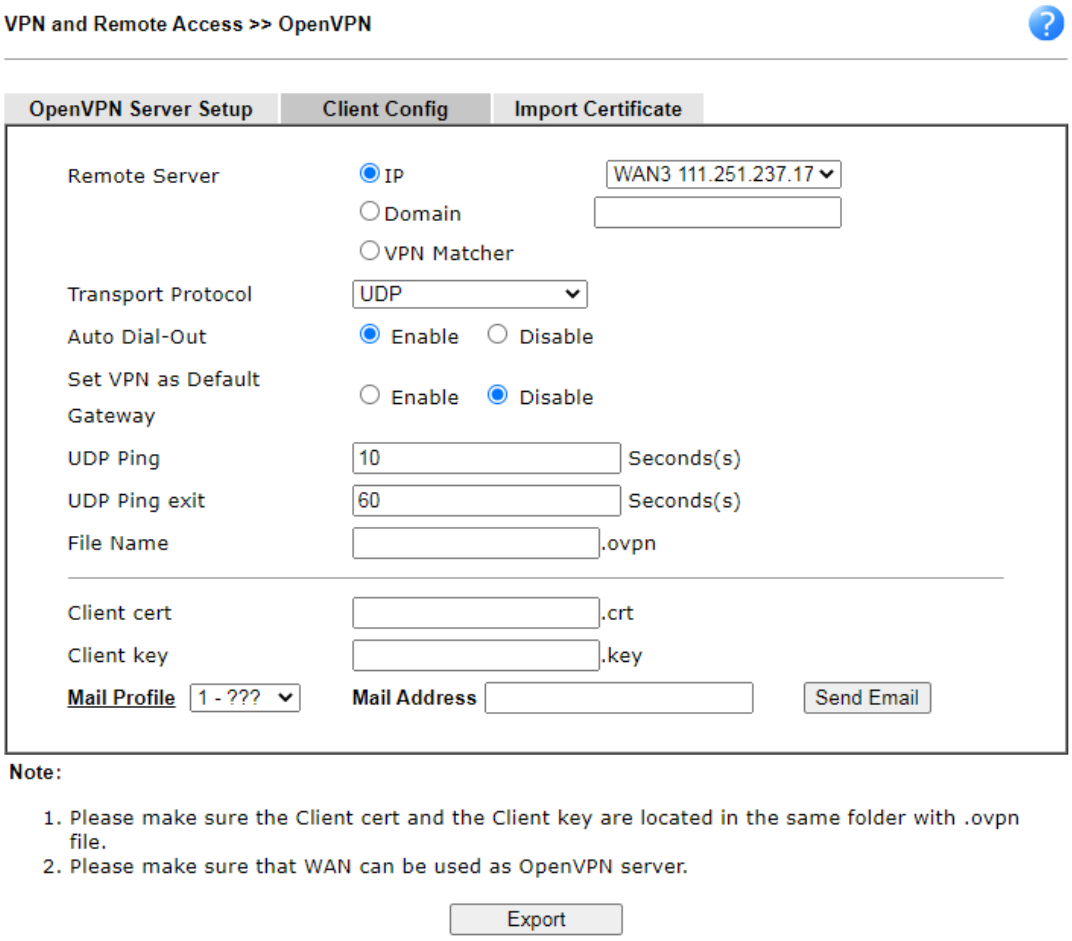
Item	Description
General Setup	
UDP	**Enable -** Select checkbox to enable UDP protocol for OpenVPN connections. **UDP Port** – Enter the UDP port number.
TCP	**Enable -** Select checkbox to enable TCP protocol for OpenVPN connections. **TCP Port** – Enter the TCP port number.
Cipher Algorithm	Select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

III-1-7-2 Client Config

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



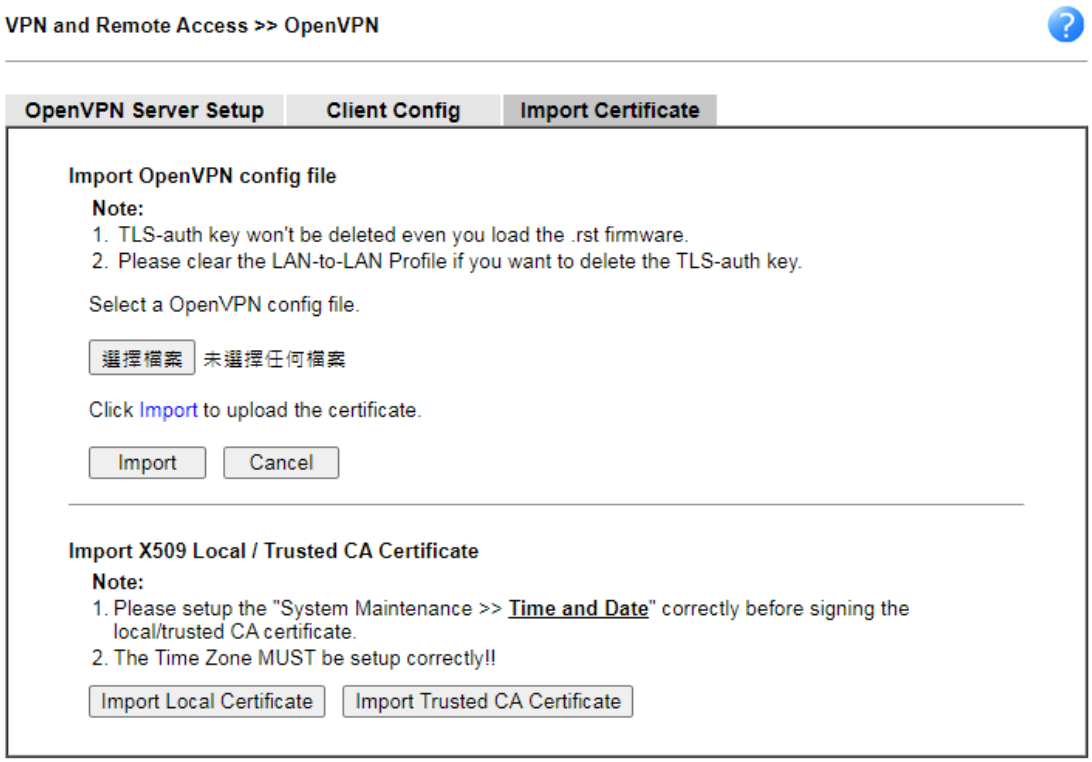
Available settings are explained as follows:

Item	Description
Remote Server	The OpenVPN client will use the IP address or domain name to connect to the router. Select either IP or Domain. **IP** – The OpenVPN configuration file will use the numeric IP address as the server address. **Domain** – The OpenVPN configuration file will use the domain as the server address. You need to ensure that the domain resolves to the IP address of a router WAN port. **VPN Matcher** – The OpenVPN configuration file will use the IP address / URL of VPN matcher server as the remote server.
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.
UDP Ping	Ping remote device over the UDP control channel, if no packets have been sent for the number of seconds configured here.
UDP Ping exit	Let OpenVPN exit after the seconds set here if no reception of a ping or other packet from the remote device.
File Name	Enter the filename of the configuration file to be downloaded from the router.
Client cert	Enter the filename of the client certificate obtained from 3rd party provider.
Client key	Enter the filename of the private key obtained from the 3rd party provider.
Mail Profile	Use the drop down list to specify a mail profile. **Mail Address** - Enter the mail address to receive the notification mail. **Send Email** - Click to send out the mail.
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.

III-1-7-3 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.

III-1-8 WireGuard

WireGuard, at present, is a secure, fast, easy, simple and modern open-source VPN Protocol. By using state-of-the-art cryptography, WireGuard can build a VPN simply by exchanging private and public keys between VPN servers (e.g., Vigor router) and VPN clients (e.g., SmartVPN Client).

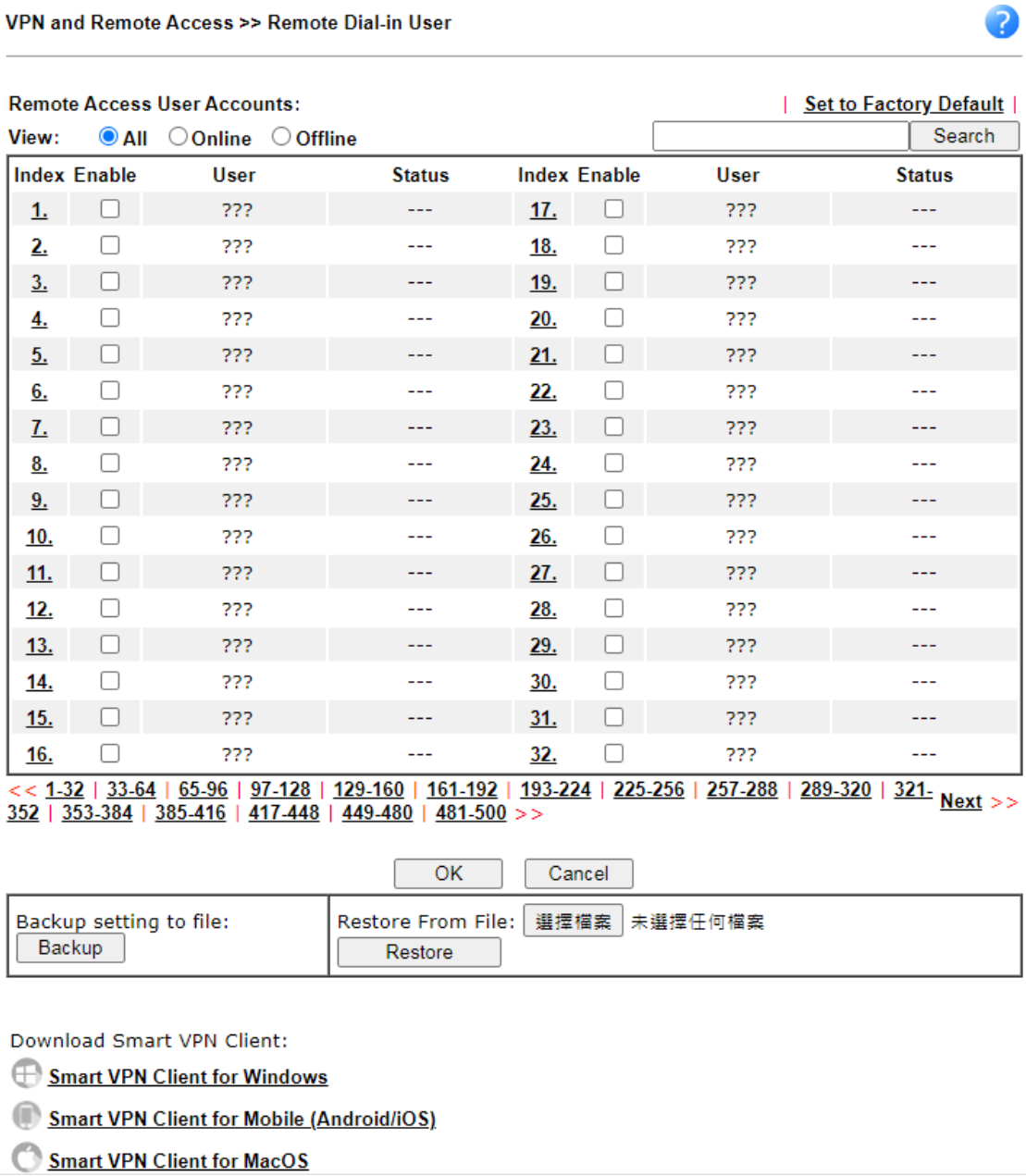
Available settings are explained as follows:

Item	Description
Server Private Key	Displays the private key generated. **Generate a Key Pair** - Generate keys for the VPN server.
Server Public Key	It is required to be configured in the WireGuard VPN client router. After clicking Generate a Key Pair, the public key and a QR code representing the public key will be shown on this page. **Copy to Clipboard** - Click to save the keys as a text file.
WireGuard Interface IP	Enter an IP address. Vigor router's LAN IP can be used as the WireGuard interface IP.
Server Listen Port	Enter a port number for WireGuard VPN server. The default number is 51820.

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

III-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.



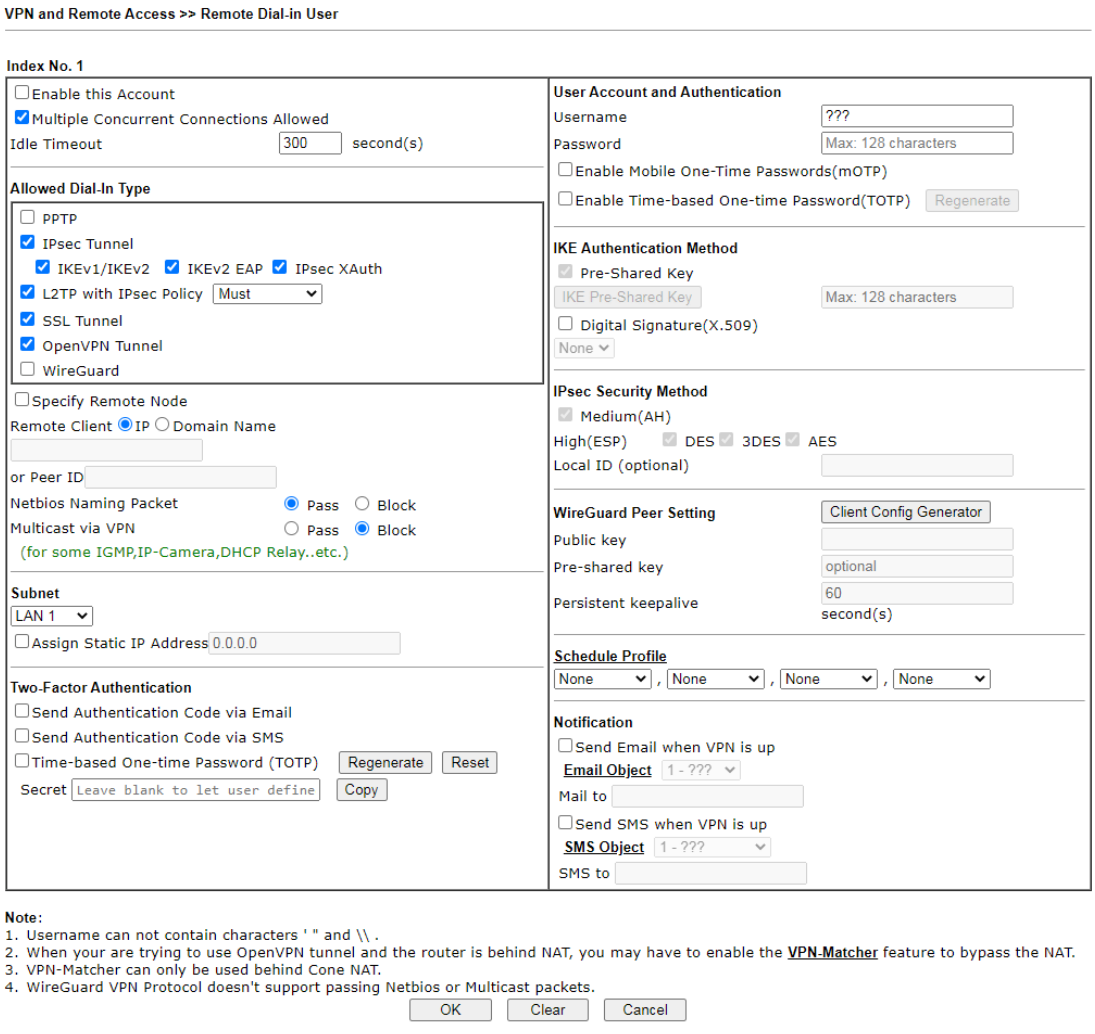
Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all remote-dial-in user profiles.
View	**All -** Click it to display the all of the user accounts. **Online** – Click it to display the online user accounts. **Offline** – Click it to display the offline user accounts.
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.

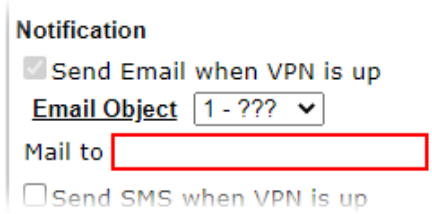
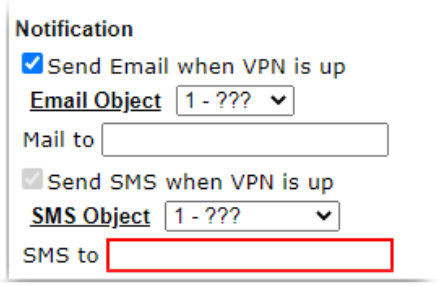
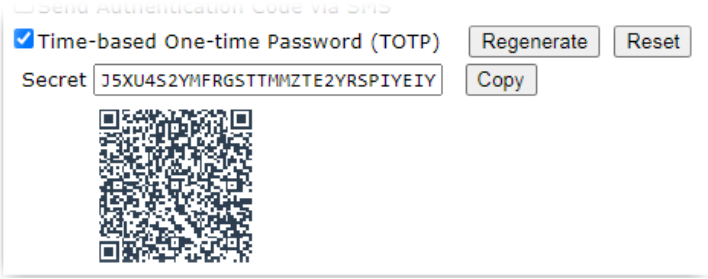
To save changes on the page, select **OK**; to discard changes, select **Cancel**.

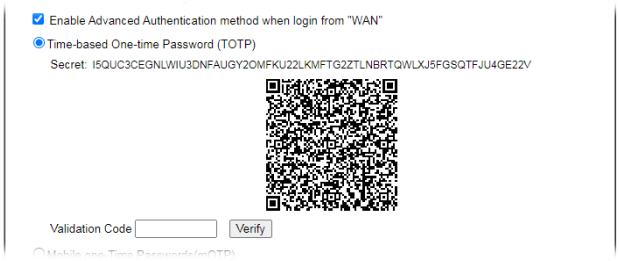
The following setup screen is shown after a profile index has been clicked.

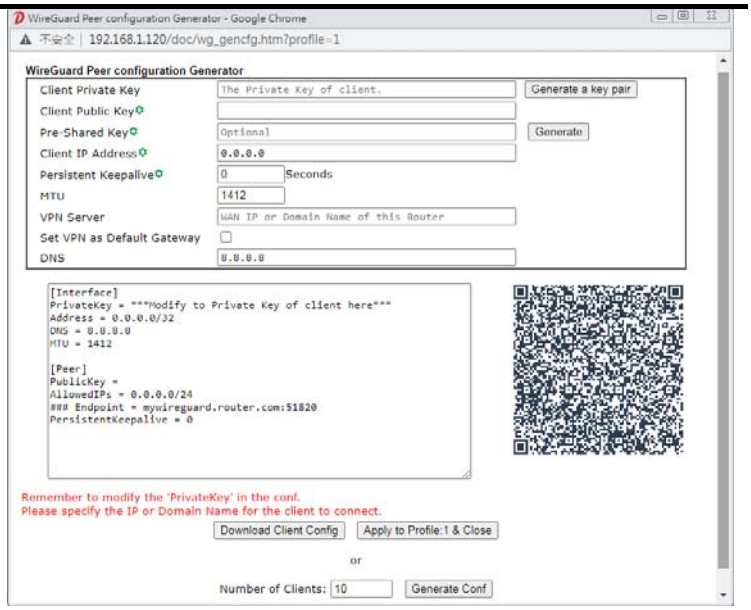


Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Select to enable this profile to be used by remote dial-in users. **Multiple Concurrent Connections Allowed** - If enabled, multiple VPN clients can connect the VPN server with the username/password set on this profile. **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.
Two-Factor Authentication	When a remote dal-in user tries to log in Vigor router from the VPN, he/she has to pass the two-factor authentication. **Send Authentication Code via Email** - Select to send the authentication code via an e-mail. The e-mail address can be specified in the field of **Mail to** under the **Notification** area.

	 **Send Authentication Code via SMS** - Select to send the authentication code via an SMS. The telephone number can be specified in the field of **SMS to** under the **Notification** area.  **Time-based One-time Password (TOTP)** - Select to display a secret generated by Vigor router. **Regenerate** - Click to regenerate a new secret and corresponing QR code. **Reset** - Click to clear the secret. **Secret** - Displays a 32 digit-secret number generated by Vigor router. Correspondign code also will be shown in this area.  **Copy** - Click to copy the secret. 但要做甚麼?
User Account and Authentication	**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). **Enable Time-based One-time Password (TOTP) -** Please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open

	the APP to scan the QR code on this page. A one-time password will be shown on your phone.  In the filed of **Validation Code**, enter the one-time password and click **Verify**. Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.
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.
WireGuard Peer Setting	Configure the settings for VPN client (peer). **Client Config Generator** - Click to pop-up the configuration window.

	 • **Client Private Key / Client Public Key** - Click the **Generate a key pair** button to generate the private and public keys. The keys will be shown on the corresponding fields. • **Pre-Shared Key** - Displays the value generated by clicking the **Generate** button. • **Client IP Address** - Enter the static IP address assigned to the client. • **Persistent Keepalive** - Default is 60 seconds. If the peer is behind a NAT or a firewall, use the default setting. • **MTU** - Enter the value. The default is 1412. • **VPN Server** - Enter the public IP address or domain name of Vigor router. • **Set VPN as Default Gateway** - If required, select the box to configure this VPN as the default gateway. • **DNS** - Enter the IP address (e.g., 8.8.8.8) of the DNS server. A QR code will be generated according to the settings configured in this pop-up window. Then, download the x.conf file by clicking **Download Client Config** and **Apply to Profiles & Close**. **Public Key** - Displays the value generated by clicking Client Config Generator. **Pre-shared Key** - Displays the value generated by clicking Client Config Generator. **Persistent Keepalive** - Default is 60 seconds. If the peer is behind a NAT or a firewall, use the default setting.
Schedule Profile	Set the VPN connection to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.
Notification	**Send Email when VPN is up** - An e-mail will be sent to the user defined in Email Object when VPN is connected and up. • **Mail to** - Enter an email address. **Send SMS when VPN is up** - An SMS will be sent to the user defined in SMS Object when VPN is connected and up.

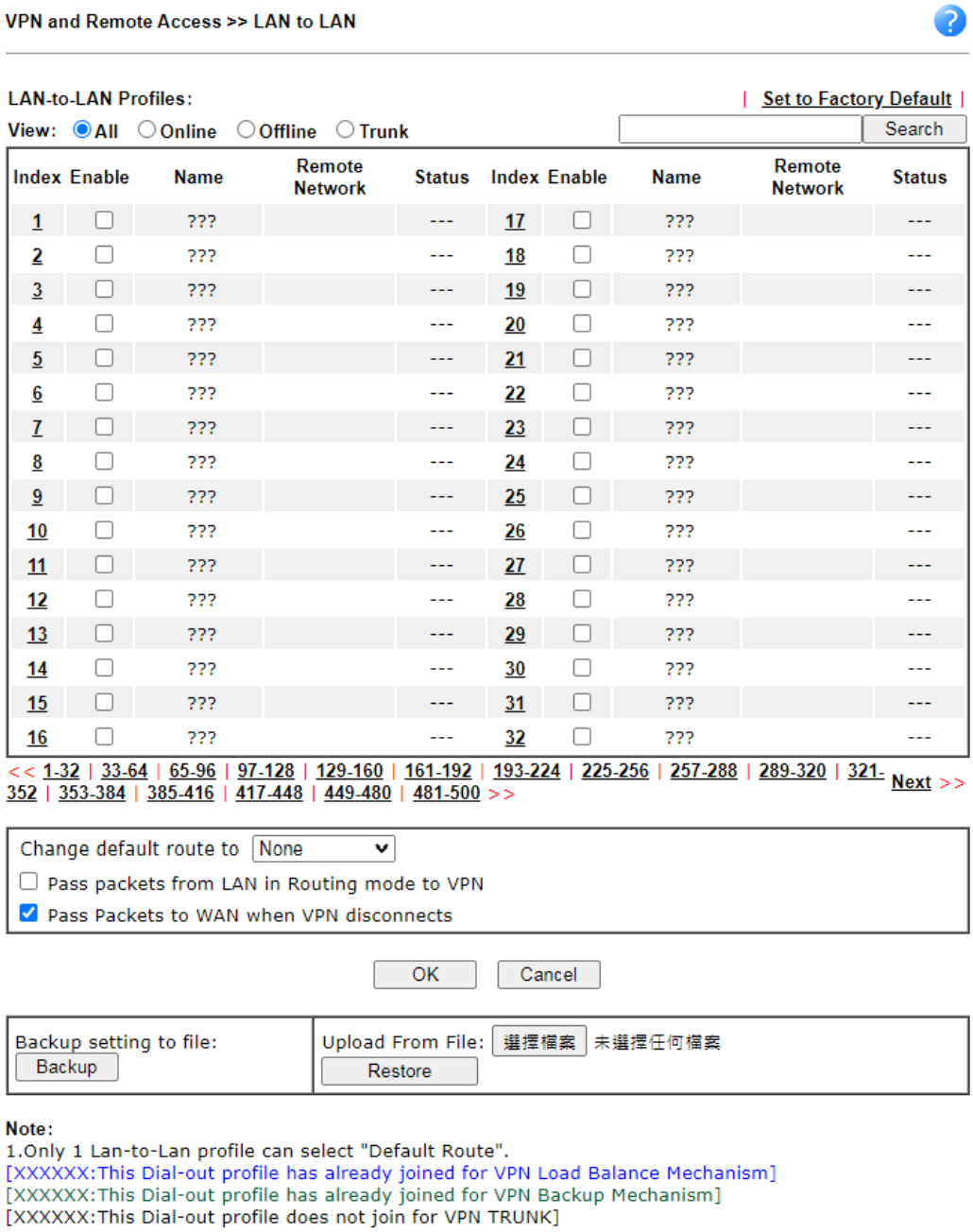
	• **SMS to** - Enter a phone number.

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**.

III-1-10 LAN to LAN

This section allows you to configure up to 500 LAN-to-LAN VPN connection profiles. LAN-to-LAN connections can be configured to allow dial-in only, dial-out only, or both dial-in and dial-out.

The following figure shows the summary table according to the item (All/Trunk) selected for **View**.

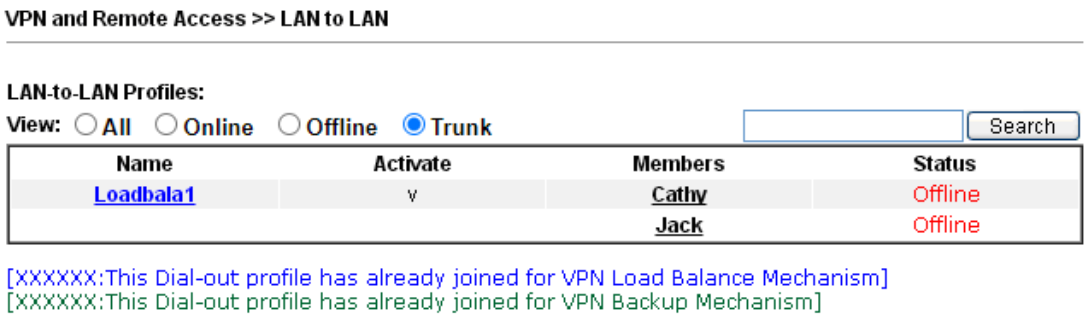


Available settings are explained as follows:

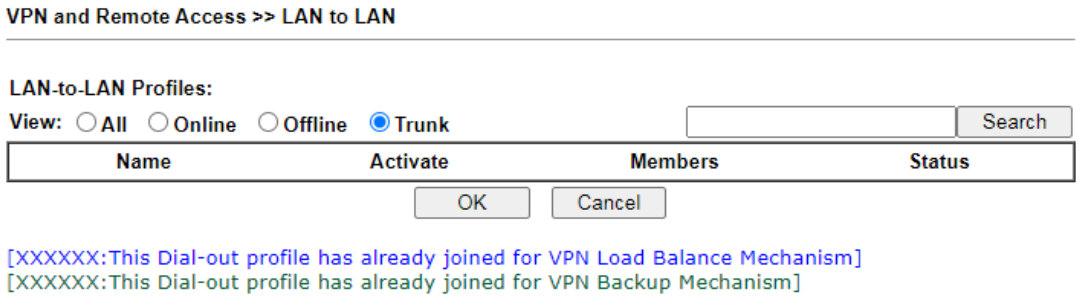
Item	Description
Set to Factory Default	Click to clear all indexes.

View	**All –** Shows all LAN-to-LAN VPN profiles. **Trunk –** Shows all Trunk profiles (see VPN and Remote Access >> VPN TRUNK Management).
Index	Click the index number of the profile to view or edit its settings.
Enable	Check to enable the LAN-to-LAN VPN profile.
Name	Display the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Remote Network	Display 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 routing LAN will pass through the VPN tunnel.
Pass Packets to WAN when VPN disconnects	If enabled, the packets can pass through via NAT 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.

The following figure shows profiles joined into VPN Load Balance and VPN Backup mechanism.

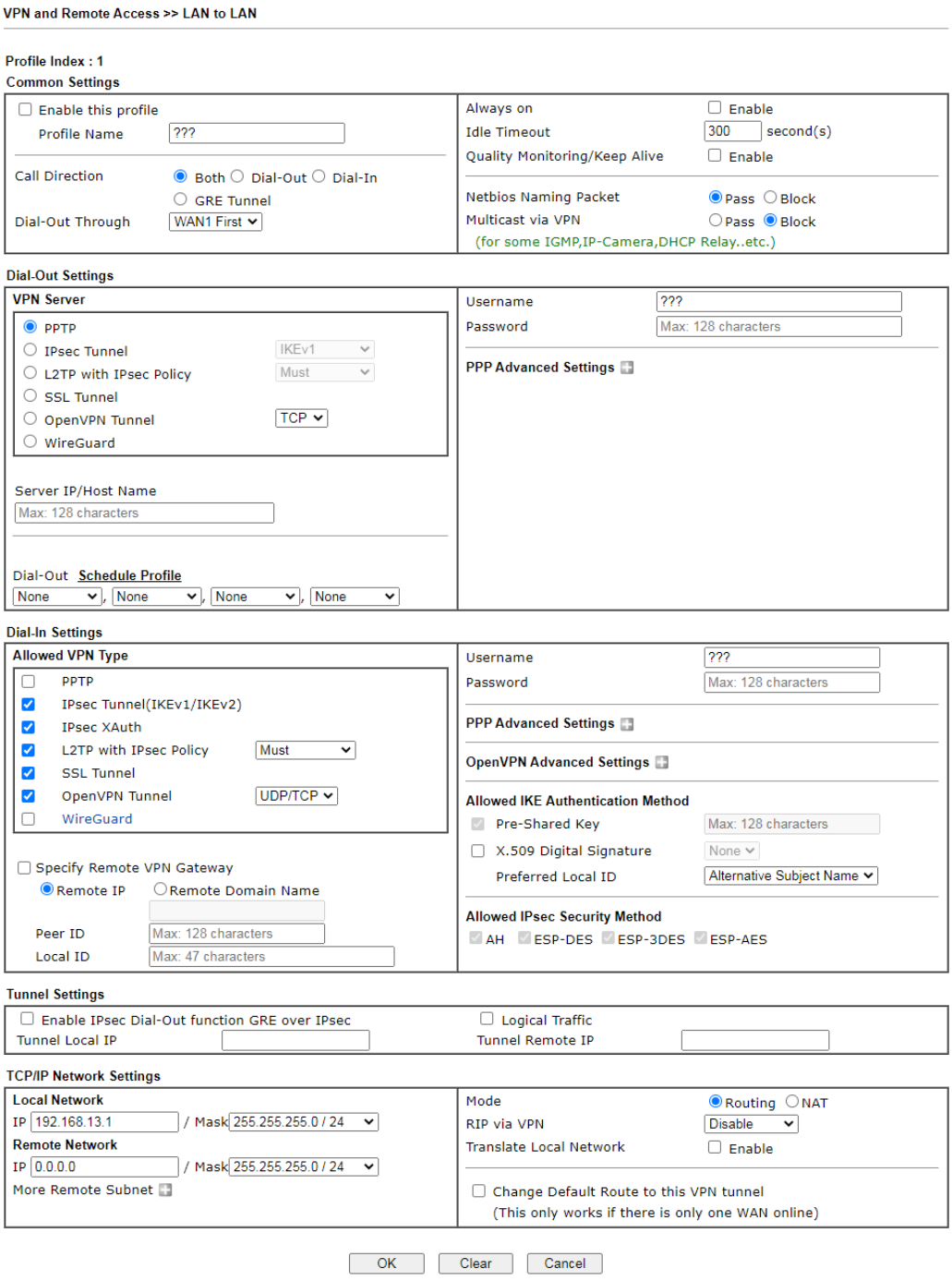


If there is no profile joined yet, this page will be shown as follows:



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, Tunnel Settings, 6in4 Settings and TCP/IP Network Settings.



Available settings are explained as follows:

Item	Description
Common Settings	
Common Settings	**Enable this profile -** Check here to activate this profile. **Profile Name -** Specify a name for the profile of the LAN-to-LAN connection. **Call Direction -** Specify the allowed call direction of this LAN-to-LAN profile. Four choices are available for connection

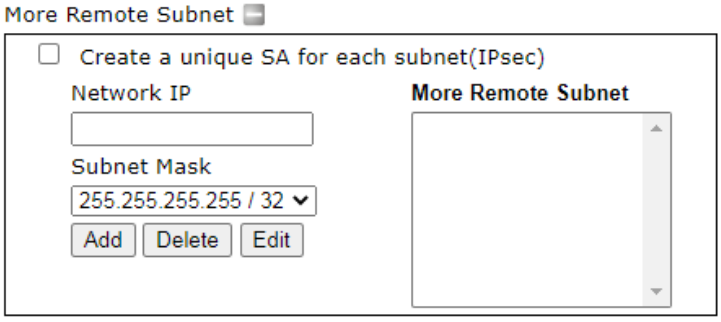
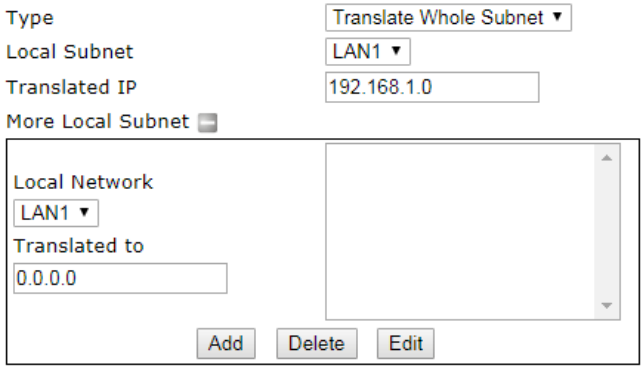
	mode: ● **Both** – Profile is to be used to initiate (dial out) or accept (dial in) connections. ● **Dial-Out** – Profile is to be used to initiate outgoing connections. ● **Dial-In** – Profile is to be used to accept incoming connections. ● **GRE Tunnel** – Connection is by means of a GRE tunnel. **Dial-Out Through -** Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only. ● **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. ● **WAN1 Only: Only establish VPN if WAN2 down** - If WAN2 failed, the router will use WAN1 for VPN connection. ● **WAN2 Only: Only establish VPN if WAN1 down** - If WAN1 failed, the router will use WAN2 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. **Quality Monitoring/Keep Alive** - Select this option to keep the VPN connection for the feature of SD-WAN quality monitoring. **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.

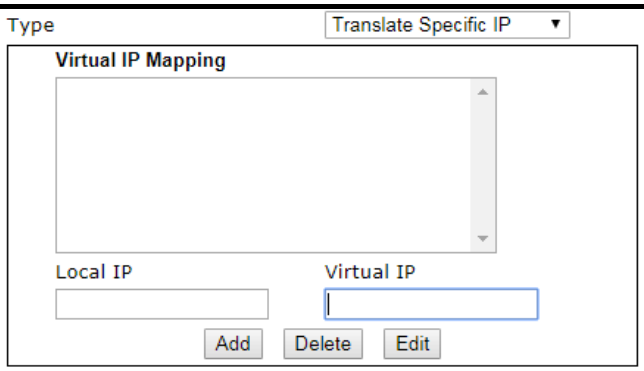
Password	Enter the password for establishing VPN connection.
If PPTP / L2TP with IPsec Policy / SSL Tunnel / is selected as VPN Server	**PPP Advanced Settings** - Click it to expand the advanced settings for PPP. ● **PPP Authentication -** PAP Only – Authenticate dial-in users using the PAP protocol 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.
If IPsec/ L2TP with IPsec Policy (Must/Nice to Have) is selected as VPN Server	**IKE Phase 1 Settings -** Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode. ● **Authentication - Digital Signature(X.509)** - **Peer ID -** Select one of the predefined Profiles set in **VPN and Remote Access >>IPsec Peer Identity.** - **Local ID -** Use **Alternative Subject Name** or **Subject Name** of local certiicate as local ID. - **Local Certificate -** Select one of the profiles set in **Certificate Management>>Local Certificate**. ● **Authentication - Pre-Shared Key** - **Pre-Shared Key -** Input 1-128 characters as pre-shared key. - **Local ID -** Enter local IKE identity to send in the exchange to establish IPsec connection. ● **proposal Encryption -** Use Auto/AES/3DES/DES for packet encryption. ● **proposal ECDH Group -** Specify a group if Auto is not selected as proposal Encryption. ● **proposal Authentication -** Select SHA256 or SHA1 for packet authentication. ● **Force UDP Encapsulation -** Select to make UDP encapsulation forcefully. All IPsec packets will be encapsulated with UDP header. **IKE Phase 2 Settings -** Specify the security protocol, proposal encryption and proposal authentication. ● **Security Protocol** - AH (Medium) means data will be authenticated, but not be encrypted. By default, this option is active. ESP (High) means payload (data) will be encrypted and authenticated. ● **Proposal Encryption** - Use AES/3DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. ● **Proposal Authentication** - Select All, SHA or None. **IKE Advanced Settings -** Specify the key life of each IKE phase, network ID, etc. ● **IKE phase 1 key lifetime-** For security reason, the

	lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. ● **IKE phase 2 key lifetime-** For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds. ● **Phase 2 Network ID -** This is optional. Change the source IP address of VPN traffic to the specified IP address for NAT mode selected on TCP/IP Network Settings field. ● **Enable Perfect Forward Secret (PFS) -** The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function. **Ping to Keep Alive -** Select to enable the function of PING to keep alive. **PING Target IP -** Enter the IP address to keep alive.
If OpenVPN Tunnel is selected as VPN Server	**OpenVPN Advanced Settings - C**lick to set the advanced settings for OpenVPN. ● **Cipher Algorithm -** Select an algorithm for encrypting the packets via OpenVPN. ● **HMAC Algorithm -** Select an algorithm for authenticating the packets via OpenVPN. ● **Client Certificate -** Select a client certificate or self-signed a new certificate or DrayDDNS certificate. ● **Trust CA -** Select a trust CA certificate. ● **Compress -** Select a method to compress the packets to reduce the bandwidth usage while transferring the compressed packets. ● **TLS - auth -** Select **On** to use the TLS authentication method. Related key information can be checked by clicking **View**. **Import OpenVPN config file -** An OpenVPN config file from other Vigor router can be imported and apply to this router. ● **Select File -** Select a file from your hard disk. ● **Import -** Click to upload the selected config file to this Vigor router.
If WireGuard with is selected as VPN Server	Click **WireGuard** to set the advanced settings. **[Interface]** - Configure the settings for Vigor router. ● **Generate a Key Pair** - Click to generate a key pair (including private key and public key). ● **Copy to Clipboard** - Click to copy the key pair to clipboard. ● **Address -** Enter an IP address that Vigor should use to access the remote VPN network. **[Peer] -** Configure the settings for the client (peer). ● **Public Key** - Enter the Public key of the Peer VPN server. ● **Pre-Shared Key -** Click **Generate** to generate the pre-shared key. ● **Keepalive** - Default is 60 seconds.
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(IKEv1/IKEv2)-** Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● **IPsec XAuth** ● **L2TP with IPsec Policy -** Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: - **None -** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. - **Nice to Have** - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. - **Must -** Specify the IPsec policy to be definitely applied on the L2TP connection. ● **SSL Tunnel-** Allow the remote dial-in user to trigger an SSL VPN connection through Internet. ● **OpenVPN Tunnel** ● **WireGuard -** A pop-up window with detailed settings will be shown on the screen. Enter the values if requried.
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.
OpenVPN Advanced Settings	**Cipher Algorithm -** Select an algorithm for encrypting the packets via OpenVPN. **HMAC Algorithm -** Select an algorithm for authenticating the packets via OpenVPN.
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**. ● **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.
Tunnel Settings	
Enable IPsec Dial-Out function GRE over IPsec	Check this box to verify data and transmit data in encryption with GRE over IPsec packet after configuring IPsec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.
Logical Traffic	Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPsec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.
Tunnel Local IP	Enter the virtual IP for router itself for verified by peer.
Tunnel Remote IP	Enter the virtual IP of peer host for verified by router.
TCP/IP Network Settings	
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 **Routing**.
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**.

III-1-11 VPN Trunk Management

A VPN Trunk combines TWO LAN-to-LAN VPN tunnels to provide VPN Backup or VPN Load Balance functionalities.

VPN Backup

VPN Backup provides redundant, uninterrupted VPN connectivity by constantly monitoring the health of a VPN tunnel, and fails over to the secondary VPN tunnel when the primary tunnel fails.

In a Backup VPN Trunk, only one of the two LAN-to-LAN VPN tunnels is connected at any given time. When one tunnel fails, the router will automatically start up and direct all VPN traffic destined for the trunk to the other tunnel.

VPN Load Balance

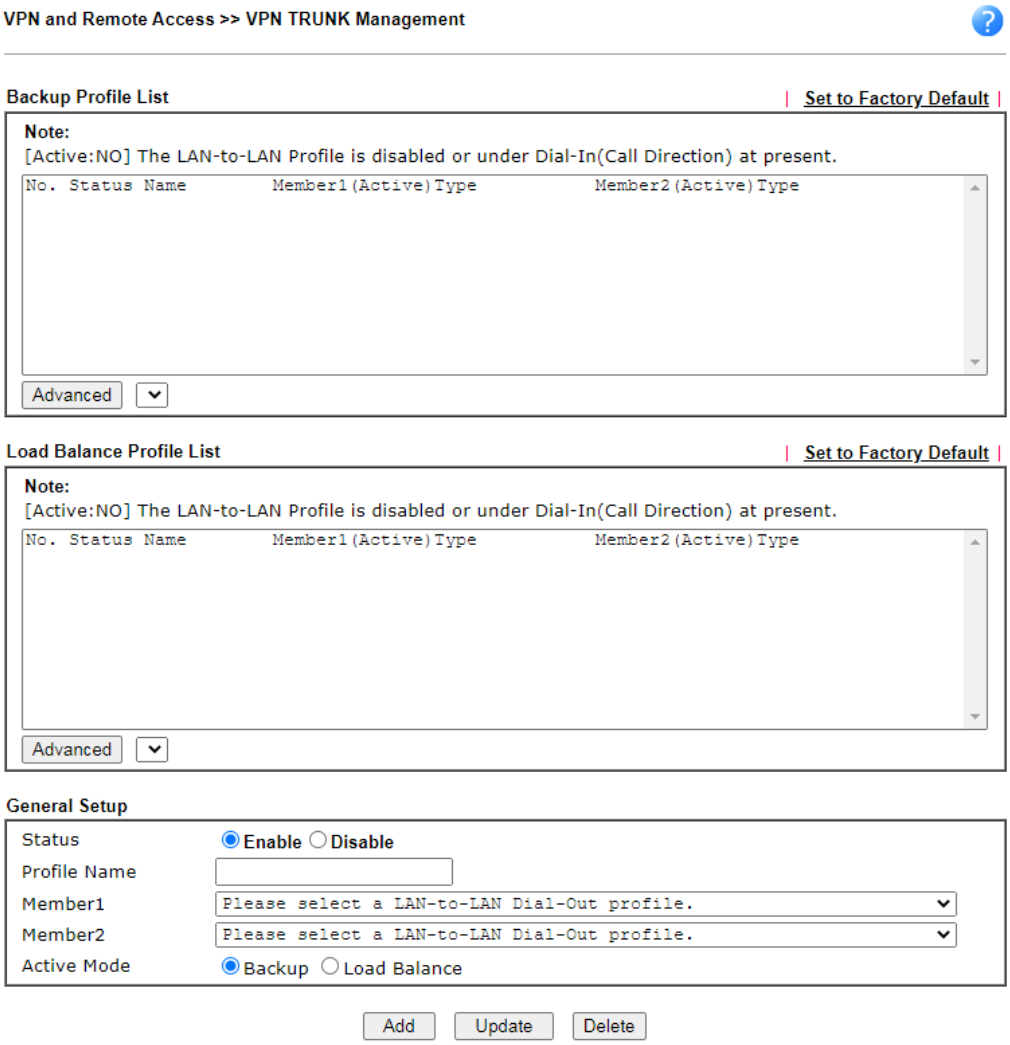
VPN Load Balance increases the bandwidth of a LAN-to-LAN connection by combining and load balancing two tunnels, with the option to direct traffic to specific tunnels by originating address, destination address or port.

In a Load Balance VPN Trunk, both LAN-to-LAN VPN tunnels are simultaneously connected. The router first attempts to match the traffic to a load balance policy rule and send it down the tunnel specified in the matching rule. Traffic not matched to any policy will be load balanced in a round-robin fashion, and the traffic ratio between the two tunnels is either determined automatically by the router or specified by the user.

In order to set up a VPN Trunk, 2 LAN-to-LAN VPN profiles must have been configured first. For details on the configuration of LAN-to-LAN VPN tunnels, see section V-1-10 LAN to LAN. When the 2 LAN-to-LAN VPN profiles are ready, follow the steps below to set up a VPN Trunk.

Creating a VPN Trunk

To create a new VPN Trunk, configure the General Setup section first.

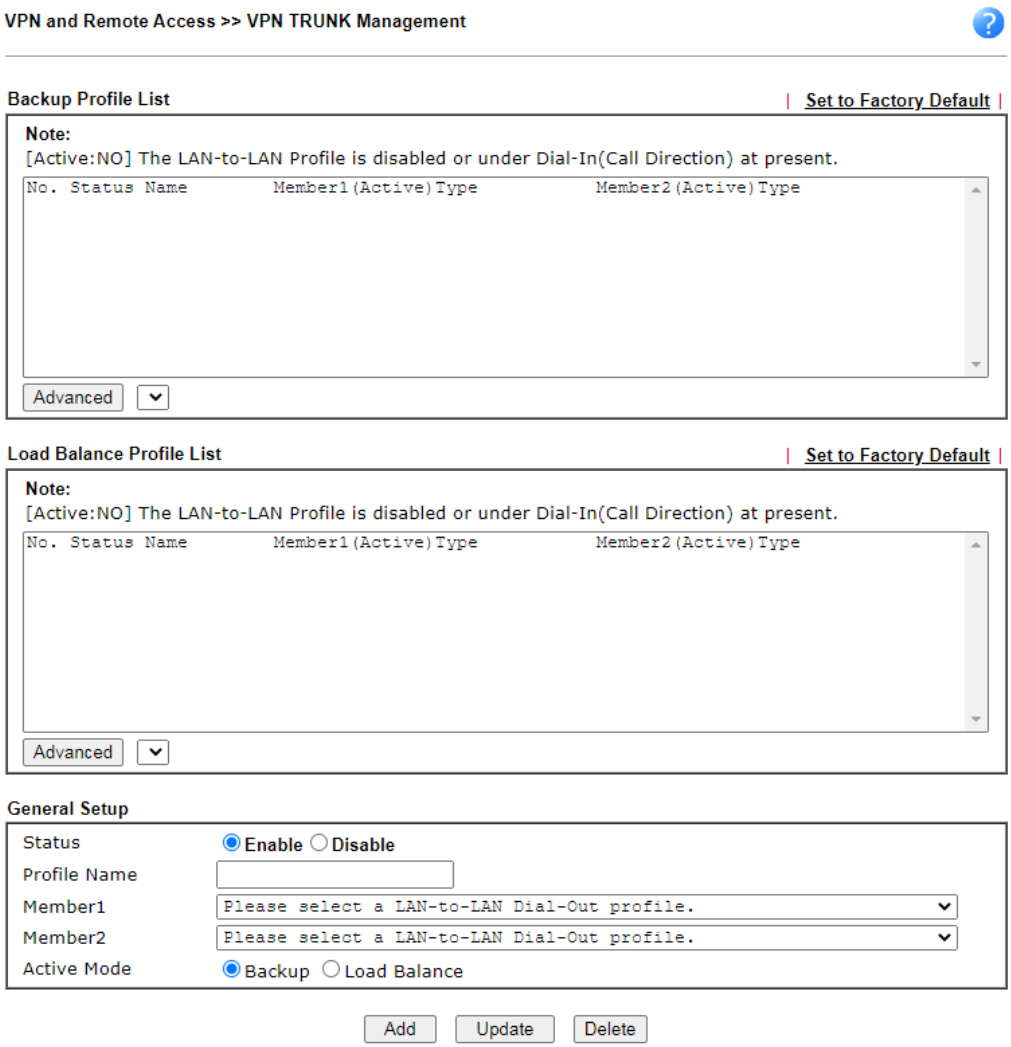


Available settings are explained as follows:

Item	Description
General Setup	**Status** - Enable or disable the VPN Trunk. ● **Enable** – Select this to enable this VPN trunk. ● **Disable** - Select this to disable this VPN trunk. **Profile Name** - Enter a name to identify this VPN Trunk profile. **Member 1/Member2** - Select LAN-to-LAN VPN profiles to be the first and second members of this VPN Trunk. **Active Mode** - Select the operation mode of the VPN Trunk. **Backup / Load Balance** – Select this to set up a Backup / Load Balance VPN Trunk. **Add** - Select it to add a VPN Trunk Profile using the entered information. **Update -** Select it to save the changes to the **Status** (Enable or Disable), profile name, member1 or member2. **Delete -** Select it to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

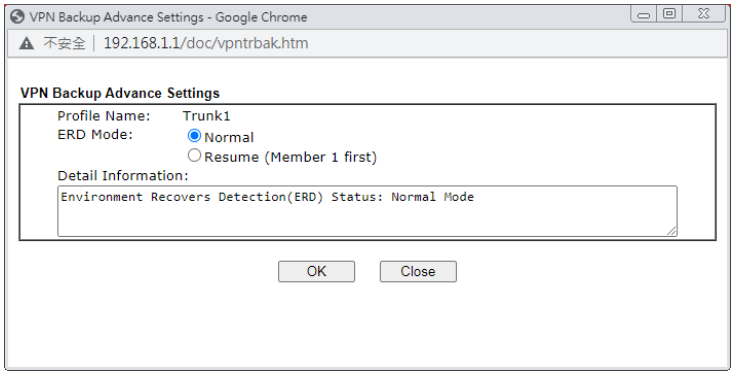
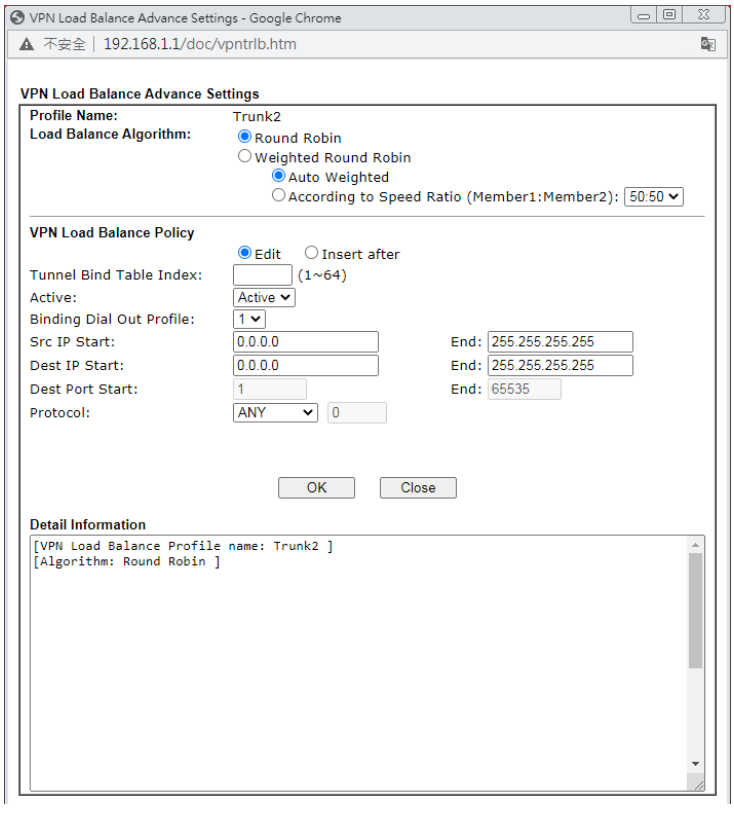
Configuring, Modifying or Deleting a VPN Trunk

To configure or modify a VPN Trunk, go to the Profile List section that corresponds to the type of the VPN trunk (Backup or Load Balance).



Available settings are explained as follows:

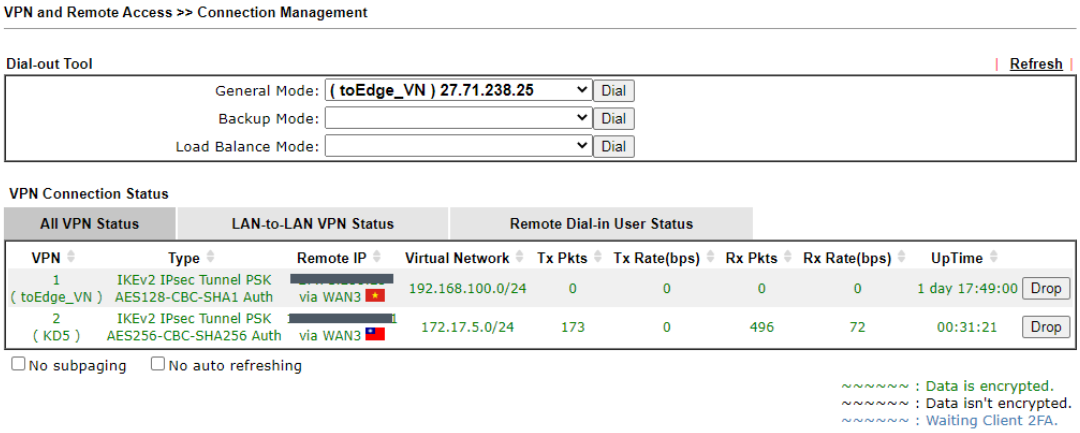
Item	Description
Backup Profile List and Load Balance Profile List	**Set to Factory Default -** Removes all VPN Trunk profiles in the Profile List. **No. –** The index number of VPN profile. **Status** - Shows whether the VPN Trunk is enabled or disabled. ● v – VPN Trunk is enabled. ● x – VPN Trunk is disabled. **Name -** The user-entered name that identifies the trunk profile. **Member1 (Active) Type / Member2 (Active) Type -** Shows the profile index, whether it is enabled or disabled, and the VPN protocol of the 2 LAN-to-LAN VPN profiles. Example: 1(YES)PPTP – the trunk member is set to use the first profile which is currently enabled and uses the PPTP protocol. **Advanced** - To configure advanced settings of a VPN Trunk

	profile, select its name from the dropdown list and click Advanced.
Advanced for Backup Profile List	If a Backup Profile was selected, the following Advanced Settings screen appears:  **Profile Name** - User-defined name that identifies this profile. **ERD Mode** - Sets the Environment Recovery Detection (ERD) mode. ● **Normal** – Both VPN tunnels have equivalent priority. ● **Resume** – Member 1 and Member 2 VPN tunnels are primary and secondary connections, respectively. The router will always attempt to use Member 1 first, and only fail over to Member 2 if Member 1 is down. **Detail Information** - Provides a detailed explanation of the ERD mode. To save Advanced Settings for the profile, select **OK**; to close without saving changes, select **Close**.
Advanced for Load Balance Profile List	If a Load Balance Profile was selected, the following Advanced Settings screen appears:  **Profile Name** - User-defined name that identifies this

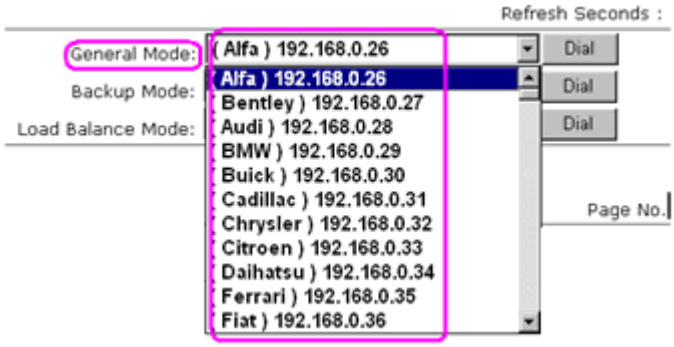
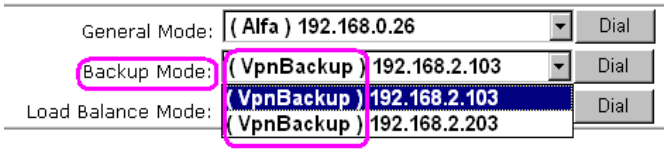
	profile. **Load Balance Algorithm** - Configures how load balancing is performed. ● **Round Robin** – All outgoing connections that do not match to any load balance policy are evenly distributed between the tunnels. ● **Weighted Round Robin** -- All outgoing connections that do not match to any load balance policy are distributed between the tunnels based on a ratio that is either automatically determined by the router (Auto Weighted), or specified by the user (According to Speed Ratio). **VPN Load Balance Policy** - This section allows the modification or addition of load balance policy profiles. **Edit / Insert After** - Select Edit to modify the existing load balance profile with index specified in Tunnel Bind Table Index, or Insert After to insert a new load balance profile immediately after the index position specified in Tunnel Bind Table Index. **Tunnel Bind Table Index**- 64 Binding tunnel tables are provided by this device. In Edit mode, the profile that matches this index will be updated. In Insert After mode, a new profile will be inserted immediately after the policy having this index. **Active** – Includes Active and Clear. In which, ● **Active** - All information will be saved into a load balance profile. ● **Clear** – The profile with index matching Tunnel Bind Table Index will be deleted. **Binding Dial Out Profile** – The LAN-to-LAN VPN tunnel to which traffic matching this policy will be sent. **Scr IP Start /End**– Specify source IP addresses as starting point and ending point. **Dest IP Start/End** – Specify the target IP addresses as starting point and ending point. **Dest Port Start /End**– Specify the target port range if the protocol is TCP or UDP. **Protocol** – Specify the protocol of the traffic. **Detail Information** - Shows all the information about the Load Balance profile. To save Advanced Settings for the profile, select **OK**; to close without saving changes, select **Close**.
Add	Select it to add a VPN Trunk Profile using the entered information.
Update	Make modifications as necessary in the General Setup section. Select it to save the changes to the Status (Enable or Disable), profile name, member1 or member2.
Delete	Select it to remove the VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

III-1-12 Connection Management

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



Available settings are explained as follows:

Item	Description
Refresh	Click to manually reload the page to refresh VPN connection information.
Dial-out Tool	The Dial-out Tool section can be used to initiate outgoing LAN-to-LAN VPN sessions. **General Mode -** It lists all LAN-to-LAN VPN profiles that do not belong to enabled VPN Trunk profiles. To manually dial a LAN-to-LAN VPN profile, select it from the combo box, and click the **Dial** button to the right. The VPN connection built by General Mode does not support VPN backup function.  **Backup Mode -** It lists all Backup VPN Trunk profiles. To manually dial a Backup VPN Trunk profile, select it from the combo box, and click the **Dial** button to the right. The VPN connection built by Backup Mode supports VPN backup function.  **Load Balance Mode -** It lists all Load Balance VPN Trunk profiles. To manually dial a Load Balance VPN Trunk profile,

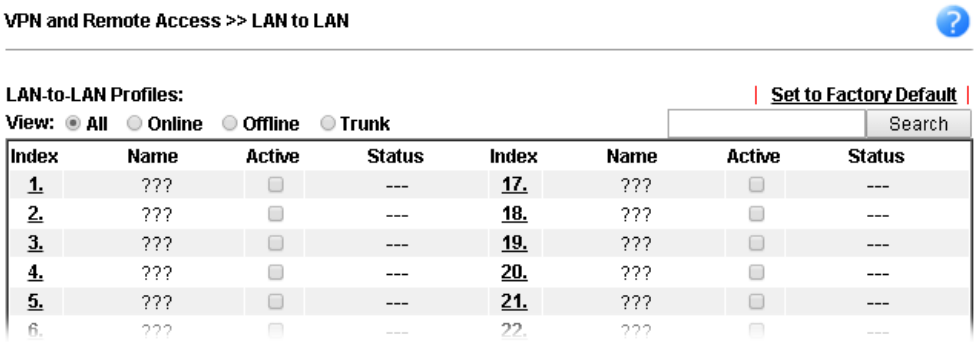
	select it from the combo box, and click the **Dial** button to the right. **Dial -** Click this button to execute dial out function. If the connect is successfully made, it will show up in the VPN Connection Status section below.
VPN Connection Status	**VPN** - Displays the VPN profile number and the 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.

Application Notes

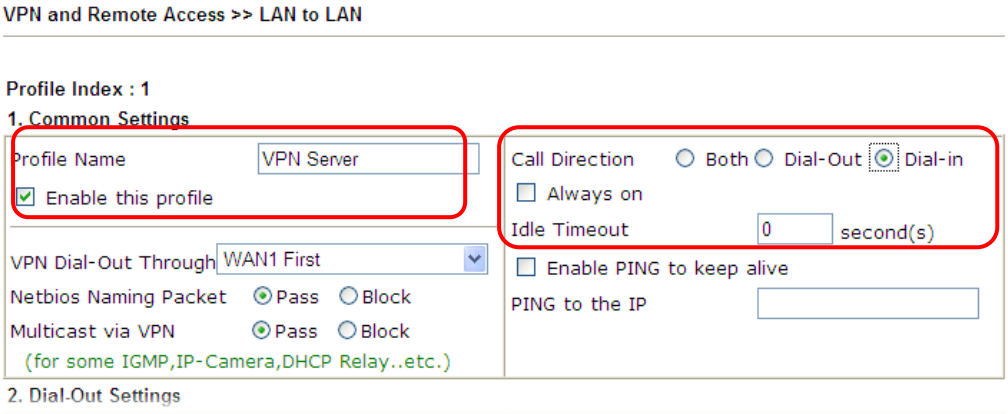
A-1 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tunnel (Main Mode)

Configuration on Vigor Router for Head Office

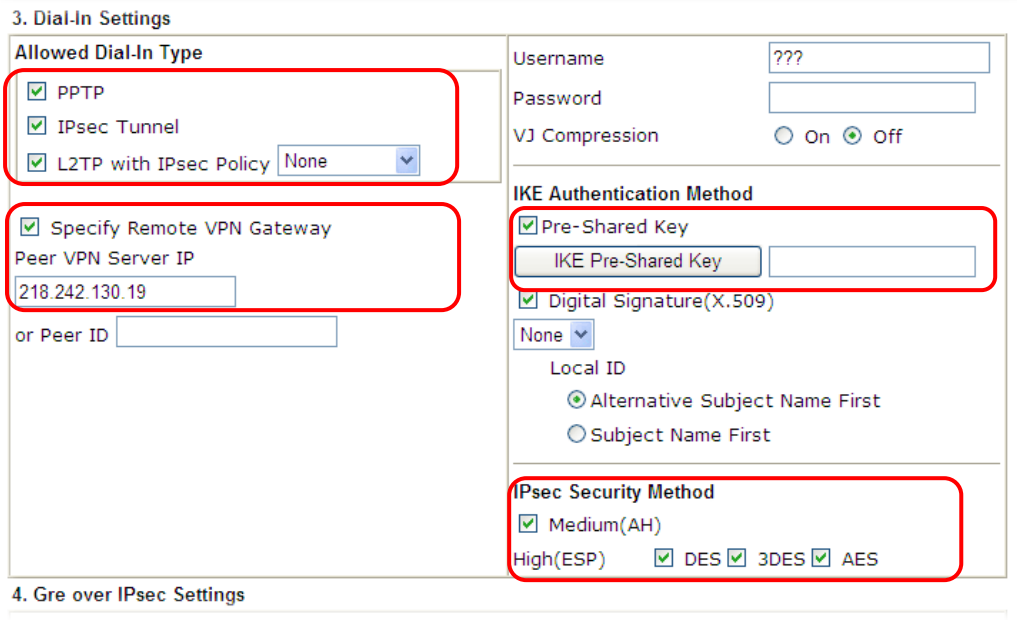
1. Log into the web user interface of Vigor router.
2. Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.



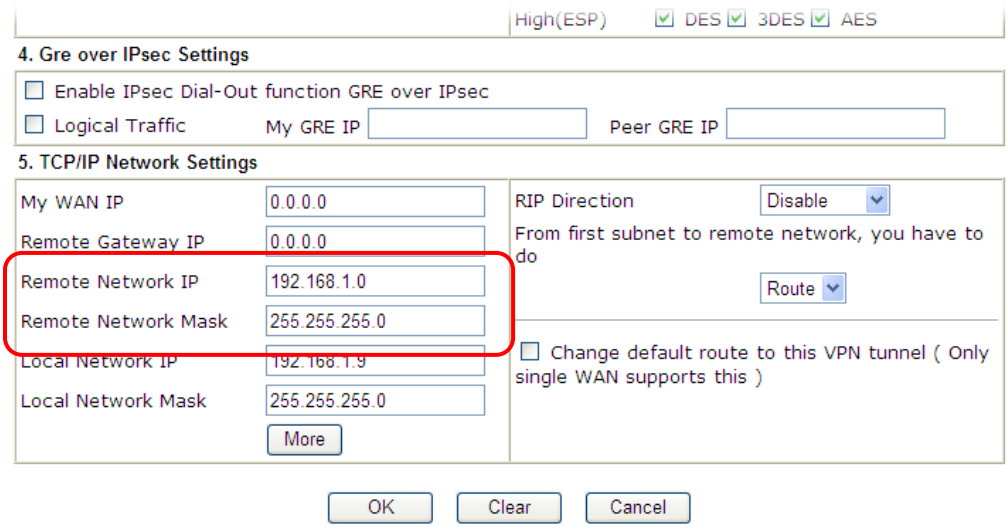
3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Server*)**,** and check the box of **Enable This Profile**. For Vigor router will be set as a **server**, the call direction shall be set as **Dial-in** and set 0 as **Idle Timeout**.



4. Now navigate to the next section, **Dial-In Settings** to check PPTP, IPsec Tunnel and L2TP boxes. Check the box of **Specify Remote...** and type the **Peer VPN Server IP** (e.g., 218.242.130.19 in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

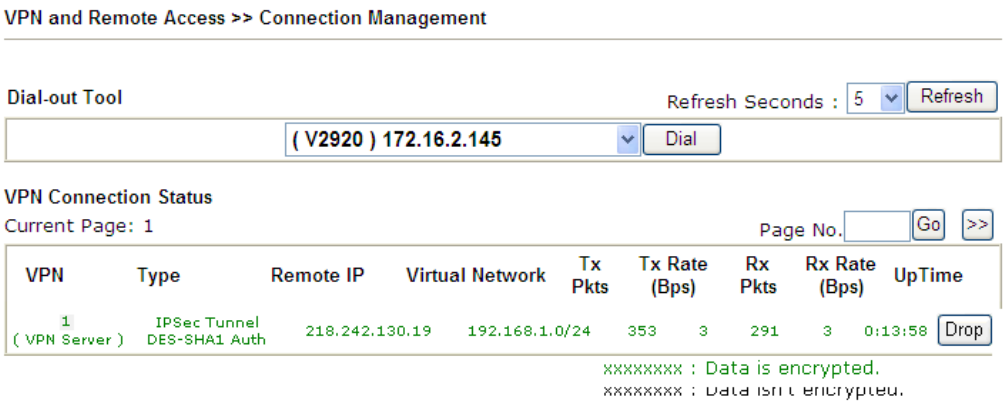


5. Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for remote side.



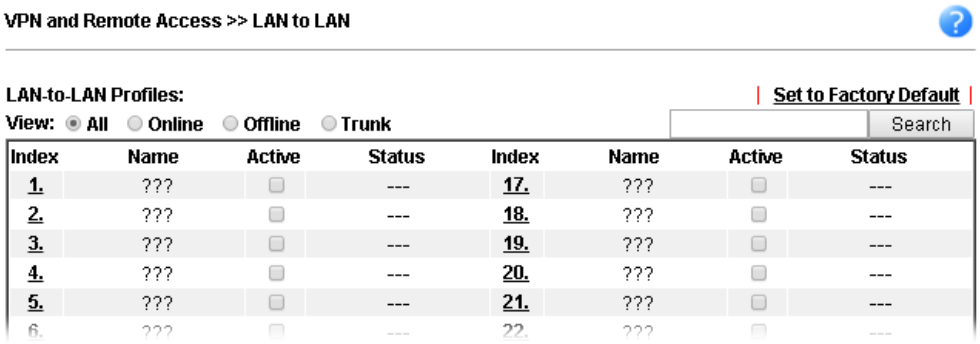
6. Click **OK** to save the settings.

7. Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from branch office).

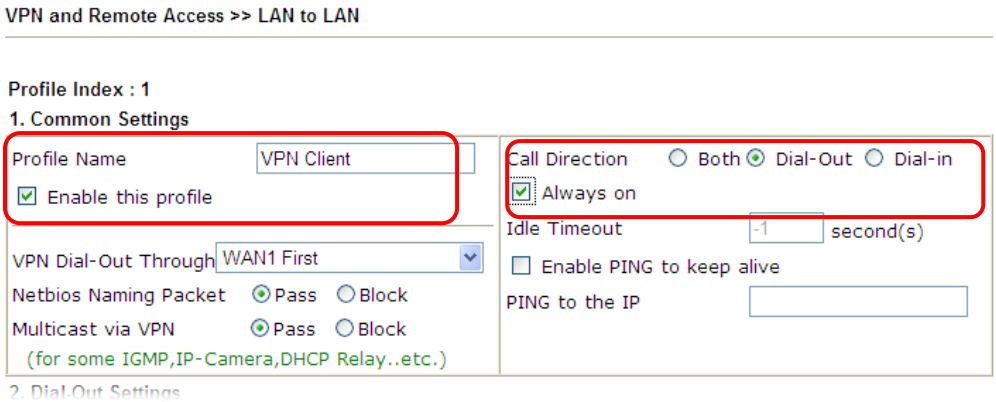


Configuration on Vigor Router for Branch Office

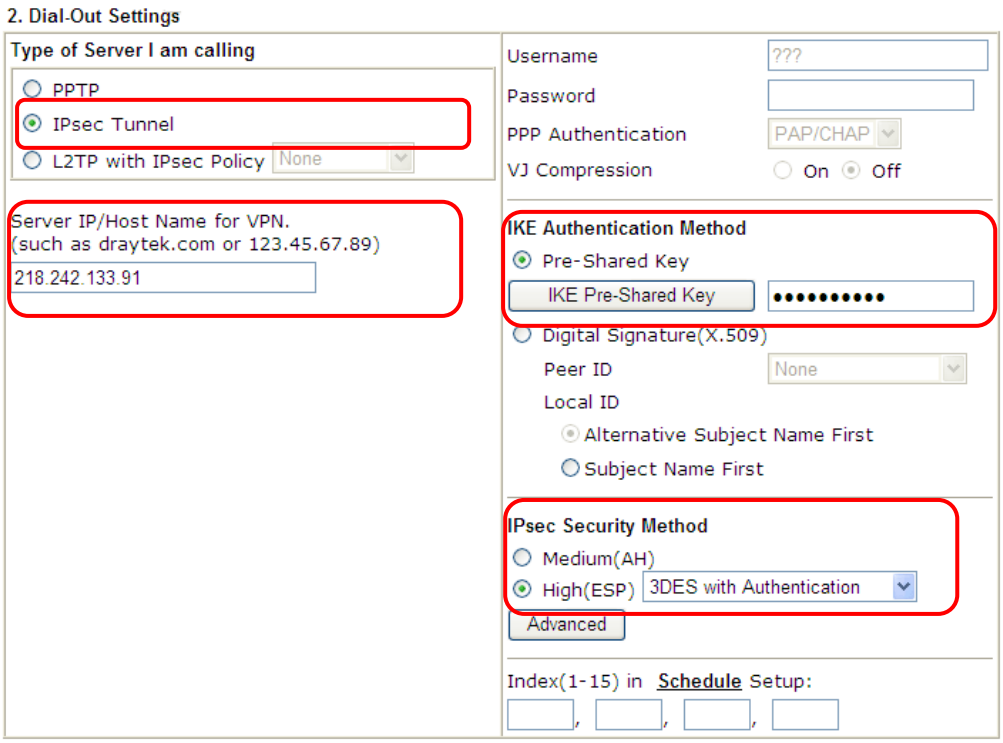
1. Log into the web user interface of Vigor router.
2. Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.



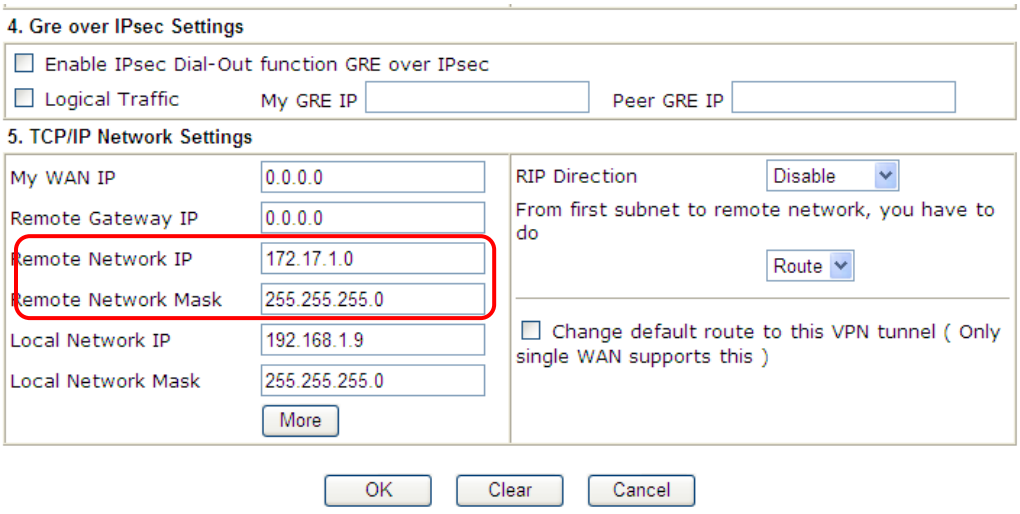
3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Client*)**,** and check the box of **Enable This Profile**. For such Vigor router will be set as a **client**, the call direction shall be set as **Dial-out.** Check the box of **Always on** for a permanent VPN connection.



4. Now navigate to the next section, **Dial-Out Settings** to select the **IPsec Tunnel** service and type the remote server IP/host name (e.g., 218.242.133.91, in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

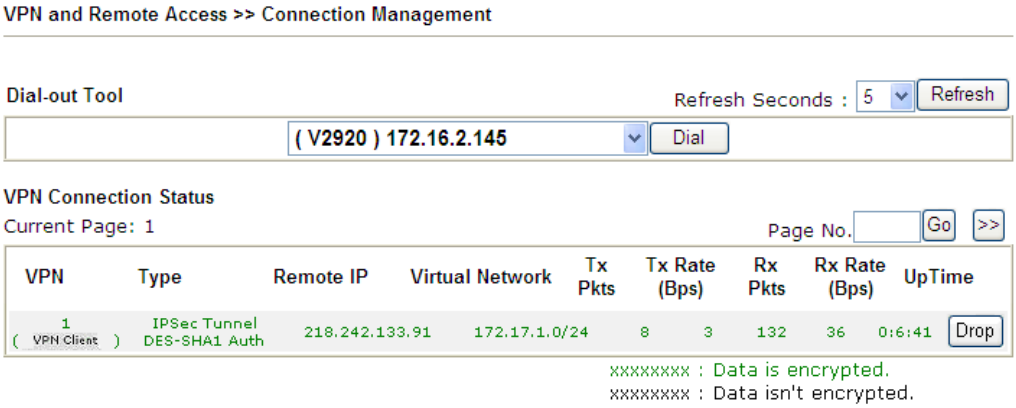


5. Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for the remote side.



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

7. Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from head office).



III-2 Certificate Management

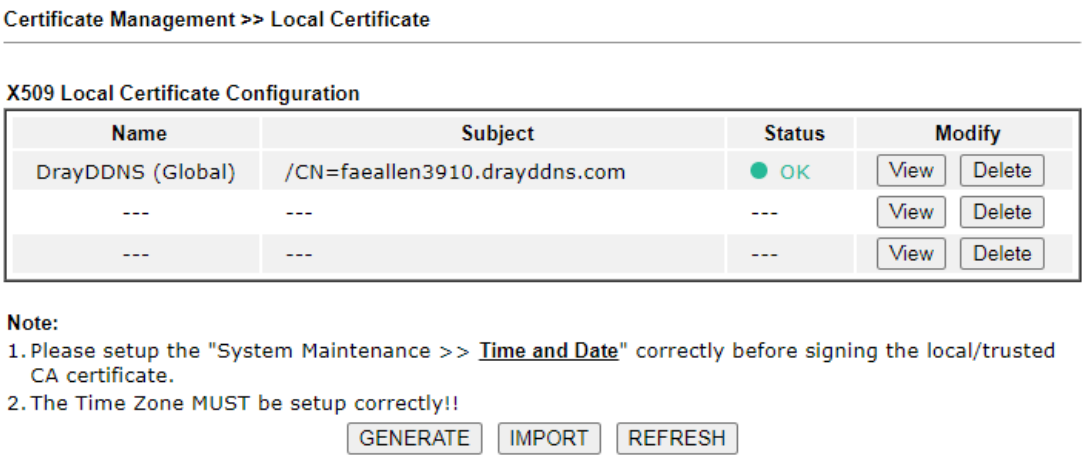
A digital certificate is an electronic document issued by a certification authority (CA) to an entity to prove ownership of a public key. It contains identifying information including the issued-to party's name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing 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

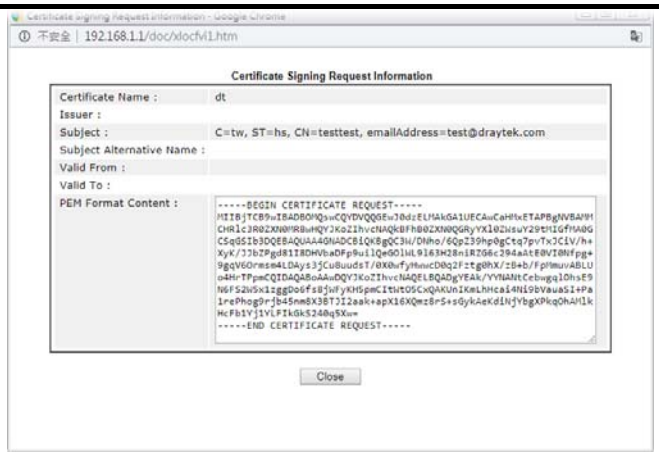
III-2-1 Local Certificate

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



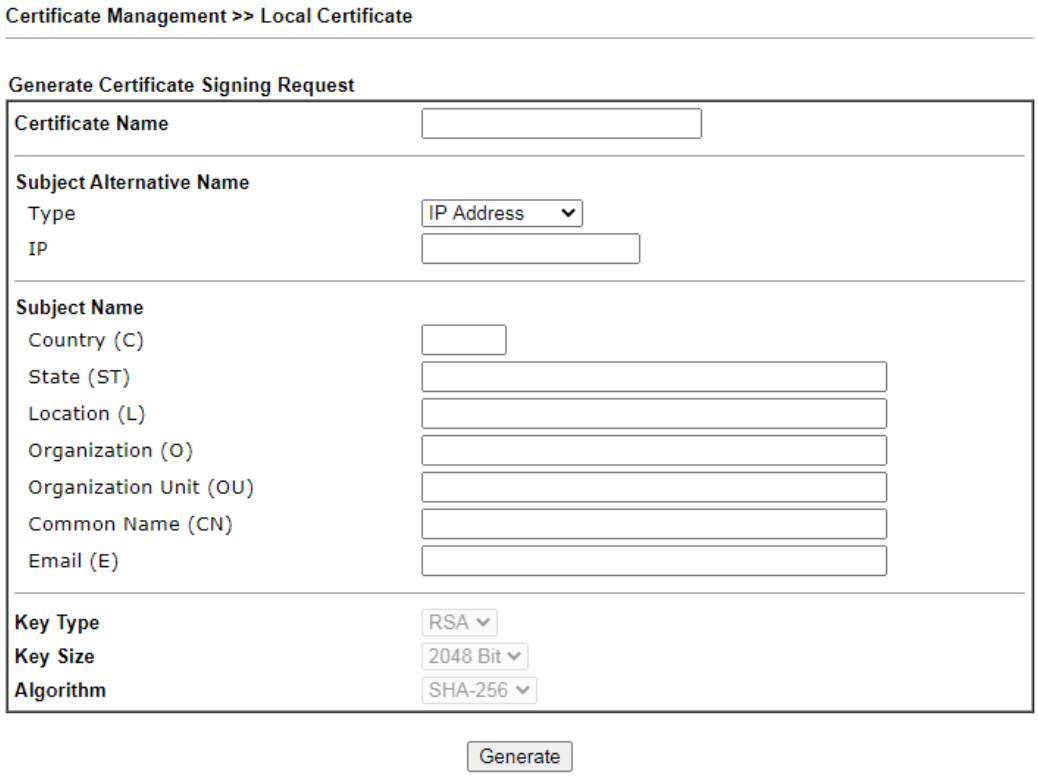
Available settings are explained as follows:

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.



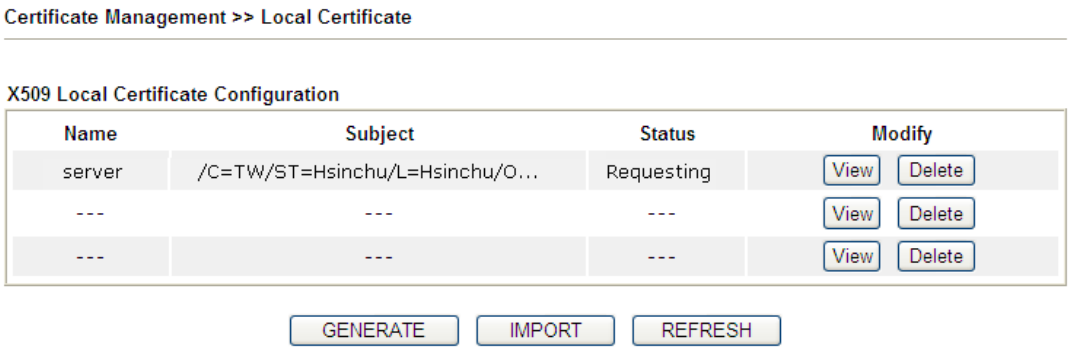
Available settings are explained as follows:

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.

Info	Please be noted that “Common Name” must be configured with rotuer’s WAN IP or domain name.

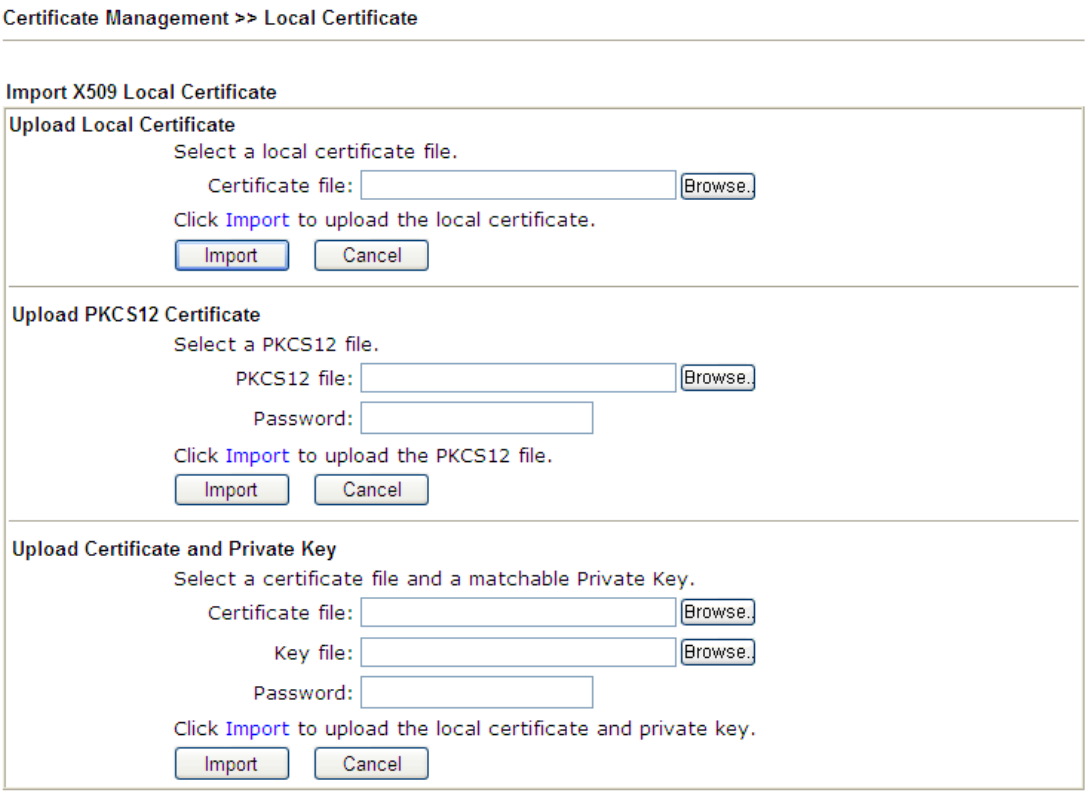
After clicking the **Generate** button, you will be taken back to the main Local Certificate screen, showing the certificate request in progress:



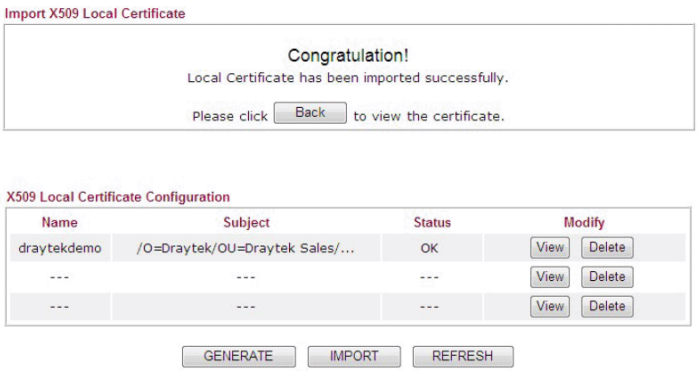
IMPORT

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.

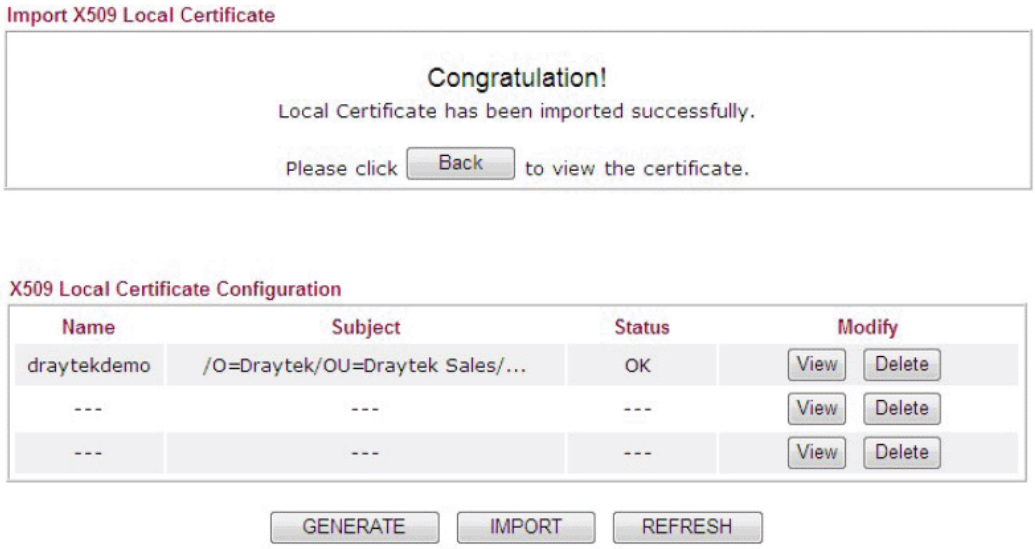


Available settings are explained as follows:

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.

III-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.

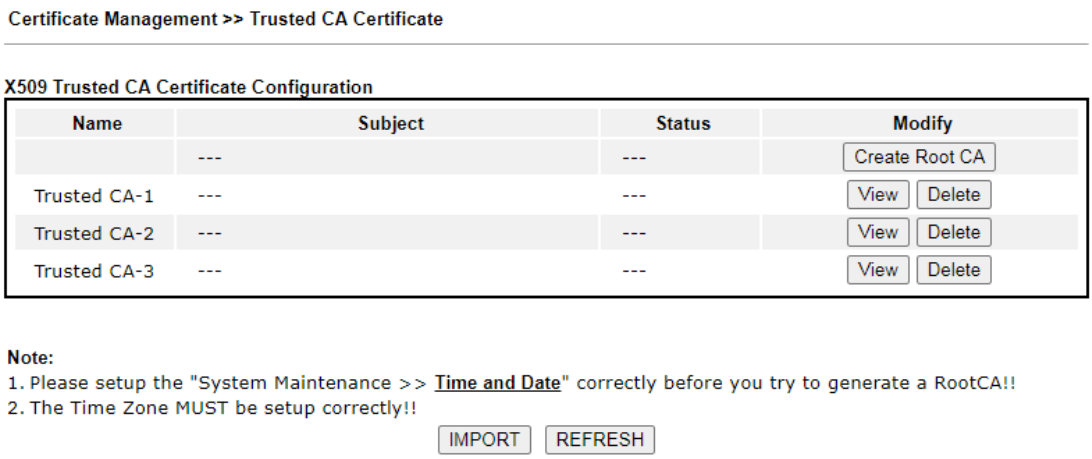
When the local client and remote client are required to make certificate authentication (e.g., IPsec X.509) for data passing through SSL tunnel and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

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

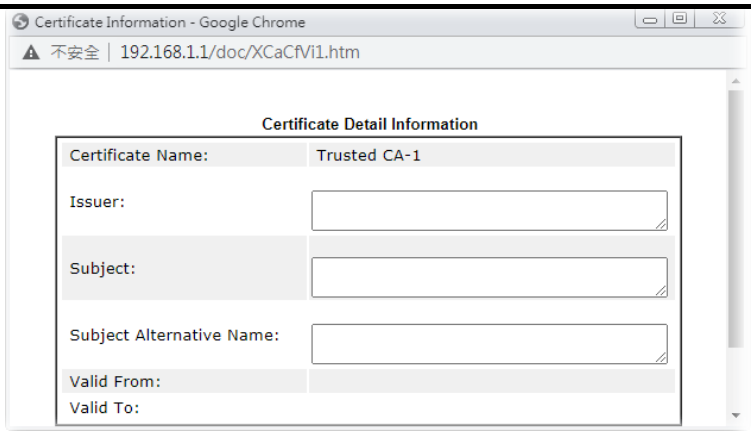
Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.

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



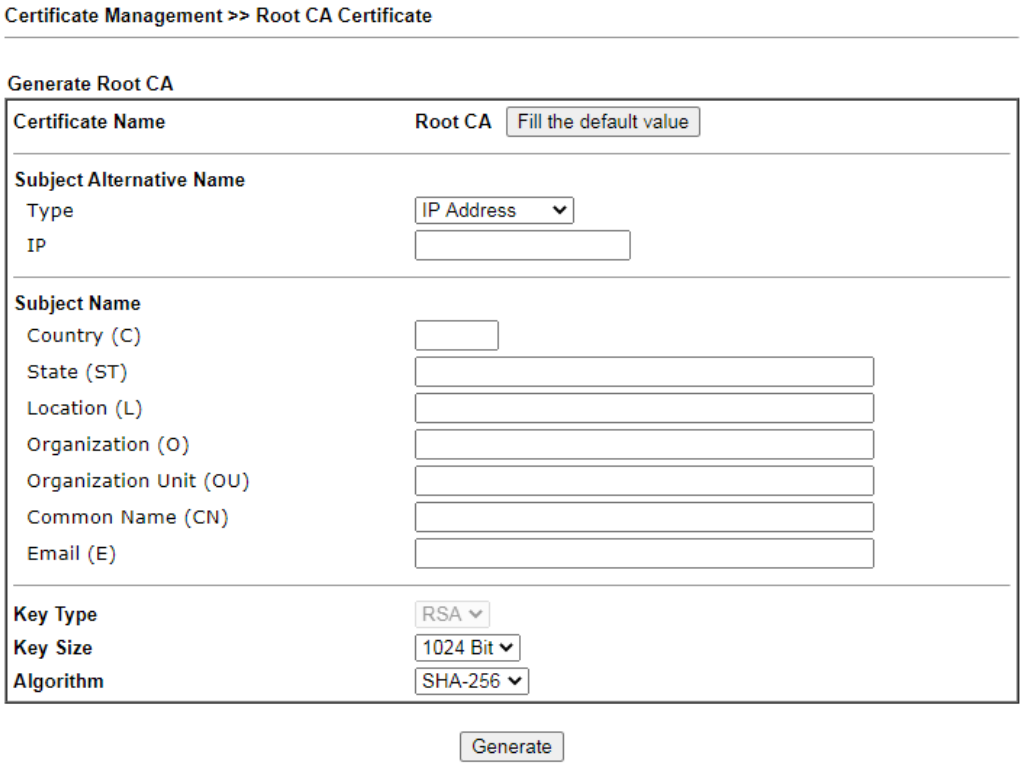
Available settings are explained as follows:

Item	Description
Name	Name that identifies the certificate.
Subject	Shows the Subject Name of the certificate.
Status	Displays the status of the certificate.
Modify	**Create Root CA -** 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 RootCA

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

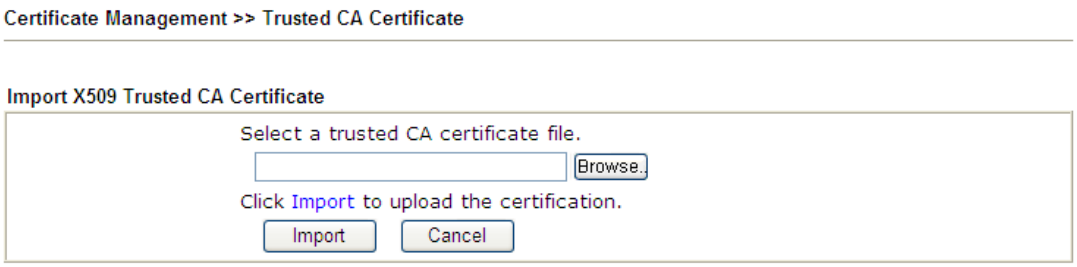


Available settings are explained as follows:

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.

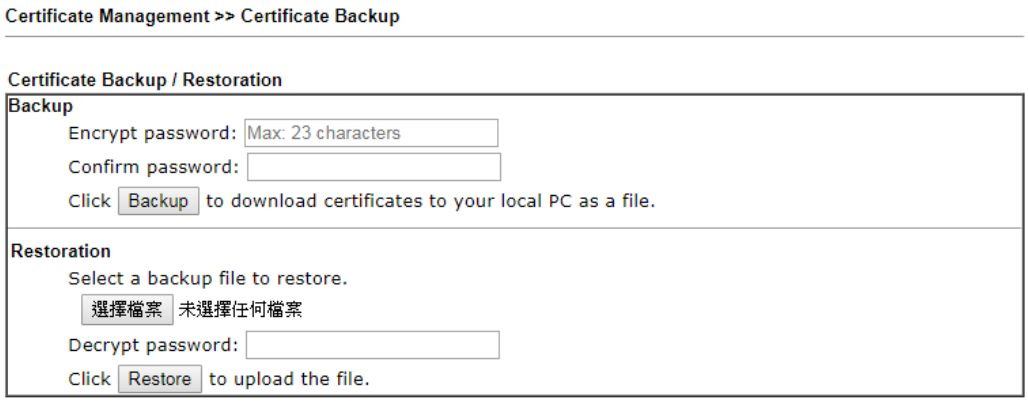


Available settings are explained as follows:

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.

III-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:

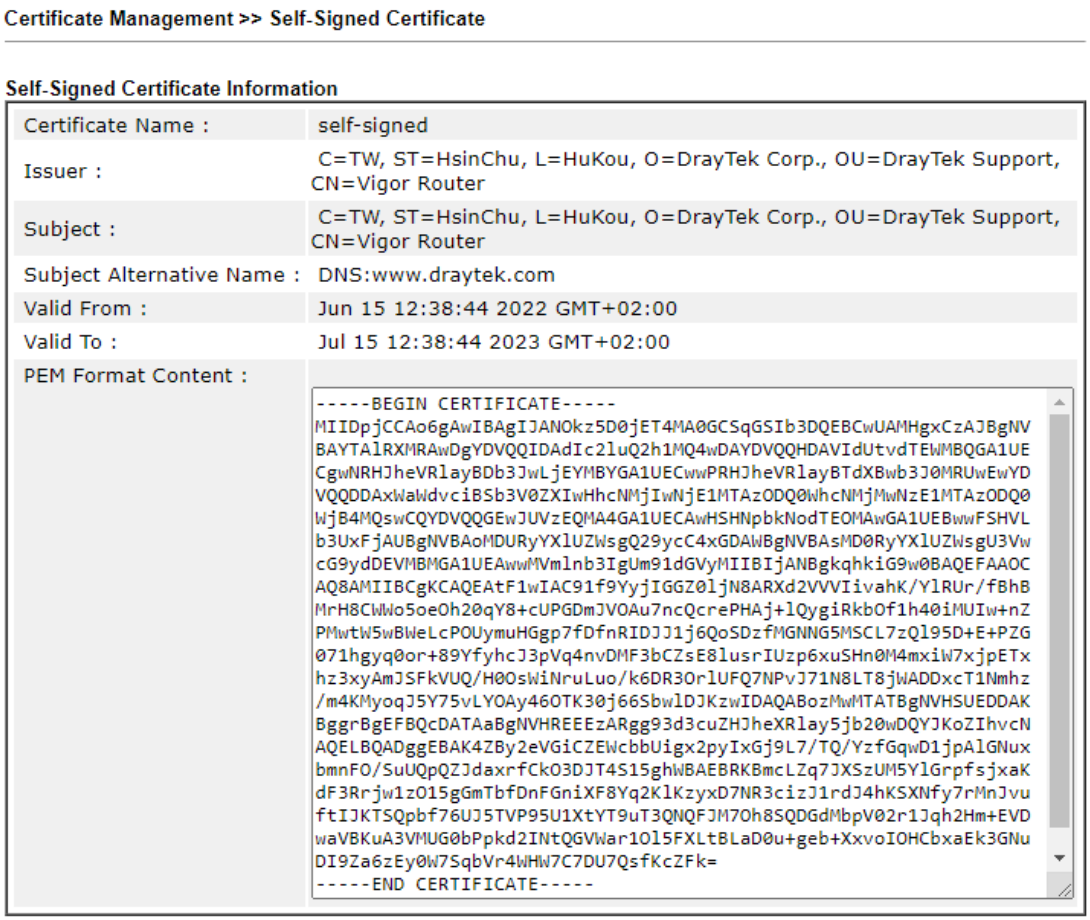
Item	Description
Backup	
Encrypt password / Confirm password	Enter the password with which you wish to encrypt the certificate.
Backup	Click to download the certificate.
Restoration	
Select a backup file to restore	Click Browse to select the backup file you wish to restore.

Decrypt password	Enter the password that was used to encrypt the certificates.
Restore	Click to retrieve the certificate.

III-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.



Certificate Management >> 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 :	DNS:www.draytek.com
Valid From :	Jun 15 12:38:44 2022 GMT+02:00
Valid To :	Jul 15 12:38:44 2023 GMT+02:00
PEM Format Content :	-----BEGIN CERTIFICATE----- MIIDpjCCAo6gAwIBAgIJANOkz5D0jET4MA0GCSqGSIb3DQEBCwUAMHgxCzAJBgNV BAYTAlRXMRAwDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvdTEWMBQGA1UE CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBwb3J0MRUwEwYD VQQDDAxWaWdvciBSb3V0ZXIwHhcNMjIwNjE1MTAzODQ0WhcNMjMwNzE1MTAzODQ0 WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVL b3UxFjAUBgNVBAoMDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsMD0RyYXlUZWsgU3Vw cG9ydDEVMBMGA1UEAwwMVmlnb3IgUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAtF1wIAC91f9YyjIGGZ0ljN8ARXd2VVVIivahK/YlRUr/fBhB MrH8CWWo5oeOh20qY8+cUPGDmJVOAu7ncQcrePHAj+lQygiRkbOf1h40iMUIw+nZ PMwtW5wBWeLcPOUymuHGgp7fDfnRIDJJ1j6QoSDzfMGNNG5MSCL7zQl95D+E+PZG 071hgyq0or+89YfyhcJ3pVq4nvDMF3bCZsE8lusrIUzp6xuSHn0M4mxiW7xjpETx hz3xyAmJSFkVUQ/H0OsWiNruLuo/k6DR3OrlUFQ7NPvJ71N8LT8jWADDxcT1Nmhz /m4KMyoqJ5Y75vLYOAy46OTK30j66SbwlDJKzwIDAQABozMwMTATBgNVHSUEDDAK BggrBgEFBQcDATAaBgNVHREEEzARgg93d3cuZHJheXRlay5jb20wDQYJKoZIhvcN AQELBQADggEBAK4ZBy2eVGiCZEWcbbUigx2pyIxGj9L7/TQ/YzfGqwD1jpAlGNux bmnFO/SuUQpQZJdaxrfCkO3DJT4S15ghWBAEBRKBmcLZq7JXSzUM5YlGrpfsjxaK dF3Rrjw1zO15gGmTbfDnFGniXF8Yq2KlKzyxD7NR3cizJ1rdJ4hKSXNfy7rMnJvu ftIJKTSQpbf76UJ5TVP95U1XtYT9uT3QNQFJM7Oh8SQDGdMbpV02r1Jqh2Hm+EVD waVBKuA3VMUG0bPpkd2INtQGVWar1Ol5FXLtBLaD0u+geb+XxvoIOHCbxaEk3GNu DI9Za6zEy0W7SqbVr4WHW7C7DU7QsfKcZFk= -----END CERTIFICATE-----

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 IV Security

Firewall

CSM

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 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.

IV-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

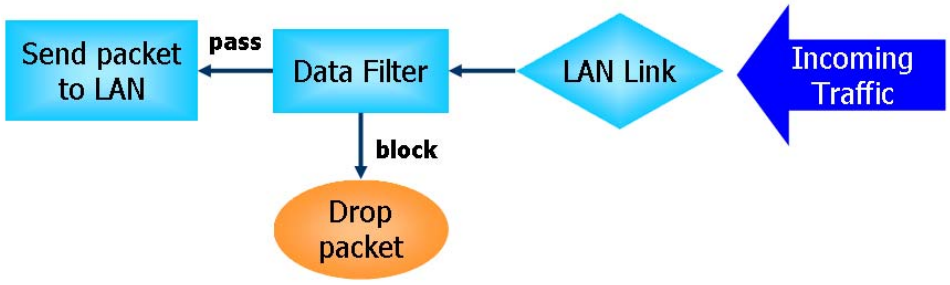
LAN users are provided with secured protection by the following firewall facilities:

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

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.

The following flowcharts show how the router treats incoming traffic and outgoing traffic respectively.



Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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.

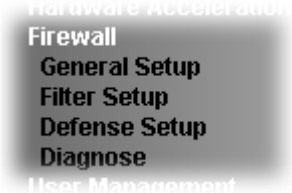
Vigor's DoS Defense functionality detects DoS attacks and mitigates their damage by inspecting every incoming packet, and malicious packets will be blocked. If Syslog is enabled, alert messages will also be sent. Abnormal traffic flow such as flood and port scan attacks that exceed allowable thresholds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

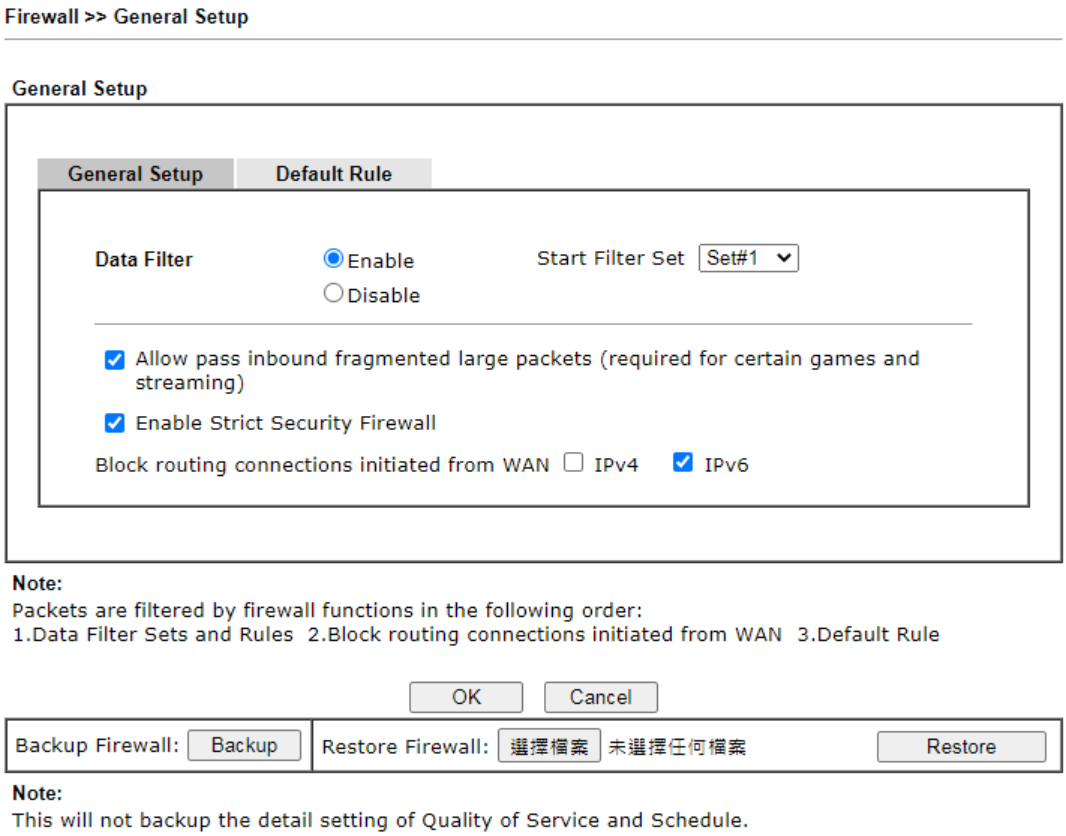
Below shows the menu items for Firewall.



IV-1-1 General Setup

General Setup Page

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



Available settings are explained as follows:

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

Allow pass inbound fragmented large…	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**.

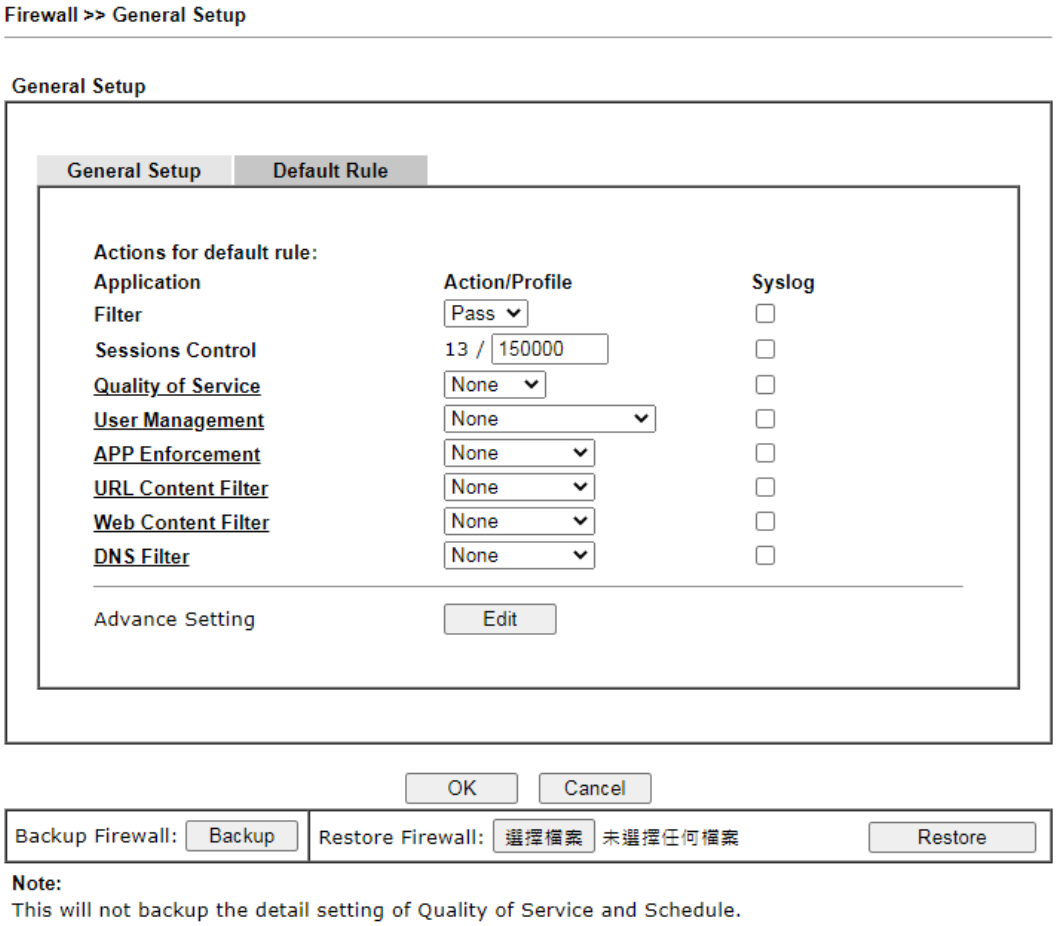
Traffic is filtered by firewall functions in the following order:

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

Default Rule Page

This page allows you to choose filtering profiles including QoS, User Management, APP Enforcement, URL Content Filter, Web Content Filter and DNS Filter for data transmission via Vigor router.

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



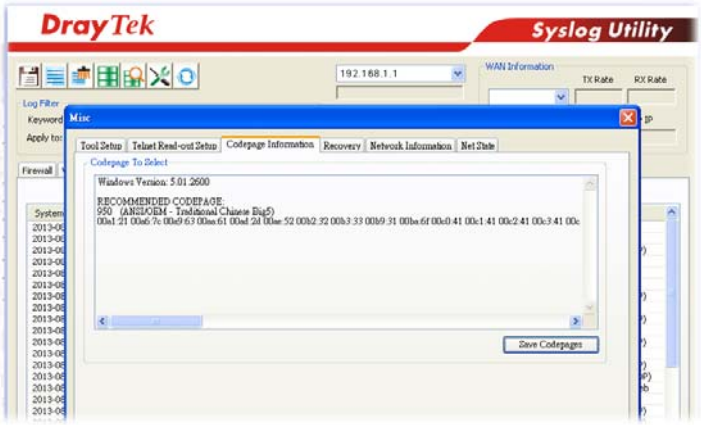
Available settings are explained as follows:

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.



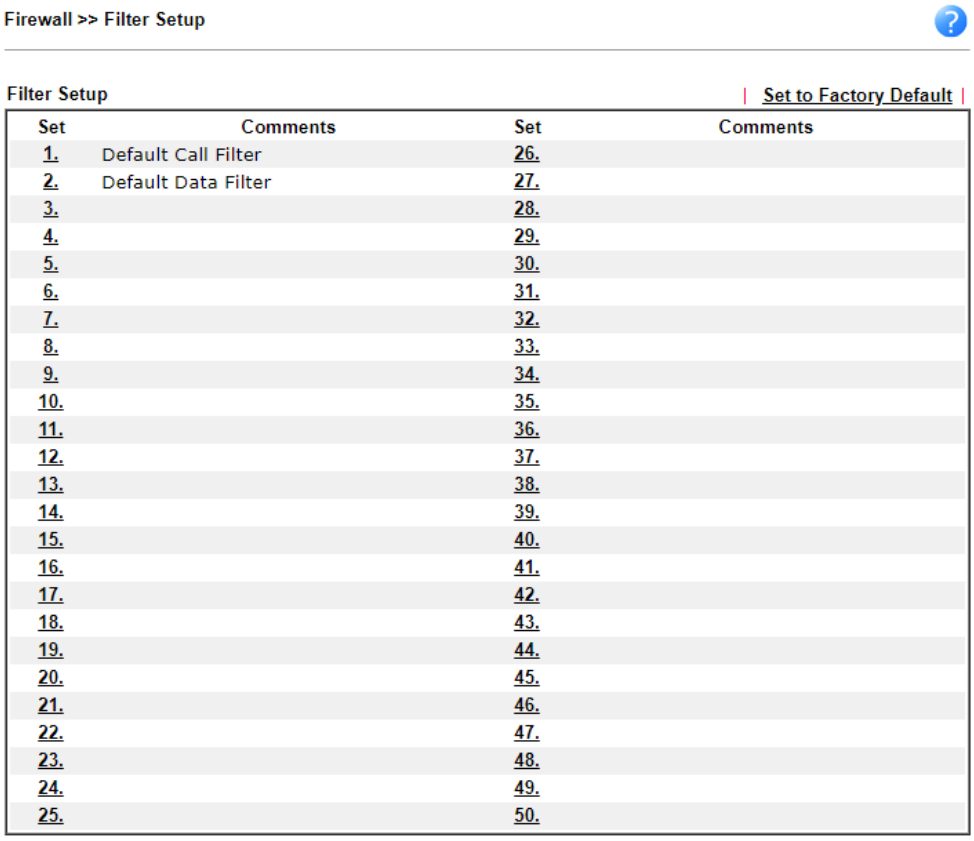
Window size – Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 65535. The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

Session timeout – Sets the timeout sessions are allowed to idle before they are removed from the system.

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

IV-1-2 Filter Setup

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

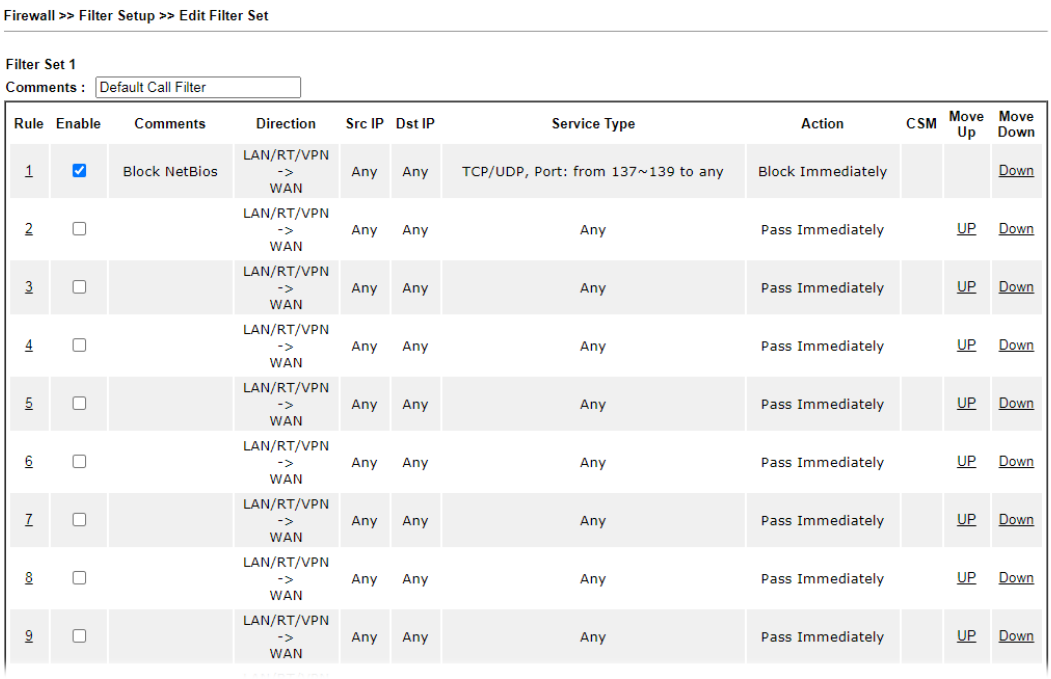


Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

Set	Comments	Set	Comments
1.	Default Call Filter	26.	
2.	Default Data Filter	27.	
3.		28.	
4.		29.	
5.		30.	
6.		31.	
7.		32.	
8.		33.	
9.		34.	
10.		35.	
11.		36.	
12.		37.	
13.		38.	
14.		39.	
15.		40.	
16.		41.	
17.		42.	
18.		43.	
19.		44.	
20.		45.	
21.		46.	
22.		47.	
23.		48.	
24.		49.	
25.		50.	

To edit a filter set, click on its set number. The following Filter Set page will be shown. Each filter set contains up to 30 rules.



Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments : Default Call Filter

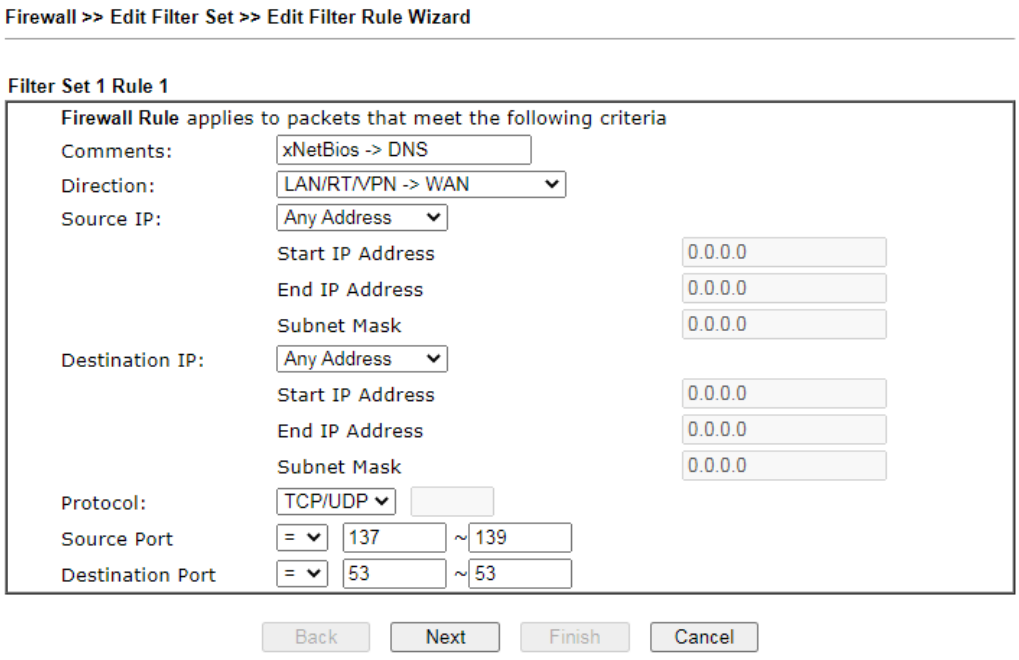
Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	☑	Block NetBios	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to any	Block Immediately			Down
2	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
8	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
9	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down

Available settings are explained as follows:

Item	Description
Rule	To edit the filter rule, click the filter rule number (1 ~ 30) 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.

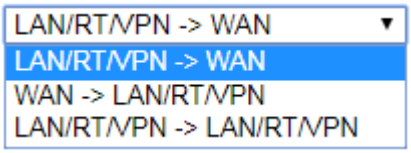
To use Wizard Mode, simple do the following steps:

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

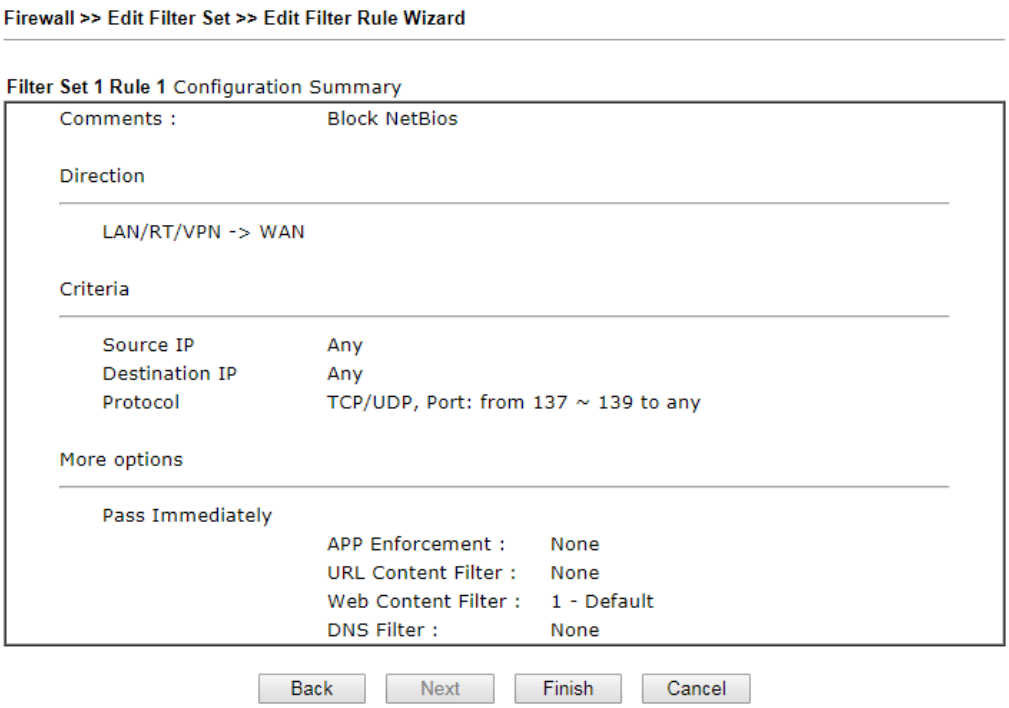
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Direction	Set the direction of packet flow.  **Note:** RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type 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.
Block Immediately	Packets matching the rule will be dropped immediately.

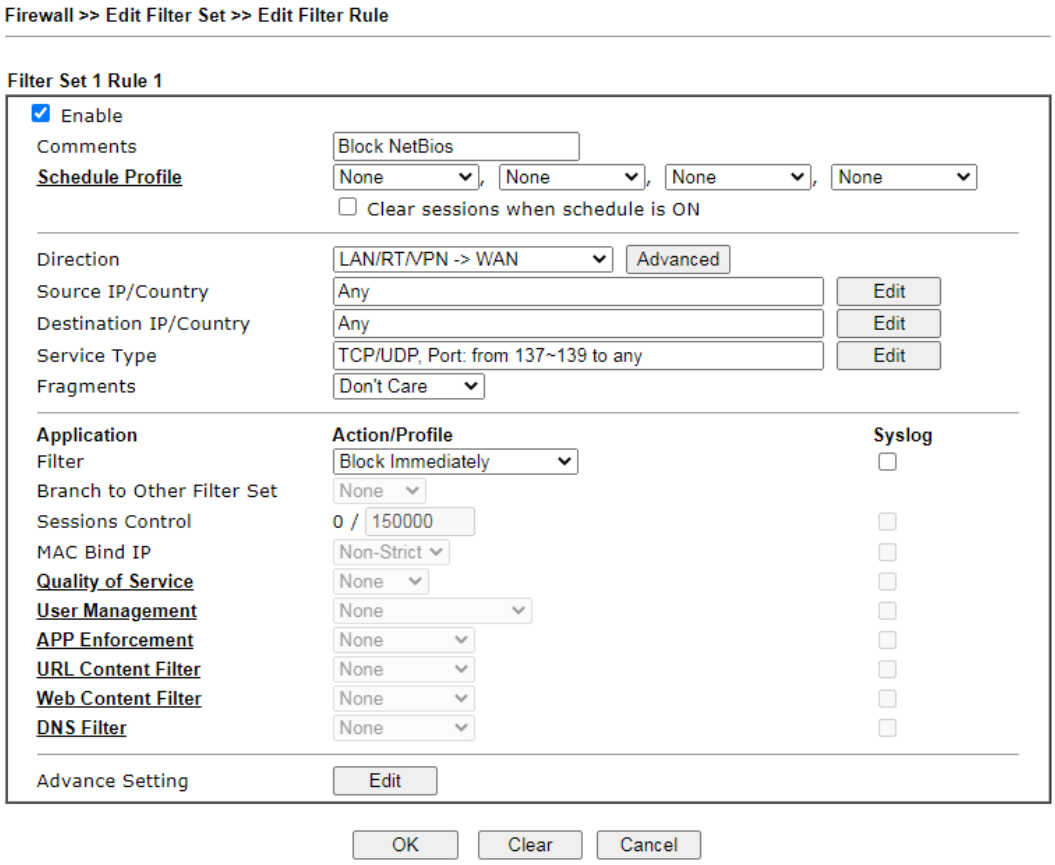
4. After choosing the mechanism, click **Next** to get the summary page for reference.



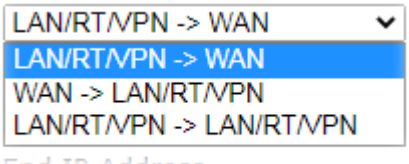
5. If there is no error, click **Finish** to complete wizard setting.

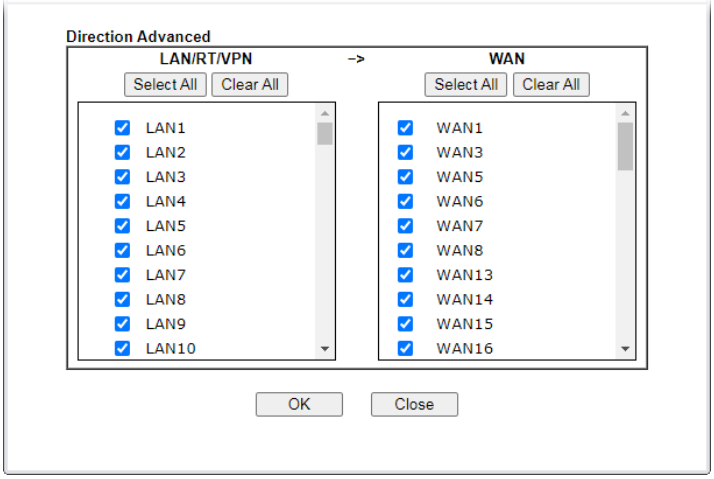
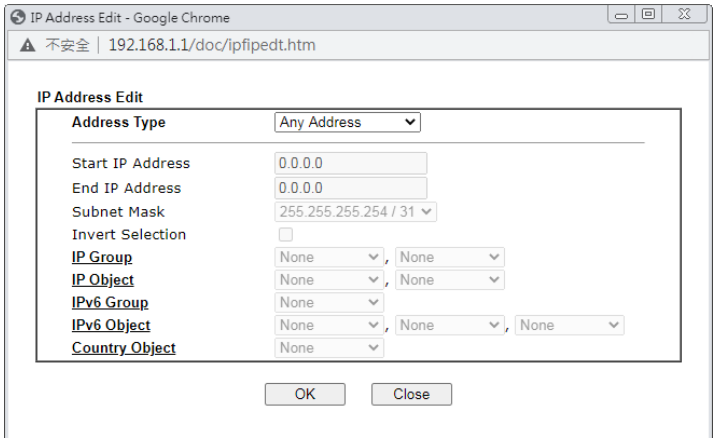
To use **Advance** Mode, do the following steps:

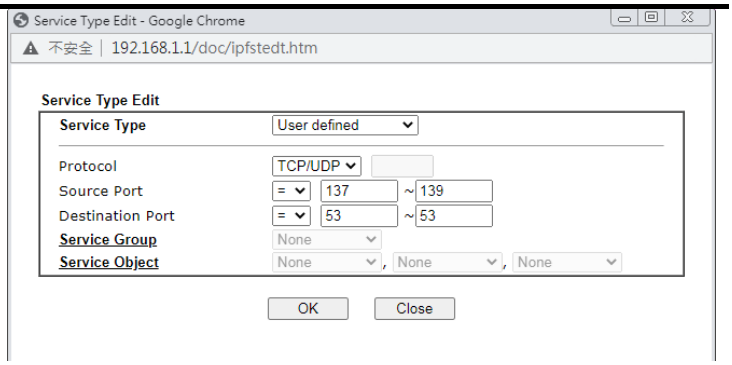
1. Click the **Advance Mode** radio button.
2. Click **Index 1** to access into the following page.



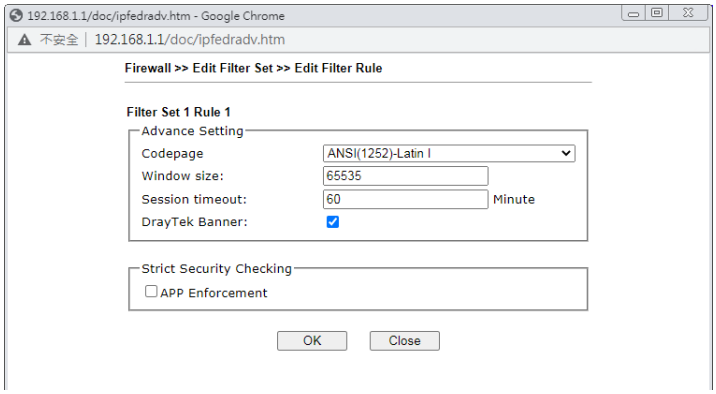
Available settings are explained as follows:

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 is ON	Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset.
Direction	Specify the direction of traffic flow to which this filter rule applies. Note that when the rule belongs to the Call Filter, the WAN -> LAN/RT/VPN option has no effect as Call Filter applies only to outgoing traffic. 

	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. 
Source IP/ Country and Destination IP / Country	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.
Service Type	Click **Edit** to bring up the following dialog box to configure the Service Type.

	 **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.

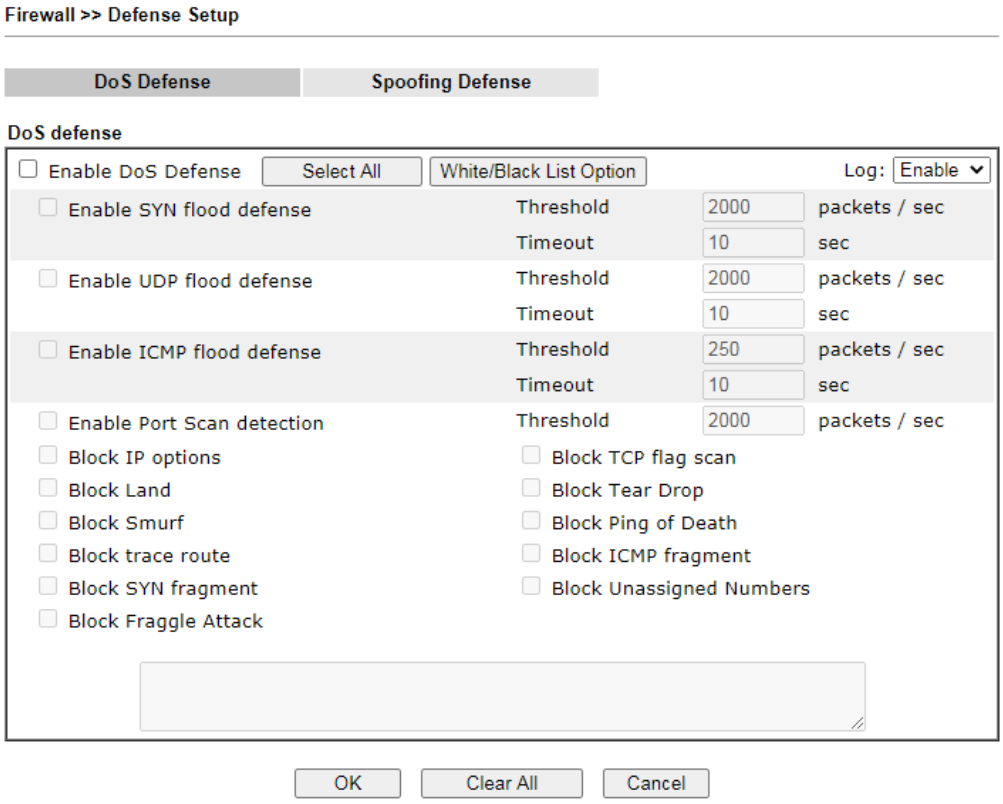
3. When you finish the configuration, please click **OK** to save and exit this page.

IV-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.

IV-1-3-1 DoS Defense

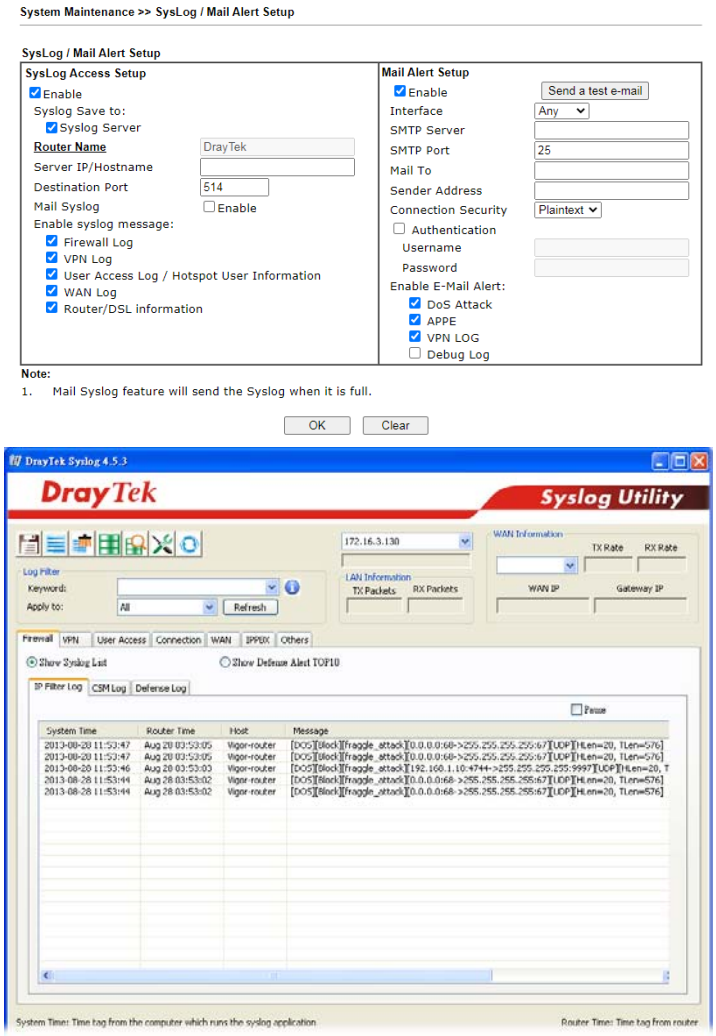
To configure DoS Defense, select DoS Defense under the Firewall menu item on the Web UI menu bar.



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

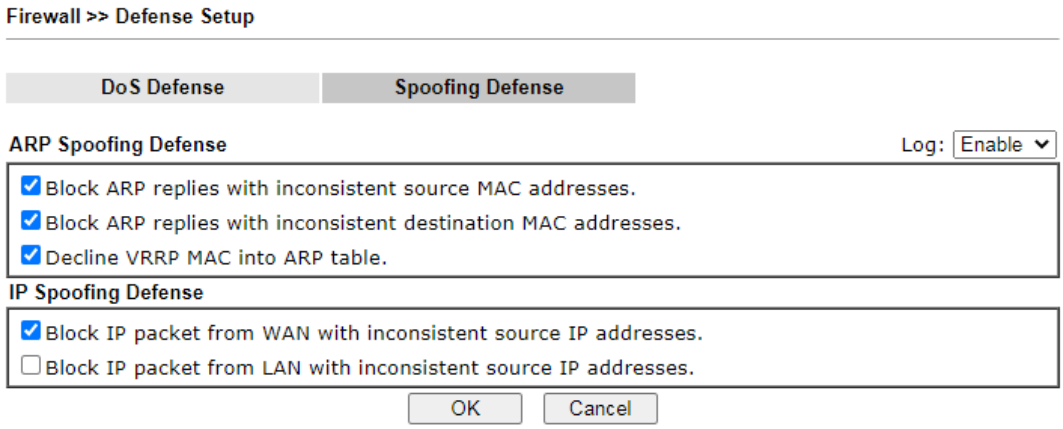
	packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Select to enable ICMP flood defense. When the arrival rate of ICMP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. The default values of threshold and timeout are 250 packets per second and 10 seconds, respectively.
Enable PortScan 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.

IV-1-3-2 Spoofing Defense

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

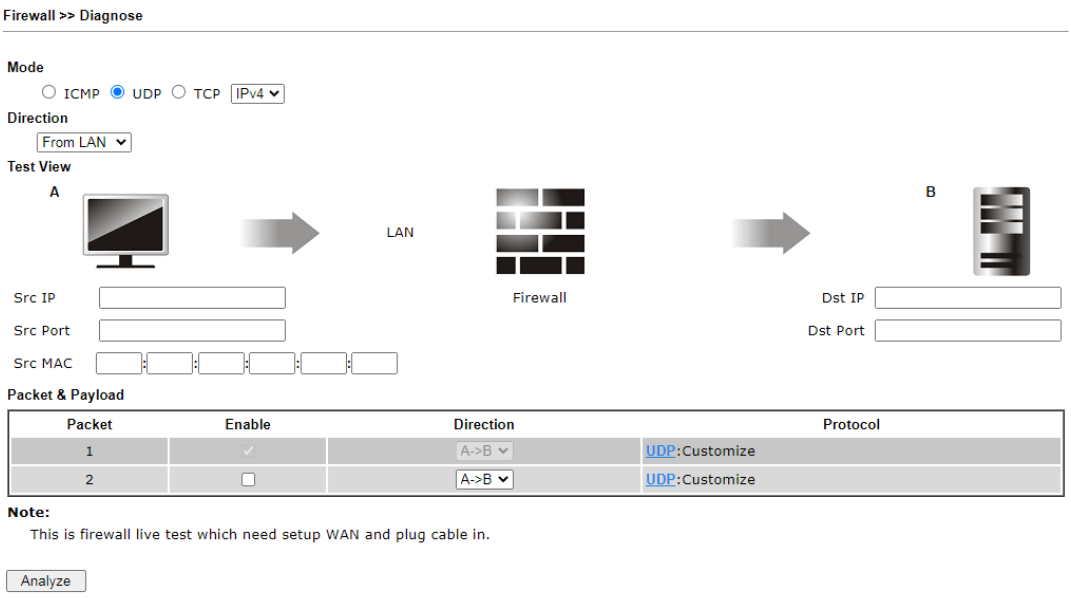


IV-1-4 Diagnose

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.

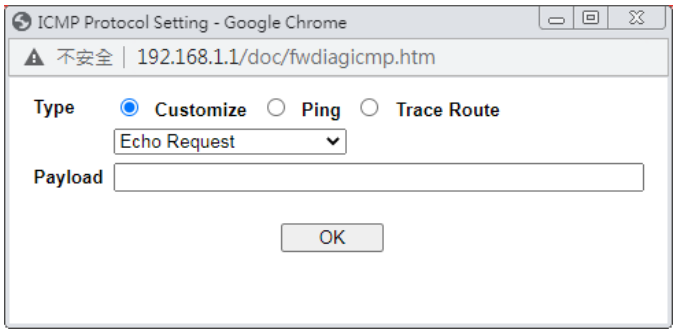
Info

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.

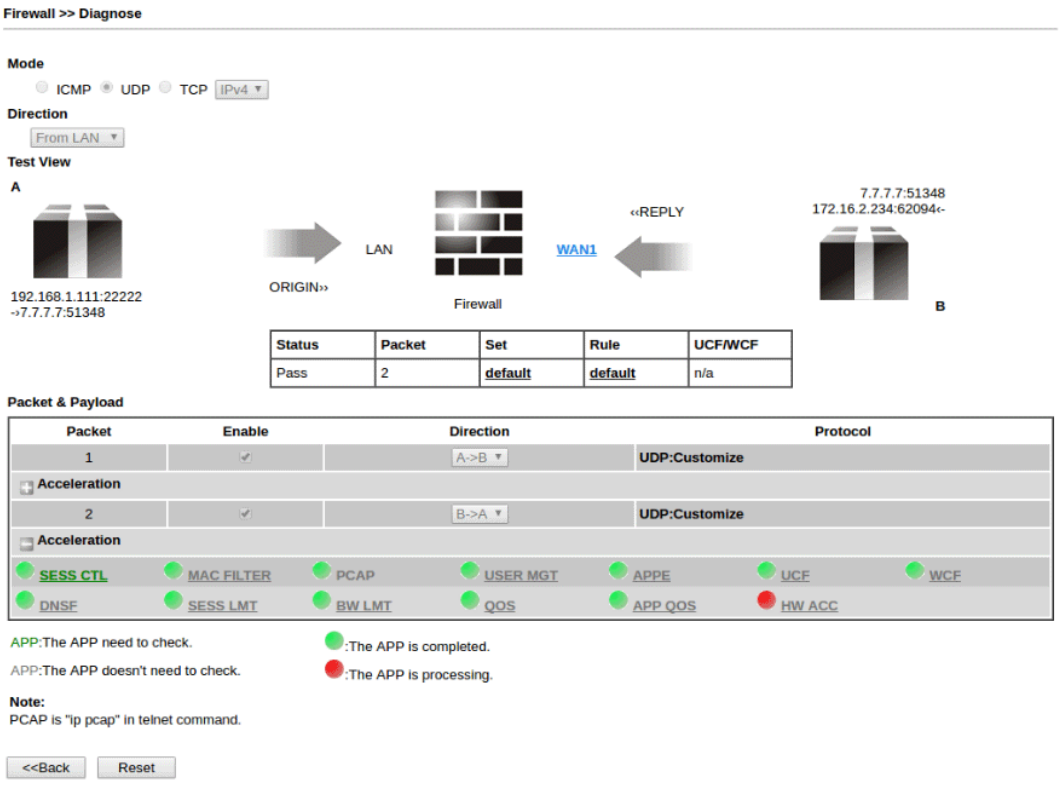


Available settings are explained as follows:

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 sate. 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 Customzie 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.

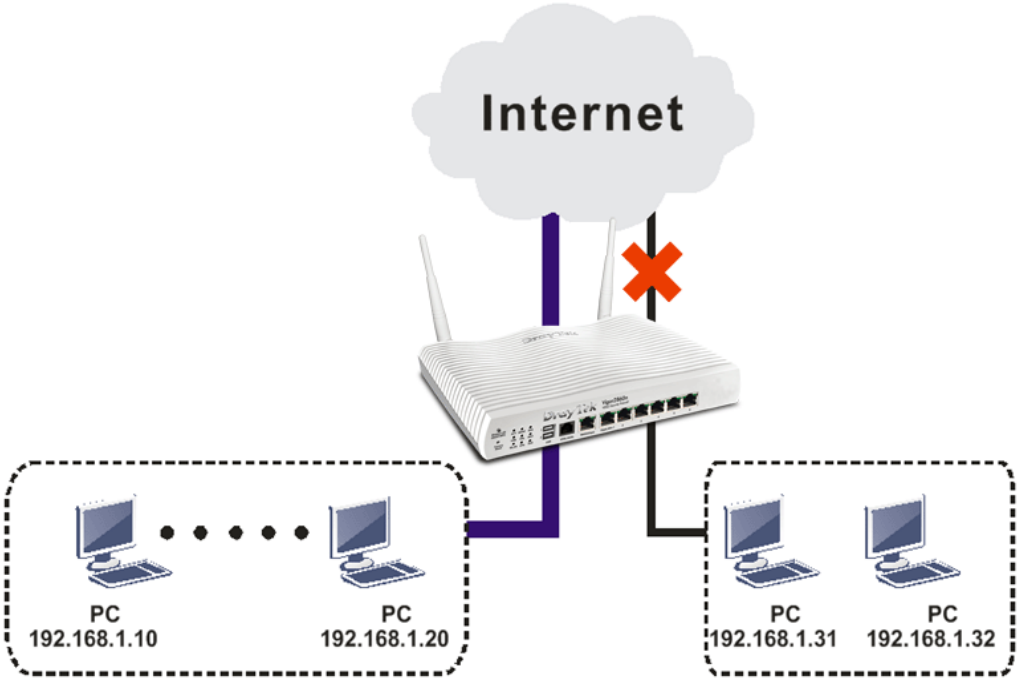
The following figure shows the test result after clicking **Analyze**. Processing state for the fuctions (MAC Filter, QoS, User management, etc.,) related to the firewall will be displayed by green or red LED.



Application Notes

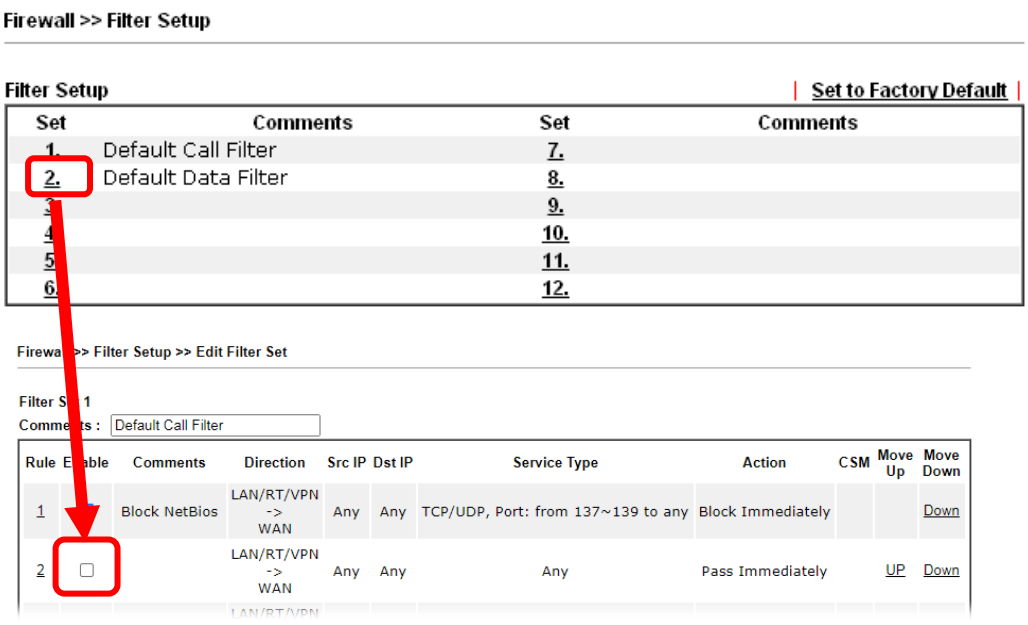
A-1 How to Configure Certain Computers Accessing to Internet

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.

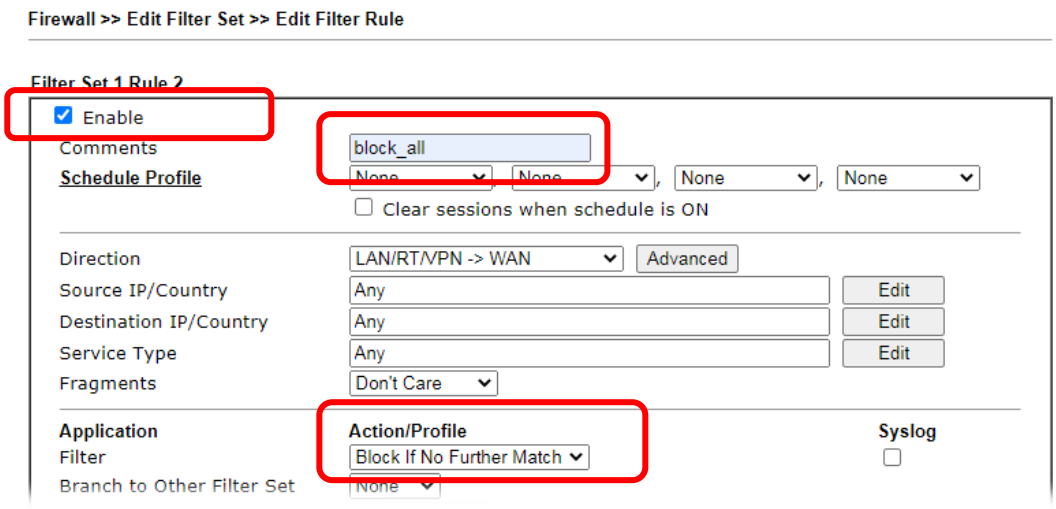


The way we can use is to set two rules under **Firewall**. For **Rule 1** of **Set 2** under **Firewall>>Filter Setup** is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

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



3. Check **Enable** to enable the filter rule. Type the comments (e.g., **block_all**). Choose **Block If No Further Match** for the **Filter** setting. Then, click **OK**.

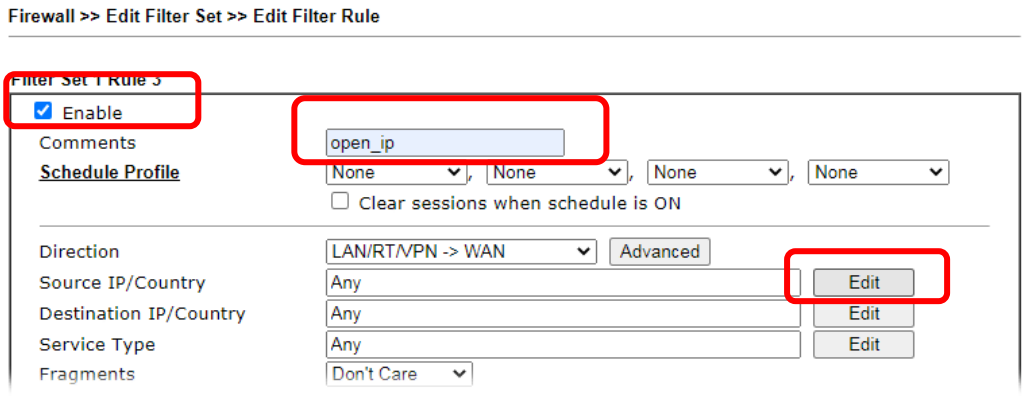


Info

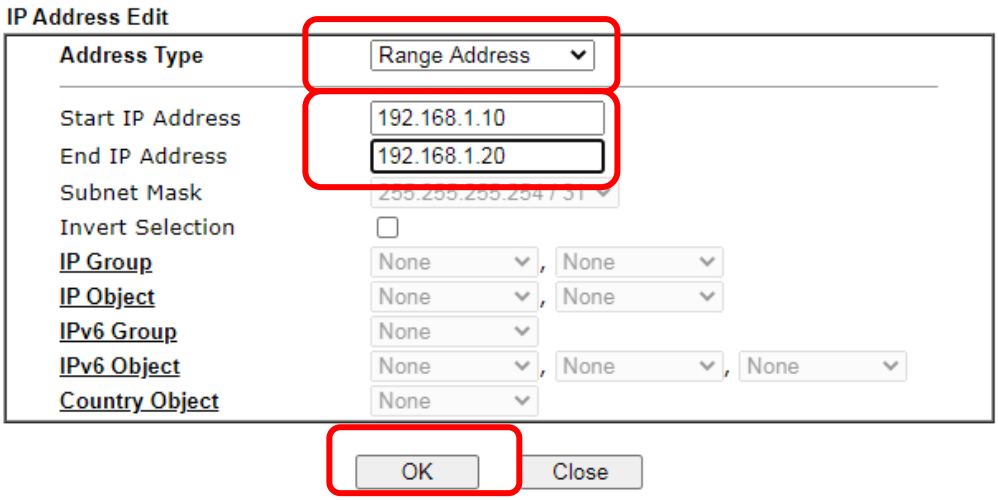
In default, the router will check the packets starting with Set 2, Filter Rule 2 to Filter Rule 7. If Block If No Further Match for is selected for Filter, the firewall of the router would check the packets with the rules starting from Rule 3 to Rule 7. The packets not matching with the rules will be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

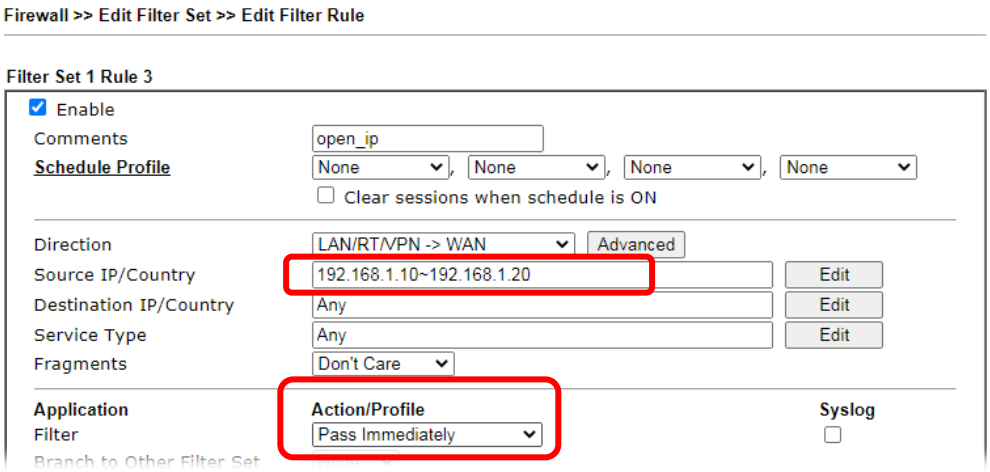
5. Check **Enable** to enable the filter rule. Type the comments (e.g., **open_ip**). Click the **Edit** button for **Source IP**.



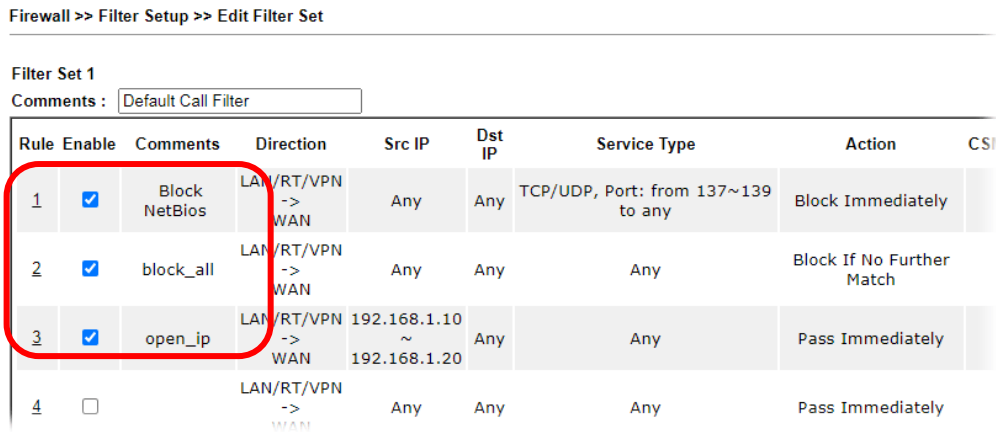
6. A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.



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.

IV-2 CSM (Central Security Management)

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.

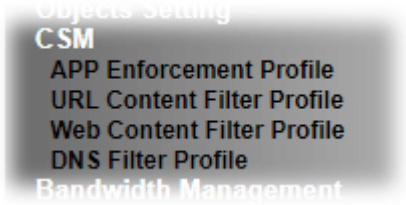
Web Content Filter

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.

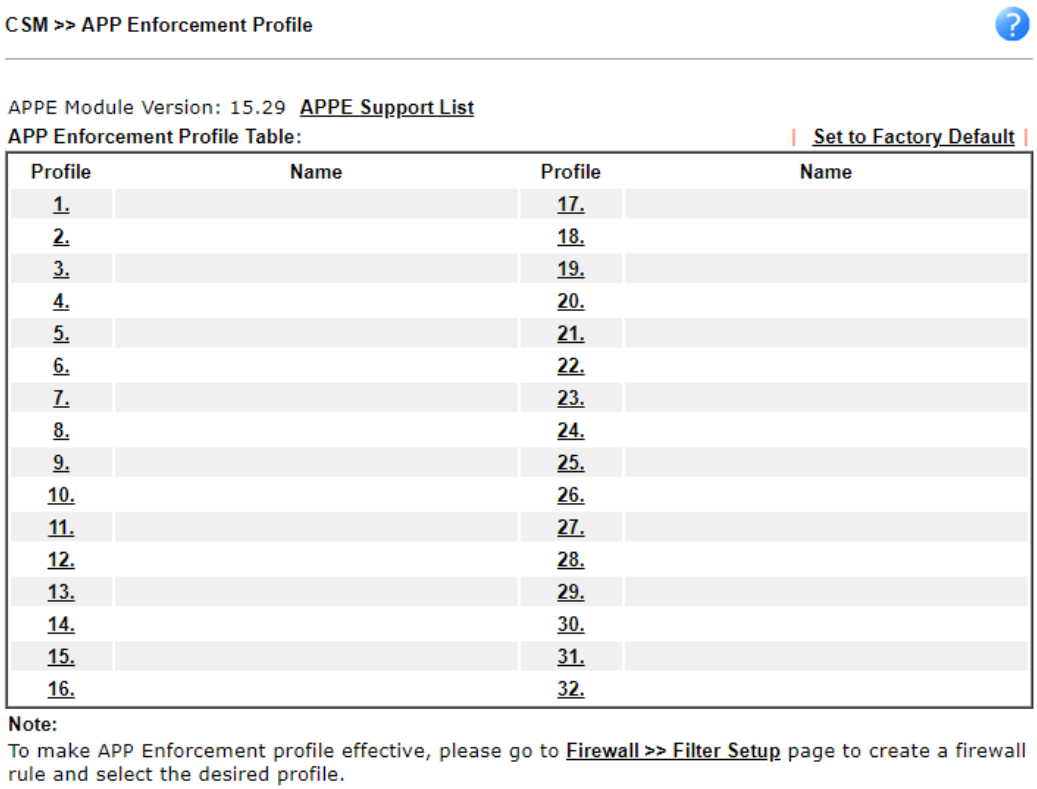
Info	The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface



IV-2-1 APP Enforcement Profile

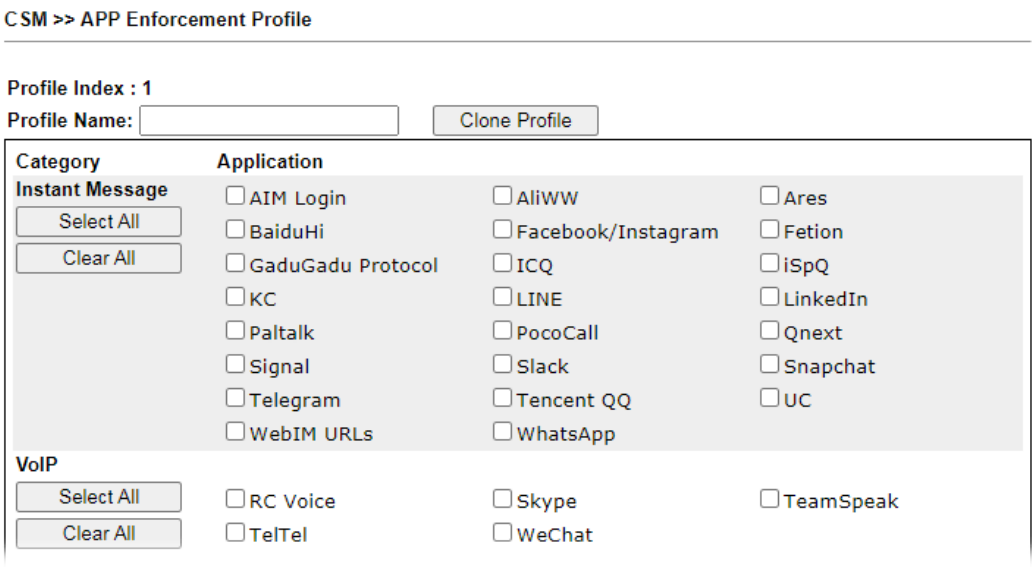
Up to 32 policy profiles for APP Enforcement can be configured.



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:



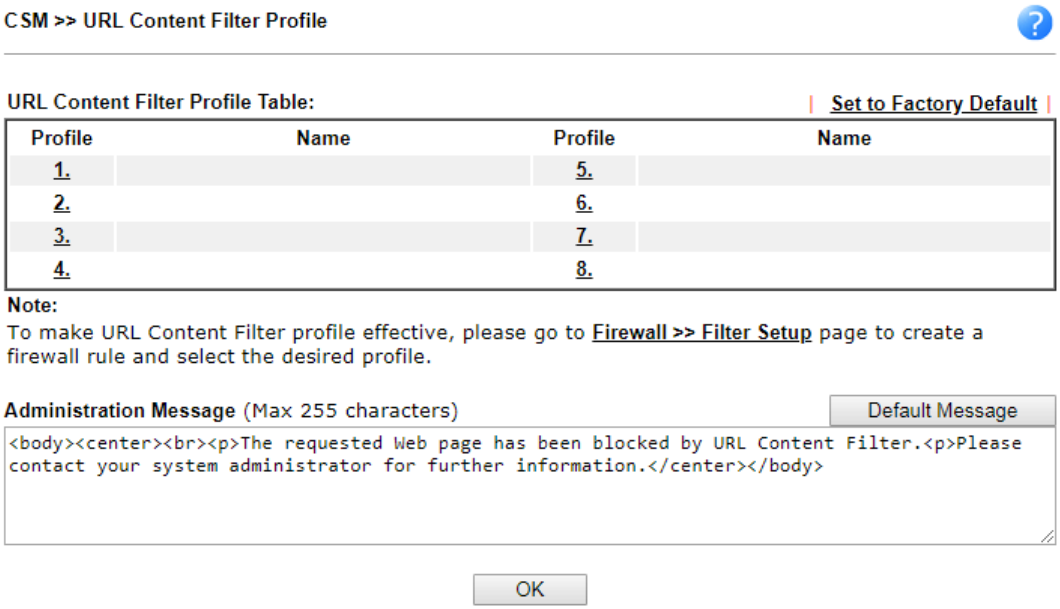
Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 15 characters.
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**.

IV-2-2 URL Content Filter Profile

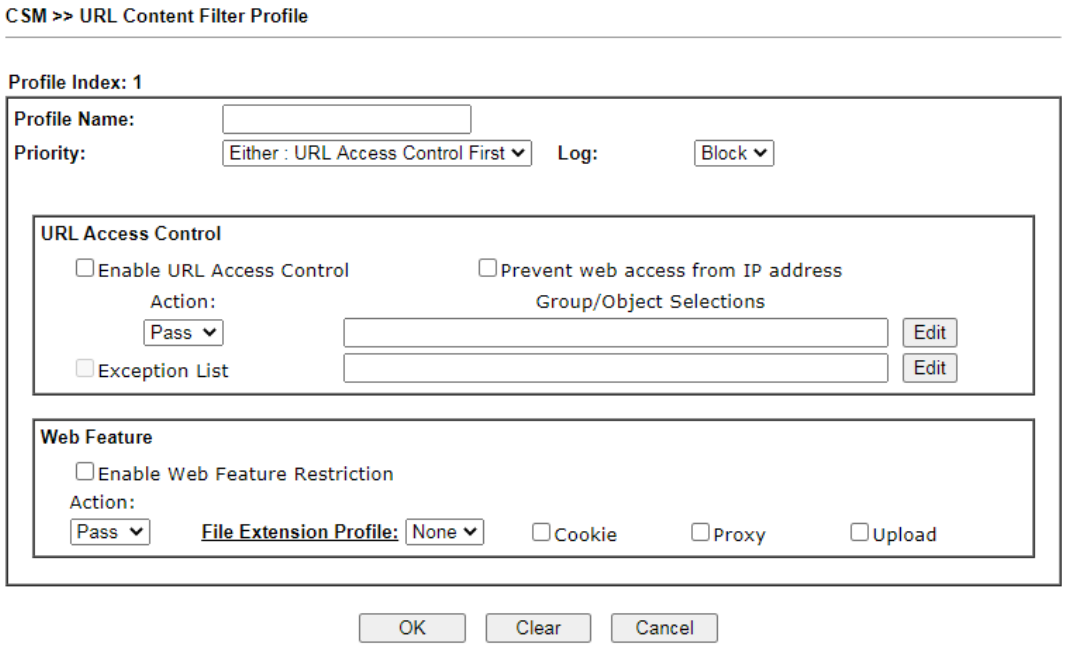
To set up URL Content Filter Profiles, click **CSM** on the Main Menu bar, and then click **URL Content Filter Profile** to open the profile setting page.



Each item is explained as follows:

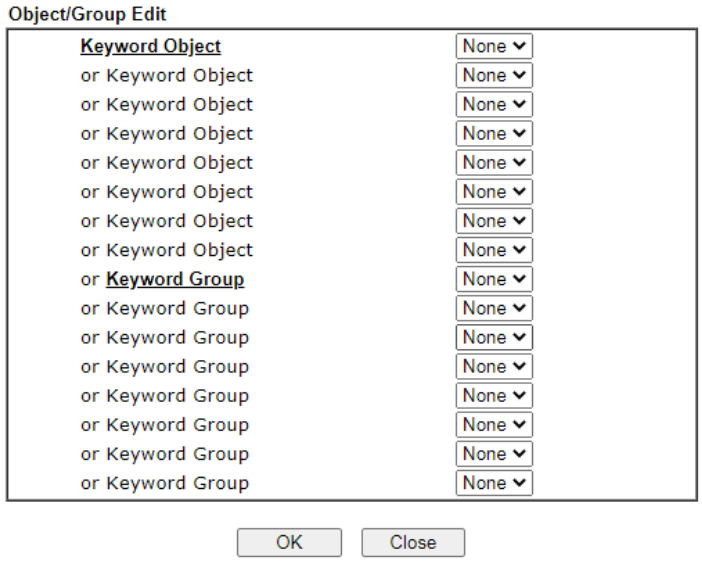
Item	Description
Set to Factory Default	Clear all profile settings.
Profile	Index number of the profile.
Name	Name that identifies the profile.
Administration Message	The message to be displayed in the browser when access to a URL has been blocked. A custom message can be entered with HTML formatting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

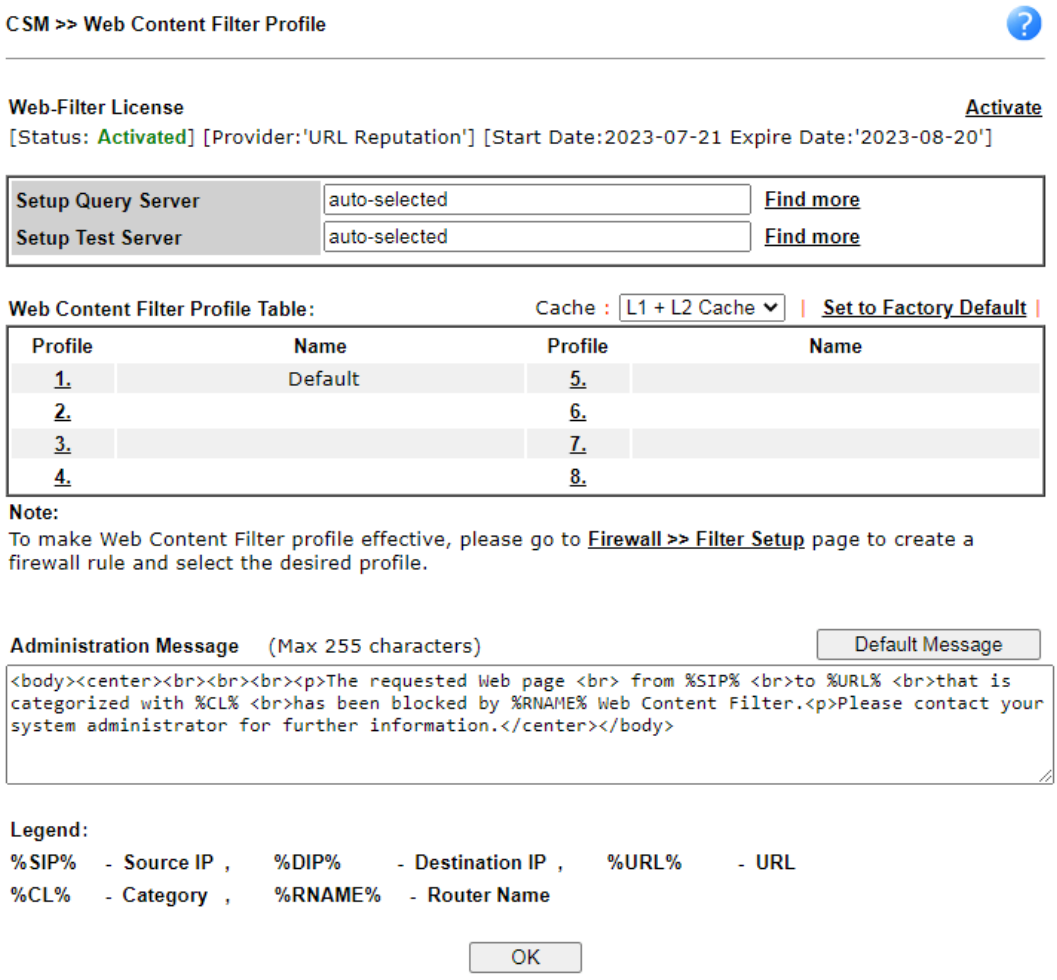
IV-2-3 Web Content Filter Profile

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.

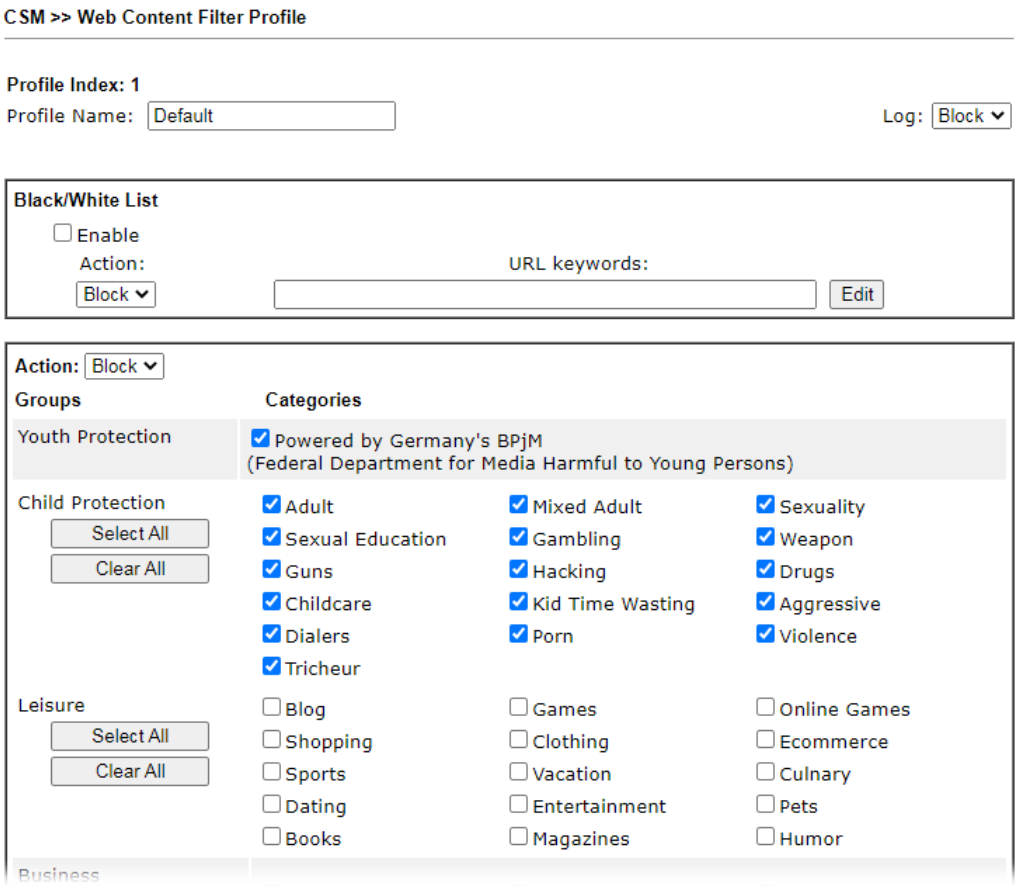
Info 1	Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by Commtouch. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor 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	**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.

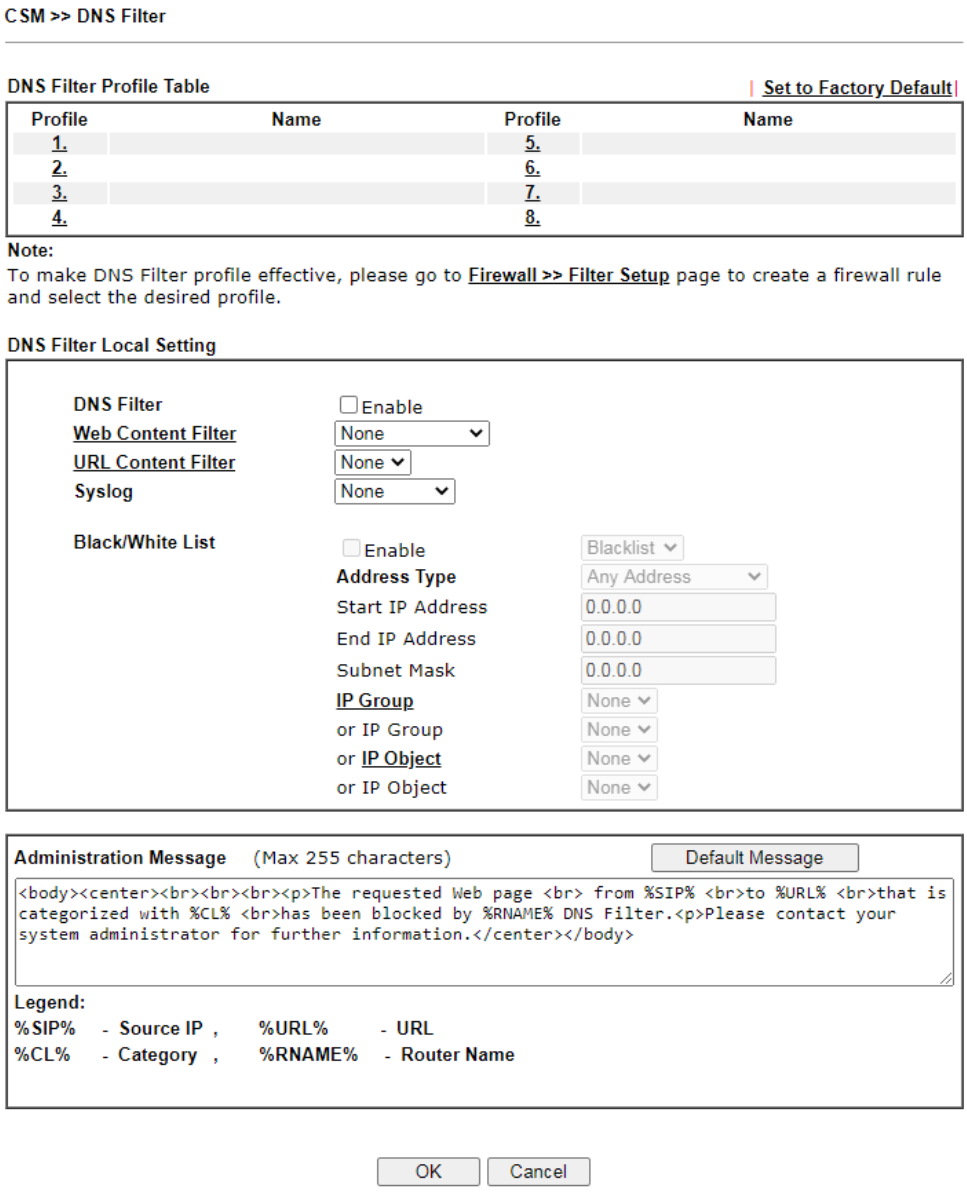
	Action - Action to take when a URL matches keyword group and object selections. ● **Pass** – allow access to the URL. ● **Block** – disallow access to the URL. **Select All -** Click to select all categories within the group. **Clear All -** Click to deselect all categories within the group.

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

IV-2-4 DNS Filter Profile

DNS Filter blocks or allows traffic to the WAN by intercepting DNS queries, and applying UCF and WCF rules to hostnames. DNS filtering is especially useful when you wish to restrict access of protocols other than HTTP, such as HTTPS. Note that a WCF license must have already been activated before WCF rules could be used.

To configure DNS Filter Profiles, select **CSM >> Web Content Filter Profile** from the main menu.



Available settings are explained as follows:

Item	Description
DNS Filter Profile Table	DNS Filter Profiles take effect when DNS servers on the WAN are used for DNS queries. The router intercepts all outgoing DNS queries on UDP port 53 and applies WCF and UCF rules on the domain names before passing the queries to the DNS servers. IP addresses of the domains are then blocked or allowed as per applicable WCF and UCF rules. DNS Filter Profiles can be applied by selecting from Firewall filter rules. **Profile -** Index number of the profile. Click to bring up the configuration page for the profile entry. **Name -** Name that identifies the profile.
Set to Factory Default	Clear all DNS Filter profile settings.
DNS Filter Local Setting	By setting the IP address of the DNS lookup server to the router's address, the router serves as a DNS lookup proxy server. When DNS Filter Local Setting is enabled, all DNS queries sent to the router will have WCF and UCF rules applied to the hostnames, and access to the resolved IP addresses will be allowed or blocked as configured in the rules. **DNS Filter -** Select to enable DNS Filter Local Setting. **Web Content Filter -** Select a WCF profile. **URL Content Filter** - Select a UCF profile. **Syslog -** The filtering result can be recorded according to the setting selected for Syslog. ● **None –** No log file will be created for this profile. ● **Pass –** Only passed access attempts will be recorded in Syslog. ● **Block –** Only blocked access attempts will be recorded in Syslog. ● **Both –** Both passed and blocked access attempts will be recorded in Syslog. **Black/White List –** Specify IP address, subnet mask, IP object, or IP group as a black list or white list for DNS packets passing through or blocked by Vigor router.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box. You can embed the following variables in the message: ● %SIP% – The source IP address that attempted the HTTP access. ● %DIP% – The destination IP address to which access was attempted. ● %URL% – The URL of the destination website. ● %CL% – The category to which the URL belongs. ● %RNAME% – The name of the router. **Default Message** - Click to reset the administration message to the factory default.

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

Application Notes

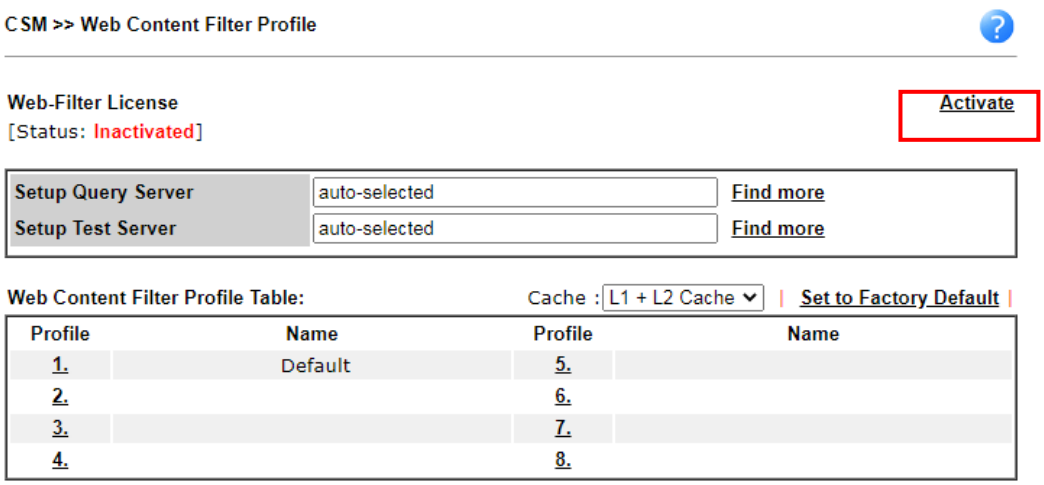
A-1 How to Create an Account for MyVigor

The website of MyVigor (a server located on http://myvigor.draytek.com) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

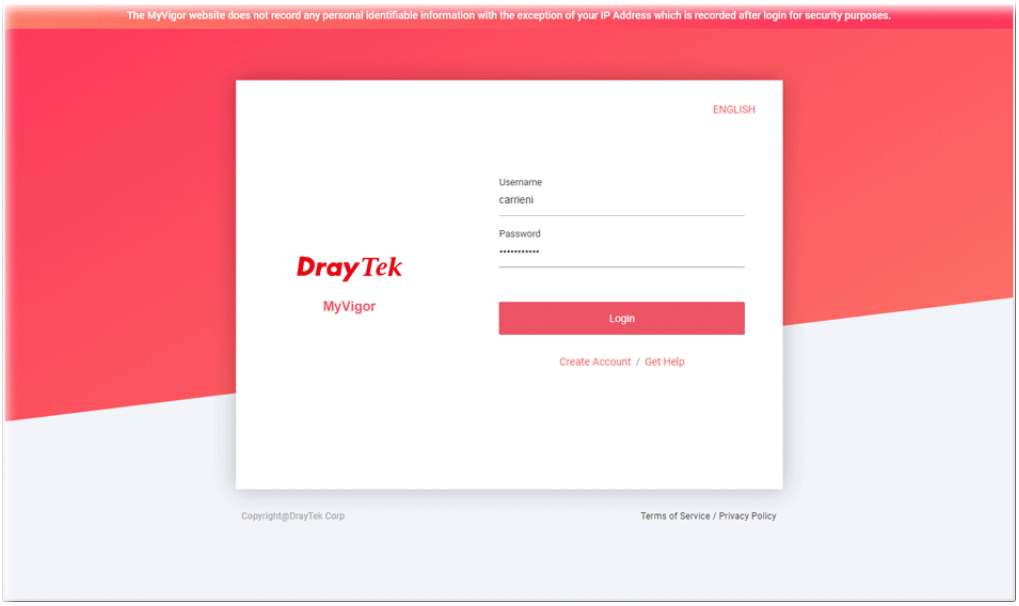
To access into MyVigor for getting more information, please create an account for MyVigor.

Create an Account via Vigor Router

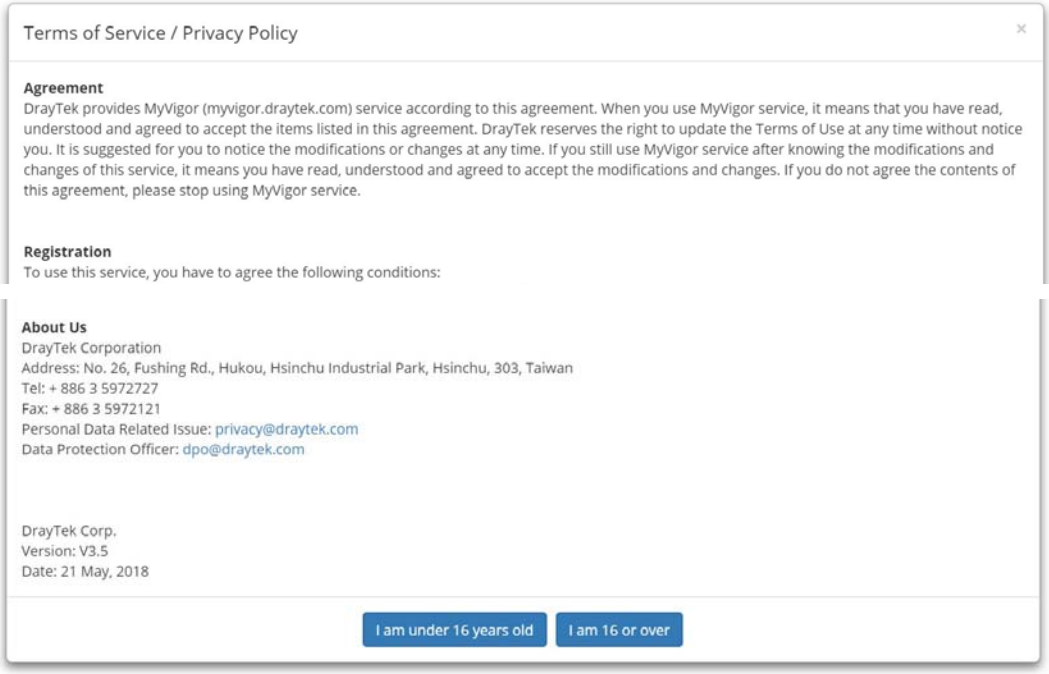
1. Click **CSM>> Web Content Filter Profile**. The following page will appear.



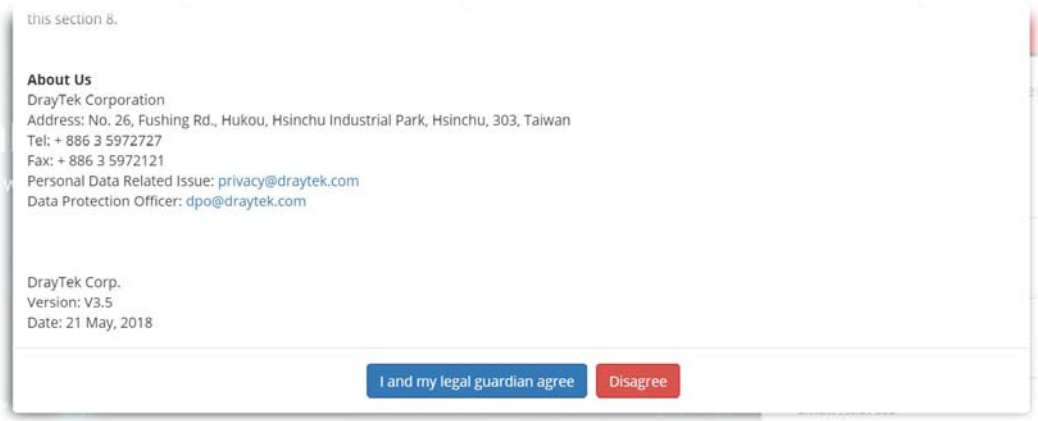
2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.



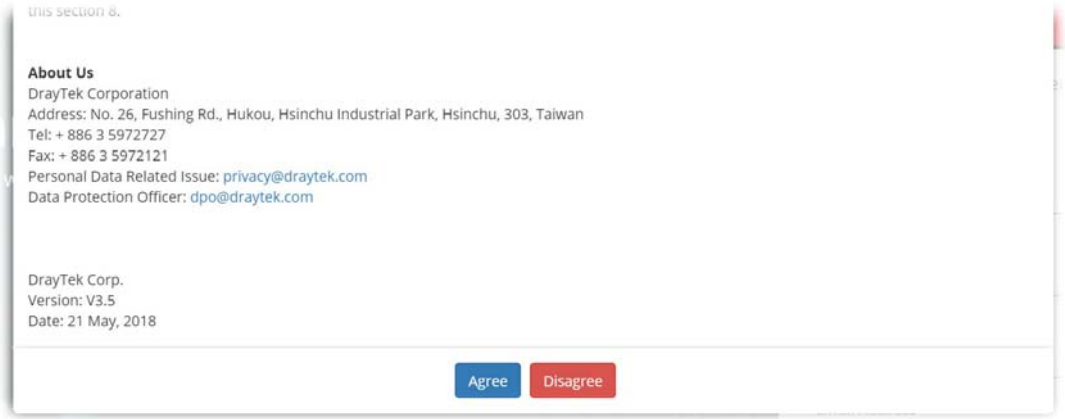
3. Click the link of **Create an account now**.
4. The system will ask if you are 16 years old or over.
   - If yes, click **I am 16 or over**.



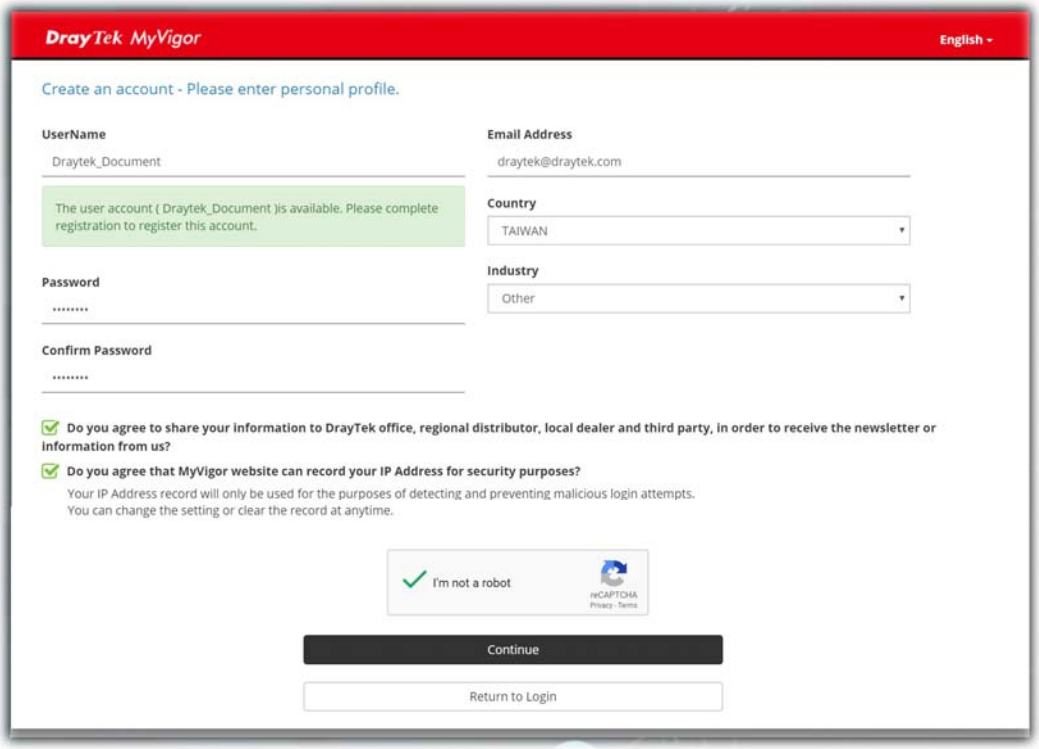
- If not, click **I am under 16 years old** to get the following page. Then, click **I and my legal guardian agree**.



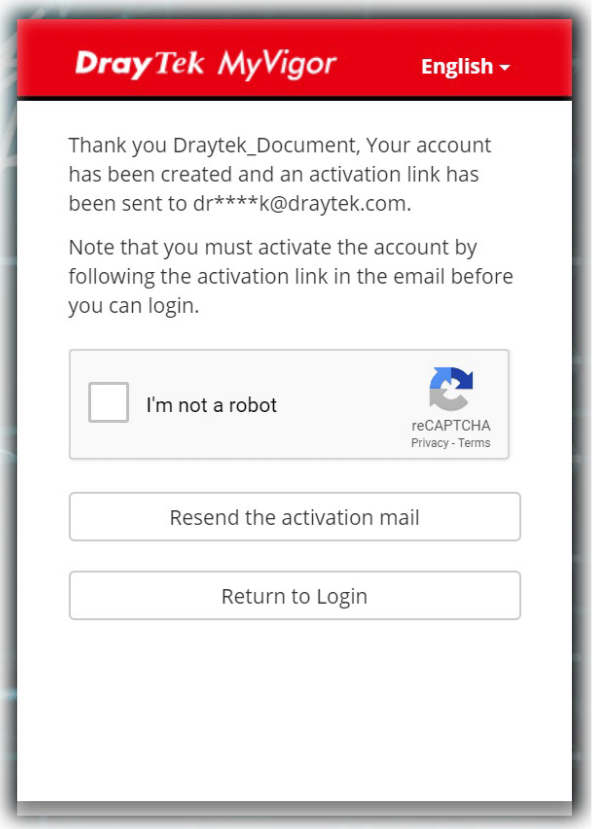
5. After reading the terms of service/privacy policy, click **Agree**.



6. In the following page, enter your personal information in this page and then click **Continue**.



7. Choose proper selection for your computer and click **Continue**.



8. Now you have created an account successfully.
9. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

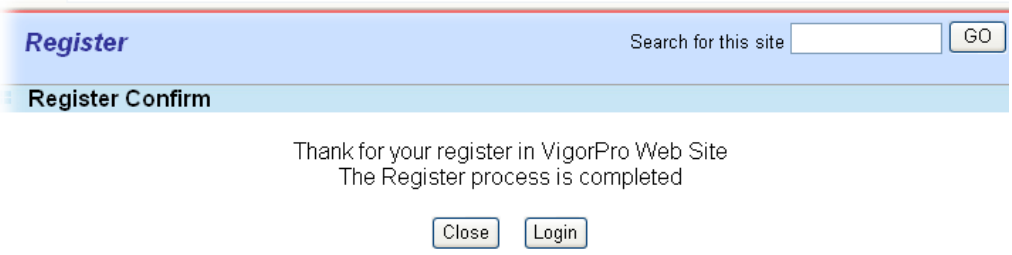
****** This is an automated message from myvigor.draytek.com.******

Thank you (**Mary**) for creating an account.

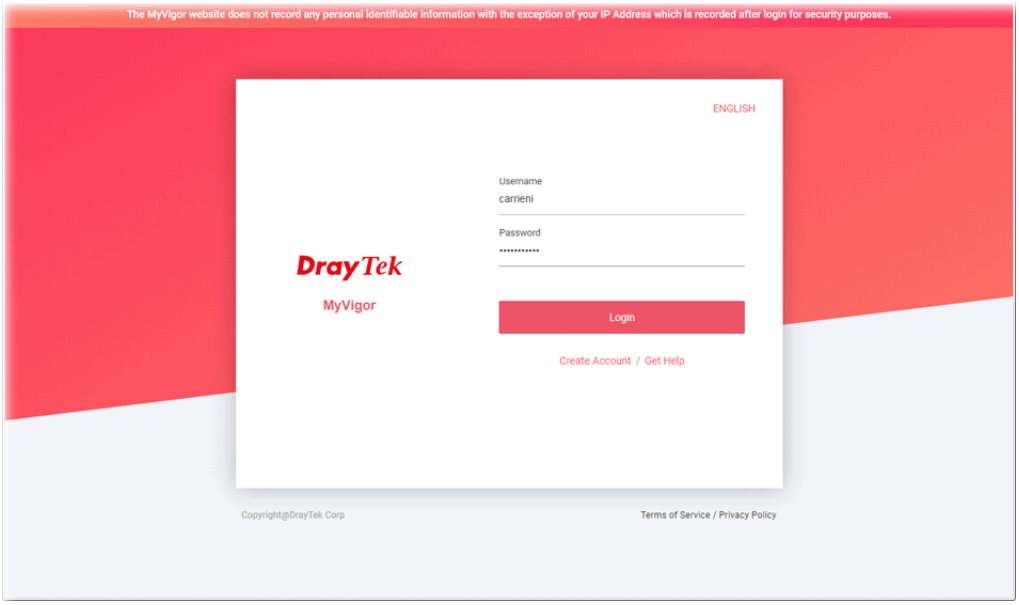
Please click on the activation link below to activate your account

Link : Activate my Account

10. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



11. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.



12. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

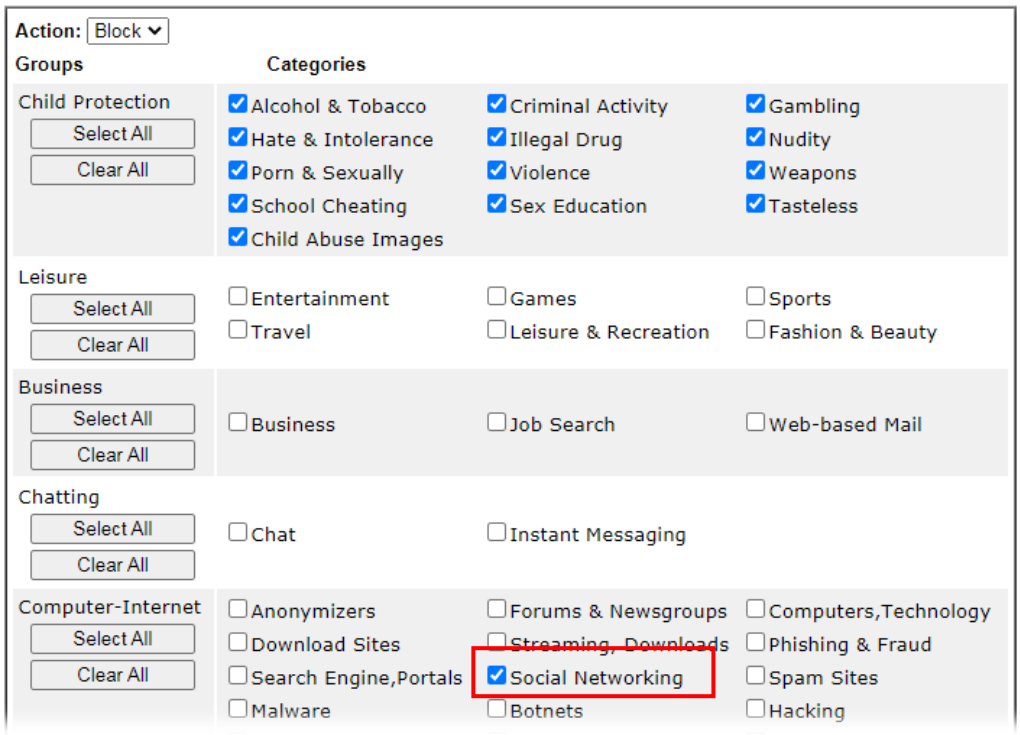
URL Content Filter,

Benefits: Free, flexible for customize webpage.

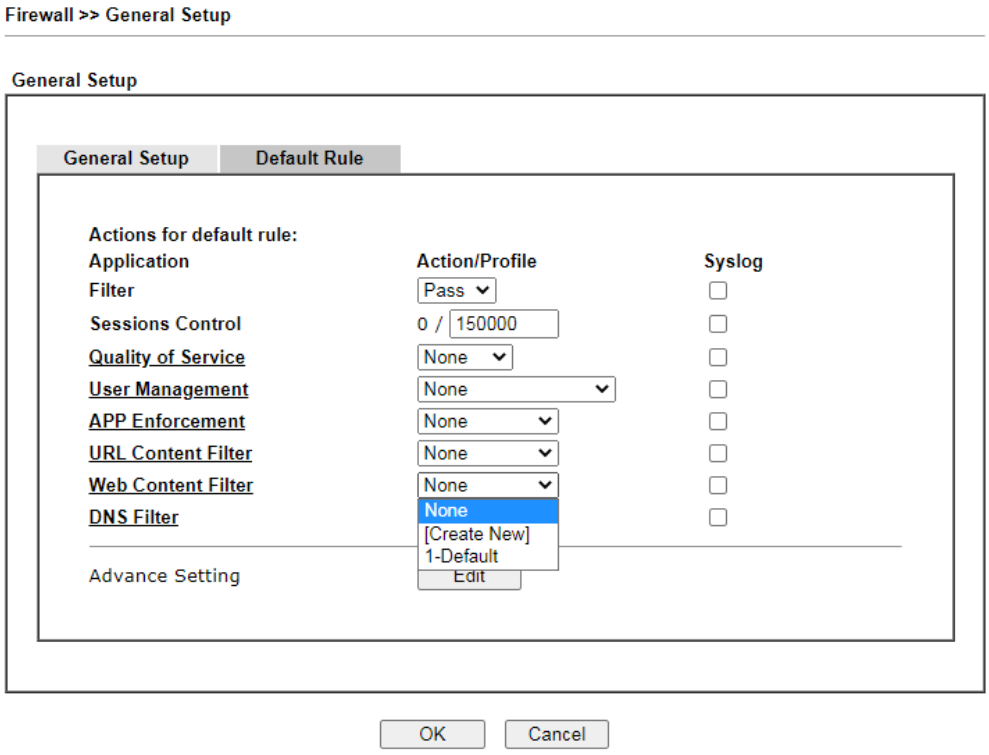
Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

1. Make sure the Web Content Filter license is valid.
2. Open **CSM >> Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with **Action, Block**.



3. Select this profile in **Firewall>>General Setup>>Default Rule**.

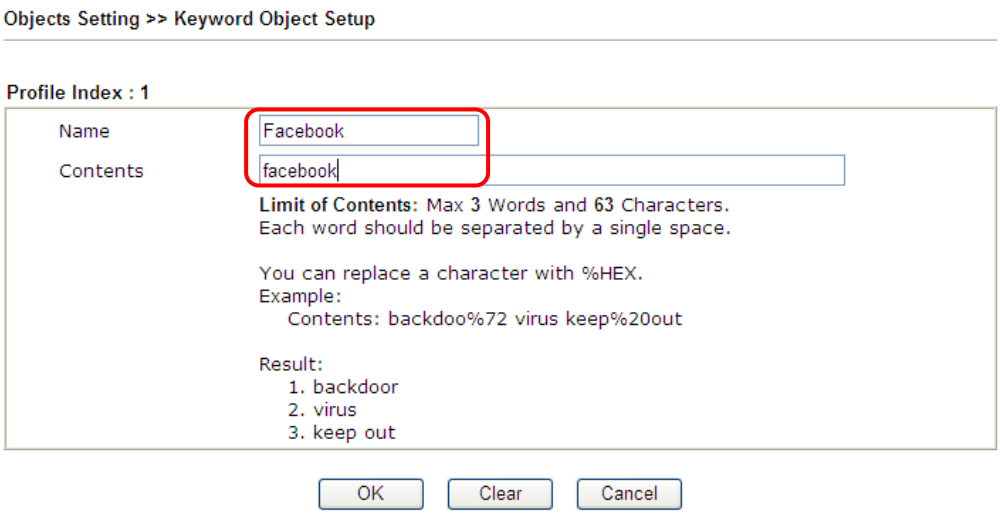


4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

II. Via URL Content Filter

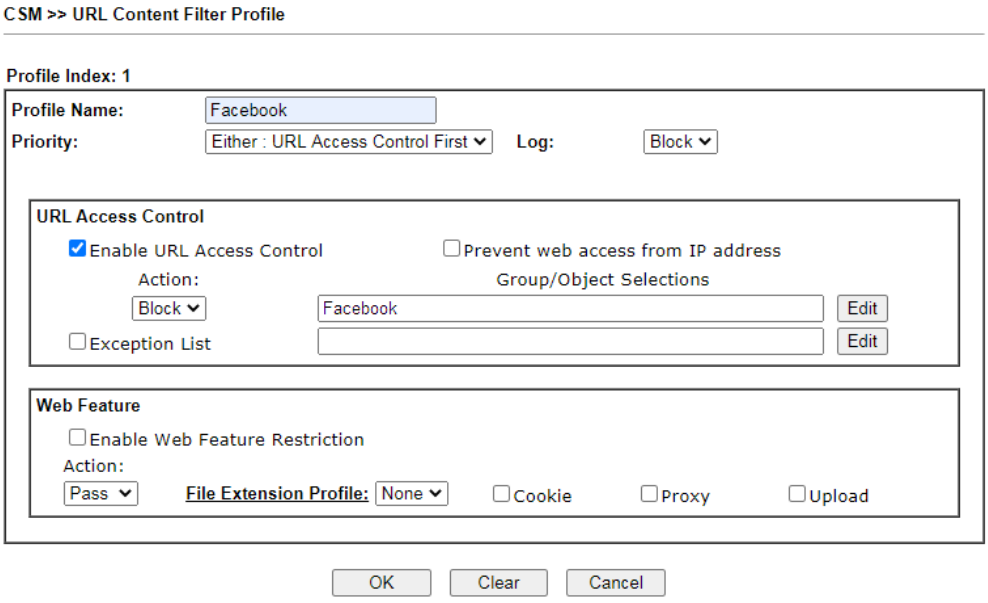
A. Block the web page containing the word of "Facebook"

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.



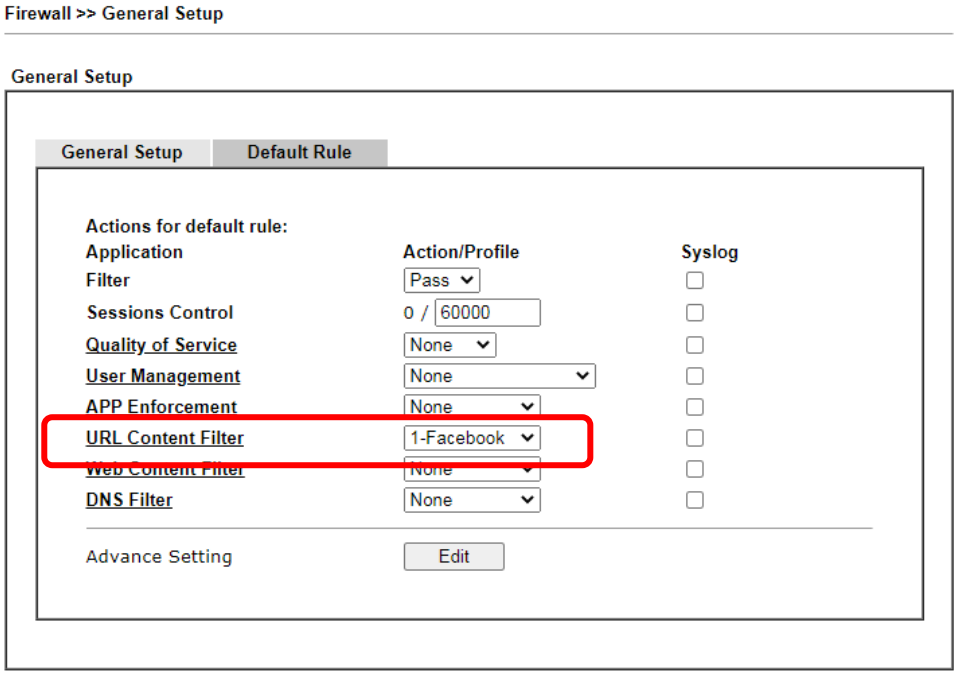
3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.



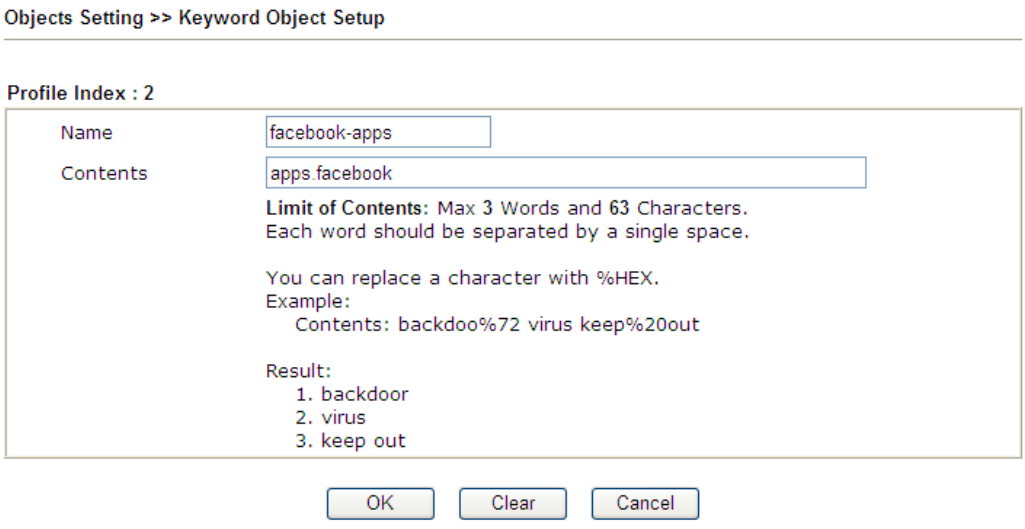
5. When you finished the above steps, click **OK**. Then, open **Firewall>>General Setup**.

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.



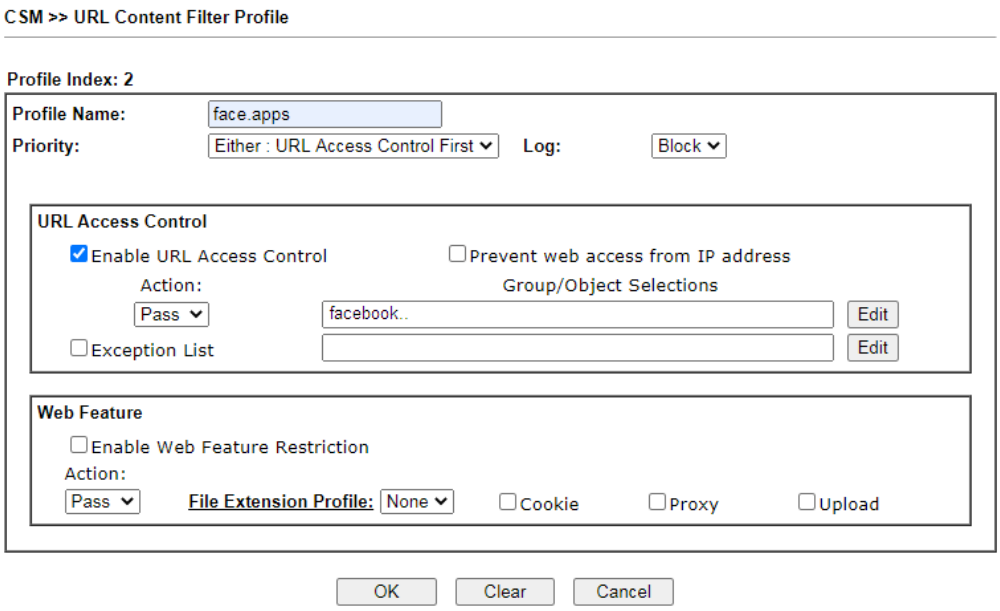
B. Disallow users to play games on Facebook

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.



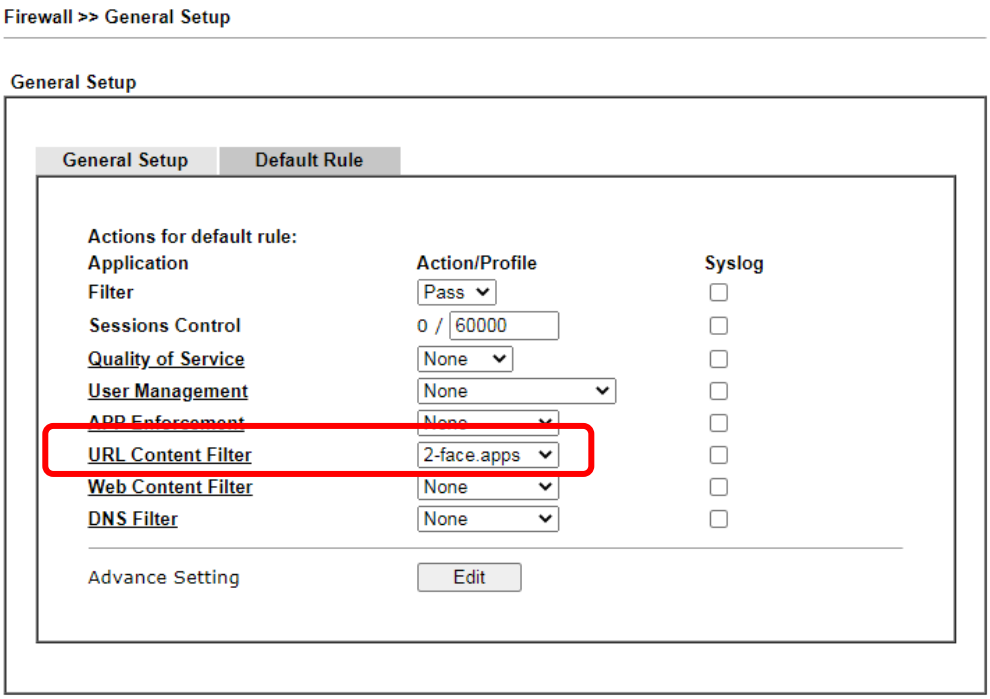
3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.



5. When you finished the above steps, please open **Firewall>>General Setup**.

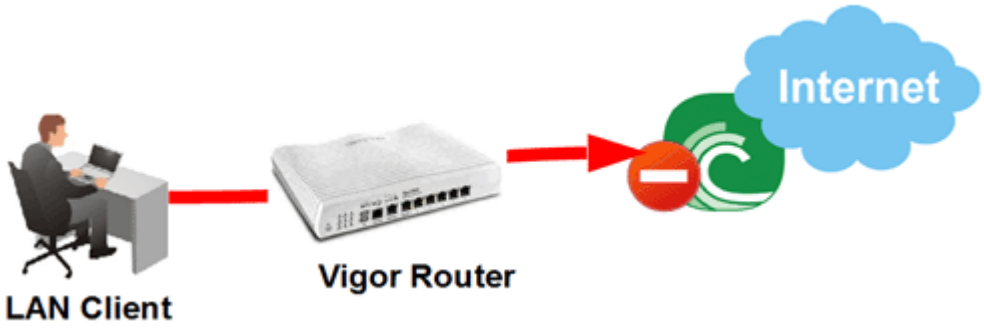
6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.



A-3 How to use APP Enforcement to block application like Facebook, YouTube or TeamViewer?

APP Enforcement helps network administrator to block applications on LAN network. Draytek routers provide a few categories to set up the profiles e.g., IM, P2P, Protocol, Stream, Remote control.

This section is going to demonstrate how to use APP Enforcement to block Facebook, Skype, YouTube and TeamViewer.



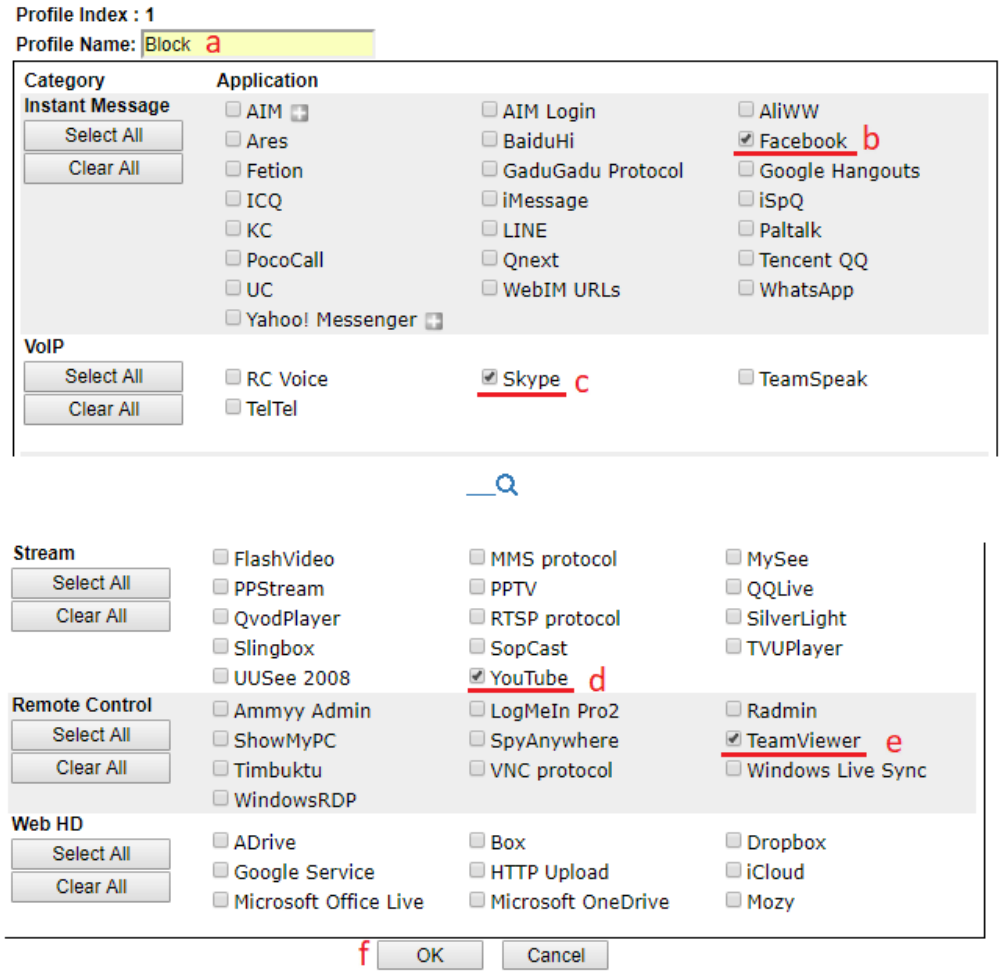
1. Create an APP Enforcement Profile: Click on an Index number to create a new profile at **CSM >> APP Enforcement Profile**.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table: | Set to Factory Default |

Profile	Name	Profile	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	

2. Set up the details in the profile.



(a) Enter Profile Name.

(b) Choose the Facebook in Instant Message.

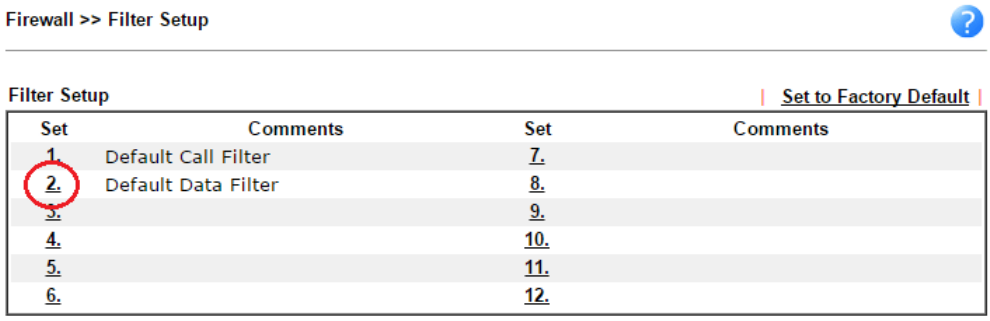
(c) Choose Skype in VoIP.

(d) Choose YouTube in Stream.

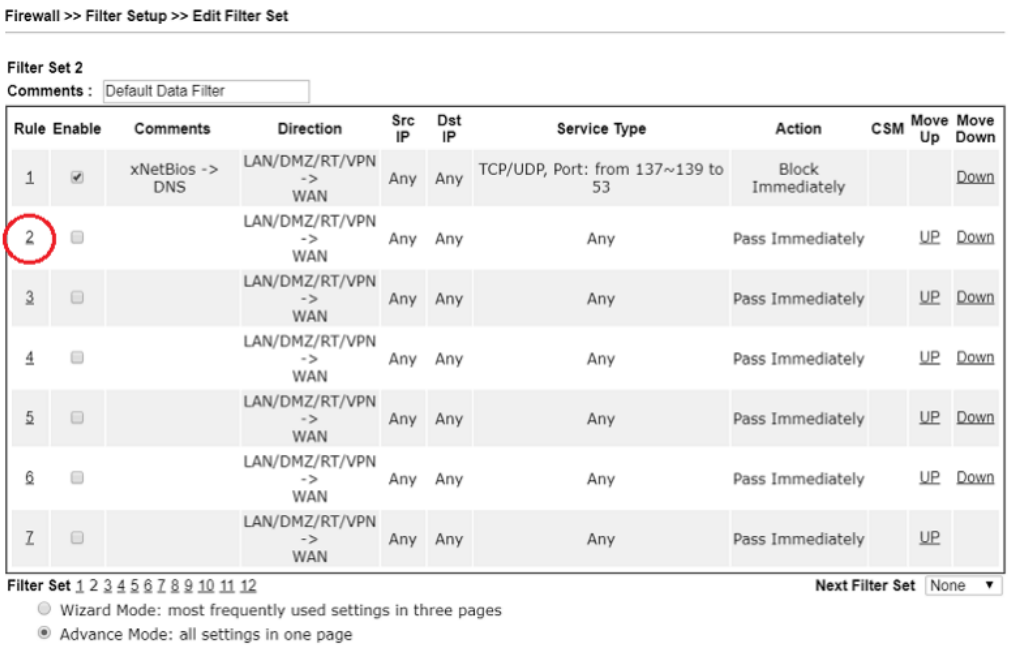
(e) Choose TeamViewer in Remote control.

(f) Click **OK** to save.

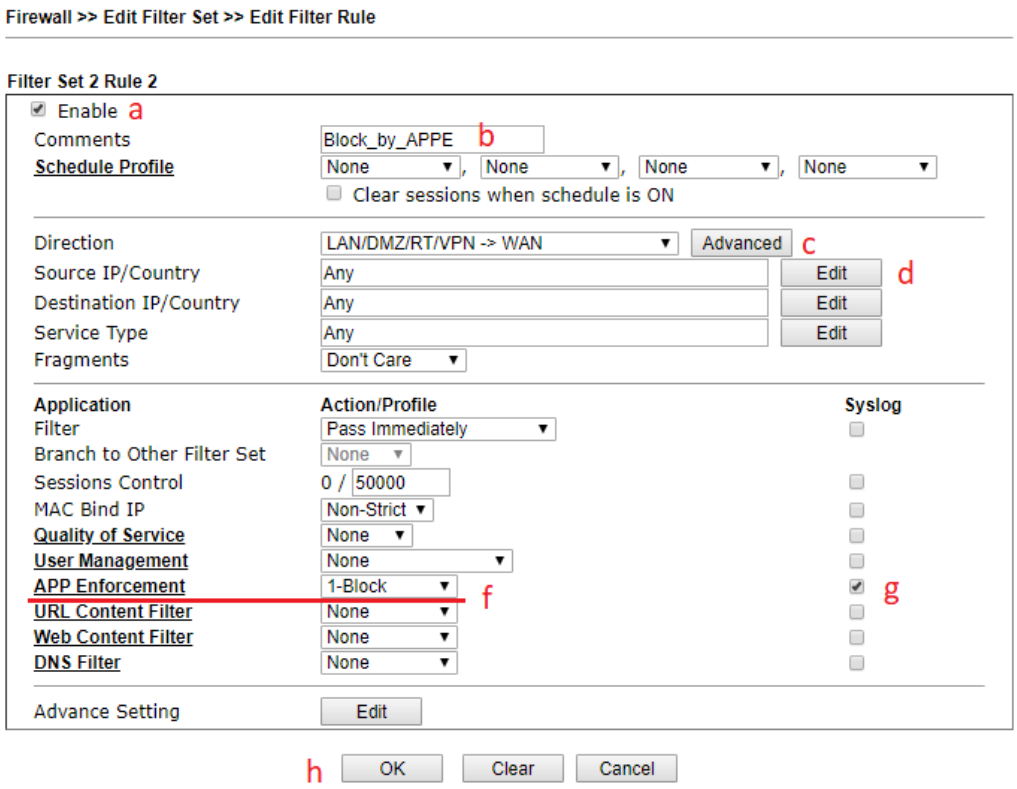
3. Apply the APP Enforcement Profile to a Firewall Filter Rule. Go to **Firewall >> Filter Setup**, and click an available set.



4. Click on a Filter Rule index to set up a filter.



5. Set up the details in the profile.



(a) Enable the Filter Rule.

(b) Put the comments of this rule.

(c) Select the Direction as **LAN/DMZ/RT/VPN -> WAN**.

(d) Edit the **Source IP** which should be blocked from the APP.

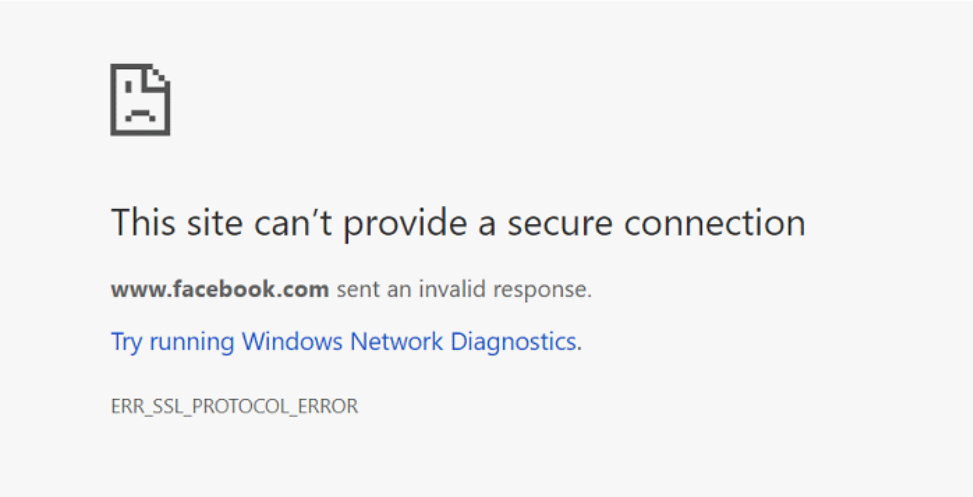
(e) Select Filter as **Pass Immediately**.

(f) Select APP Enforcement as the profile we created in Step 2.

(g) You may also check the **Syslog** if needed.

(h) Click **OK** to save.

6. With the above configuration, LAN clients cannot be able to use the APP and website.



Part V 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, Configuration Export, Syslog /Mail Alert, Time and Date, SNMP, Management, Self-Signed Certificate, Reboot System, Firmware Upgrade, Activation, Internal Service User List, Dashboard Control and NAT Sessions

Bandwidth Management

It is used to control the bandwith of data transmission through configuration of Sessions Limit, Bandwidth Limit, and Quality of Servie (QoS).

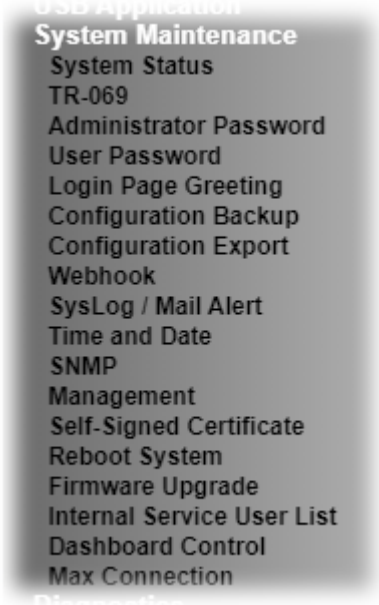
User Management

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.

V-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, Panel Control, Reboot System, Firmware Upgrade, Internal Service User List, Dashboard Control and NAT Sessions.

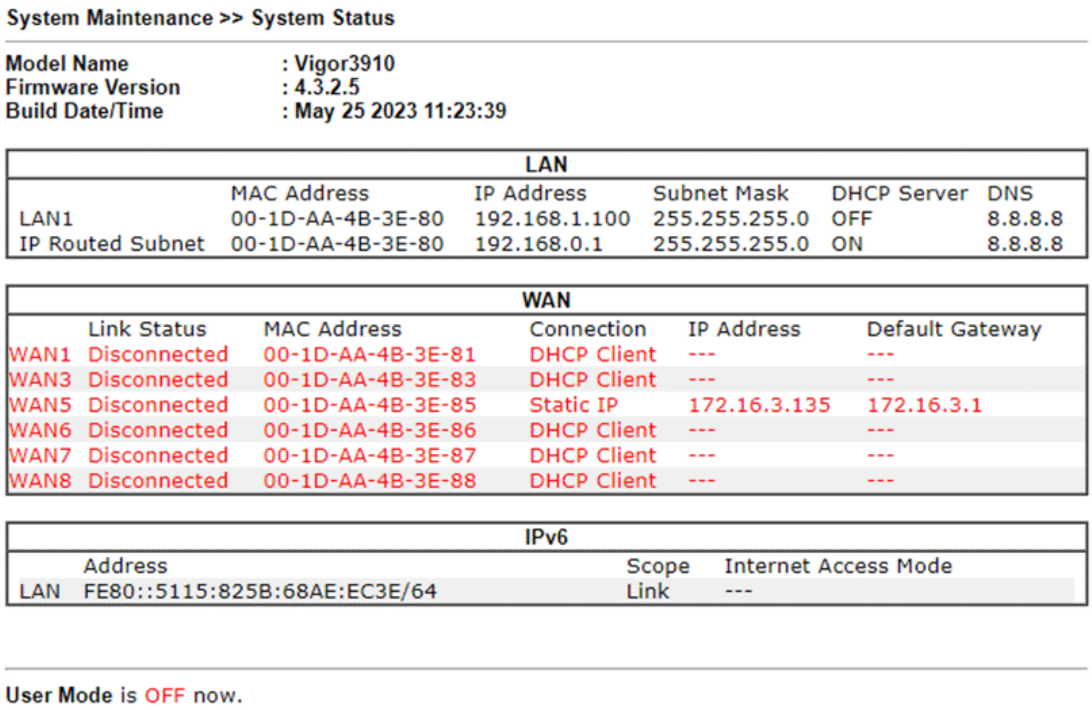
Below shows the menu items for System Maintenance.



Web User Interface

V-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 Maintenance >> System Status

Model Name : **Vigor3910**
Firmware Version : **4.3.2.5**
Build Date/Time : **May 25 2023 11:23:39**

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-4B-3E-80	192.168.1.100	255.255.255.0	OFF	8.8.8.8
IP Routed Subnet	00-1D-AA-4B-3E-80	192.168.0.1	255.255.255.0	ON	8.8.8.8

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-4B-3E-81	DHCP Client	---	---
WAN3	Disconnected	00-1D-AA-4B-3E-83	DHCP Client	---	---
WAN5	Disconnected	00-1D-AA-4B-3E-85	Static IP	172.16.3.135	172.16.3.1
WAN6	Disconnected	00-1D-AA-4B-3E-86	DHCP Client	---	---
WAN7	Disconnected	00-1D-AA-4B-3E-87	DHCP Client	---	---
WAN8	Disconnected	00-1D-AA-4B-3E-88	DHCP Client	---	---

IPv6

	Address	Scope	Internet Access Mode
LAN	FE80::5115:825B:68AE:EC3E/64	Link	---

User Mode is OFF now.

Available settings are explained as follows:

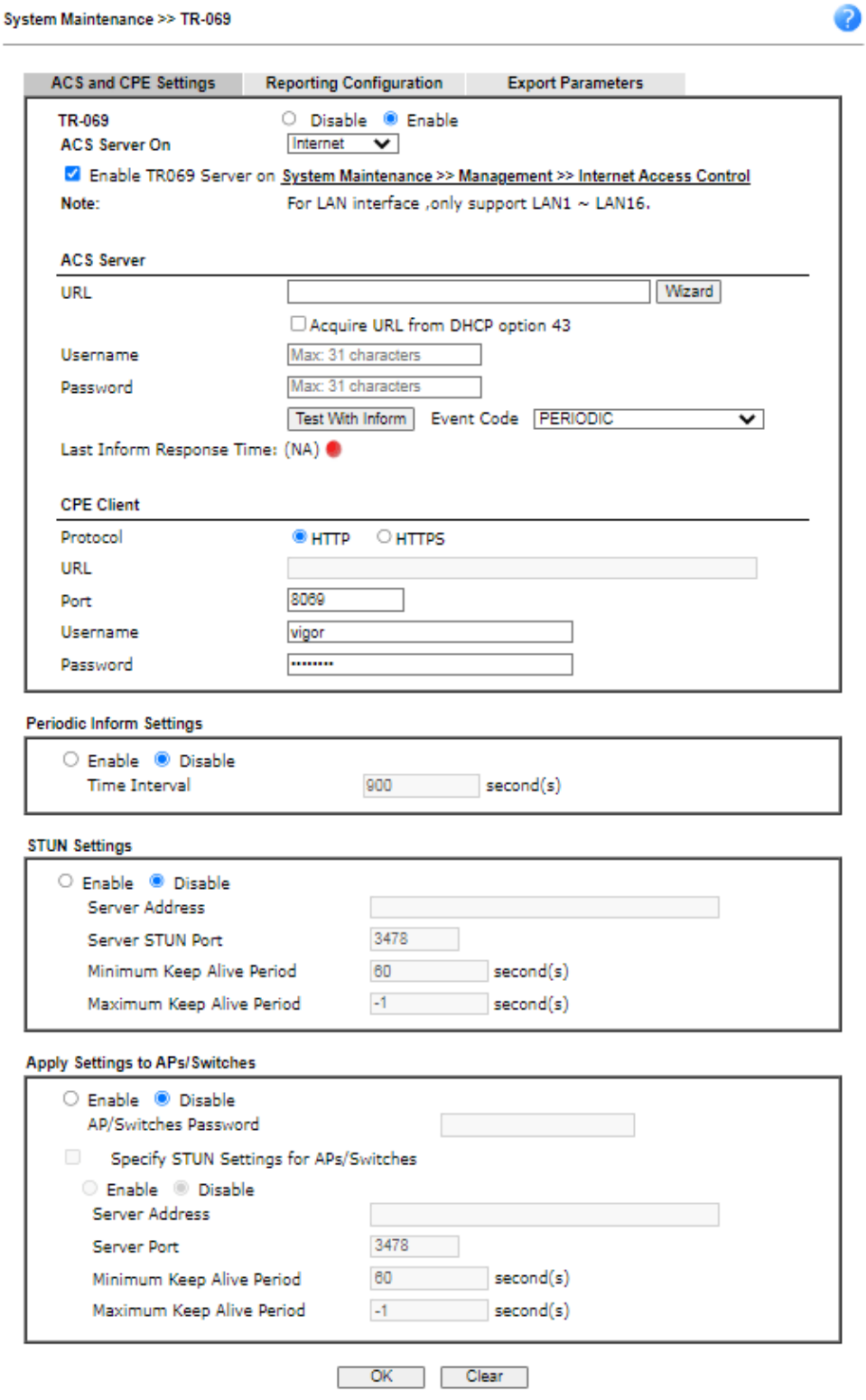
Item	Description
Model Name	Displays the model name of the router.
Firmware Version	Displays the firmware version of the router.
Build Date/Time	Displays the date and time of the current firmware build.
LAN	**MAC Address** - Displays the MAC address of the LAN Interface. **IP Address** - Displays the 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.

V-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.

V-1-2-1 ACS and CPE Settings



Available settings are explained as follows:

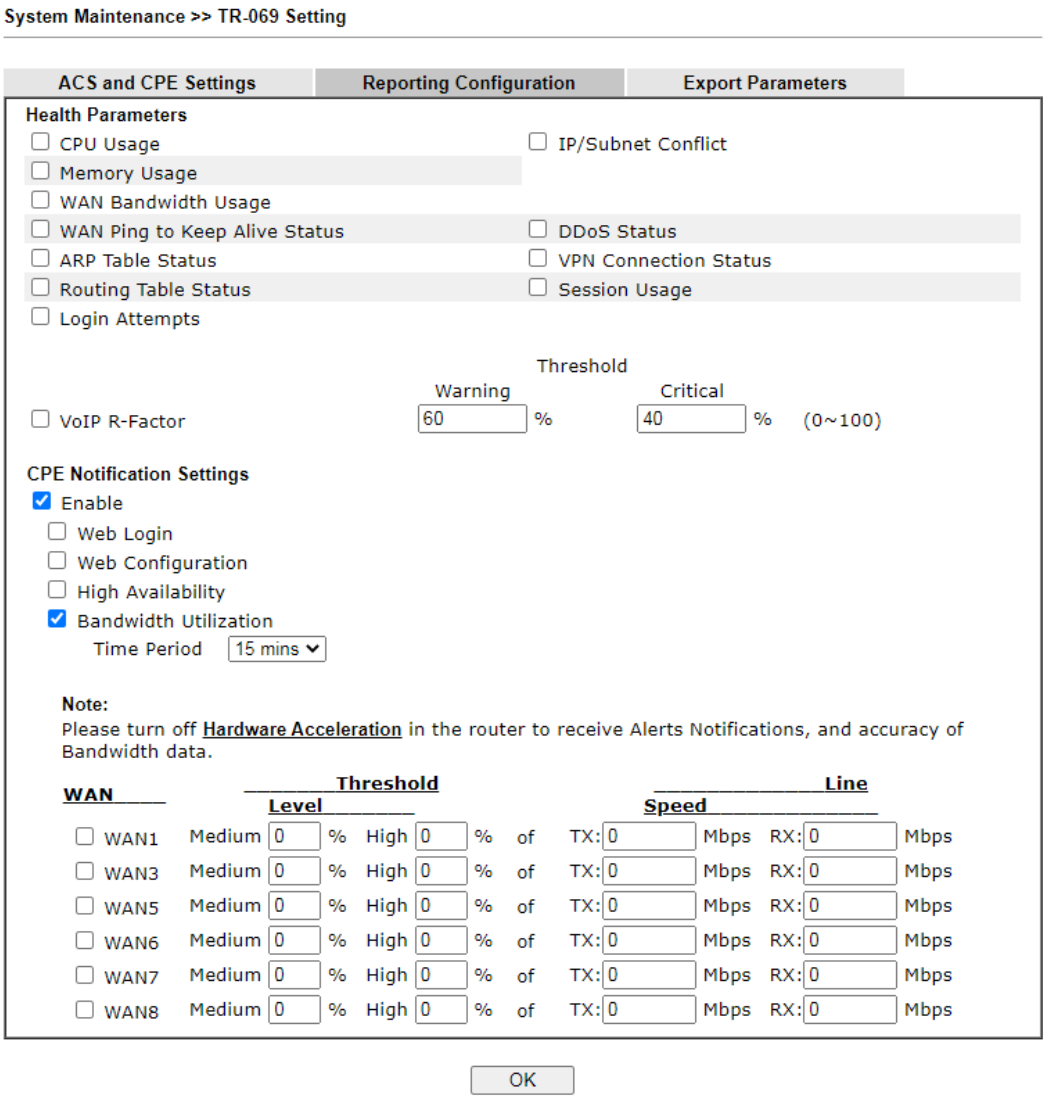
Item	Description
TR-069	Enables or disables TR-069 functionality.
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server.
Enable TR069 Server on System Maintenance >> Management >> Internet Access Control	If enabld, a user will be allowed to access into TR-069 from WAN.
ACS Server	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 STUN 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 Vigor router 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/Switches Password** – Enter the password of the VigorAP that you want to apply Vigor router'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 Vigor3910 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.

V-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.



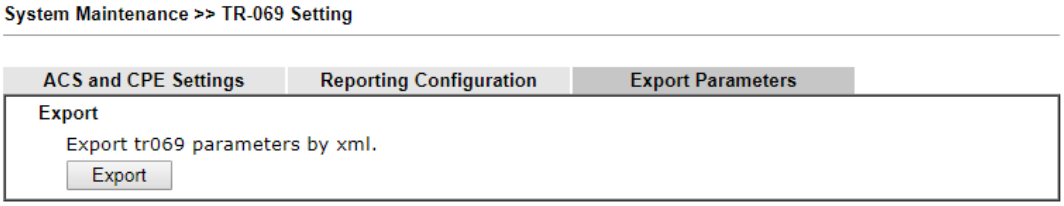
Available settings are explained as follows:

Item	Description
Health Parameters	Check the one that Vigor router will send the status information to VigorACS. **Threshold** (for VoIP R-Factor) - Once the quality of VoIP is lower than warning limit value or critical limit value, the router will send the result to VigorACS.
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.

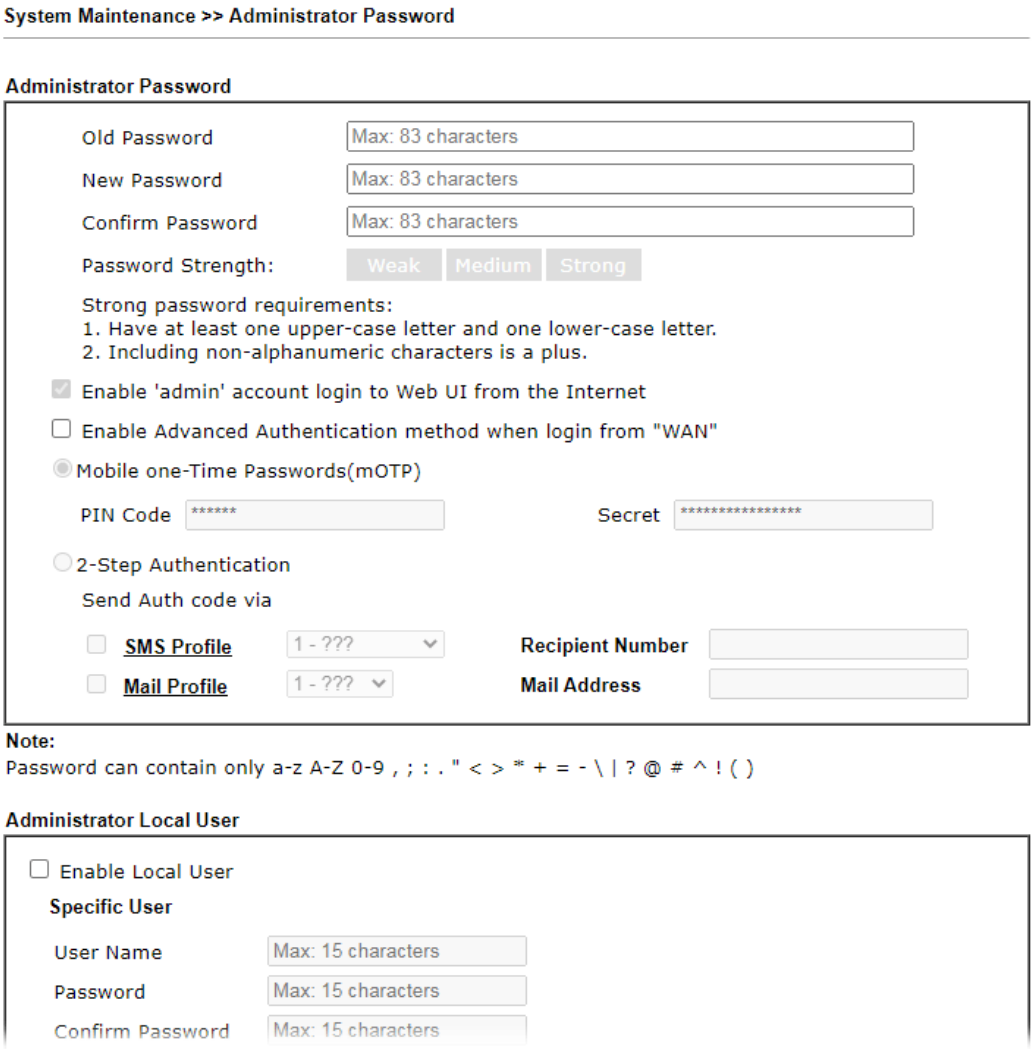
V-1-2-3 Export Parameters

Click **Export** to save the TR-069 parameter settings as an ".xml".



V-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. **Password Strength** - Shows the security strength of the password specified above. **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**

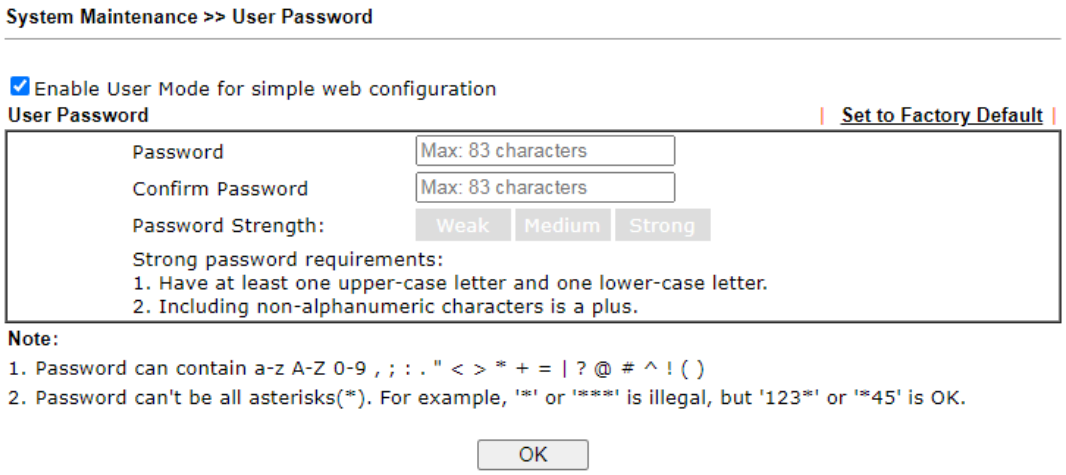
	"WAN" login – Advanced authentication method can offer a **more secure** network connection. Select to require mOTP or 2-step authentication when logging in from the WAN. • **Mobile one-Time Password (mOTP)** – Select to allow the use of mOTP passwords. Enter the PIN Code and Secret settings for getting 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. **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. • **Password** – Enter the password for the local user. • **Confirm Password** - Enter the new password again for confirmation. • **User Name and Password only** - If selected, you need to enter a user name and password. • **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. • **Enable Advanced Authentication method when login from "WAN"**– Advanced authentication method can offer a **more secure** network connection. Select to require mOTP or 2-step authentication when logging in from the WAN. • **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. • **Local User List** – Shows all the users that are set up to administer the router.
Administrator LDAP Setting	**Enable LDAP/AD login for admin users** – Select to allow authentication using an LDAP/Active Directory Server. **LDAP Server Profiles Setup** – Click to set up the LDAP/Active

	Directory server.
Administrator TACACS+ Setting	**Enable TACACS+ login for admin users** – If it is enabled, any user can access into the web user interface of Vigor router through the TACACS+ server authentication. ● **Fallback to local Authentication** - If it is enabled, the administrator can use other login methods for authentication once the TACACS+ server has no response.

Click **OK** to save changes on the page, and you will be directed to the login screen. Please log in with the new password.

V-1-4 User Password

This page allows you to set new password for user operation.



Available settings are explained as follows:

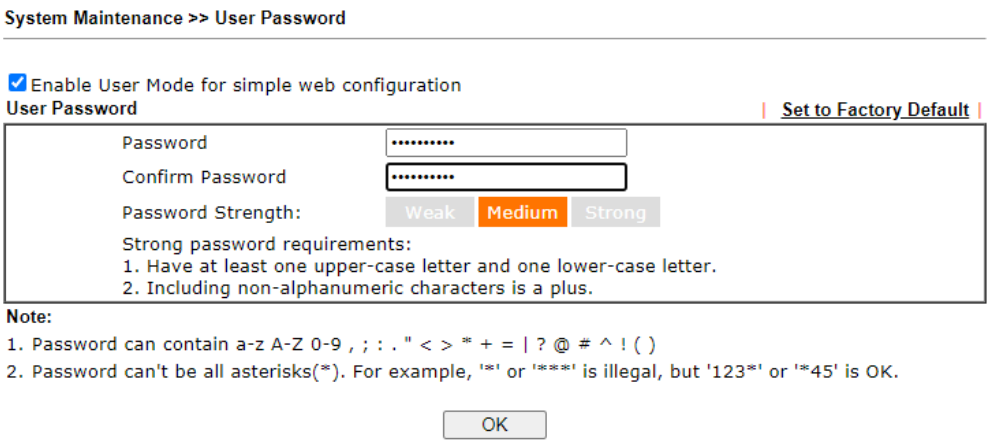
Item	Description
Enable User Mode for simple web configuration	Check this box to enable User Mode for web user interface with the password typed here for simple web configuration. The simple web user interface settings differ from those on the full web user interface seen when logged in using the administrator 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.

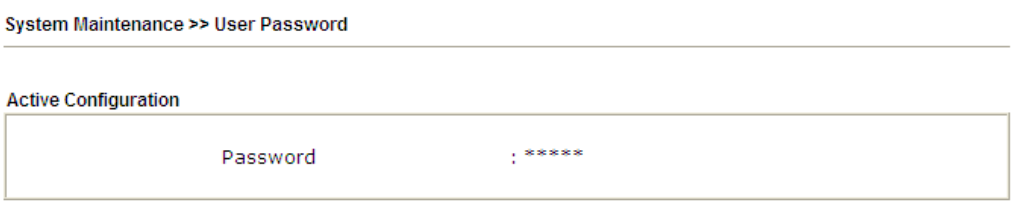
Here are the steps involved in setting up the router for User Mode Access:

1. Navigate to **System Maintenance>>User Password** in the web user interface.

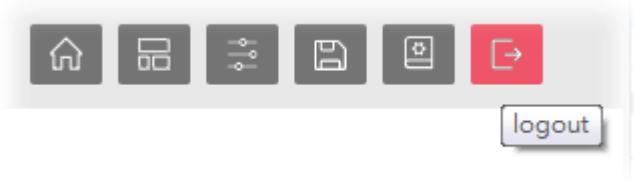
2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Enter a new password in the field of New Password and click **OK**.



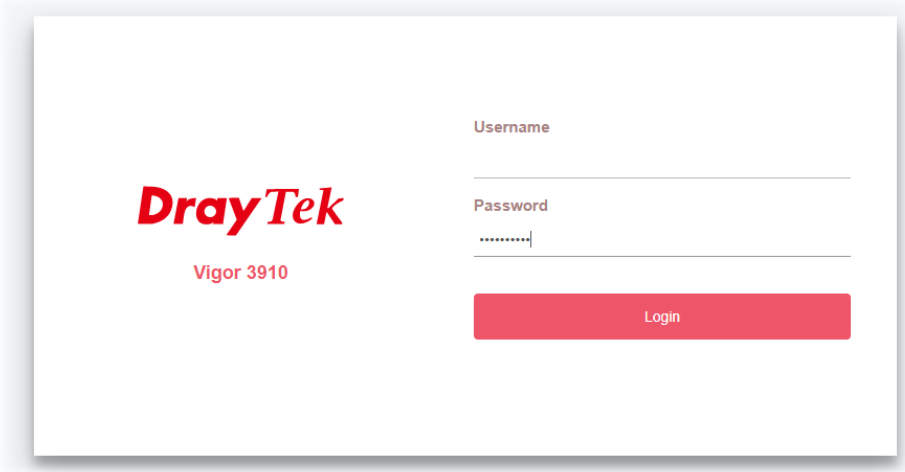
3. The following screen will appear. Simply click **OK**.



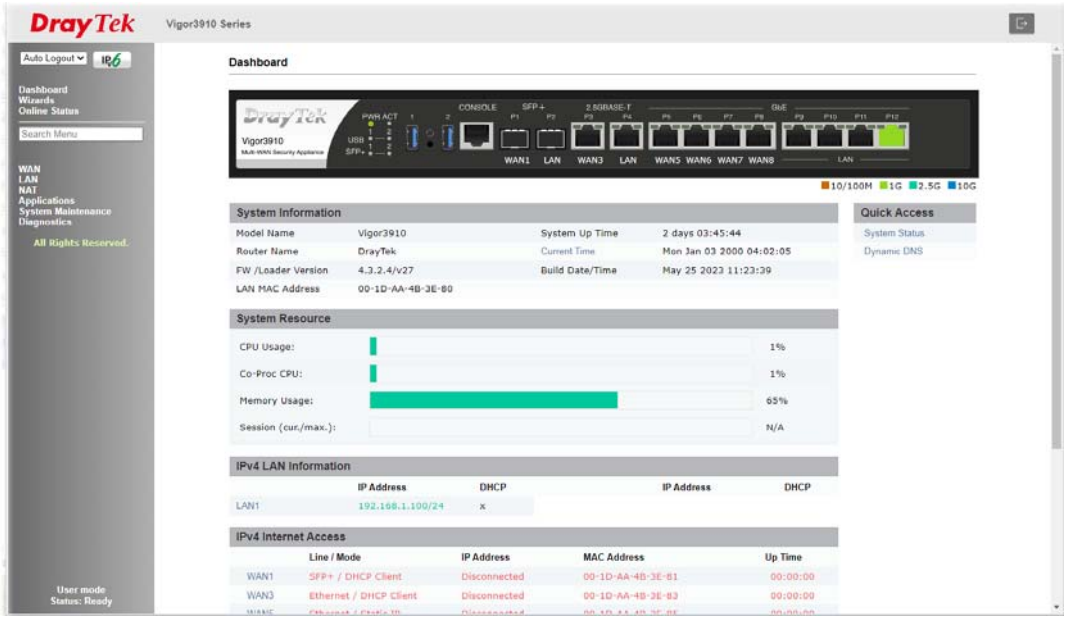
4. Log out the Vigor router web user interface by clicking the Logout button.



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:



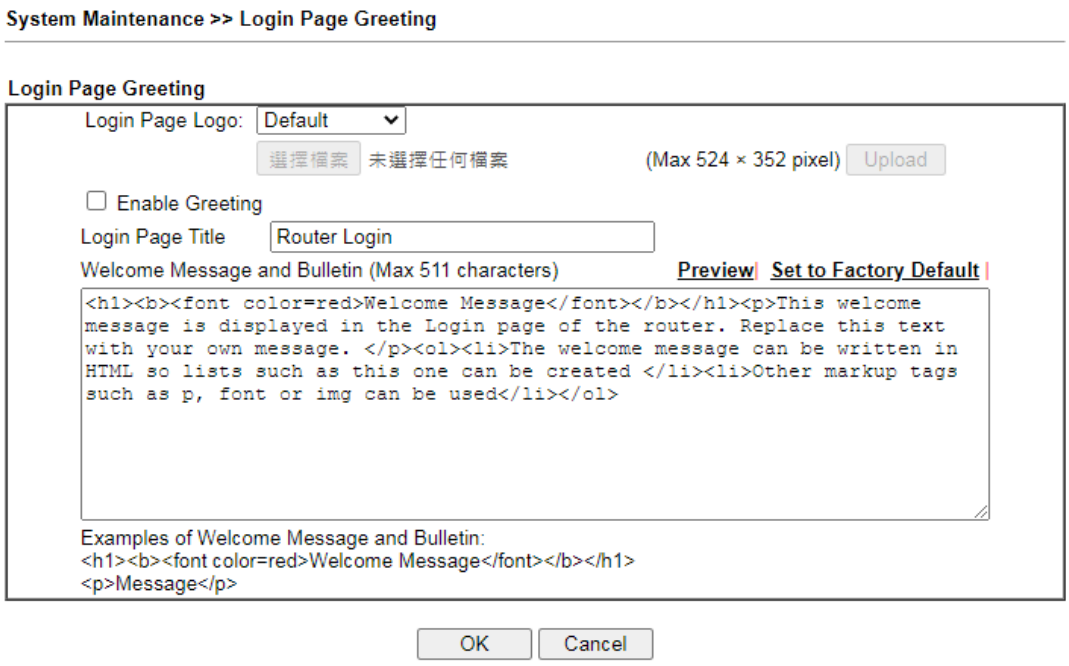
Only basic settings are available in User Mode. These are a subset of the Admin Mode settings.

Info	Setting in User Mode can be configured as same as in Admin Mode.

V-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.

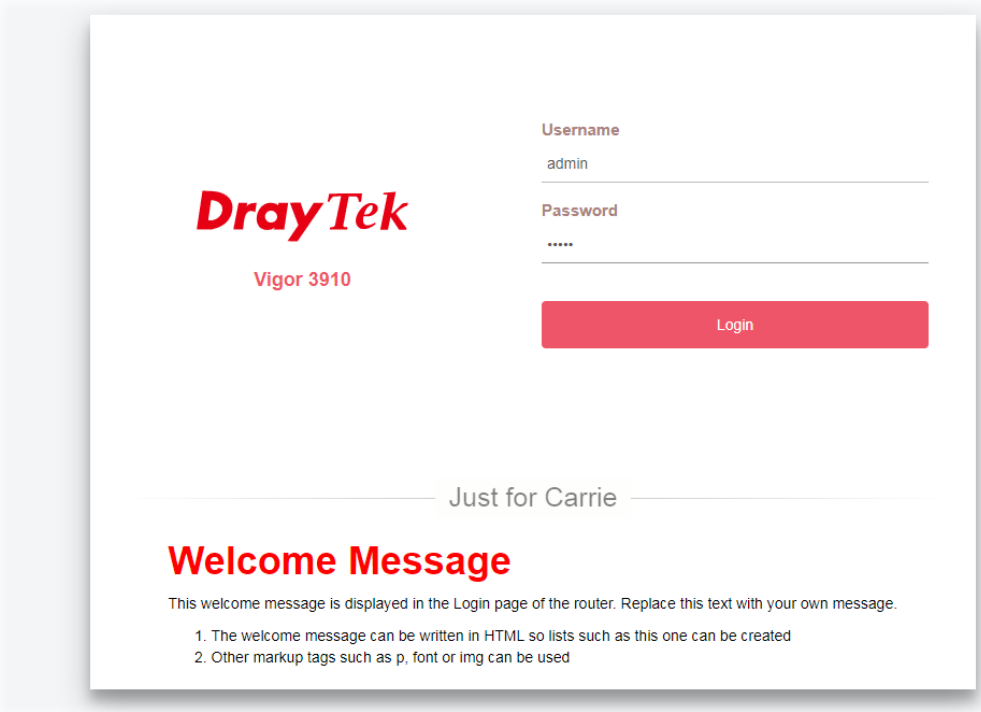
This section allows you to customize the login page by adding a message and/or setting the page title.



Available settings are explained as follows:

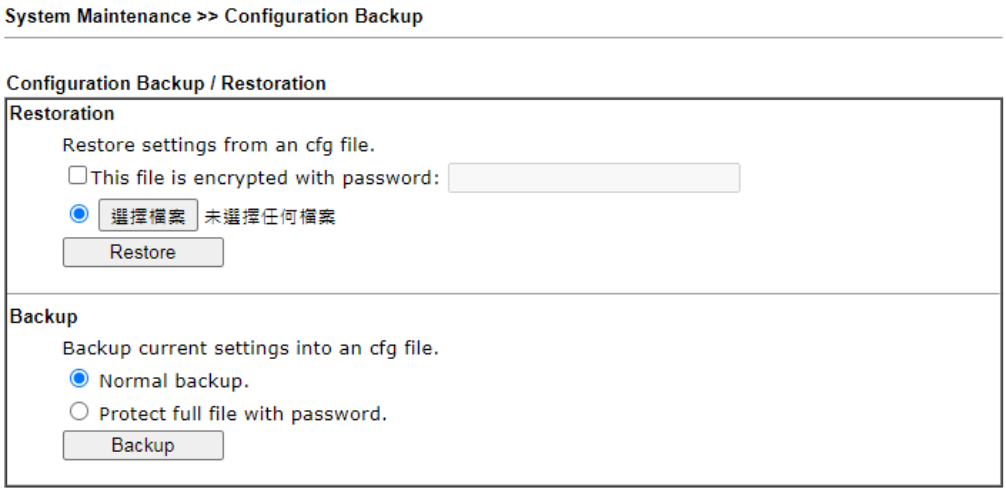
Item	Description
Login Page Logo	Set an image which will be shown above the log in window. **Default -** The **Enable Greeting** feature is available to set the login page title. **Blank -** No image / no greeting. **Upload a file -** Choose an image file and click **Upload**. Later the selected image 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.

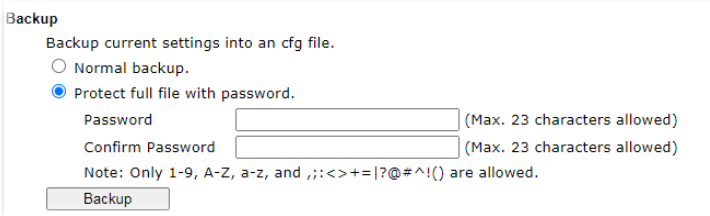

DrayTek
Vigor 3910
Username
admin
Password
Login
Just for Carrie
Welcome Message
This welcome message is displayed in the Login page of the router. Replace this text with your own message.
1. The welcome message can be written in HTML so lists such as this one can be created
2. Other markup tags such as p, font or img can be used

V-1-6 Configuration Backup

This function allows the backup and restoration of Vigor router settings.



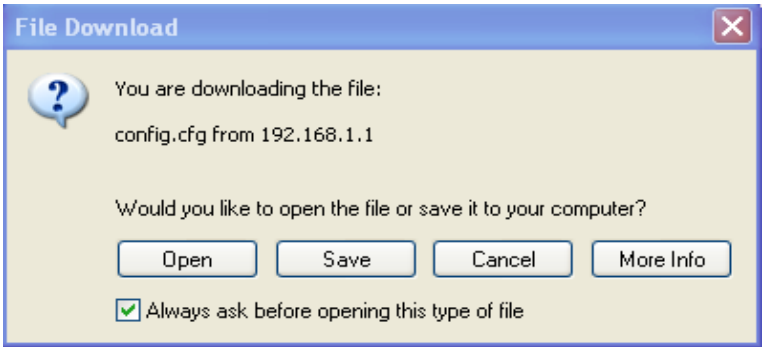
Available settings are explained as follows:

Item	Description
Restore	**Restore settings from an cfg 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. **This file is encrypted with password** – Select to specify a password. **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. **Normal backup** - Select to backup without a password. **Protect full file 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.

Backing up the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**.
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**.

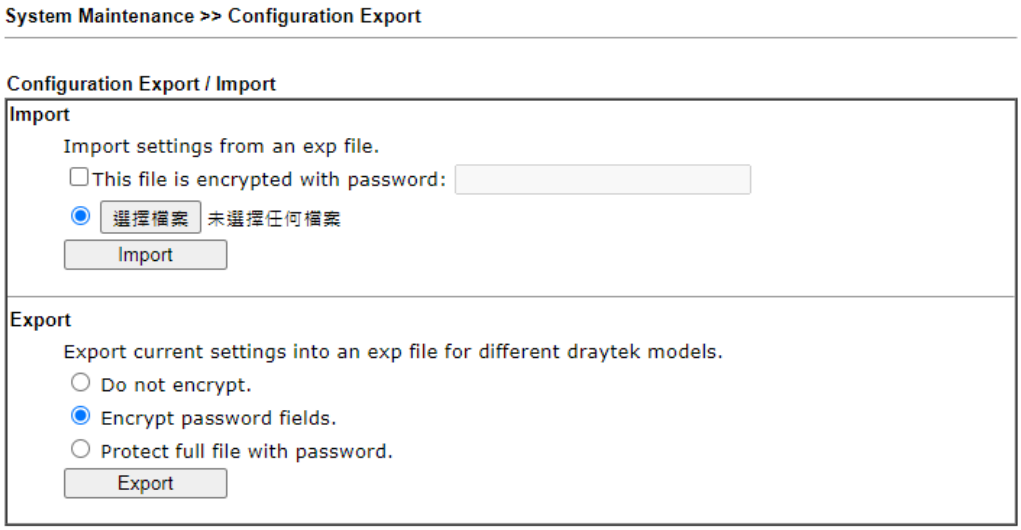
Restoring the Configuration

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be shown.
2. Click the **Choose File** button under **Restoration** 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.

V-1-7 Configuration Export

Configuration for Vigor3910 can be exported as an user-readable text-based (.exp) file which can be applied to other Vigor router.

In addition, it is possible to import an ".exp" file from other DrayTek routers onto the Vigor3910.

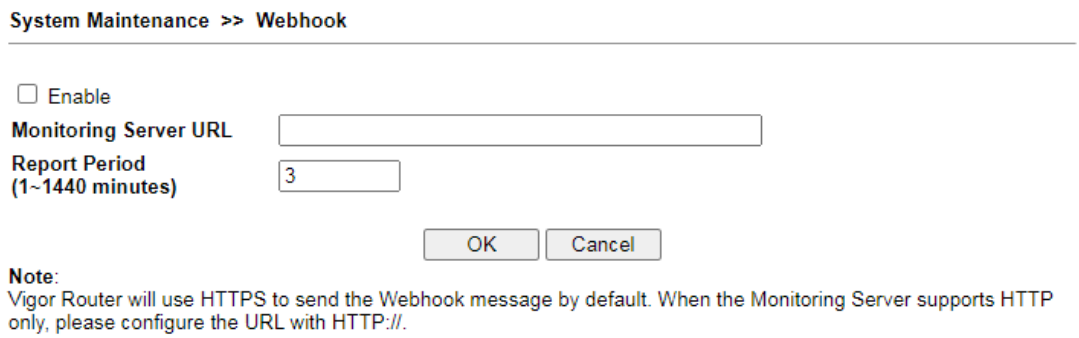


Available settings are explained as follows:

Item	Description
Import	**This file is encrypted with password** – Check the box and enter a password for dencrypting the configuration file (if the.exp file is encrypted). Click the **Select File** button to specify an exp file. **Import** - Click to import a configuration file. If the file is encrypted, you will need to enter the password set on the above password field.
Export	**Do not encrypt** - The configuration file (.exp) will be output as an fully user-readable text-based file. **Encrypt password fields** - The configuration file (.exp) will be output as a user-readable text-based file except for password related fields (user passwords will be encrypted). **Protect full file with password** - The configuration file is protected by full encryption. The password will be needed when importing the "exp" file on Vigor router. **Export** - Click it to export the configuration of Vigor router as a file with the extension of "exp".

V-1-8 Webhook

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



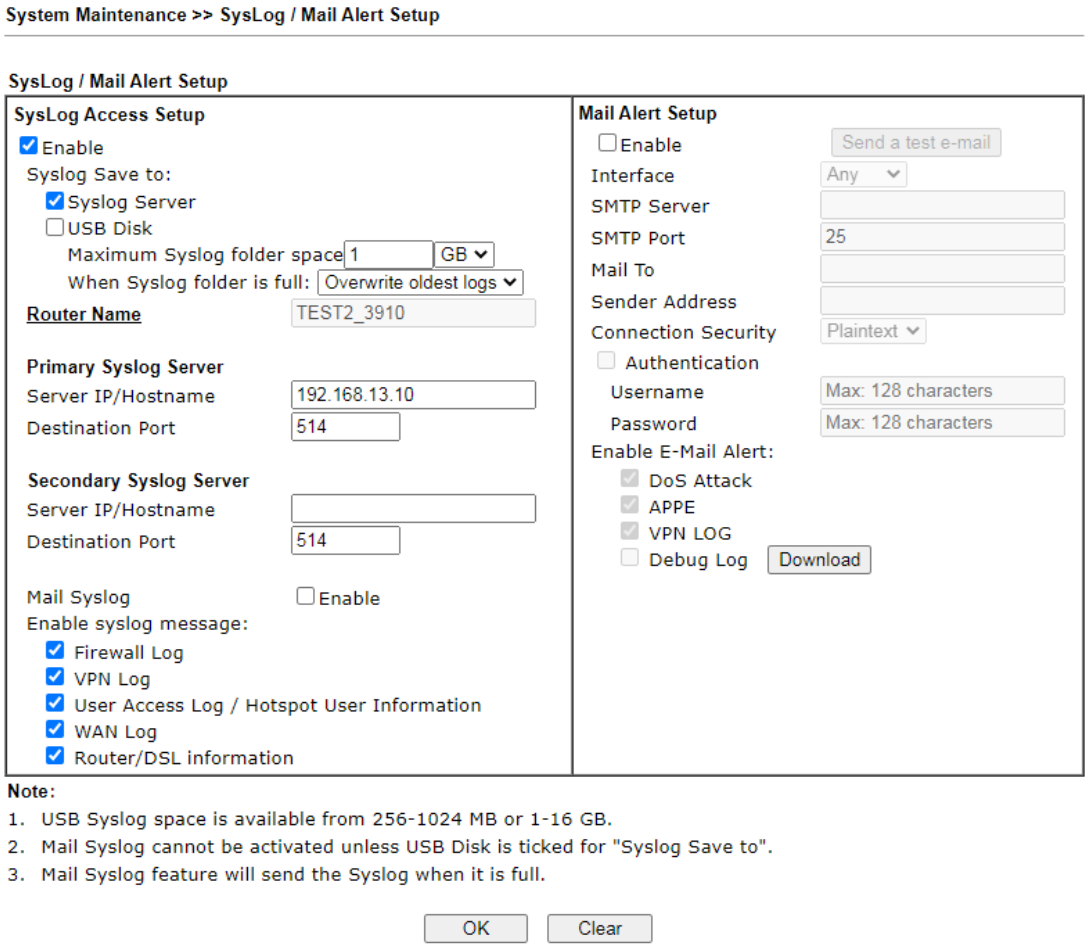
Available settings are explained as follows:

Item	Description
Enable	Select it to enable this function.
Monitoring Server URL	Enter the URL of a server.
Report Period	Define the interval time for each report to be sent.

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

V-1-9 Syslog/Mail Alert

SysLog function is provided for users to monitor router.



Available settings are explained as follows:

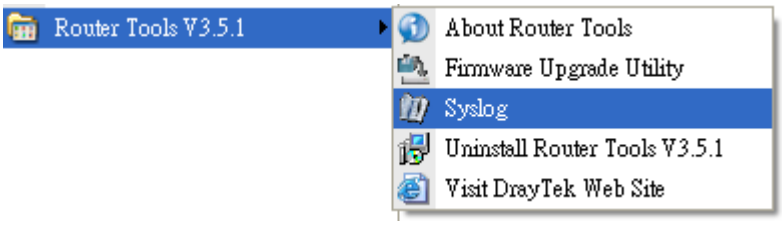
Item	Description
SysLog Access Setup	**Enable** - Check **Enable** to activate function of syslog. **Syslog Save to** – Check **Syslog Server** to save the log to Syslog server. Check **USB Disk** to save the log to the attached USB storage disk. ● **Maximum Syslog folder space** - Set the storage space as 1 GB or 1000MB. ● **When Syslog folder is full** - When Syslog folder is full, simply overwrite the oldest logs or stop logging.
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.
Primary Syslog Server /	**Primary Syslog Server / Secondary Syslog Server -** Vigor

Secondary Syslog Server	router will send the data to Syslog server for analysis based on the server settings configured here. It might send to both servers simultaneously if primary and secondary servers are set; or send to either one of the servers which has been set here. **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 -** Assign a mail address for sending mails out. **Connection Security** - Select a method (Plaintext, SSL or StartTLS) to ensure the connection security. SSL means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. ● Accept using plain text if StartTLS connection failed. ● Force StartTLS. Stop if StartTLS connection failed. **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.

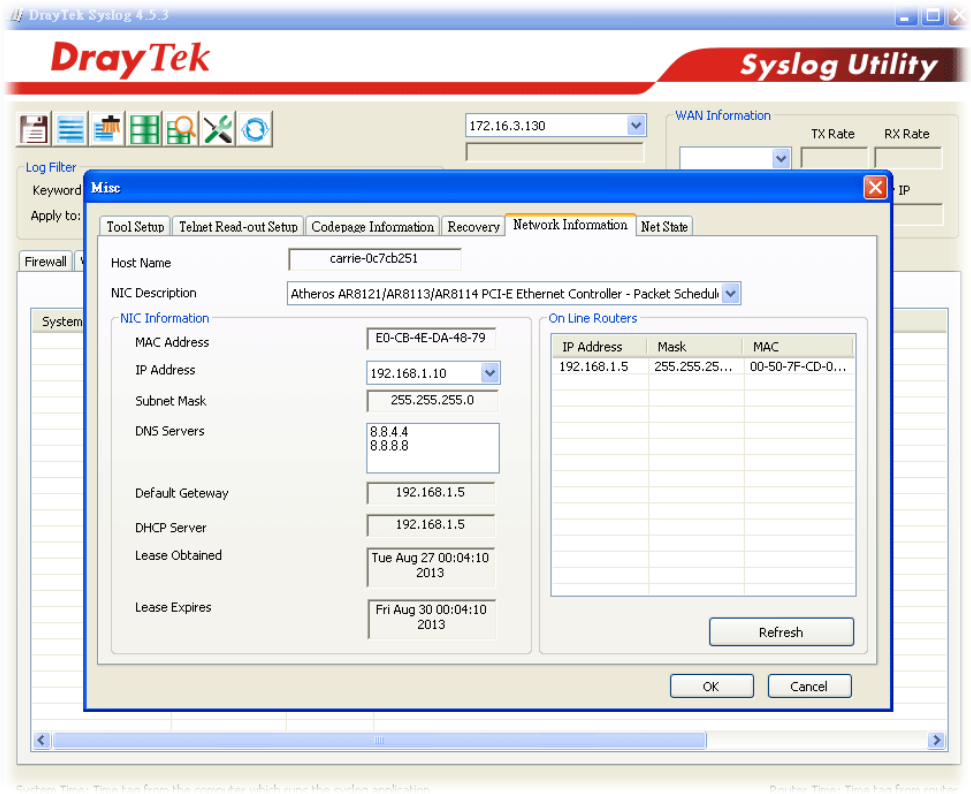
Select **OK** to save changes on the page, or **Clear** to reset all settings to factory defaults.

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. On the **Syslog / Mail Alert Setup** screen, enter the monitor PC's IP address in the **Server IP Address** field.

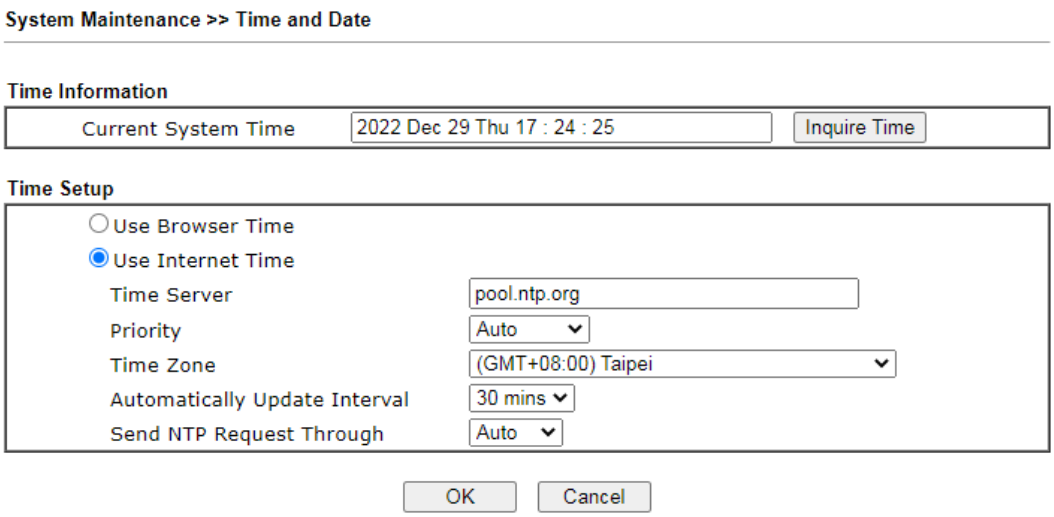


3. In the Syslog application, select the router you wish to monitor. Rember to select the network adapter to be used to connect to the router under Network Information, or else Syslog traffic cannot be received from the router.



V-1-10 Time and Date

This section allows you to configure settings related to the system date and time.



Available settings are explained as follows:

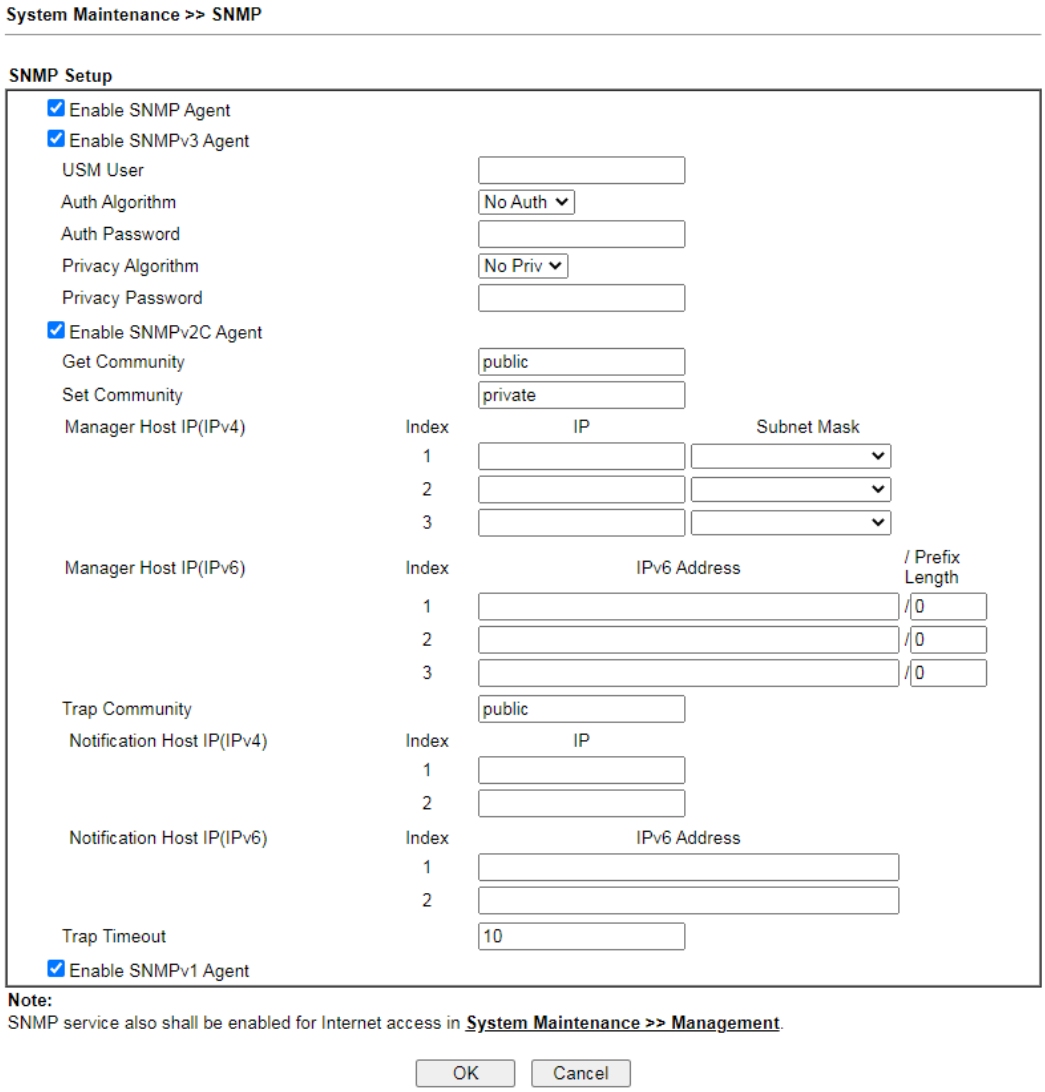
Item	Description
Current System Time	Click **Inquire Time** to retrieve the current time from the time server.
Use Browser Time	Select this option to let the router set its system time using the time reported by the web browser.
Use Internet Time	Select this option to let the router set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP).
Time Server	Enter the IP address / Host name of the time server.
Priority	Select **Auto** or **IPv6 First** as the priority.
Time Zone	Select the time zone where the router is located.
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.

V-1-11 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, SNMv2C, and / or SNMPv3 agent.
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.
Enable SNMPv2C Agent	Check to enable SNMPv2C function.
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 SNMPv1 Agent	Check to enable SNMPv1 function.

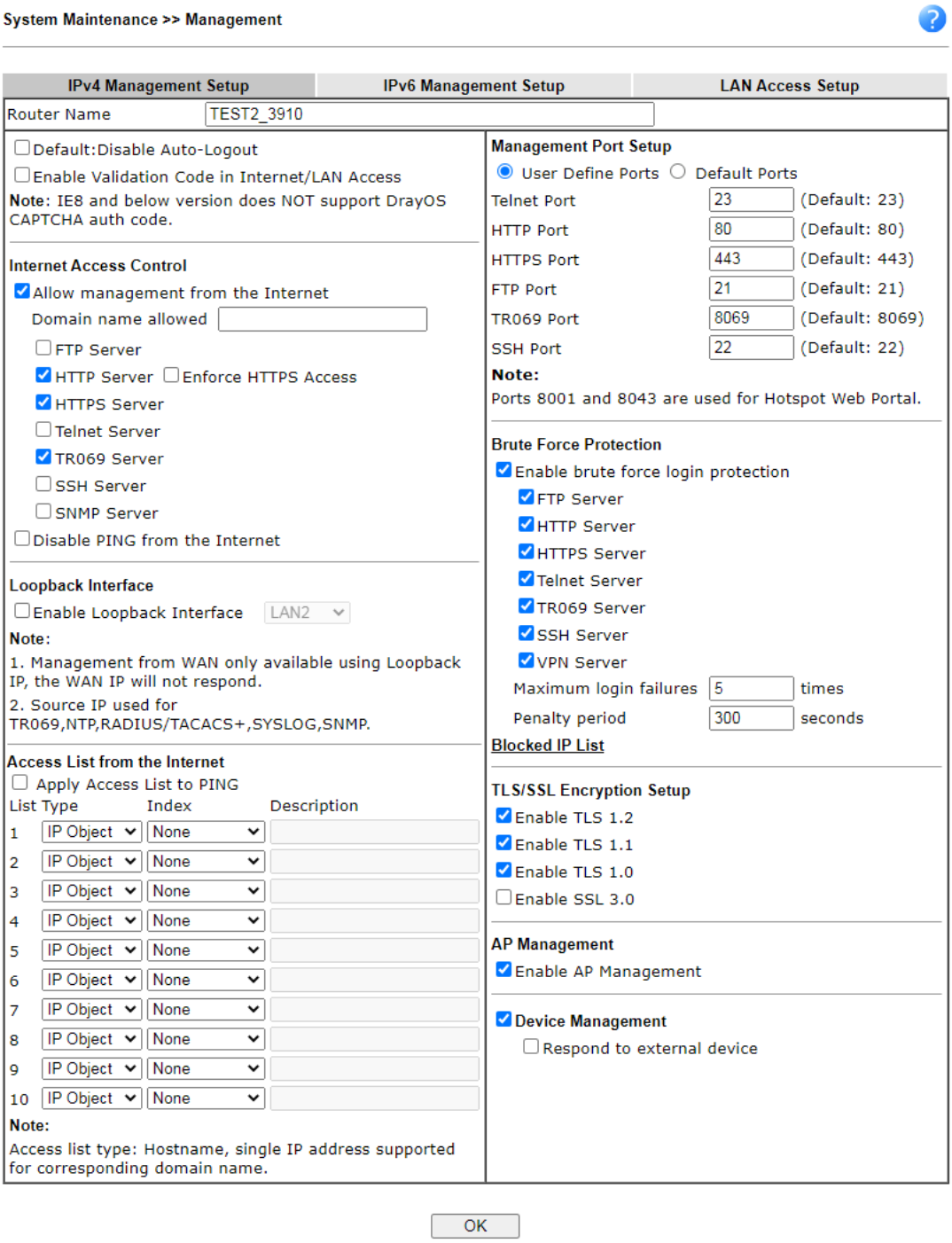
Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

V-1-12 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.

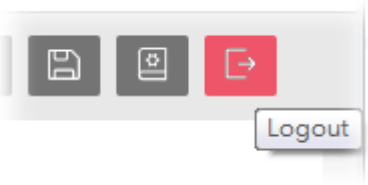
The management pages for IPv4 and IPv6 protocols are different.

V-1-12-1 IPv4 Management Setup



Available settings are explained as follows:

Item	Description

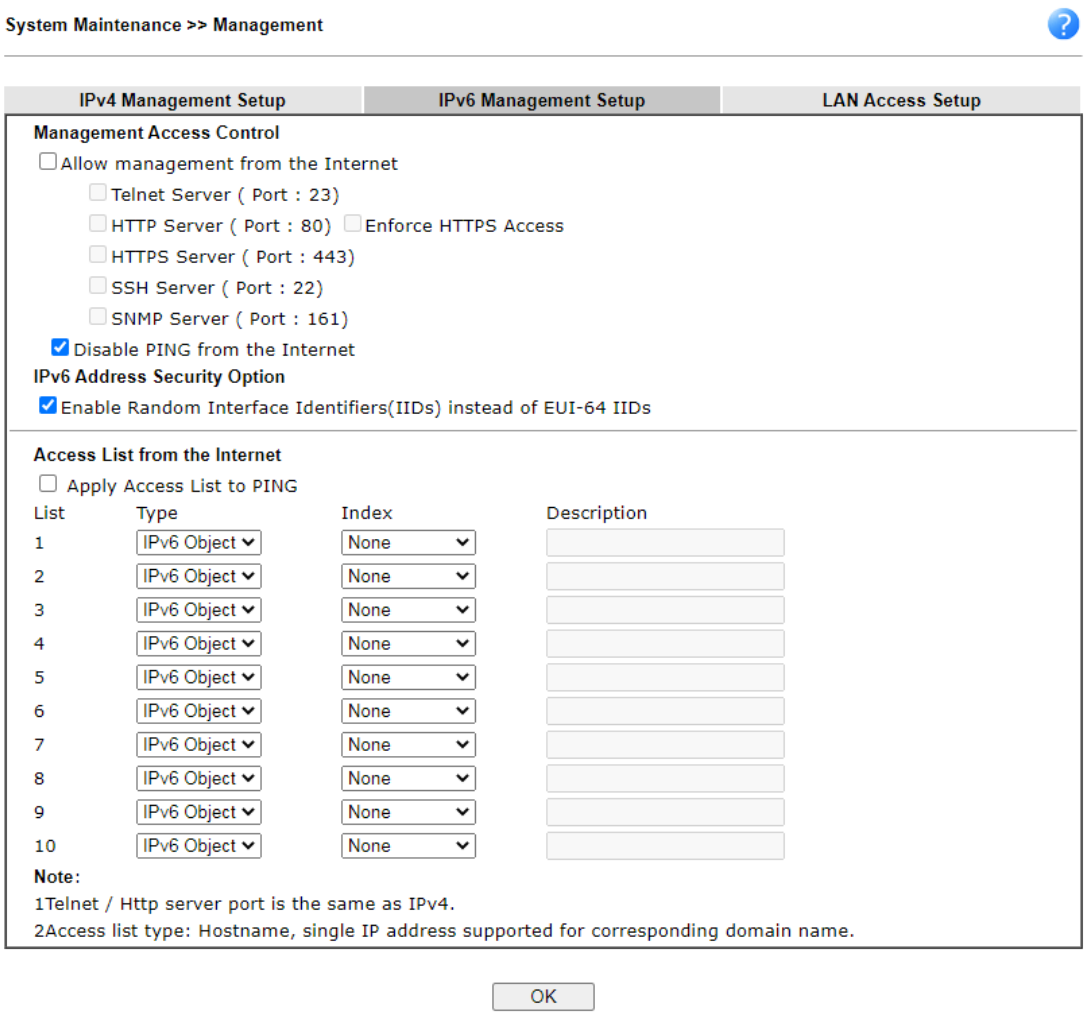
Router Name	Enter the router name as provided by ISP.
Default: Disable Auto-Logout	If enabled, the auto-logout function for the web user interface will be disabled. The web user interface will not terminate until you manually click the Logout icon. 
Enable Validation Code in Internet/LAN Access	If enabled, 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.
Loopback Interface	A loopback interface is a logical virtual interface created on a router simulating a real interface. This can be used to connect to management services such as Web (HTTPS), SNMP, ACS (TR069), Syslog, or SSH as well as authentication services such as TACACS+ or RADIUS instead of using a LAN IP. For the authentication function, using the dedicated loopback address will reduce the administrative overhead since there is no need to add multiple router IP addresses to the AAA server. In addition, security will be enhanced by isolating authentication from the user network. Using a loopback address means the virtual interface is always up, especially when the CPE has multiple WAN interfaces. For example, if BGP connected on WAN1 is down, management and AAA traffic can be routed to the defined loopback interface through the VPN tunnel connected on WAN2. Another benefit is that the loopback IP can be an IP address (with a 32-bit mask). This means that the interface is not assigned to any LAN port, which improves security and saves a lot of IP address space. We can imagine that if we assign 24-bit mask IPs to many managed routers, there will be insufficient network IPs.

	Enable Loopback Interface - Select to enable the function of Loopback Interface. **LAN#**- Select a LAN subnet as the Loopback Interface.
Access List from the Internet	The ability of system administrators to log into the router can be restricted to up to 10 specific hosts or networks. **Apply Access List to PING** - When this option is checked and **Disable PING from the Internet** is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if **Disable PING from the Internet** is checked, which blocks all pings from the Internet. **Type** - Select **IP Object** or **Hostname.** **Index** - Select the index number of a configured IP object, keyword object or IP group object. **Description** - Shows a brief comment for the selected IP object (with subnet mask).
Management Port Setup	**User Define Ports -** Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers. **Default Ports -** Check to use standard port numbers for the Telnet and HTTP servers.
Brute Force Protection	Any client trying to access into Internet via Vigor router will be asked for passing through user authentication. Such feature can prevent Vigor router from attacks when a hacker tries every possible combination of letters, numbers and symbols until find out the correct combination of password. **Enable brute force login protection –** 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 and TLS 1.0/1.1/1.2 –** Check the box to enable SSL 3.0/1.0/1.1/1.2 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, Vigor3910 will function as a slave device. When an external device (master

	device) sends packets to the Vigor3910 to attempt to manage it, the Vigor3910 will respond to the request coming from the external device which is able to manage Vigor3910.

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

V-1-12-2 IPv6 Management Setup



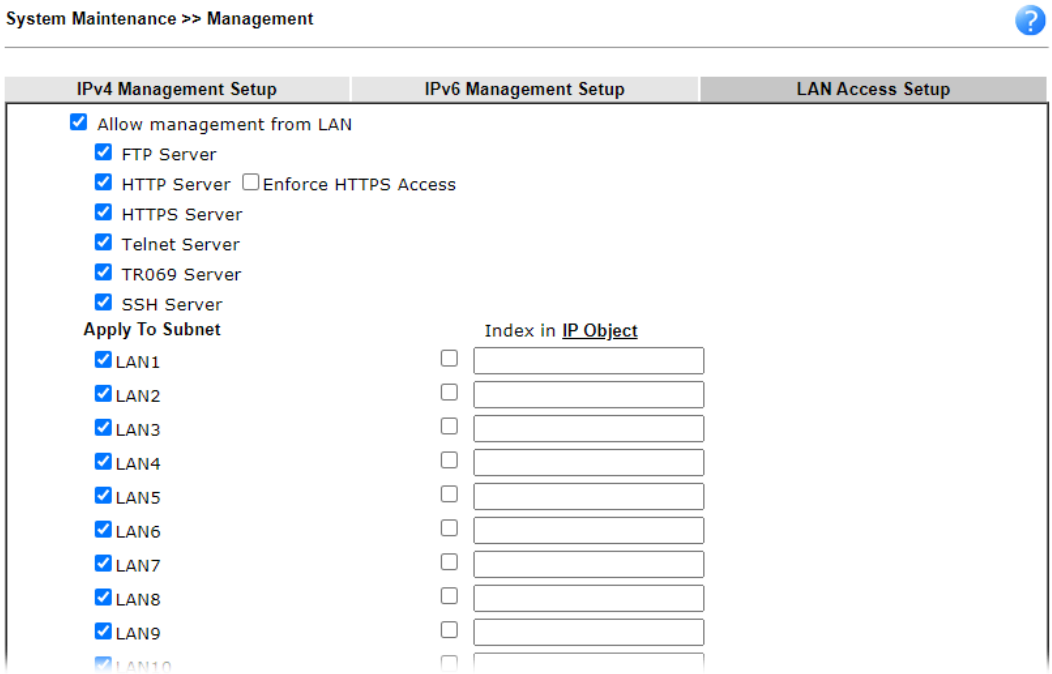
Available settings are explained as follows:

Item	Description
Management Access Control	**Allow management from the Internet** – Select to allow system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered. **Disable PING from the Internet -** Select 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 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, such that no pings from the Internet are accepted. **Type** - Select **IPv6 Object** or **Hostname**. **Index** - Select the index number of a configured IPv6 object.

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

V-1-12-3 LAN Access Control



Available settings are explained as follows:

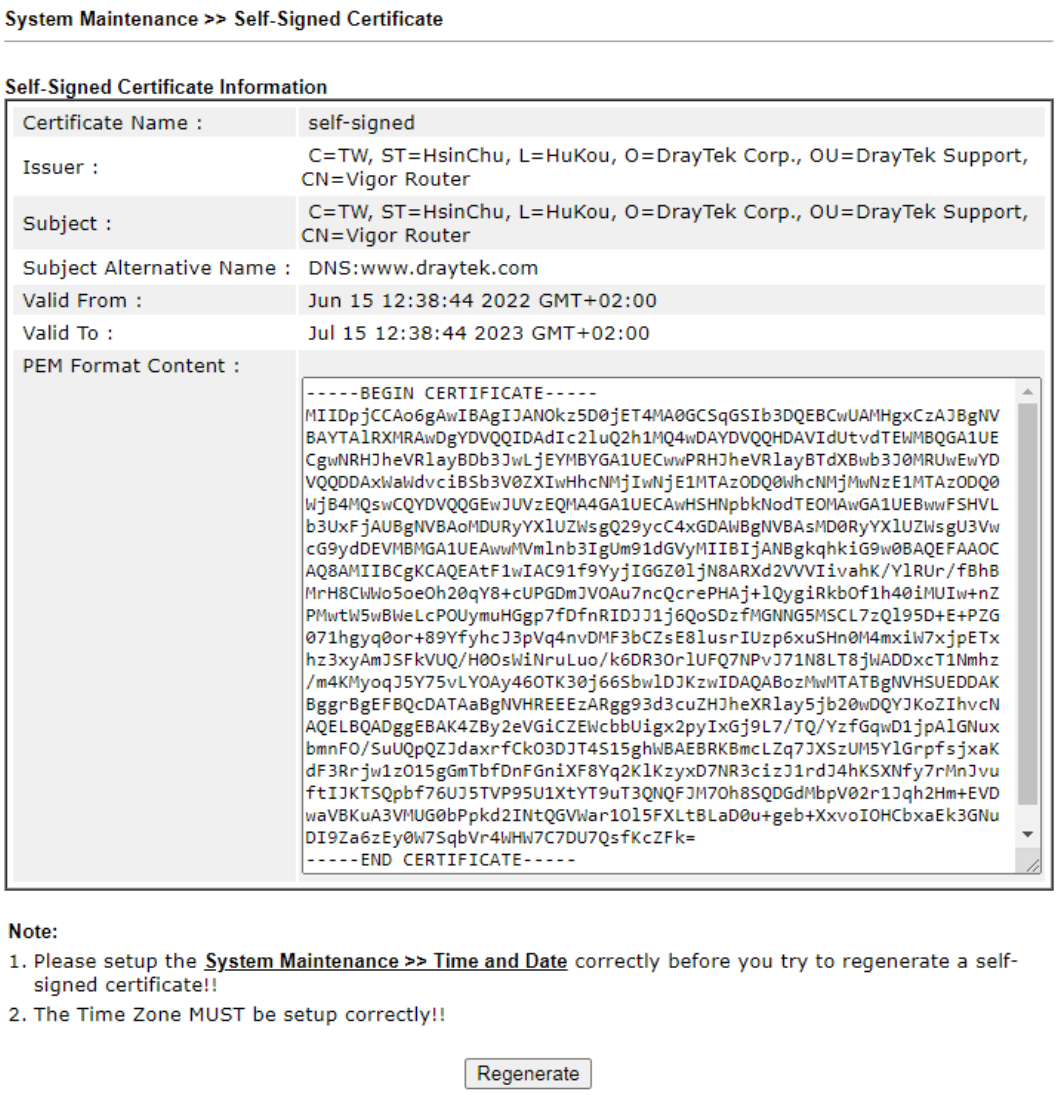
Item	Description
Allow management from LAN	Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.
Apply To Subnet	Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router. **Index in IP Object**- Type the index number of the IP object profile. Related IP address will appear automatically.

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

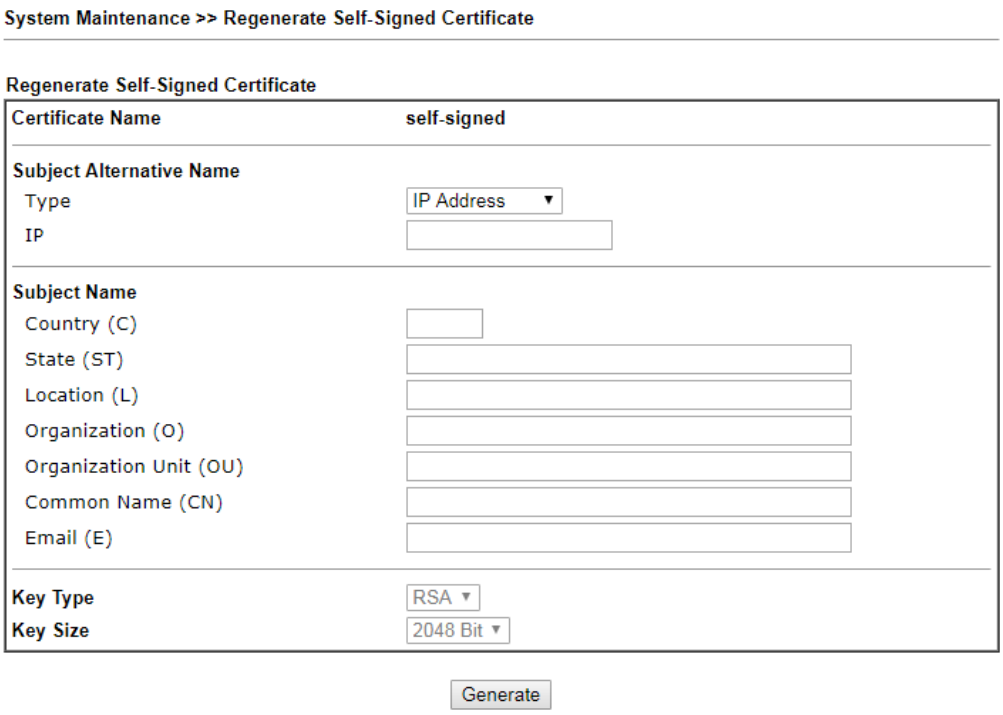
V-1-13 Self-Signed Certificate

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.



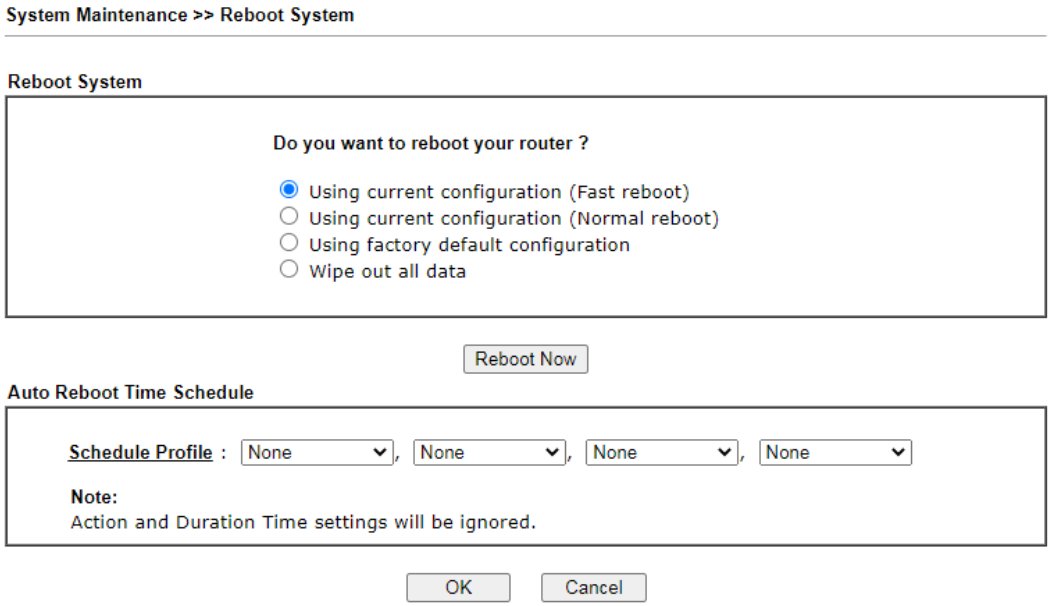
Click **Regeneration** to open **Regenerate Self-Signed Certificate** window.



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**.

V-1-14 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:

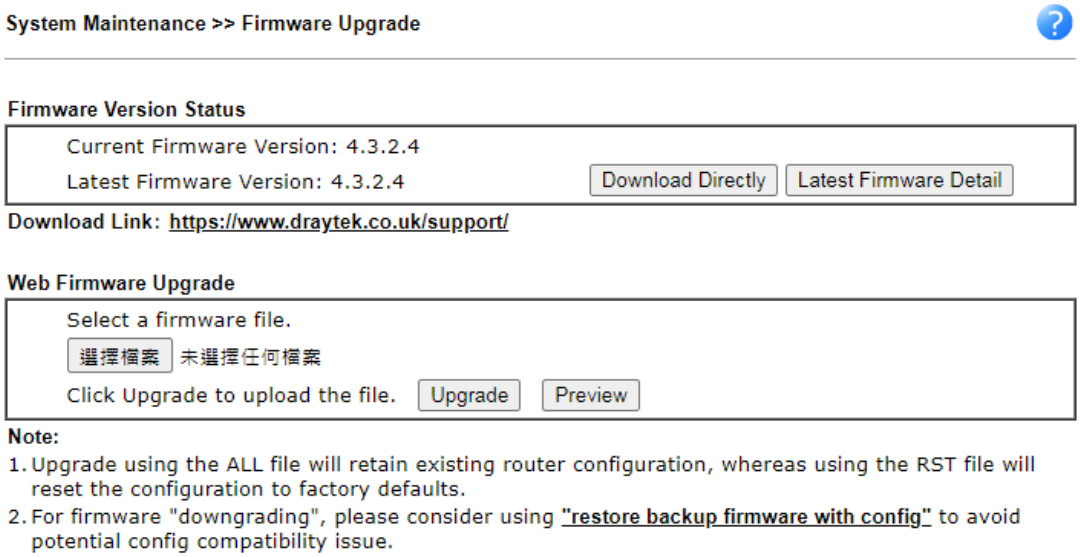
Item	Description
Reboot System	Select one of the following options, and press the **Reboot Now** button to reboot the router. **Using current configuration (Fast reboot/Normal reboot)** – Select this option to reboot the router using the current configuration. ● **Fast reboot** - Reboot the router quickly by a certain daemon. ● **Normal reboot** - Reboot the router with current configurations slowly and completely. **Using factory default configuration** – Select this option to reset the router's configuration to the factory defaults before rebooting. **Wipe out all data** - Select this option to wipe out all data.
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.

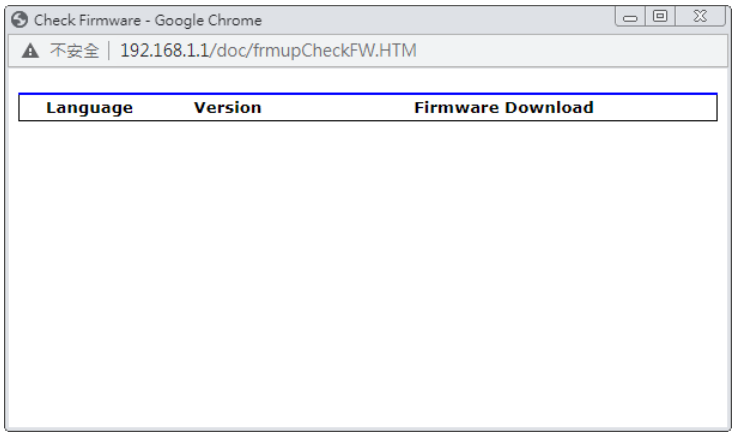
Info	When the system pops up Reboot System web page after you configure web settings, please click Reboot Now to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

V-1-15 Firmware Upgrade

Click **System Maintenance>> Firmware Upgrade** to upgrade firmware upgrade.



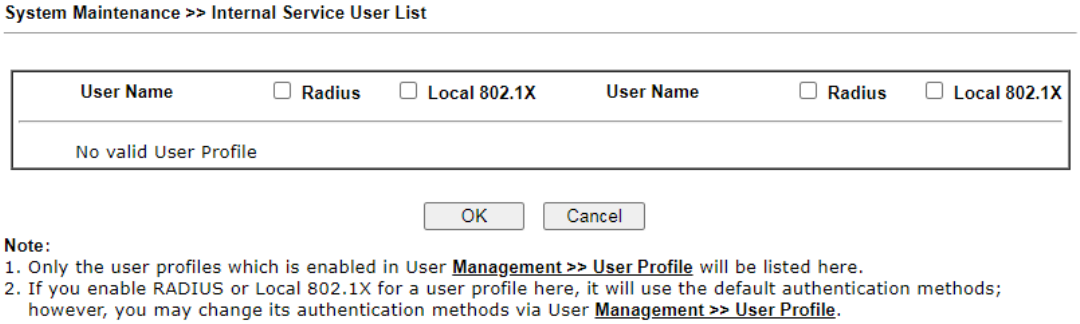
Available settings are explained as follows:

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. 
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:

V-1-16 Internal Service User List

User profiles (clients) defined and enabled in **User Management>>User Profile** will be displayed in this page.

Such page allows you to turn on or turn off security authentication service (offered by internal RADIUS and/or Local 802.1X) for each user profile without accessing into the User Management configuration page.



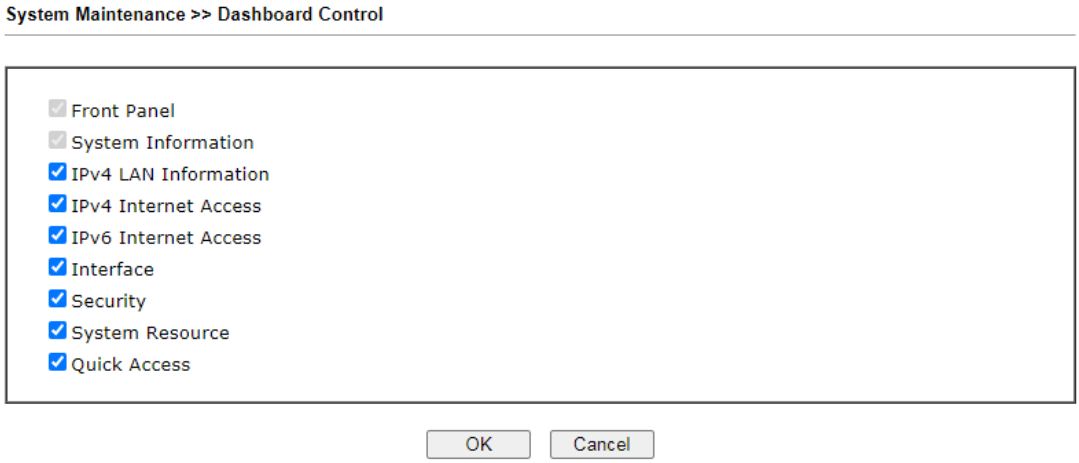
Available settings are explained as follows:

Item	Description
User Name	Display the name of the existed user profile. To modify the detailed settings, simply click the user name link to access into the web page for modification.
Radius	Check the box to turn on the security authentication service offered by internal RADIUS server for the user profile. Uncheck the box to turn off ecurity authentication service offered by internal RADIUS server for the user profile. If you check the box next to such item, all of the user profiles listed in this page will be enabled with RADIUS service enabled vice versa.
Local 802.1X	Check the box to turn on the security authentication service offered by Local 802.1X server for the user profile. Uncheck the box to turn off ecurity authentication service offered by Local 802.1X server for the user profile. If you check the box next to such item, all of the user profiles listed in this page will be enabled with Local 802.1X service enabled; vice versa.

Info	For the detailed setting (such as IP address, port number) configuration of internal RADIUS, refer to **Applications>>RADIUS/TACACS+**.

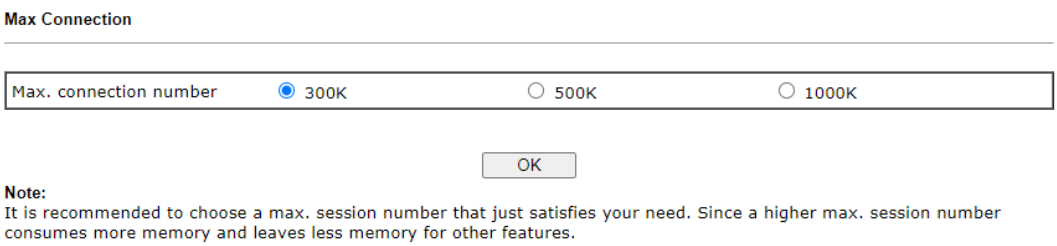
V-1-17 Dashboard Control

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.



V-1-18 Max Connection

Set the maximum NAT session number.



V-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.

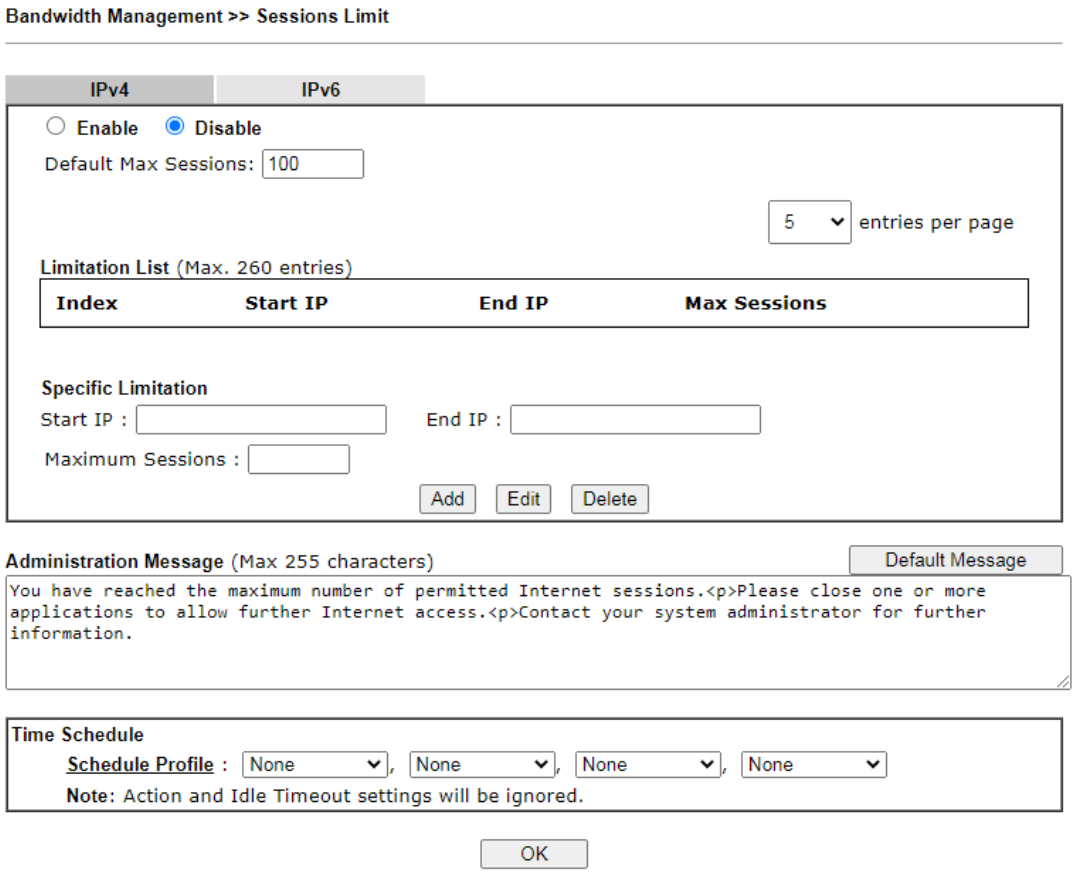
Web User Interface

Bandwidth management ensures efficient allocation of network bandwidth for various applications.

To set up Bandwidth Management, from the Main Menu, select **Bandwidth Management**.

V-2-1 Sessions Limit

To configure Sessions Limit, from the **Bandwidth Management** menu, select **Sessions Limit** to open the setup page.



To activate the function of limit session, simply click **Enable** and set the default session limit.

Available settings are explained as follows:

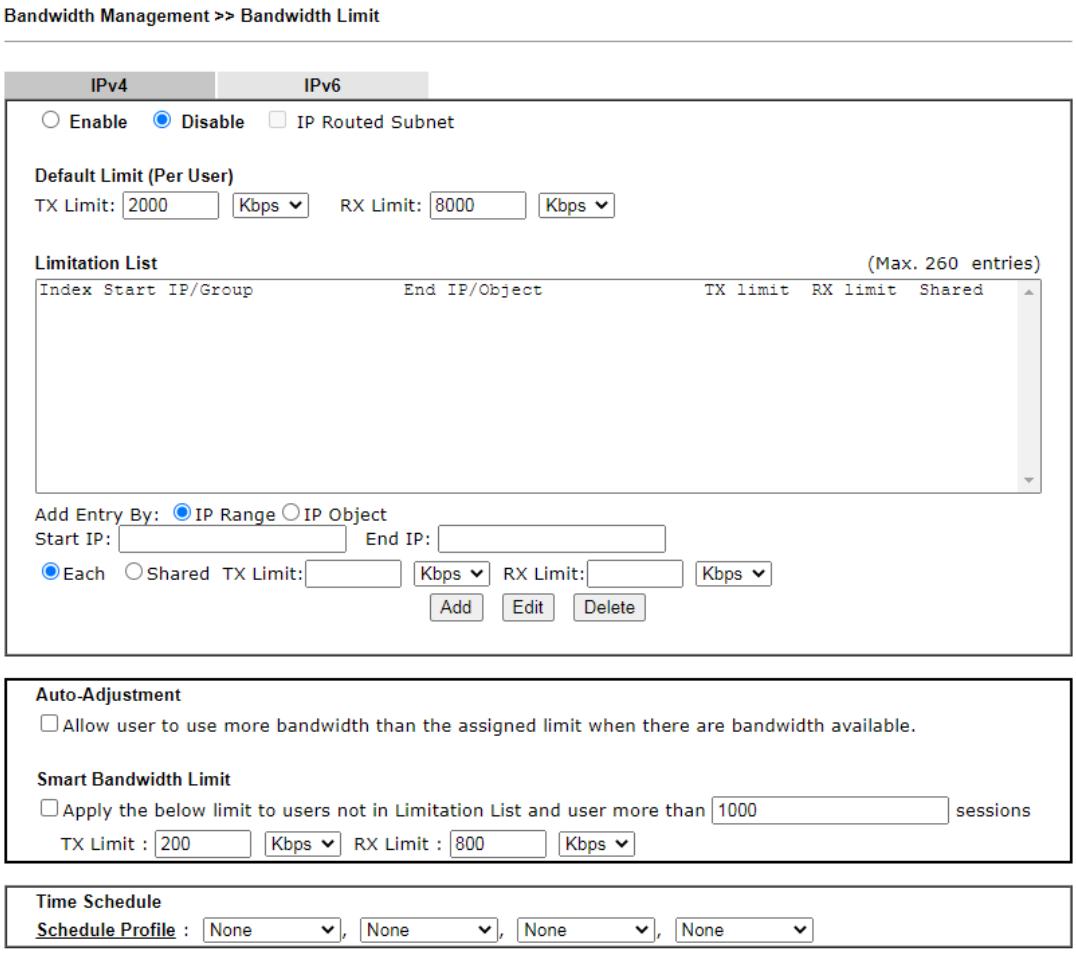
Item	Description
Enable/Disable	**Enable -** Select to activate session limit function. **Disable -** Select to deactivate session limit function. **Default Max Session -** The default maximum number of

	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**.

V-2-2 Bandwidth Limit

To configure the Bandwidth Limit feature, from the **Bandwidth Management** menu, select **Bandwidth Limit** to bring up the configuration page.



To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

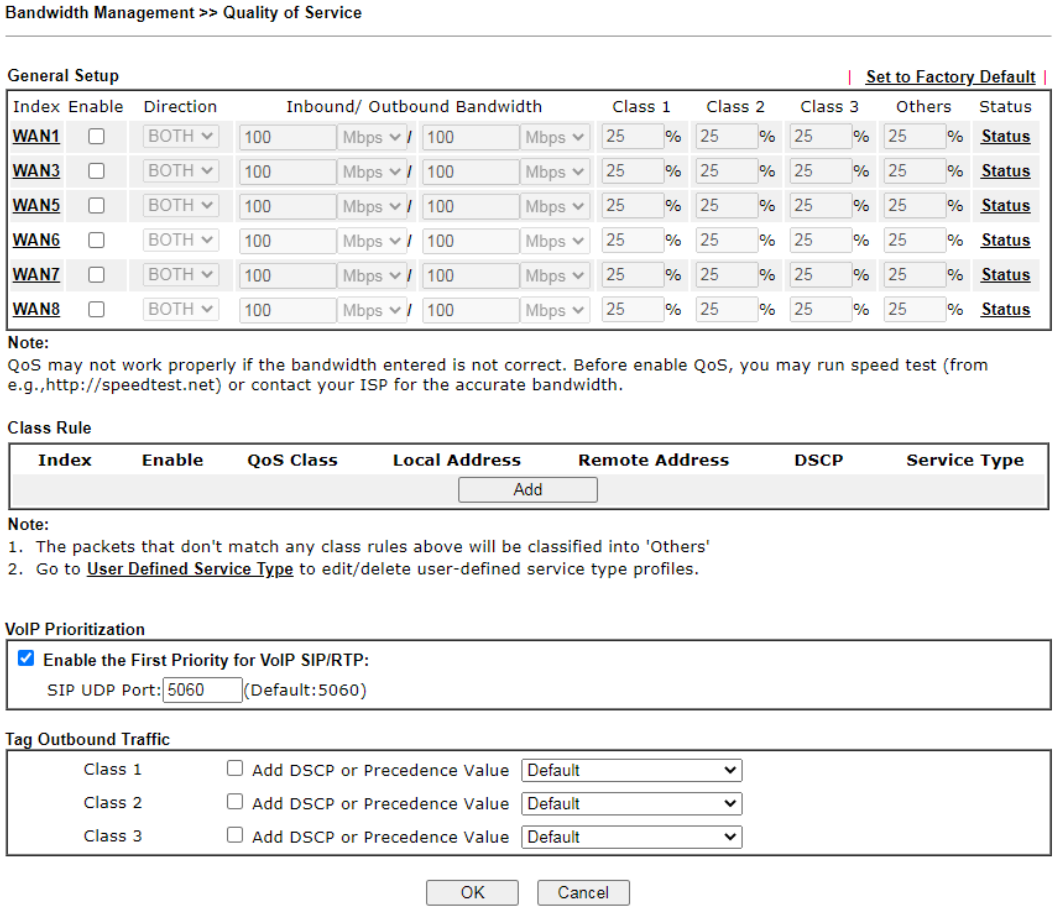
Available settings are explained as follows:

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.

V-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:

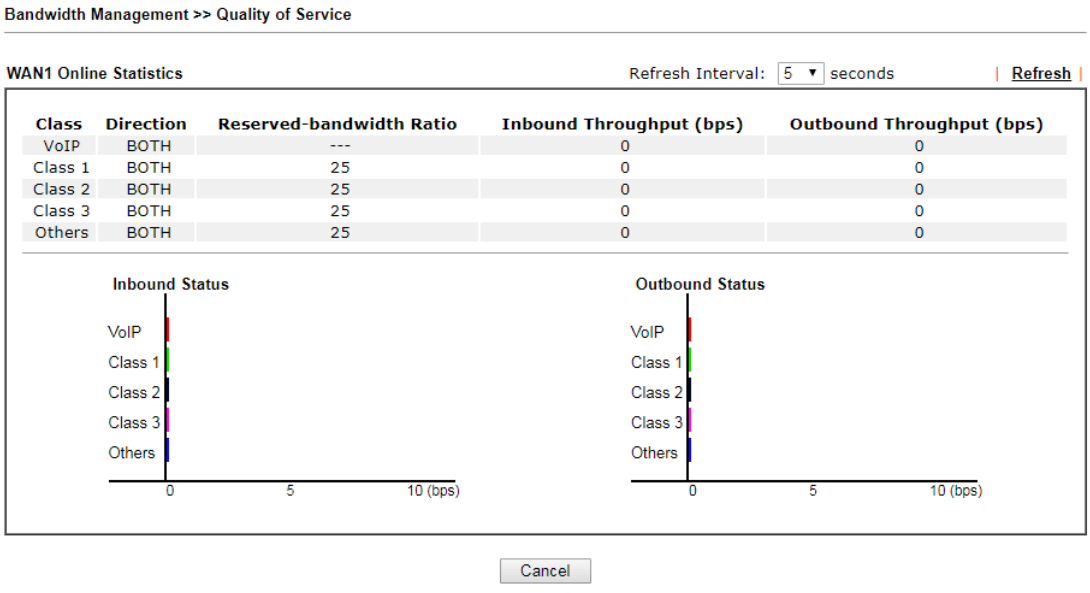
Item	Description
General Setup	**Index** – Link of WAN interface. **Enable** – Check the box to enable the QoS function for WAN interface. If it is enabled, you can configure general QoS setting for each WAN interface. ● **Direction** –Direction of traffic to which QoS is to be applied (Inbound, Outbound, 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. This option is not available on ADSL/VDSL WAN1 interface. ● **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.

Item	Description
	Index – Displays the class number that you can edit. **Enable** - Displays the status of this class rule. **QoS Class** - Displays the QoS class level. **Local Address** - Displays the local IP address for the rule. **Remote Address** - Displays the remote IP address for the rule. **DSCP** - Displays the levels of the data for processing with QoS control. **Service Type** – Displays detailed settings for the service type. **Add** - Click it to create a class rule for QoS.
VoIP Prioritization	**Enable the First Priority for VoIP SIP/RTP** - Select to allow VoIP traffic to receive the highest priority. **SIP UDP Port –** Port number to be monitored for SIP traffic.
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**.

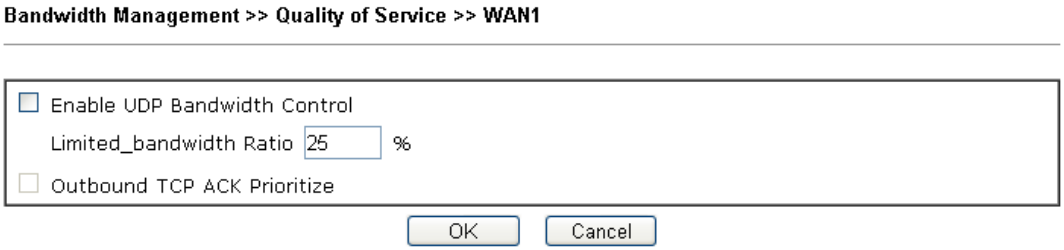
Online Statistics

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.

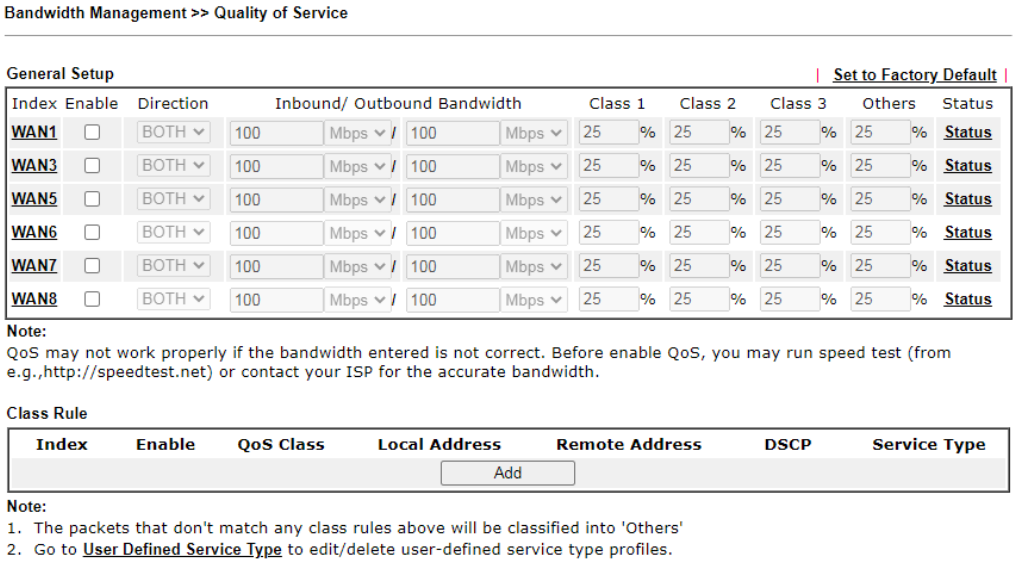
Info

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.

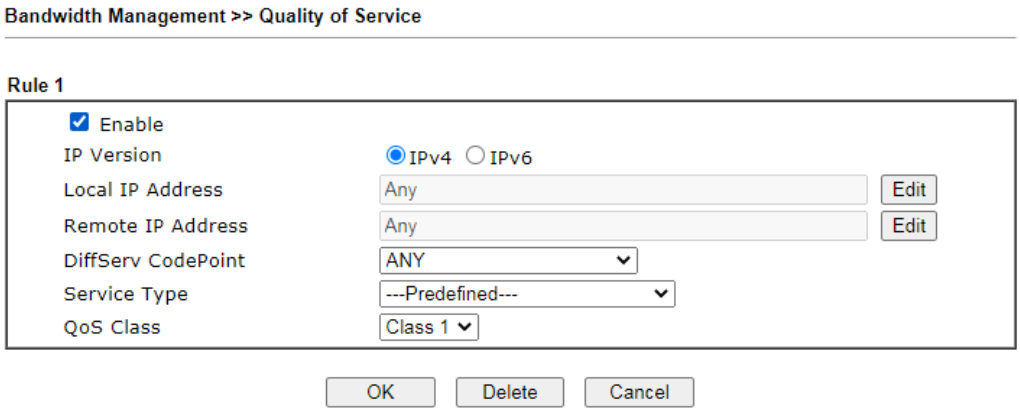
Add / edit the Class Rule for QoS

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.

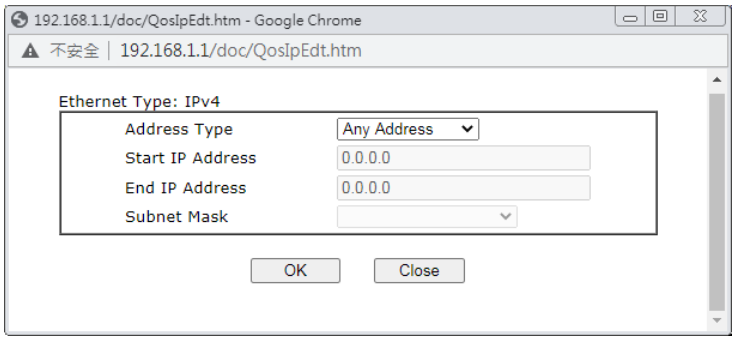


2. For adding a new rule, click **Add** to open the following page.

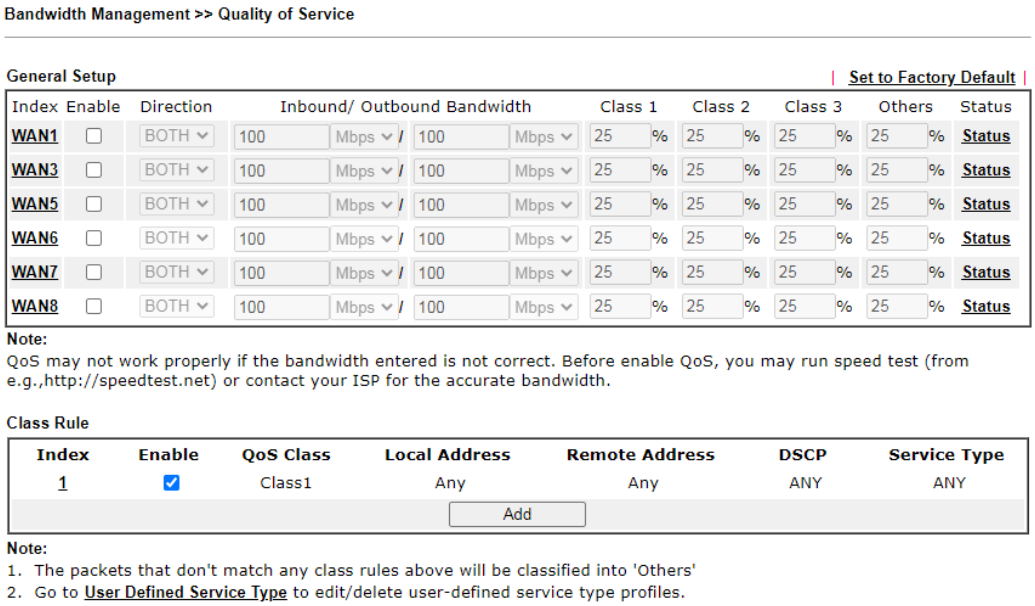


Available settings are explained as follows:

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.



Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

Index	Enable	Direction	Inbound/ Outbound Bandwidth	Class 1	Class 2	Class 3	Others	Status
WAN1	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status
WAN3	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status
WAN5	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status
WAN6	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status
WAN7	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status
WAN8	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status

Note:
QoS may not work properly if the bandwidth entered is not correct. Before enable QoS, you may run speed test (from e.g.,http://speedtest.net) or contact your ISP for the accurate bandwidth.

Class Rule

Index	Enable	QoS Class	Local Address	Remote Address	DSCP	Service Type
1	☑	Class1	Any	Any	ANY	ANY

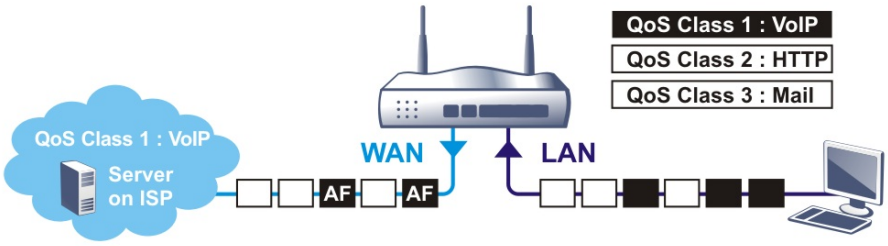
Add

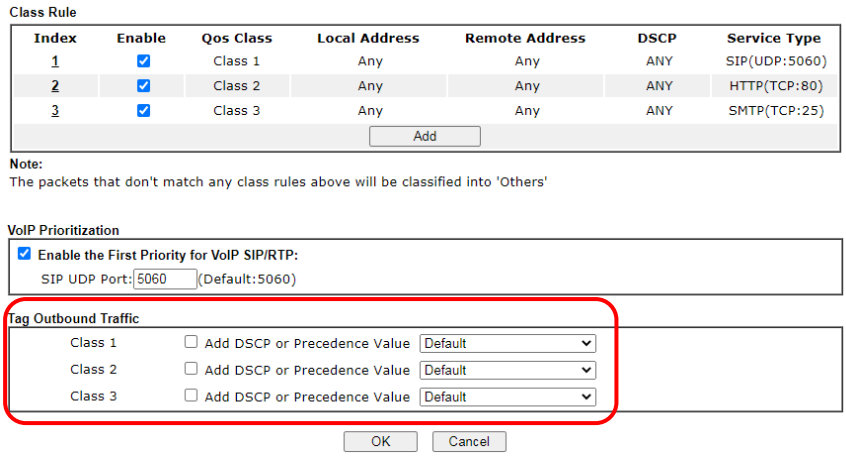
Note:
1. The packets that don't match any class rules above will be classified into 'Others'
2. Go to User Defined Service Type to edit/delete user-defined service type profiles.

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.

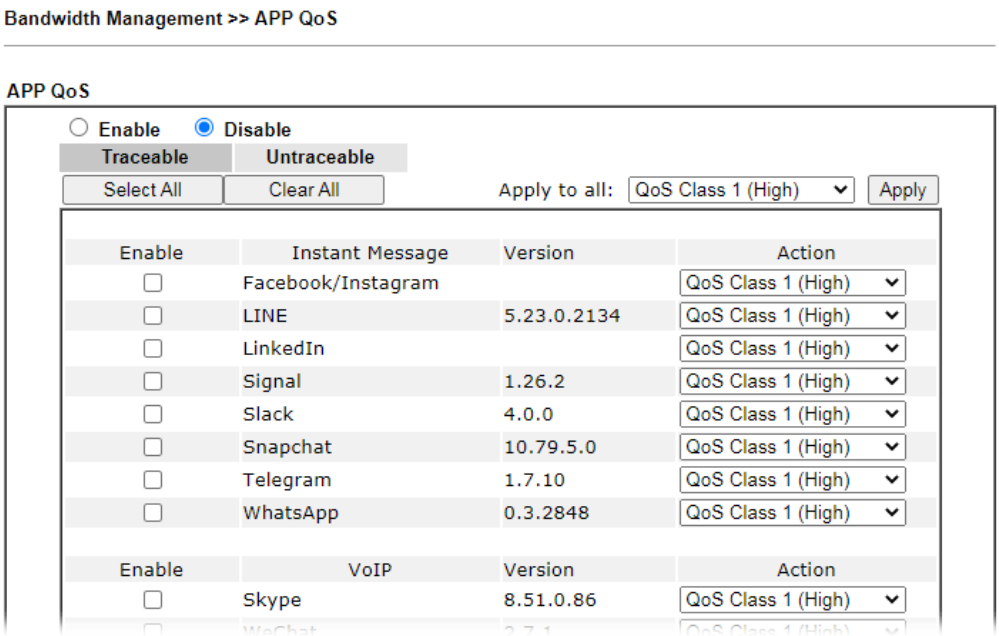
In the following illustration, outbound VoIP packets from the LAN arrive at the Vigor router with the QoS value unset. The router sets the DSCP value to AF before forwarding them to the ISP server via the WAN interface.





V-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.



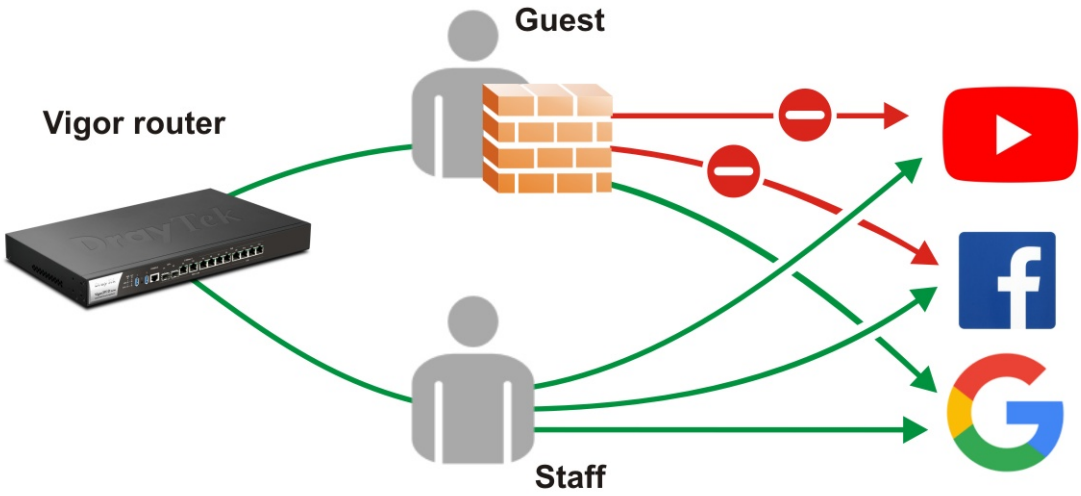
Available settings are explained as follows:

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.

V-3 User Management

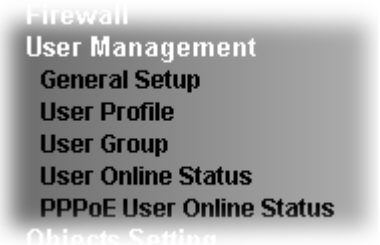
User Management is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password. Instead of managing with IP address/MAC address, User Management function manages hosts with user account. Network administrator can give different firewall policies or rules for different hosts with different User Management accounts. This is more flexible and convenient for network management. Not only offering the basic checking for Internet access, User Management also provides additional firewall rules, e.g. CSM checking for protecting hosts.



Info

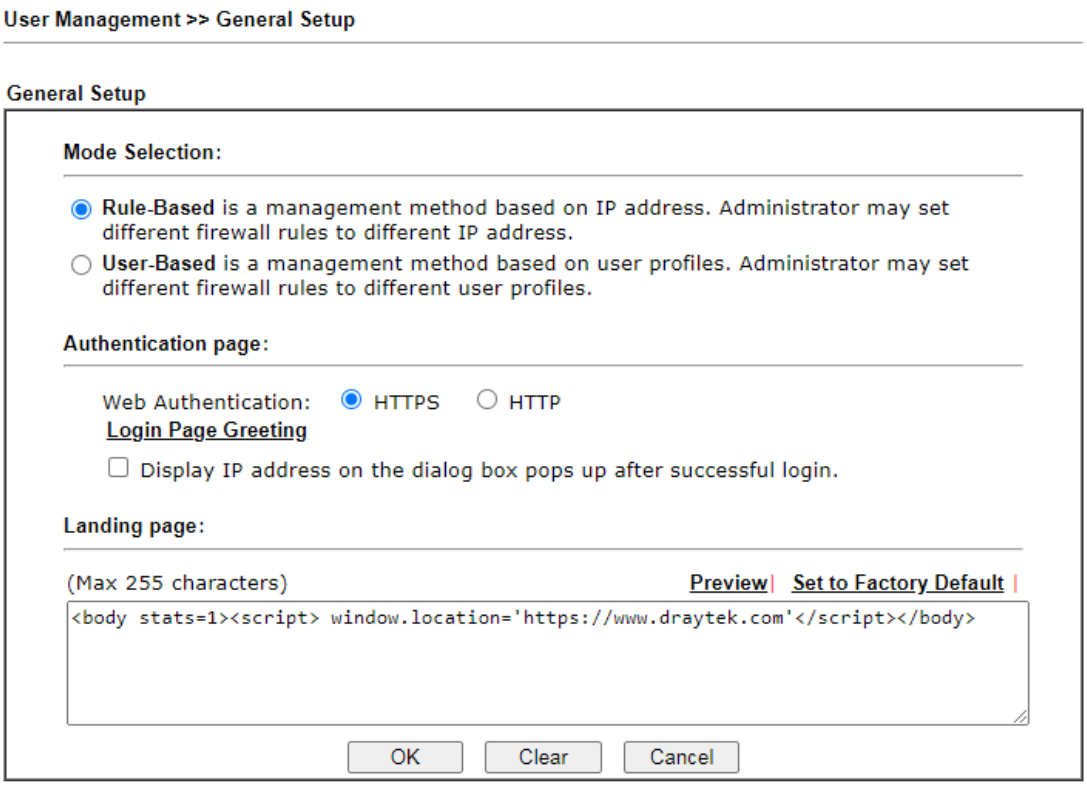
Filter rules configured under Firewall usually are applied to the host (the one that the router installed) only. With user management, the rules can be applied to every user connected to the router with customized profiles.

Web User Interface



V-3-1 General Setup

General Setup can determine the standard (rule-based or user-based) for the users controlled by User Management. The mode (standard) selected here will influence the contents of the filter rule(s) applied to every user.



Available settings are explained as follows:

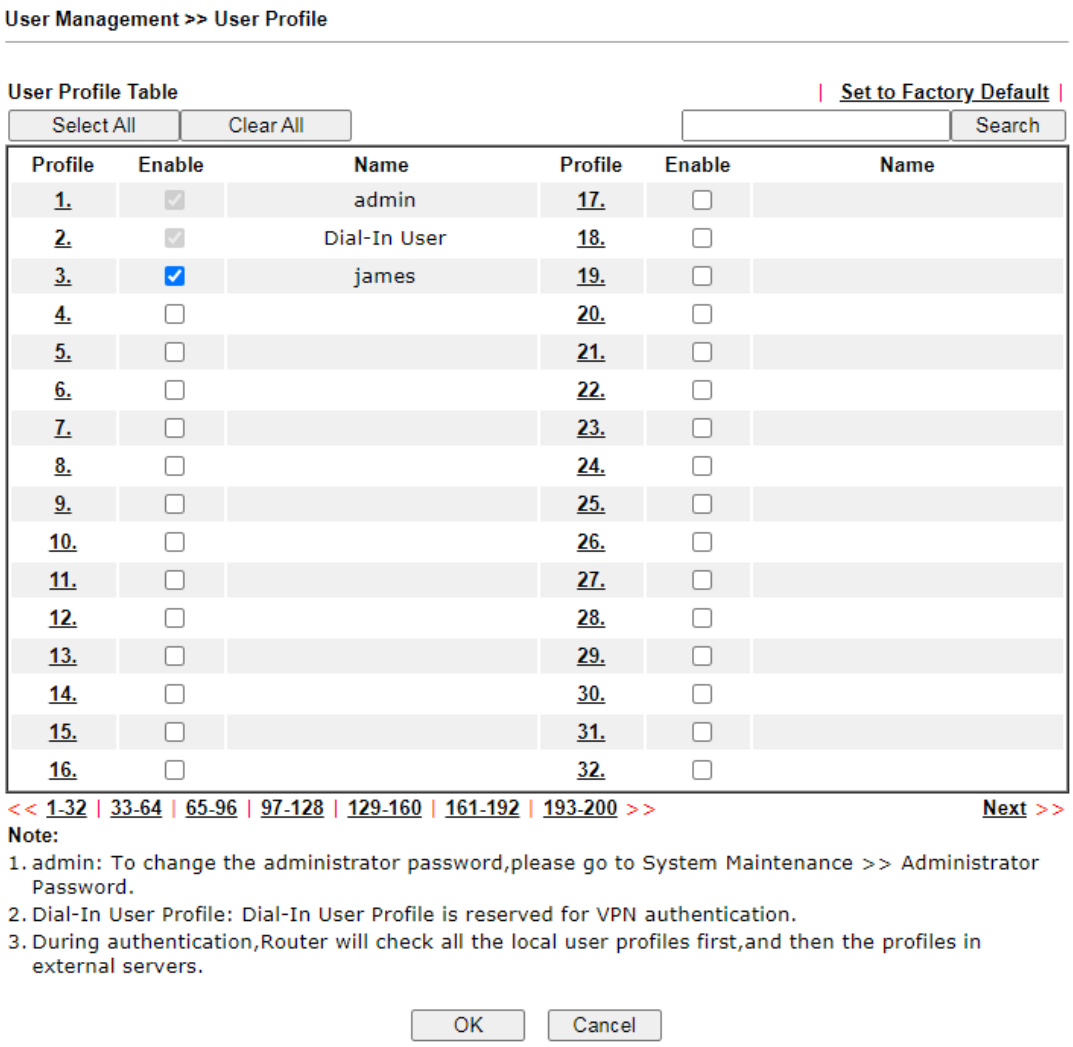
Item	Description
Mode Selection	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved. **User-Based** - If you choose such mode, the router will apply the filter rules configured in **User Management>>User Profile** to the users. **Rule-Based** –If you choose such mode, the router will apply the filter rules configured in **Firewall>>General Setup** and

	Filter Rule to the users.
Authentication page	**Web Authentication** - Choose the protocol for web authentication. **Login Page Greeting** - Such link allows you to access into the setting page for login greeting. For detailed information, refer to **System Maintenance>>Login Page Greeting**. **Display IP Address on ...** – Check the box to display the IP address of the client on the tracking window.
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

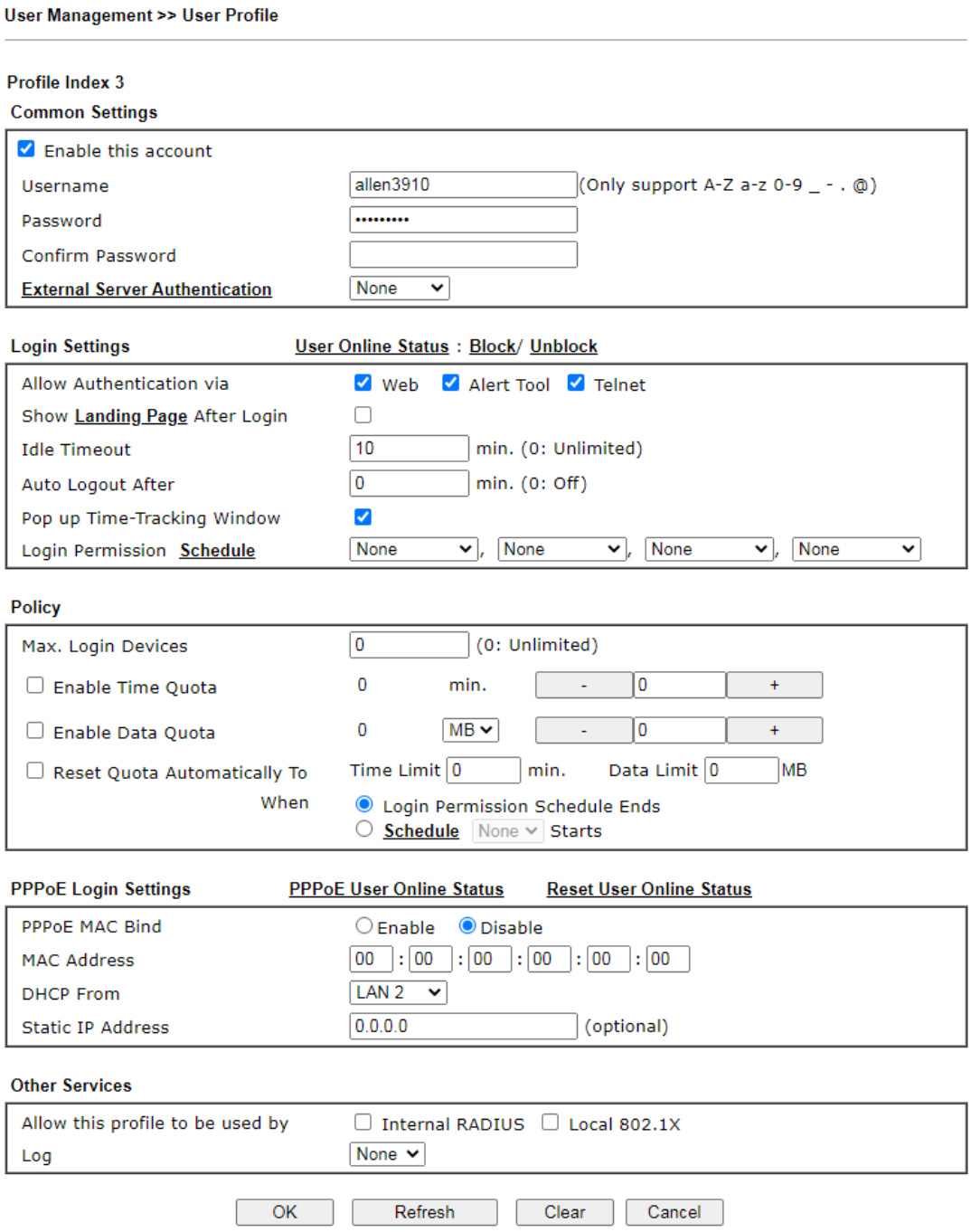
After finishing all the settings here, please click **OK** to save the configuration.

V-3-2 User Profile

This page allows you to set customized profiles (up to 200) which will be applied for users controlled under **User Management**. Simply open **User Management>>User Profile**.



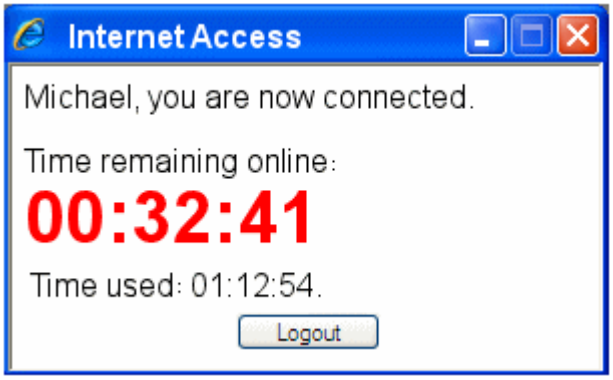
To set the user profile, please click any index number link to open the following page. Notice that profile 1 (**admin**) and profile 2 **(Dial-In User)** are factory default settings. Profile 2 is reserved for future use.



Available settings are explained as follows:

Item	Description
Common Settings	**Enable this account** - Check this box to enable such user profile. **Username** - Type a name for such user profile (e.g., *LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B,* etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the User Name specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile. The maximum length of the name you can set is 24

	characters. **Password** - Type a password for such profile (e.g., *lug123, wug123,wug456,* etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile. The maximum length of the password you can set is 24 characters. **Confirm Password** - Type the password again for confirmation. **External Service Authentication -** The router will authenticate the dial-in user by itself or by external service such as LDAP server or RADIUS server or TACACS+ server. If LDAP, Radius or TACACS+ is selected here, it is not necessary to configure the password setting above.
Login Settings	**Allow Authentication via**- Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication. • **Web** – If it is selected, the user can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a **Welcome Message** (configured in **User Management >> General Setup)** will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router. • **Alert Tool** – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site. • **Telnet** – If it is selected, the user can use Telnet command to perform the authentication job. **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 the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 10 minutes. **Auto Logout After** – Such account will be forced to logout after a certain time set here. **Pop up Time-Tracking Window** - If such function is enabled, a pop up window will be displayed on the screen with time remaining for connection if Idle Timeout is set. 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 type in four sets of time schedule for your request. All the schedules can be set

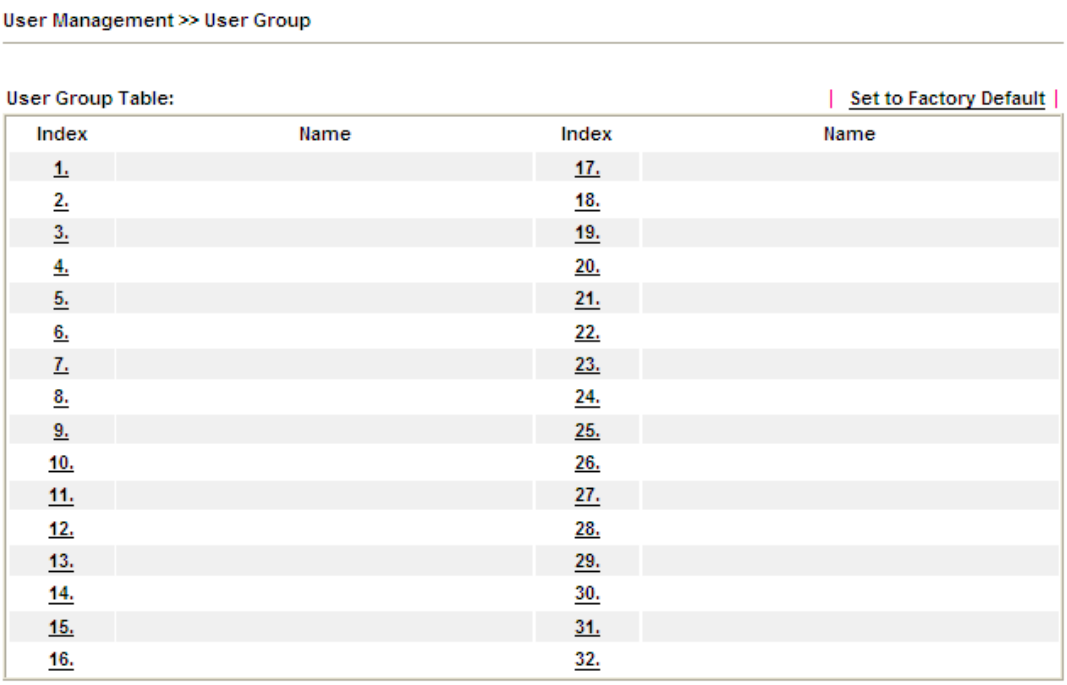
	previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.
Policy	**Max Login Devices** - Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users. **Enable Time Quota** - Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet. [+] – Click this box to set and increase the time quota for such profile. [-] – Click this box to decrease the time quota for such profile. **Note:** A dialog will be popped up to notify how many time remained when a user accesses into Internet through Vigor router successfully. When the time is up, all the connection jobs including network, IM, social media, facebook, and etc. will be terminated.  **Enable Data Quota** - Data Quota means the total amount for data transmission allowed for the user. The unit is MB/GB. [+] – Click this box to set and increase the data quota for such profile. [-] – Click this box to decrease the data quota for such profile. **Reset Quota Automaticlly To -** Set default time quota and data quota for such profile. When the scheduling time is up, the router will use the default quota settings automatically. Check it to use the default setting for time quota and data quota. ● **Time Limit** – Type the value for the time manually. ● **Data Limit** – Type the value for the data manually. **Login Permission Schedule Ends** - When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically. **Schedule** – The router will reset the quota with user-defined time/data values at the starting time configured in the

	selected schedule profile.
PPPoE Login Setting	Such user account will be used (1) by the client with the IP address specified or (2) by the client with the MAC address bound with the IP address, for accessing into Vigor3910 web user interface. **PPPoE MAC Bind –** Specify a MAC address which is limited and used for such PPPoE account. ● **Enable/Disable** - Click it to enable/disable the function of PPPoE MAC Bind. **MAC Address** – Type the MAC address to be bound with the IP address set below if **PPPoE MAC Bind** is enabled. **DHCP From** – Use the drop down list to specify LAN/DMZ interface. The IP address for binding with the MAC address (above) set in the selected interface will be assigned from the IP address set in the selected interface. **Static IP Address** (optional)– Type an IP address.
Other Services	**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. **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.

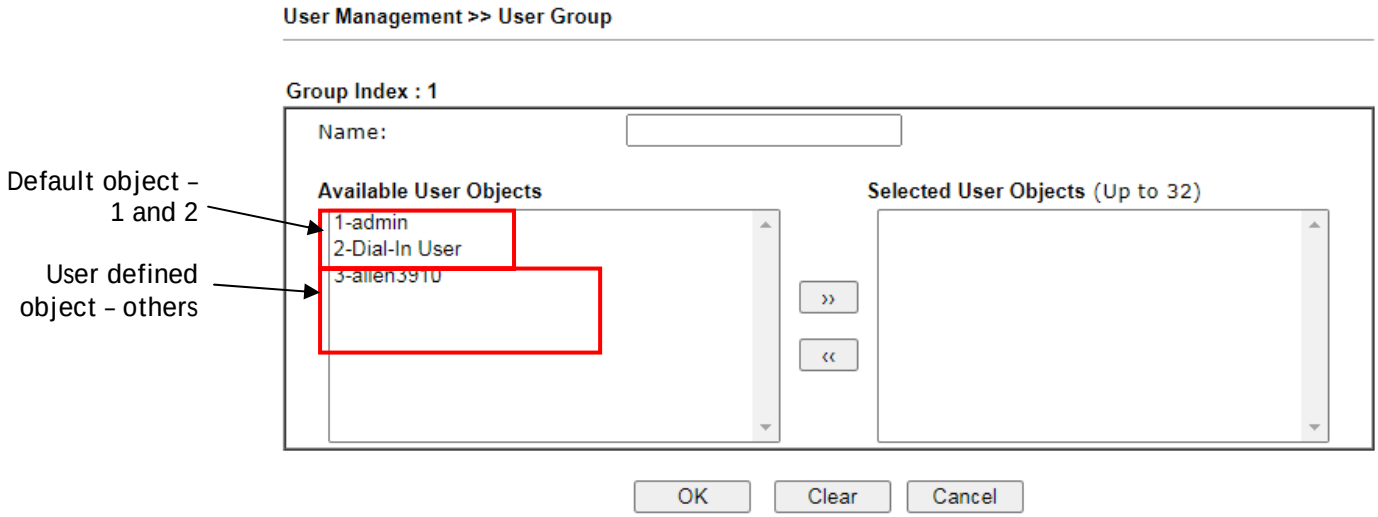
After finishing all the settings here, please click **OK** to save the configuration.

V-3-3 User Group

This page allows you to bind several user profiles into one group. These groups will be used in **Firewall>>General Setup** as part of filter rules.



Please click any index number link to open the following page.



Available settings are explained as follows:

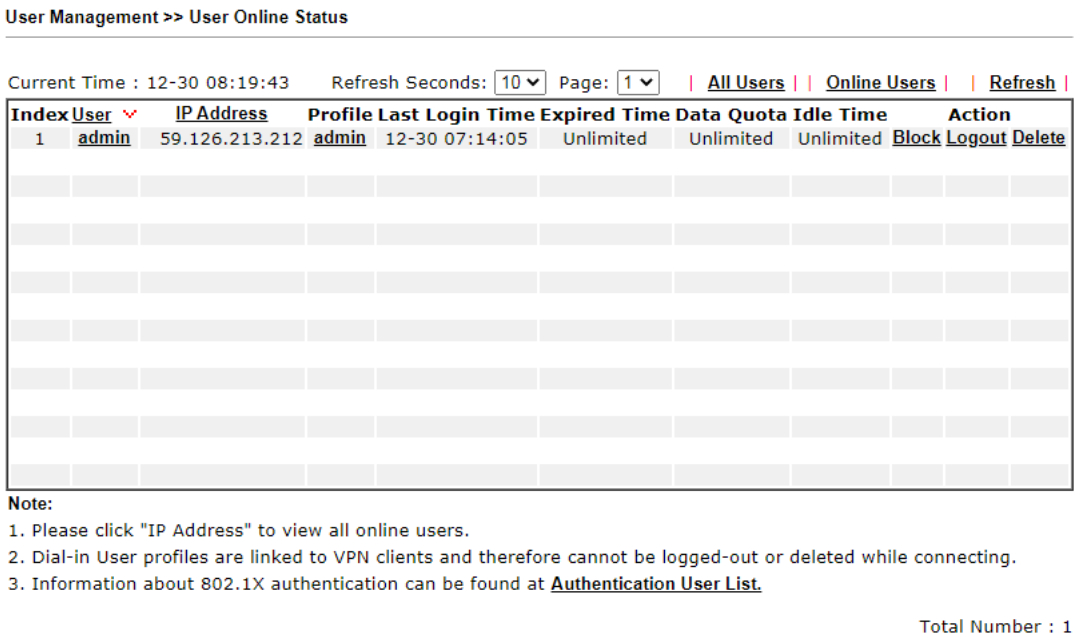
Item	Description
Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from **User Profile** page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined profiles will be numbered with 3, 4, 5 and so on.

Selected Keyword Objects	Click » button to add the selected user objects in this box.

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

V-3-4 User Online Status

This page displays the user(s) connected to the router and refreshes the connection status in an interval of several seconds.



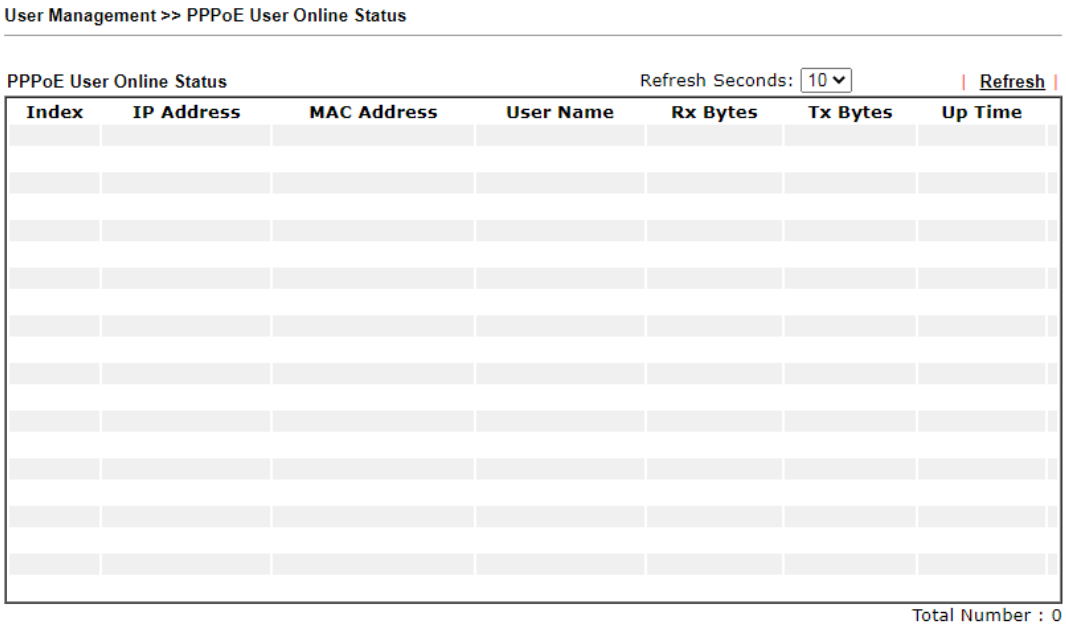
Available settings are explained as follows:

Item	Description
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
User	Display the users which connect to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.
IP Address	Display the IP address of the device.
Profile	Display the authority of the account.
Last Login Time	Display the login time that such user connects to the router last time.
Expired Time	Display the expired time of the network connection for the user.
Data Quota	Display the quota for data transmission.
Idle Time	Display the idle timeout setting for such profile.

Action	**Block** - can avoid specified user accessing into Internet. **Unblock** – allow the user to access into Internet. **Logout** – the user will be logged out forcefully.

V-3-5 PPPoE User Online Status

PPPoE User Online Status displays connection information (including IP address, MAC address,user name, transmitted bytes, received bytes, up time and so on) for the LAN client who accesses Internet via the built-in PPPoE server of Vigor router.



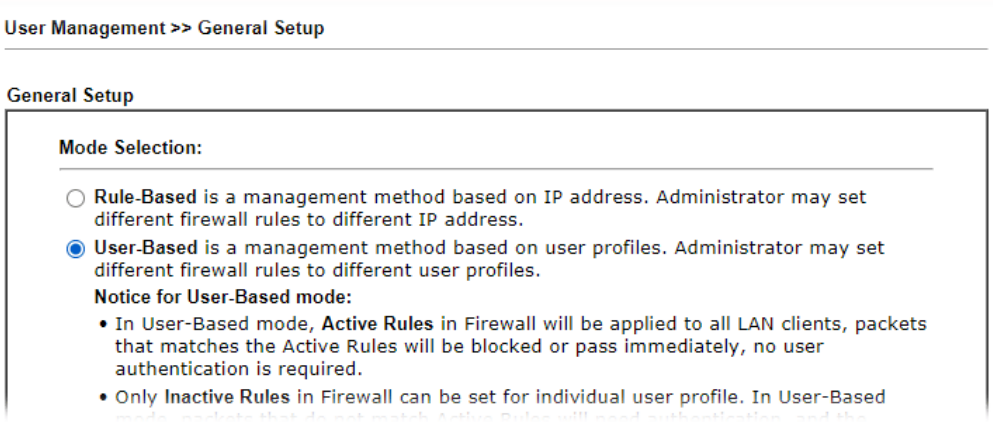
Available settings are explained as follows:

Item	Description
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.
Refresh	Click this link to refresh this page manually.
IP Address	Displays the IP address of the client in LAN.
MAC Address	Displays the MAC address of the client in LAN.
User Name	Displays the name of user connecting to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.
Rx Bytes	Displays the speed of octets received through such PPPoE user.
Tx Bytes	Displays the speed of octets transmitted through such PPPoE user.
Up Time	Displays the connection time of such PPPoE user.

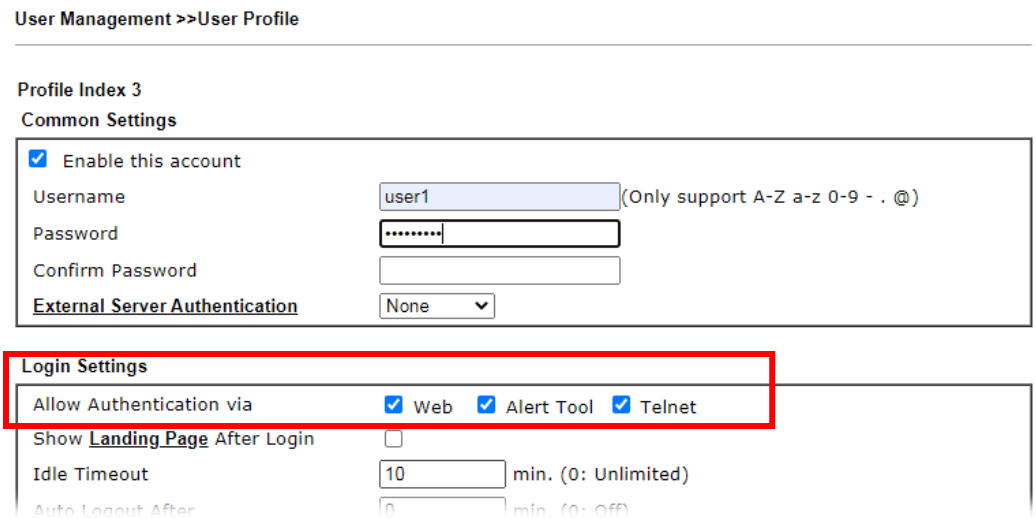
Application Notes

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.

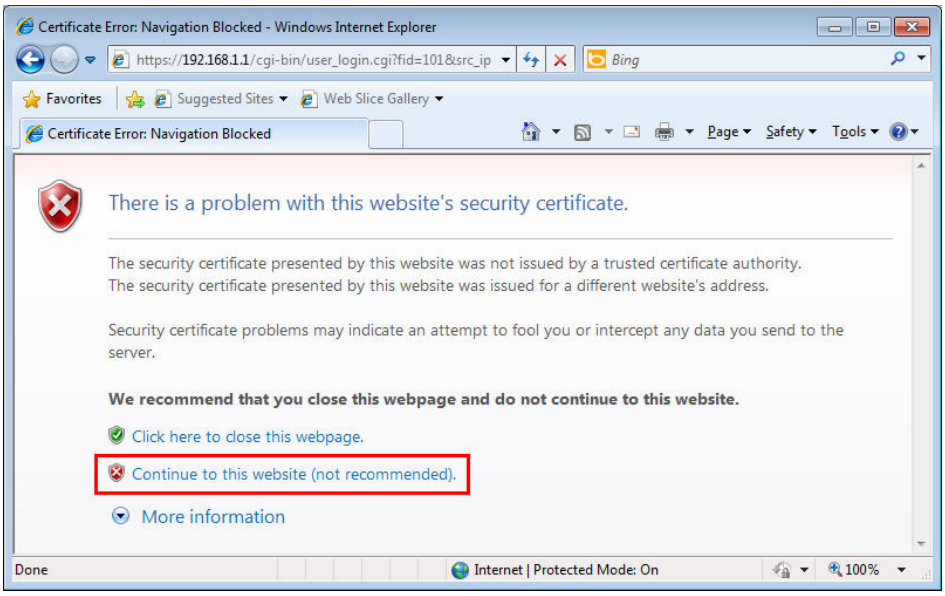


With **User Management** authentication function, before a valid username and password have been correctly supplied, a particular client will not be allowed to access Internet through the router. There are three ways for authentication: **Web**, **Alert Tool and Telnet**.

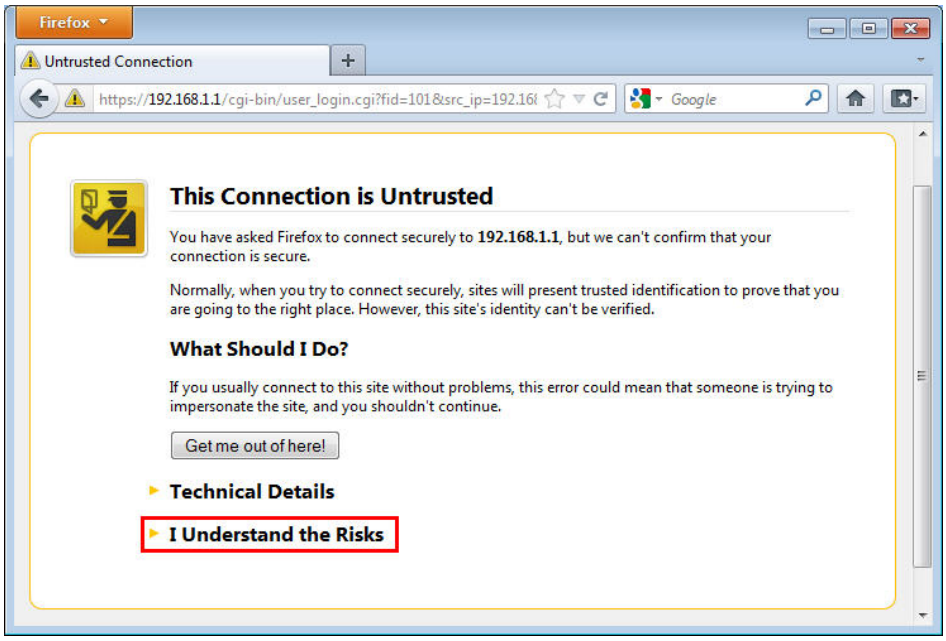


Authentication via Web

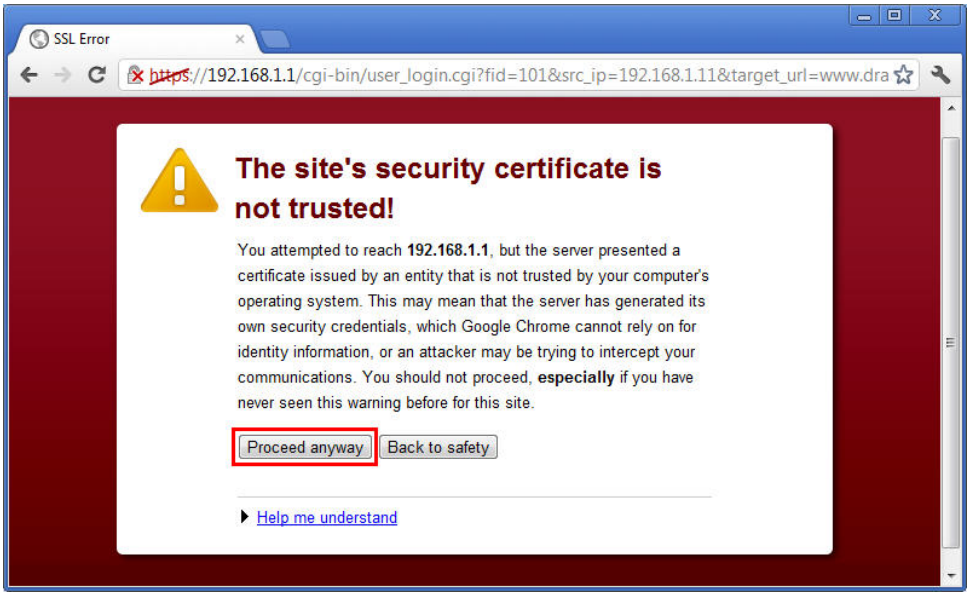
- If a LAN client who hasn't passed the authentication opens an external web site in his browser, he will be redirected to the router's Web authentication interface first. Then, the client is trying to access http://www.draytek.com and but brought to the Vigor router. Since this is an SSL connection, 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)**.



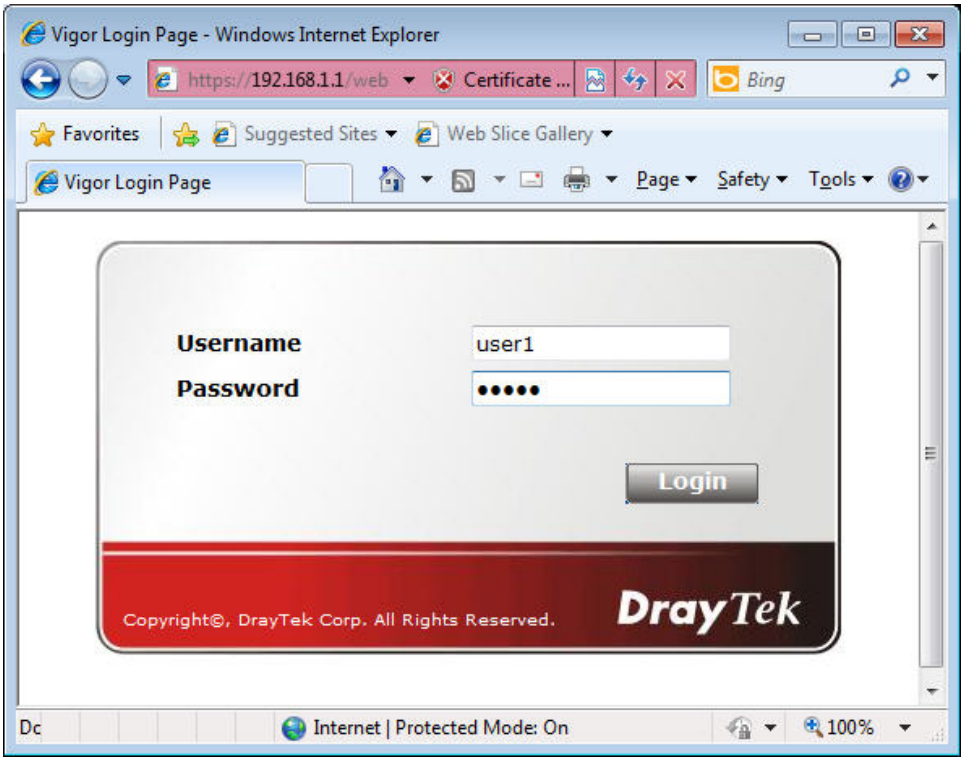
- With Mozilla Firefox, you may get the following warning message. Select **I Understand the Risks**.



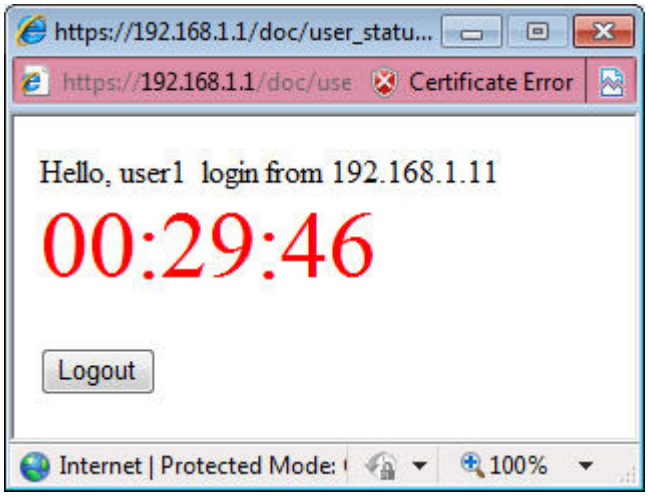
- With Chrome browser, you may get the following warning. Click **Proceed anyway**.



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**.

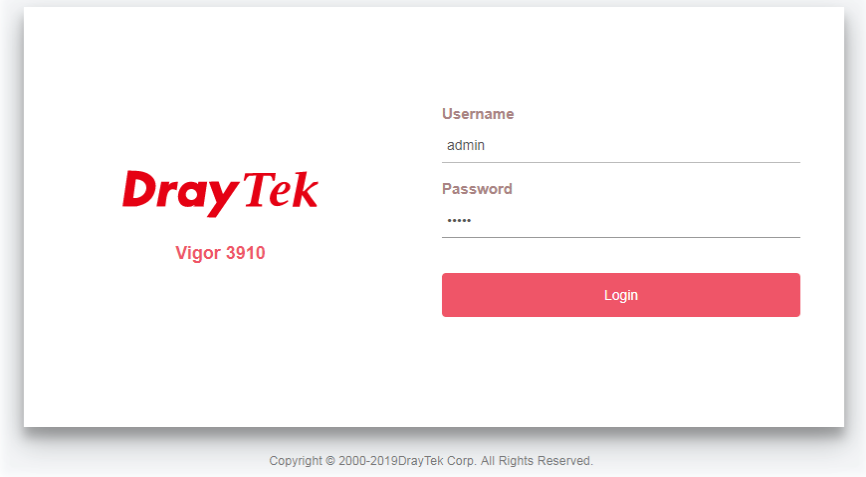


If the authentication is successful, the client will be redirected to the original web site that he tried to access. In this example, it is http://www.draytek.com . Furthermore, you will get a popped up window as the following. Then you can access the Internet.



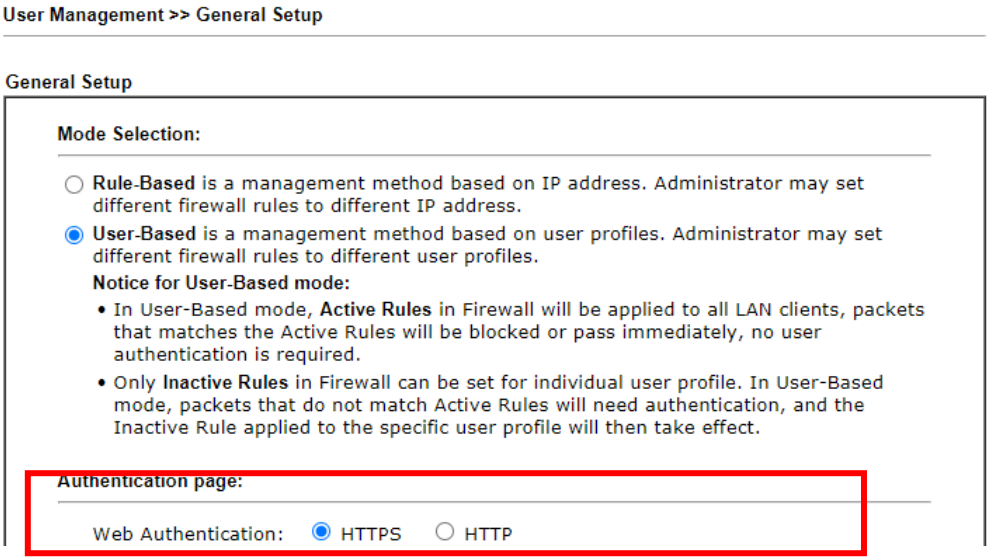
Note, if you block the web browser to pop up any window, you will not see such window.

If the authentication is failed, you will get the error message, **The username or password you entered is incorrect**. Please login again.

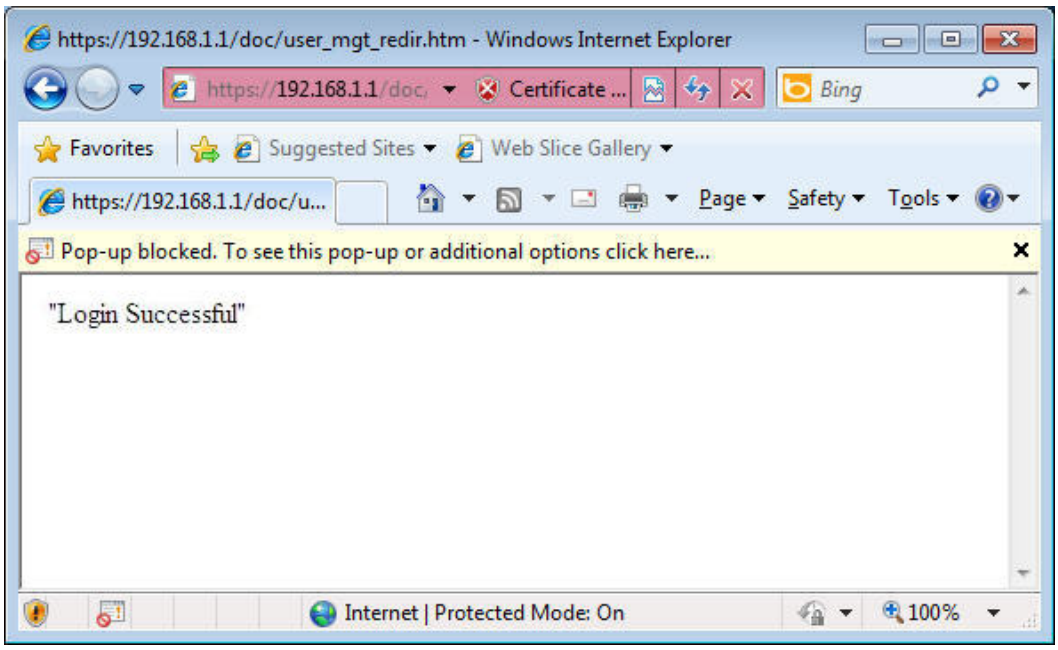


- In above description, you access an external web site to trigger the authentication. You may also directly access the router's Web UI for authentication. Both HTTP and HTTPS are supported, for example http://192.168.1.1 or https://192.168.1.1 . Replace 192.168.1.1 with your router's real IP address, 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.

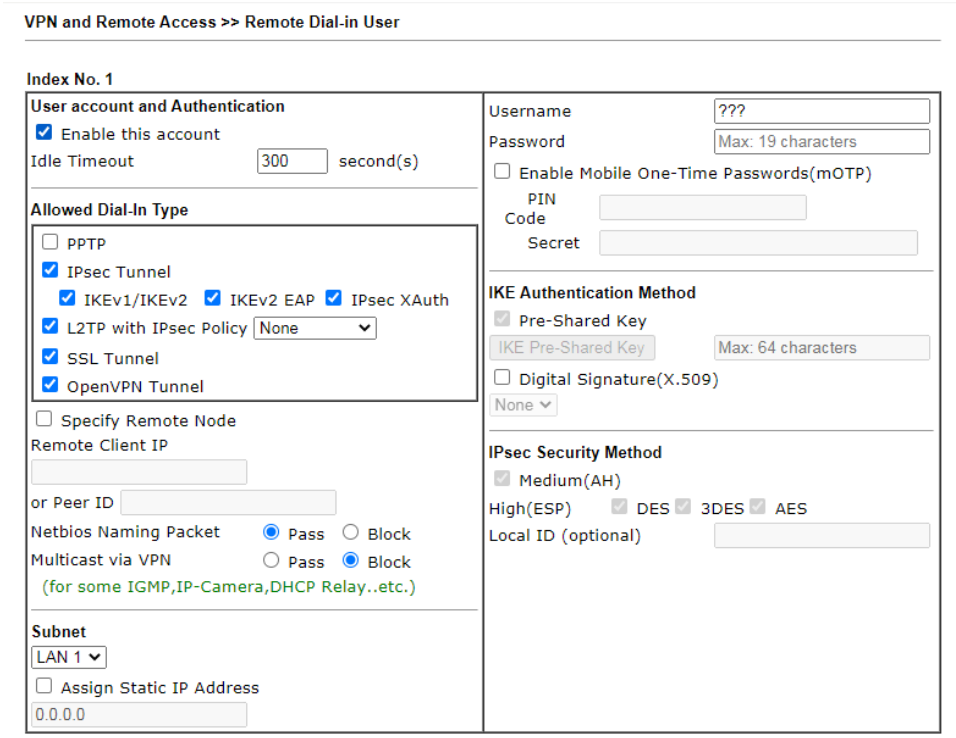


Also you will get a **Tracking Window** if you don't block the pop-up window.

- 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.

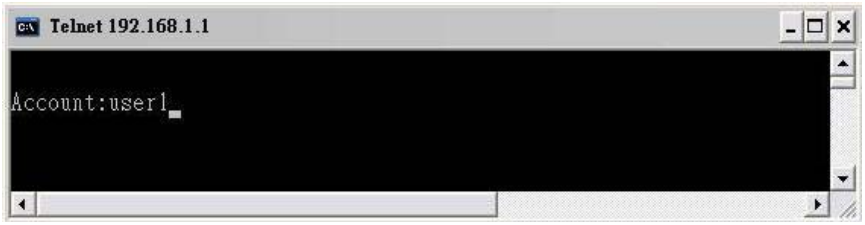


- If **SSL Tunnel** or **SSL Web Proxy** is disabled in the VPN profile, a User Management account and a remote dial-in VPN profile can use the same Username, even with different passwords. However, we recommend you to use different usernames for different user profiles in User Management and VPN profiles.

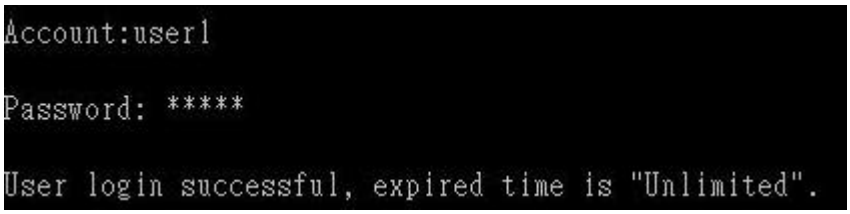
Authentication via Telnet

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:



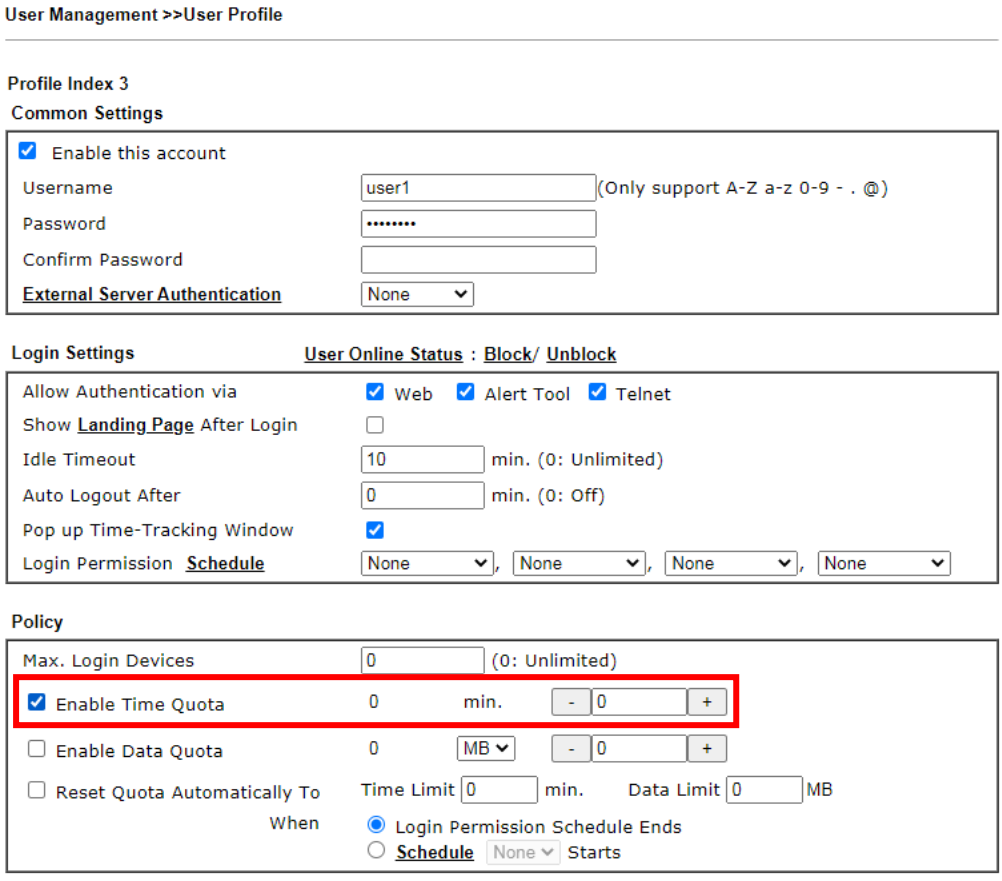
2. Type the password for authentication and press **Enter**. The message **User login successful** will be displayed with the expired time (if configured).



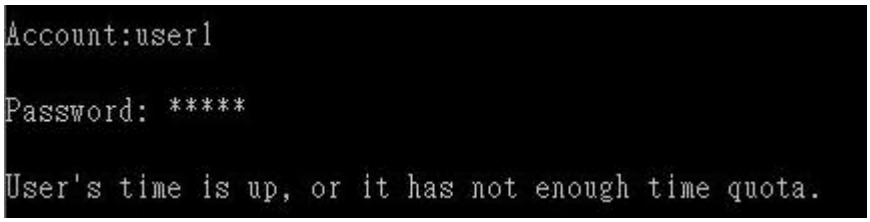
Info

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.

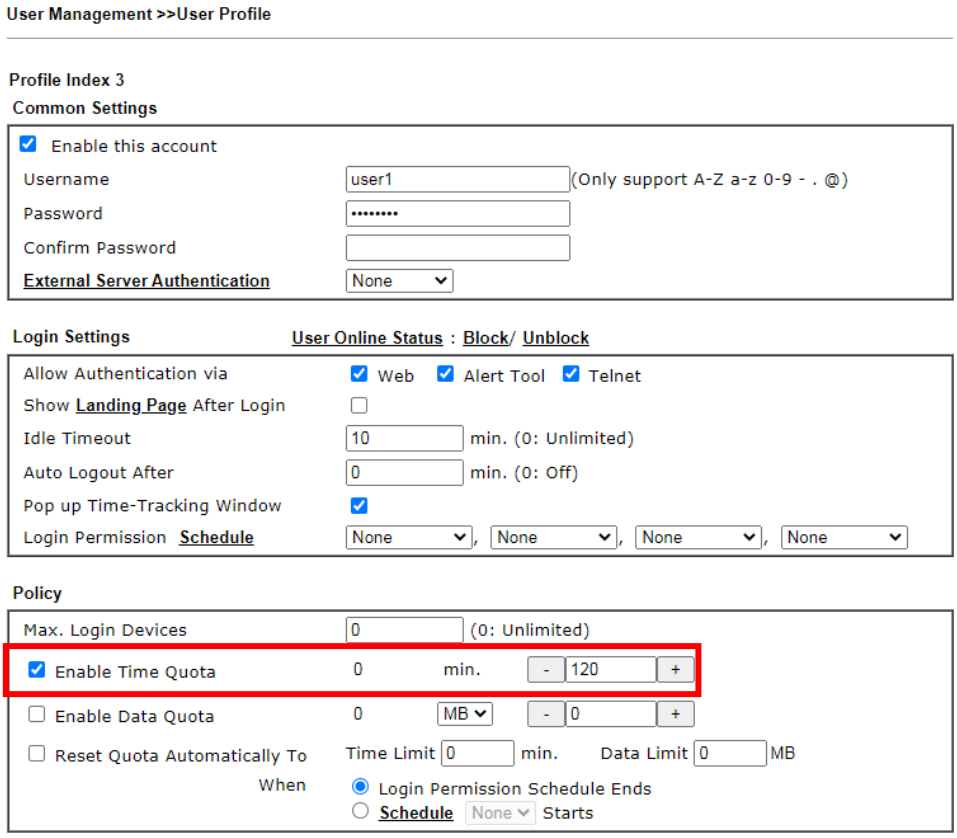
3. In the Web interface of router, the configuration page of **Time Quota** is shown as below.



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.

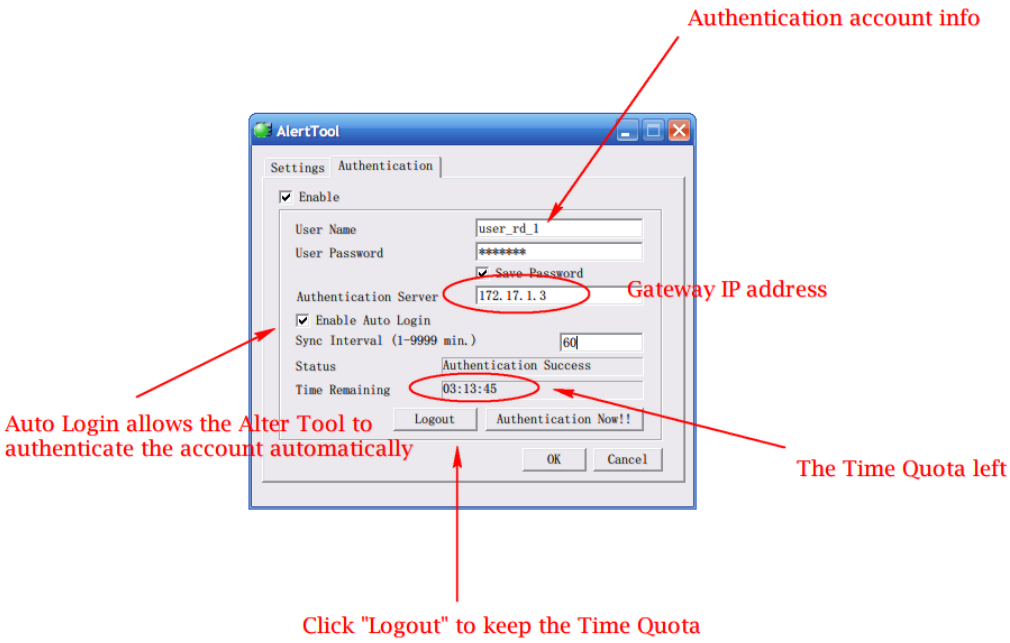
After you run out the available time, you can’t use this account any more until the administrator manually adds additional time for you.

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.

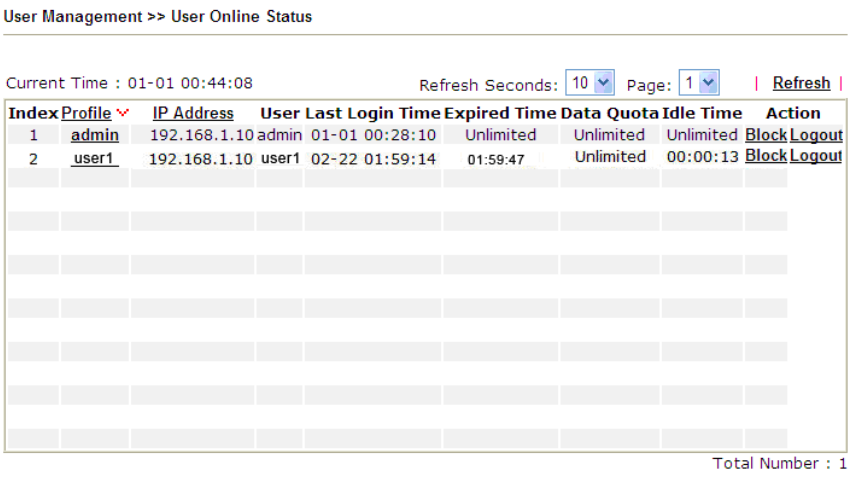
The configuration of the VigorPro Alert Notice Tool is as follows:

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.

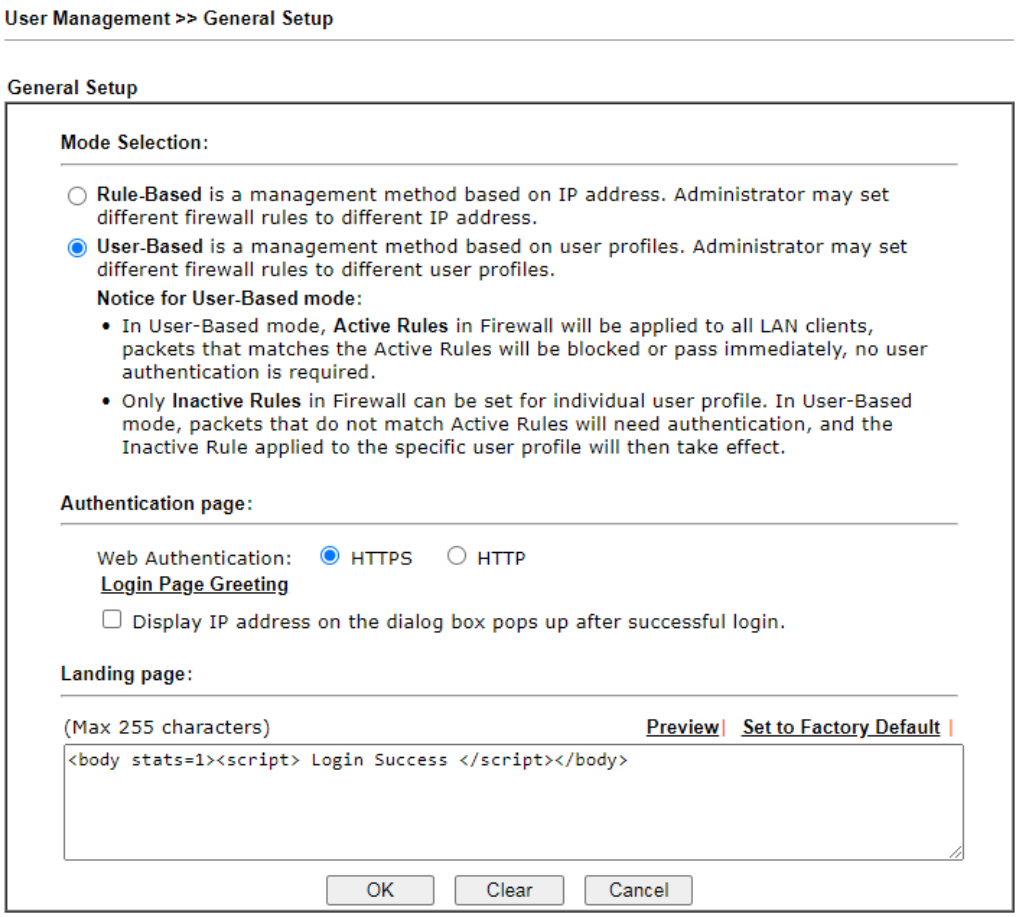


A-2 How to use Landing Page Feature

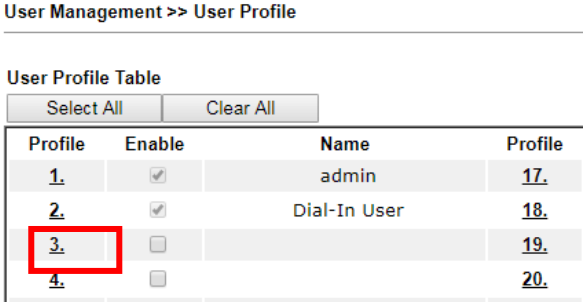
Landing Page is a special feature configured under **User Management**. It can specify the message, content to be seen or specify which website to be accessed into when users try to access into the Internet by passing the authentication. Here, we take Vigor3910 Series router as an example.

Example 1 : Users can see the message for landing page after logging into Internet successfully

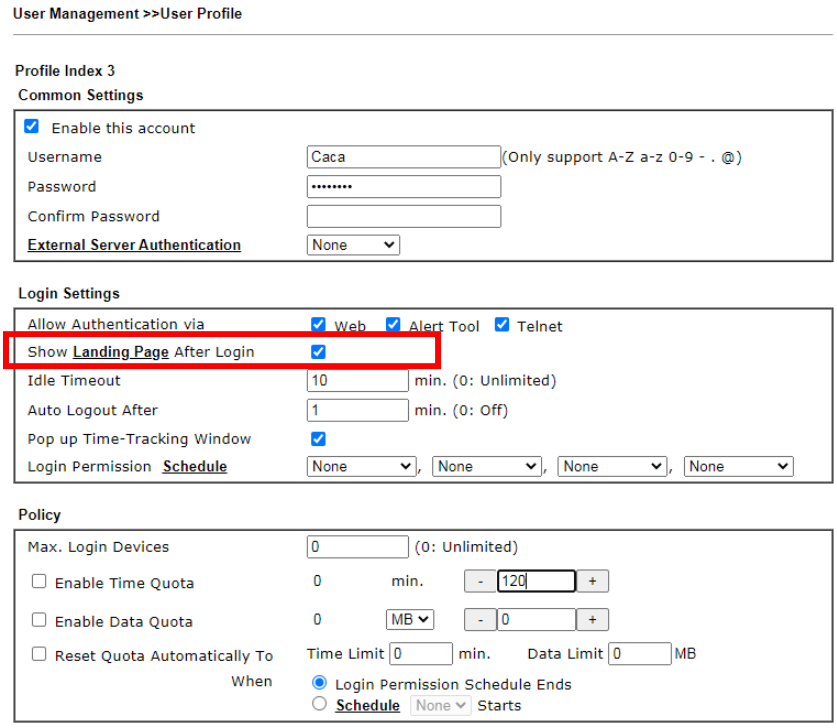
1. Open the web user interface of Vigor3910.
2. Open **User Management -> General Setup** to get the following page. In the field of **Landing Page**, please type the words of "**Login Success**". Please note that the maximum number of characters to be typed here is 255.



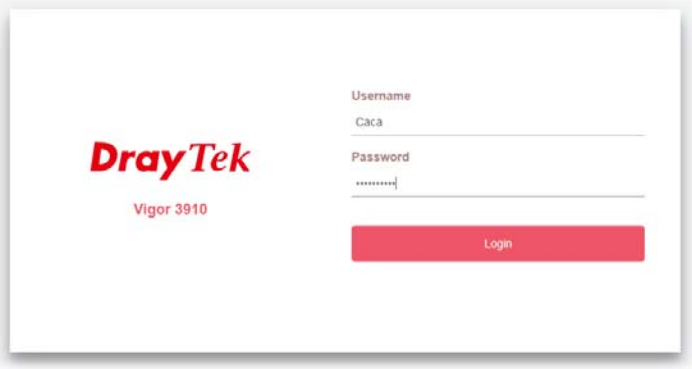
3. Now you can enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.



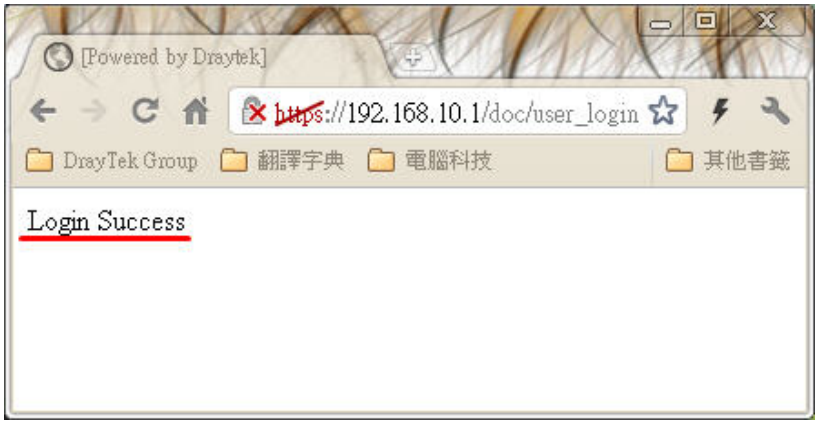
4. In the following page, check the box of **Landing page** and click **OK** to save the settings.



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.

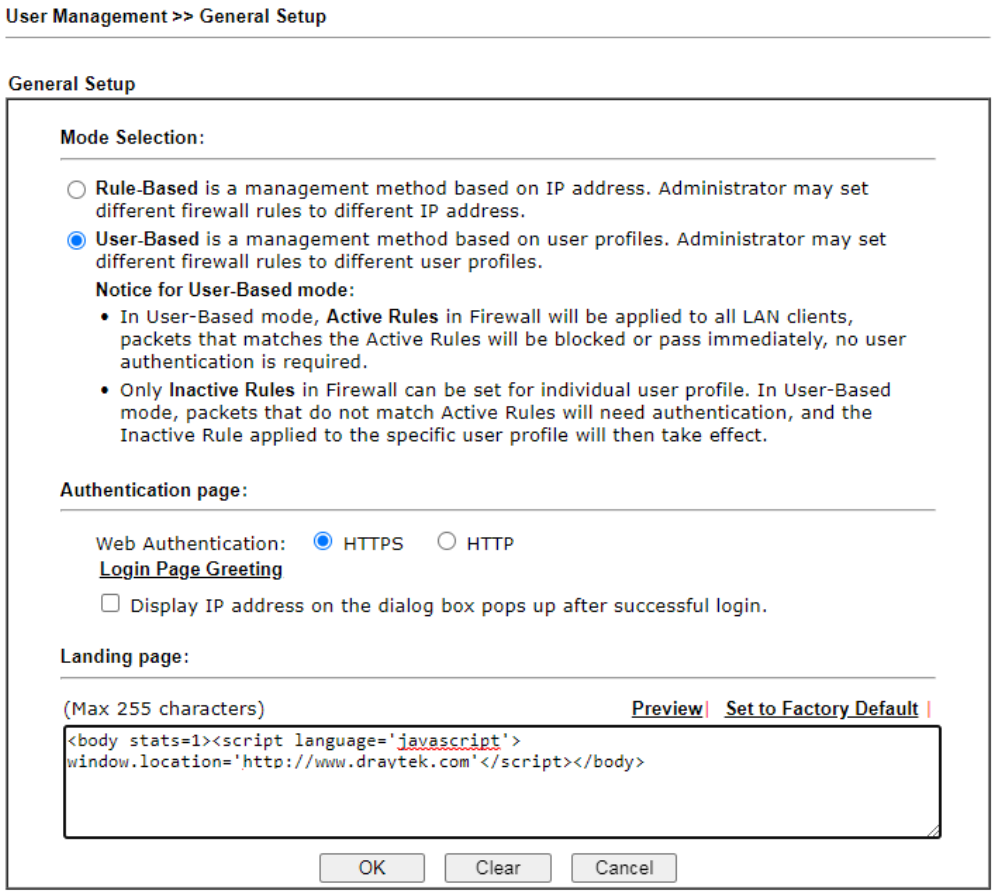


Example 2：The system will connect to http://www.draytek.com automatically after logging into Internet successfully

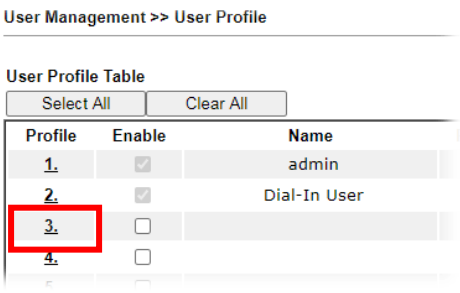
1. In the field of **Landing Page**, please type the words as below:

   “ <body stats=1><script language='javascript'>

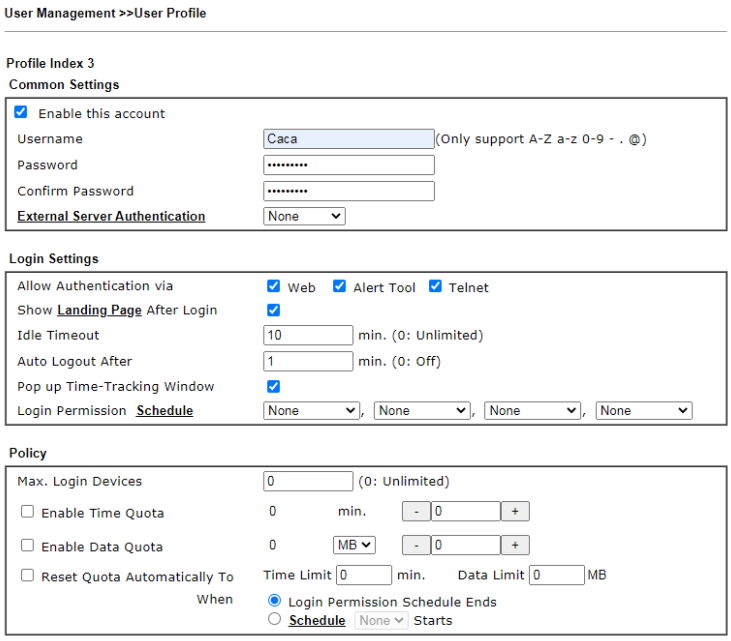
   window.location='http://www.draytek.com'</script></body>”



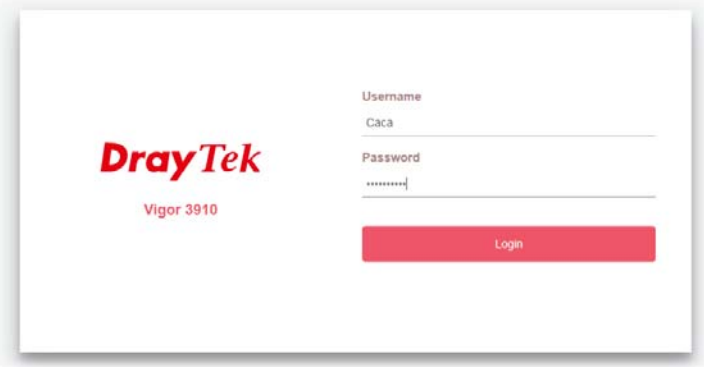
2. Next, enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.



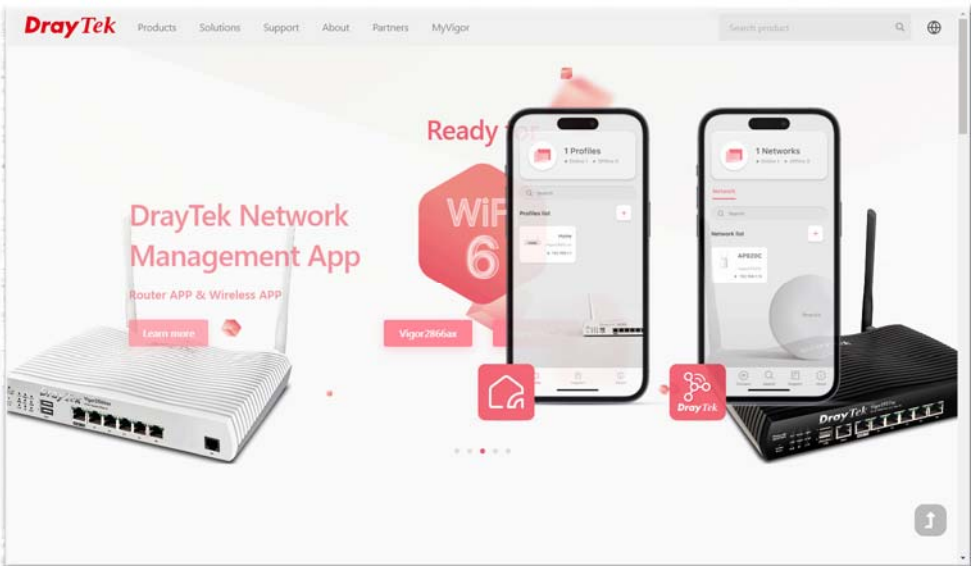
3. In the following page, check the box of **Landing page** and click **OK** to save the settings.



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.



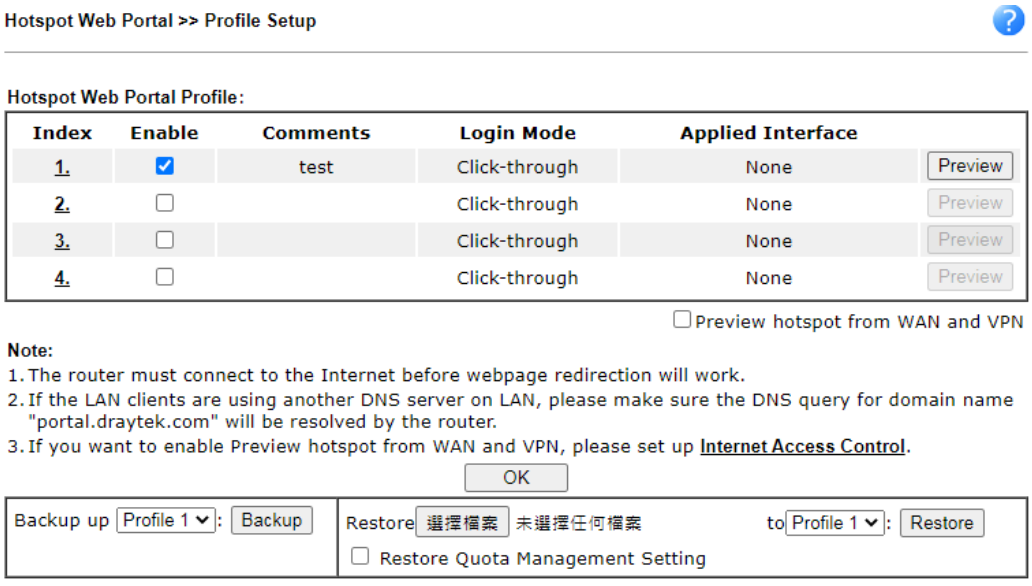
V-4 Hotspot Web Portal

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 attempt to 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

V-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.
Preview hotspot from WAN and VPN	Select this box to enable the function of previewing the hotspot page from WAN or VPN. Later, click **Preview**.
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.

V-4-1-1 Login Method

There are five 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.

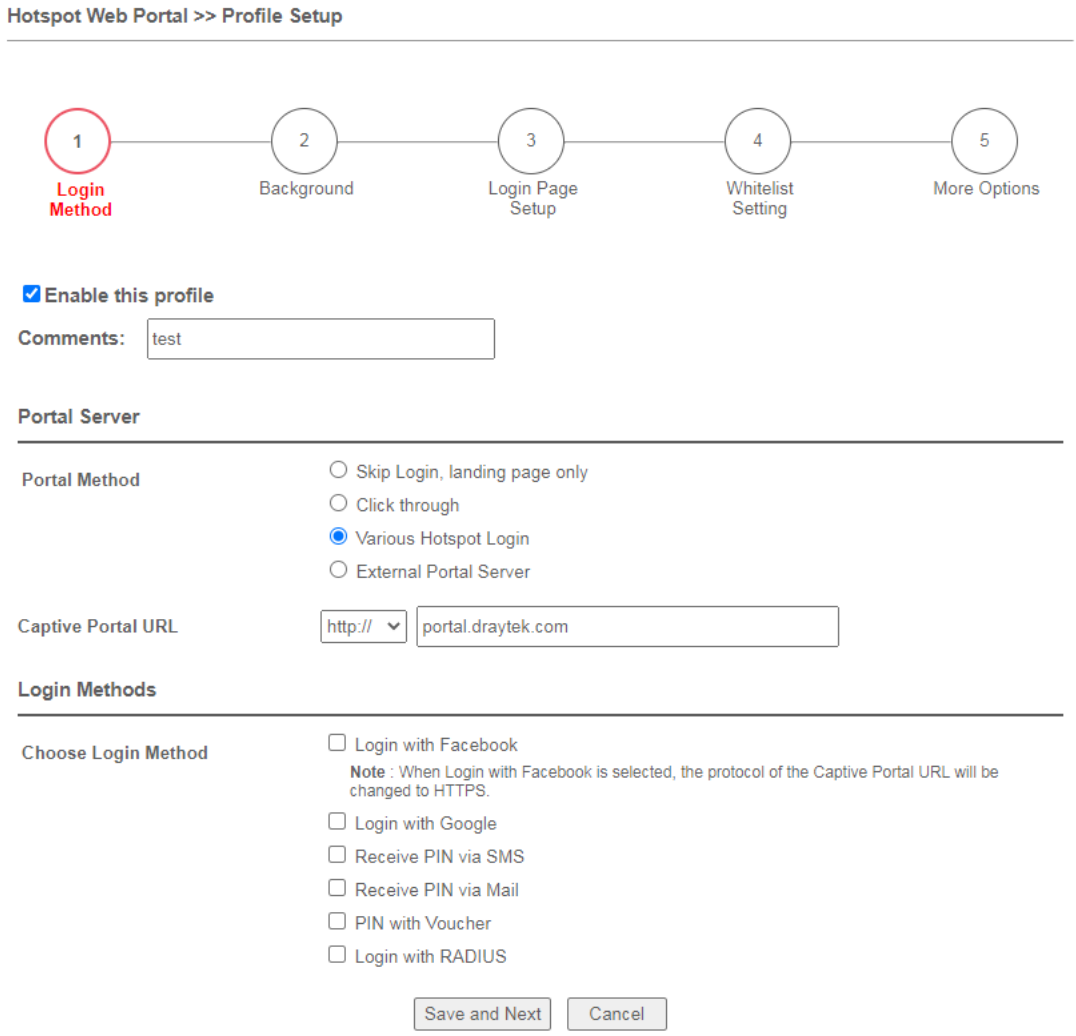
(D) External Portal Server

External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.

V-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 ● PIN with Voucher ● 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 used to send PIN notifications 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.

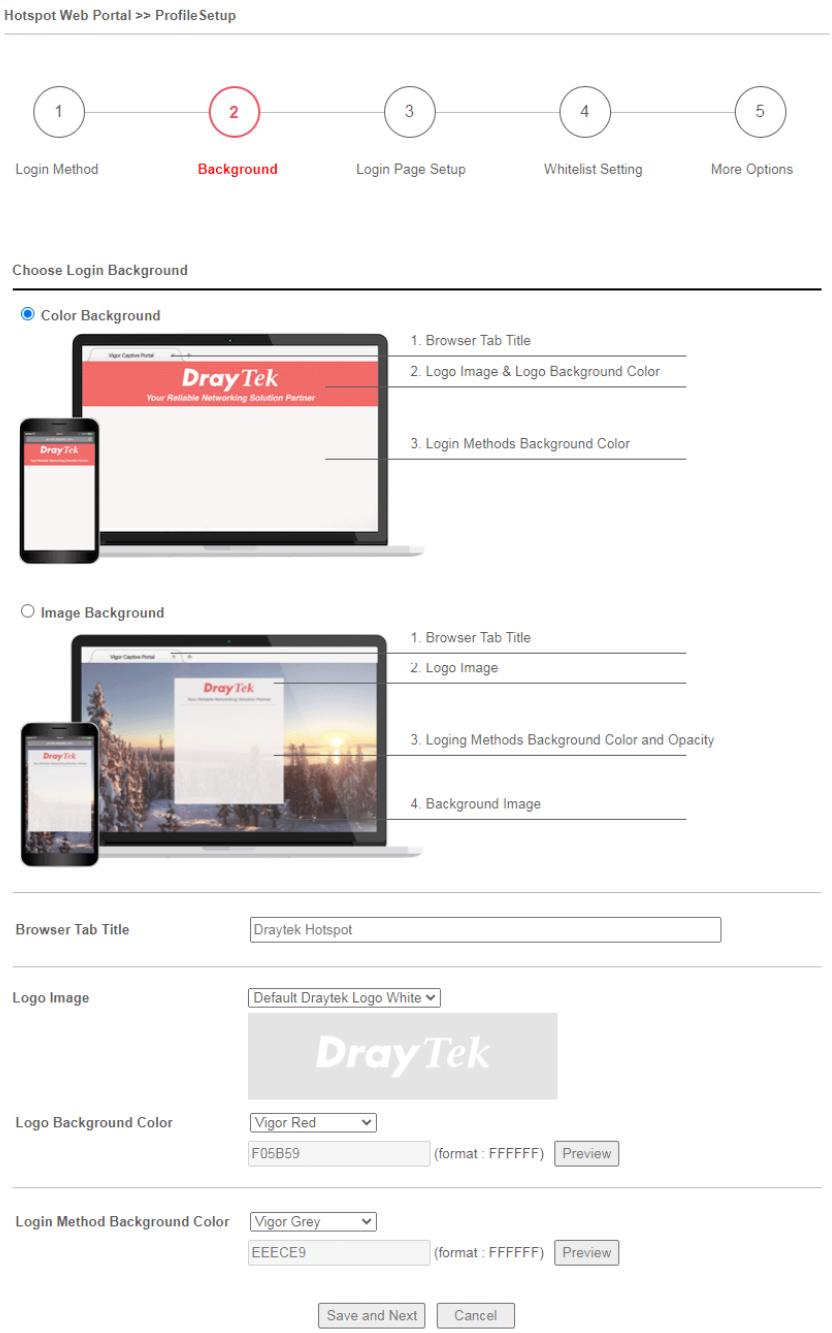
	RADIUS NAS-Identifier - It is an attribute of the RADIUS server, used by a client as an identification on a RADIUS server. Enter a string with less than 32 characters.
When External Portal Server is selected as Portal Method	
Captive Portal URL	Enter the captive portal URL.
Redirection URL	Enter the 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. **RADIUS NAS-Identifier** - It is an attribute of the RADIUS server, used by a client as an identification on a RADIUS server. Enter a string with less than 32 characters.
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.

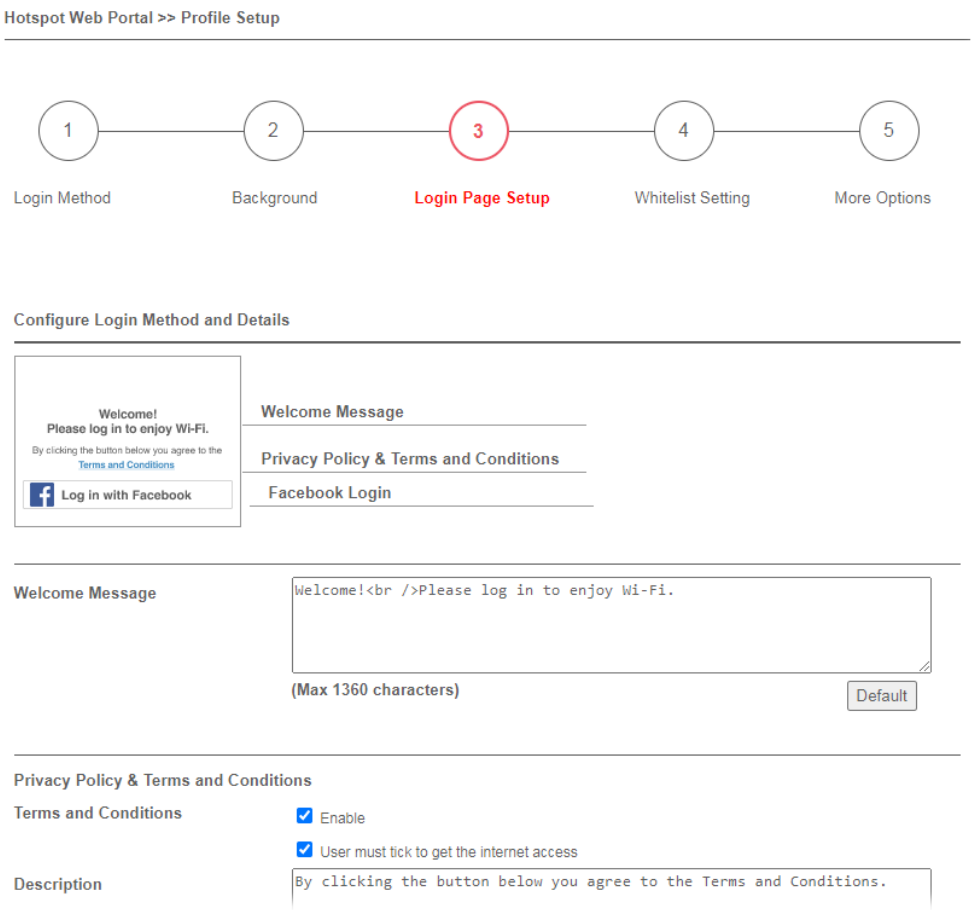
If you have selected **Skip Login, landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup.*

3 Login Page Setup

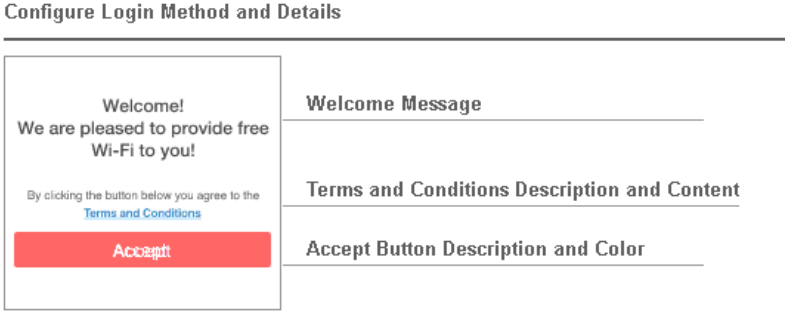
In this step you can configure settings for the login page.

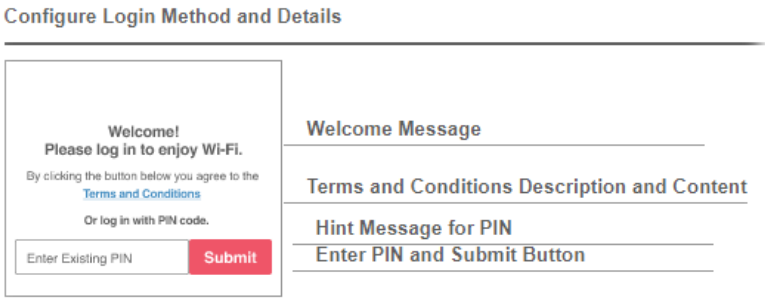
Click Through

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:	

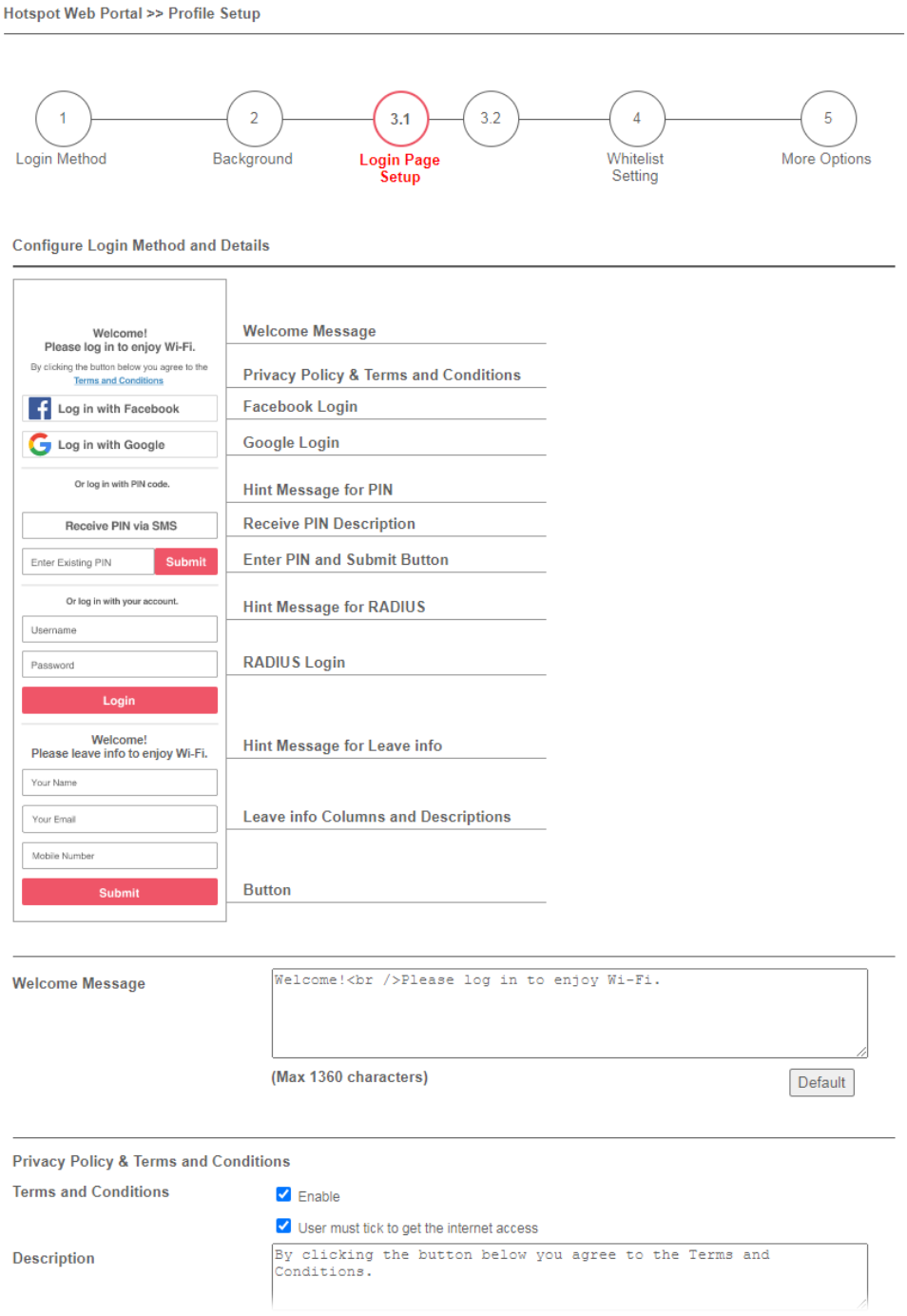


Welcome Message	Enter the text to be displayed as the welcome message.
Privacy Policy & Terms and Conditions	
Terms and Conditions	**Enable** - Check the box to enable the option. **User must tick to get the internet access** - This check box is enabled in default if **Terms and Conditions** is enabled. **Description** - Enter the text to be displayed in the Terms and Conditions pop-up window. **Content -** It contains **Internal Content** and **External Content.** Choose Internal Content to enter the text to be displayed as the Terms and Conditions hyperlink text. Or choose External Content to enter an URL that will display the terms and conditions.
Data Collection for Marketing	**Enable** - Check the box to enable the option. **User must tick to get the internet access** - Check the box to enable the option. **Description** - Enter the text to inform the user.
Error message when the user does not tick	Enter the text to notify the user.
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.
When **PIN with Voucher** is selected as the login method,	
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.
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:

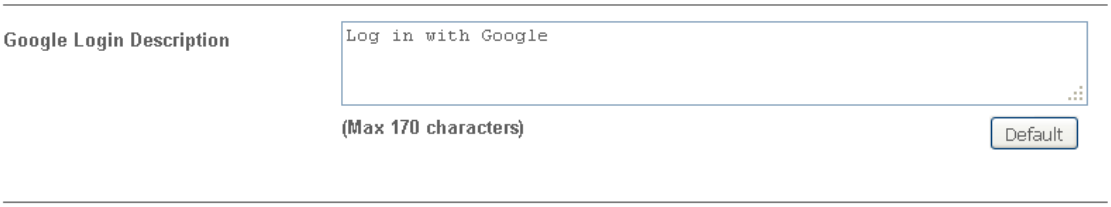
Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.

Privacy Policy & 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:

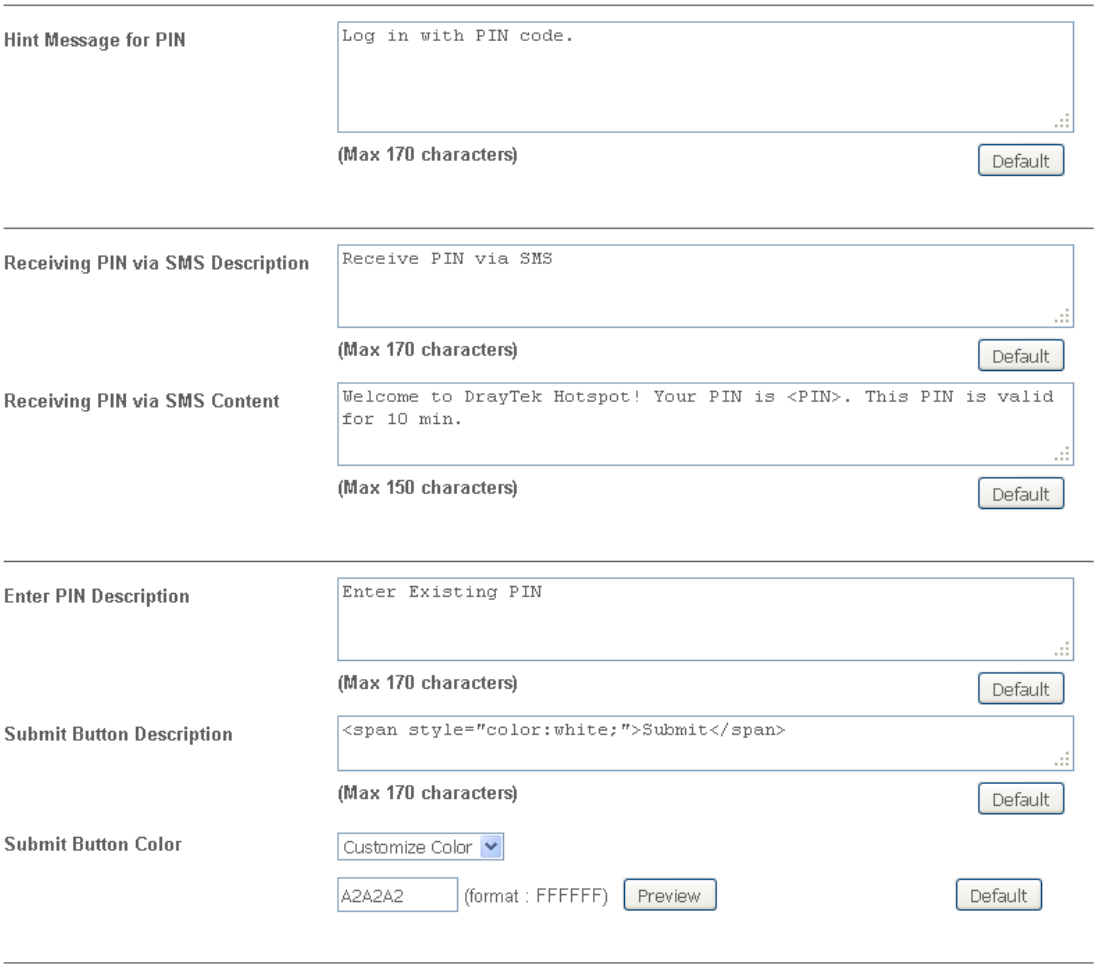
Item	Description
Facebook Login Description	Enter the text to be displayed on the Facebook login button.

If you have selected Google login, the setting will appear:



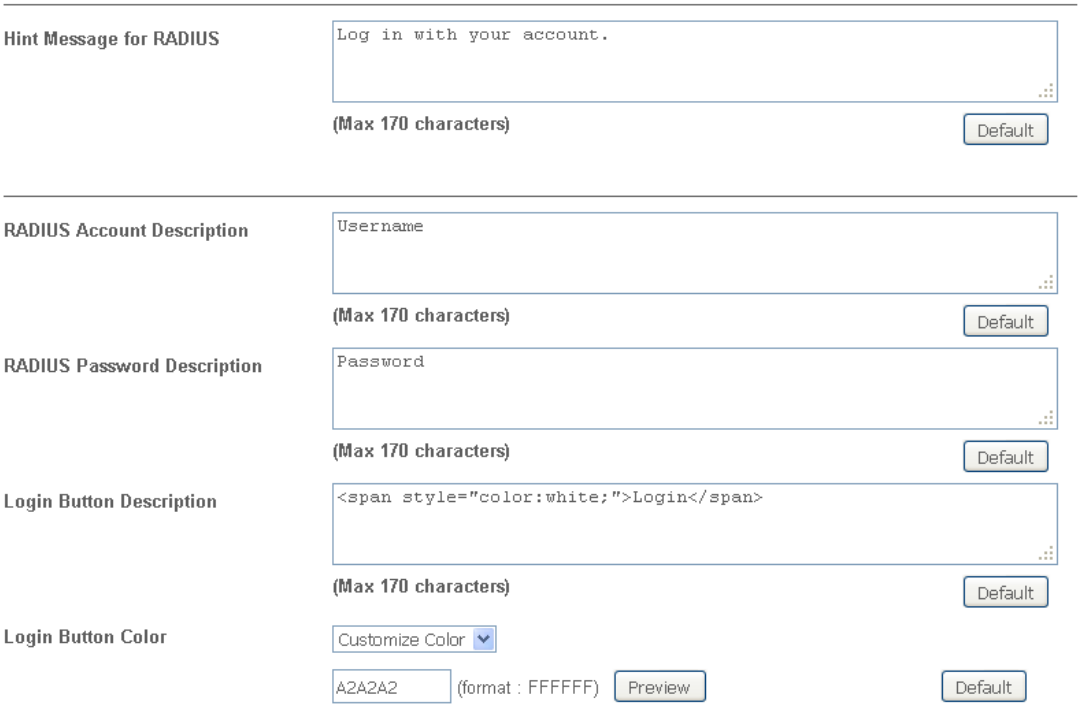
Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.

If you have selected PIN login, these settings will appear:



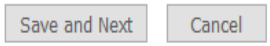
Item	Description
Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by **<PIN>** within the message.
Receiving PIN via Mail Subject	Enter the subject of the mail to inform the user about the PIN code.
Receiving PIN via Mail Content	Enter the content of the mail to inform the user about the PIN code.
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.

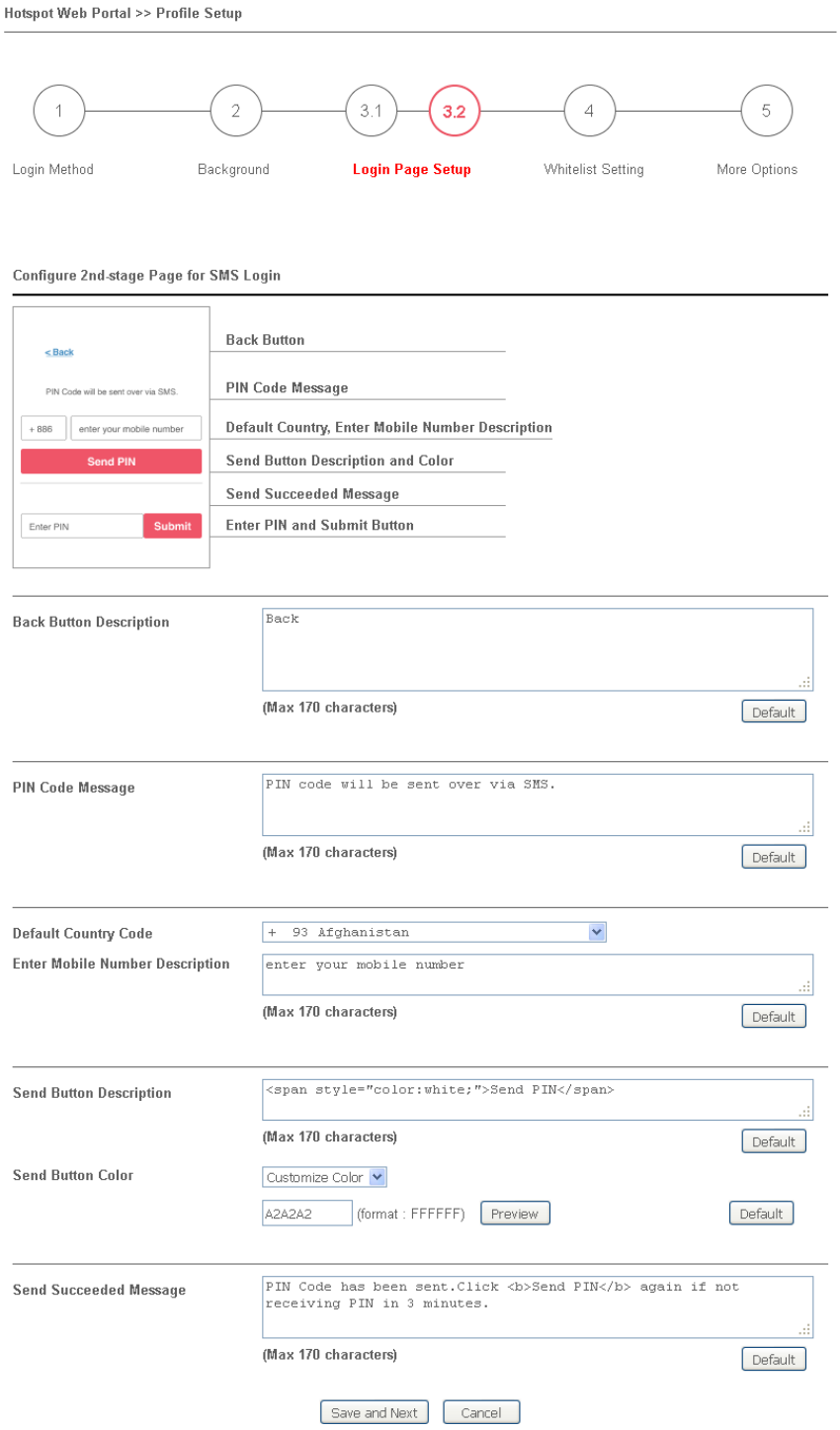
And finally, the save and cancel buttons are always displayed.



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.



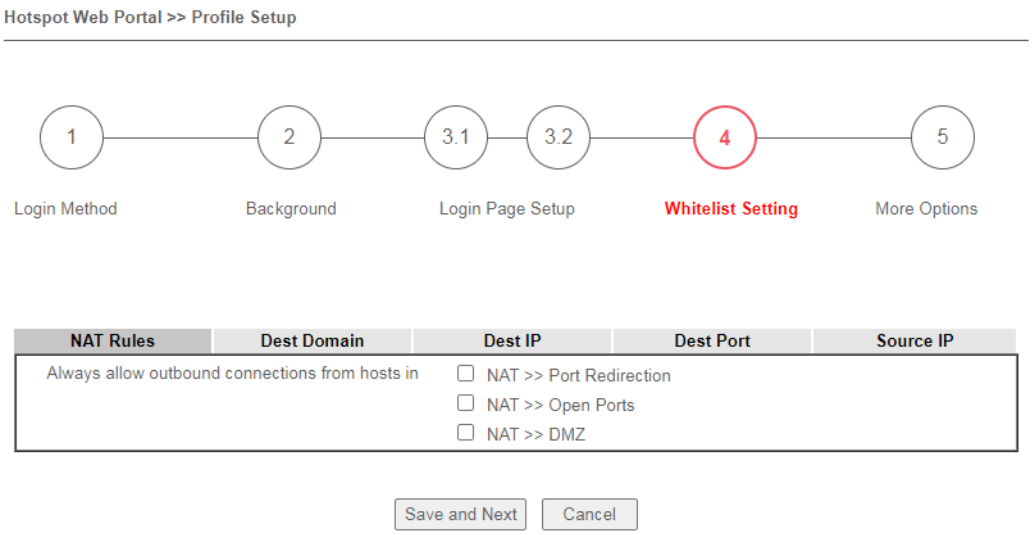
Available settings are explained as follows:

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	Select the default country code to be displayed using the dropdown

Code	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.

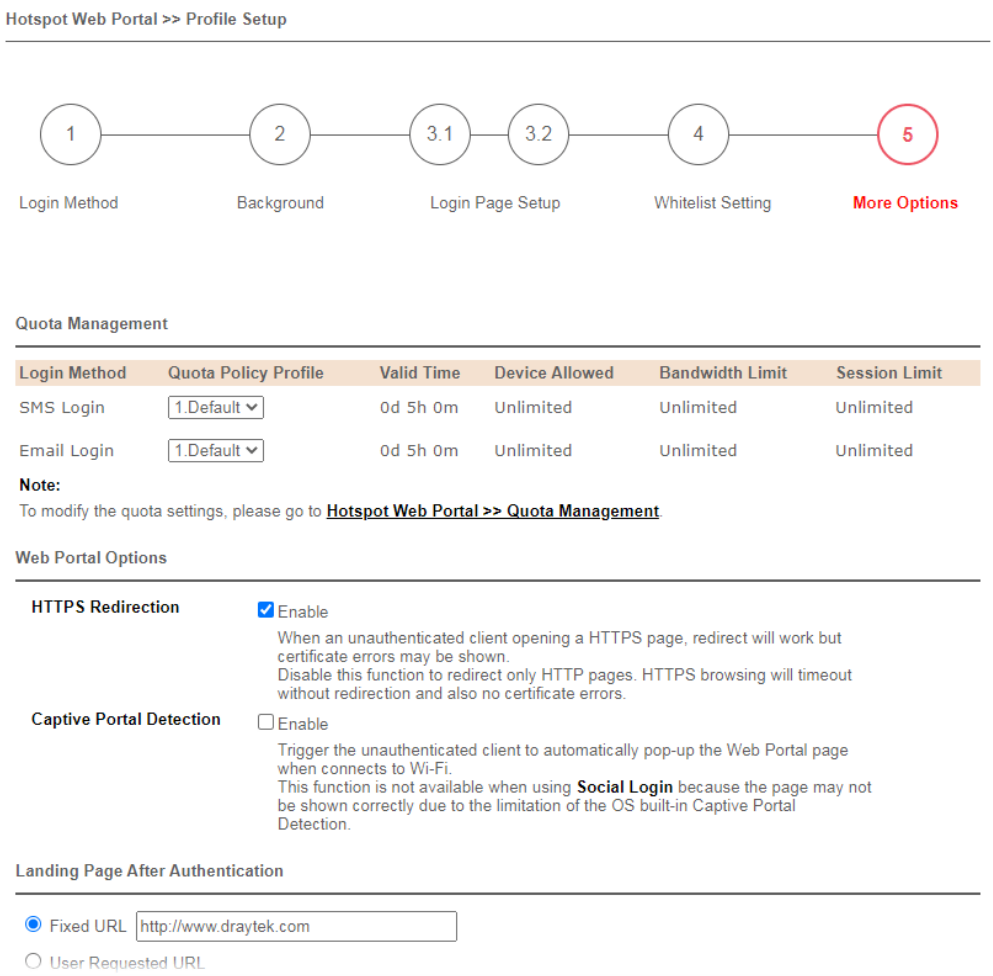


Available settings are explained as follows:

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.
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 the number of HTTPS sessions exceeds the default limit, the web portal would temporarily bypass them without authentication.

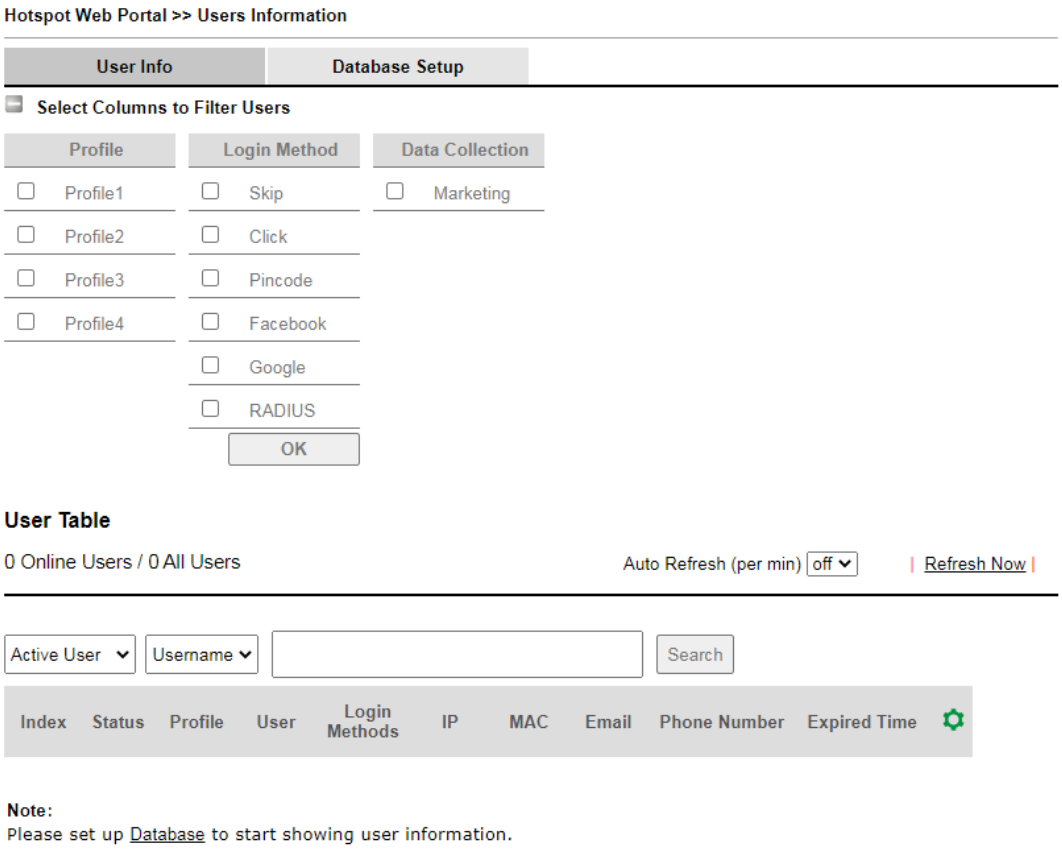
	Those clients would be redirected to the web portal and authenticate later.
Landing Page After Authentication	
Fixed URL	Specifies the webpage that will be displayed after the user has successfully authenticated. The user will be redirected to the specified URL. This could be used for displaying advertisements 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.
Force Landing Page Stay	This option is useful for mobile phone user. The mobile phone users can access into Internet by means of Wi-Fi connection. In general, when **Captive Portal Detection** is enabled on Vigor router, the login page will appear once the mobile phone detects the Wi-Fi signal. After entering the username and password (for authentication), the landing page will appear first on the screen of the mobile phone. Yet, some mobile phone will skip the landing page and access the Internet instead. This feature can force the landing page to stay on the screen of the mobile phone for a while. **Enable -** Select it to enter the period of time for keeping the landing page.
Applied Interfaces	
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
Finish	Click to complete the configuration.
Cancel	Click to abort the configuration process and return to the profile summary page.

V-4-2 Users Information

The log information for users accessing into Internat through web portal will be shown on this page. Click a user link can open another web page displaying more detailed information.

V-4-2-1 User Info

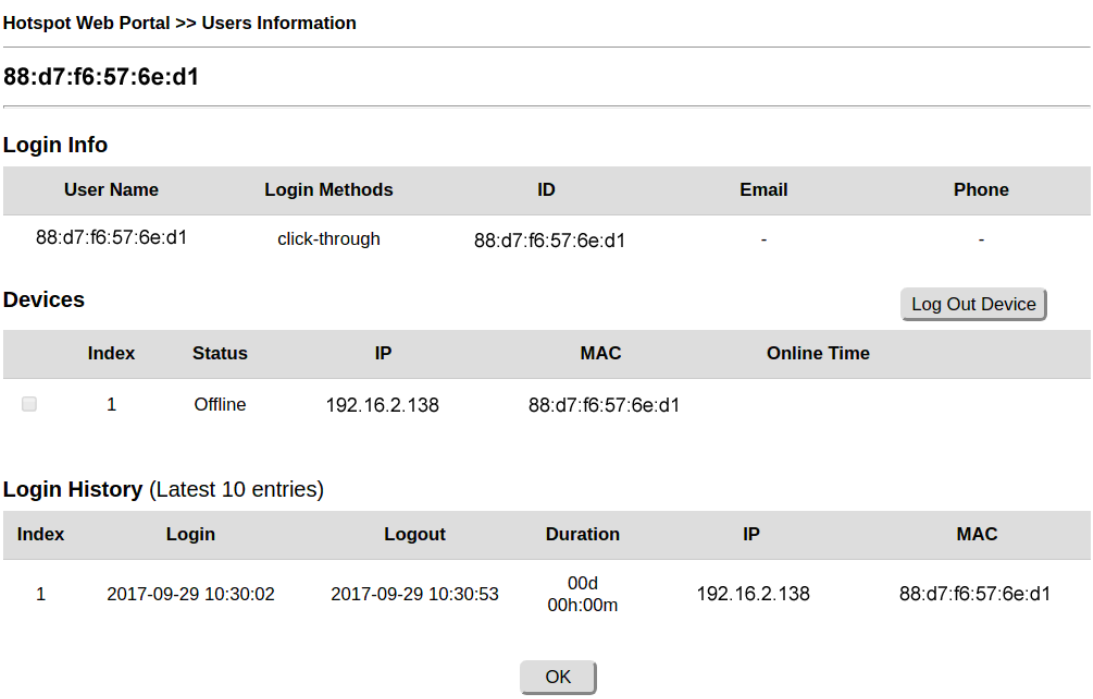
The page can display user information based on the filtering conditions (profile or login method).



Available settings are explained as follows:

Item	Description
Select Columns to Filter Users	Simply specify the profile and the login method for filtering users who want to access Internet through the login method. It is useful for system administrator to manage the user's access based on different conditions when there are a lot of users requiring to access into Internet.
User Table	Information for the users accessing into Internet via Hotsport Web Portal will be displayed and recorded in this page.

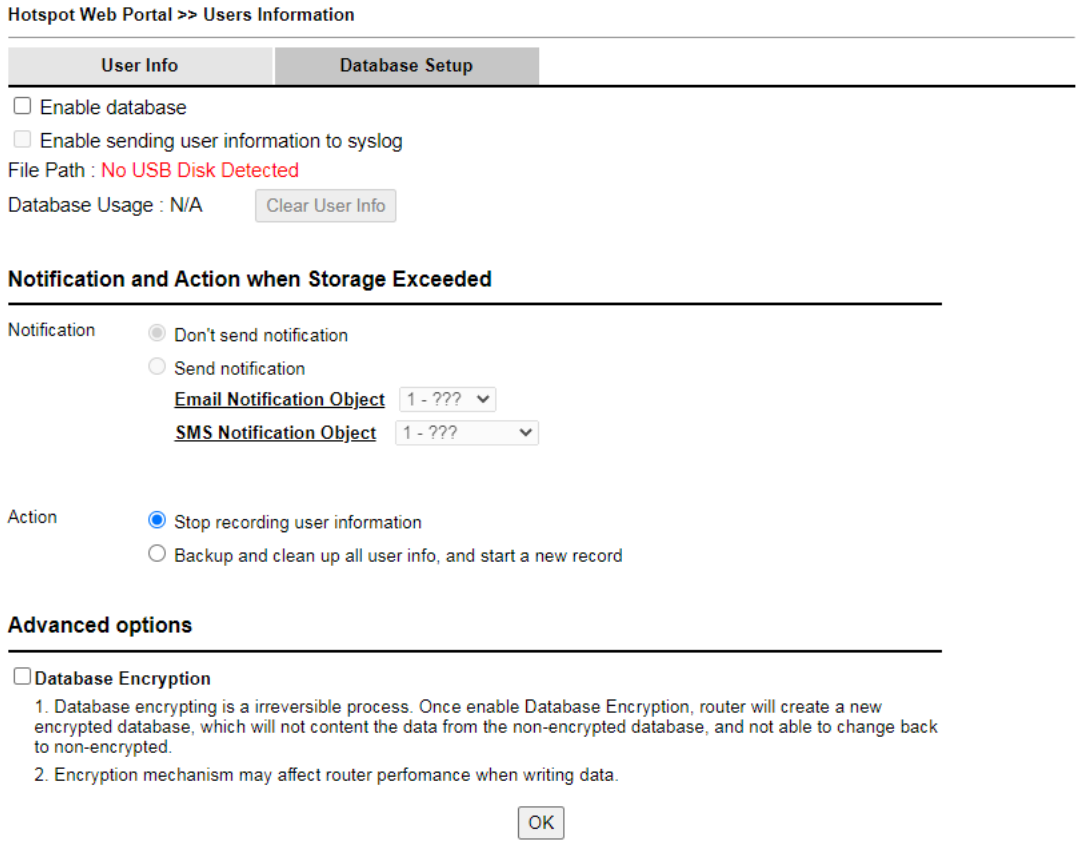
Click the MAC address link for certain user, information page related to the selected device will be shown as the following page.



Basic information for the device will be shown on the field of Login Info; online/offline status for the device can be send on the field of Devices; and historical information for device login will be shown on the field of Login History. In addition, to forcefully log out a selected device, simply check the one you want to logout and click the **Log Out Device** button.

V-4-2-2 Database Setup

This page allows the user to configure settings for database on USB disk.



Available settings are explained as follows:

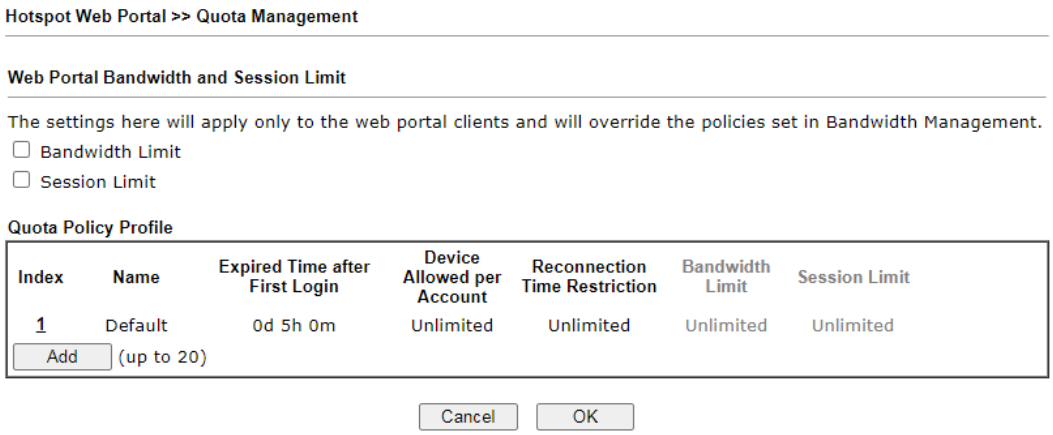
Item	Description
Enable database	Check the box to record user information on router's database. Before checking this box, insert a USB disk with adequate storage space, first.
Enable sending user information to syslog	Check the box to send user information to syslog.
File Path	If a USB disk has been inserted into the USB port of Vigor router, the file path will be shown in this area.
Database Usage	Display the usage and remaining space on the database. **Clear User Info** – The user information will be displayed on the page of User Info. You can delete the information by clicking this button.
Notification and Action when Storage Exceeded	
Notification	**Don't send notification –** Vigor router system will not send any notification to any receipient. **Send notification** - Vigor router system will send a notification e-mail to specified receipient(s) that selected from **Email Notification Object** and **SMS Notification Object**.
Action	**Stop recording user information –** Vigor router system will stop to record the user information onto USB disk.

	Backup and clean up all user info, and start a new record – Vigor router system will backup all existed information on the USB disk onto the host and clean up the information from USB disk. Later, it will start a new record.
Advanced options	
Database Encryption	Select to have the router create a new encrypted database. Once this is done, you will not be able to revert to an unencrypted database.

V-4-3 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

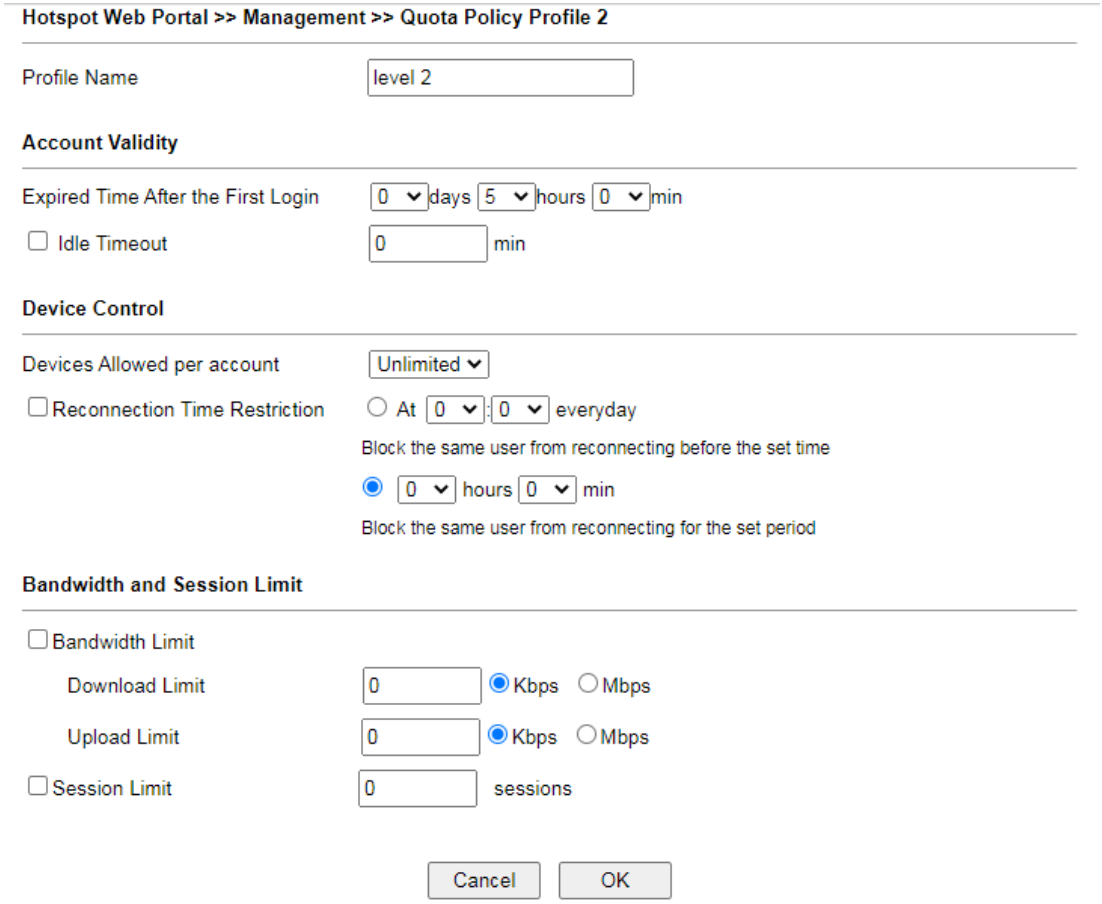
Settings configured in Quota Management will override the policies set in **Bandwidth Management>>Bandwidth Limit** and **Bandwidth Management>>Limit**.



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	**Bandwidth Limit** – Check the box to configure bandwidth limit for

Session Limit	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.

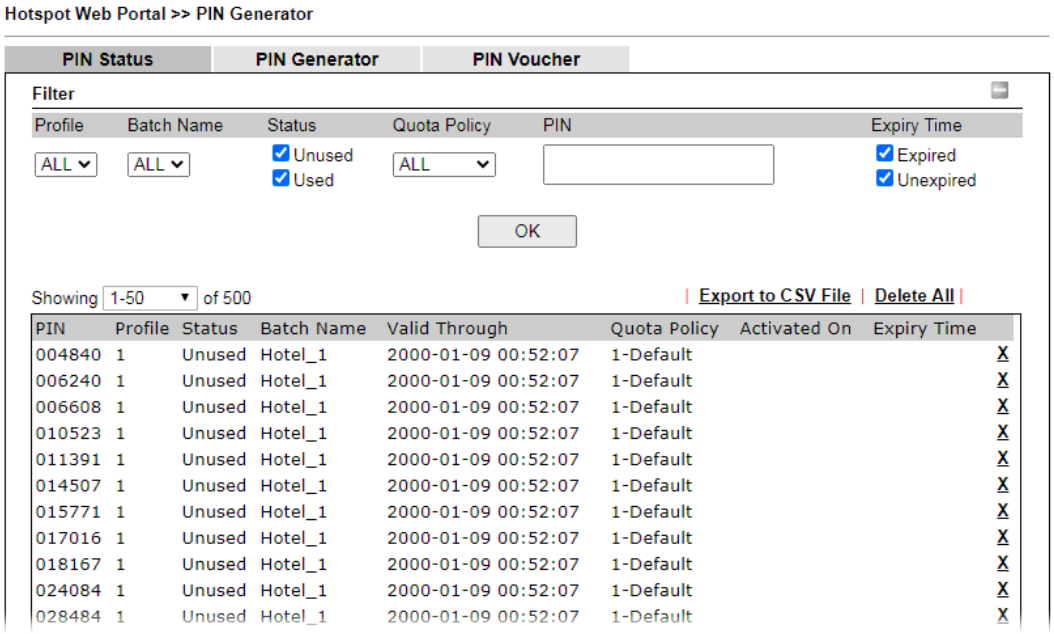
After finishing all the settings here, please click **OK** to save the configuration.

V-4-4 PIN Generator

The system administrator can generate multiple PIN codes for various usage. Before generating PIN codes, please make sure a **USB** has been inserted onto your Vigor device.

V-4-4-1 PIN Status

This page displays the PIN codes generated by PIN Generator.

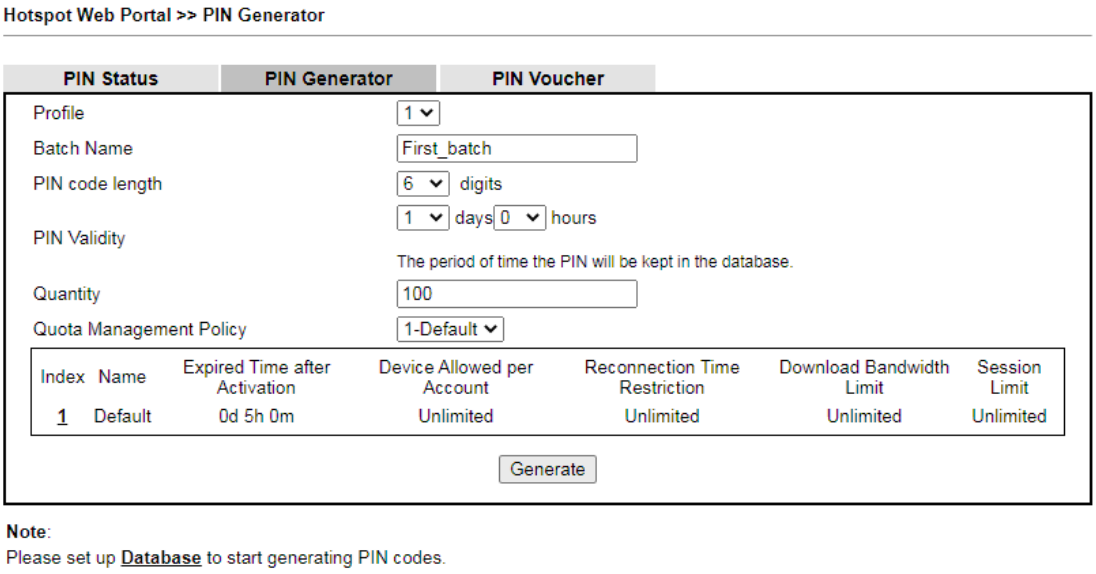


Available settings are explained as follows:

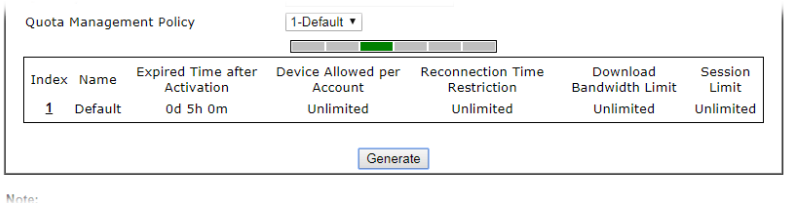
Item	Description
Profile	Use the drop down menu to choose an index number (1 to 4) for PIN generator profile.
Batch Name	Use the drop down menu to choose an existed PIN profile or choose ALL to display the PIN status.
Status	**Unused** - After checking the box, only the unused PIN codes will be shown on this page. **Used** - After checking the box, only the used PIN codes will be shown on this page.
Quota Policy	Use the drop down menu to choose a quota management policy to display related PIN codes.
PIN	Enter the PIN code to display related information on this page.
Expiry Time	**Expired** - After checking the box, only the expired PIN codes will be shown on this page. **Unexpired** - After checking the box, only the unexpired PIN codes will be shown on this page.
OK	Click it to display the PIN code according to the above filtering condition.
Export to CSV File	Click it to export the configuration of PIN code as a CSV file.

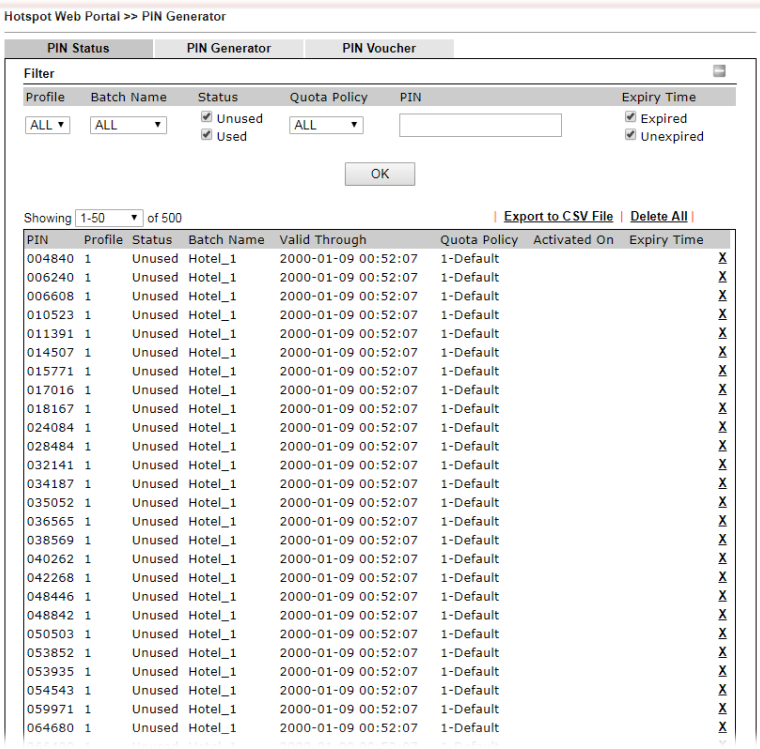
V-4-4-2 PIN Generator

The system administrator can generate multiple PIN codes in response to the user's (e.g., enterprise) demand.



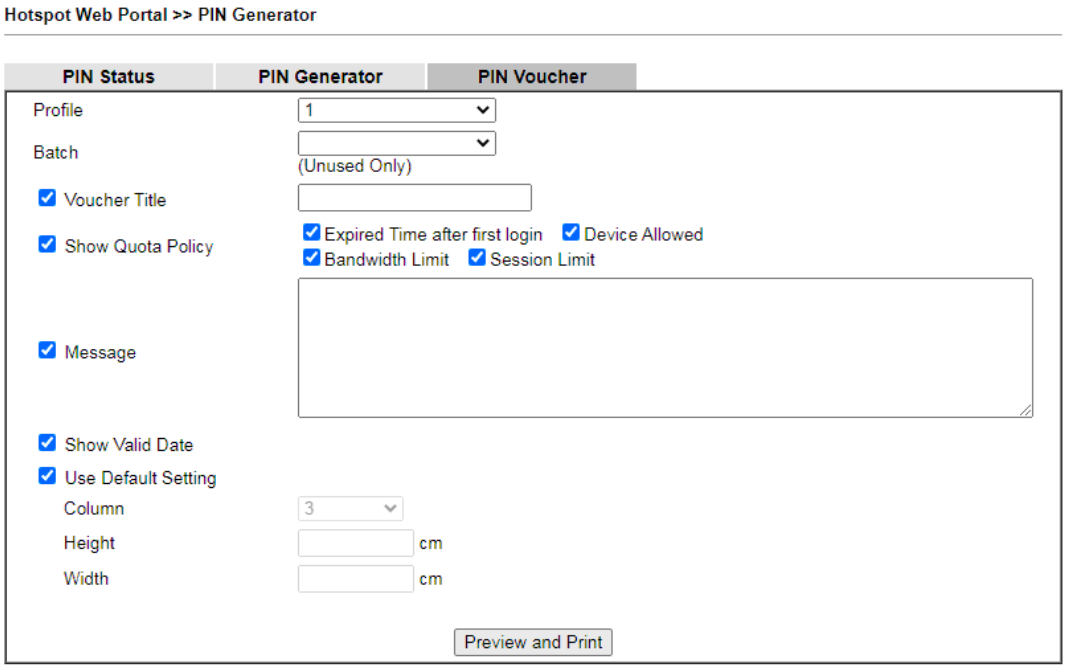
Available settings are explained as follows:

Item	Description
Profile	Use the drop down menu to specify an index number (from 1 to 4).
Batch Name	Enter a string as a batch name.
PIN code length	Specify the length of PIN code.
PIN Validity	Set the period of time.
Quantity	Set the quantity of the PIN code.
Quota Management Policy	Use the drop down list to choose policy profile.
Generate	Click it to generate a PIN code as a voucher. The system will ask you to set up **Database** before executing the generation.  Later, available PIN code will be shown on PIN Status.



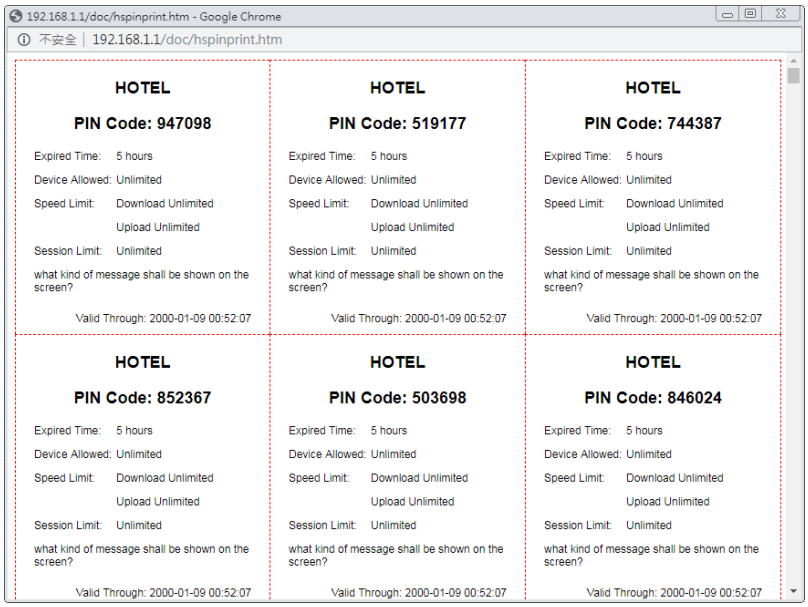
V-4-4-3 PIN Voucher

This page allows to print out the PIN code list.



Available settings are explained as follows:

Item	Description
Profile	Use the drop down menu to specify an index number (from 1 to 4).
Batch	Use the drop down menu to specify an unused batch profile.
Voucher Title	Enter a string as a title which will be shown on a print out paper.

Show Quota Policy	Select the item(s) to be shown on the print-out PIN code list.
Message	Enter a brief description that the client should know.
Show Valid Date	Check the box to display the valid date and time on the printed out list.
Use Default Setting	Set the paper size for printing the vouchers on label printer. **Column** - Use the drop-down list to specify the column value. **Height** - Enter the value of the height. **Width** - Enter the value of the width. Or select to use the default settings.
Preview and Print	Click it to display the PIN code list. This list can be printed out if required. 

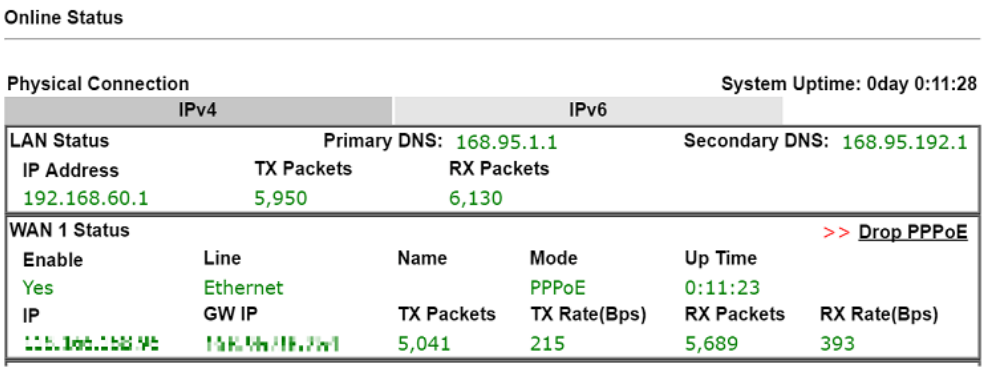
Application Notes

A-1 How to allow users login to Vigor's Hotspot with their social media accounts (e.g., Facebook & Google)

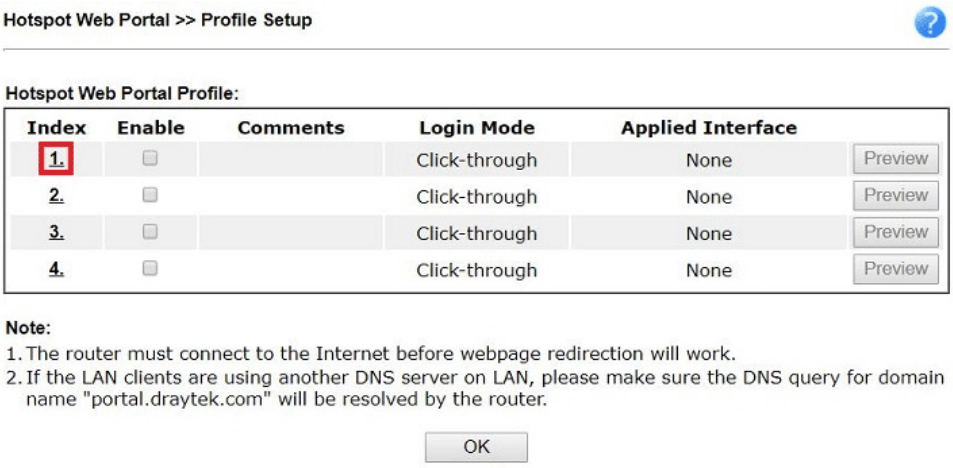
Vigor Router supports Hotspot Web Portal function. The network administrator can set Vigor Router as a Hotspot provider with web authentication and allow users to log in with their social media accounts, such as Facebook and Google. We demonstrate how to set up the hotspot web portal with Facebook login in the following paragraphs.

Vigor Router Setup

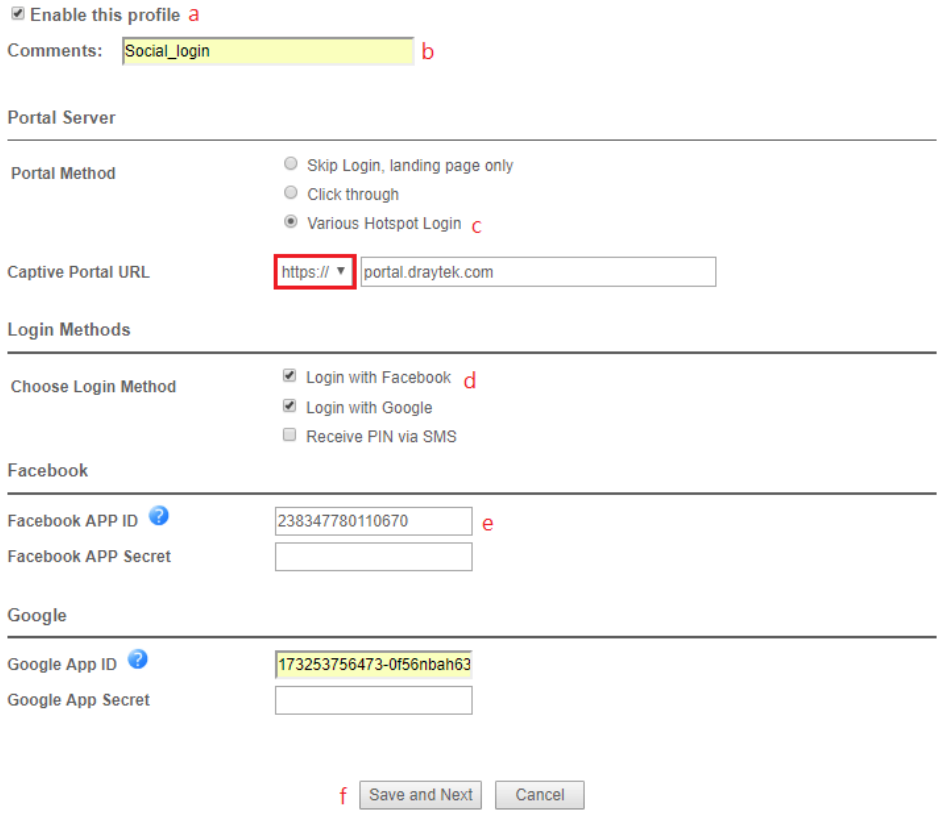
1. Make sure the router is connected to the Internet.



2. Go to **Hotspot Web Portal >> Profile Setup**, click on an available index.



3. Enter the values as the following figure.



(a) Click **Enable this profile**.

(b) Enter the comments.

(c) Select **Various Hotspot Login** for Portal Method.

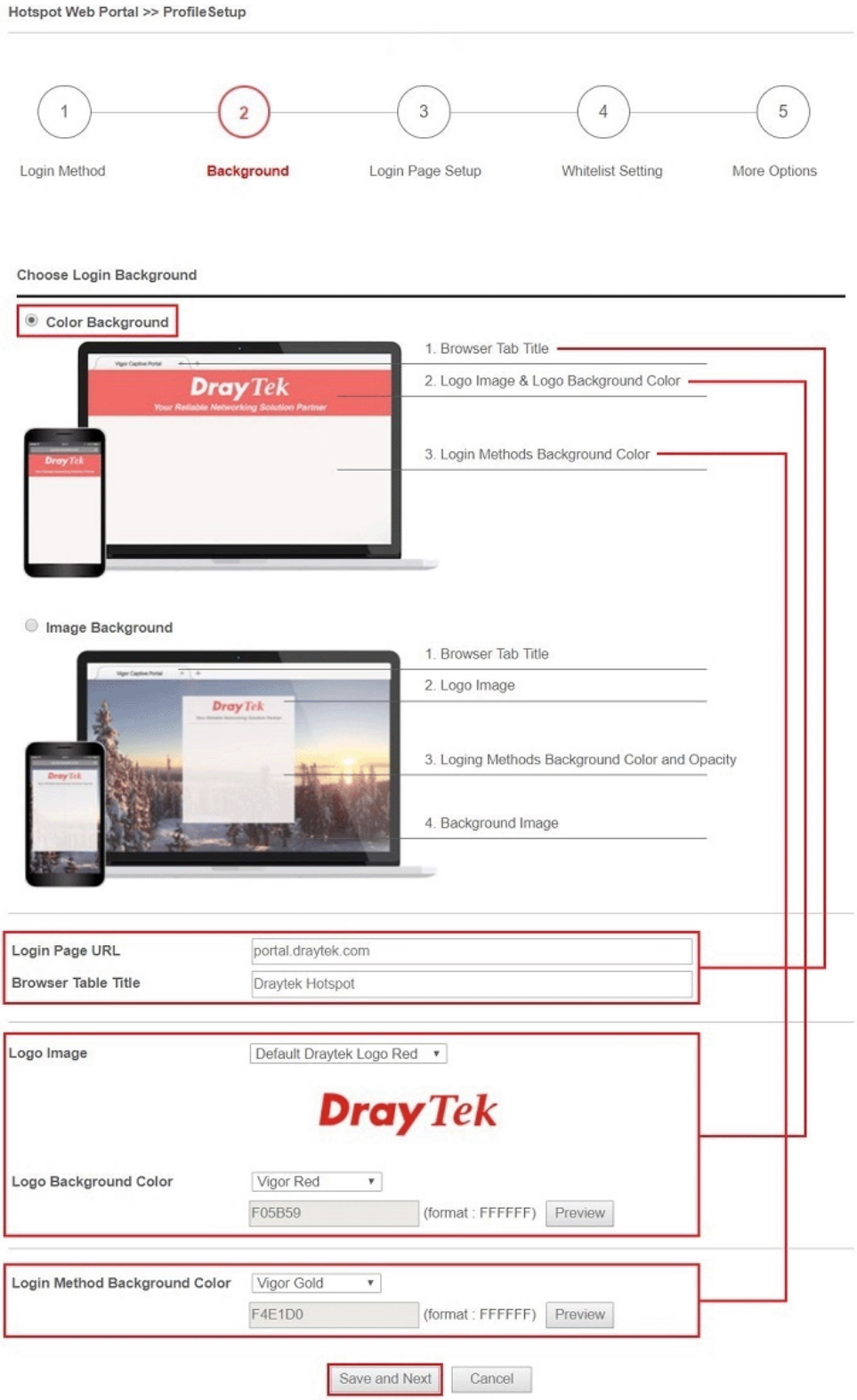
(d) Choose **Login with Facebook** or **Login with Google** as Login Method.

If **Login with Facebook** is selected, the protocol of the **Captive Portal URL** need to be changed to **HTTPS** instead of HTTP because Facebook force to use **HTTPS** URL in their policy.

(e) Enter the **APP ID** and **secret**.

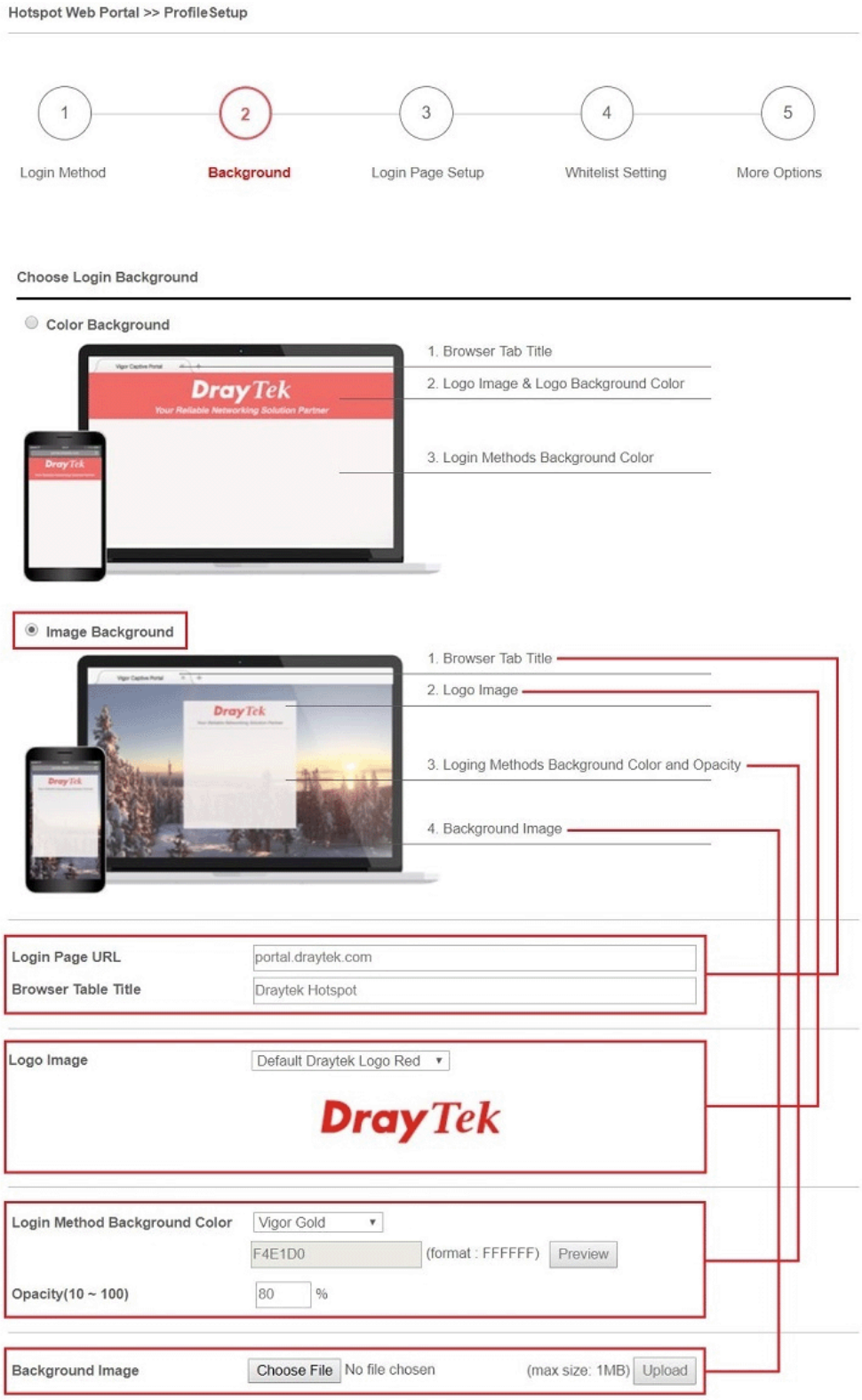
(f) Click **Save and Next**.

4. Choose the **Color Background**, customize the information a logo color, and click **Save and Next**.

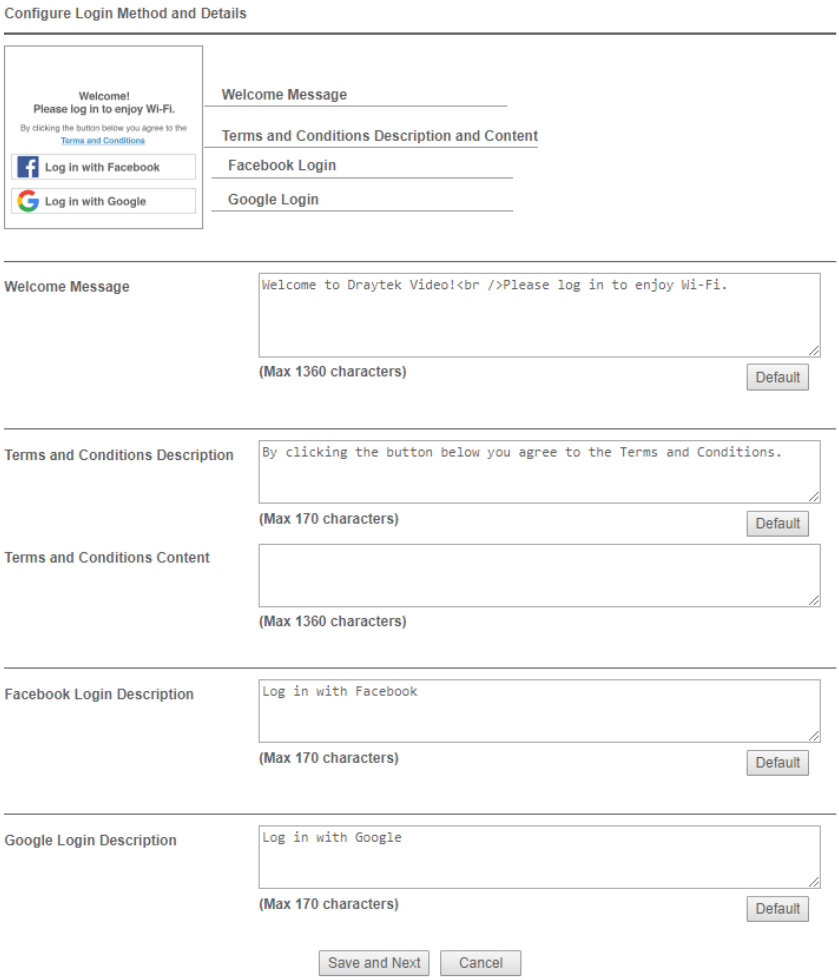


You can click the Step Icon on the top of the page to go to the step you want. The router will save your setting automatically.

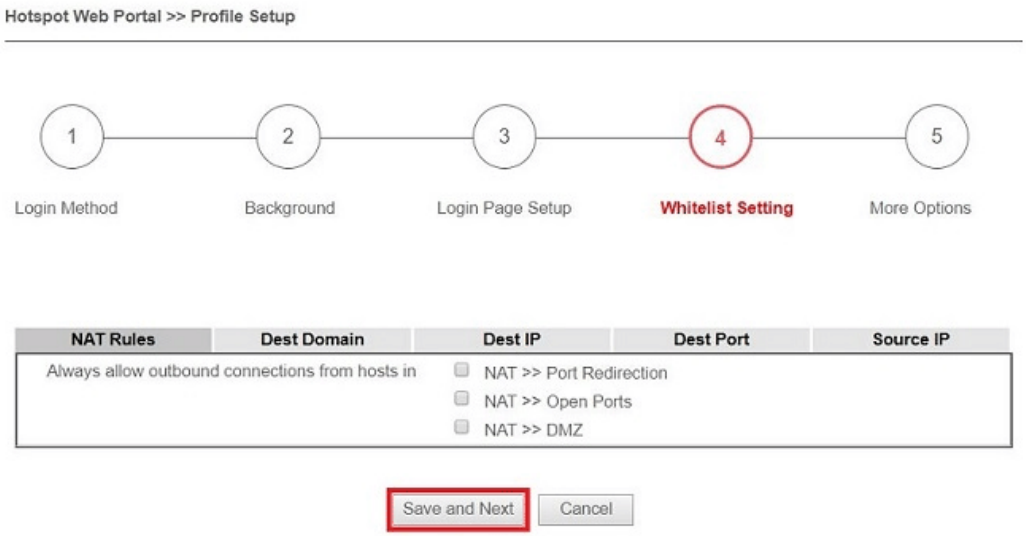
Or choose the **Image Background**, customize the information and background image, and click **Save and Next**.



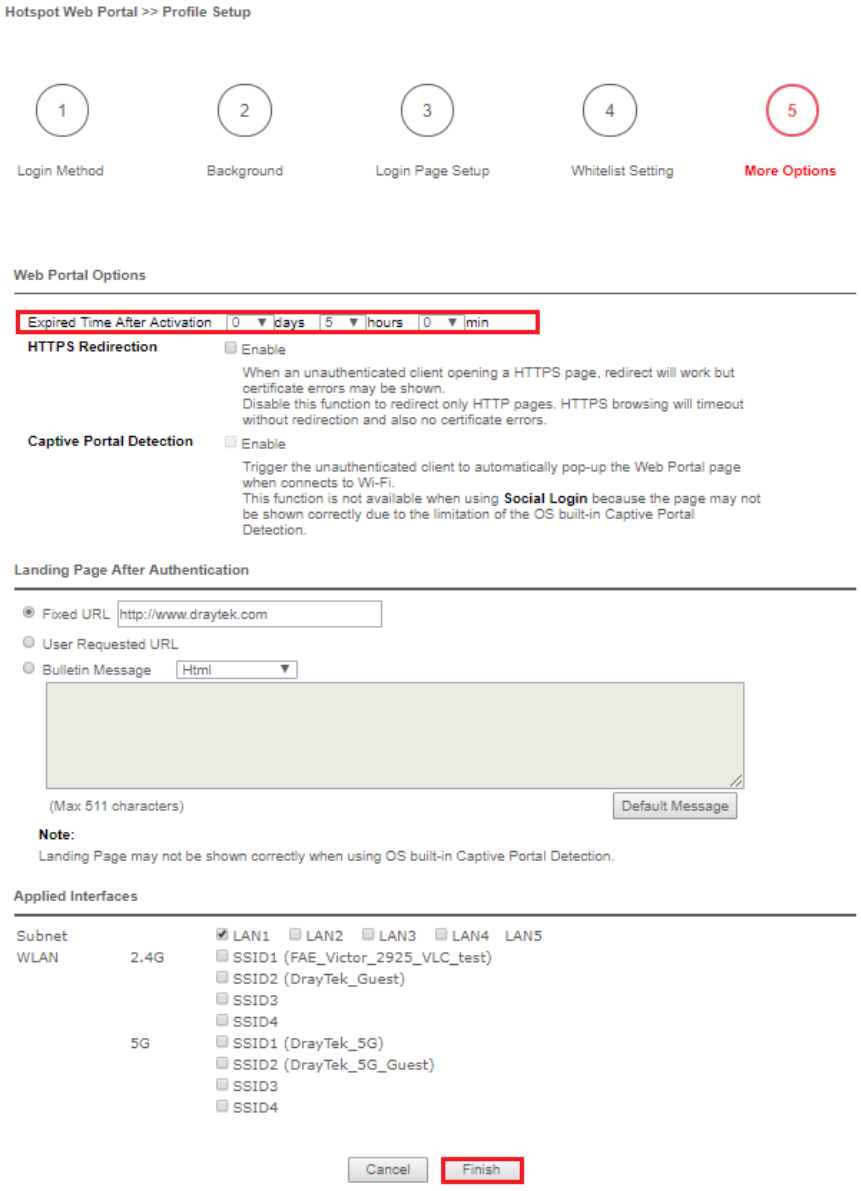
5. Customize the descriptions on the login page, then click **Save and Next**.



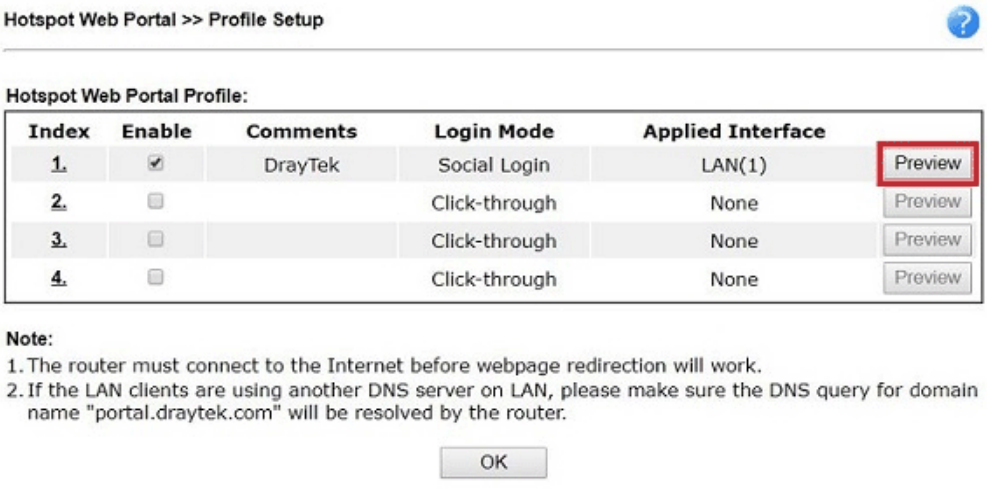
6. You can set the **Whitelist** for the profile here to allow specific clients to access the internet or certain websites can be visited without login.



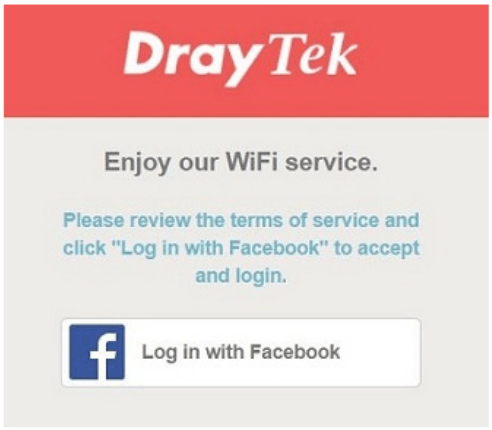
7. Set up the **Expired Time After Activation** and **Landing Page After Activation** that Hotspot clients will see after they login successfully. Finally, select the interfaces to which you would like this hotspot profile apply to, then click **Finish** to save the setting.



8. Then the Hotspot setup is finished. You may click Preview to check the login page.

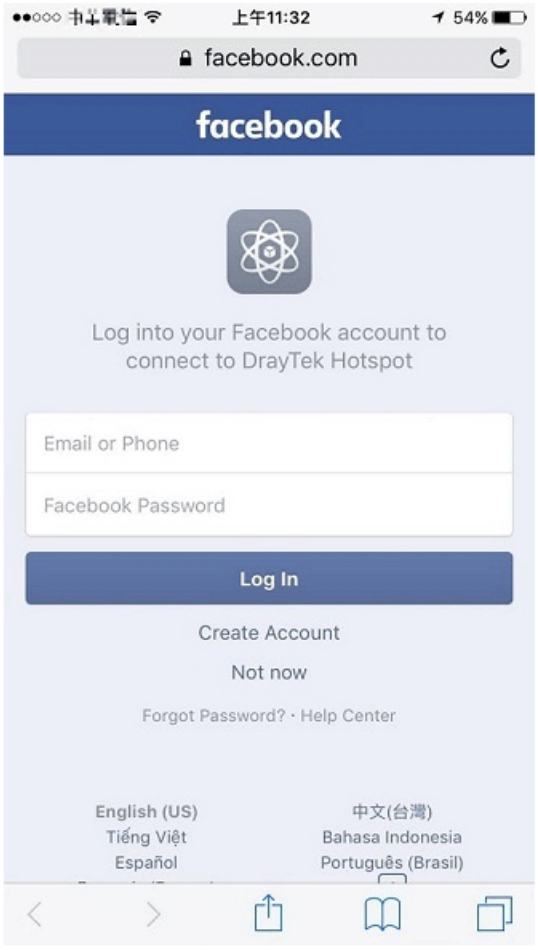


9. Now, when clients connect to the selected router interface, and try to access internet, they will be redirected to "portal.draytek.com".



- Due to security concerns, the browser might warns that it cannot verify server identity, the clients would need to tap "Continue" before they can proceed to portal.draytek.com.
- The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.

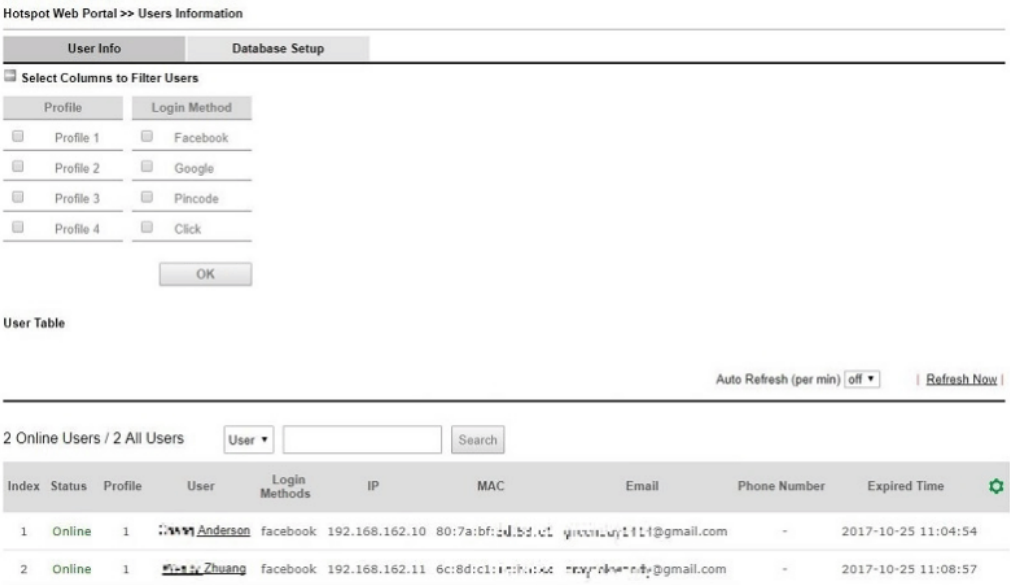
10. Tap on a login method, and it will open the social media login page. Enter the social media accounts and password to log in.



11. If the credentials are correct, the client will be redirected to the landing page and be able to access the Internet afterward.

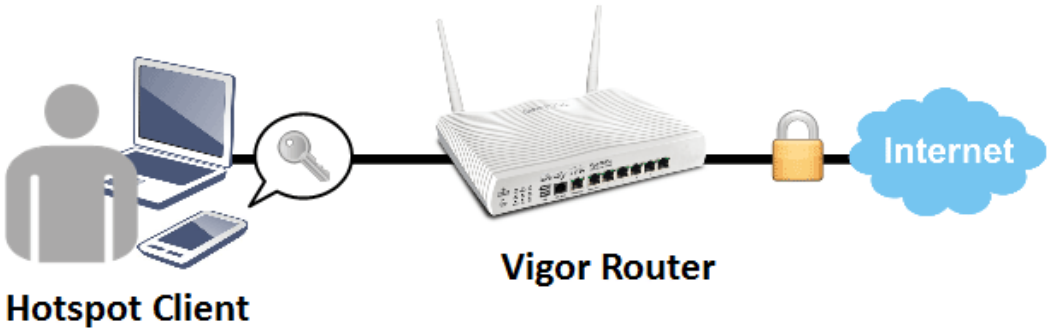
User Information

Network administrator can plug the USB disk to router, to record the basic information of the users who connect to the Wi-Fi and login with their social media accounts. The users' basic information will be listed on Hotspot Web Portal >> Users Information page.



A-2 How to allow hotspot clients to get login PIN code via SMS?

Since 3.8.4.3 version firmware, Vigor Router can act as a hotspot gateway and provide internet access only to the authenticated clients. Network Administrator may set up the router to allow hotspot client to get the login PIN code from an SMS message. This note is going to demonstrate how to set up Vigor Router as a hotspot gateway and be able to send the PIN code to clients by SMS messages.



Vigor Router Setup

1. Make sure the router is connected to the Internet.

Online Status

Physical Connection — **System Uptime: 0day 0:11:28**

IPv4	IPv6

LAN Status	Primary DNS: 168.95.1.1	Secondary DNS: 168.95.192.1
IP Address	TX Packets	RX Packets
192.168.60.1	5,950	6,130

WAN 1 Status — >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:11:23	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
[redacted]	[redacted]	5,041	215	5,689	393

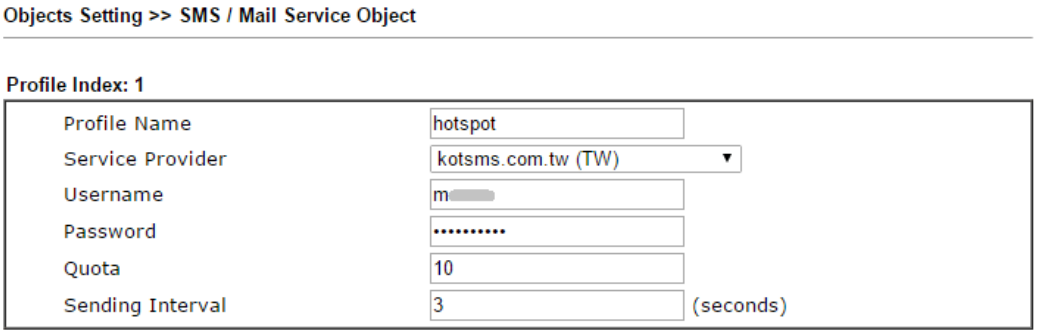
2. Create an SMS Object to send SMS messages. Go to **Objects Setting >> SMS Service Object**, and click on an available profile.

Objects Setting >> SMS / Mail Service Object

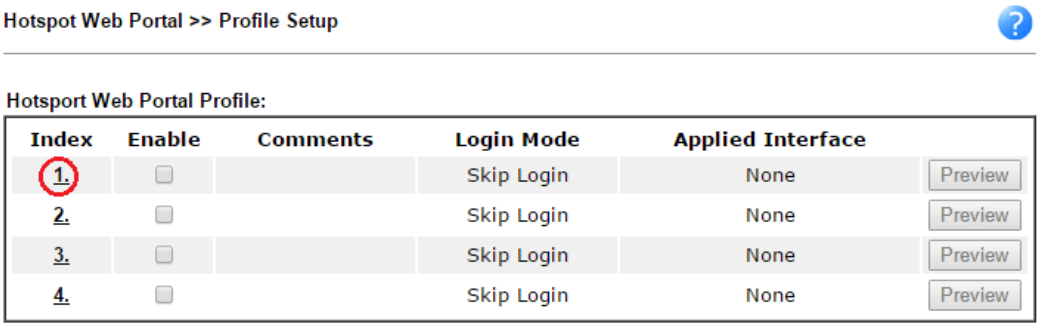
SMS Provider | Mail Server | Set to Factory Default

Index	Profile Name	SMS Provider
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

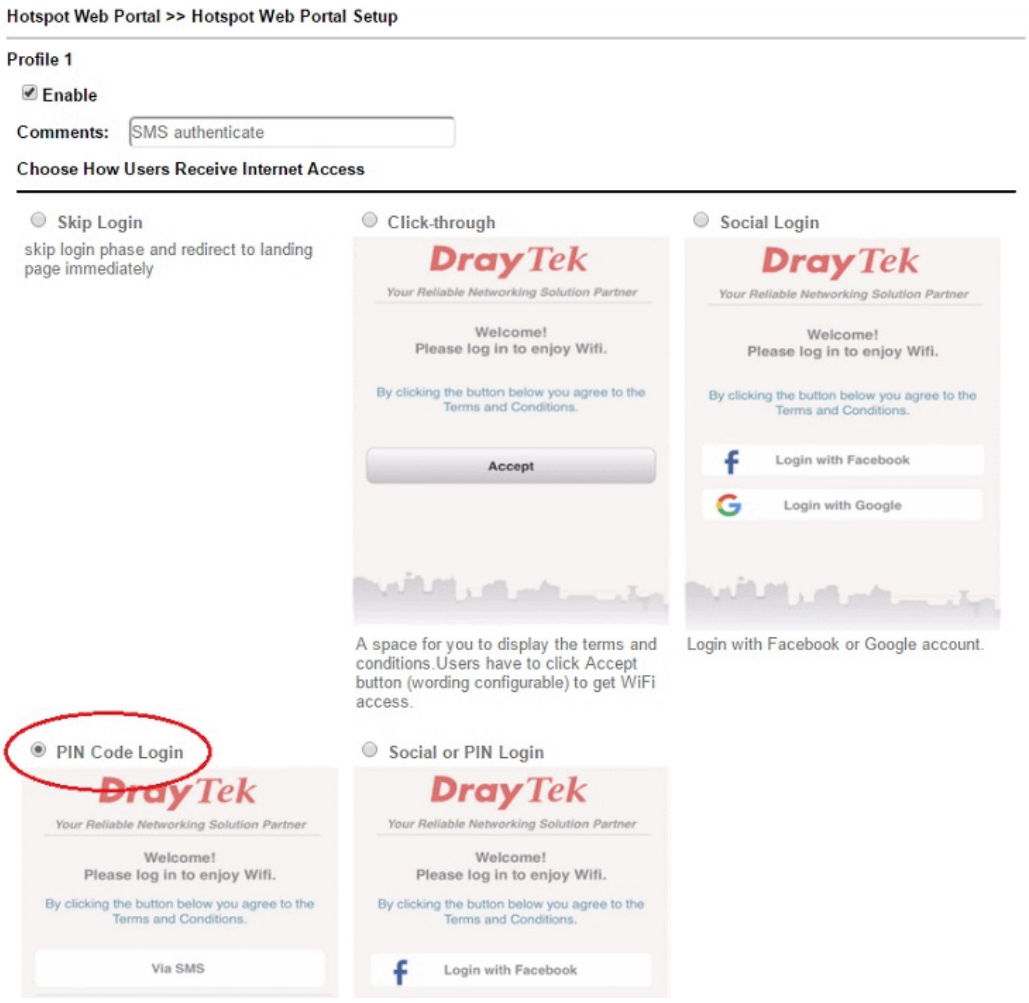
3. Enter the Service Provider details, and click **OK** to apply.



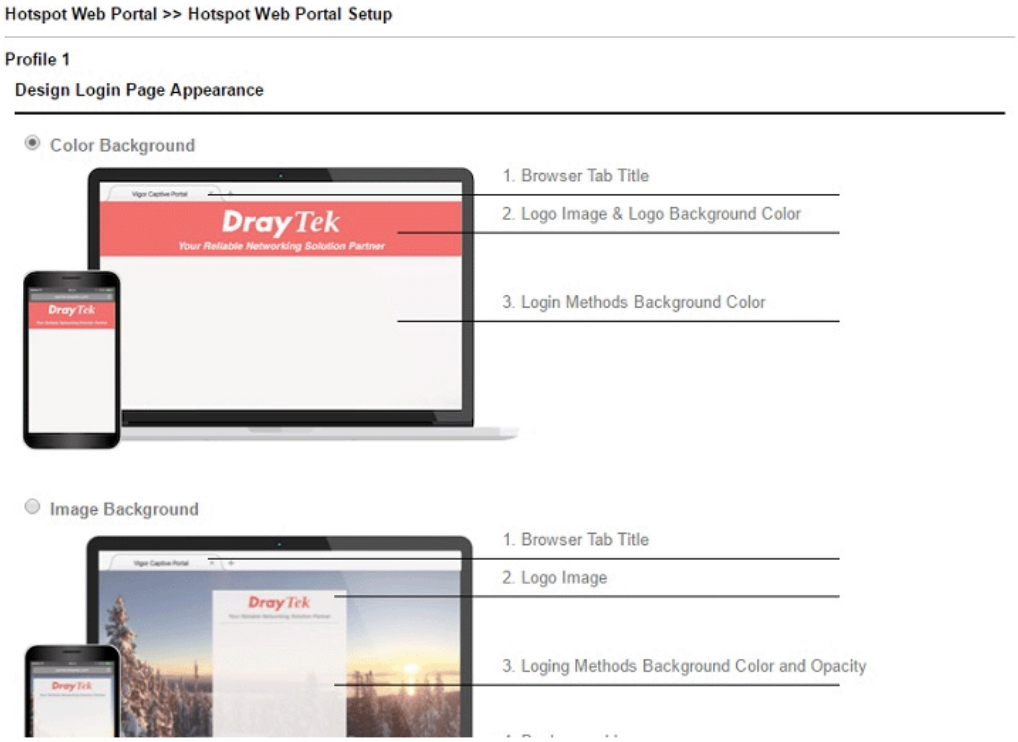
4. Go to Hotspot Web Portal >> Profile Setup, click on an available profile.



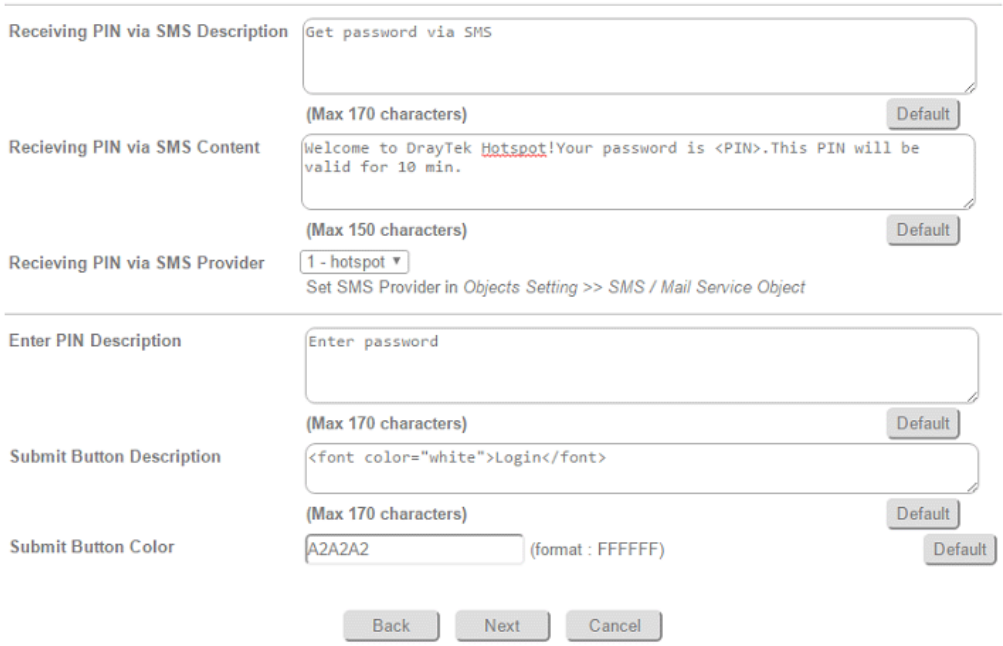
5. **Enable** the profile, give a comment, and choose "PIN Code Login". Then click **Next**.



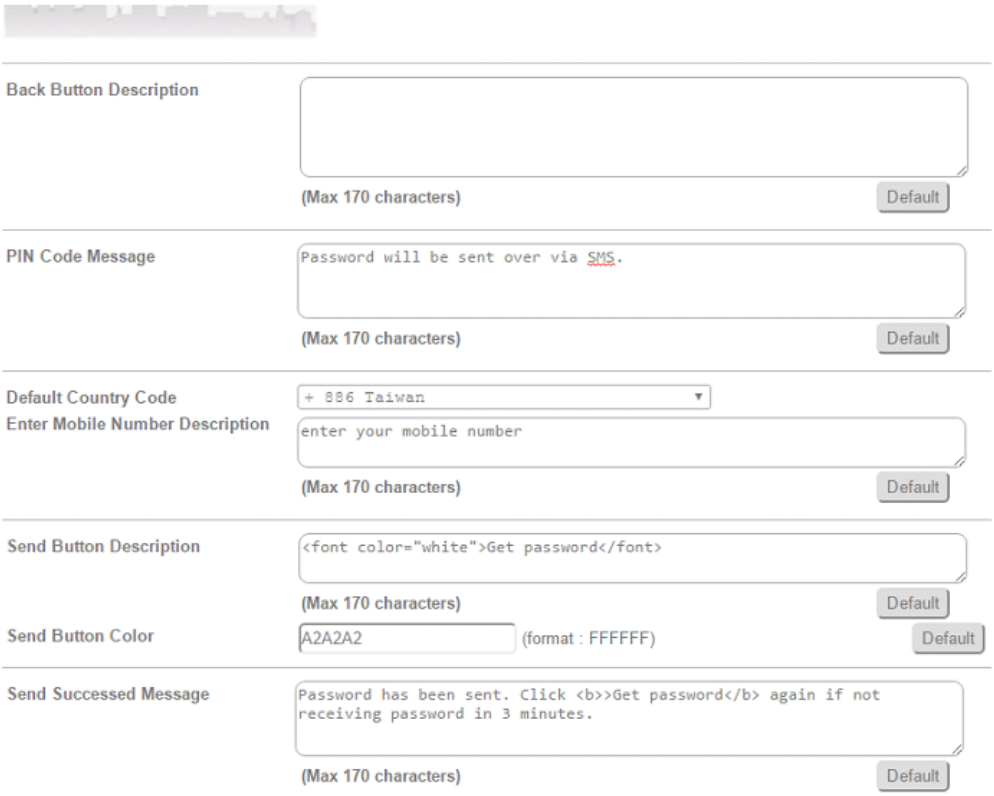
6. Choose a login page design, customize the details, and click **Next**.



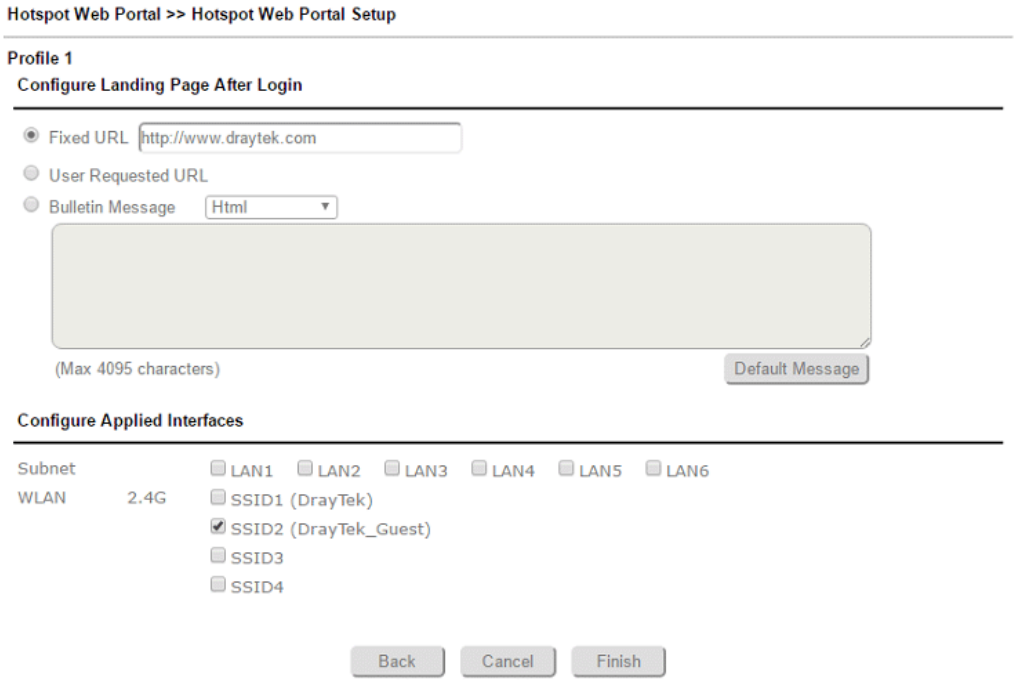
7. Edit the message on the login page, and click **Next**.



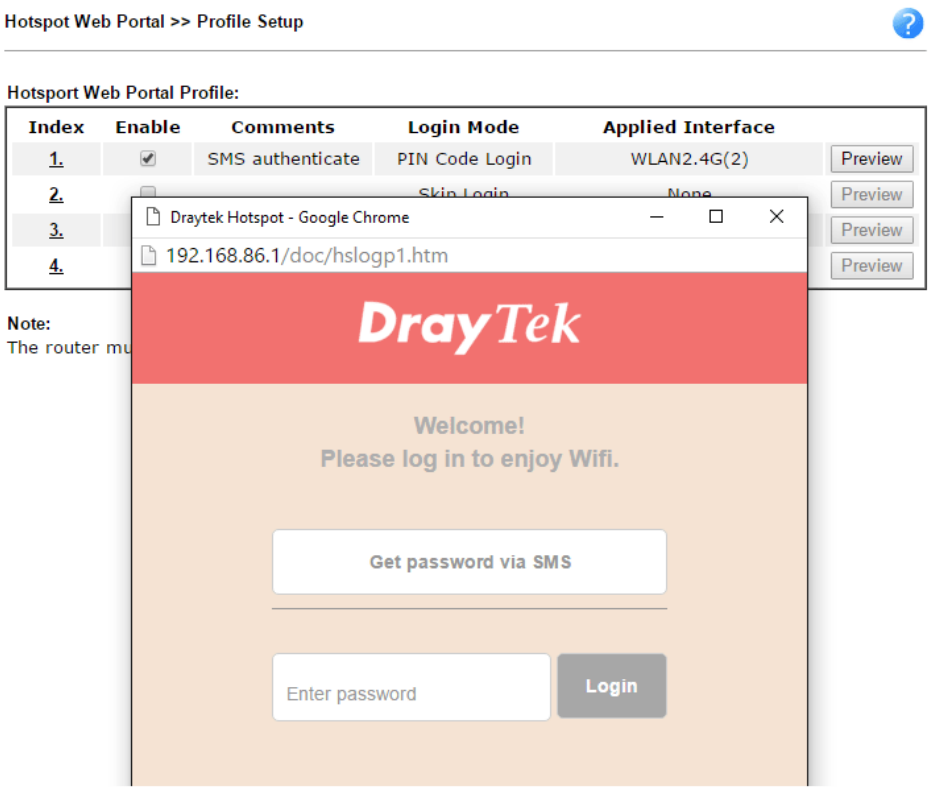
8. Edit the details for SMS settings, then click **Next**.



9. Edit the landing page, choose the interfaces to which the SMS login should apply, and then click **Finish**.



10. Now, the hotspot settings are applied to the selected interfaces. You may click **Preview** to check how the login page looks.



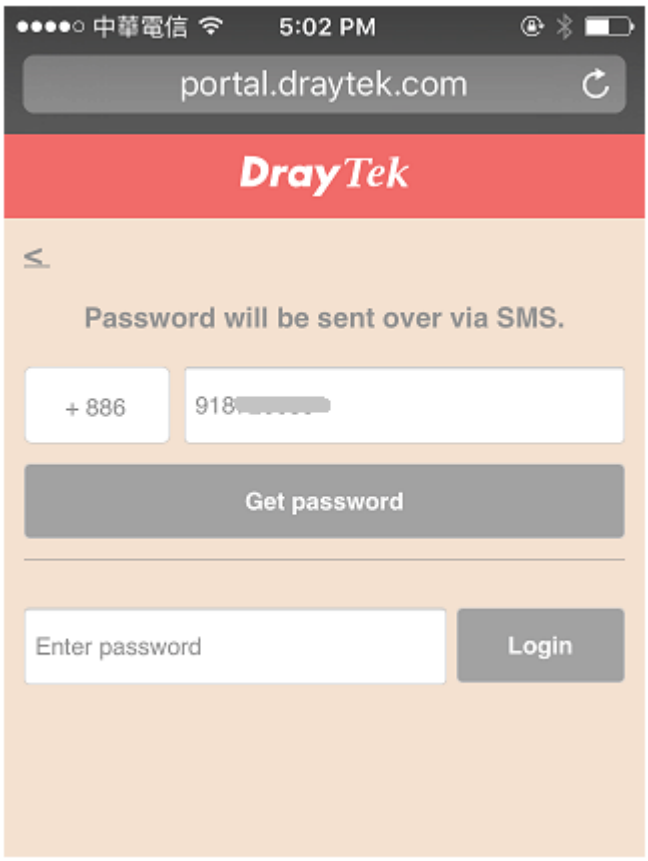
Hotspot Client Login

11. If the client connected to the selected interface of the router and try to open a webpage, they will be redirected to hotspot login page. If they do not have a password yet, they can click on the button to get a password.

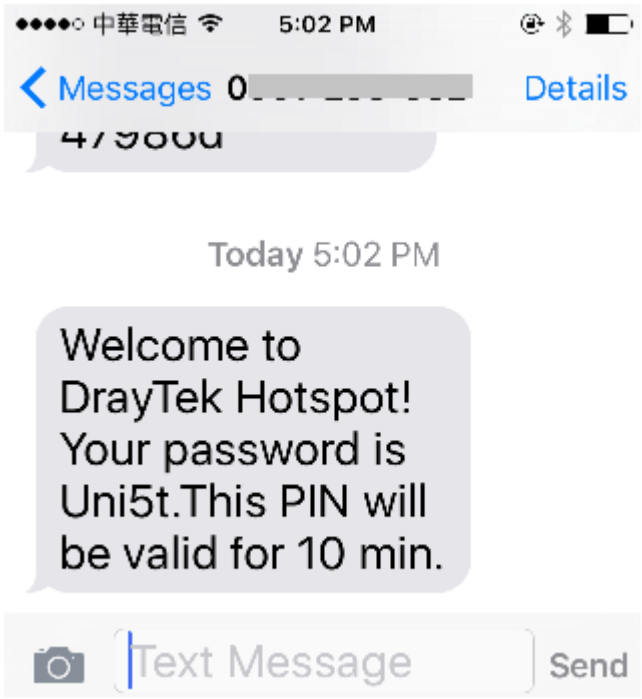
Info

- Due to security concerns, the browser might warns that it cannot verify server identity, the clients would need to tap "continue" before they can proceed to portal.draytek.com.
- The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.

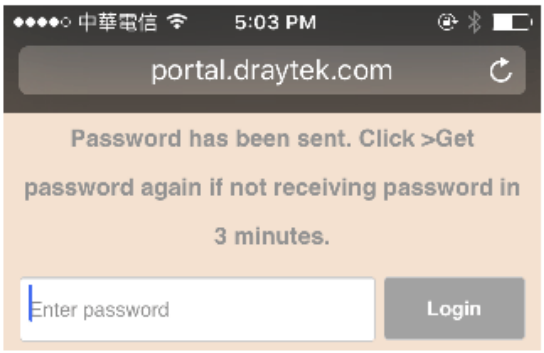
12. Enter the mobile phone number to receive the SMS message.

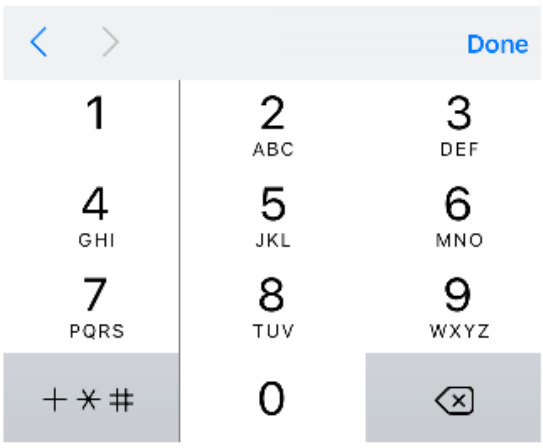


13. The number will get a message about the password.



14. Enter the password on the login page, and click **Login**.





15. If the password is correct, the client will be redirected to the landing page, and after that, they will be able to surf the Internet.

V-5 Central Management (AP)

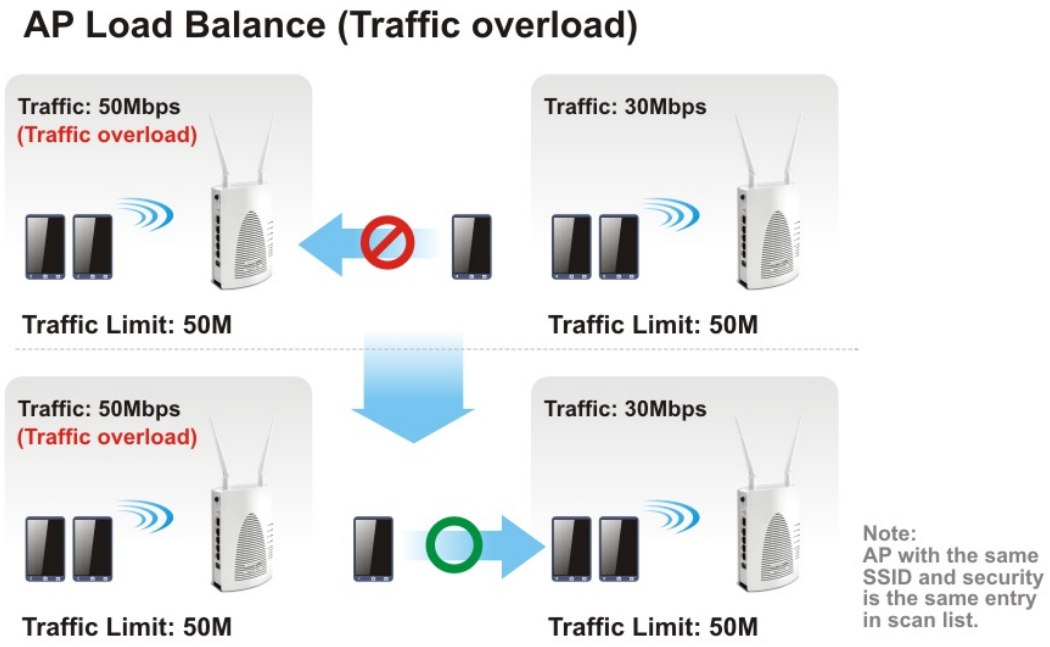
Vigor3910 can manage the access points supporting AP management via Central AP Management.

AP Maintenance

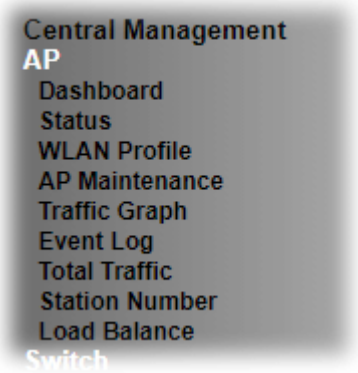
Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

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.

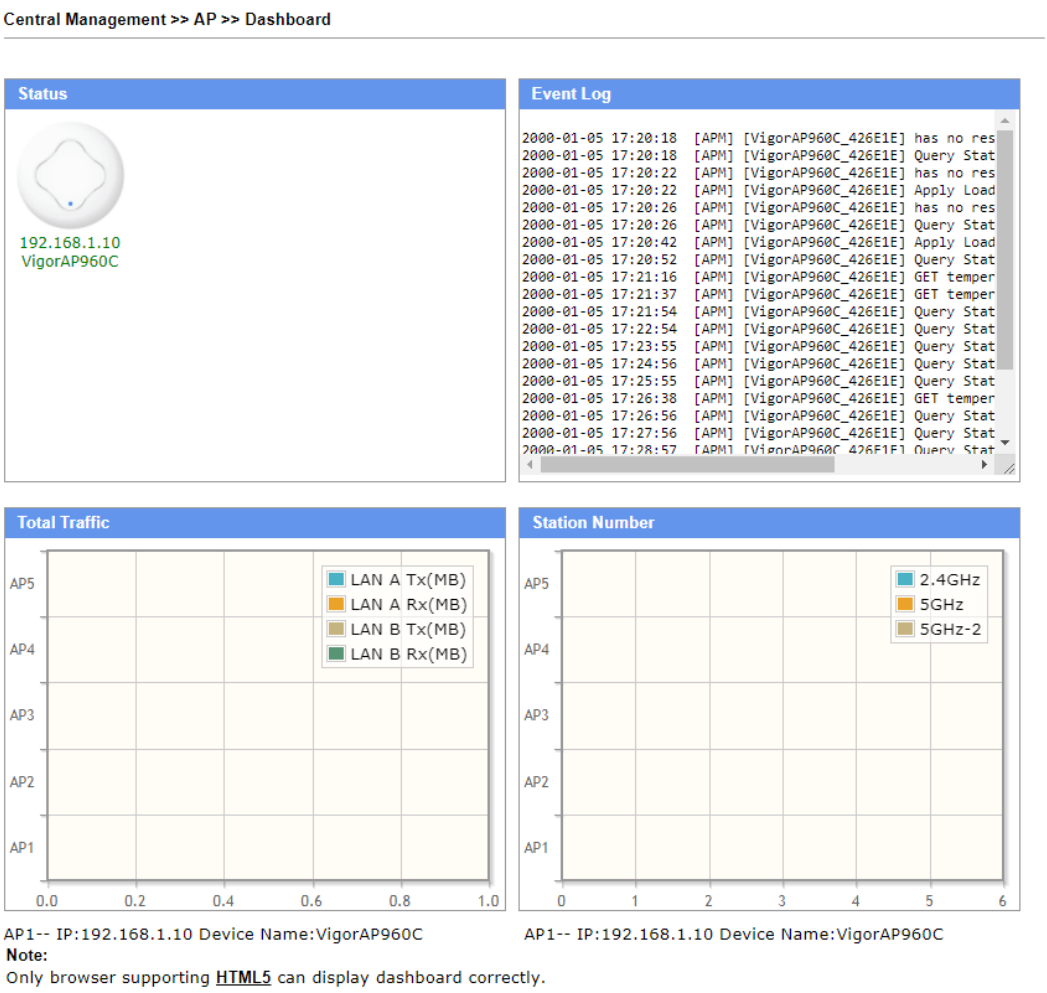


Web User Interface



V-5-1 Dashboard

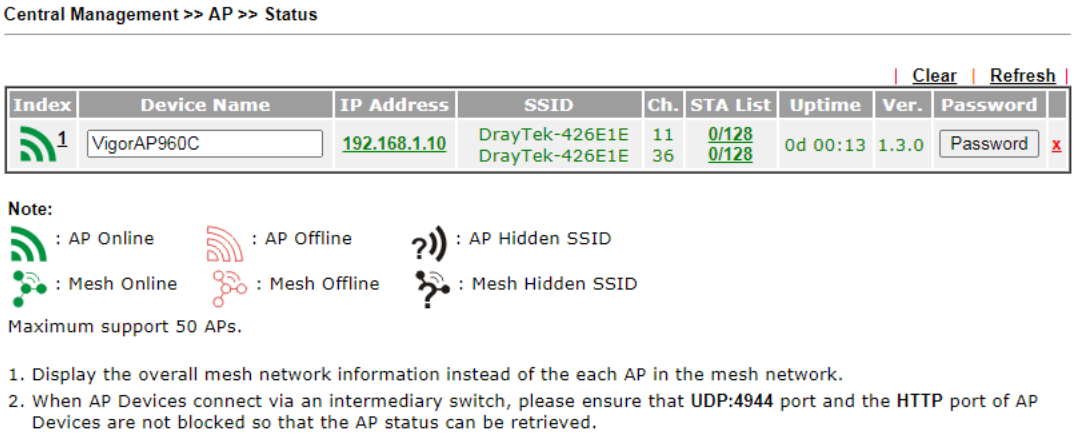
This page shows VigorAP's information about **Status, Event Log, Total Traffic** or **Station Number** by displaying VigorAP icon, text and histogram. Just move and click your mouse cursor on **Status, Event Log, Total Traffic** or **Station Number.** Corresponding web pages will be open immediately.



To access into the web user interface of VigorAP, simply move your mouse cursor on the VigorAP icon and click it. The system will guide you to access into the web user interface of VigorAP.

V-5-2 Status

This page displays current status (online, offline or SSID hidden, IP address, encryption, channel, version, password and etc.) of the access points managed by Vigor router. Please open **Central AP Management>>Function Support List** to check what AP Models are supported.

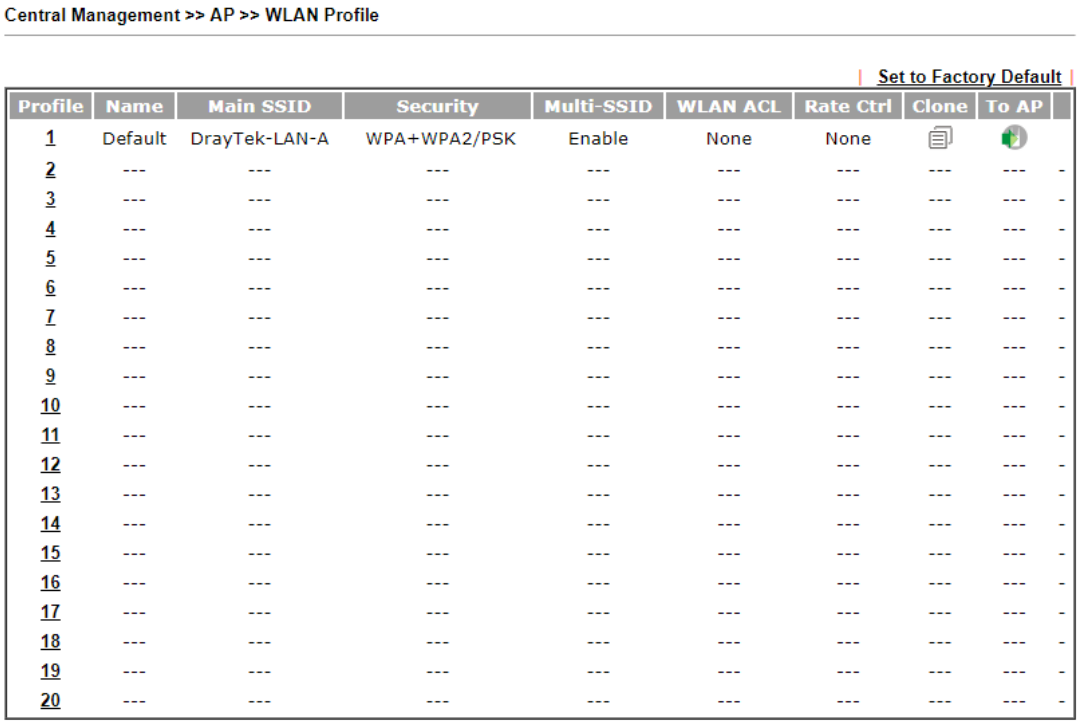


Available settings are explained as follows:

Item	Description
Index	Click the index number link for viewing the settings summary of the access point.
Device Name	The name of the AP managed by Vigor router will be displayed here.
IP Address	Display the true IP address of the access point.
SSID	Display the SSID configured for the access point(s) connected to Vigor2962.
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.
Uptime	Display the duration of the AP powered up.
Version	Display the firmware version used by the access point.
Password	Vigor2962 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.

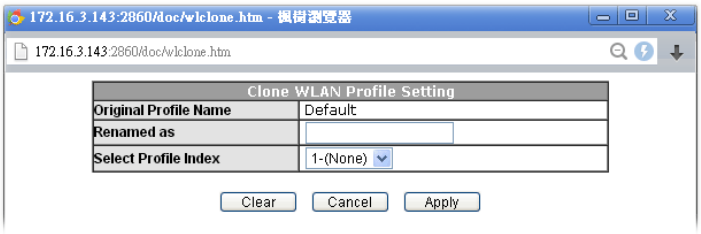
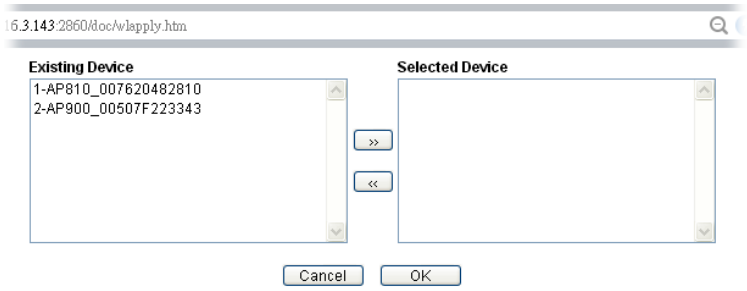
V-5-3 WLAN Profile

WLAN profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.



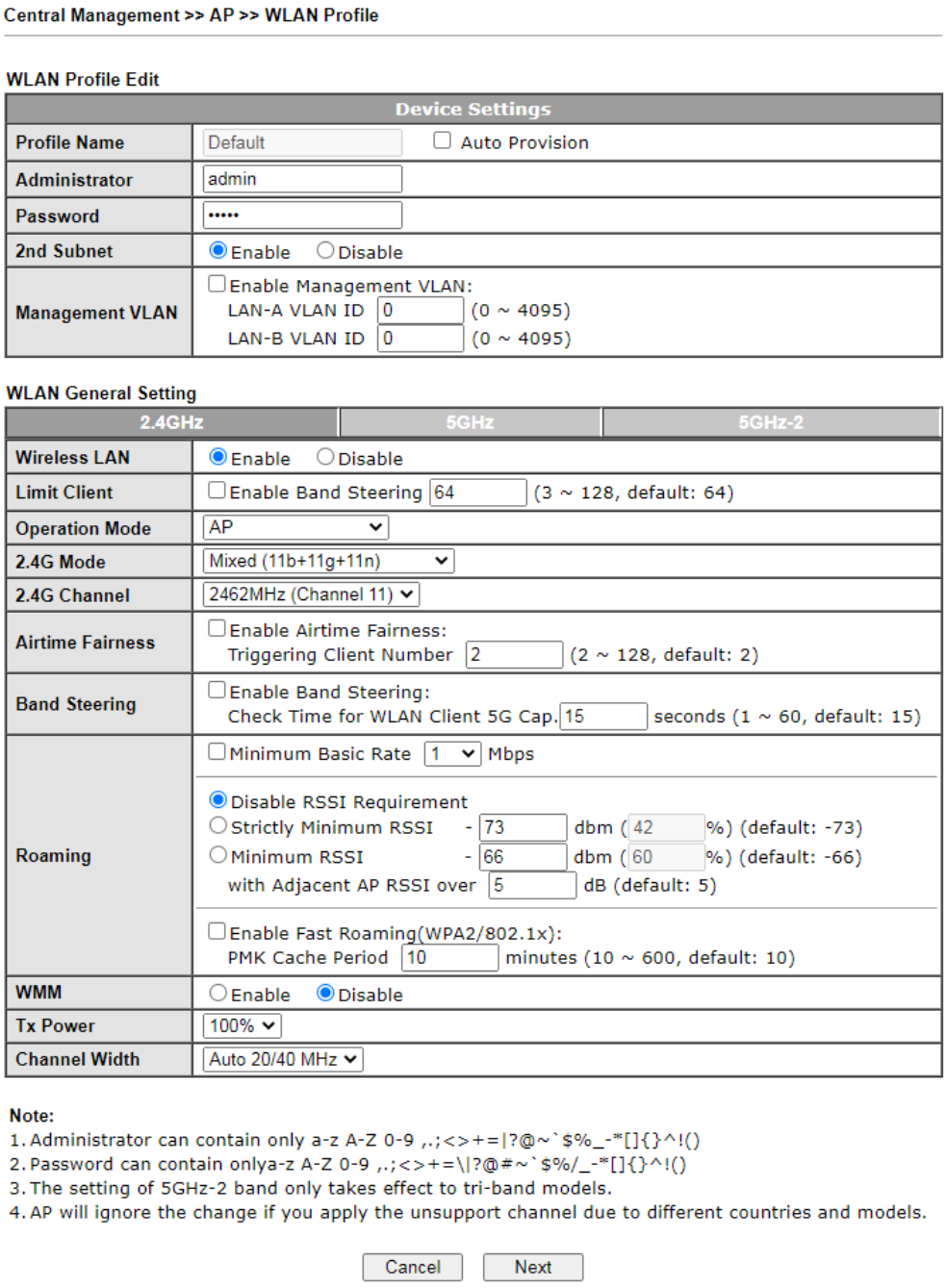
Click the number link of the selected profile to modify the content of the profile. Available settings are explained as follows:

Item	Description
Profile	There are five WLAN profiles offered to be configured. Simply click the index number link to open the modification page.
Name	Display the name of the profile. The default profile cannot be renamed.
Main SSID	Display the SSID configured by such wireless profile.
Security	Display the security mode selected by such wireless profile.
Multi-SSID	Enable means multiple SSIDs (more than one) are active. Disable means only SSID1 is active.
WLAN ACL	Display the name of the access control list.
Rate Ctrl	Display the upload and/or download transmission rate.
Clone	It can copy settings from an existing WLAN profile to another WLAN profile. First, you have to check the box of the existing profile as the original profile. Second, click **Clone**. The following dialog will appear.

	 Third, choose the profile index to accept the settings from the original profile. Forth, type a new name in the field of **Renamed as**. Last, click **Apply** to save the settings on this dialog. The new profile has been created with the settings coming from the original profile.
To AP	Click it to apply the selected wireless profile to the specified Access Point.  Simply choose the device you want from **Existing Device** field. Click **>>** to move the device to **Selected Device** field. Then, click **OK**. The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot.
To Local	WLAN Profile configured in this page is specified for VigorAP connected to Vigor router. If required, these settings also can be applied to Vigor router. Select and check one of wireless profiles and click this button to apply the settings onto the WI-Fi wireless settings configured for such Vigor router.

How to edit the wireless LAN profile?

1. Select the WLAN profile (index number 1 to 5) you want to edit.
2. Click the index number link to display the following page.



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

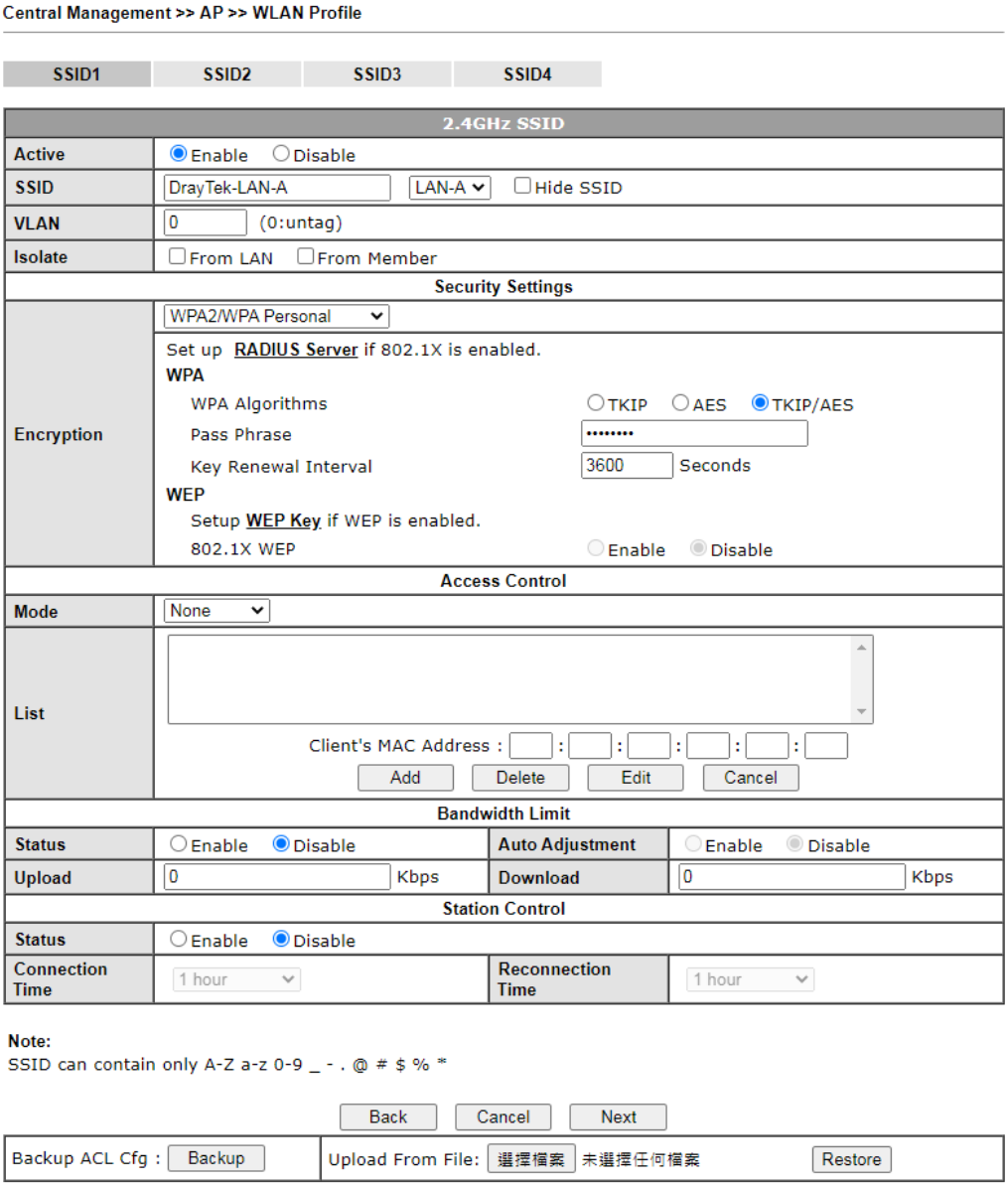
2.4GHz	5GHz	5GHz-2
Wireless LAN	◉ Enable ○ Disable	
Limit Client	☐ Enable Band Steering 64 (3 ~ 128, default: 64)	
Operation Mode	AP	
2.4G Mode	Mixed (11b+11g+11n)	
2.4G Channel	2462MHz (Channel 11)	
Airtime Fairness	☐ Enable Airtime Fairness: Triggering Client Number 2 (2 ~ 128, default: 2)	
Band Steering	☐ 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	

Note:
1. Administrator can contain only a-z A-Z 0-9 ,.;<>+=|?@~`$%_-*[]{}^!()
2. Password can contain onlya-z A-Z 0-9 ,.;<>+=\|?@#~`$%/_-*[]{}^!()
3. The setting of 5GHz-2 band only takes effect to tri-band models.
4. AP will ignore the change if you apply the unsupport channel due to different countries and models.

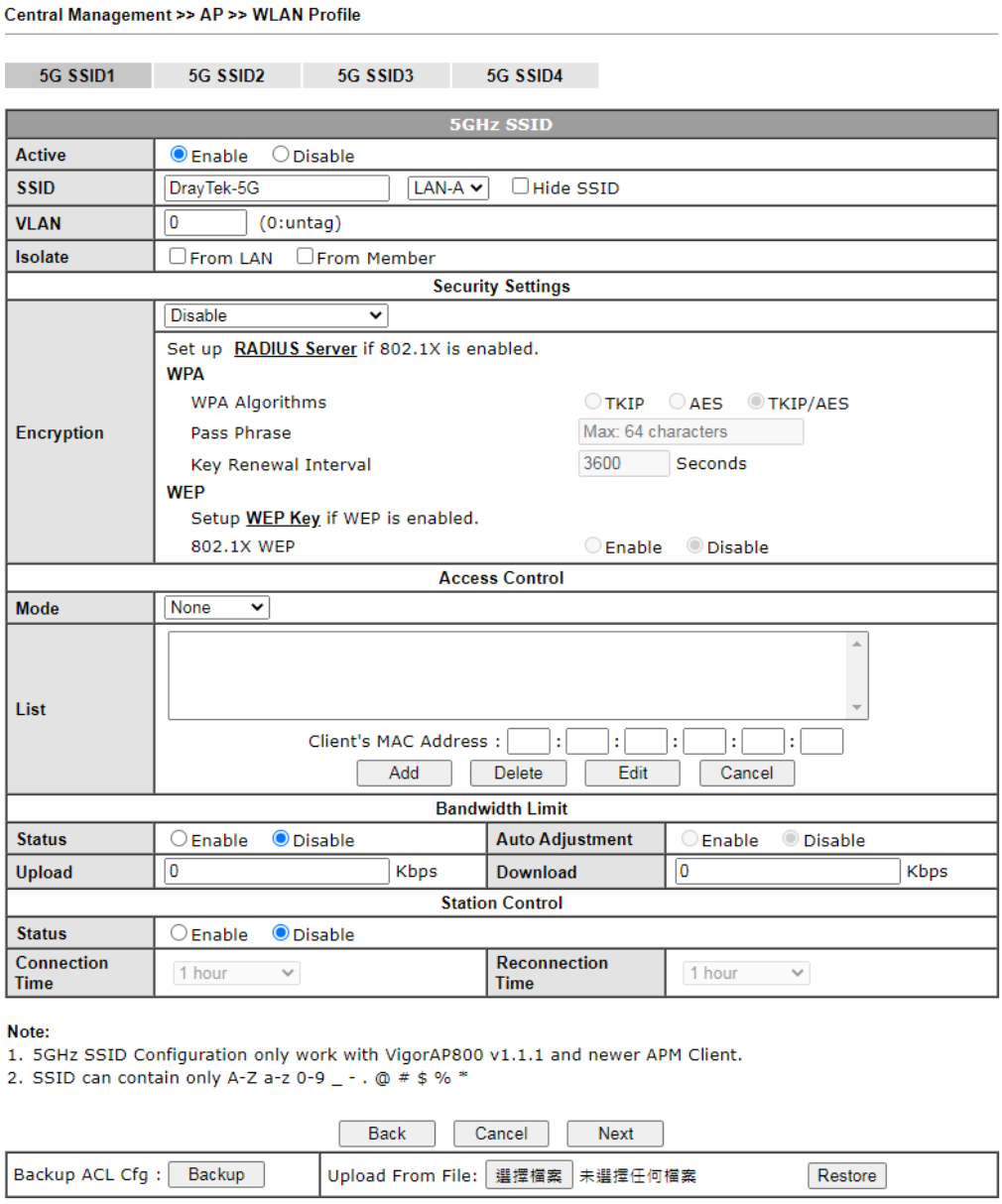
Cancel Next

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

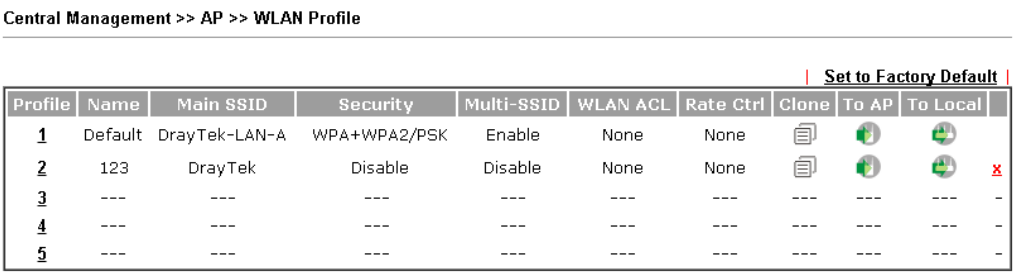
5GHz SSID			
Active	Enable Disable		
SSID	DrayTek-5G LAN-A Hide SSID		
VLAN	0 (0:untag)		
Isolate	From LAN From Member		
Security Settings			
Encryption	Disable Set up RADIUS Server if 802.1X is enabled. WPA WPA Algorithms TKIP AES TKIP/AES Pass Phrase Max: 64 characters Key Renewal Interval 3600 Seconds 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

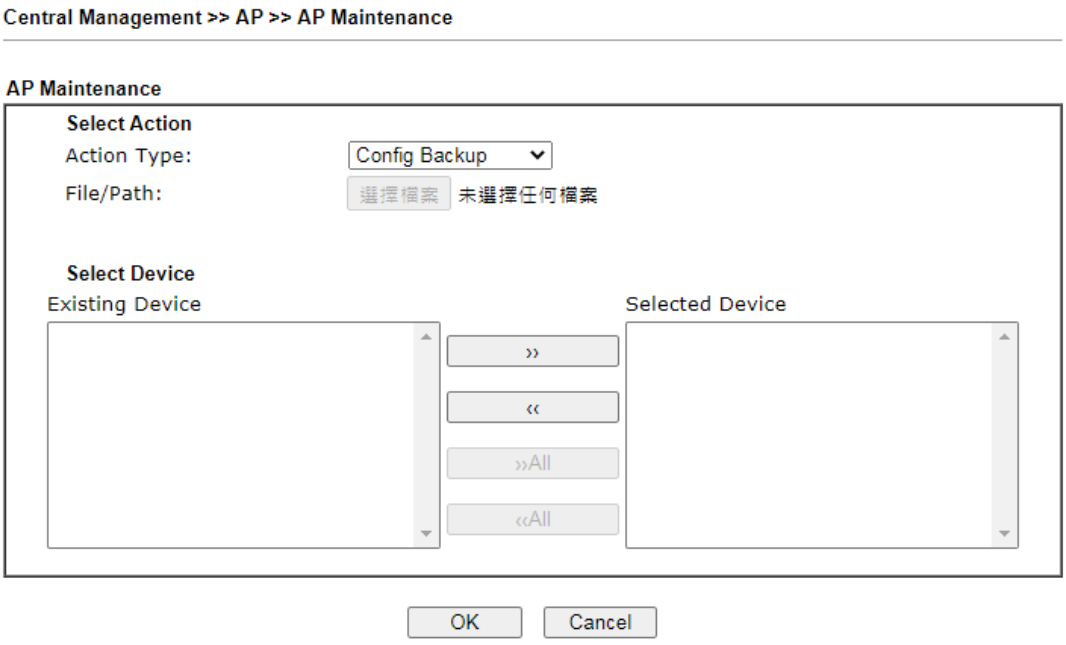
Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local	
1	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None				
2	123	DrayTek	Disable	Disable	None	None				x
3	---	---	---	---	---	---	---	---	---	-
4	---	---	---	---	---	---	---	---	---	-
5	---	---	---	---	---	---	---	---	---	-

V-5-4 AP Maintenance

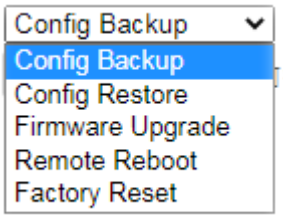
Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

Info

Config Backup can be performed to one AP at one time. Others functions (e.g., Config Restore, Firmware Upgrade, Remote Reboot can be performed to more than one AP at one time by using Vigor2962.



Available settings are explained as follows:

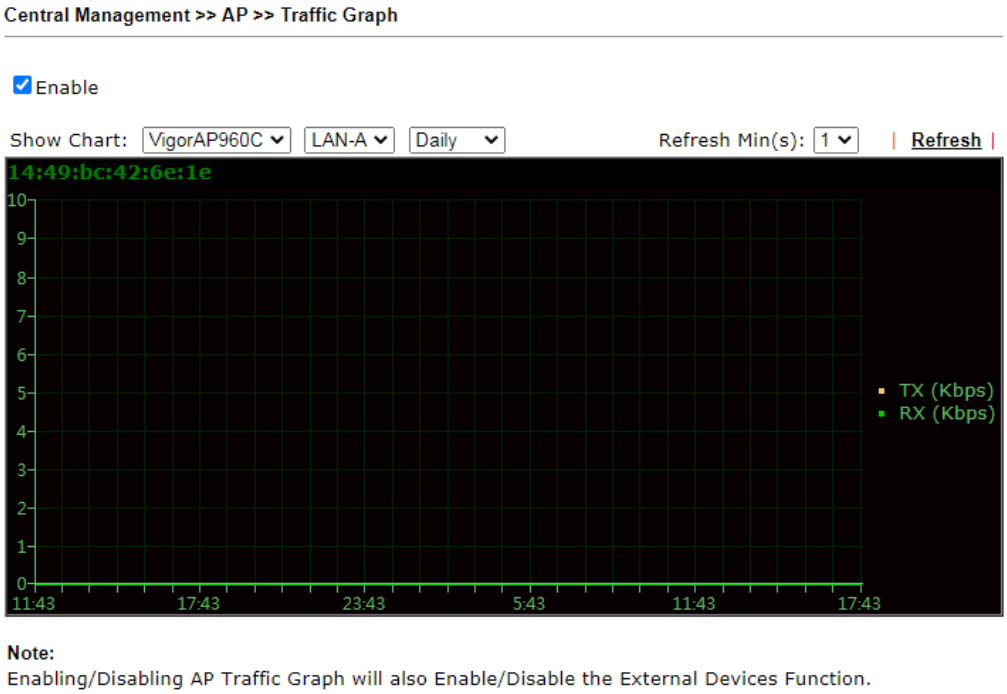
Item	Description
Action	There are four actions provided by Vigor router to manage the access points.  Vigor router can **backup** the configuration of the selected AP, **restore** the configuration for the selected AP, perform the **firmware upgrade** of the selected AP, **reboot** the selected AP remotely 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.

V-5-5 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.

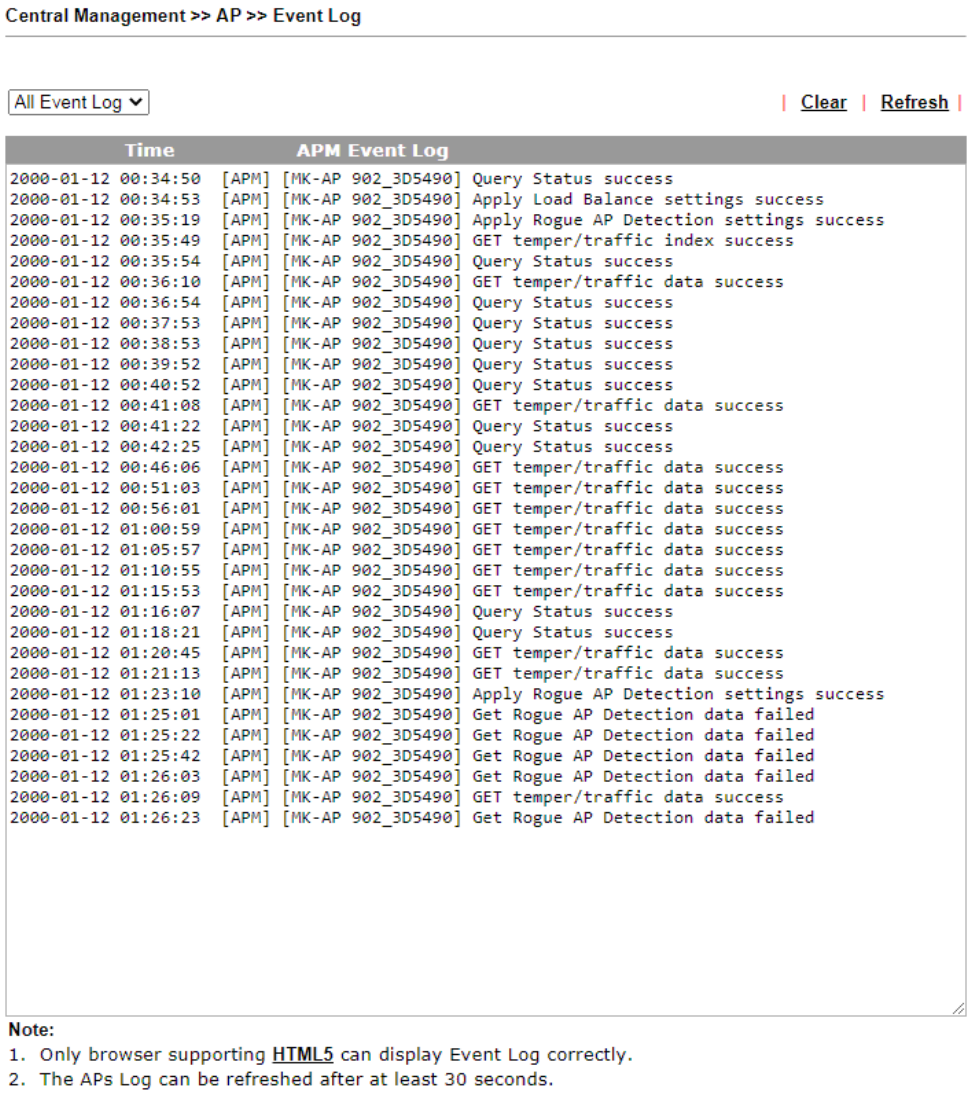


The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).

Info	Enabling/Disabling such function will also enable/disable the External Devices function.

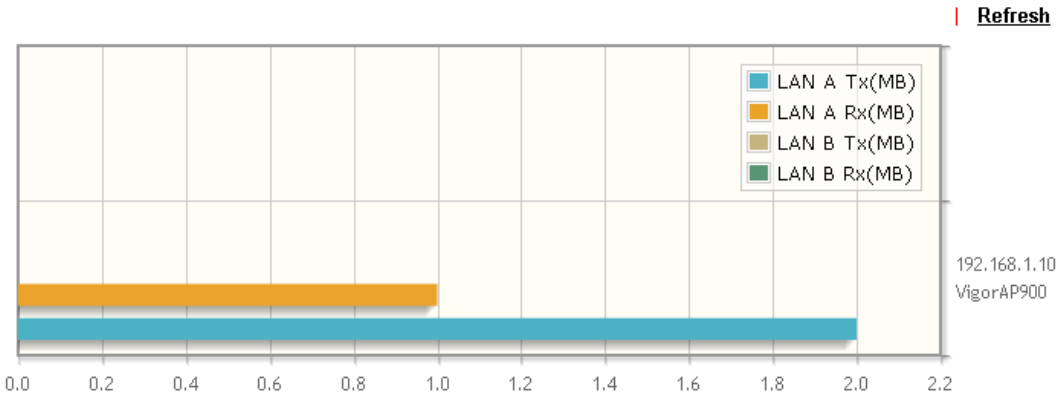
V-5-6 Event Log

Time and event log for all of the APs managed by Vigor router will be shown on this page. It is userful for troubleshooting if required.



V-5-7 Total Traffic

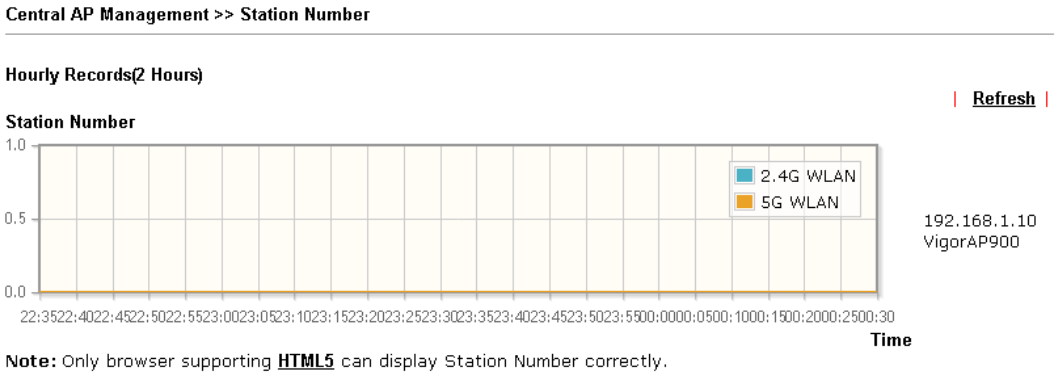
Such page will display the total traffic of data receiving and data transmitting for VigorAPs managed by Vigor router.



Note: Only browser supporting **HTML5** can display Total Traffic correctly.

V-5-8 Station Number

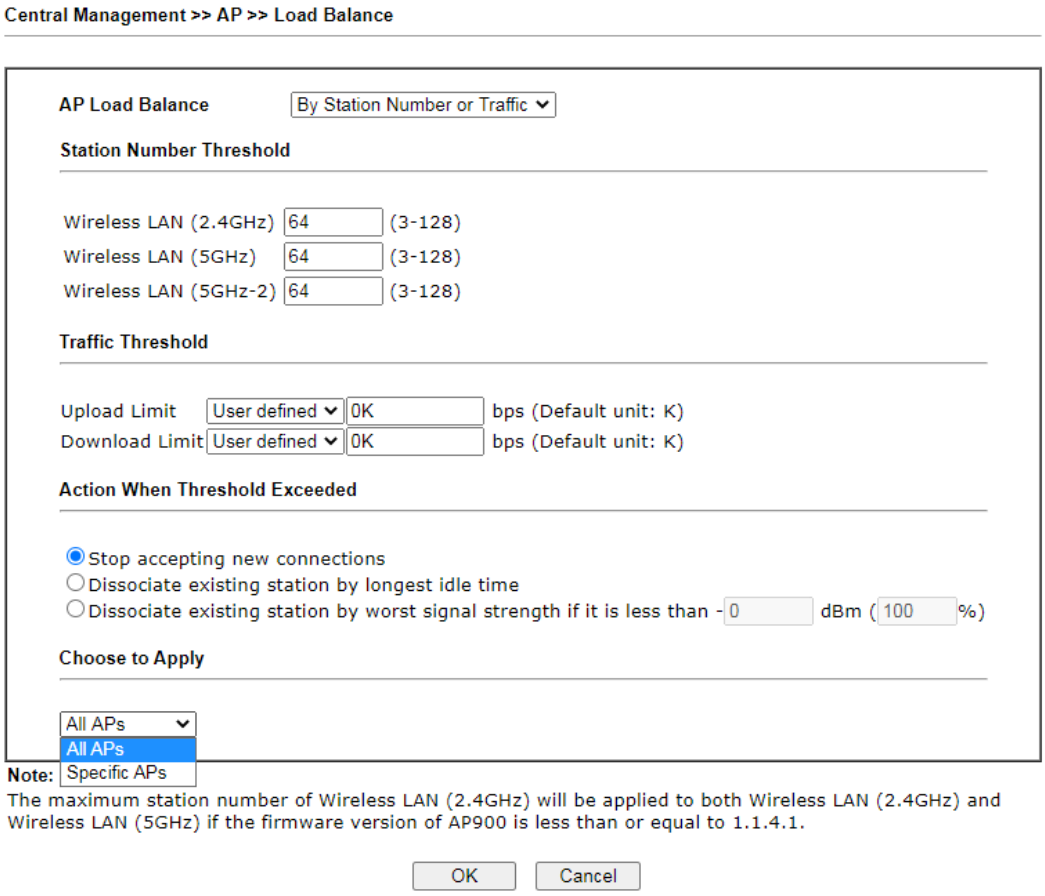
The total number of the wireless clients will be shown on this page, no matter what mode of wireless connection (2.4G WLAN or 5G WLAN) used by wireless clients to access into Internet through VigorAP.



Note: Only browser supporting **HTML5** can display Station Number correctly.

V-5-9 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:

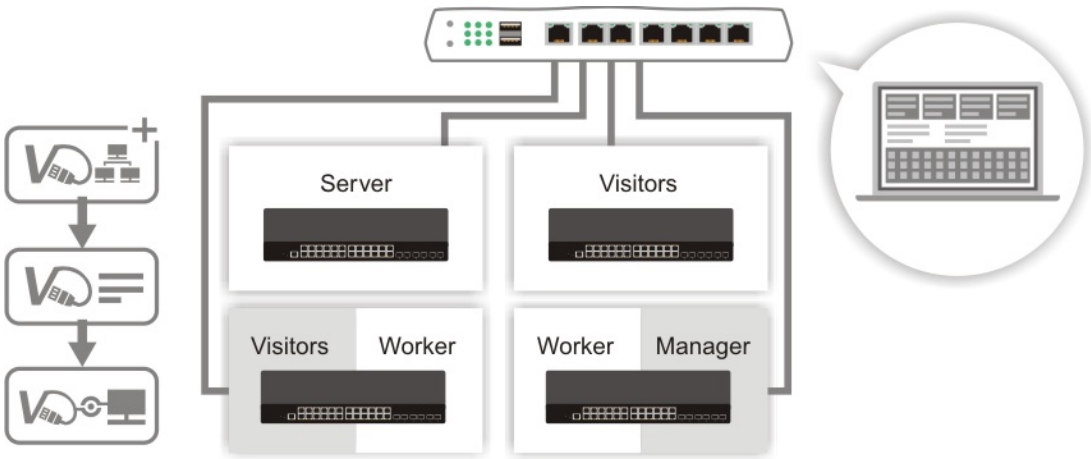
Item	Description
AP Load Balance	It is used to determine the operation mode when the system detects overload between access points. **Disable** – Disable the function of AP load balance. **By Station Number** –The operation of load balance will be executed based on the station number configured in this 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.

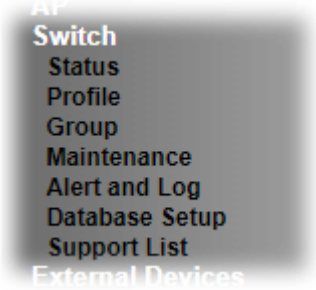
After finishing all the settings here, please click **OK** to save the configuration.

V-6 Central Management (Switch)

Vigor router can manage lots of VigorSwitch devices connected to it. Through profile and group settings, the administrator can execute firmware/configuration backup, restore for VigorSwitch device, reboot the device or return to factory default settings of VigorSwitch at one time.



Web User Interface

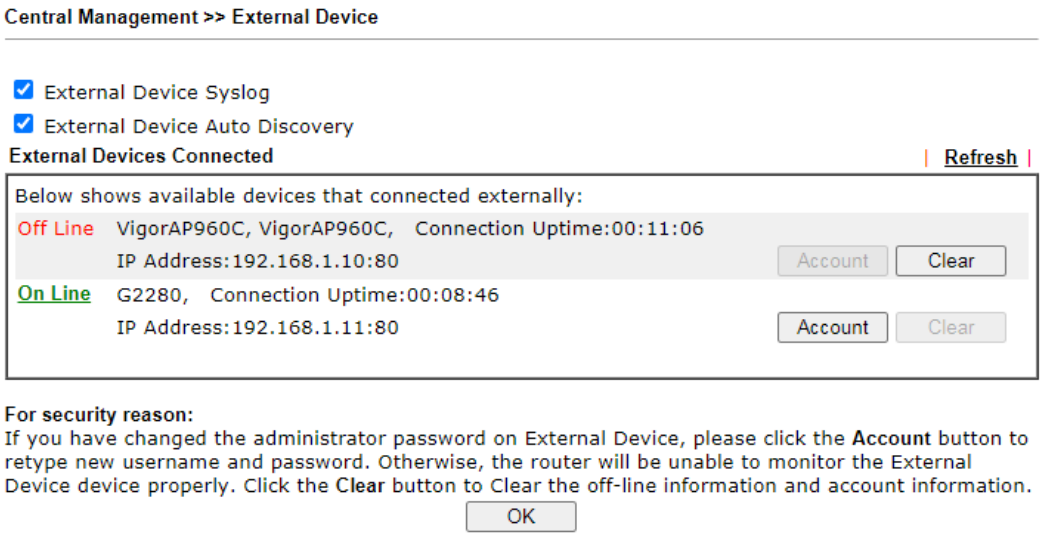


V-6-1 Status

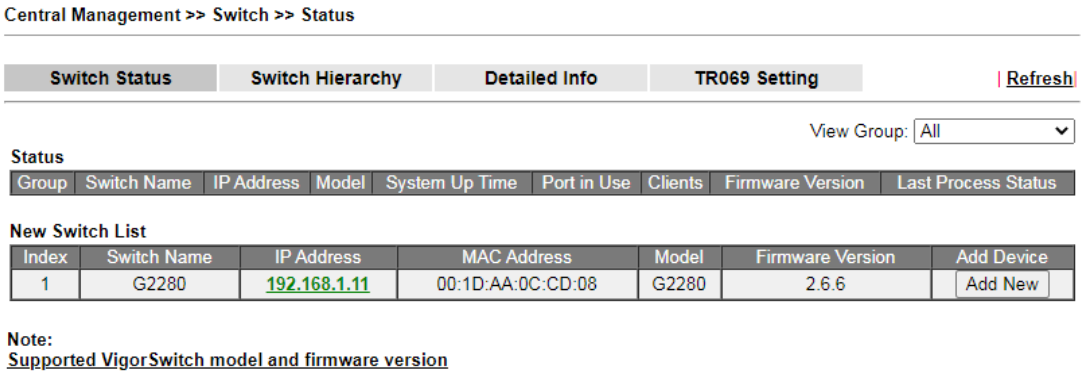
V-6-1-1 Switch Status

Such page displays information, including Group, Switch name, IP address, model, System Up Time, Port in Use, Clients, and Firmware Version of VigorSwitch **connected to** Vigor2962 series.

Before checking the switch status, go to **Central Management>>External Device** to enable **External Device Auto Discovery**. Wait for the system to display available device(s).



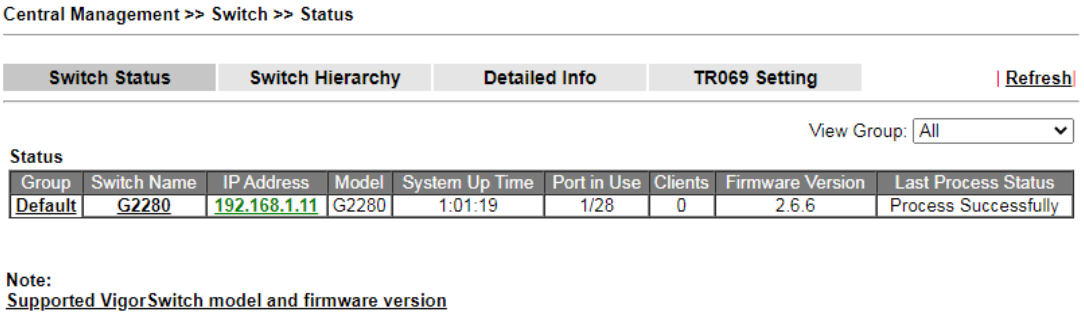
Later, open **Central Management>>Switch>>Status**. Available VigorSwitch to be managed by such router will be listed under the New Switch List.



Info

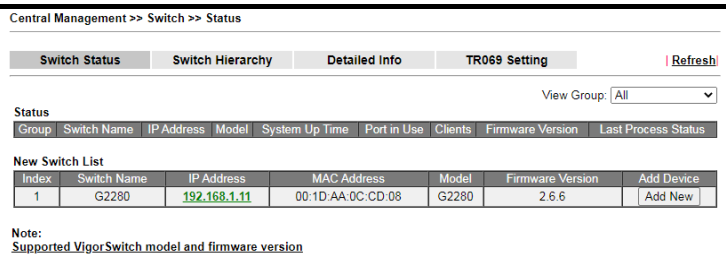
VigorSwitch listed below Status means the switch is managed by Vigor3910; VigorSwitch listed below New Switch List means it is not managed by Vigor3910 yet.

Click **Add** to make the selected VigorSwitch to be managed by Vigor router.



Available settings are explained as follows:

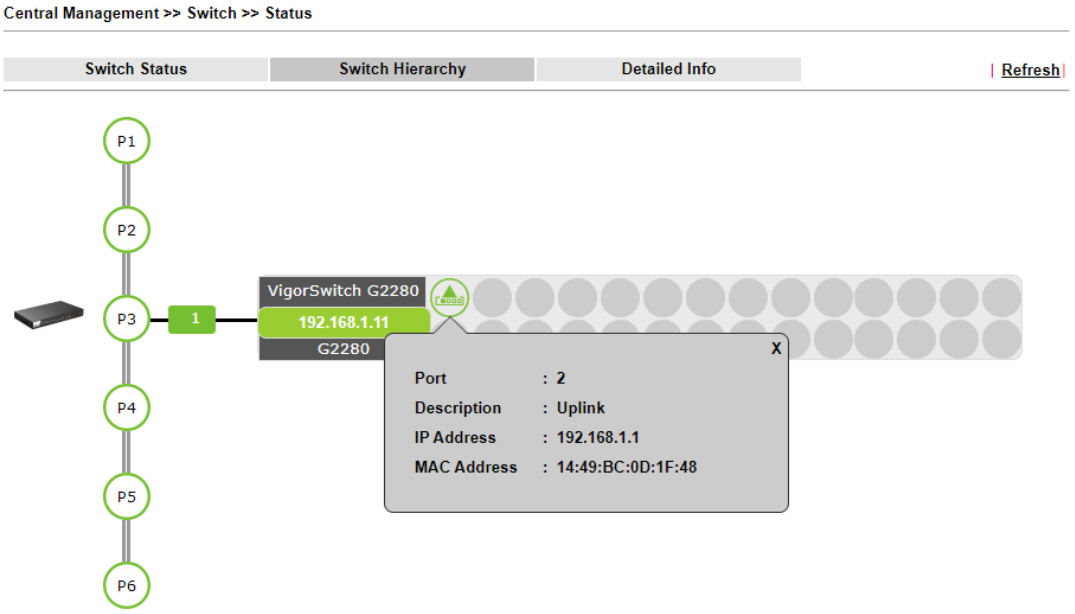
Item	Description
Group	Display the name link of the group. You can click the link to modify the group settings if required.
Switch Name	Display the name link of VigorSwitch. You can click the name link to access into the switch profile.
IP Address	Display the IP address of VigorSwitch.
Model	Display the model name of VigorSwitch.
System Up Time	Display the time accumulated since this Vigorwitch is powered up.
Port in Use	Display how many devices connected to VigorSwitch.
Clients	Display the number of LAN ports used in VigorSwitch.
Firmware Version	Display the firmware version that VigorSwitch current used.
Add	Such button will appear only when there is more than one switch connected to Vigor3910. The one under New Switch List is allowed to be managed under current used group. Simply click **Add**.

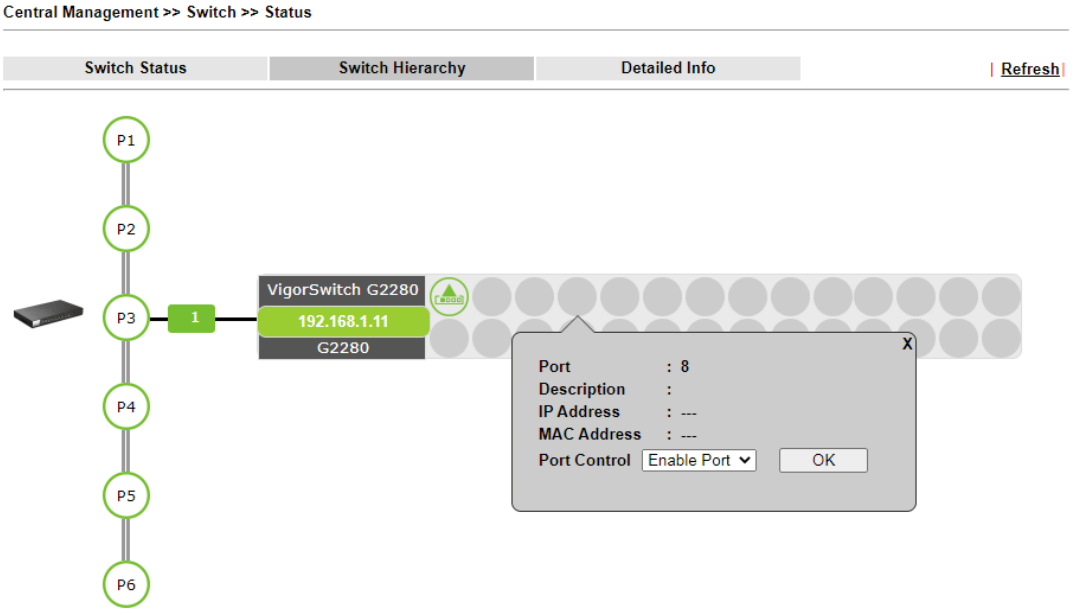


It will be better to group VigorSwitch devices with the same model.

V-6-1-2 Switch Hierarchy

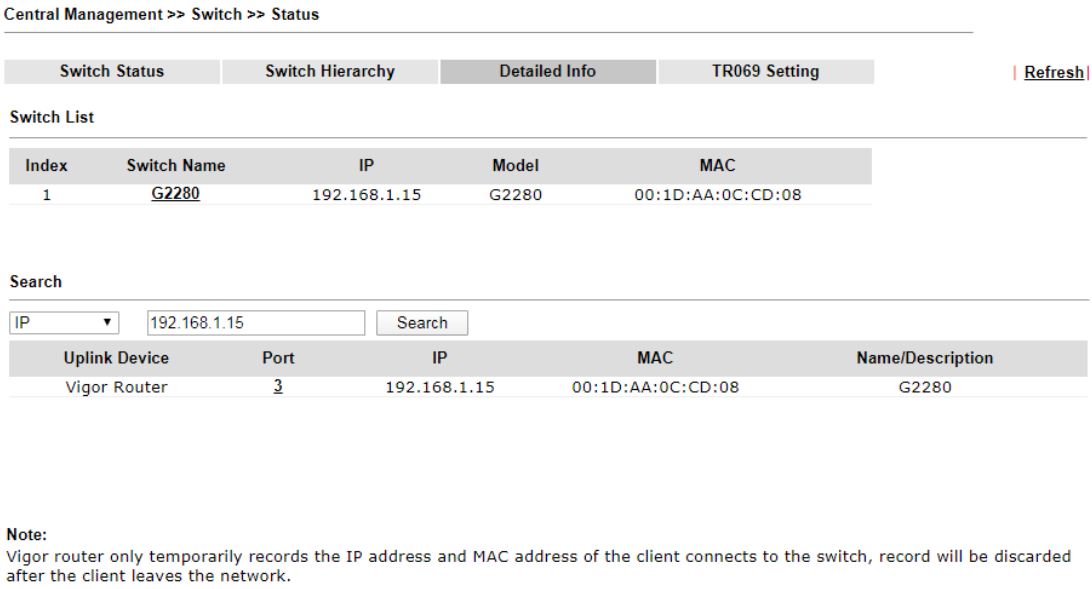
This page displays the hierarchy of VigorSwitch(es) managed under Vigor2962.





V-6-1-3 Detailed Info

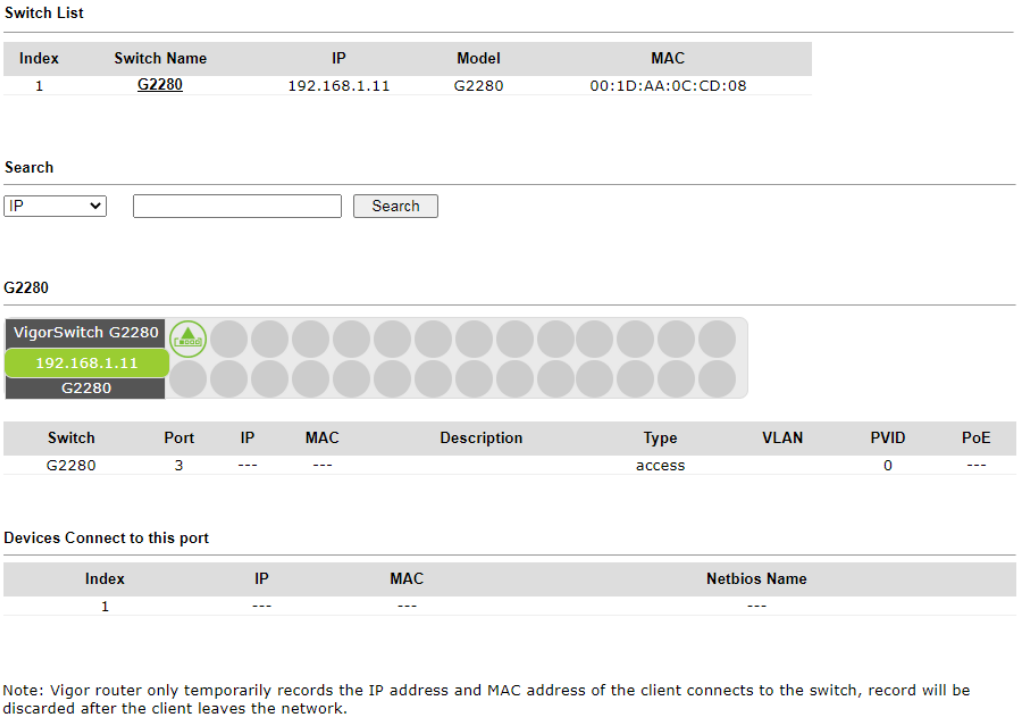
This page displays the hierarchy of VigorSwitch(es) managed under Vigor3910.



Available settings are explained as follows:

Item	Description
Switch List	Displays the index number, switch name, IP address, model name and MAC address of the VigorSwitch device. **Switch Name** - The name link allows you to access into the web user interface of the Vigor Switch. **IP** - Displays the IP address of the switch. **Model** - Displays the model name of the switch. **MAC** - Displays the MAC address of the switch.
Search	**Search** - After specifying IP address, MAC address or name of the switch, click the Search button to find out the device and display the searching result on this page. **Uplink Device** - Displays the name of the server that Vigor switch connects to. **Port** - Indicates the port where the switch is connected to the router. This number link allows you to click to view more detailed information of the searched device.

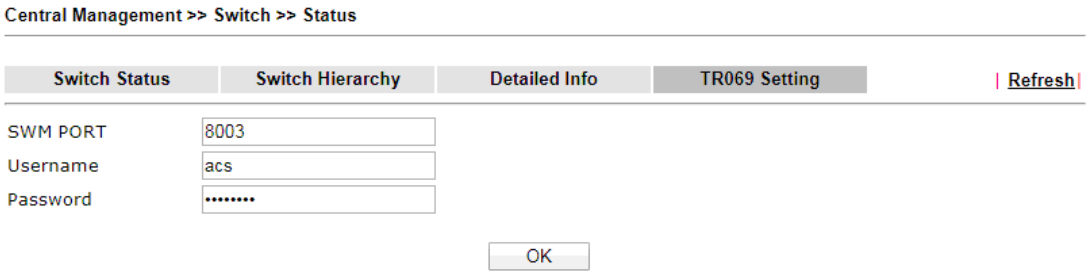
Click the port number link (e.g., 3) to open the following page. Detailed information of the name, port number, IP address, MAC address, description, type, VLAN number, PVID value and PoE capability of the switch will be shown on this page.



In addition, this page will display the basic information (IP address, MAC address and Netbios Name) of "other" devices connected to this switch.

V-6-1-4 TR069 Setting

In addition to HTTP/HTTPS, the Vigor router is able to manage the VigorSwitch with the protocol of TR-069.

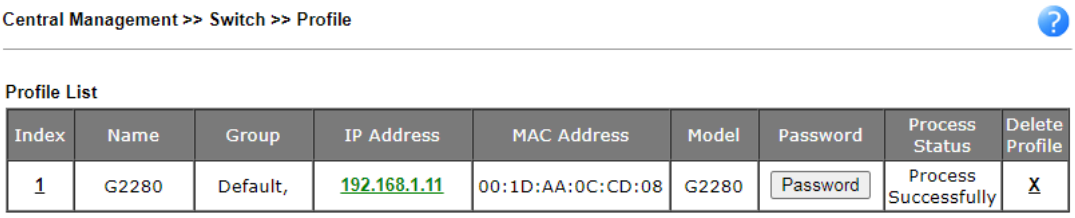


Available settings are explained as follows:

Item	Description
SWM Port	The default value is 8003. In the event of port conflicts, change the port number.
Username	Displays the username that the Vigor switch will use to connect to this router. Keep the default value.
Password	Displays the password that the Vigor switch will use to connect to this router. Keep the default value.

V-6-2 Profile

This page will show general information, such as name, group, IP address, MAC address, model and password of VigorSwitch only when it connects to Vigor2962 series. By clicking the index number link, a profile setting page for that switch will be shown. Note that each profile represents one VigorSwitch.

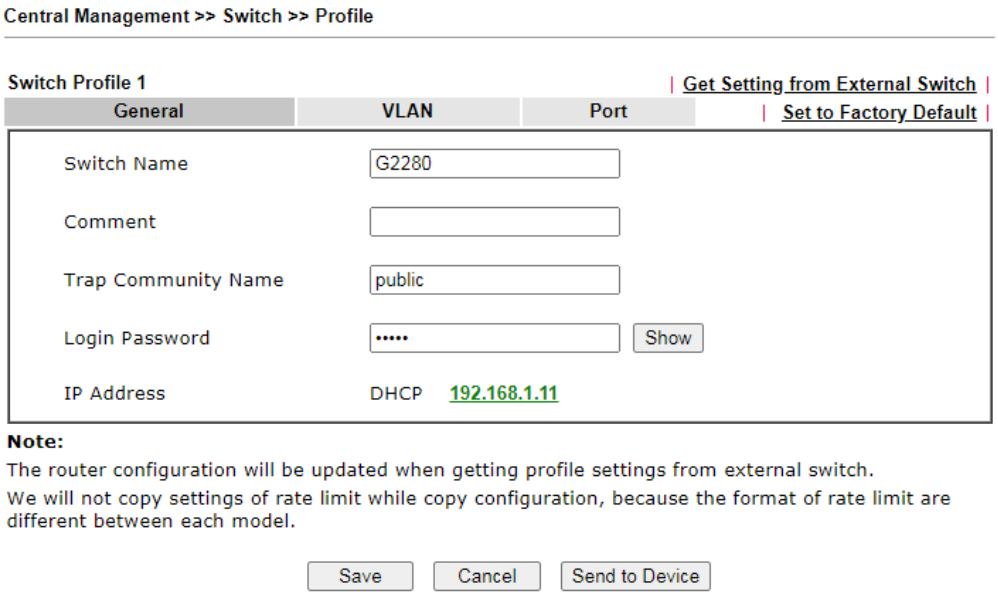


Available settings are explained as follows:

Item	Description
Index	Click the number link to access into the switch profile. Note: Each connected VigorSwitch will have one setting profile. If there are many switches connected to Vigor3910, different index number will be used to represent different VigorSwitch.
Name	Display the user defined name of VigorSwitch.
Group	Display the group name of VigorSwitch(es).
IP Address	Display the IP address of VigorSwitch.
MAC Address	Display the MAC address of VigorSwitch.
Model	Display the model name of VigorSwitch.
Password	Click it to display the account information including username and password.
Delete Profile	Click the mark of “X” to delete the switch profile.

To edit profile for the selected switch:

1. Click index number link (e.g. #1) to open the following page.

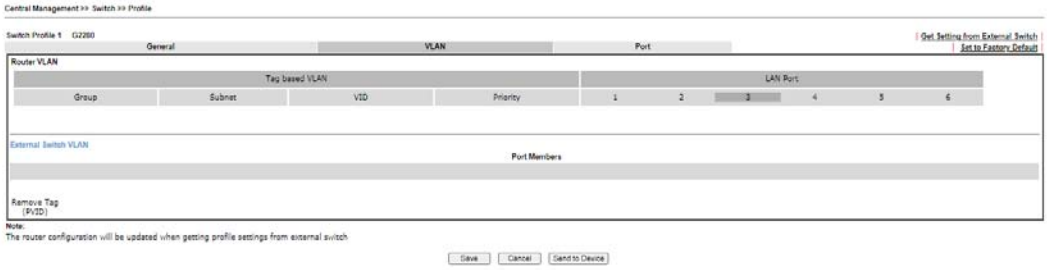


Available settings are explained as follows:

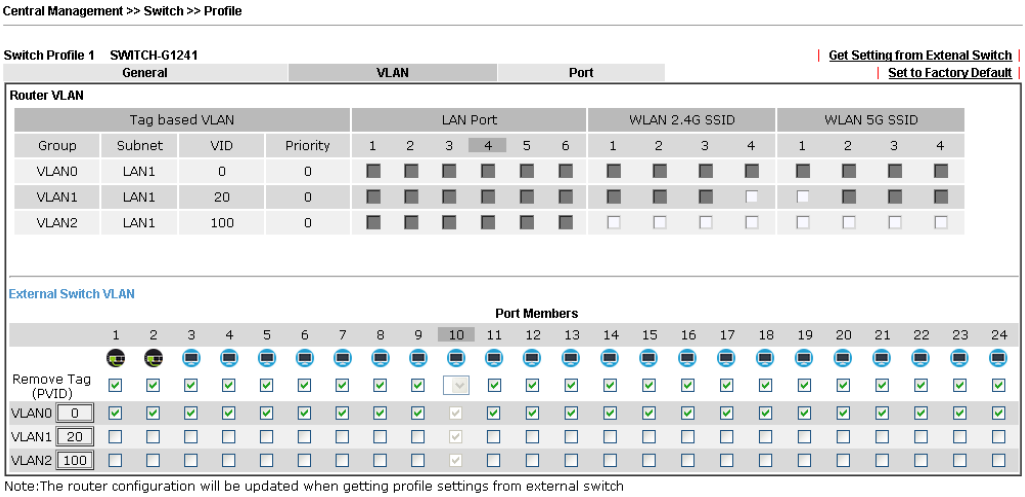
Item	Description
Switch Name	Type a name for the Switch. The purpose of name is used for identification. It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor3910 seres.
Comment	Enter the text in such field if additional explanation for the switch is required.
Trap Community Name	Enter the text in such field as trap community.
Login Password	Display the original login password for the VigorSwitch. However, if Group Password (in **Central Management >>Switch>>Group**) is configured with other string, then such field is not allowed to type any other password. And only the group password will be shown, instead.
IP Address	Display the dynamic IP address (of the connected switch) assigned by Vigor3910.
Save	Click it to save the settings.
Cancel	Click it to return to previous web page without saving the setting changes.
Send to Device	Click it to transfer the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately.

2. After finished the settings, click **VLAN** tab to open following page.

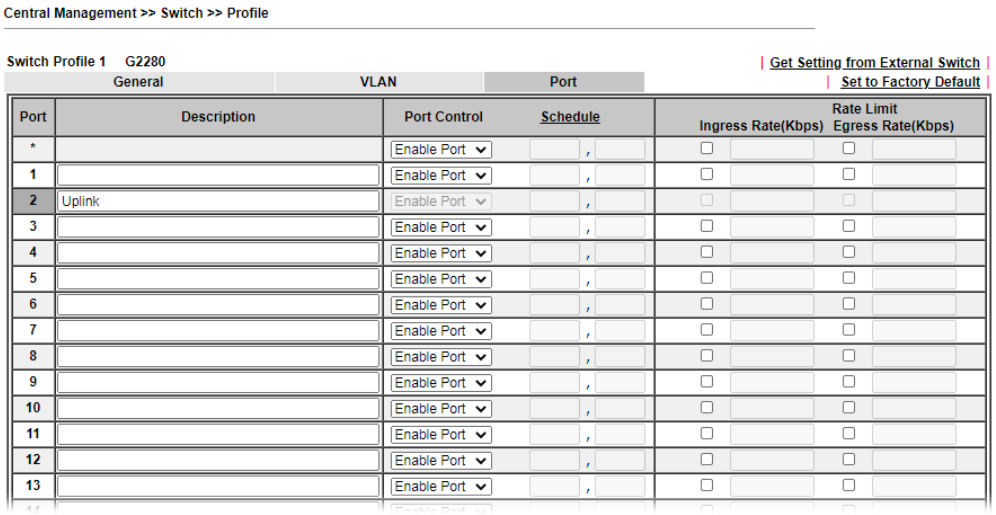
   Blank page due to LAN>>VLAN not configured previously:



Setting page with **LAN>>VLAN** configured previously:



3. Click **Save** to save VLAN configuration. Then, click **Port** tab to access the following page:

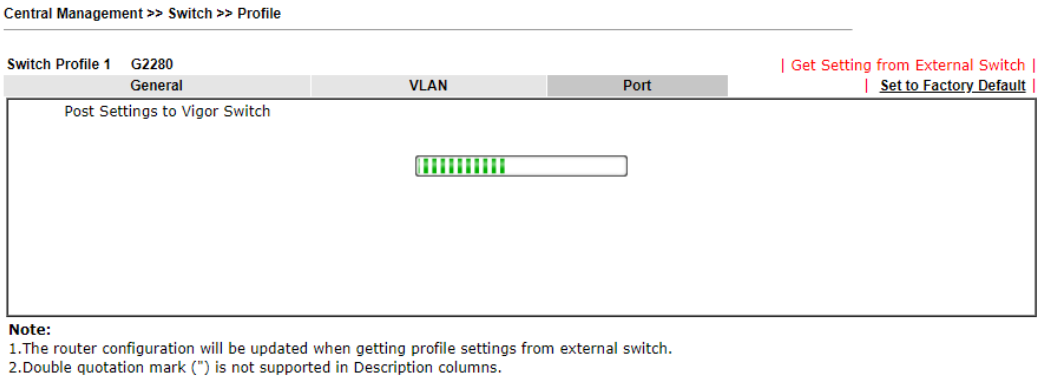


Available settings are explained as follows:

Item	Description
Description	If required, type a brief description to explain the device connected to VigorSwitch via the LAN port.
Port Control	**Disable Port** – The port (e.g, Port 2 in this case) which is used to connect VigorSwitch and Vigor3910 will not be shutdown by Vigor3910. Other LAN ports of VigorSwitch allow to connect to any LAN device. When it is checked, after clicking Save, the network connection between that device and VigorSwitch will be terminated.

	By Schedule – Two sechule profiles can be specified here to force Vigor3910 executing specific action to VigorSwitch.
Rate Limit	Check the box for typing the ingress rate / egress rate for the selected VigorSwitch. After clicking **Save**, the value modified in this page will be written to VigorSwitch and enabled.

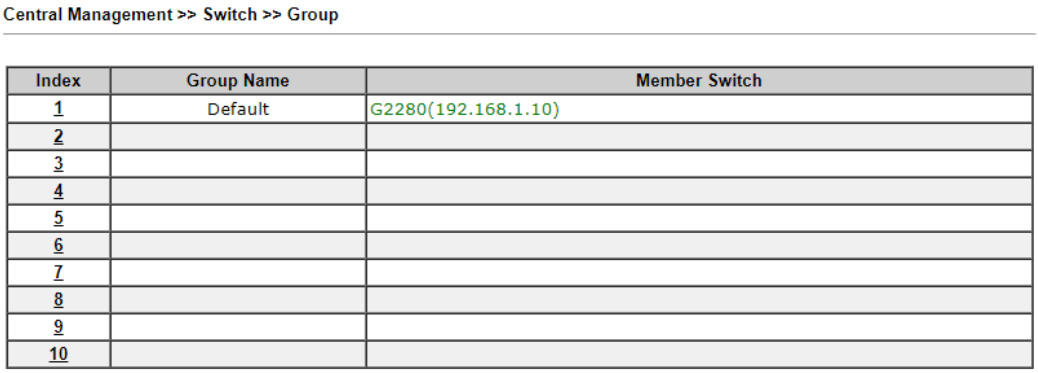
4. Click **Save** to save the changes and then click **Send to Device**. Settings will be sent to VigorSwitch immediately.



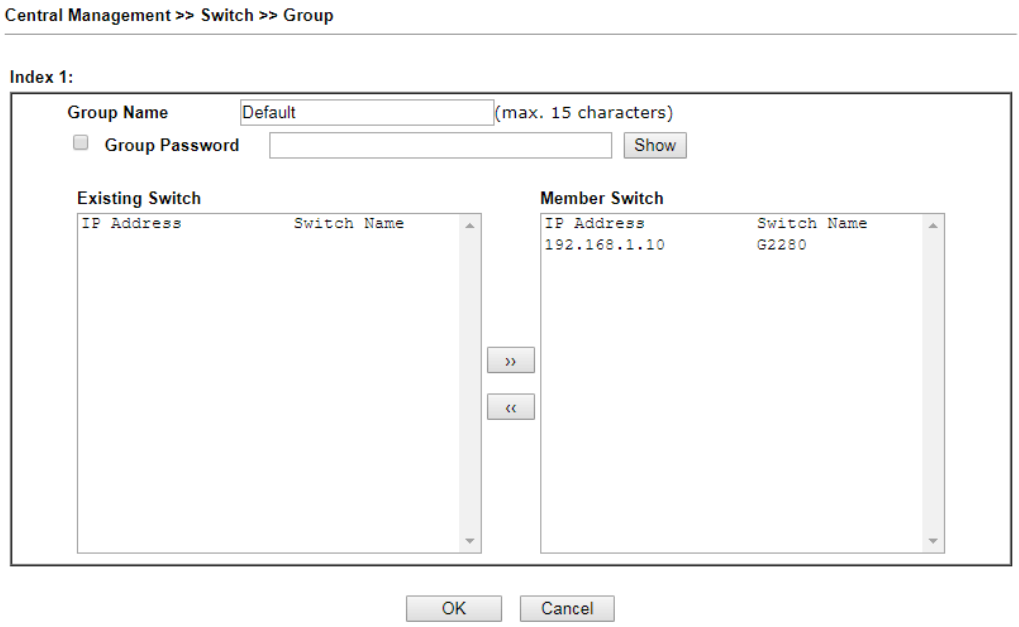
V-6-3 Group

Different switches can be classified into different group(s). Specifc password for a group can be defined and applied to every switch uder that group.

Through the common password setting, it is not necessary for the system administrator to remember various login passwords to access into different VigorSwitch devices.



Click any index number link to create a new switch group.

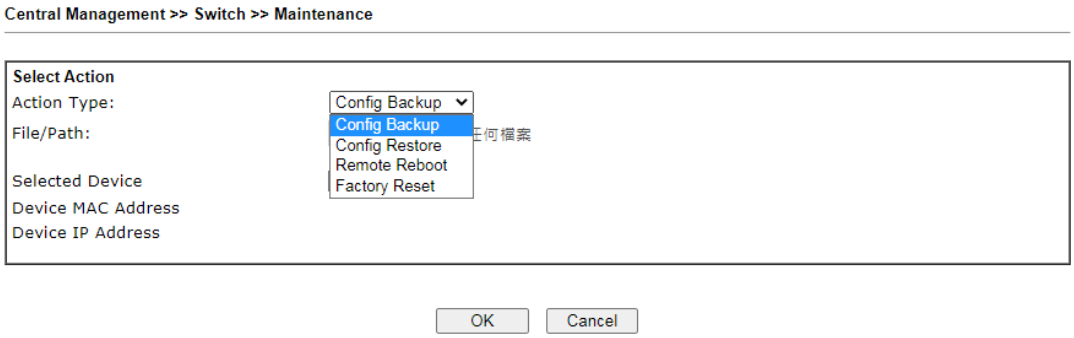


Available settings are explained as follows:

Item	Description
Group Name	Type a name as the group name. Different switches can be classified within a group.
Group Password	Type a password that administrator can use to access into the managed VigorSwitch connecting to Vigor3910. All of the switches under the same group can be accessed into via such group password.
Existing Switch	Display all of the VigorSwitch devices connecting to Vigor3910.
Member Switch	Choose the switches you want to group and click the button “>>” to move the selected devices onto the field of Member Switch. Devices under Member Switch will be grouped under such group profile.
OK	Click it to save the configuration.
Cancel	Click it to exit the setting page without saving any change.

V-6-4 Maintenance

Such feature can execute configuration backup, restore of selected VigorSwitch device(s) or reboot the VigorSwitch devices remotely or reset the VigorSwitch devices with factory default settings, without accessing into the web user interface of VigorSwitch respectively. It is convenient for system administrator to manage VigorSwitch devices.



Available settings are explained as follows:

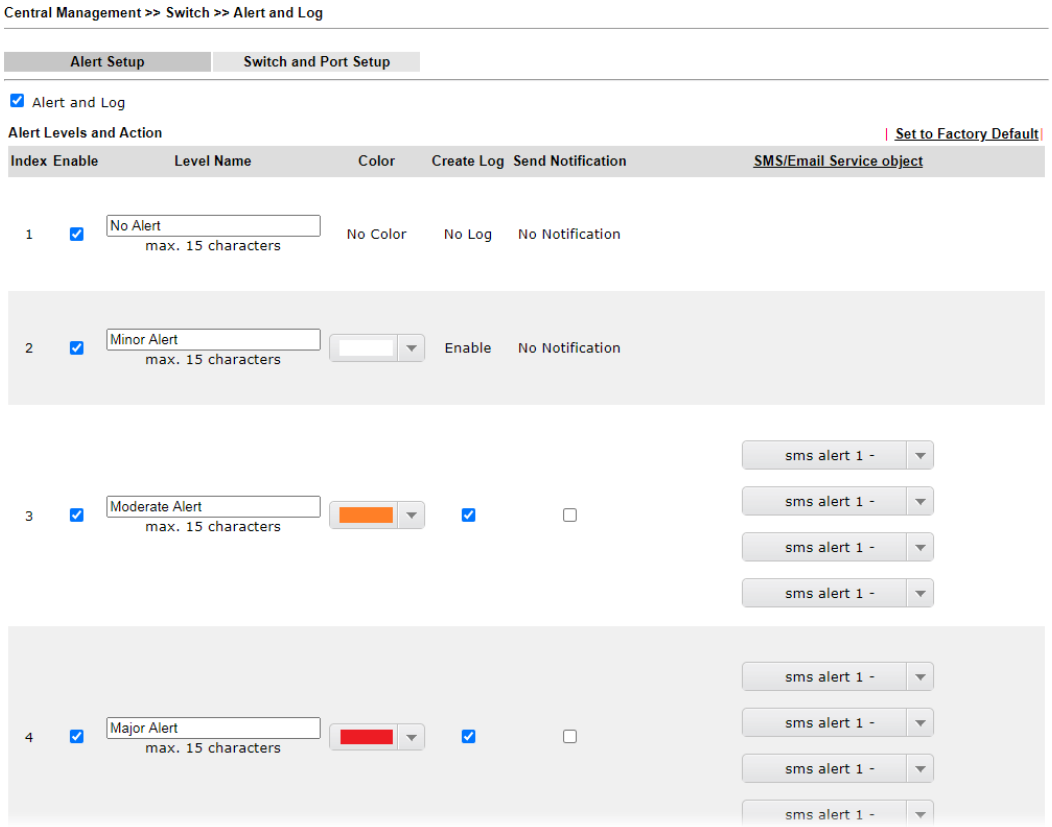
Item	Description
Select Action	**Action Type** – Four actions including configuration backup, configuration restore, remote reboot and factory reset are offered by Vigor3910 to perform on VigorSwitch. **File/Path** – Click the button to find out the required file.
Selected Device	Use the drop down list to specify a VigorSwitch. Then the MAC address and IP address related to the device will be displayed on this area.
OK	Click it to immediately perform the action (configuration backup, configuration restore, remote reboot and factory reset) on the device(s) listed in Selected Device.
Cancel	Click it to cancel the setting changes.

V-6-5 Alert and Log

Alert and Log is helpful for the user to understand the abnormal situation occurred in VigorSwitch quickly. When the system detects an error, information of abnormal condition will be recorded to the database; or the system will send an alert to the specified device (via e-mail or SMS) to warn the user.

V-6-5-1 Alert Setup

This page is used to define the name of alert, level of alert (in color), and determine to record the data in the database, or send a notification message to the user based on the level.



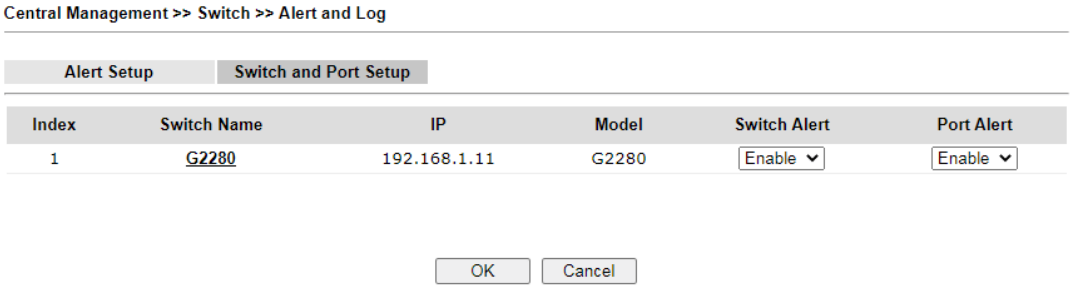
Available settings are explained as follows:

Item	Description
Alert and Log	Check it to enable this feature.
Alert Levels and Action	**Level Name –** Define names for representing the severity of alert event. The default names for index 1 to index 4 will be shown on each setting box. Index 5 to index 8 are reserved for user-defined. **Color** – Define the color for each level of alert. However, the color of index 1 is No color and unable to be changed. **Create Log** – Check the box to create log of alert. Such log will be seen on Alert Logs page. Note that No Log for index 1; and log for index 2 is enabled in default. **Send Notification** – If it is checked, Vigor router's system will send notification to specified phone number via SMS. **SMS/Email Service Object –** Choose the SMS object which

	will get the SMS from Vigor router. Up to 4 objects can be selected at one time.

V-6-5-2 Switch and Port Setup

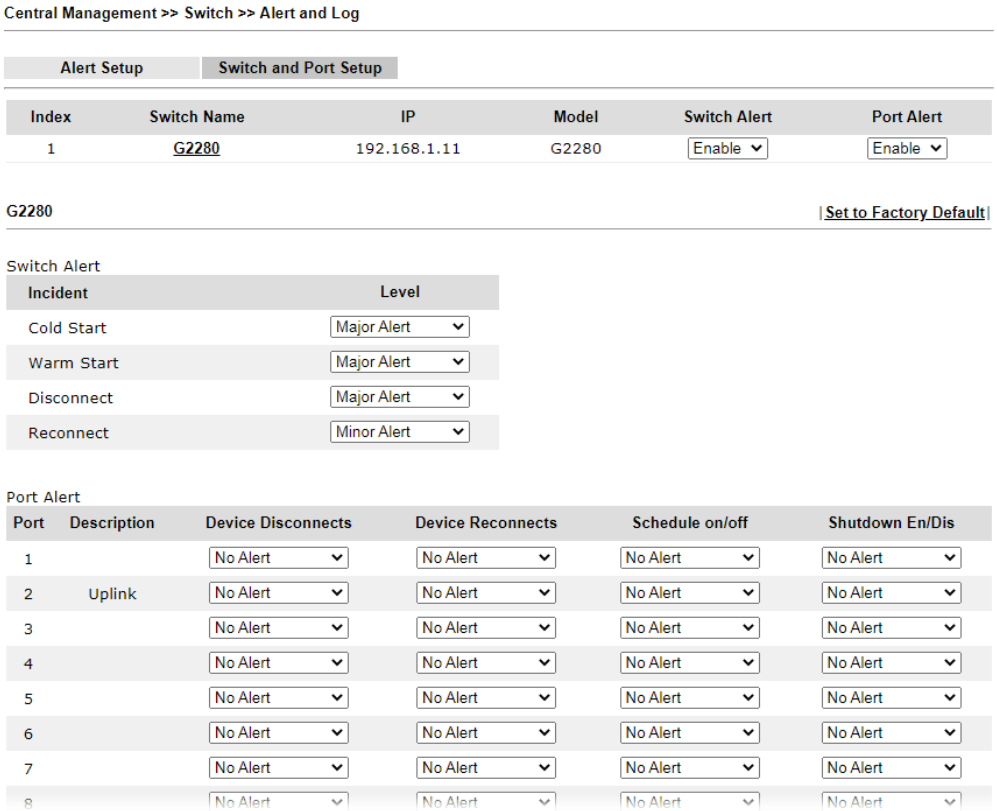
This page defines enabling switch alert and/or port alert for each switch.



Available settings are explained as follows:

Item	Description
Switch Alert	**Enable -** Check it to enable alert mechanism for VigorSwitch.
Port Alert	**Enable -** Check it to enable alert mechanism for each port of VigorSwitch.

Click the Switch Name link (e.g., G2280 in this case) to get detailed settings.



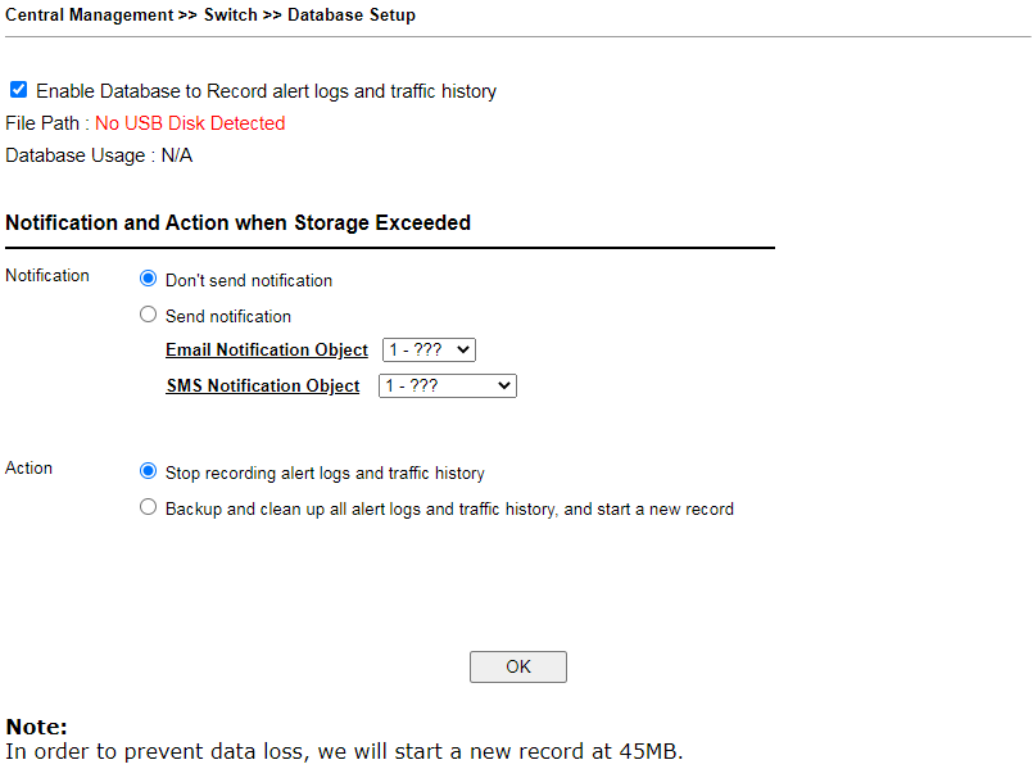
Available settings are explained as follows:

Item	Description
Switch Alert	When VigorSwitch encounters the following alert events, alert mechanism will perform corresponding actions based

	on the servity level of the incident encountererd. **Incident –** At present, **Cold Start, Warm Start, Disconnect** and **Reconnect** will be treated as alert events. **Level –** Specify the severity level for each incident. To defined more severity level for choosing in this page, simply open **Central Management>>Switch>>Alert and Log** and click **Alert Setup**.
Port Alert	**Port –** Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this page. Each port can be confgiured with different alert level for different alert event.

V-6-6 Database Setup

The database of switch can be used to record alert logs and traffic history. This page is used to determine if it is necessary for the user information to be recorded in the database of switch.



Note:
In order to prevent data loss, we will start a new record at 45MB.

Available settings are explained as follows:

Item	Description
Enable Database to Record alert logs and traffic history	Check the box to make the database (in USB disk) to record the alert logs and traffic history.
Notification and Action when Storage Exceeded	
Notification	**Don't send notification** – No notification will be sent out when there is no capacity for storage in USB. **Send notification** – A notification will be sent out when there is no capacity for storage in USB.
Action	**Stop recording user information** – When the capacity of log is full, the system will stop recording. **Backup and clean up all user infor, and start a new record** - Only the newest events will be recorded by the system.

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

V-6-7 Support List

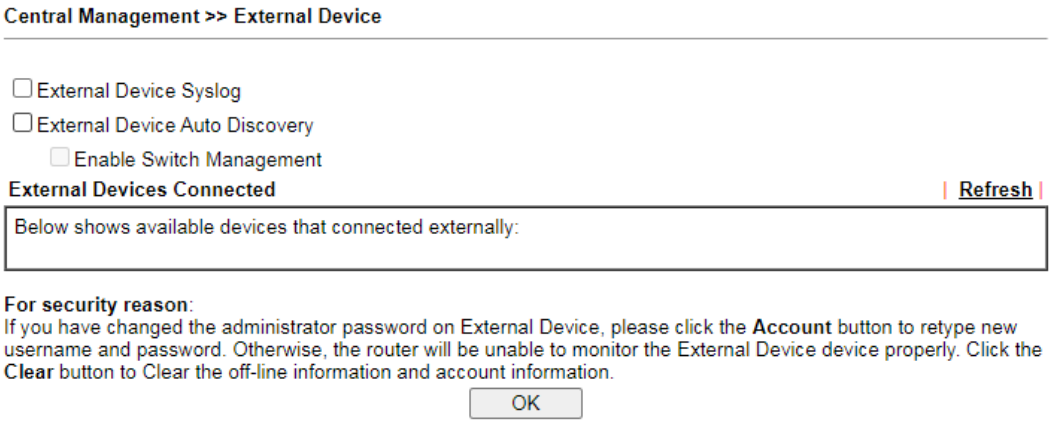
This page lists all models of VigorSwitch which can be managed by Vigor3910 via **Central Management>>Switch**.

Central Management >> Switch >> Support List

Model	Status	Firmware Version
Vigor Switch P2261	V	v3.48
Vigor Switch G2260	V	v3.48
Vigor Switch P1280	V	2.2.1
Vigor Switch G1280	V	2.2.1
Vigor Switch P2280	V	2.2.1
Vigor Switch G2280	V	2.2.1
Vigor Switch P2121	V	2.3.2
Vigor Switch G2121	V	2.4.3
Vigor Switch P1092	V	1.04.05
Vigor Switch G1080	V	1.04.05
Vigor Switch P2500	V	2.4.1
Vigor Switch G2500	V	2.4.1
Vigor Switch P2280x	V	2.4.2
Vigor Switch G2280x	V	2.4.2
Vigor Switch P1085	V	2.4.3
Vigor Switch G1085	V	2.4.3
Vigor Switch P2540x	V	2.6.0
Vigor Switch P2540xh	V	2.6.0
Vigor Switch G2540x	V	2.6.0
Vigor Switch P2100	V	2.6.4
Vigor Switch G2100	V	2.6.4
Vigor Switch PQ2200xb	V	2.6.9
Vigor Switch Q2200x	V	2.6.9
Vigor Switch FX2120	V	2.6.9
Vigor Switch P1282	V	2.6.9
Vigor Switch G1282	V	2.6.9
Vigor Switch PQ2121xb	V	2.8.1
Vigor Switch PQ2121x	V	2.8.1
Vigor Switch Q2121x	V	2.7.1
Vigor Switch G2540xs	V	3.7.0
Vigor Switch P2540xs	V	3.7.0

V-7 Central Management (External Devices)

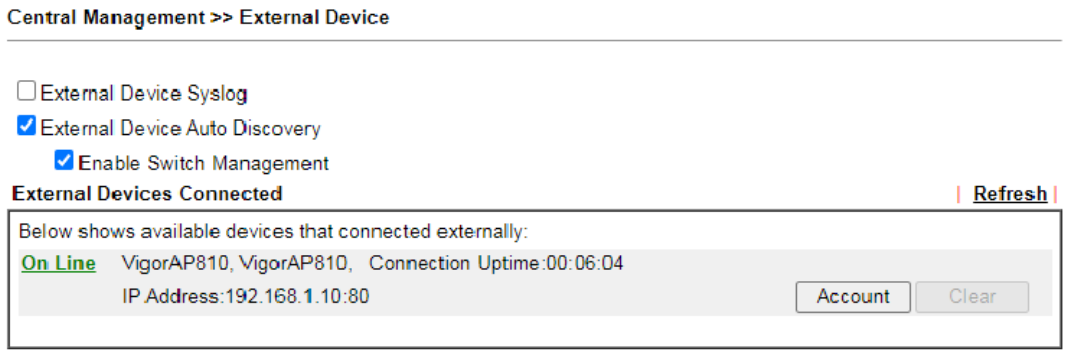
Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.



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. **Enable Switch Management** - It is available only if External Device Auto Discovery is enabled. When it is disabled, the switch status and switch profile(s) under **Central Management >> Switch** will also disabled.

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.

This page is left blank.

Part VI 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.

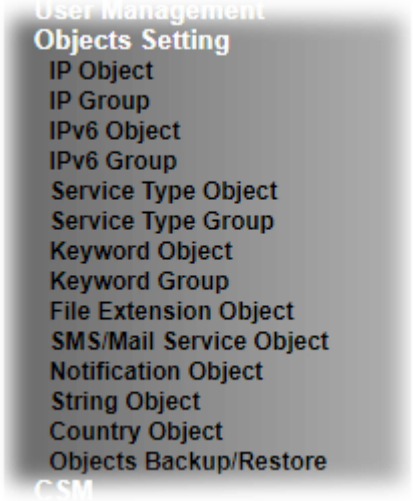
USB

USB device connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications.

VI-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.

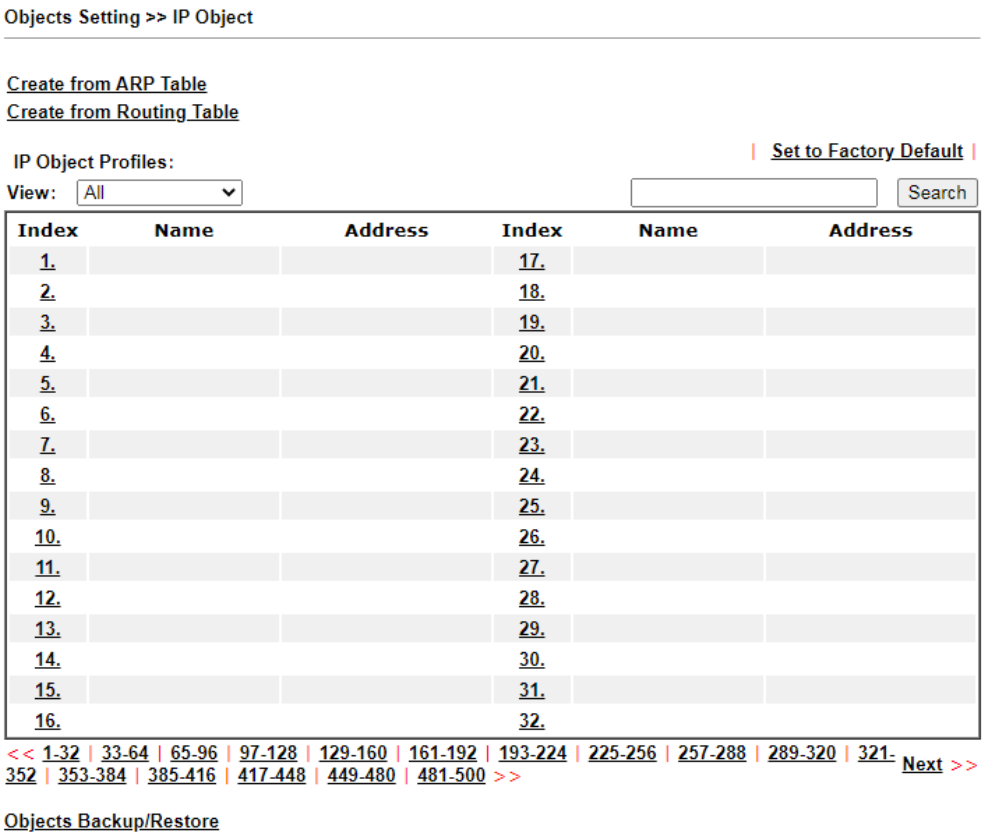
Web User Interface



VI-1-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

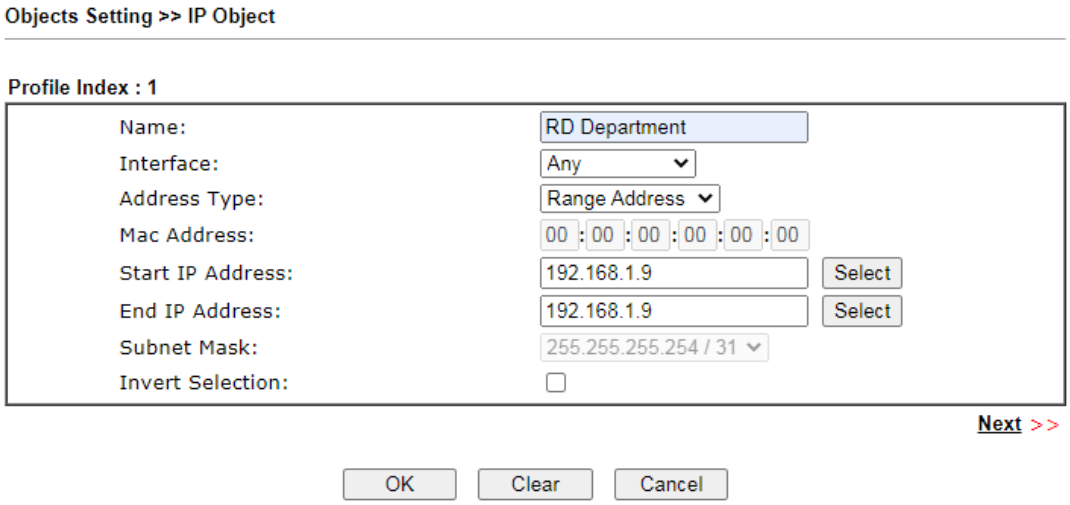
You can set up to 500 sets of IP Objects with different conditions.



Available settings are explained as follows:

Item	Description
View	Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page.
Set to Factory Default	Clear all profiles.
Search	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.

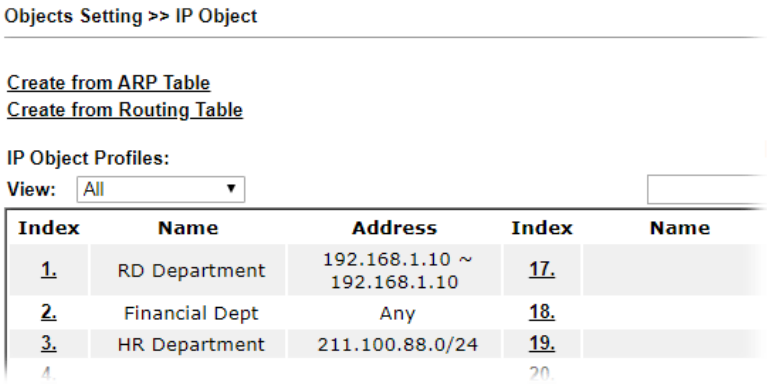


Available settings are explained as follows:

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/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

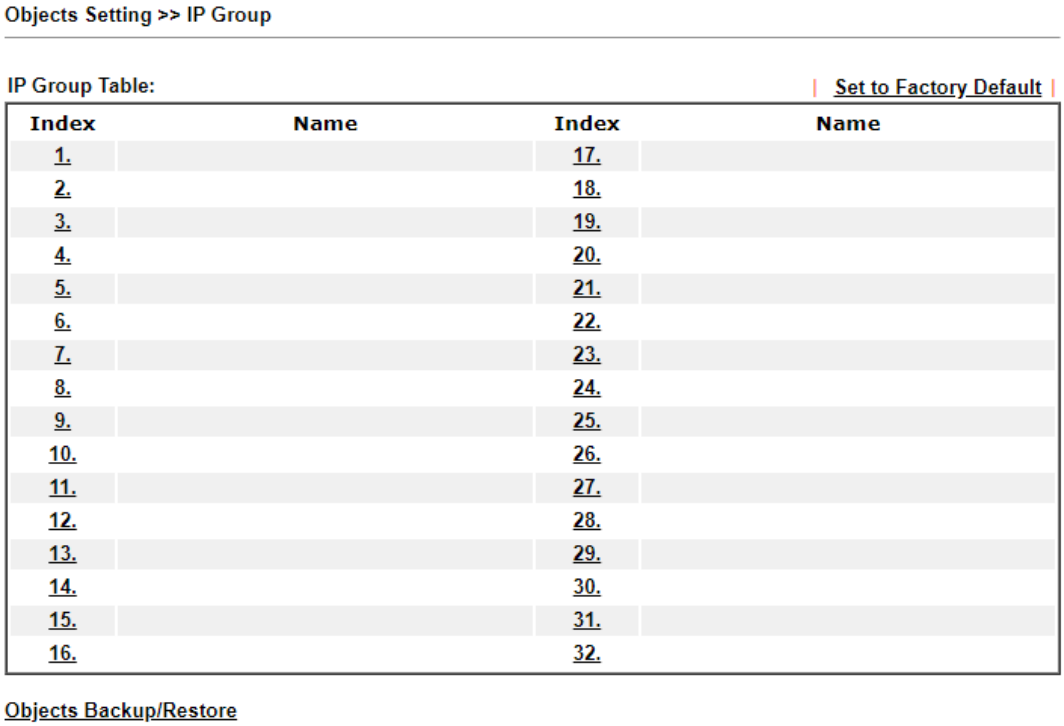
	Mac Address.
Start IP Address	Enter beginning IP address, if Address Type is one of Single Address, Range Address and Subnet Address.
End IP Address	Enter ending IP address, if Address type is one of Single Address, Range Address and Subnet Address.
Subnet Mask	Enter subnet mask, if Address type is Subnet 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**.



VI-1-2 IP Group

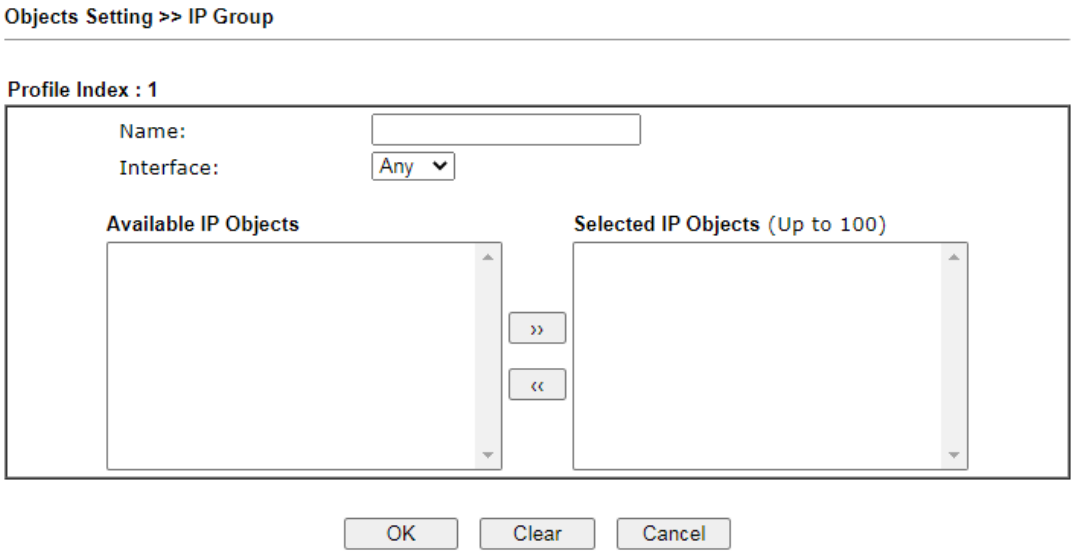
Multiple IP Objects can be placed into an IP Group.



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:

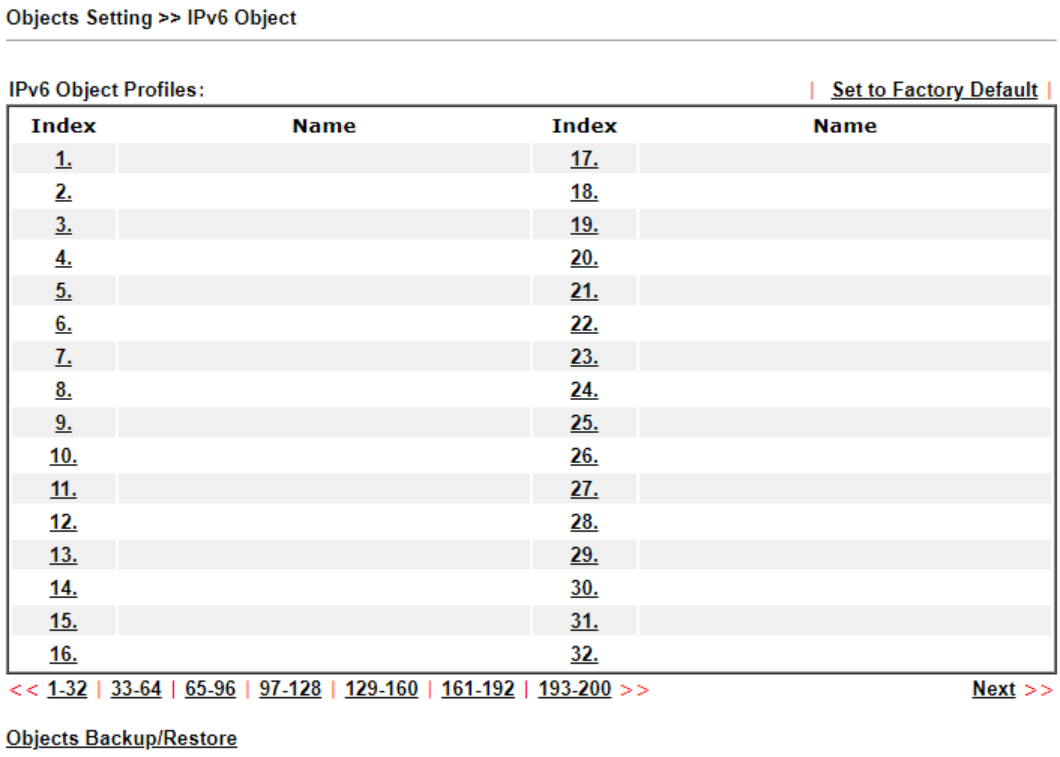
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Interface	Select WAN, LAN or Any to filter IP objects.
Available IP Objects	All available IP objects that are associated with the selected interface.
Selected IP Objects	IP objects that have been added to this profile.

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**.

VI-1-3 IPv6 Object

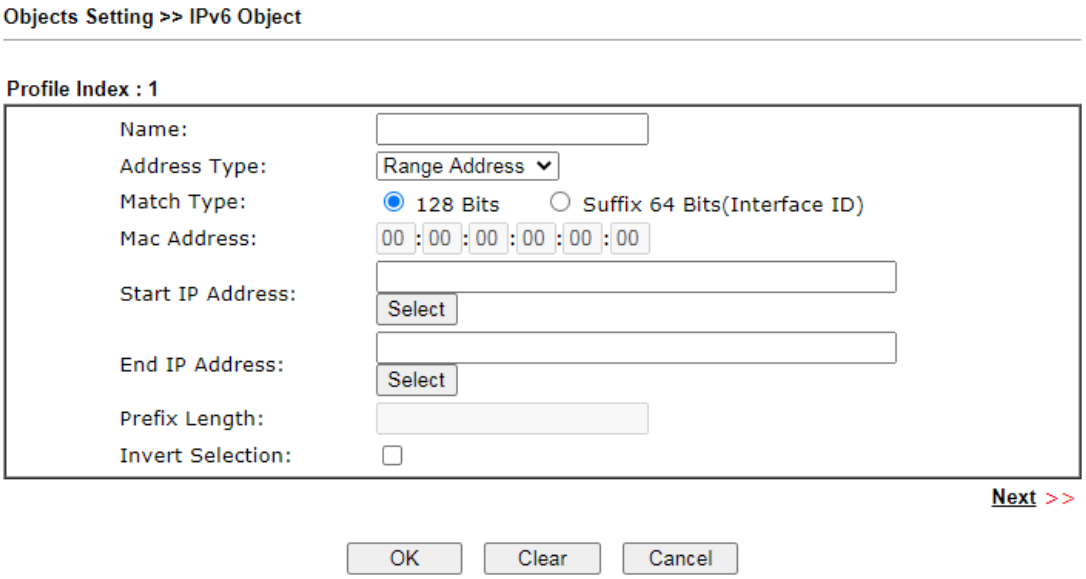
Up to 200 IPv6 Objects can be created.



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.



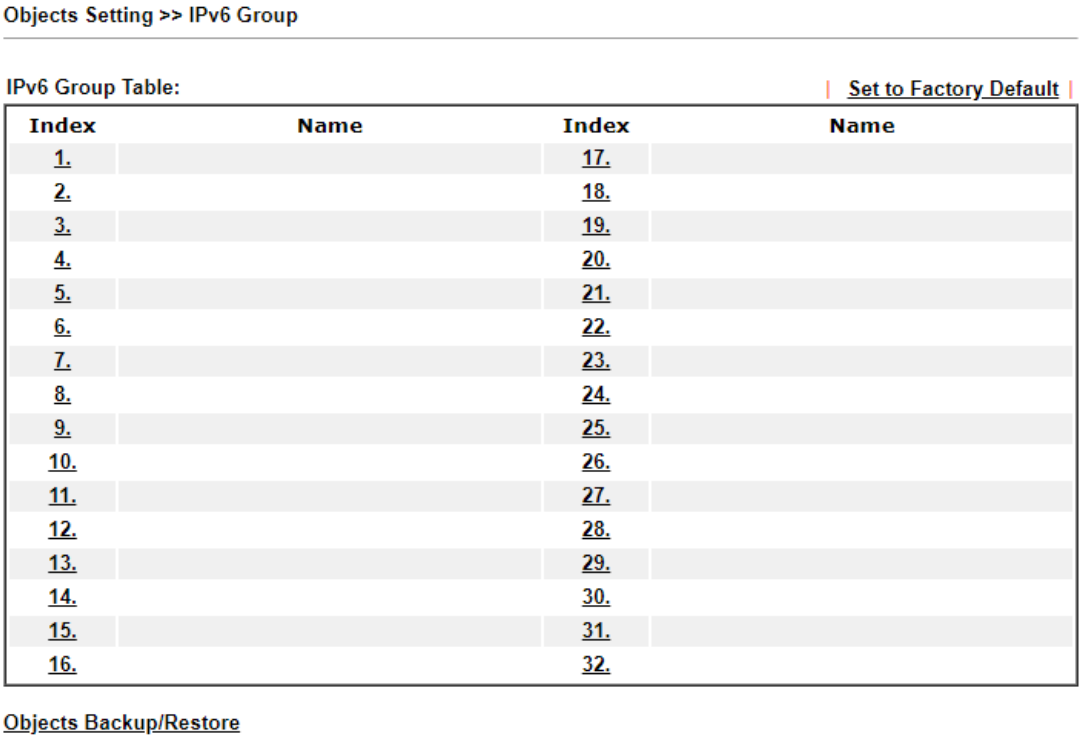
Available settings are explained as follows:

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**.

VI-1-4 IPv6 Group

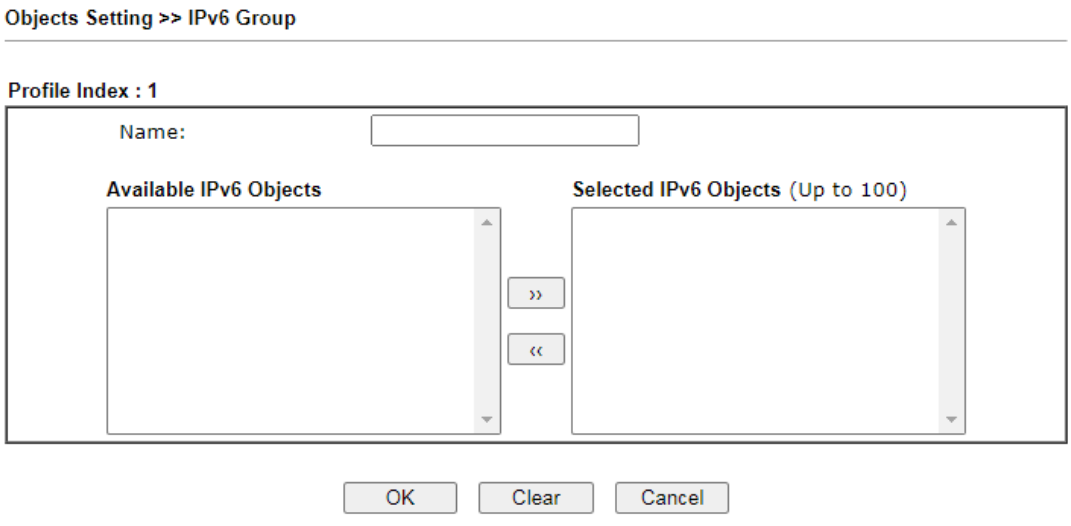
Multiple **IPv6 Objects** can be placed into an **IPv6 Group**.



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:

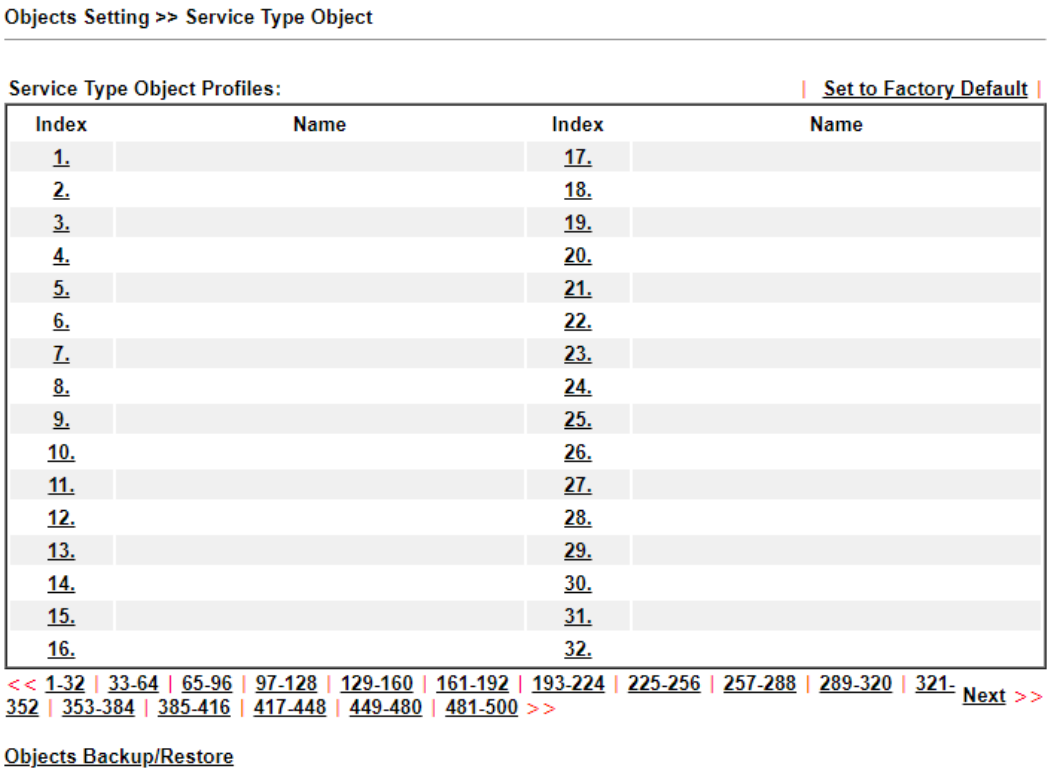
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available IPv6 Objects	All available IP objects that are associated with the selected interface.
Selected IPv6 Objects	IPv6 objects that have been added to this profile.

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**.

VI-1-5 Service Type Object

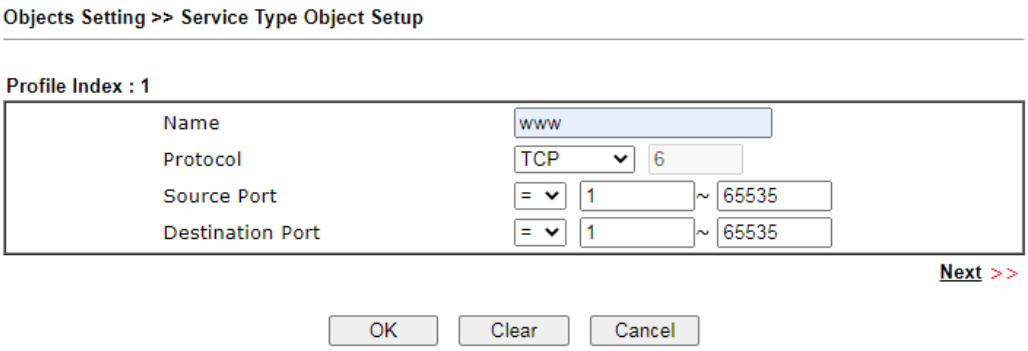
Up to 500 Service Type Objects can be created.



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.

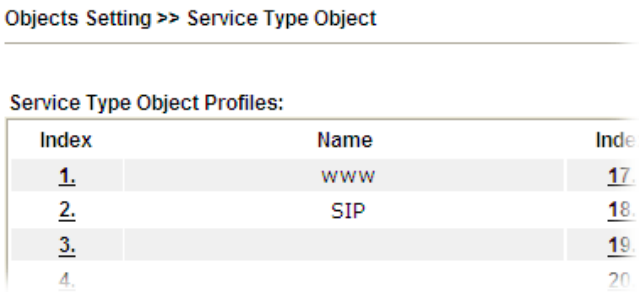
To set up a profile, click the profile number under Index column to bring up the configuration page.



Available settings are explained as follows:

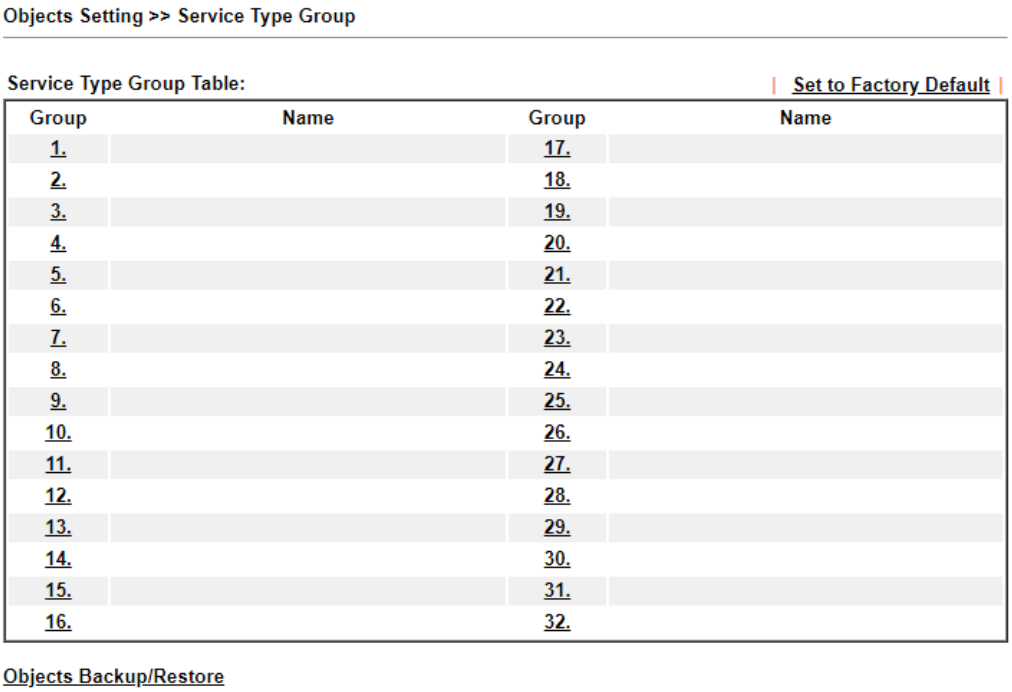
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Protocol	Protocol(s) to which this profile applies. **Any** – All protocols. **ICMP** – Internet Control Message Protocol **IGMP** – Internet Group Management Protocol **TCP** – Transmission Control Protocol **UDP** – 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**.



VI-1-6 Service Type Group

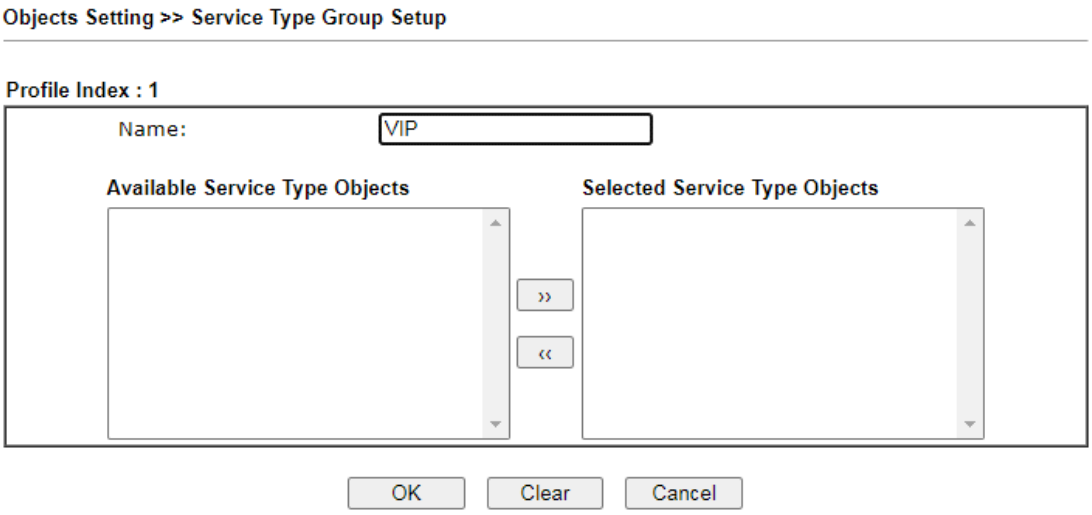
Multiple **Service Type Objects** can be placed into a **Service Type Group**.



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:

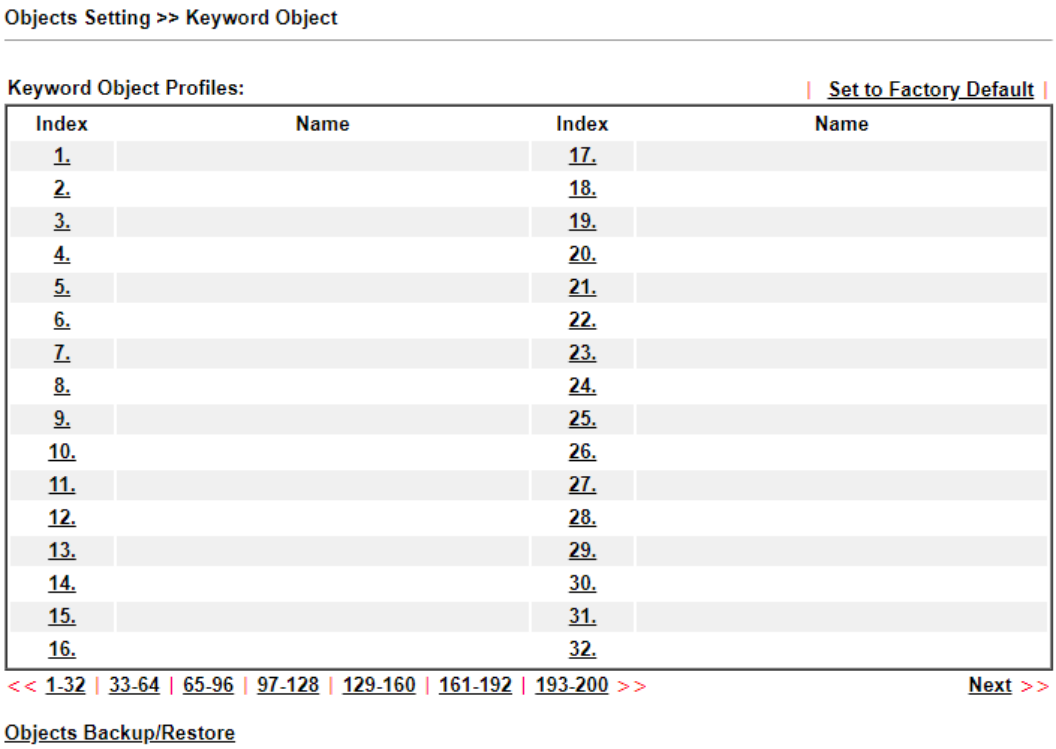
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available Service Type Objects	All available service type objects.
Selected Service Type Objects	Service type objects that have been added to this profile.

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**.

VI-1-7 Keyword Object

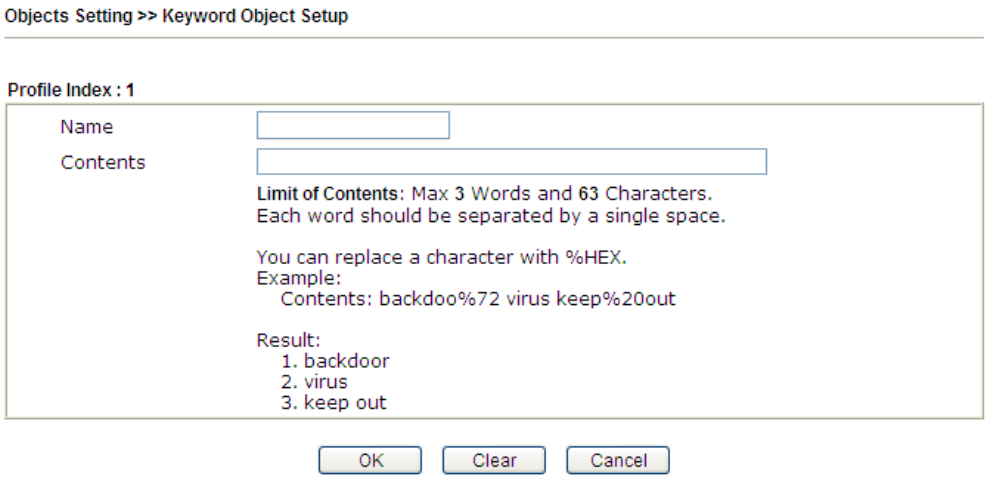
200 Keyword Object Profiles can be created for use as blacklists or white lists in **CSM >>URL Content Filter Profile** and **Web Content Filter Profile**.



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:

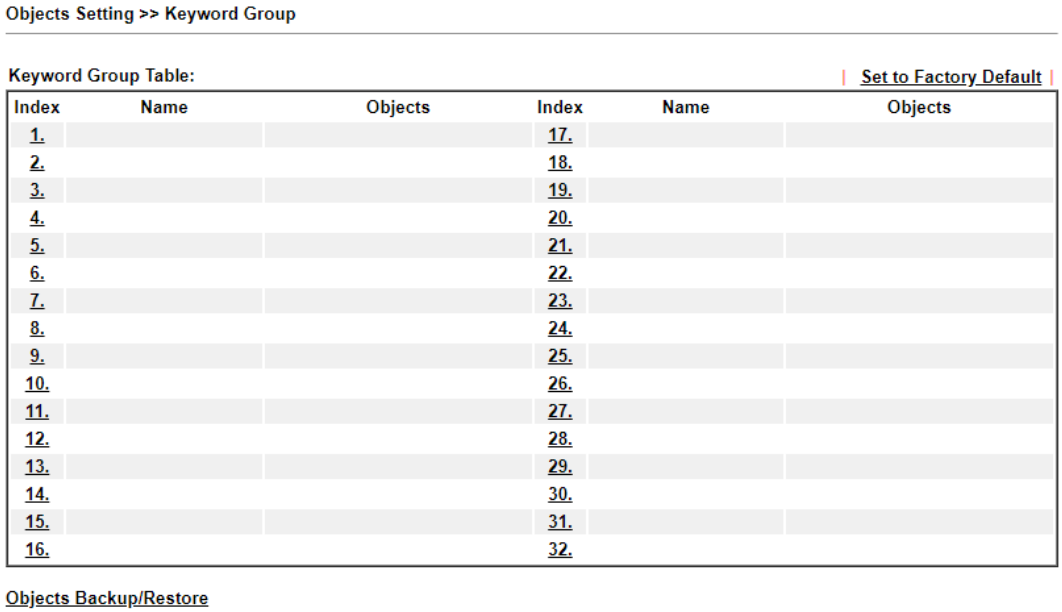
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Contents	Keywords to be matched. Enter the content for this profile. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked 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**.

VI-1-8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.

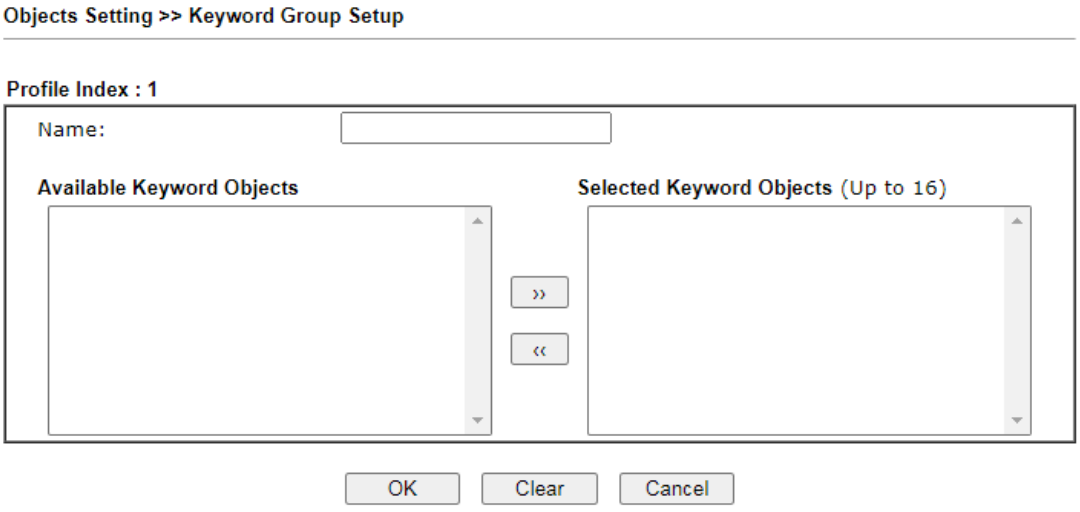
Keyword groups can be chosen as blacklists or white lists in **CSM >>URL /Web Content Filter Profile**.



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:

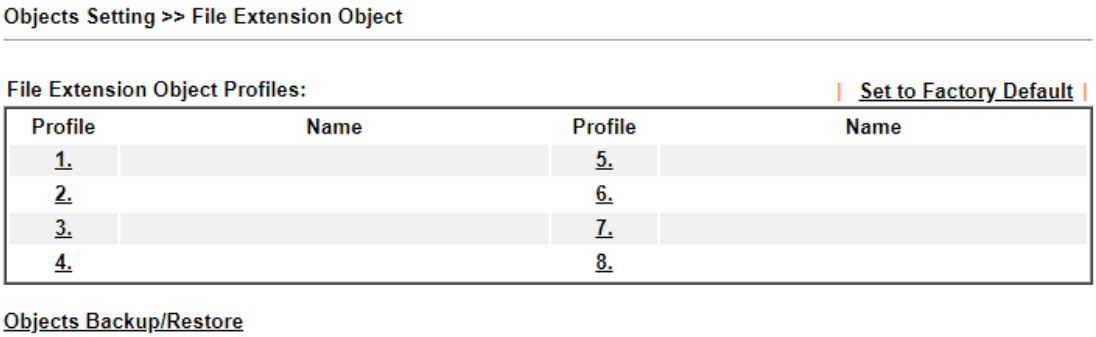
Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available Keyword Objects	All keyword objects that have not been added to this profile.
Selected Keyword Objects	Keyword objects that have been added to this profile.

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**.

VI-1-9 File Extension Object

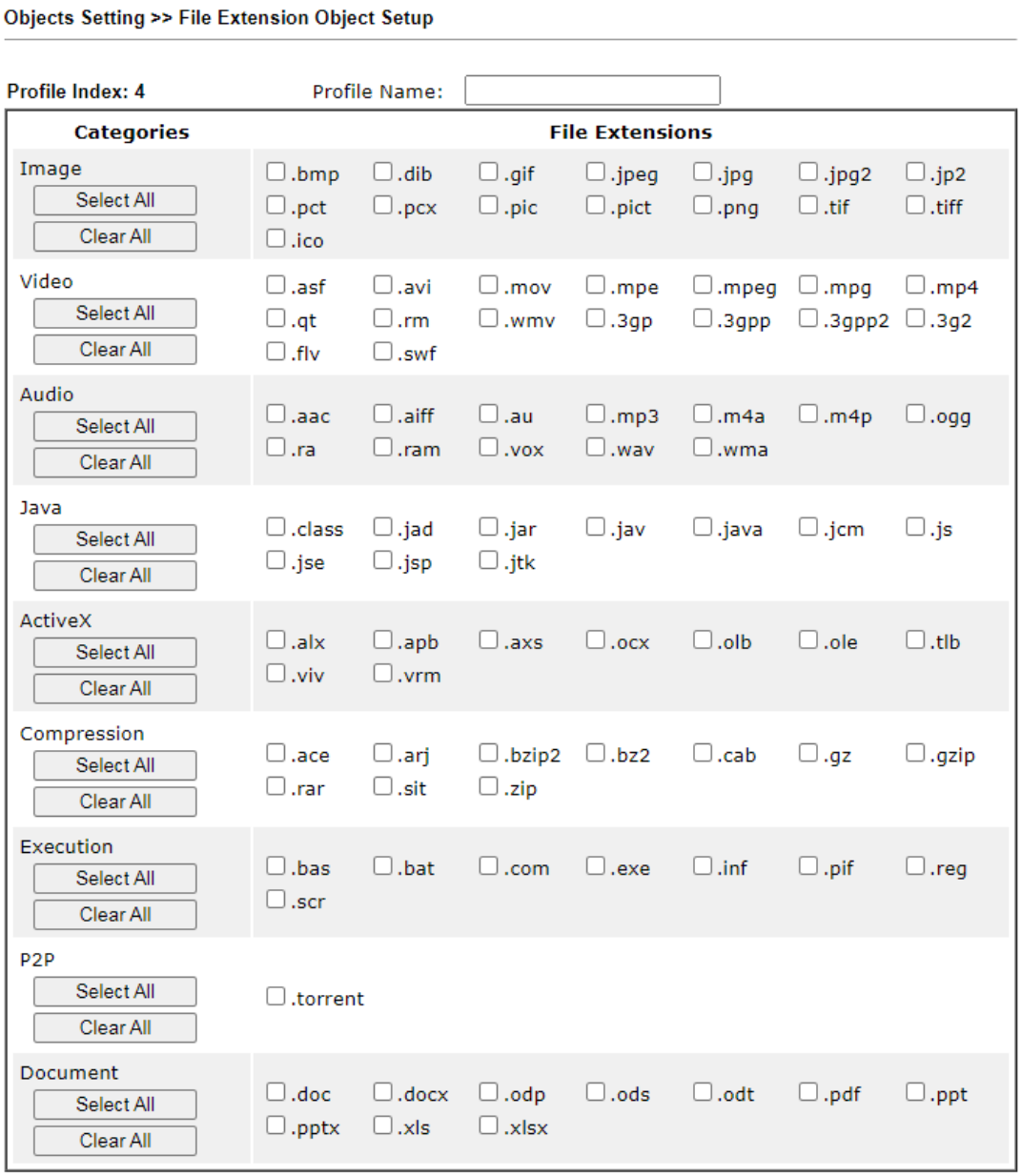
Up to 8 File Extension Objects can be set up for use with **CSM>>URL Content Filter**.



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:

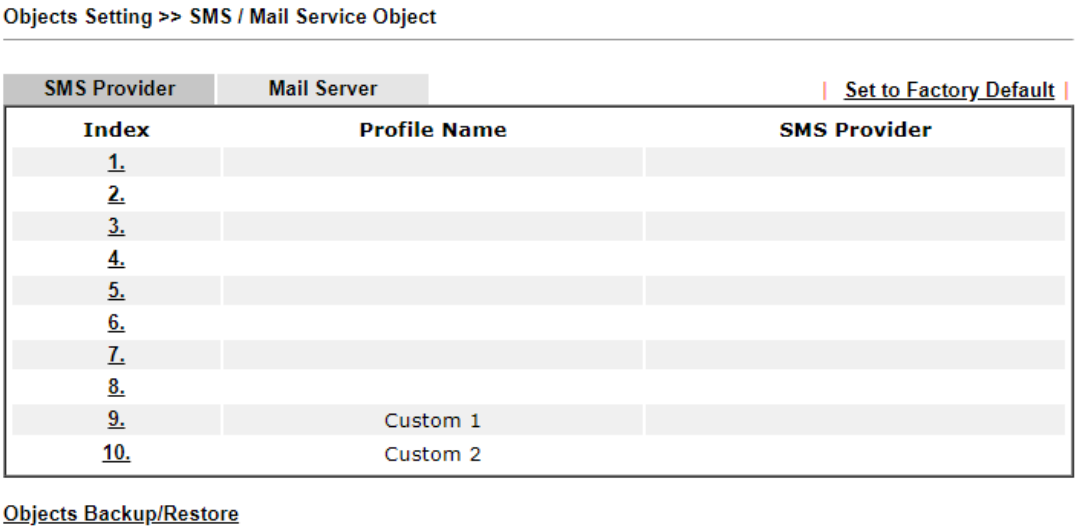
Item	Description
Profile Name	Name that identifies this profile. Maximum length is 7 characters.
Select All	Selects all file extensions for the category.
Clear All	Deselects all file extensions for the category.

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**.

VI-1-10 SMS/Mail Service Object

SMS Service Object

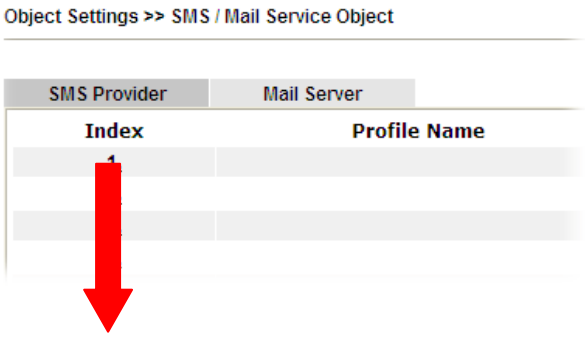
Up to 10 SMS Service Objects can be set up for use with **Application>>SMS Alert Service**.

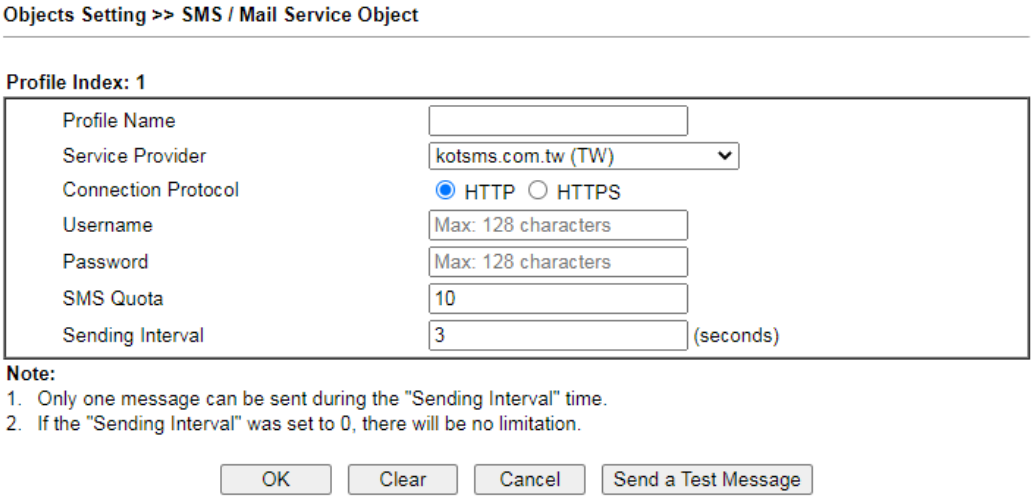


Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Profile	Name 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.





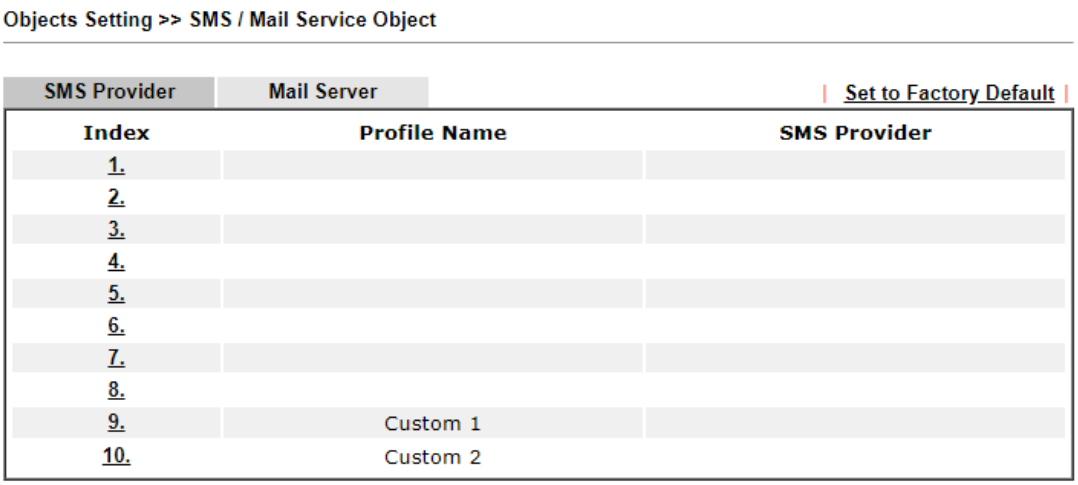
Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 31 characters.
Service Provider	Select a Service Provider from the dropdown list.
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.

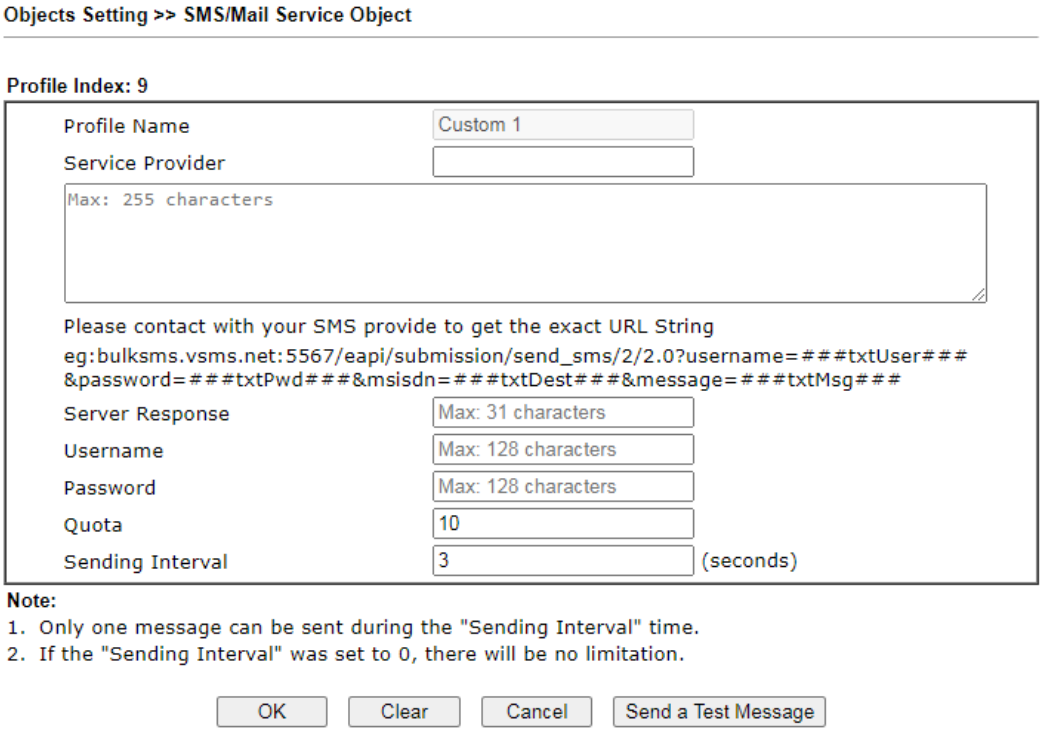
To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the SMS service object, click **Clear**.

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:

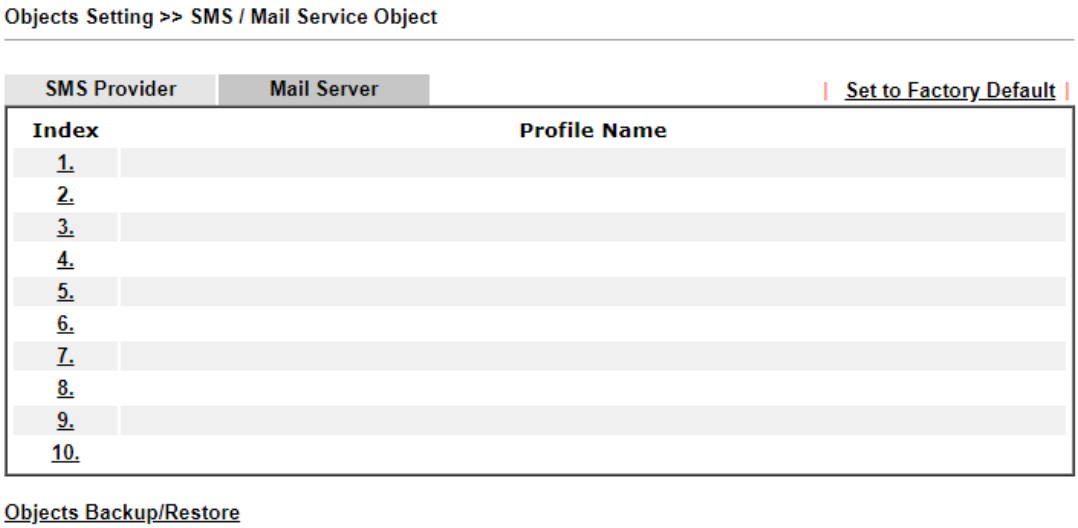
Item	Description
Profile Name	Display-only profile name, which is Custom 1 for Index 9 and Custom 2 for Index 10.
Service Provider	Enter an identifier for the service provider.
Entry box	Enter the URL for the SMS service. Maximum length is 255 characters. Contact the service provider for the appropriate 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.
Password	Password used to log in to the service.
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.

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

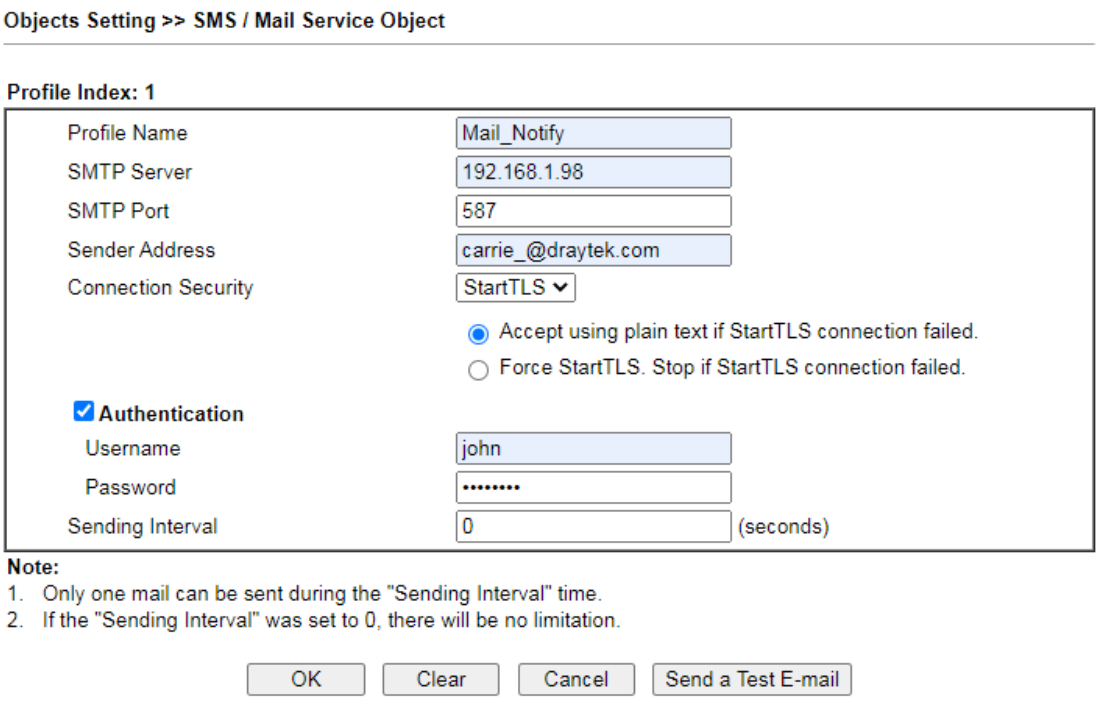
Up to 10 **Mail Service Objects** can be set up for use with **Application>>SMS/Mail Alert Service**.



Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Profile	Name 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.
Connection Security	There are three methods to enhance the connection security of SMTP server. **Plaintext** - No SSL. Packets will be transferred without encryption. **SSL** - Packets will be transferred with encrypted connection. Select to use SMTPS (SMTP over SSL) to communicate with the SMTP server. Note that the port number used for SMTPS server is 465. **StartTLS** - Specify one of the two modes. The packets will be transferred or stopped transmission according to the practical situation that occurred. ● "Accept using plain text if StartTLS connection failed" - If selected, the connection security will be done by StartTLS server. However, if the connection failed, then the packets will be transferred without encryption instead. ● "Force StartTLS. Stop if StartTLS connection failed" - If selected, the connection security will be done by StartTLS server. However, if the StartTLS connection failed, the packets will not be transferred.
Authentication	Select to send username and password to SMTP server for authentication. **Username** – Username for authentication. Maximum length is 31 characters.

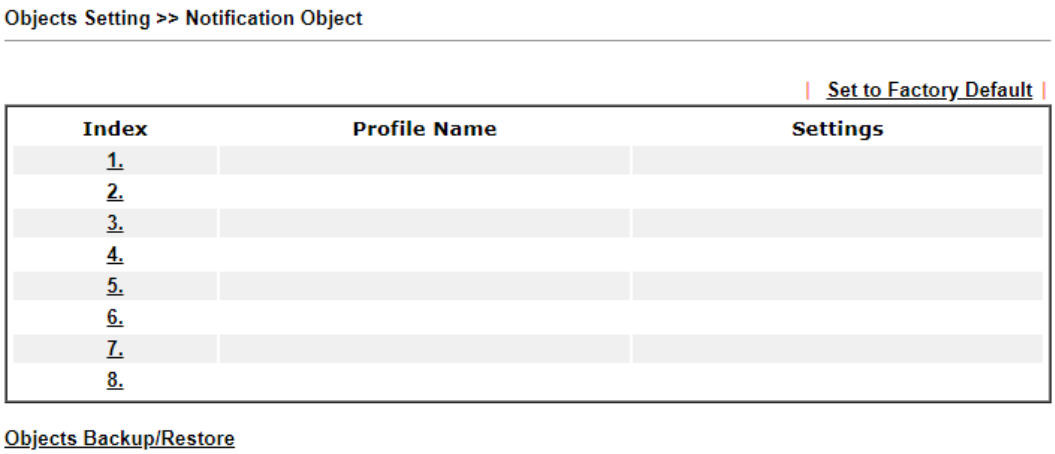
	Password – Password for authentication. Maximum length is 31 characters.
Sending Interval	Minimum amount of time, in seconds, to wait between sending e-mail messages.
Send a Test E-mail	Click it to send a test e-mail according to above configuration.

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**.

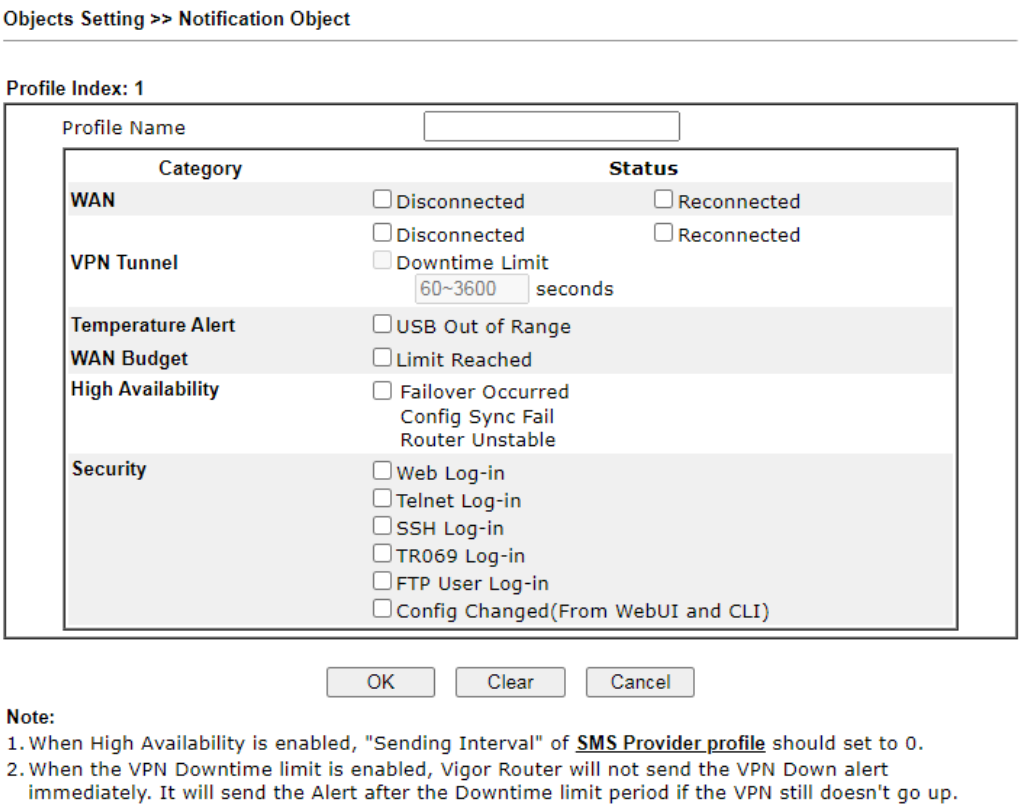
VI-1-11 Notification Object

Up to 8 Notification Objects can be set up for use in Application>>SMS Alert Service and Application>>Mail Alert Service.

You can set an object with different monitoring situation.



To set up a profile, click its index to bring up the configuration page.



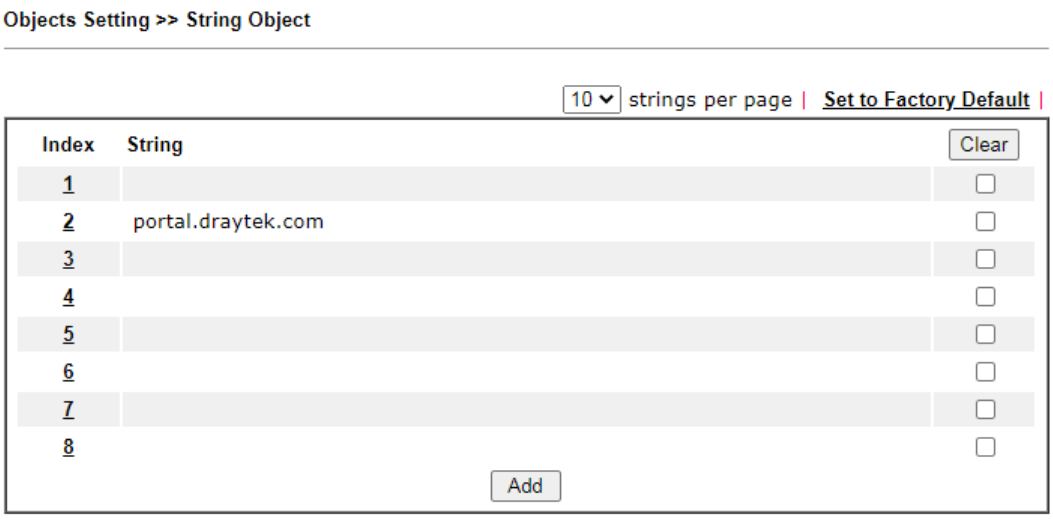
Available settings are explained as follows:

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.

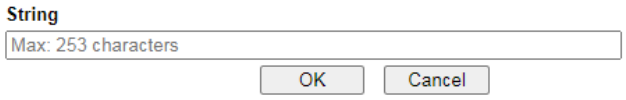
To save changes on the page, click OK. To discard changes, click Cancel. To blank out all settings in the notification object, click Clear.

VI-1-12 String Object

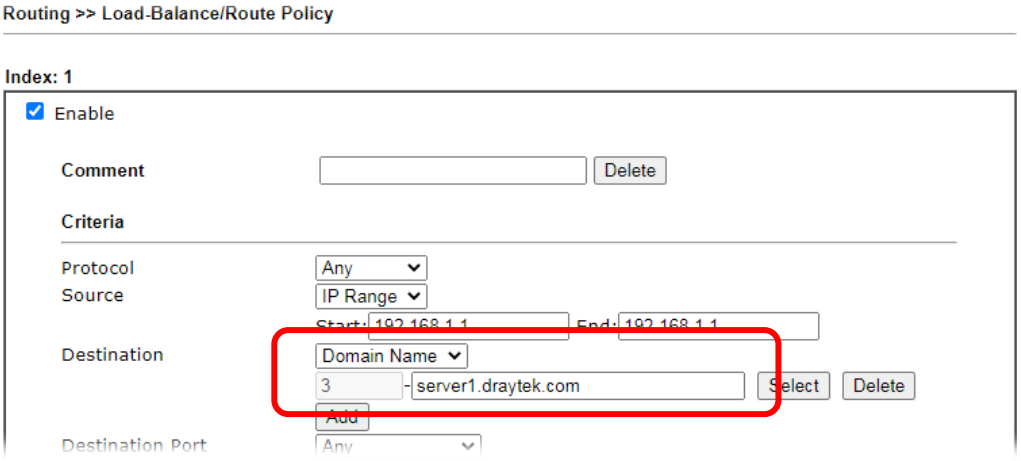
This page allows you to set string profiles which will be applied in route policy (domain name selection for destination) and etc.



Available settings are explained as follows:

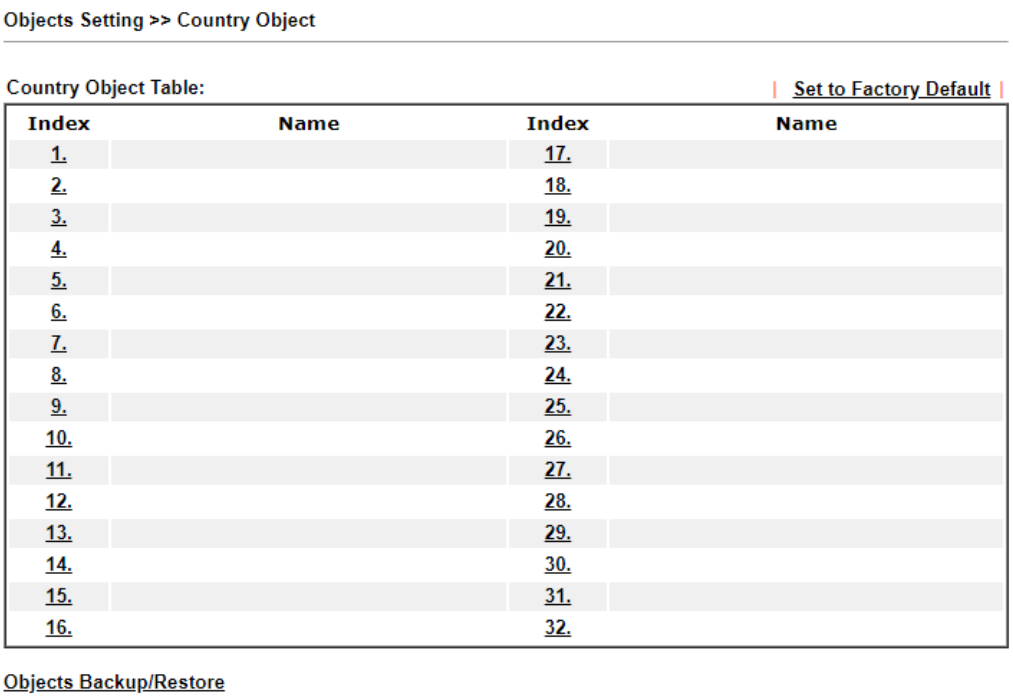
Item	Description
Add	Click it to open the following page for adding a new string object. 
Set to Factory Default	Click it to clear all of the settings in this page.
Index	Display the number link of the string profile.
String	Display the string defined.
Clear	Choose the string that you want to remove. Then click this check box to delete the selected string.

Below shows an example to apply string object (in Route Policy):

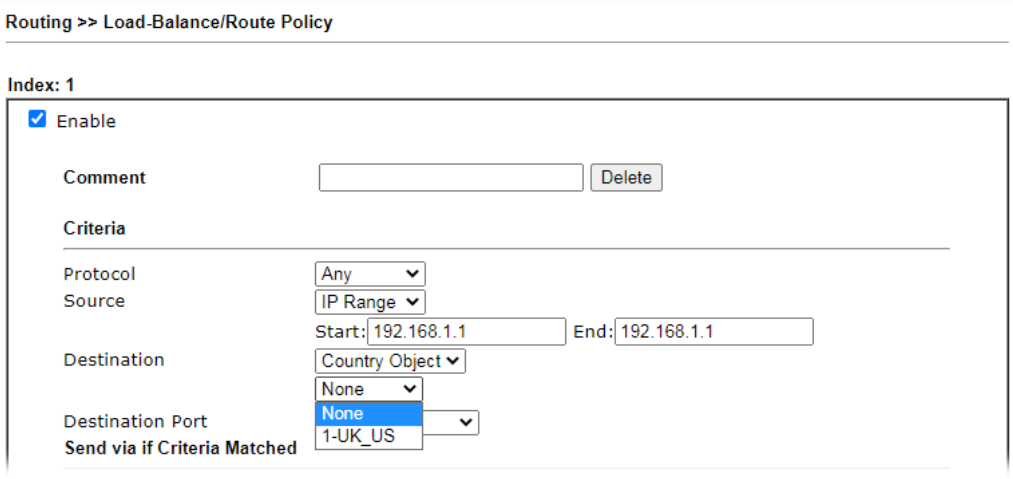


VI-1-13 Country Object

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:

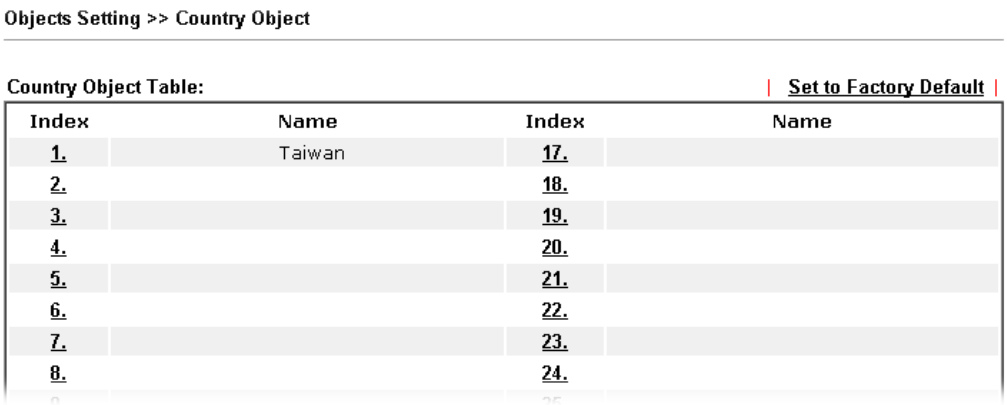
1. Open **Object Setting>>Country Object**, and click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Available settings are explained as follows:

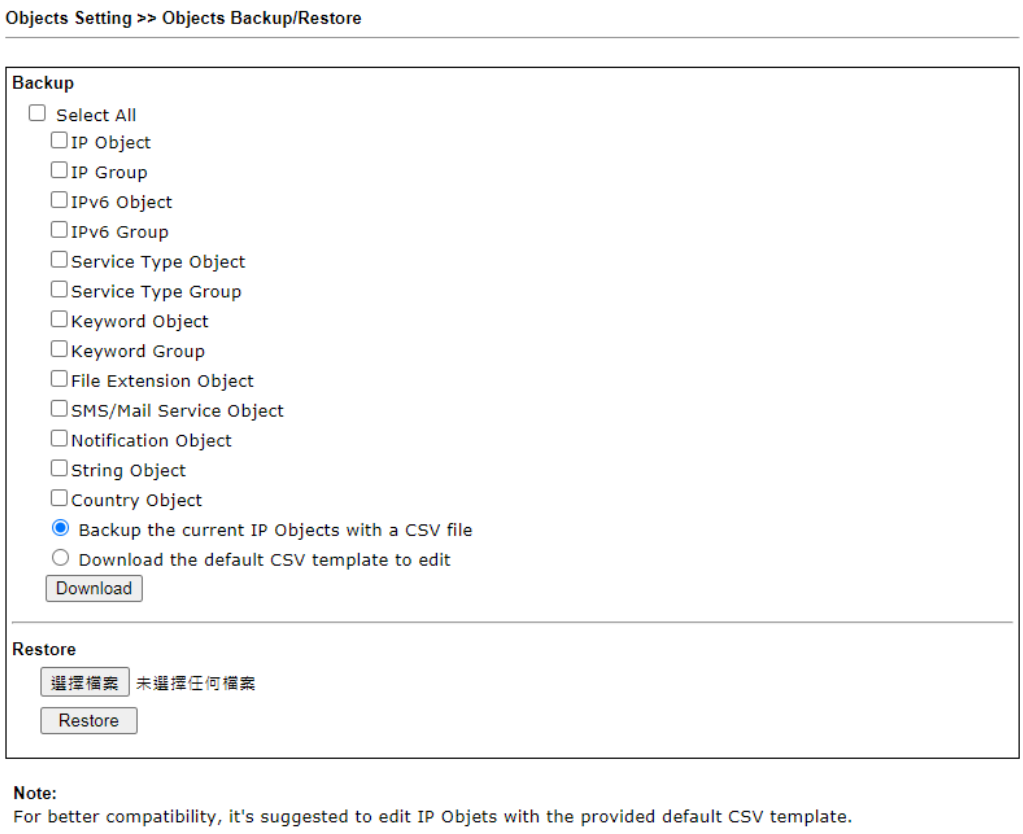
Item	Description
Name	Type a name for such profile. The maximum length of the name you can set is 15 characters.
Available Country / Selected Country	Select any country from Available Country. Click >> to move the selected country and place on Selected Country. Note that one country profile can contain 1 up to 16 countries.

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



VI-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:

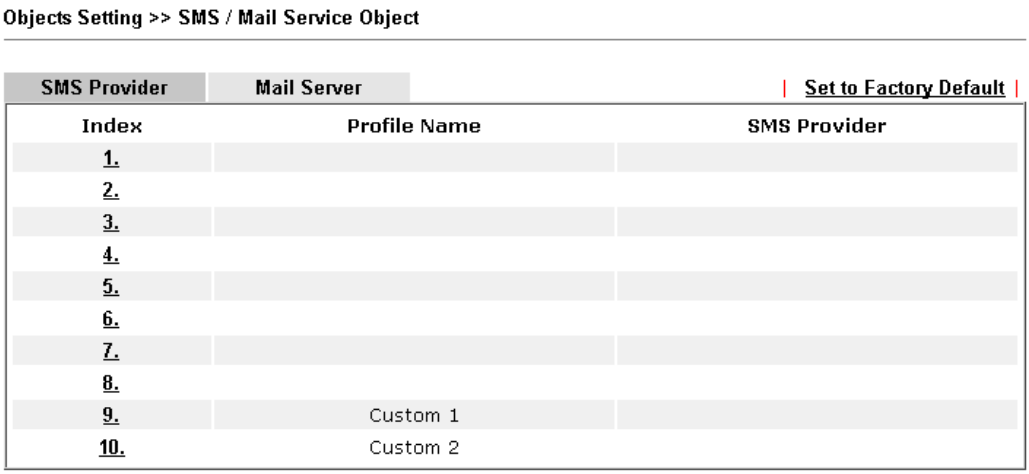
Item	Description
Backup	Usually, the IP objects can be created one by one through the web page of **Objects>>IP Object**. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file. All 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

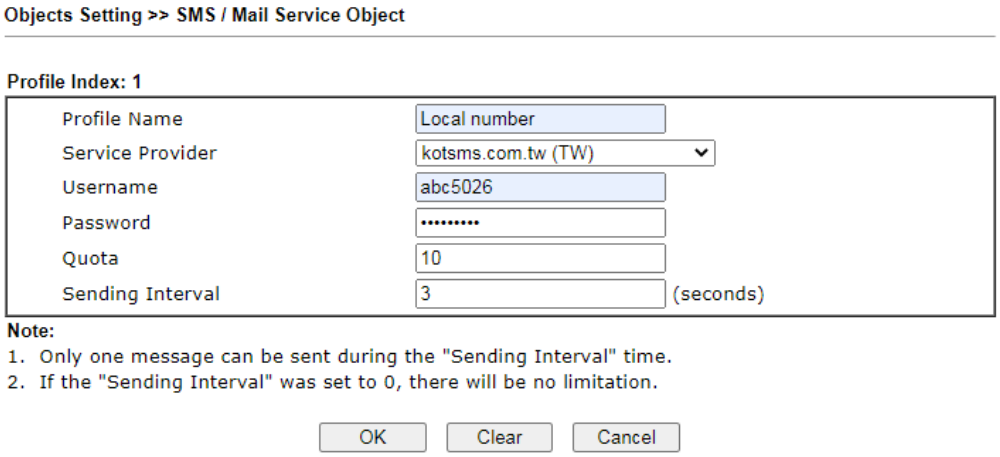
Follow the steps listed below:

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.

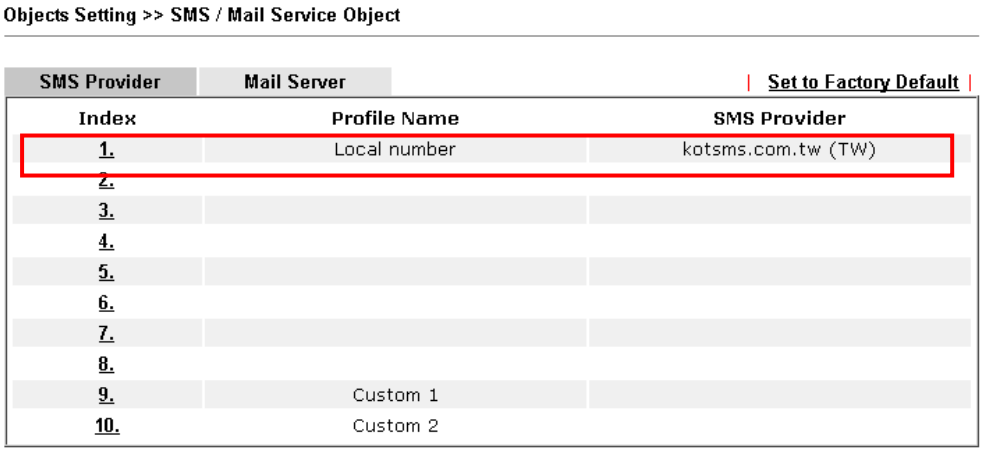


Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

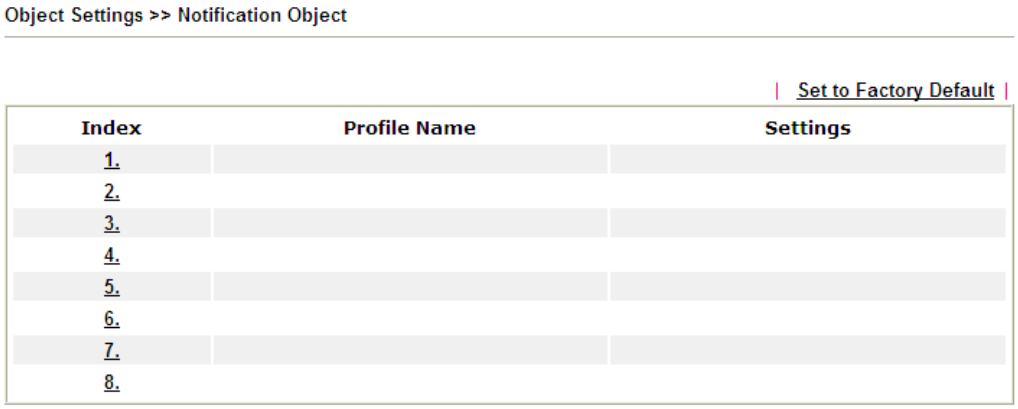
3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.



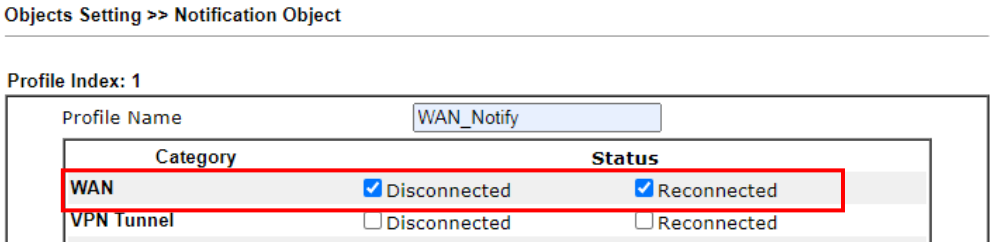
4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.



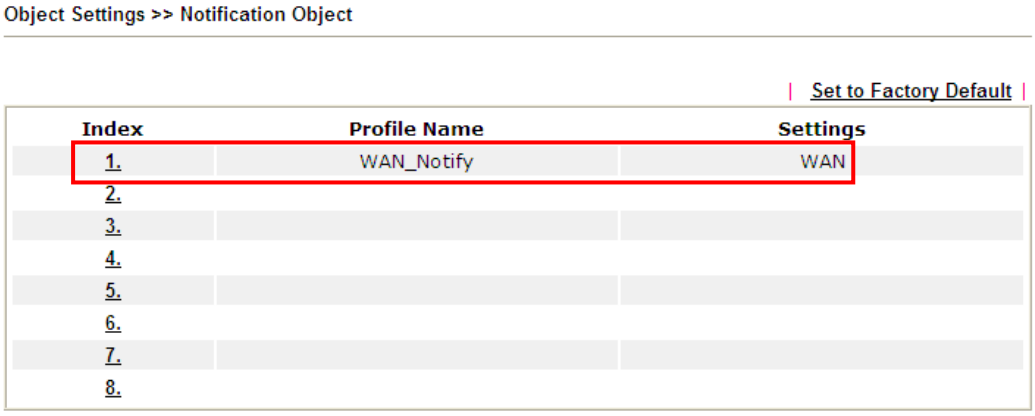
5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.



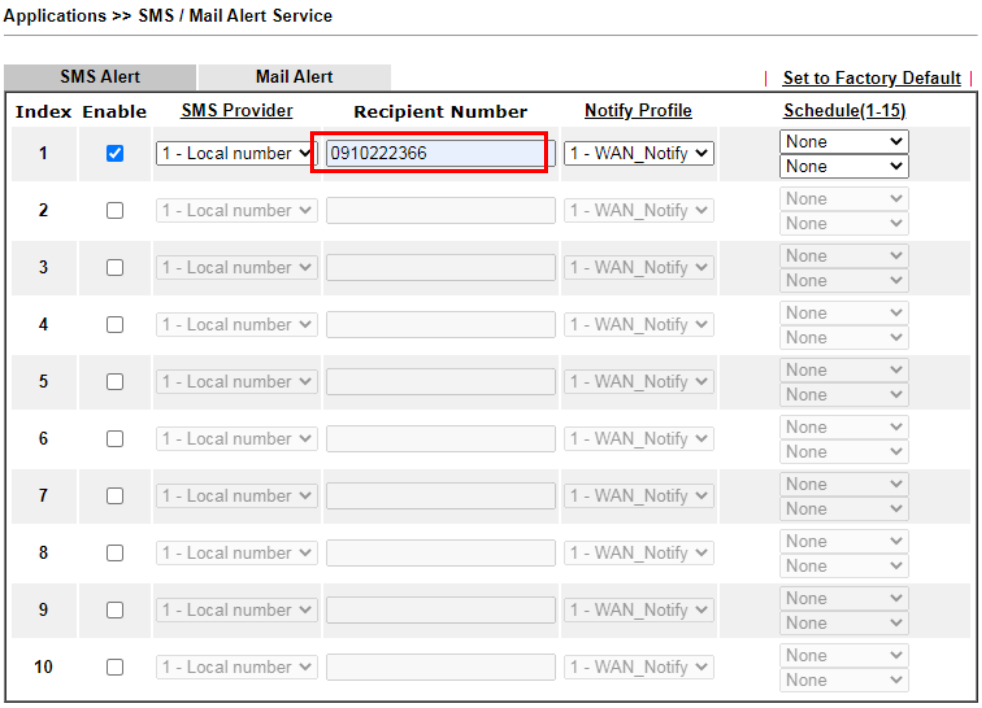
6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, type the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.



7. After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.



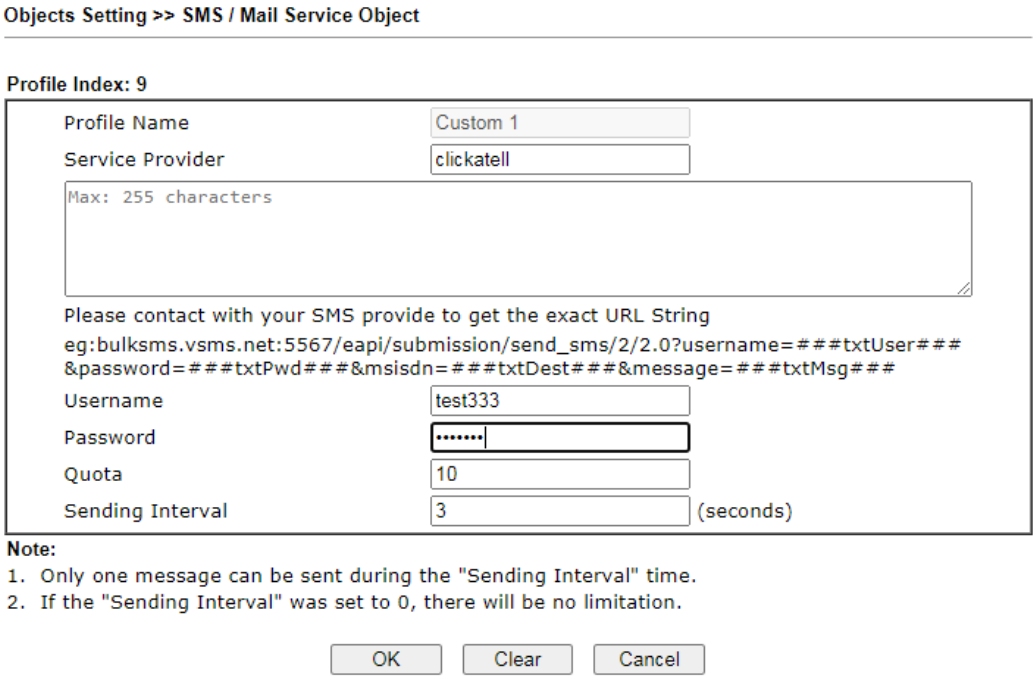
8. Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, type the phone number in the field of Recipient (the one who will receive the SMS).



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, type the URL string of the SMS provider and type 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.

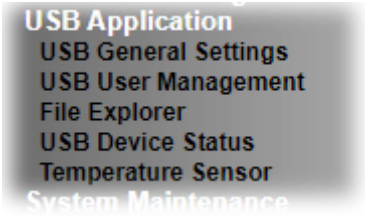


VI-2 USB Application

USB devices connected to the Vigor router can function as storage servers or thermometers.

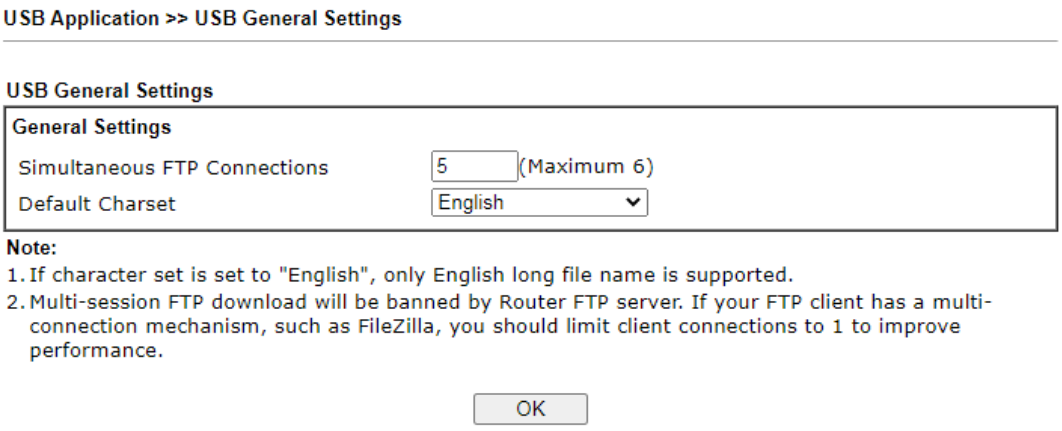
After setting the configuration in USB Application, a USB storage device can be accessed using either the FTP or SMB protocol from LAN clients with the IP address of the Vigor router and the username and password entered in **USB Application>>USB User Management**.

Web User Interface



VI-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.



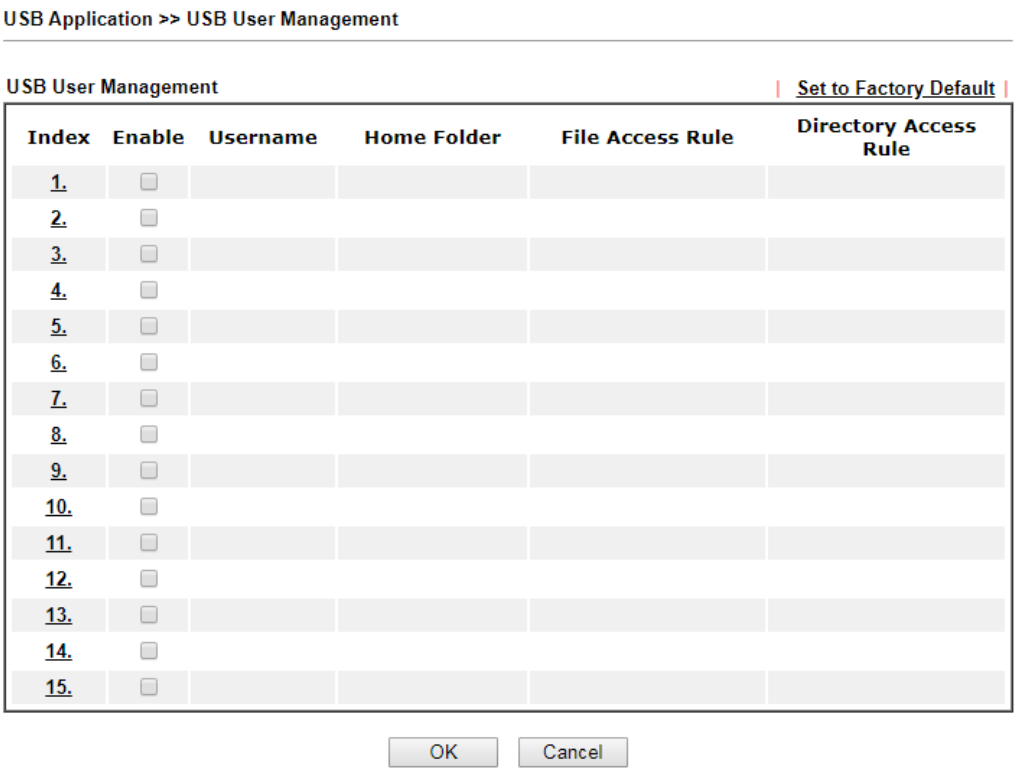
Available settings are explained as follows:

Item	Description
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.

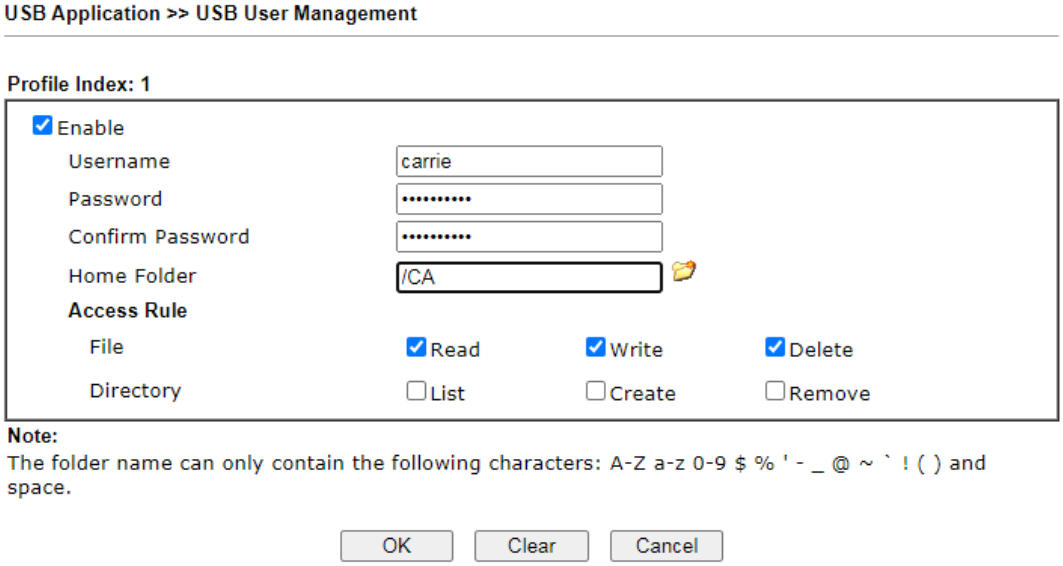
Select **OK** to save changes on the page.

VI-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.

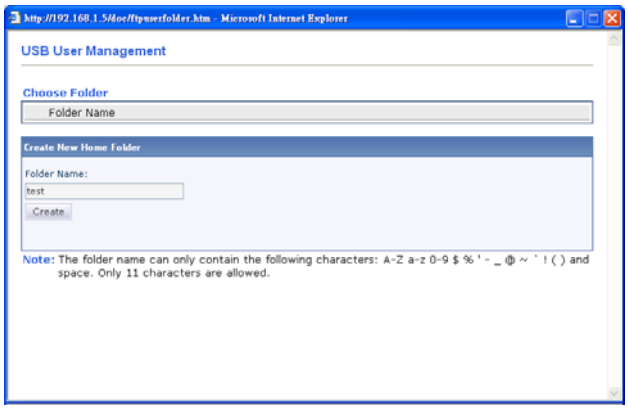


Click index number to access into configuration page.



Available settings are explained as follows:

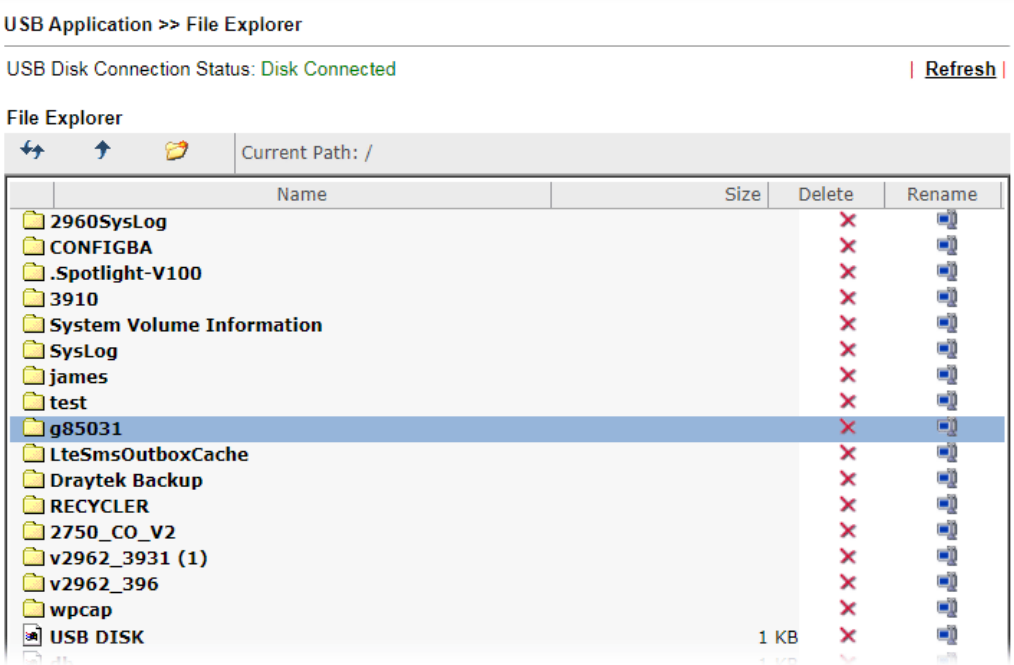
Item	Description
Enable	Check to activate this profile (account) for FTP service and / or SMB service. Later, the user can use the username specified in this page to login into FTP server.
Username	Enter the username for this user profile. Maximum allowed length of the username is 11 characters. **Note:** 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**.

VI-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.

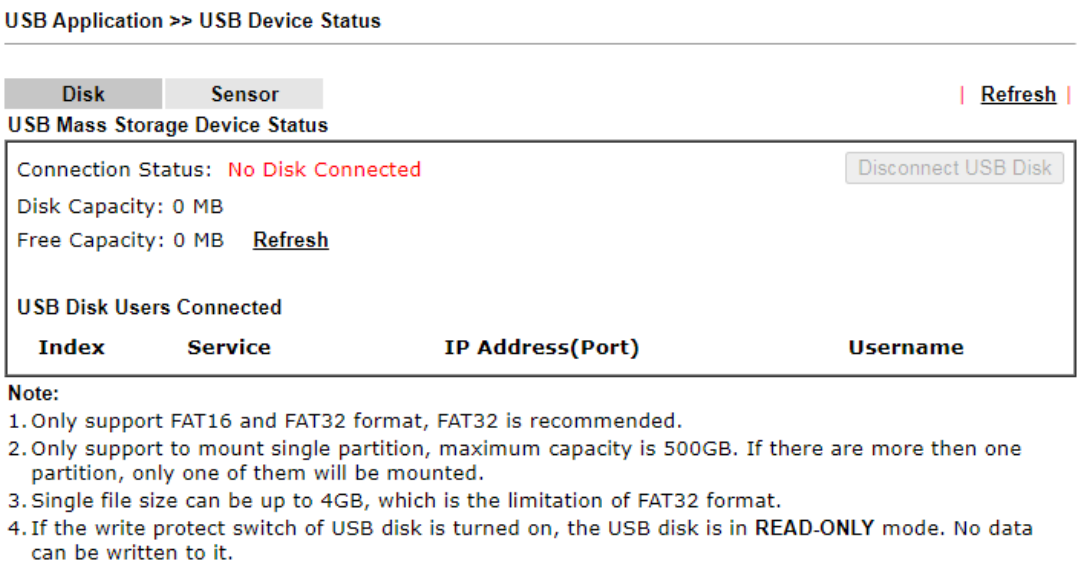


Available settings are explained as follows:

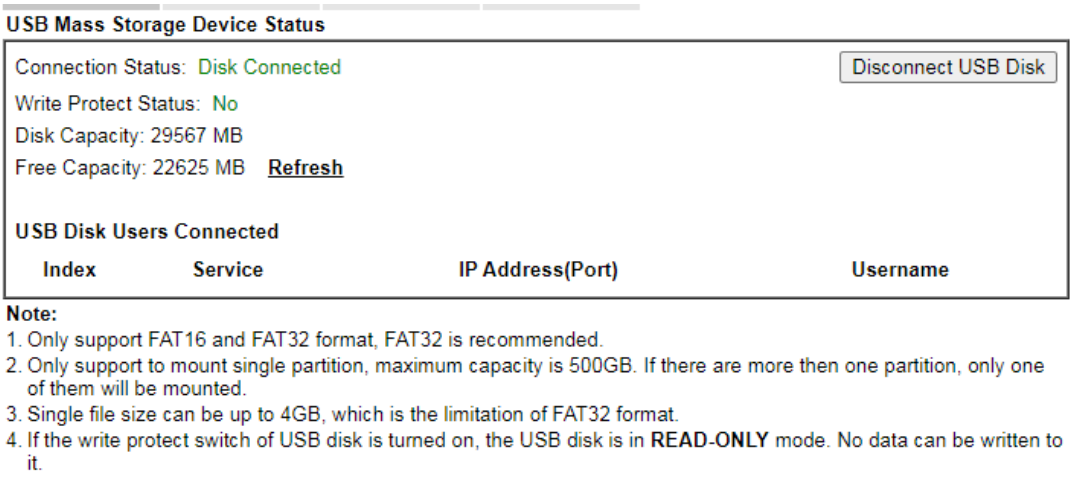
Item	Description
Refresh	Click this icon to refresh the list of files and folders.
Back	Click this icon to return to the parent folder.
Create	Click this icon to add a new folder.
Current Path	Shows current folder.
Upload	To upload a file to the USB storage device, click the **Browse...** button to bring up the file selection dialog box. Select the file you wish to upload, and click the **Upload** button to initiate the upload process.

VI-2-4 USB Device Status

This page allows monitoring of the status of USB devices (disk 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.

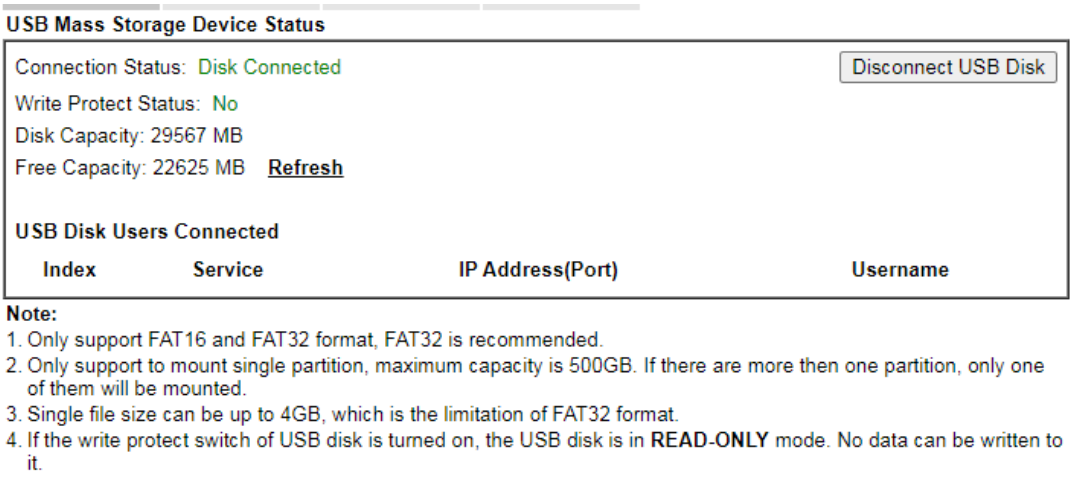


Available settings are explained as follows:

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.



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.

VI-2-5 Temperature Sensor

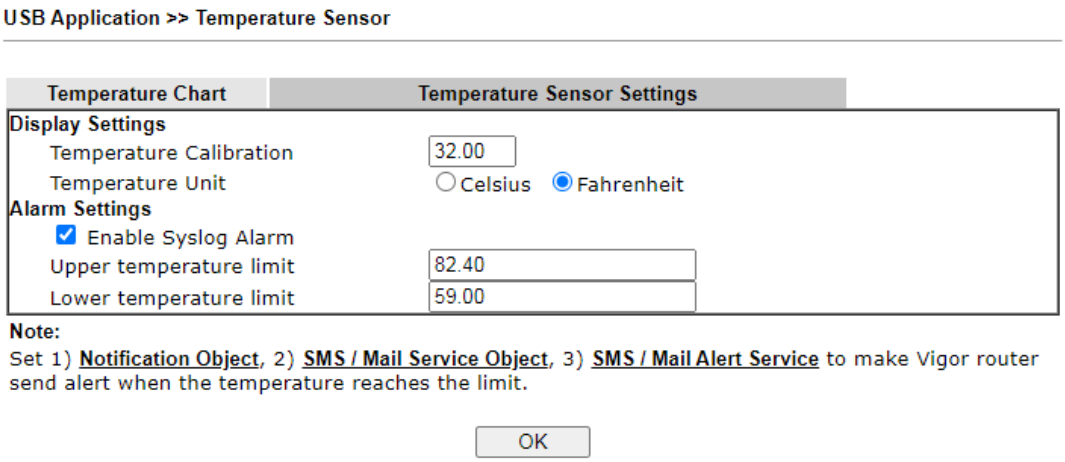
A USB Thermometer is now available. It complements your installed DrayTek router installations which will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

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



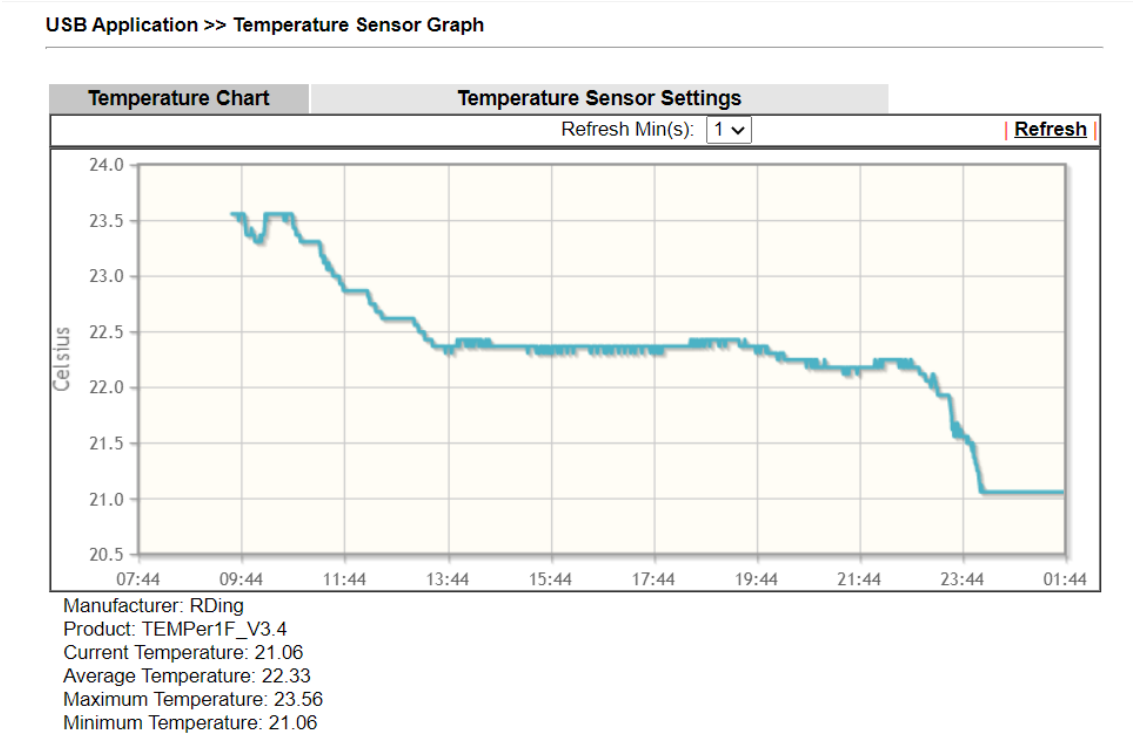
Available settings are explained as follows:

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:



Part VII 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.

VII-1 Diagnostics

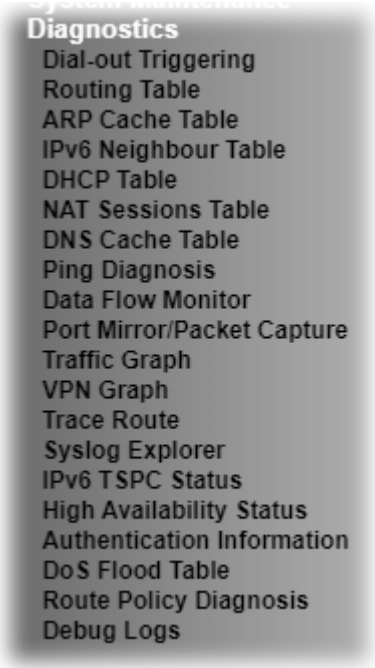
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- 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.

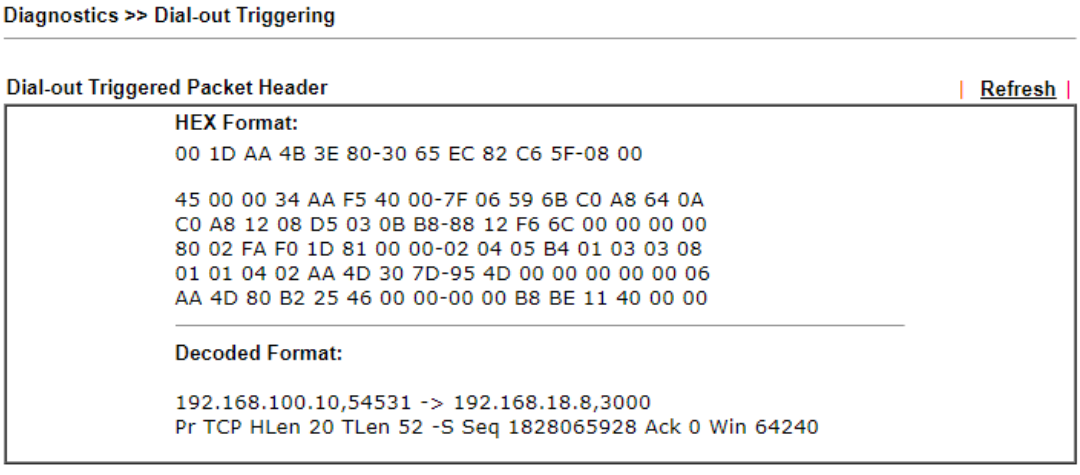
Web User Interface

This section contains utilities that can assist you in analyzing issues and failures during the setup and operation of the router.



VII-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.



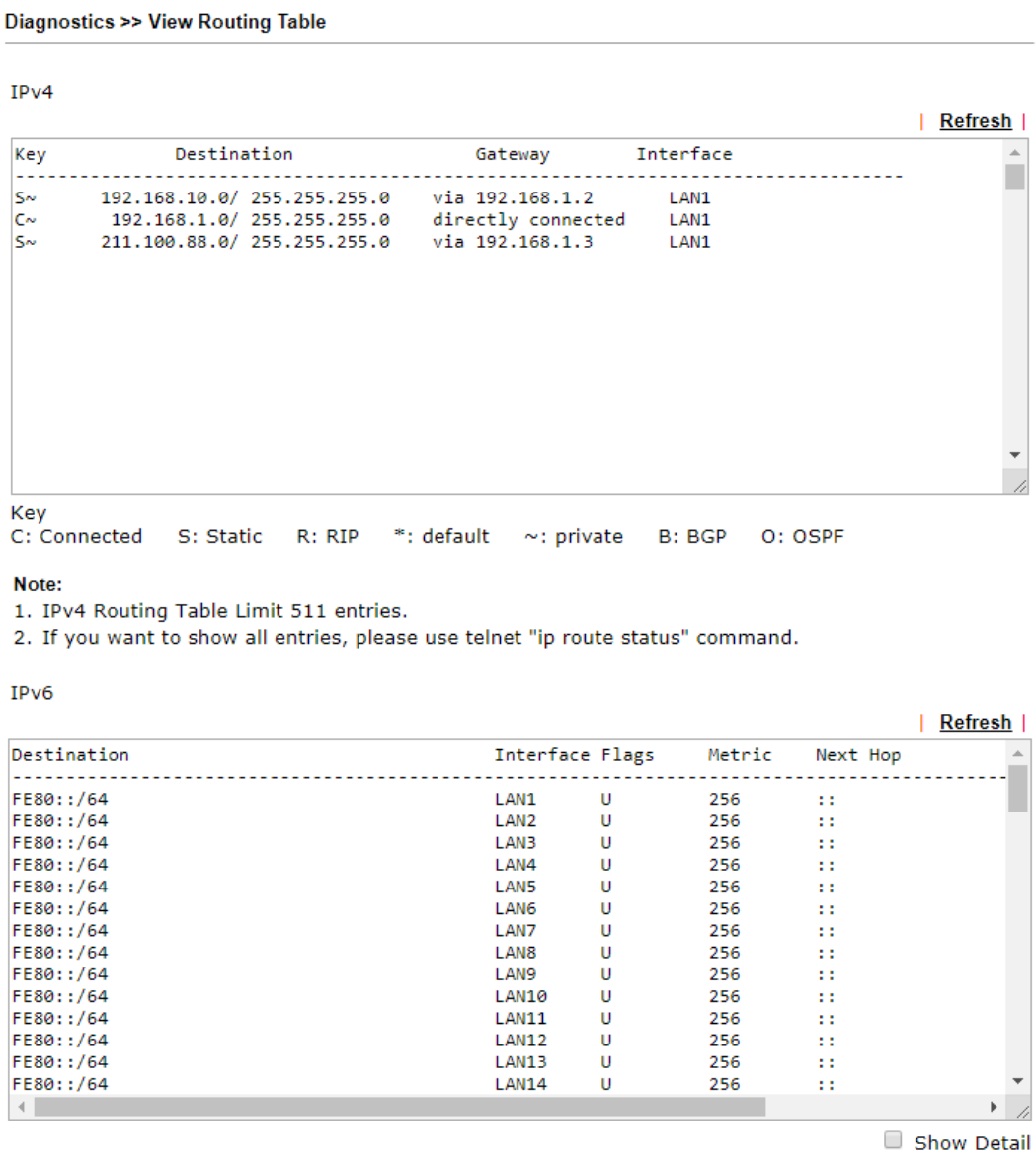
Available settings are explained as follows:

Item	Description
Decoded Format	Shows the dial-out triggered packet header in hexadecimal format.

Refresh	Shows the dial-out triggered packet header in human-readable format.

VII-1-2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

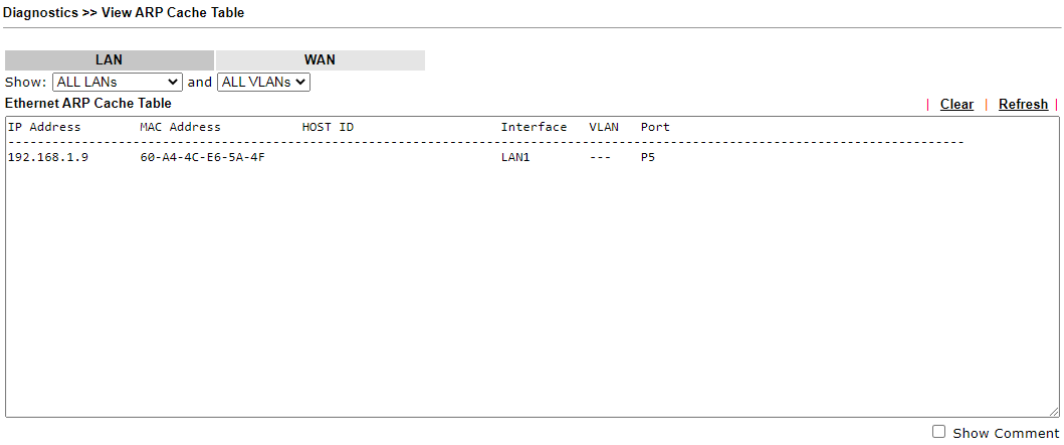


Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VII-1-3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



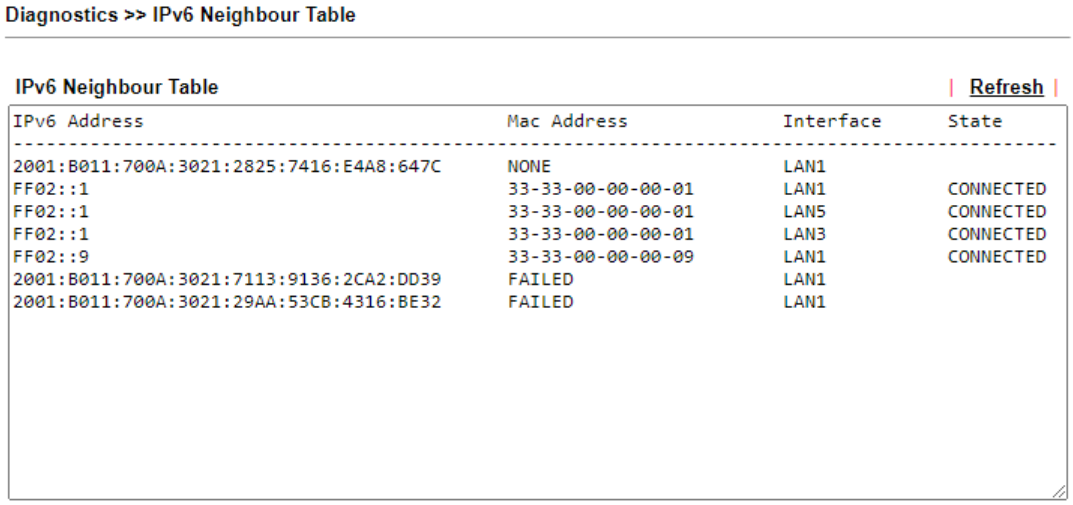
Available settings are explained as follows:

Item	Description
Show	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.

VII-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.



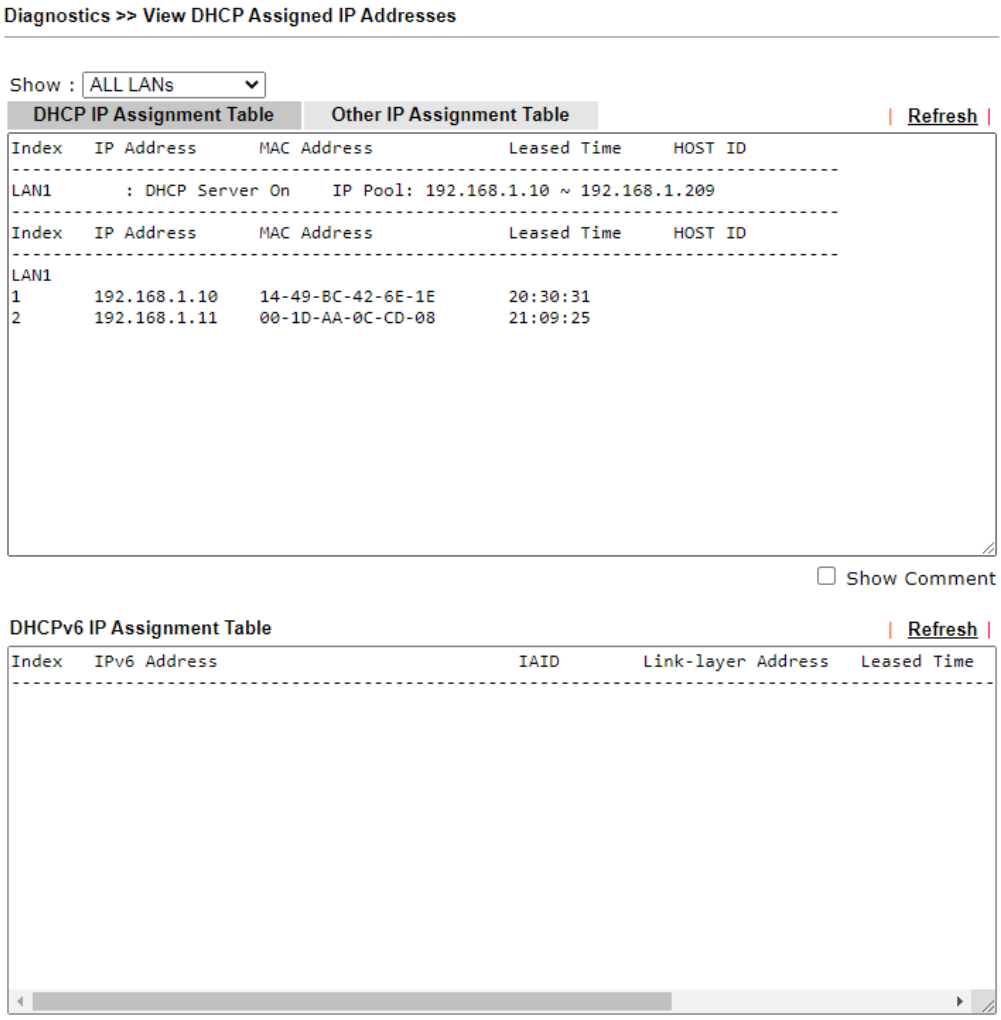
Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page with the most up-to-date information.

VII-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.

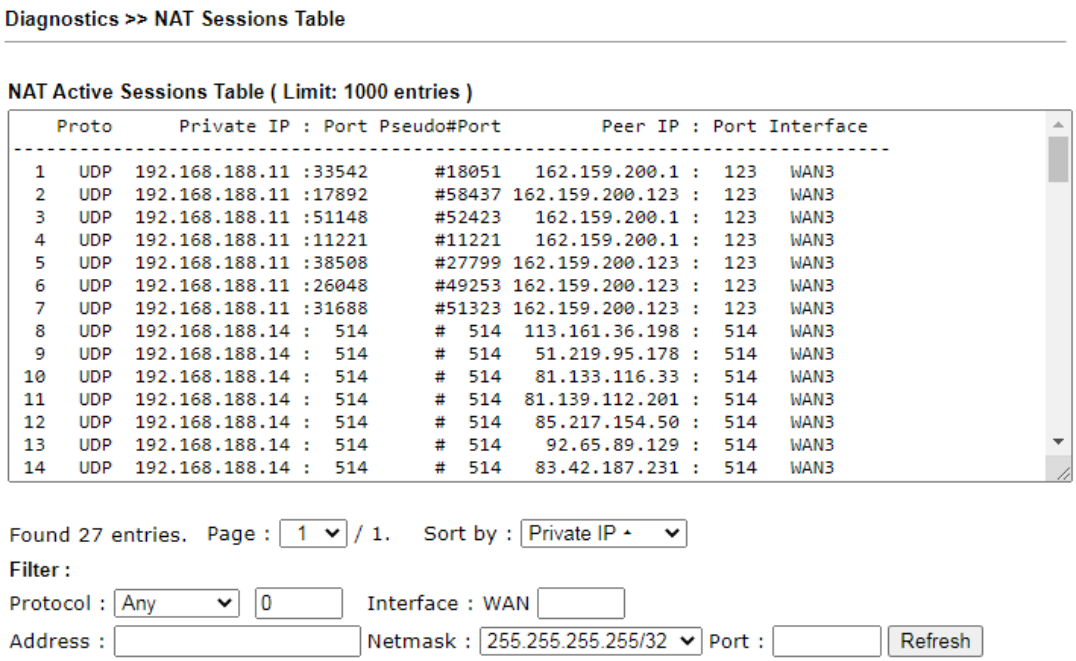


Available settings are explained as follows:

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.

VII-1-6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.



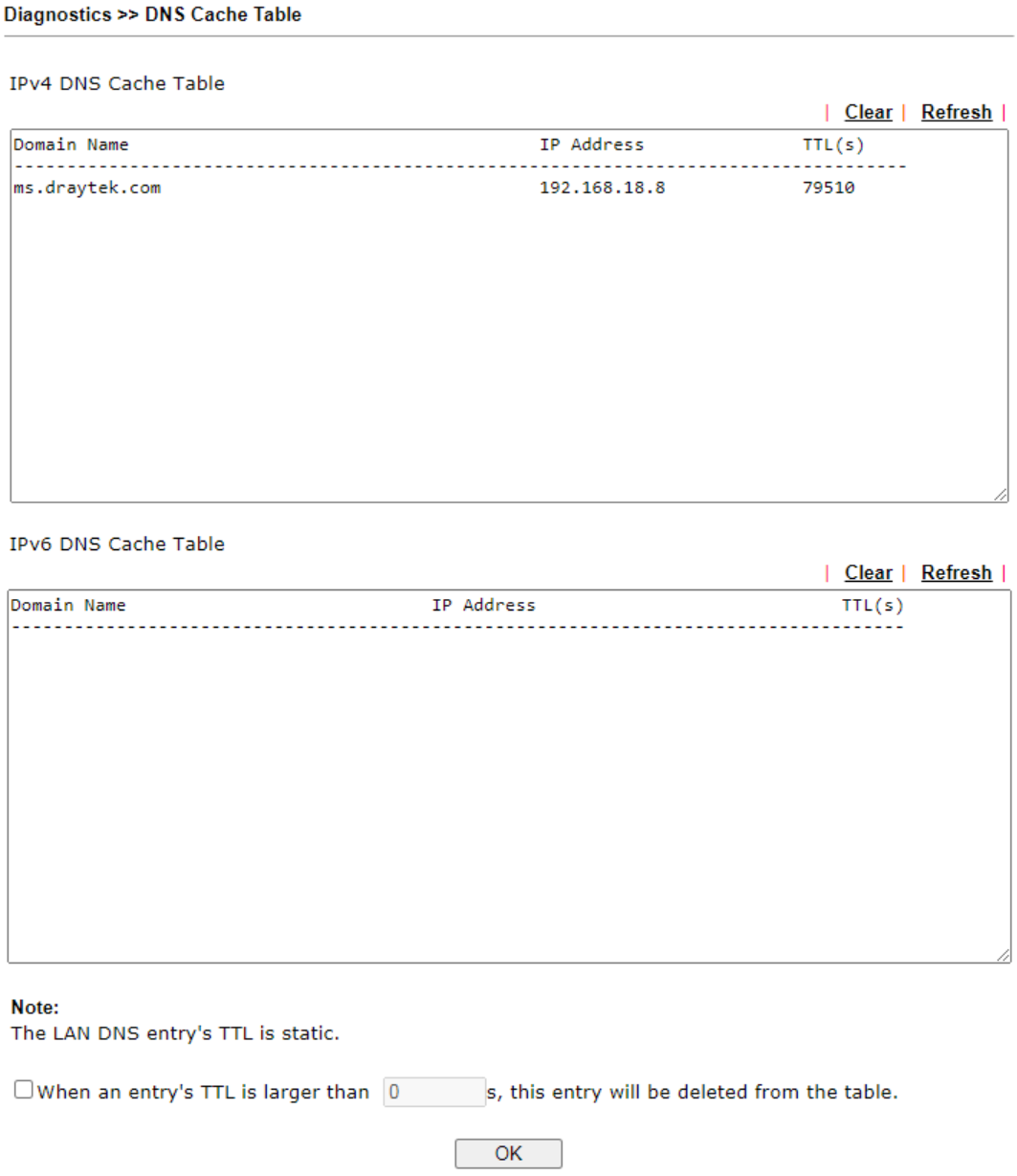
Available settings are explained as follows:

Item	Description
Private IP:	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.
Filter	Shows the sessions table according to the specified conditions.
Refresh	Click to reload this page with the most up-to-date information.

VII-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.

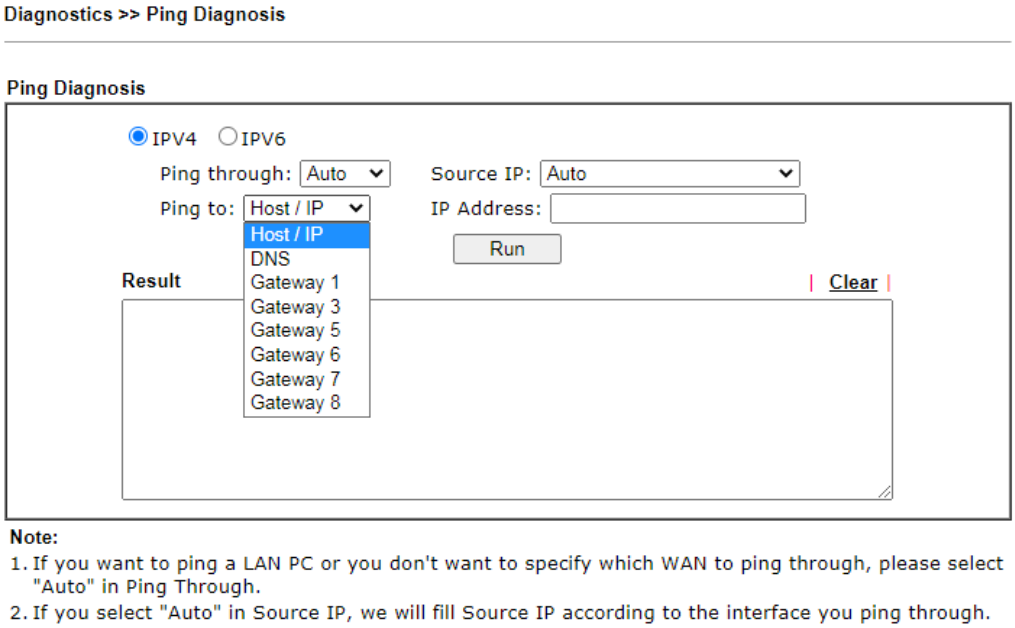


Available settings are explained as follows:

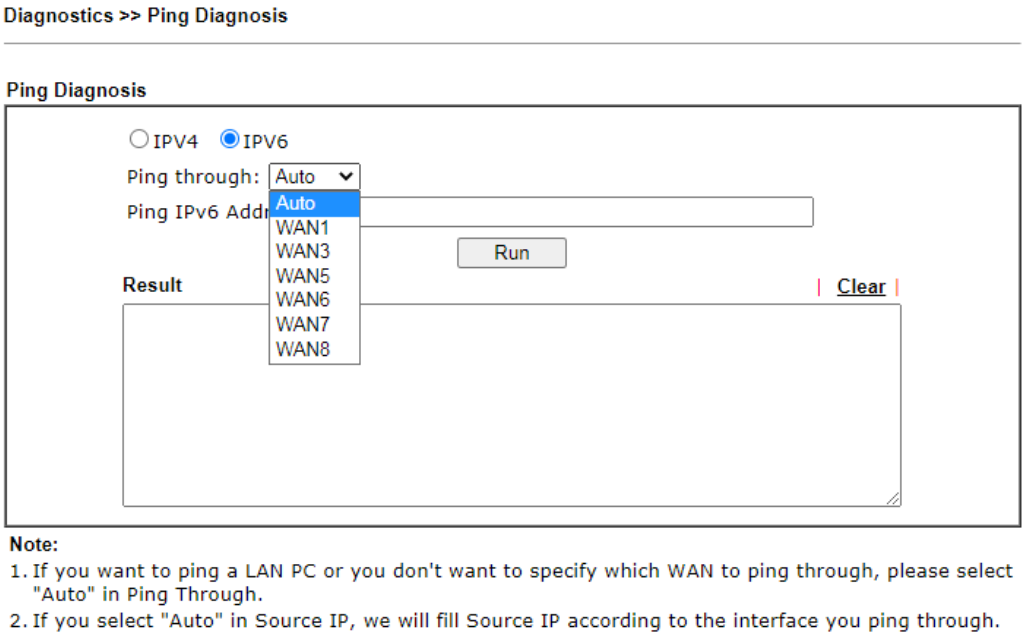
Item	Description
Clear	Click to clear all cached DNS lookup entries.
Refresh	Click it to reload the page.
When an entry's TTL is larger than….	When this box is checked, DNS entries whose TTL (time to live, in seconds) exceeds the valued specified here will be deleted from the router's cache automatically. Be sure to click OK after making changes to have them saved.

VII-1-8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to open the web page.



or



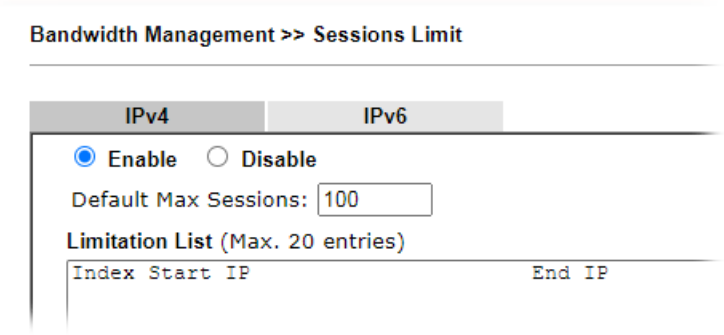
Available settings are explained as follows:

Item	Description
IPV4 / IPV6	Choose the interface for such function. Select the protocol to perform the ping operation.
Ping through	Select a WAN interface from drop down list to through which you want to perform the ping operation, or choose **Auto** to

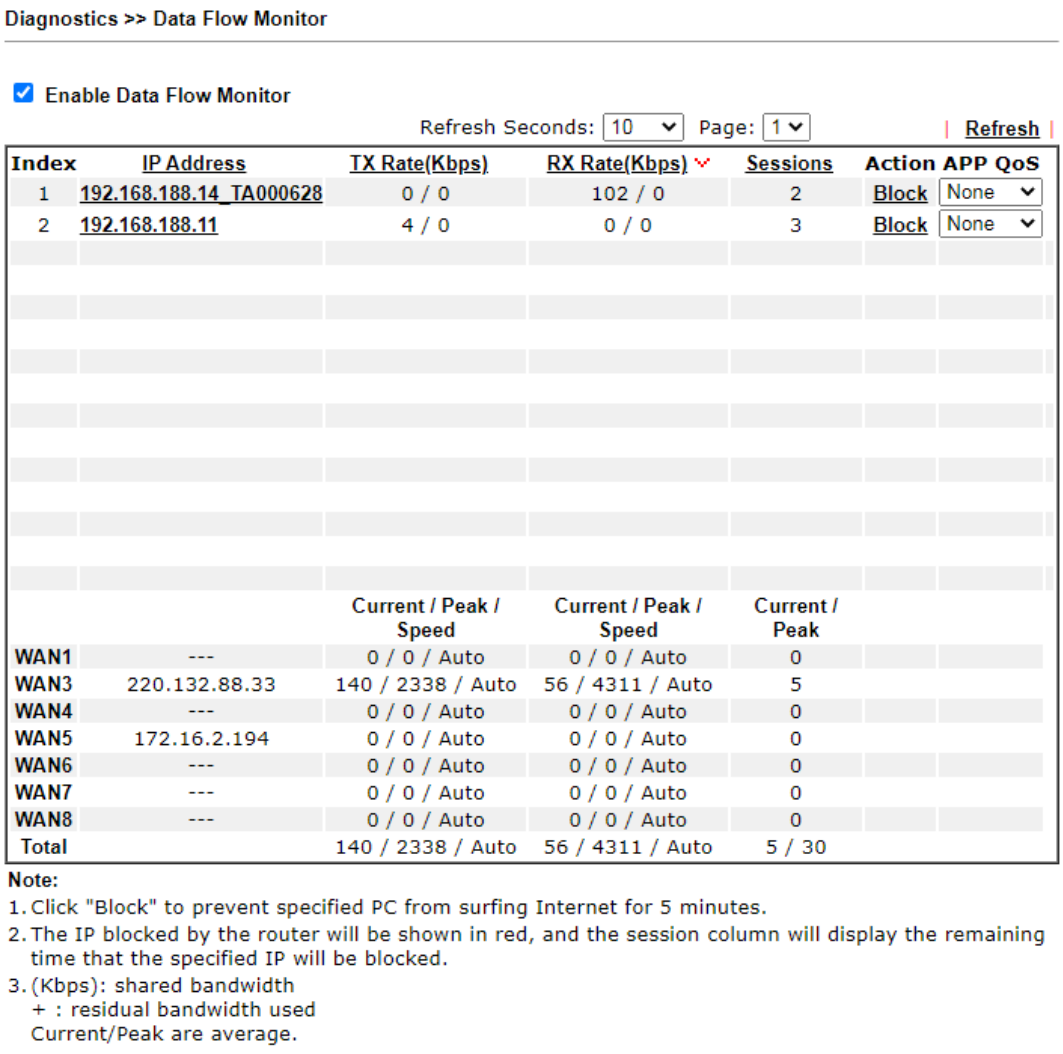
	be let the router select the WAN interface.
Ping to	Select the type of target to which you wish to ping.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Enter the IPv6 address that you want to ping.
Run	Click this button to initiate the ping process.The result will be displayed on the screen.
Clear	Click this link to clear the ping result.

VII-1-9 Data Flow Monitor

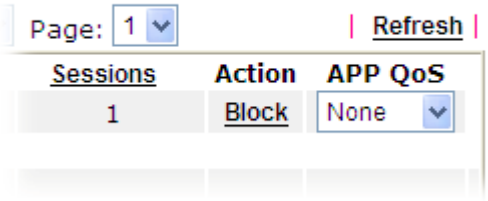
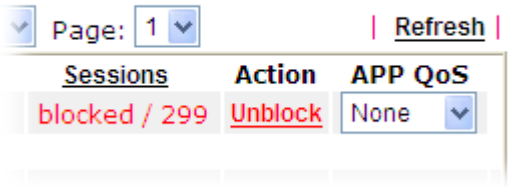
This page displays the uplink and downlink rates, and number of sessions of each LAN client. The information is refreshed at an interval specified by the user. Before using the Data Flow Monitor, LAN clients that are to be monitored need to have their IP addresses configured in Bandwidth Management, 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 **Session** links in the header to sort the displayed data.



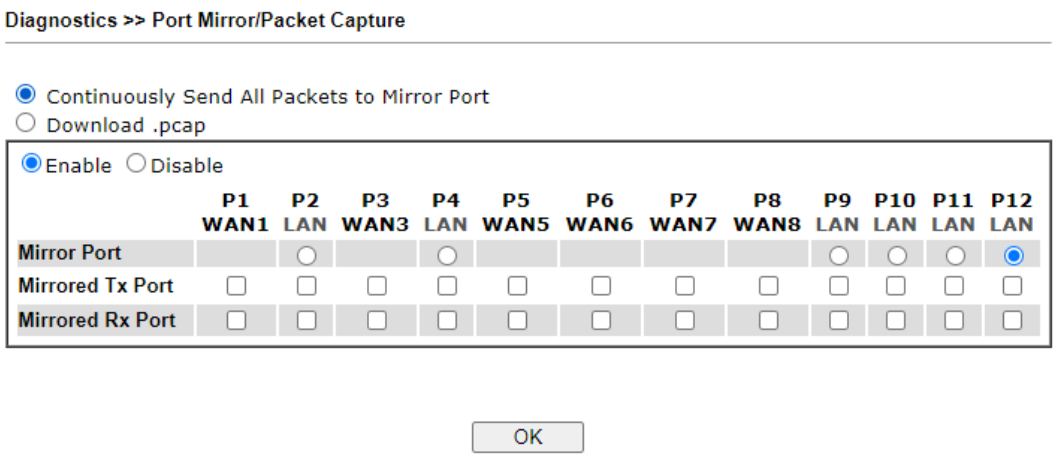
Available settings are explained as follows:

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.

VII-1-10 Port Mirror/Packet Capture

The **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.

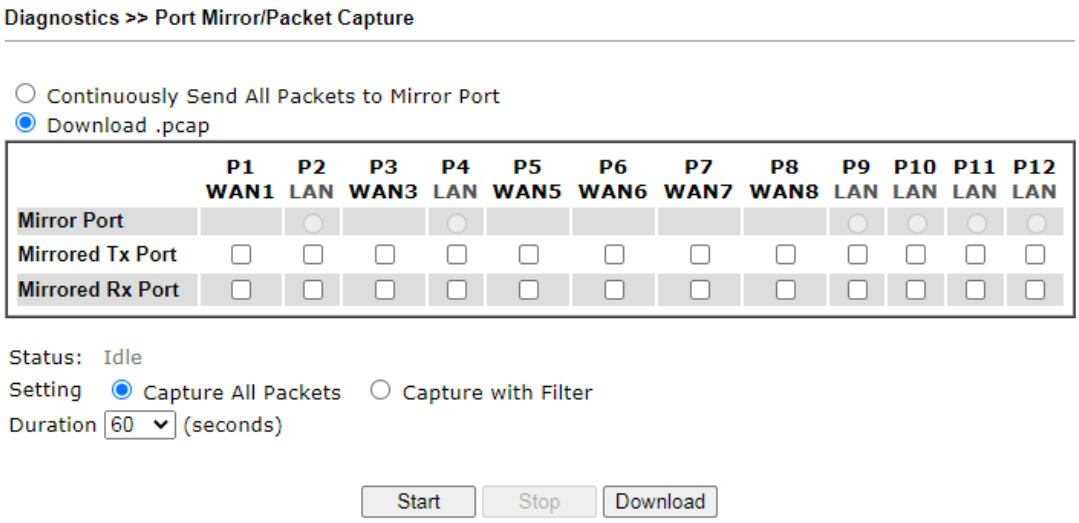
If selecing "Continuously Send All Packets to Mirror Port", the setting page will be shown as follows:



Available settings are explained as follows:

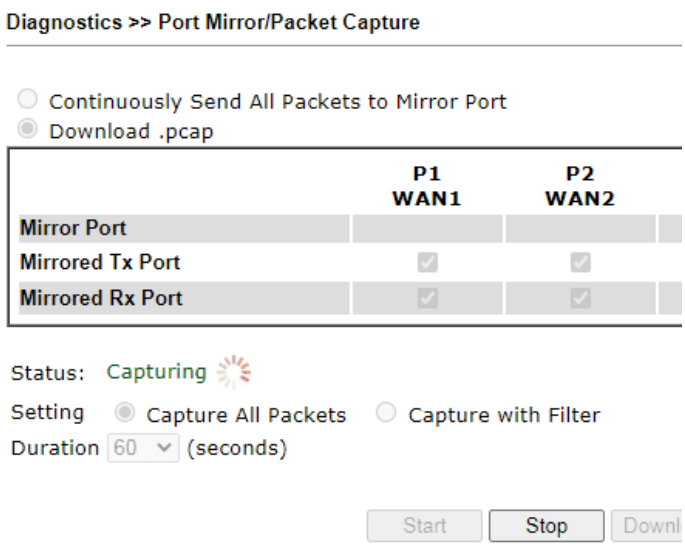
Item	Description
Continuously Send All Packets to Mirror Port	Select to send all packets to mirror port.
Enable/Disable	Select Enable to activate the function. Select Disable to cancel the function.
Mirror Port	One and only one port is selected as the mirror port, to which traffic is to be forwarded.
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.
OK	Save the settings.

If selecting "Download .pcap", the setting page will be shown as follows:



Available settings are explained as follows:

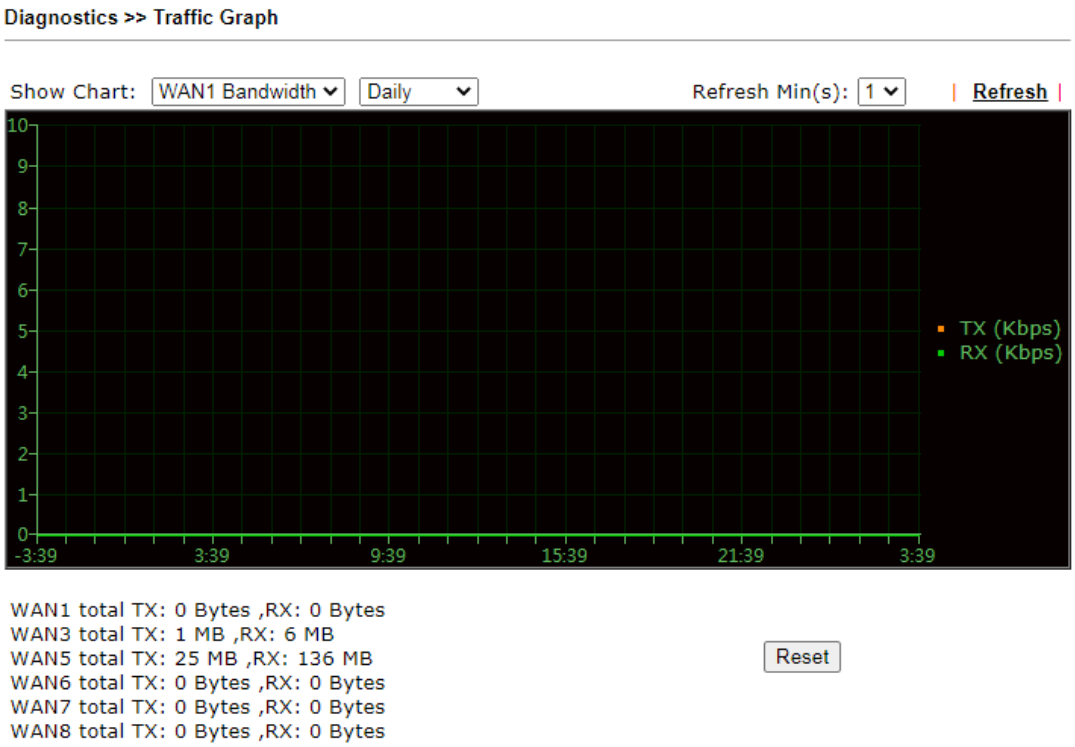
Item	Description
Download .pcap	If it is selected, the packets from the specified mirror port can be downloaded for analysis.
Mirror Port	One and only one port is selected as the mirror port, to which traffic is to be forwarded.
Mirrored Tx Port	Port(s) whose outbound traffic will be forwarded to the mirror port.
Mirrored Rx Port	Port(s) whose inbound traffic will be forwarded to the mirror port.
Setting	**Capture All Packets** - All packets will be captured for analysis. **Capture with Filter** - Only the packets filtered by ICMP, TCP, UDP, or TCP/UDP will be captured for analysis.
Duration	Set a period of time for Vigor router to capture the packets.
Filter Settings	It is available only when Capture with Filter is selected. **Protocol** - Filter the packet by using Any, ICMP, TCP, UDP, and TCP/UDP. **IP Address** - Filter the packet by IP address. If Customized IP is selected, please enter an IP address in the entry box. **Port** - It is available when TCP, UDP, or TCP/UDP is selected as the Protocol. Select Any or Customize Port. If Customize Port is selected, please enter a port number in the entry box.
Start	Click to begin the packet capturing.

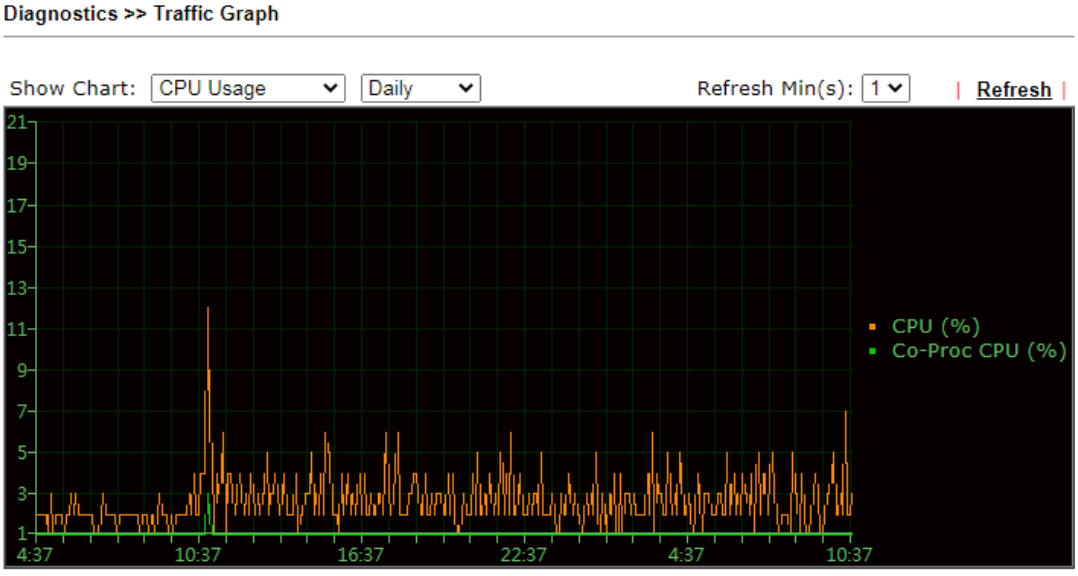
	
Stop	Click to terminate the scanning job.
Download	Click to download the packet capture result as a file with the file format,.pcap.

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

VII-1-11 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN3/WAN5/WAN6/WAN7/WAN8 Bandwidth, Sessions, 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/WAN5/WAN6/WAN7/WAN8 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

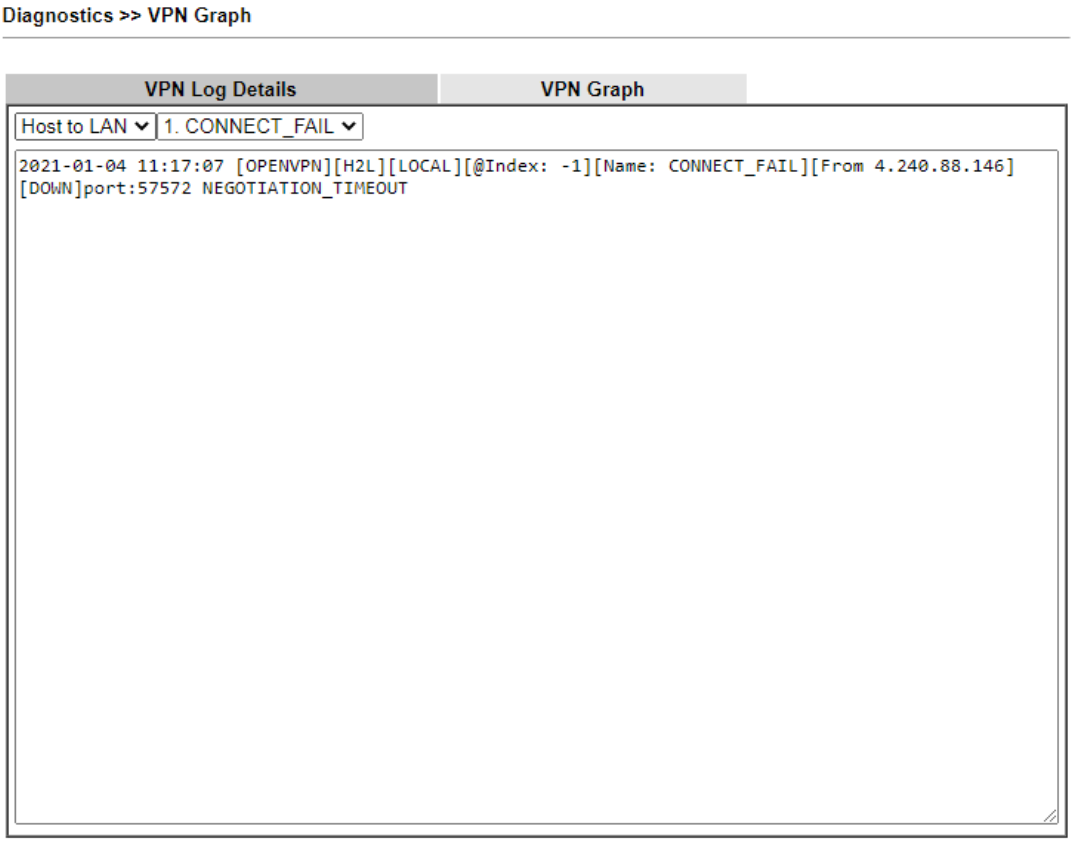
For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

VII-1-12 VPN Graph

Click **Diagnostics** and click **VPN Graph** to open the web page.

VPN Log Details

Select VPN Log Details to see log entries about VPN connections.

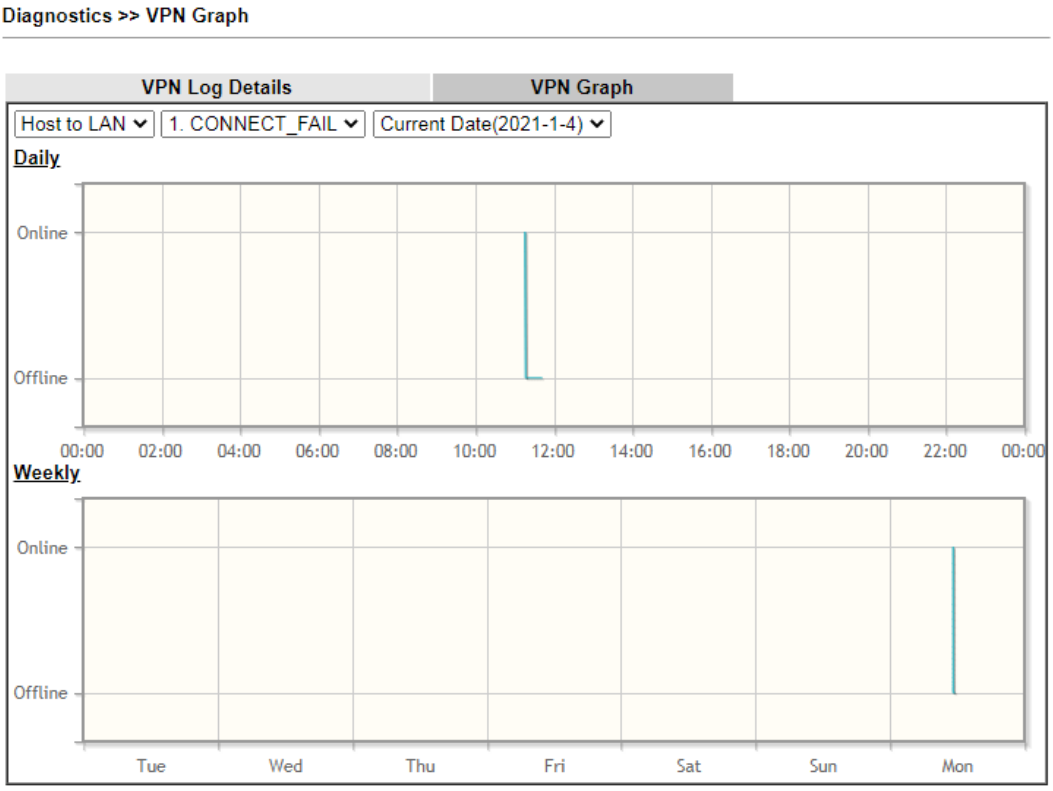


Available settings are explained as follows:

Item	Description
Host to LAN/LAN to LAN	Select Host to LAN to view log entries on VPN connections that were initiated by VPN teleworkers. Select LAN to LAN to view log entries on LAN-to-LAN VPN connections to or from this router.
Index	Select a VPN connection to view its log entries.

VPN Graph

Select this tab to see a graphical representation of VPN traffic over time.

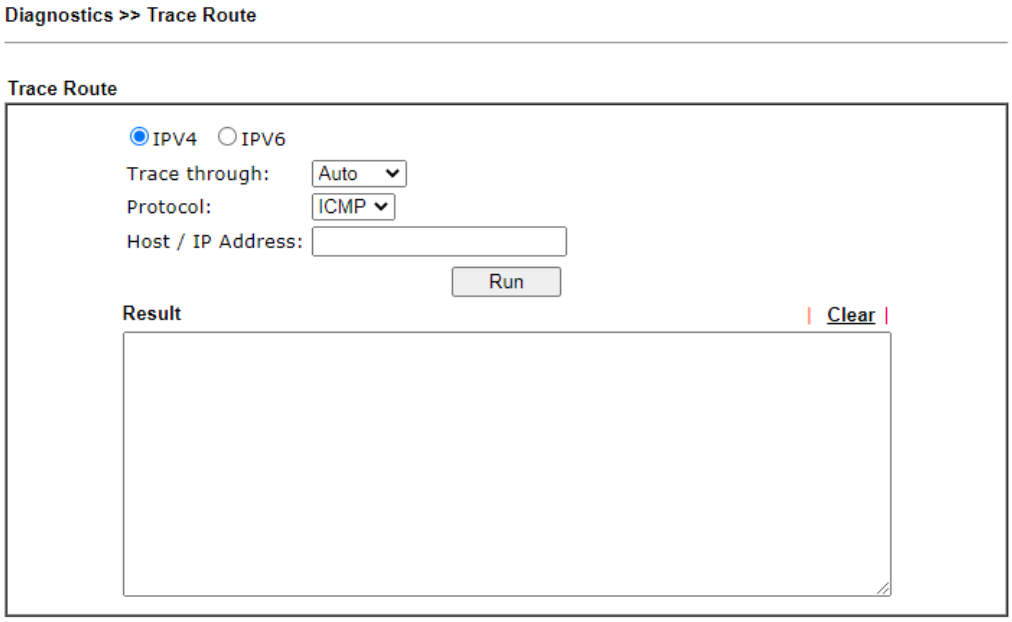


Available settings are explained as follows:

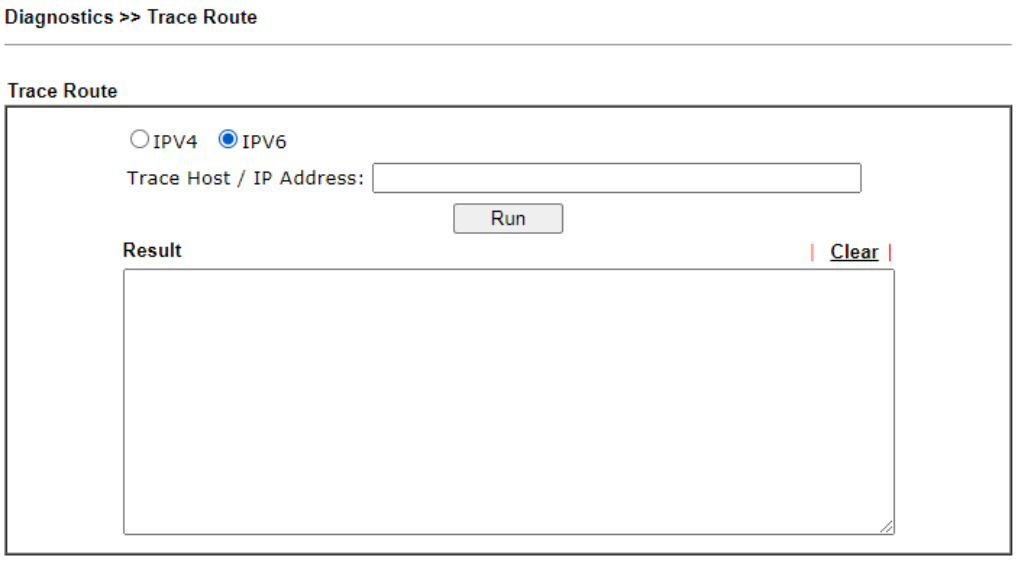
Item	Description
Host to LAN/LAN to LAN	Select Host to LAN to view log entries on VPN connections that were initiated by VPN teleworkers. Select LAN to LAN to view log entries on LAN-to-LAN VPN connections to or from this router.
Index	Select a VPN connection to view its log entries.
Date	Select the date for which you wish to view traffic statistics. The traffic information for this date will be shown in the daily graph, and the traffic information for the week before this date will be shown in the weekly graph.

VII-1-13 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:

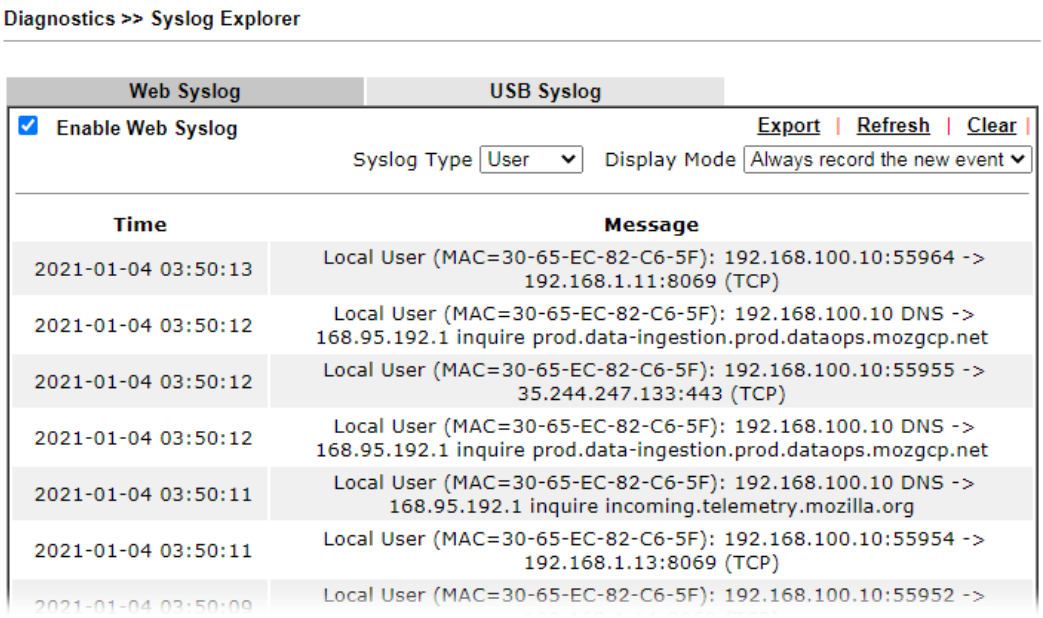
Item	Description
IPv4 / IPv6	Select the IP version used to perform the trace route.
Trace through	Select the WAN interface used to perform the trace route.
Protocol	Select either UDP or ICMP used to perform the trace route.
Host/IP Address	Enter the hostname or the IP address of trace route destination.

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.

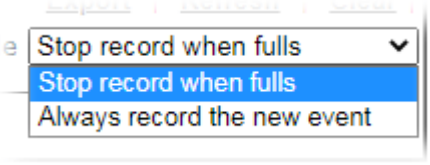
VII-1-14 Syslog Explorer

This page displays syslog information in real time. There are two options for displaying syslog information: Web Syslog and USB 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.

VII-1-15 IPv6 TSPC Status

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

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

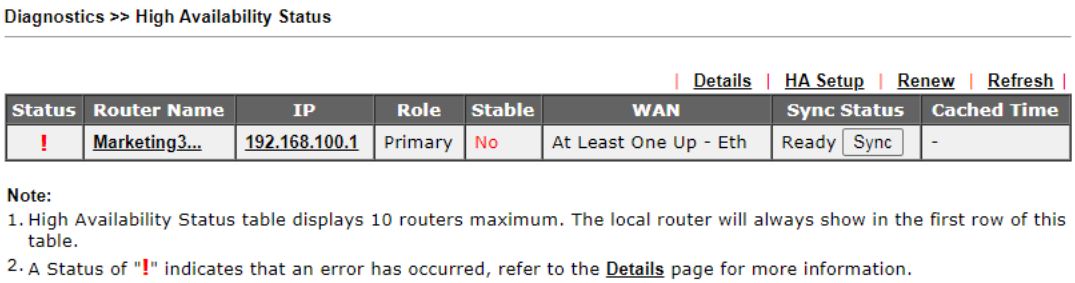
VII-1-16 High Availability Status

This page displays the High Availability status of all routers that belong to the same DARP (DrayTek Address resolution Protocol) group.

Vigor routers that satisfy the following conditions are considered to be in the same DARP group:

- HA enabled
- the same Redundancy method
- the same Group ID
- the same Authentication Key
- the same Management Interface

Open **Diagnostics>>High Availablity Status**.

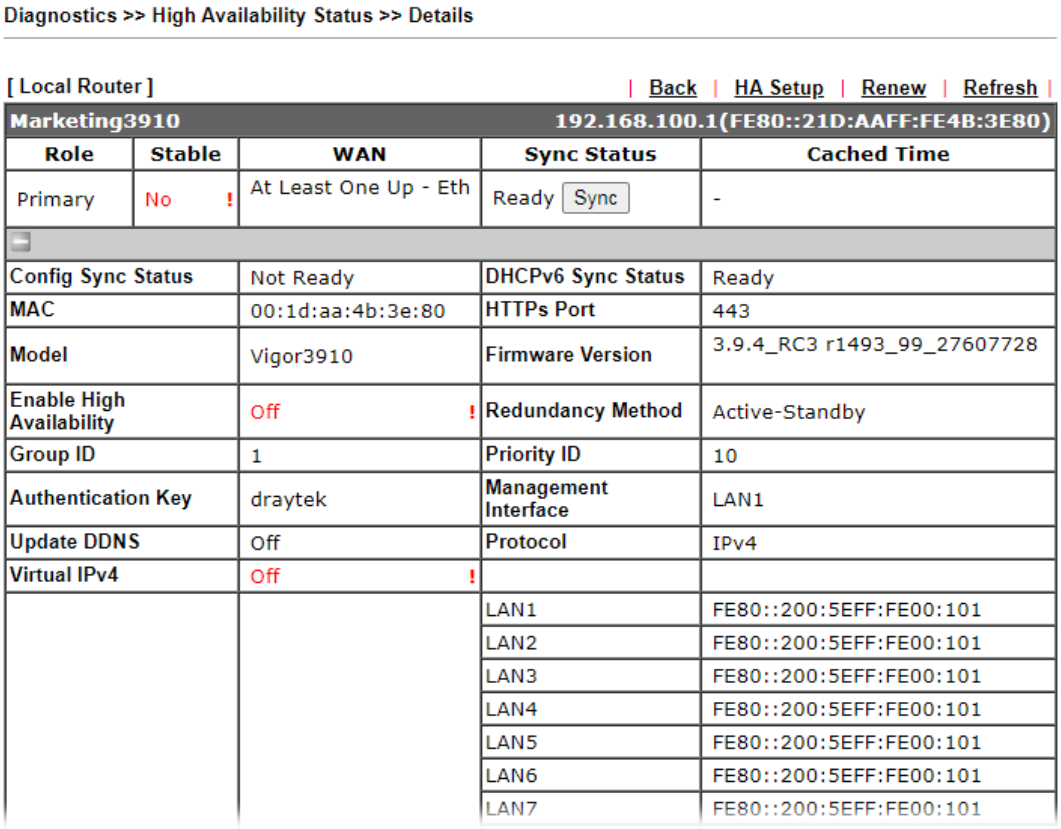


Available settings are explained as follows:

Item	Description
Details/Back	**Details –** Click to display detailed status about HA configuration for the selected router. **Back –** Click to return to the previous page.
HA Setup	Click to navigate to **Applications>>High Availability** to modify the HA configuration.
Renew	Click to get the latest status of routers other than the primary router.
Refresh	Click to get the latest status of the primary router.
Status	**"!"** means an error has occurred. Refer to **Detailed** information and modify HA settings if required.
Router Name	Display the name of the device.
IP	Display the IPv4 address of such router.
Role	"Down" means the function of HA is disabled. "Primary" means the router is the primary HA router. "Secondary" means the router is a secondary HA router.
Stable	"No" means the primary router has not been identified yet. DARP is still negotiating. "YES" means the primary router is identified.
WAN	"At Least One UP" means that at least one WAN interface is connected to Internet. "All WANs Down" means that no WAN interface is currently

	connected to Internet.
Sync Status	"Not Ready" means configuration synchronization is unable to execute, or configuration synchronization is disabled, or synchronization initialization has executed but failed. "Ready" means configuration synchronization is ready to execute. "Progressing" means configuration synchronization is in progress. "Fail" means configuration synchronization has executed and failed; or the model name is incorrect. "Equal" means the corresponding settings are equal to the primary router.
Cached Time	Displays the elapsed time since the last status update of the other routers (i.e., other than the primary router).

To view detailed information of a router, click Status, Router Name IPv4 or Details, and the following page will be shown:



Diagnostics >> High Availability Status >> Details

[Local Router] | Back | HA Setup | Renew | Refresh |

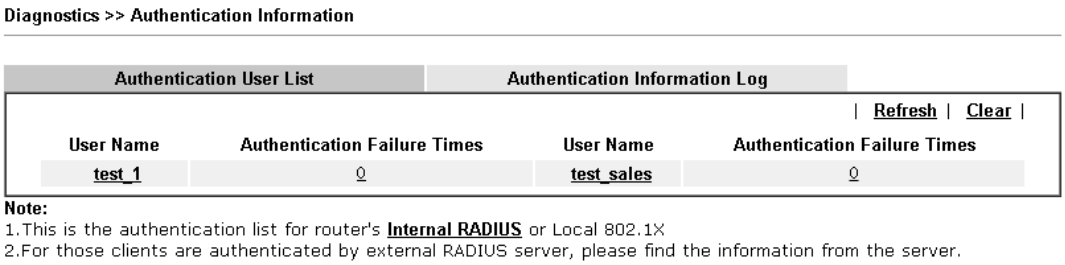
Marketing3910			192.168.100.1(FE80::21D:AAFF:FE4B:3E80)	
Role	**Stable**	**WAN**	**Sync Status**	**Cached Time**
Primary	No !	At Least One Up - Eth	Ready Sync	-
Config Sync Status		Not Ready	**DHCPv6 Sync Status**	Ready
MAC		00:1d:aa:4b:3e:80	**HTTPs Port**	443
Model		Vigor3910	**Firmware Version**	3.9.4_RC3 r1493_99_27607728
Enable High Availability		Off !	**Redundancy Method**	Active-Standby
Group ID		1	**Priority ID**	10
Authentication Key		draytek	**Management Interface**	LAN1
Update DDNS		Off	**Protocol**	IPv4
Virtual IPv4		Off !		
			LAN1	FE80::200:5EFF:FE00:101
			LAN2	FE80::200:5EFF:FE00:101
			LAN3	FE80::200:5EFF:FE00:101
			LAN4	FE80::200:5EFF:FE00:101
			LAN5	FE80::200:5EFF:FE00:101
			LAN6	FE80::200:5EFF:FE00:101
			LAN7	FE80::200:5EFF:FE00:101

VII-1-17 Authentication Information

Authentication User List

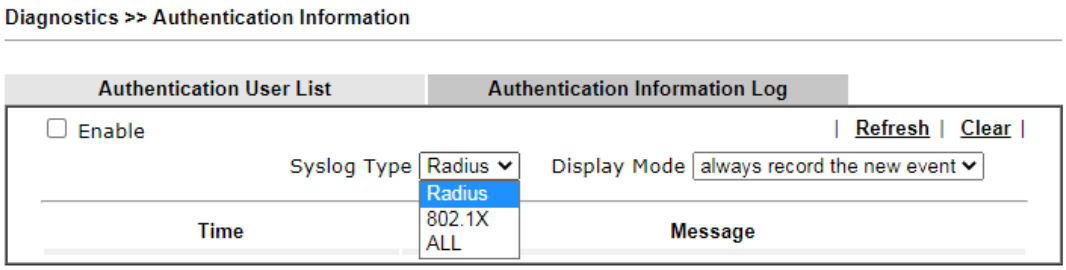
This page shows authentication requests handled by the Internal RADIUS or Local 802.1X services.

When the mouse cursor is hovered over a link under User Name, information about the RADIUS or 802.1X authentication attempt (including authentication failure information) will appear in a pop-up dialog box.



Authentication Information Log

This page will display the complete authentication log information.



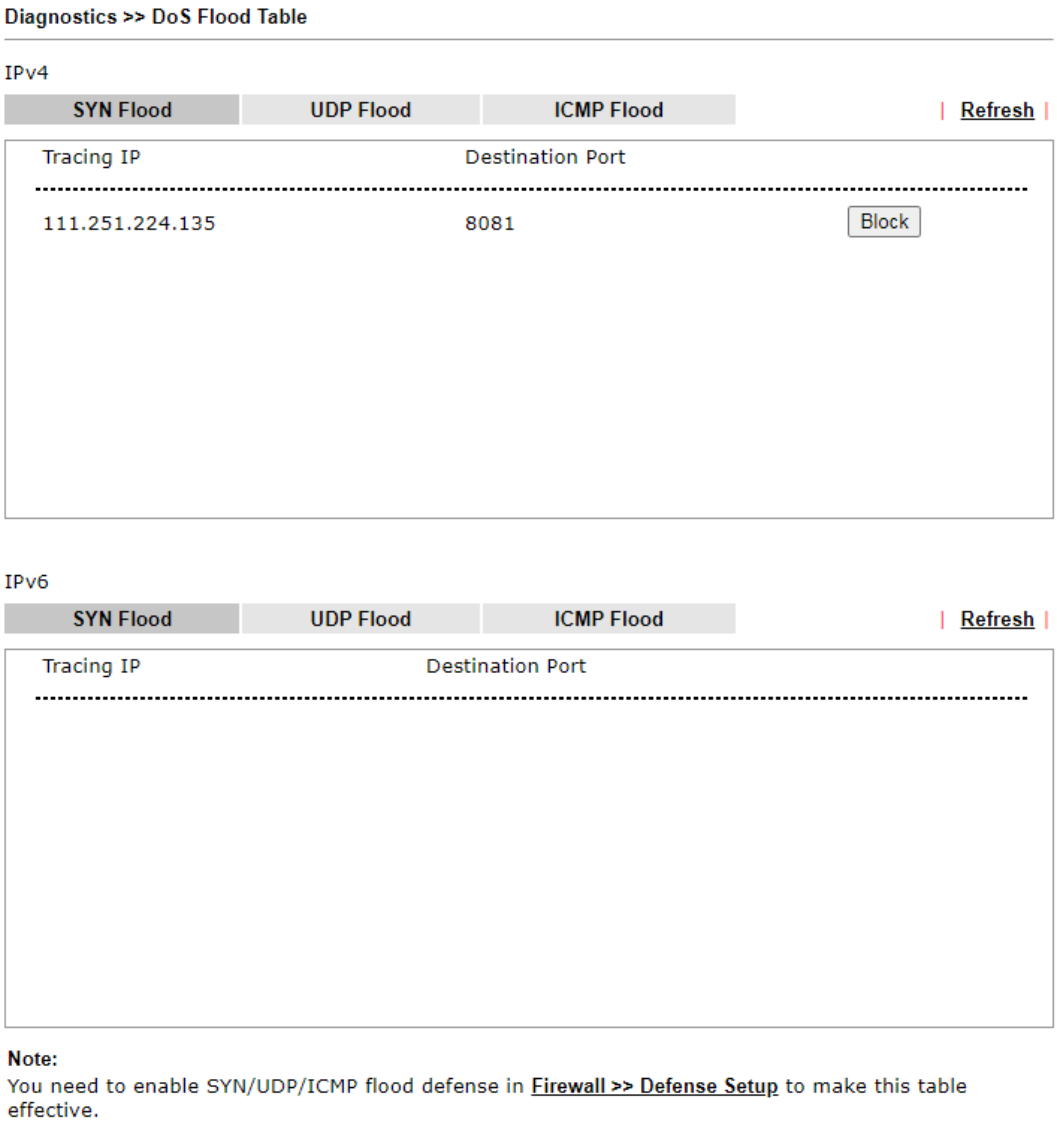
Available settings are explained as follows:

Item	Description
Enable	Check to enable Authentication Information Log.
Refresh	Click to refresh the Authentication Information Log.
Clear	Click to clear the Authentication Information Log.
Syslog Type	Select the type of authentication information to be displayed: Radius, 802.1X, or ALL (both Radius and 802.1X).
Display Mode	Choose the mode that the logging information will be shown. **Stop record when fulls** – when the buffer is full, the system will stop recording. **Always record the new event** – when the buffer is full, the oldest event will be purged to make room for the new event.
Time	Display the time of the event.
Message	Displays the details of the authentication event.

VII-1-18 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.

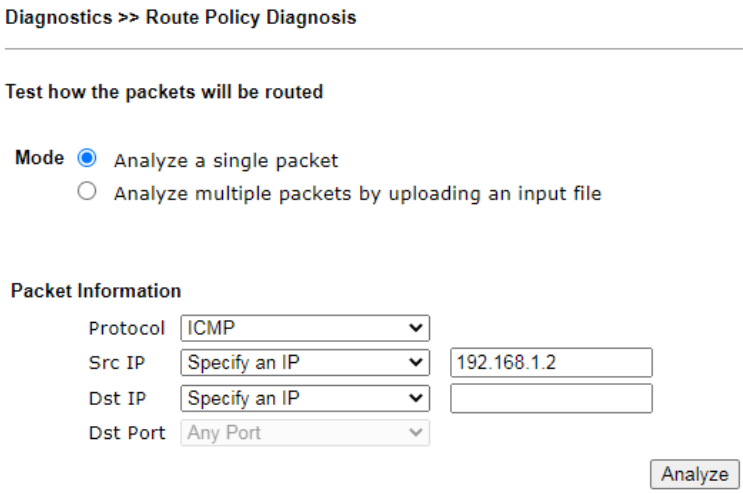


Info

The icon - (⊗) - means there is something wrong (e.g., attacking the system) with that IP address.

VII-1-19 Route Policy Diagnosis

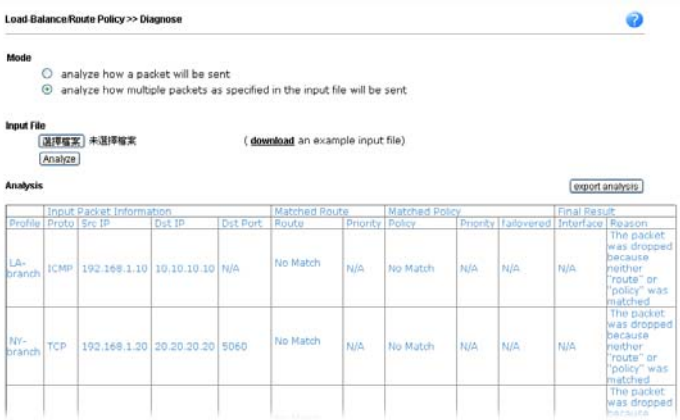
With the analysis done by such page, possible path (static route, routing table or policy route) of the packets sent out of the router can be traced.



or

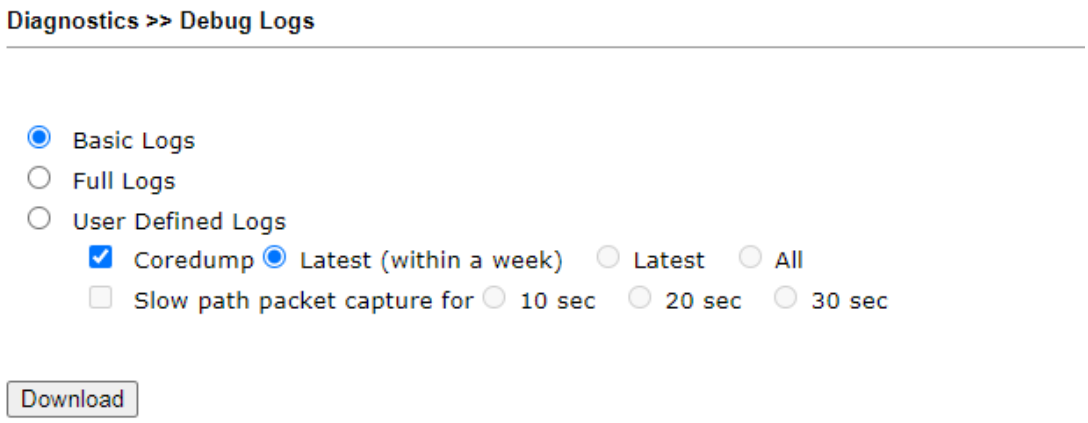
Available settings are explained as follows:

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.

VII-1-20 Debug Logs

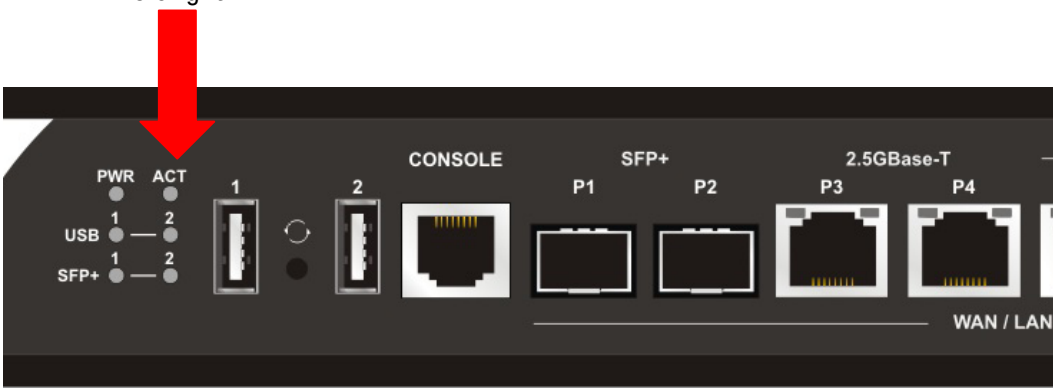
This page allows downloading the logs for debugging by a technician.



VII-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.

VII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not

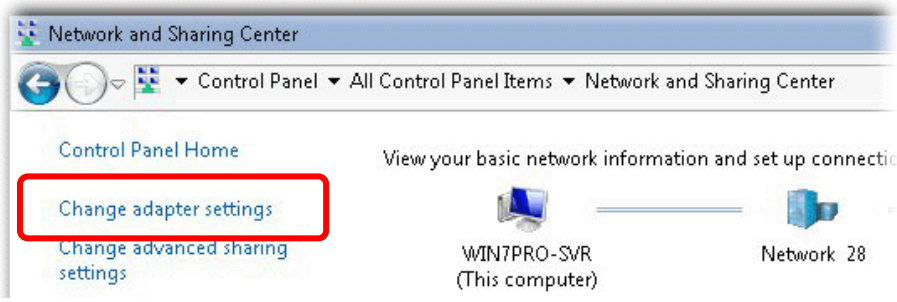
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

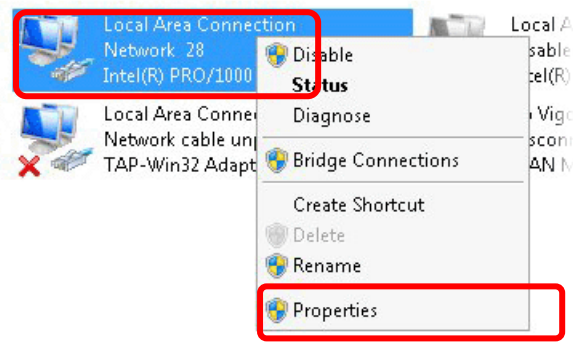
Info	The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

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

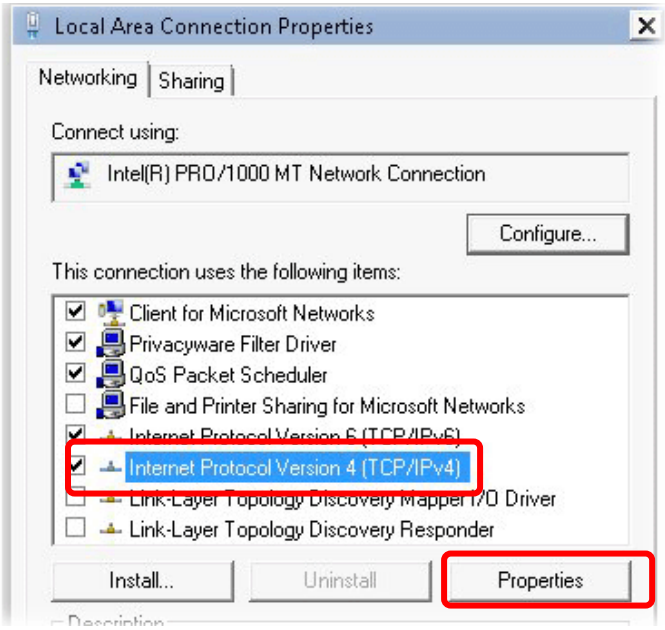
2. In the following window, click **Change adapter settings**.



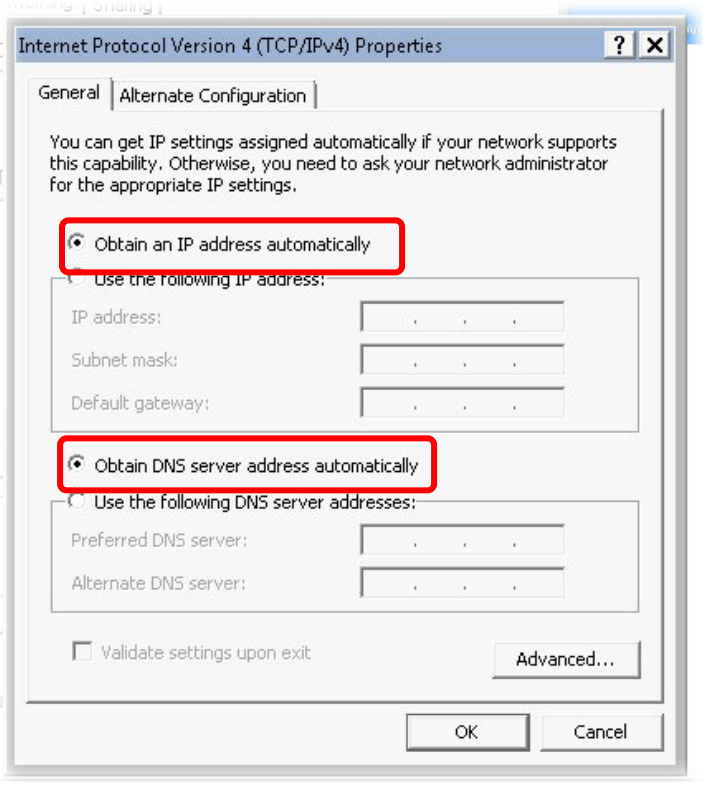
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

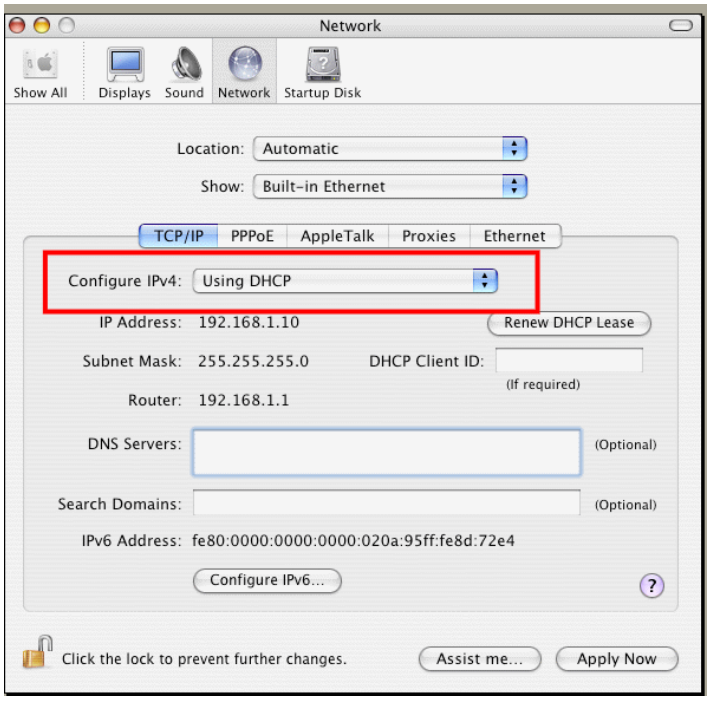


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



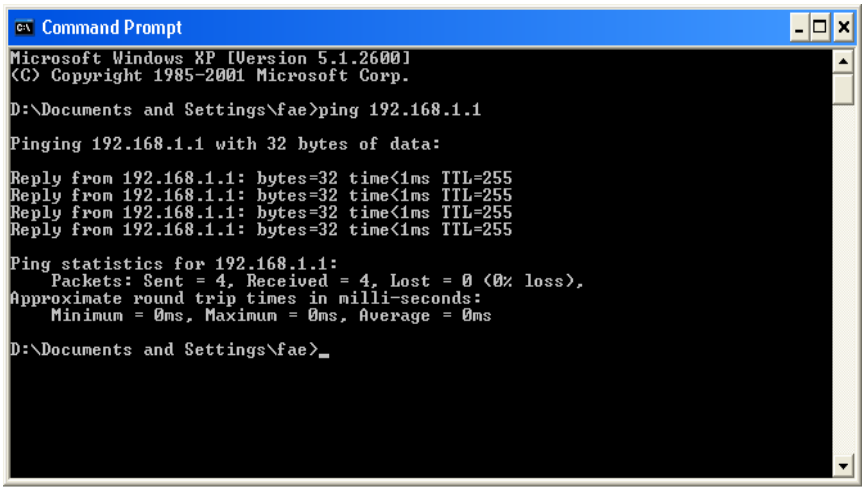
VII-4 Pinging the Router from Your Computer

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 section VIII-3)

Please follow the steps below to ping the router correctly.

For Windows

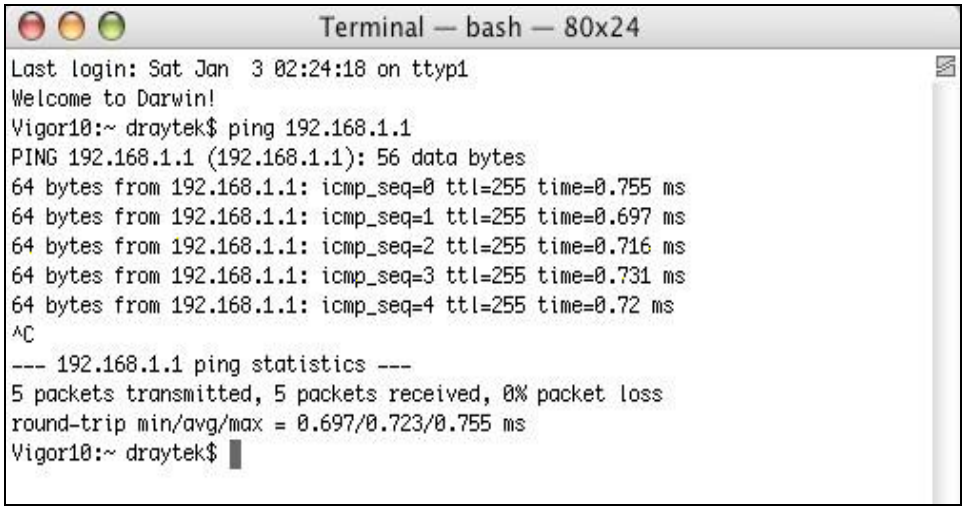
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7/8). The DOS command dialog will appear.



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

For Mac OS (Terminal)

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


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

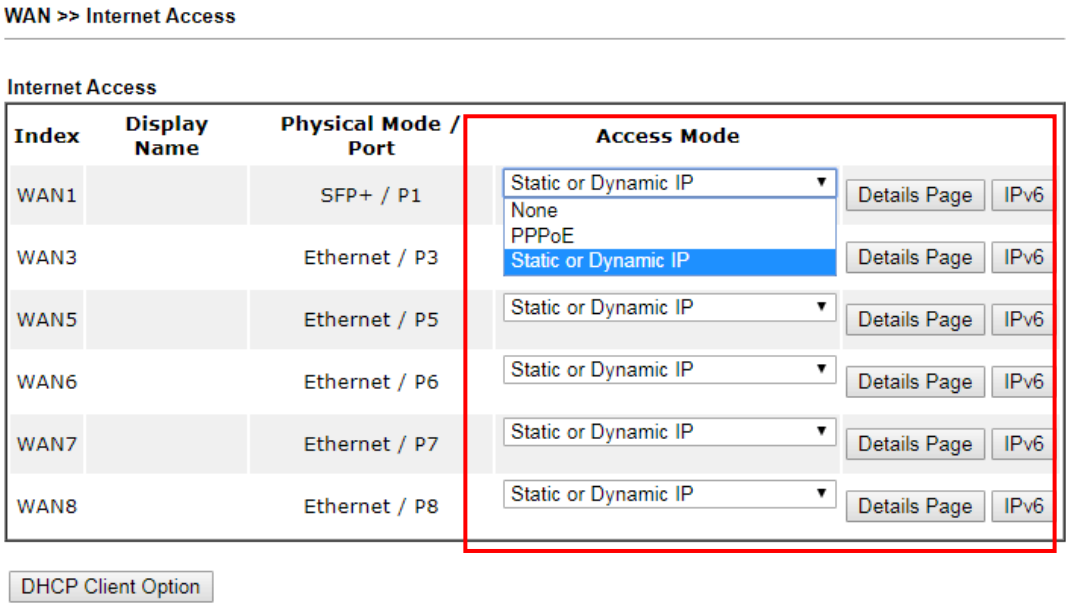
VII-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section I-1) 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~WAN8 to review the settings that you configured previously.



VII-6 Backing to Factory Default Setting If Necessary

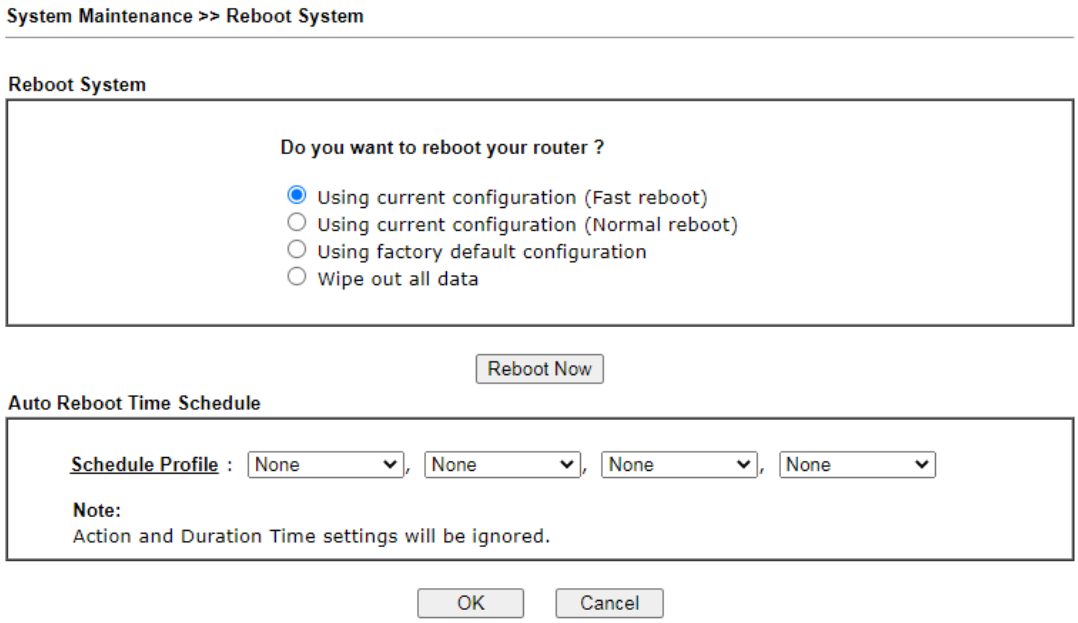
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

Info	After pressing factory default setting, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

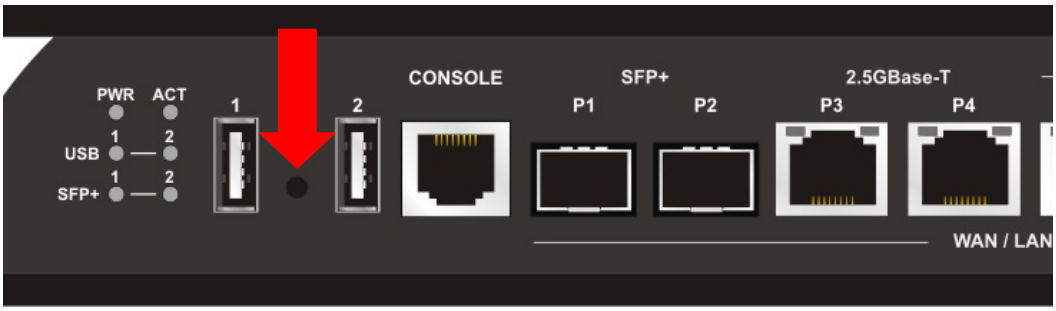
You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.



Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

VII-7 Contacting DrayTek

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

This page is left blank.

Part VIII DrayTek Tools

VIII-1 SmartVPN Client

VIII-1-1 DrayTek Android-based SmartVPN APP for the establishment of SSL VPN connection

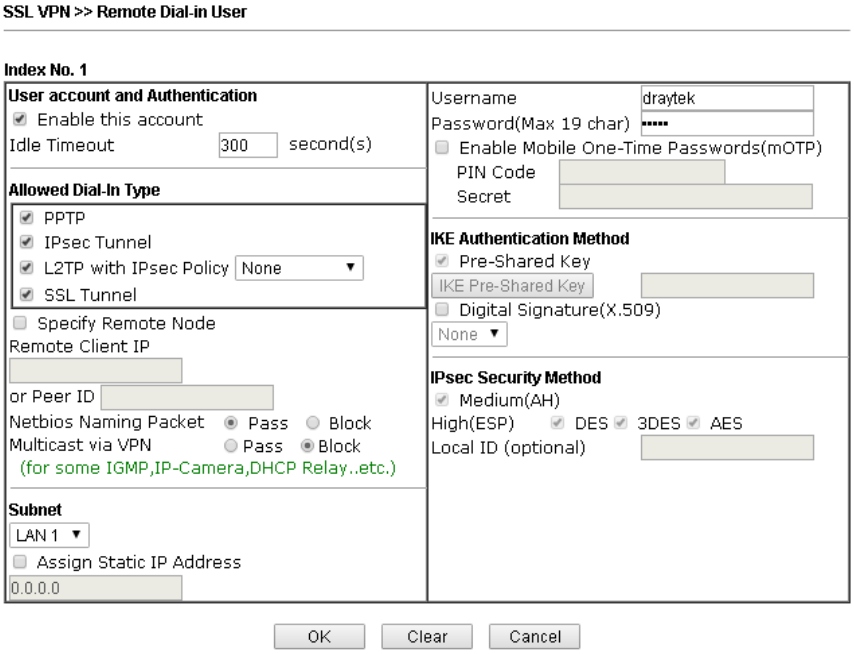
DrayTek has been the world-leading company to integrate VPN with Vigor SOHO routers to serve professionals and business customers with secure data transactions over Internet. The facilities of VPN let businesses are able to receive and send data over Internet with secure tunnels. We provide multiple protocol VPN connections such as IPSec/PPTP/L2TP protocols for secure data exchange and communication. With SSL VPN embedded on Vigor routers, teleworkers can have convenient and simple access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe.

DrayTek provided free SmartVPN for Windows-based users to easily establish VPN tunnels. There were million downloads. Now, DrayTek released Android-based SmartVPN app for those who would like to set up SSL VPN connection with the VPN server working at the main office. The SmartVPN app is available for your free download! Then, you can use the SmartVPN App on smartphone/tablet PC to establish SSL VPN tunnels with your main office.

VIII-1-2 How to Use SmartVPN Android APP to Establish SSL VPN Tunnel?

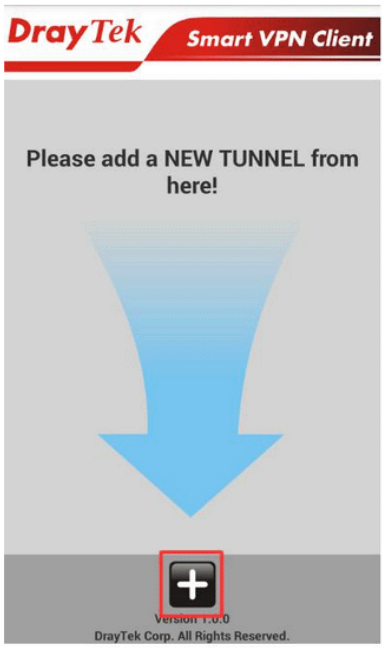
SmartVPN APP for Android is now available on Google play. This document demonstrates how to use the APP to establish a SSL VPN tunnel.

1. On VPN server, create a SSL user account. Please refer to "How to Set up SSL VPN" on www.draytek.com for detailed instructions.



2. Download the APP from Google play, and run the APP.

3. Click "+" to add a new profile.



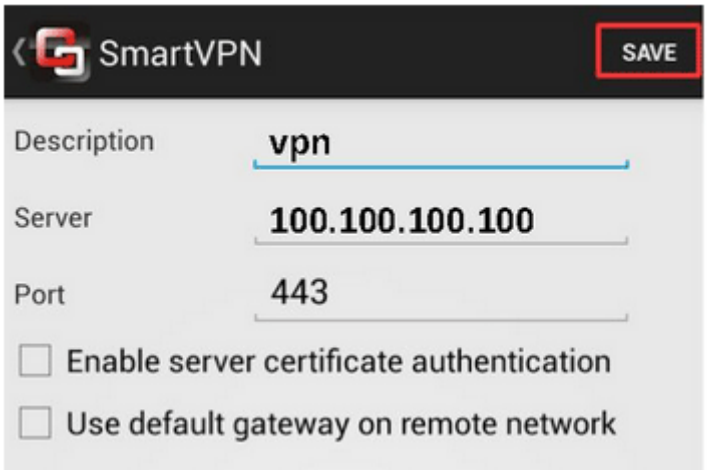
4. Edit the profile.

   a. Enter description of this profile.

   b. Enter VPN Server's IP in Server.

   c. Enter Port as the port which VPN server uses for SSL VPN; for Vigor Routers, it is 443 by default.

   d. Tap SAVE to save the profile or "<" to cancel.



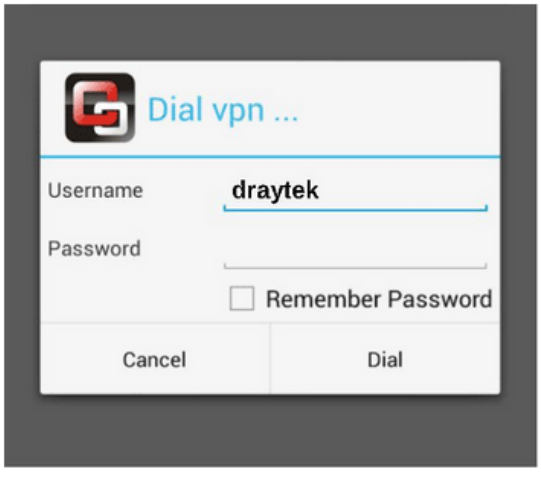
Info

Installation of relevant Root CA is required to enable server certificate authentication.

If you check "Use default gateway on remote network", all the traffic of this smart device will be forwarded to the remote gateway.

5. Tap the profile bar to establish SSL VPN tunnel.

6. Enter Username and Password, then tap Dial.



7. When the tunnel is up, the profile will turn green. Tap the bar again will disconnect the tunnel.

8. Tap the pencil icon to edit or remove the profile.

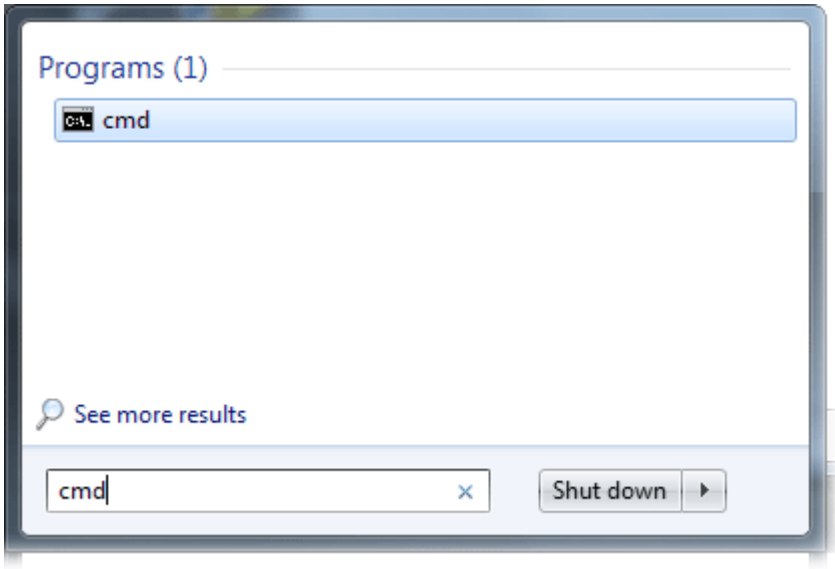
This page is left blank.

Part IX Telnet Commands

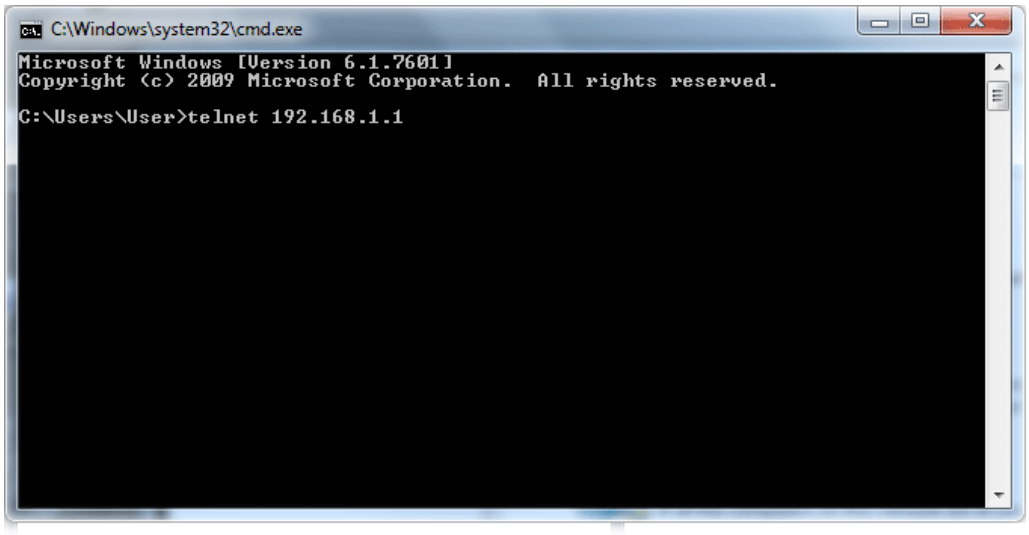
Accessing Telnet of Vigor3910

This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.

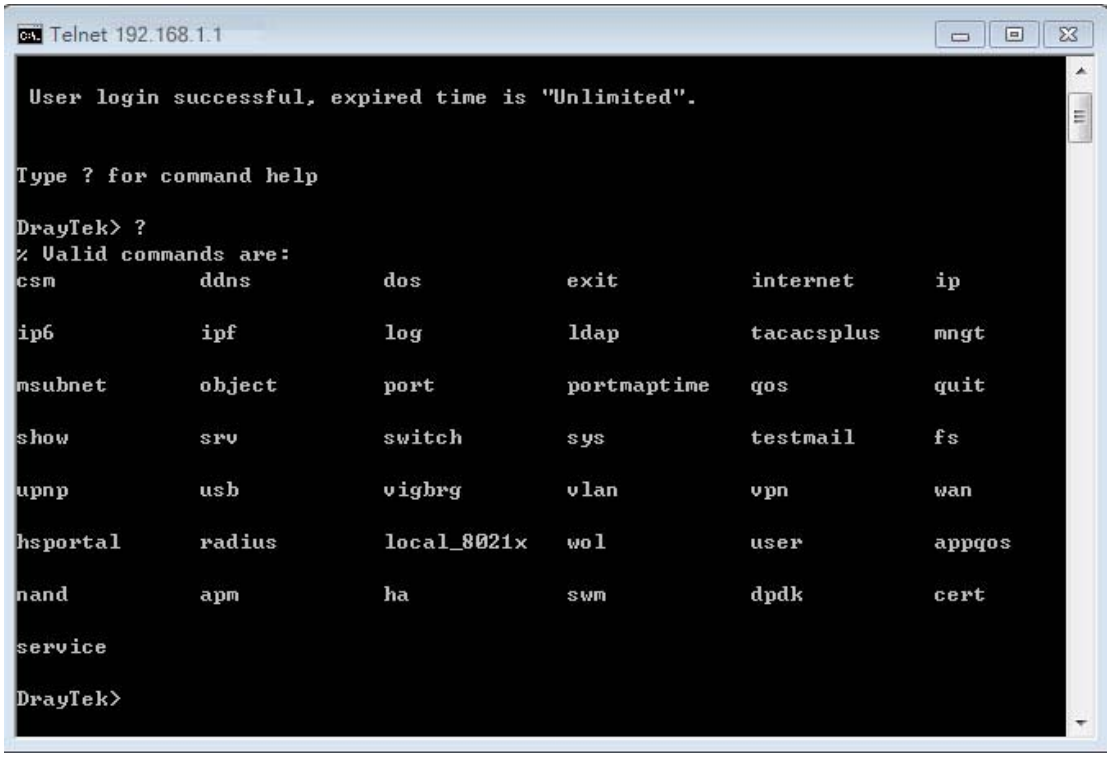
Type **cmd** and press Enter. The Telnet terminal will be open later.



In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, 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 ldap tacacsplus mngt
msubnet object port portmaptime qos quit
show srv switch sys testmail fs
upnp usb vigbrg vlan vpn wan
hsportal radius local_8021x wol user appqos
nand apm ha swm dpdk 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	Specify the index number of CSM profile, from 1 to 32.
- v	View the configuration of the CSM profile.
- n	Set a name for the CSM profile.
NAME	Specify a name for the CSM profile, less then 15 characters.
setdefault	Reset to default settings.

Example

```
> csm appe prof -i 1 -n 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.

Syntax

csm appe set *-i INDEX <-v GROUP/ -e AP_IDX / -d AP_IDX/ -p AP_IDX/-q 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.
-p	Enable the policy route for a specific application.
-q	Disable the policy route for a 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 1 -a 1 1
Profile 1 - : <NULL> action set to Pass.
>
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.

Syntax

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.

Syntax

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     A
vance Enable
 Advance abbreviation: Message, File Transfer, Game, Conference, and Other
 Advance abbreviation: : M, F, G, C, and O
-----------------------------------------------------------------
   OTHERS        TUNNEL       75            DNSCrypt           Disable
   OTHERS        TUNNEL       76            DynaPass           Disable
   OTHERS        TUNNEL       77               FreeU           Disable
   OTHERS        TUNNEL       78           HTTP Proxy          Disable
   OTHERS        TUNNEL       79          HTTP Tunnel          Disable
   OTHERS        TUNNEL       80             Hamachi           Disable
   OTHERS        TUNNEL       81       Hotspot Shield          Disable
   OTHERS        TUNNEL       82            MS Teredo          Disable
   OTHERS        TUNNEL       83              PGPNet           Disable
   OTHERS        TUNNEL       84          Ping Tunnel          Disable
.
.
.
-----------------------------------------------------------------
Total 66 APPs
>
```

Telnet Command: csm appe interface

It is used to configure APPE signature download interface.

Syntax

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**).

Syntax

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|N*

csm ucf obj *INDEX uac*

csm ucf obj *INDEX wf*

Syntax Description

Parameter	Description
show	Display all of the profiles.

setdefault	Return to default settings for all of the profile.
msg MSG	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	Specify the object for the profile.
INDEX	Specify the index number of CSM profile, from 1 to 8.
-n	Set the profile name.
PROFILE_NAME	Specify the name of the profile (less than 16 characters)
-p	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	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
MSG	Specify the Administration Message, less then 255 characters
uac	Set URL Access Control part.
wf	Set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[pass]
[ ]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- --------------------------------
```

```
 No  Grp NO.    Group Name
--- -------- --------------------------------
```

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	Specify the index number of CSM profile, from 1 to 8.
- v	View the protocol configuration of the CSM profile.
-e	Enable the function of URL Access Control.
-d	Disable the function of URL Access Control.
-a	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	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	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.

Example

```
> csm ucf obj 1 uac -i E
```

```
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[pass]
 [v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------

> csm ucf obj 1 uac -a B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[block]
 [v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------
```

Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

Syntax

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

csm ucf obj *INDEX wf -a P|B*

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 8.
- v	View the protocol configuration of the CSM profile.
-e	Enable the restriction of web feature.
-d	Disable the restriction of web feature.
-a	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	Enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
-u	Cancel the web feature configuration.
-f	Set the file extension object index number.
File_Extension_Object_index	Type the index number (1 to 8) for the file extension object.

Example

```
> csm ucf obj 1 wf -s c
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]
```

```
[ ]Enable URL Access Control
 Action:[block]
 [v] Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------

[ ]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	Display the web content filter profiles.
Look	Display the license information of WCF.
Cache	Set the cache level for the profile.
Server WCF_SERVER	Set web content filter server.

Msg MSG	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
setdefault	Return to default settings for all of the profile.
obj	Specify the object profile.
INDEX	Specify the index number of web content filter profile, from 1 to 8.
- v	View the web content filter profile.
-a	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	Set the profile name.
PROFILE_NAME	Specify the name of the profile (less than 16 characters)
-l	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
-o	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.
-w	Set the action for the black and white list. E:Enable, D:Disable, P:Pass, B:Block
-s	It means to choose the items under CATEGORY or WEB_GROUP.
-u	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes: Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating,Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers

	& Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites,Malware, Botnets, Hacking, Illegal Software, Information Security,Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government,Health & Medcine, News, Non-profits & NGOs, Personal Sites,Politics, Real Estate, Rligion, Restaurants & Dining,Shopping, Translators, General, Cults,Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

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.

Syntax

csm dnsf enable *ON|OFF*

csm dnsf syslog *N|P|B|A*

csm dnsf wcf *INDEX*

csm dnsf ucf *INDEX*

csm dnsf cachetime *CACHE_TIME*

csm dnsf blockpage *show/on/off*

csm dnsf profile_show

csm dnsf profile_edit *INDEX*

csm dnsf profile_edit *INDEX -n PROFILE_NAME*

csm dnsf profile_edit *INDEX -l N|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	Enable or disable DNS Filter. ON: enable. OFF: disable.
syslog	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.
blockpage	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. 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: Type the name of the DNS filter profile that you want to modify.
-l N|P|B|A	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
-w WCF_PROFILE	WCF_PROFILE: Type the index number of the WCF profile.
-u UCF_PROFILE	UCF_PROFILE: Type 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/a/g/o/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". a 0/1/2/3/4 [value]: Set the address type. 0=mask, 1=single, 2=any, 3=range, 4=group and objects g item_number group_index: Select the group index (for the address type set with 4, group and objects) item_number=1 or 2 (group 1 or group 2) group_index=1 to 192 o item_number object_index: Select the object index (for the address type set with 4, group and objects)

	item_number=1 or 2 (object 1 or object 2) object_index=1 to 32 s: Show the config setting. c: Clear the config setting and reset to factory default settings.

Example

```
> csm dnsf profile_setdefault
setdefault!!!
>csm dnsf cachetime 20
dns cache time set up!!!
> csm dnsf local_bw e
Enable the Block and White List.
> csm dnsf local_bw a 1 192.168.1.11
Address Type: 0:mask, 1:single, 2:any, 3:range, 4:object and group
Set the [SINGLE] Address type
> csm dnsf local_bw s
Show Block/White List information for DNS Filter Local Setting
 Block/White List:[ENABLE]
 Action:[PASS]
 Address type:[SINGLE]
 Start ip address:[192.168.1.11]
 End/Mask ip address:[0.0.0.0]
 Group 1:[0]
 Group 2:[0]
 Object 1:[0]
 Object 2:[0]
```

Telnet Command: ddns enable

This command allows users to enable or disable the DDNS service.

Syntax

ddns enable *[0/1]*

Syntax Description

Parameter	Description
0/1	0 – Disable the DDNS service. 1 – Enable the DDNS service.

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
-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	It means to type Domain Name.

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"
-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
-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>=1~14 1: WAN1 First 2: WAN1 Only 3: WAN2 First 4: WAN2 Only 5: WAN3 First 6: WAN3 Only 7: WAN4 First 8: WAN4 Only 9: WAN5 First 10: WAN5 Only 11: WAN 6 First 12: WAN6 Only example: To set WAN Interface: WAN1 First
-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
-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	Type the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 14400
%Now: 14400
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 14400
%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. [value]: value must be between 1-6

Example

```
> ddns show -i 1

------------------------------------------------

 Index: 1

 [ ] Enable Dynamic DNS Account

 WAN Interface: WAN1 First

 Service Provider: dyn.com (www.dyn.com)

 Service Type: Dynamic

 Domain Name: [].[]

 Login Name:

 [ ] Wildcards

 [ ] Backup MX

 Mail Extender:

 Determine Real WAN IP: WAN IP


DrayTek>
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

Syntax

dos <*-V | D | A*>

dos <*-s ATTACK_F <THRESHOLD><TIMEOUT>*>

dos <*-a | e <ATTACK_F><ATTACK_0> | 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*>

dos -o <*0/1*>

dos -p <*0/1*>

dos -l <*0/1/2/3*>

dos -f <*0/1/show*>

dos -i <*/1/2/3/4/show*>

Syntax Description

Parameter	Description
-V	View the configuration of DoS defense system.
-D	Deactivate the DoS defense system.

-A	Activate the DoS defense system.
-s	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	Enable the defense function for all attacks listed in ATTACK_0.
-e	Enable defense function for a specific attack(s).
ATTACK_0	Specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	Disable the defense function for a specific attack(s).
-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.
-o <0/1>	Enable/Disable dos defense log. 0: Disable 1: Enable
-p <0/1>	Enable/Disable spoofing defense log.

	0: Disable 1: Enable
-l <0/1/2/3>	Enable/Disable dos defense black/white list log. 0: None 1: White list 2: Black List 3: All
-f <0/1/show>	Set the priority of white list / black list. 0: White list 1: Black List show: Show the setting result
-i </1/2/3/4/show>	Set the time interval for sending the log. 1: 30 seconds 2: 60 seconds 3: 180 seconds 4: 300 seconds

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
-W n	W means to set WAN interface. 1=WAN1, 2=WAN2,…. Default is WAN1.
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 7)

	n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP n=4: PPTP with Dynamic IP, n=5: PPTP with Static IP, n=6: L2TP with Dynamic IP n=7: L2TP with Static IP
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-S <isp name>	Set ISP Name (max. 23 characters).
-P <on/off>	Enable PPPoE Service.
-u <username>	Set username (max. 49 characters) for Internet accessing.
-p <password>	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	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>	Assign gateway IP for such WAN connection.
-s <server ip>	It means to set PPTP/L2TP Server IP. <server ip>= ppp.qqq.rrr.sss: PPTP/L2TP server IP
-A <idx>	It means to set Always On mode, and <idx> as backup WAN#.
-B <mode>	It means to set Backup mode. <mode> 0: When any WAN disconnect; 1: When all WAN disconnect.
-V	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.
-U n	(DHCP mode) MTU(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
> internet -W 1 -M 1 -u link1 -p link1 -a 0
 You are going to watching and setting in WAN 1
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 Username set to link1
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
>
```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the IP routing subnet for your router.

Syntax

ip pubsubnet <*Enable/Disable*>

Syntax Description

Parameter	Description
Enable	Enable the function.
Disable	Disable the function.

Example

```
> ip 2ndsubnet enable
public subnet enabled!
```

Telnet Command: ip pubaddr

This command allows to set the **IP routed subnet** for the router.

Syntax

ip pubaddr *?*

ip pubaddr <*public subnet IP address*>

Syntax Description

Parameter	Description
?	Display 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 lanalias

This command is used for configuring LAN IP Alias.

Syntax

ip lanalias <*idx***><***option***>**

Syntax Description

Parameter	Description
<*idx***>**	It means the index number of the profile. Idx: 1 to 5
<option>	The available commands with parameters are listed below.

-e <0/1>	It means to enable / disable the function of .. 0: disable 1: enable
-a <IP address>	It means to set auxiliary IP address.
-w n	It means to add an address for the selected WAN interface (1 to 5). N=0, none N=1, means WAN1 N=2, means WAN2 …
-r	Delete an existed WAN IP address.

Example

```
> ip lanalias 1 -a 192.168.1.56
>
```

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	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	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 *[0/1/2/3/4/5status]*

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	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 status
[ARP Table]
 Index IP Address     MAC Address        Netbios Name    Interface  VLAN   Port
   1   192.168.1.5    00-05-5D-E4-D8-EE                  LAN1       VLAN0  P1


>
```

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. -h: display usage -l: list all custom set DHCP options -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 -u: update by index number -v: set option value by string -w: set WAN number (e.g., 1=WAN1) -x: set option value by raw byte (hex)
release	It means to release current WAN IP address.
renew	It means to renew the WAN IP address and obtain another new one.
status	It displays current status of DHCP client.

Example

```
> ip dhcpc option -e 1 -w 1/2 -c 18 -v /path1
> ip dhcpc option -e 0 -w 2/6/7 -c 18 -x 2f70617468
% DHCP client option number and wan settings are duplicate!

> ip dhcpc option -e 0 -w 3/6/7 -c 18 -x 2f70617468
> 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:

DHCP Client Status: None active DHCP client!

=====================================
WAN5:

DHCP Client Status: None active DHCP client!

=====================================
WAN6:

DHCP Client Status: None active DHCP client!


=====================================
WAN7:

DHCP Client Status: None active DHCP client!


=====================================
WAN8:  <Virtual WAN>
```

```
DHCP Client Status: None active DHCP client!


====================================
WAN9:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN10:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN11:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN12:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN13:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN14:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN15:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
```

```
WAN16:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN17:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN18:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN19:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN20:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN21:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN22:  <Virtual WAN>

DHCP Client Status: None active DHCP client!


====================================
WAN23:  <Virtual WAN>

DHCP Client Status: None active DHCP client!
...
```

```
...
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2 for verifying if the WAN connection is OK or not.

Syntax

ip ping *[IP address] [AUTO/WAN1/WAN2] [Source IP Address]*

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.
AUTO/WAN1/WAN2	It means the WAN port 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 / WAN2 / WAN3 / WAN4 / WAN5 / WAN6 / WAN7 / WAN8 / WAN9 / WAN10 / WAN11 / WAN12] [Udp/Icmp]*

Syntax Description

Parameter	Description
IP address	The target IP address.
WAN1 ~ WAN12	It means the WAN port that the above IP address passes through.
Udp/Icmp	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	Type 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 and 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: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 **Note**: PVC3 ~PVC5 are virtual WANs.
-e	It means to disable or enable RIP setting for specified WAN interface. 1: Enable the function of setting RIP of WAN IP. 0: Disable the function.

Example

```
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol disable
> ip wanrip 5 -e 1
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol 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 *tel*

ip route *default [wan1/wan2/off/?]*

ip route *clean [1/0]*

Syntax Description

Parameter	Description
add	It means to add an IP address as static route.
del	It means to delete specified IP address.
status	It means current status of static route.
dst	It means the IP address of the destination.
netmask	It means the netmask of the specified IP address.
gateway	It means the gateway of the connected router.
ifno	It means the connection interface. 3=WAN1, 4=WAN2, 5=WAN3, 6=WAN4
rtype	It means the type of the route. default : default route; static: static route.
cnc	It means current IP range for CNC Network.
tel	It means to display current IP range for China Telecom Network.
default	Set WAN1/WAN2/off as current default route.
clean	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~       192.168.9.0/   255.255.255.0 is directly connected, DMZ
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 *query*

ip igmp_proxy *ppp <0/1>*

ip igmp_proxy *status*

ip igmp_proxy *version*

ip igmp_proxy *syslog*

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.
query	It means to set IGMP general query interval. The default value is 125000 ms.
ppp <0/1>	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 specify the IGMP version. v2, v3, auto, show
Syslog <0/1>	Make IGMP log be recorded on syslog. 0: disable 1: enable

Example

```
> ip igmp_proxy set
% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
> ip igmp_proxy status
%% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
%%% igmp_proxy WAN:
    239.255.255.250    state=1
    239.255.255.250    timer=0
```

Telnet Command: ip igmp_snoop

This command is used to enable/disable igmp snoop server.

Syntax

ip igmp_snoop *enable*

ip igmp_snoop *disable*

ip igmp_snoop *status*

ip igmp_snoop *table*

ip igmp_snoop *txquery <on|off><v2|v3>*

ip igmp_snoop *mode <hw/sw>*

ip igmp_snoop *chkleave <on|off>*

ip igmp_snoop *separate <on|off>*

ip igmp_snoop *portchk <on|off>*

Syntax Description

Parameter	Description
enable	It means to enable proxy server.
disable	It means to disable proxy server.
status	It means to display current status for proxy server.
table	Display the whole table of IGMP Snoop configuration.
txquery <on|off><v2|v3>	IGMP query will be sent out to LAN periodically.
mode <hw/sw>	Make IGMP snooping work on software or hardware.
chkleave <on|off>	Off – Vigor router will drop LEAVE if clients still on the same group.
separate <on|off>	On – IGMP packets will be separated by NAT/Bridge mode.

Example

```
> ip igmp_snoop mode sw
 igmp snooping works on SW mode now.
```

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	Turn on session limit for each IP.
off	Turn off session limit for each IP.
default<num>	Set the default number of session num limit.
defaultp2p <num>	Set the default number of session num limit for p2p.
status	Display the current settings.
show	Display all session limit settings in the IP range.
timer <num>	Set when the IP session block works. The unit is second.
<block/unblock><IP>	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>	add/del: Add or delete the session limits in an IP range. IP1-IP2 - It means the range of IP address specified for this command. num - It means the number of the session limits, e.g., 100. p2pnum - It means the number of the session limits, e.g., 50 for P2P.

Example

```
>ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

  IP range:
    192.168.1.5 - 192.168.1.100 : 100

  Current ip session limit is turn on

  Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

Syntax

ip bandwidth *on*

ip bandwidth *off*

ip bandwidth *default <tx_rate><rx_rate>*

ip bandwidth *status*

ip bandwidth *show*

ip bandwidth *routing <on/off>*

ip bandwidth *schedule <s1> <s2> <s3> <s4>*

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.
show	It means to display all the bandwidth limits settings within the IP range.
routing <on/off>	on/off: Apply (on) or not apply (off) to the IP Routed Subnet.
schedule <s1> <s2> <s3> <s4>	Set the schedule profile. <*s1*> <*s2*> <*s3*> <*s4*>: Specify the profile index number. Up to four profiles can be set at one time. Available profiles numbers range from 1 to 16.
<add/del> <IP1-IP2> <tx> <rx> <shared>	Add/del: Add or 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: the bandwidth will be shared for the IP range.

Example

```
> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

  IP range:
    192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K
```

```
Current ip Bandwidth limit is turn off



Auto adjustment is off
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

Syntax

ip bindmac *on*

ip bindmac *off*

ip bindmac *strict_on*

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 and only those IP can access network.
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>: Enter 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>: It means to elete all the IP bindmac settings.
subnet <all/set LAN_Index/unset LAN_Index/clear/show>	It means to set the LAN subnet(s) for applying the rules of Bind IP to MAC all: Make all LAN subnets apply for the rules. set <LAN_Index>: Specify certain LAN subnet, e.g., set LAN2. unset <LAN_Index>: Remove certain LAN subnet by specifying the index number of LAN port, e.g., unset LAN3. clear: Remove all LAN subnets.

	show: Display current LAN subnet settings.
show	It means to display the IP address and MAC address of the pair of binded one.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned ON
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 Comment : just
```

Telnet Command: ip bgp

This command allows users to configure settings for BGP.

Syntax

ip bgp mode <*0/1*>

ip bgp as <*0~4294967295*>

ip bgp hold <*10~65535*>

ip bgp retry <*3~255* >

ip bgp id <*x.x.x.x*>

ip bgp show

ip bgp neighbor <*idx*> **mode** <*0/1*>

ip bgp neighbor <*idx*> **name** <*max len*>

ip bgp neighbor <*idx*> **ip** <*x.x.x.x*>

ip bgp neighbor <*idx*> **as** <*1~4294967295*>

ip bgp neighbor <*idx*> **weight** <*0~7*>

ip bgp neighbor <*idx*> **prepend** <*0~7*>

ip bgp neighbor <*idx*> **md5** <*0/1*>

ip bgp neighbor <*idx*> **key** <*max len*>

ip bgp neighbor <*idx*> **show**

ip bgp neighbor show all

ip bgp static <*sidx*> <*ip*> <*netmask*>

ip bgp static <*sidx*> **delete**

ip bgp static show

Syntax Description

Parameter	Description
mode <0/1>	Enable or disable the GMP. 0: disable 1: enable
as <0~4294967295>	Set the AS number for local router. <0~4294967295>
hold <10~65535>	Set the time interval (in seconds) to determine the peer is dead

	when the router is unable to receive any keepalive message from the peer within the time. <10~65535>: Default is 180 sec.
retry <3~255>	Set the BGP conntion retry time. <3~255>: Default is 120 sec
id <x.x.x.x>	Select a enabled local subnet IP as router ID. <x.x.x.x>: Enter an IP address.
show	Display all BGP settings.
neighbor <idx> mode <0/1>	Enable or disable the neighbor profile. <idx>: 1 to 8. Index number of the neighbor profile. 0: disable 1: enable
neighbor <idx> name <max len>	Set a name of the neighbor profile. <idx>: 1 to 8. Index number of the neighbor profile. <max len>: Enter a name (no more than 20 characters).
neighbor <idx> ip <x.x.x.x>	Set the IP address for the specified neighbor profile. <idx>: 1 to 8. Index number of the neighbor profile. <x.x.x.x>: Enter an IP address (e.g., 192.168.1.33).
neighbor <idx> as <1~4294967295>	Set an AS number for the specified neighbor profile. <idx>: 1 to 8. Index number of the profile. <1~4294967295>: Enter a number.
neighbor <idx> weight <0~7>	Set the weight value for the specified neighbor profile. <idx>: 1 to 8. Index number of the neighbor profile. <0~7>: higher is better.
neighbor <idx> prepend <0~7>	Set the prepend value for the specified neighbor profile. <idx>: 1 to 8. Index number of the neighbor profile. <0~7>: lower is better.
neighbor <idx> md5 <0/1>	Enable or disable the MD5 authentication for the neighbor profile. <idx>: 1 to 8. Index number of the profile. 0: Disable. 1: Enable.
neighbor <idx> key <max len>	Set the key used for the MD5 authentication. <idx>: 1 to 8. Index number of the neighbor profile. <max len>: Enter a name (no more than 20 characters).
neighbor <idx> show	Display the BGP setting for the specified neighbor profile. <idx>: 1 to 8. Index number of the profile.
neighbor show all	Display the BGP setting of neighbor profiles.
static <sidx> <ip> <netmask>	Set the IP address and subnet mask for specified static network profile. <sidx>: 1 to 8. Index number of the static network profile. <ip>: Enter an IP address. <netmask>: Enter a netmask.
static <sidx> delete	Remove / clear the settings for the selected static network profile. <sidx>: 1 to 8. Index number of the profile.

static show	Display the BGP setting of static network profiles.

Example

```
> ip bgp static 1 192.168.2.56 255.255.255.0
Set static network index: 1
IP addr: 192.168.2.56
Net mask: 255.255.255.0
> ip bgp static show
BGP is disable
Local autonomous system number: 0
Hold time: 180
Connect retry time: 120
Router ID: 192.168.1.1

BGP neighbor:
Idx Mode As Number  Name      IP Addr         Status       weight prepend
--- ---- ---------- ---------- --------------- ------------ ------ --------
1   Dis  0                 Empty          None         0     0
2   Dis  0                 Empty          None         0     0
3   Dis  0                 Empty          None         0     0
4   Dis  0                 Empty          None         0     0
5   Dis  0                 Empty          None         0     0
6   Dis  0                 Empty          None         0     0
...
...
...
63  Dis  0                 Empty          None         0     0
64  Dis  0                 Empty          None         0     0

BGP static networks:
>
```

Telnet Command: ip ospf

Users could use this command to configure OSPF (Open Shortest Path First) setting.

Syntax

ip ospf *en*

ip ospf *dis*

ip ospf *status*

ip ospf *cfg show*

ip ospf *cfg set <idx> state <dis/en>*

ip ospf *cfg set <idx> area <value>*

ip ospf *cfg set <idx> lan <value>*

ip ospf *cfg set <idx> wan <value>*

ip ospf *nbr*

Syntax Description

Parameter	Description
en	Enable the function of Open Short Path First.
dis	Disable the function of Open Short Path First.
status	Display interface status.
cfg show	Display configuiration setting for all interfaces.
cfg set <idx> state <dis/en>	Enable or disable the interface (LAN/WAN) setting. <idx>: 1 to 64. <dis/en>: disable or enable.
cfg set <idx> area <value>	Set interface for area id: <idx>: 1 to 64. <value>: 1 to 2147483647.
cfg set <idx> lan <value>	Set interface for LAN. <idx>: 1 to 64. <value>: 1 to 20.
cfg set <idx> wan <value>	Set interface for WAN. <idx>: 1 to 64. <value>: 1 to 2.
nbr	Display interface neighbors.

Example

```
> ip ospf cfg set 1 state en
> ip ospf cfg set 1 area 100
> ip ospf cfg set 1 wan 1
> ip ospf cfg show

OSPF: Enable
-----------------------------------------------------
  Idx  State  Area_id    Interface   Auth  Key ID
    0    En     100         WAN_1    Dis    0
    1   Dis       0         LAN_1    Dis    0
    2   Dis       0         LAN_1    Dis    0
...
...
>
```

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 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_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 ~ Policy60 LAN1 ~ LAN8 IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_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	View current failback setting.
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
mat
ched 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
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-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	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.

-s <*0/1*>	0:reply all 1:reply only same subnet packet.
-z	Update LAN DNS config to DNS Cache.

Example

```
>ip lanDNSRes -i 1 -p test
% Configure Set1's Profile:test
> ip lanDNSRes -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name:
% -------- Address Mapping Table --------
% Not Set Address Mapping.
>
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

Syntax

ip dnsforward *[-<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 <IP Address>	Set forwarded DNS server IP Address.
-d <DNS server mapping index number>	Delete the selected LAN DNS profile.
-e <0/1>	0: disable such function. 1: enable such function.
-i <profile setting index number>	Type the index number of the profile.
-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.
-R	Set to factory default settings.

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
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
<*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 0
% Setting saved:
> ip spoofdef LAN 1
Setting saved:
DrayTek> ip spoof def ?
Invalid Paremeter
IP Spoofing Defense Usage:
Set IP Spoofing Defense: spoofdef <WAN/LAN> <0/1>
Ex: "spoofdef WAN 1" to block IP packet from WAN with inconsistent source
IP add
ress
Current setting:
```

```
Block IP packet from WAN with inconsistent source IP address : Disable
Block IP packet from LAN with inconsistent source IP address : Enable
```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

ip6 addr -s *<prefix> <prefix-length> <LAN1/..LAN100/ WAN1/..WAN10/ VPN1/..VPN500>*

ip6 addr -d *<prefix> <prefix-length> <LAN1/..LAN100/ WAN1/..WAN10/ VPN1/..VPN500>*

ip6 addr -a *<LAN1/..LAN100/ WAN1/..WAN10/ VPN1/..VPN500> -u*

ip6 addr -v *<LAN1/..LAN100/ WAN1/..WAN10 >*

ip6 addr -t *<old-prefix><old-prefix-length><new-prefix> <new-prefix-length> <LAN1/..LAN100/ WAN1/..WAN10 >*

ip6 addr -o *<1/2>*

ip6 addr -o 3 *<prefix> <prefix-length> <WAN1/..WAN10 >*

ip6 addr -l *<prefix> <prefix-length> <LAN1/..LAN100>*

ip6 addr <-*p/-b***>** *<prefix> <prefix-length> <WAN1/..WAN10 >*

ip6 addr -x *<LAN1/..LAN100 >*

ip6 addr -c *<LAN1/..LAN100>*

ip6 addr -e *<type> < LAN1/..LAN100>*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <LAN1/..LAN100/ WAN1/..WAN10/ VPN1/..VPN500>	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/..LAN100/ WAN1/..WAN10/VPN1/..VPN500>: It means to specify LAN/WAN/ VPN interface for such address.
-d <prefix> <prefix-length> <LAN1/..LAN100/ WAN1/..WAN10/ VPN1/..VPN500>	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/..LAN100/ WAN1/..WAN10 /VPN1/..VPN500>: It means to specify LAN/WAN/VPN interface for such address.
-a <LAN1/..LAN100/ WAN1/..WAN10/VPN1/..VPN 500> -u	It means to show current address(es) status. <LAN1/..LAN100/ WAN1/..WAN10/ VPN1/..VPN500>: It means to specify LAN/WAN/VPN interface. <-u>: It means to show unicast address only.
-v <LAN1/..LAN100/ WAN1/..WAN10>	It means to show prefix list status.

-t <old-prefix><old-prefix-length><new-prefix> <new-prefix-length> < LAN1/..LAN100/ WAN1/..WAN10>	It means to update WAN static IPv6 address table. <old-prefix>: It means to enter the prefix number of IPv6 address. <old prefix-length>: It means to enter a fixed value as the length of the prefix. <new-prefix>: It means to enter the prefix number of IPv6 address. <new-prefix-length>: It means to enter a fixed value as the length of the prefix. <LAN1/..LAN100/ WAN1/..WAN10>: It means to specify LAN/WAN 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/..WAN10 >	<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/..WAN10>: It means to specify a WAN interface for such address.
-l <prefix> <prefix-length> < LAN1/..LAN100>	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/..LAN100>: It means to specify a LAN interface for such address.
-p/-b <prefix> <prefix-length> < WAN1/..WAN10>	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/..WAN10>: It means to specify a WAN interface for such address.
-x <LAN1/..LAN100>	It means to generate a ULA automatically. <LAN1/..LAN100>: It means to specify a LAN interface.
-c <LAN1/..LAN100>	It means to delete a ULA . <LAN1/..LAN100>: It means to specify a LAN interface.
-e <type> <LAN1/..LAN20>	It means to set ULA type. <type>: 0, disable; 1, static; 2, auto <LAN1/..LAN100>: It means to specify a LAN interface.

Example

```
> ip6 addr -a
DMZ
Unicast Address:
 FE80::21D:AAFF:FE4B:3E80/64 (Link)
Multicast Address:
 FF02::1:FF00:0
 FF02::1:FF4B:3E80
 FF02::1
LAN100
Unicast Address:
 FE80::21D:AAFF:FE4B:3E80/64 (Link)
Multicast Address:
 FF02::1:FF00:0
 FF02::1:FF4B:3E80
 FF02::1
LAN99
Unicast Address:
 FE80::21D:AAFF:FE4B:3E80/64 (Link)
Multicast Address:
 FF02::1:FF00:0
 FF02::1:FF4B:3E80
 FF02::1
LAN98
Unicast Address:

 FE80::21D:AAFF:FE4B:3E80/64 (Link)
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

Syntax

ip6 dhcp *req_opt <LAN1|…|LAN100|WAN1|…|WAN10> [-<command> <parameter>| …]*

Syntax Description

Parameter	Description
req_opt	It means option-request.
<LAN1|LAN2|…|LAN100|W	It means to specify LAN or WAN interface for such address.

AN1|…|WAN10>	
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-s	It means to ask the SIP.
-S	It means to ask the SIP name.
-d	It means to ask the DNS setting.
-D	It means to ask the DNS name.
-n	It means to ask NTP.
-i	It means to ask NIS.
-I	It means to ask NIS name.
-p	It means to ask NISP.
-P	It means to ask NISP name.
-b	It means to ask BCMCS.
-B	It means to ask BCMCS name.
-r	It means to ask refresh time.
Parameter	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%    sip name
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

Syntax

ip6 dhcp *client <WAN1|…|WAN10> [-<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 type in several commands in one line.
-a	It means to show current DHCPv6 status.
-r	It means to send RELEASE MESSAGE.
-p [IAID]	It means to request identity association ID for Prefix Delegation.
-n [IAID]	It means to request identity association ID for Non-temporary Address.
-t <time>	It means to set solicit interval. <time>: 0 ~ 7 seconds (default value is 0).
-c <parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-i <parameter>	It means to send information request to server. 1: Enable 0: Disable
-e <parameter>	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable
-m <parameter>	It means to enable/disable server DUID set by Link layer and time. 1: Enable 0: Disable
-d	It means to display the client DUID.
-A <parameter>	It means to set authentication protocol. 0: Undefine 2: delayed protocol
-R <parameter>	It means to set realm value (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-S <parameter>	It means to set shared secret (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-K <parameter>	It means to set key ID (1~65535) in delayed protocol. <parameter>: Enter a number.

Example

```
> ip6 dhcp client WAN2 –p 2008::1
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
       DHCPv6 client enabled
       request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 –n 1023456
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
       DHCPv6 client enabled
       request IA_NA whose IAID equals to 2008
> system reboot
```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

Syntax

ip6 dhcp *server [-<command> <parameter>| …]*

Syntax Description

Parameter	Description
server	It means the dhcp server settings.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
-a	It means to show current DHCPv6 status.
-b	It means to show current DHCPv6 IP assignment table.
-n <name>	It means to set a 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 -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
```

```
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%    DHCPv6 server disabled
%    maximum address of the pool: FF02::3
%    minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet *-W n -M n [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
-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
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-m n	It means to set IPv6 MTU. N = any value (0 means “unspecified”).
6rd	It means to set Username.

	<username>= type a name as the username (maximum 63 characters).
-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	It means to view IPv6 Internet Access Profile.
-s <server>	It means to set 6in4 remote endpoint IPv4 address.
-l <IPv6 Addr>	It means to set the IPv6 address for 6in4 connection.
-P <n>	It means to set IPv6 WAN prefix length for 6in4 connection.
-p <prefix>	It means to set 6in4 LAN Routed Prefix.
-l <n>	It means to set 6in4 LAN Routed Prefix length.
-T <n>	It means to set 6in4 Tunnel TTL.
TSPC/AICCU	
-u <username>	It means to set username (max. 63 characters). <username>: Enter a string.
-P <password>	It means to set Password (max. 63 characters). <password>: Enter a password.
-s <server>	It means to set Tunnel Server IP. <server>: Enter an IPv4 Address or URL (max. 63 characters)
AICCU	
-p <prefix>	It means to set Subnet Prefix (AICCU). <prefix>: Enter a prefix number of IPv6 address.
-l <n>	It means to set Subnet Prefix length (AICCU). <n>: Enter a number.
-o <1/0>	It means to set AICCU always on. 1: on 0: off
-f	It means to set AICCU tunnel ID.
Static	
-w <addr>	It means to set Default Gateway. <addr>: Enter an IPv6 address.

Others	
-d <server>	It means to set 1st DNS Server IP. <server>: Enter an IPv6 address.
-D <server>	It means to set 2nd DNS Server IP. <server>: Enter an IPv6 address.
-t <dhcp/ra/none>	It means to set ipv6 PPP WAN test mode for DHCP or RA. <dhcp/ra/none> : Enter dhcp, ra or none.
-V	It means to view IPv6 Internet Access Profile.
-k	It means to dial the Tunnel on the WAN.
-j	It means to drop the Tunnel on the WAN.
-r n	It means to set Prefix State Machine RA timeout.
-c n	It means to set Prefix State Machine DHCPv6 Client timeout.
-q <0/1/2>	It means to set WAN detection mode. 0:NS Detect 1:Ping Detect 2:Always On
-z <value>	It means to set Ping Detect TTL (0-255). <value>: Enter 0~255.
-x <hostname/ IPv6 addr>	It means to set Ping Detect Host (hostname or IPv6 address). <hostname/ipv6 addr> : Enter a hostname or an IPv6 address.
-i <value>	It means to set ipv6 connection interval. <value>: Enter a number (1500-60000 (unit:10ms)).
-b <0/1>	It means to enable DNSv6 based on DHCPv6. 1 = on 0 = off
-R <0/1>	It means to Enable RIPng. 1 = on 0 = off

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 –s amsterdam.freenet6.net
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

ip6 neigh *-s <inet6_addr> <eth_addr> <LAN1/..LAN100/WAN1/...WAN10>*

ip6 neigh *-d <inet6_addr> <LAN1/..LAN100/WAN1/...WAN10>*

ip6 neigh *-a <inet6_addr> <LAN1/..LAN100/WAN1/...WAN10>*

Syntax Description

Parameter	Description
-s <inet6_addr> <eth_addr> <LAN1/..LAN100/WAN1/...WAN10>	It means to add a neighbour. <inet6_addr>: Enter an IPv6 address. <eth_addr>: Enter a submask address. <LAN1/..LAN100/WAN1/...WAN10>: Specify an interface for the neighbor.
-d <inet6_addr> <LAN1/..LAN100/WAN1/...WAN10 >	It means to delete a neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN100/WAN1/...WAN10>: Specify an interface for the neighbor.
-a <inet6_addr> <LAN1/..LAN100/WAN1/...WAN10>	It means to show neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN100/WAN1/...WAN10>: Specify an interface for the neighbor.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2
        Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a


I/F  ADDR                                    MAC              STATE
-------------------------------------------------------------------------
LAN1 ::                                                       NONE
 LAN1 2001:2222:3333::1111                                    FAILED
>
```

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

Syntax

ip6 pneigh *-s <inet6_addr> <LAN1|LAN2|...|LAN100|WAN1|...|WAN10>*

ip6 pneigh *-d <inet6_addr> <LAN1|LAN2|...|LAN100|WAN1|...|WAN10>*

ip6 pneigh *-a <inet6_addr><-N LAN1|LAN2|...|LAN100|WAN1|...|WAN10>*

Syntax Description

Parameter	Description
-s <inet6_addr> < LAN1|LAN2|…|LAN100| WAN1|…|WAN10>	It means to add a proxy neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1|LAN2|…|LAN100|WAN1|…|WAN10>: Specify an interface for the proxy neighbor.
-d <inet6_addr> < LAN1|LAN2|…|LAN100| WAN1|…|WAN10>	It means to delete a proxy neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1|LAN2|…|LAN100|WAN1|…|WAN10>: Specify an interface for the proxy neighbor.
-a <inet6_addr> < LAN1|LAN2|…|LAN100| WAN1|…|WAN10>	It means to show proxy neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1|LAN2|…|LAN100|WAN1|…|WAN10>: Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 LAN
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to set ip6 route.

Syntax

ip6 route *-s <prefix> <prefix-length> <gateway> < LAN1|LAN2|…|LAN100|WAN1|…|WAN10 |VPN1|…|VPN500> <-D>*

ip6 route -*d <prefix> <prefix-length>*

ip6 route -*a < LAN1|LAN2|…|LAN100|WAN1|…|WAN10|VPN1|…|VPN500>*

ip6 route -*D*

ip6 route -*I*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <gateway> < LAN1|LAN2|…|LAN100|WAN1 |…|WAN10|VPN1|…|VPN500 > <-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|…|LAN100|WAN1|…|WAN10|VPN1|…|VPN500>***:** It means to specify LAN or WAN or VPN interface for such address. <-D>: It means that such route will be treated as the default route.
-d <prefix> <prefix-length>	It means to delete a route.

	<prefix>: It means to enter the prefix number of IPv6 address. <prefix length>: It means to enter a fixed value as the length of the prefix.
-a < *LAN1*|*LAN2*|…|*LAN100*|*WAN1*|…|*WAN10*|*VPN1*|…|*VPN500* >	It means to show the route status. <*LAN1*|…|*LAN100*|*WAN1*|…|*WAN10*|*VPN1*|…|*VPN500*>**:** It means to specify LAN or WAN or VPN interface for such address.
-l	It means to clear the routing table.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN1
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN1

PREFIX/PREFIX-LEN                       I/F METRIC FLAG NEXT-HOP
------------------------------------------------------------------------
 ::0.0.0.1/128                          LAN1    0 U ::
 FE80::/128                             LAN1    0 U ::
 FE80::21D:AAFF:FE4B:3E80/128           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|…|LAN100|WAN1|…|WAN10> <send count> <data_size>*

Syntax Description

Parameter	Description
<IPV6 address/Host>	It means to specify the IPv6 address or host for ping.
<LAN1|LAN2|…|LAN100|WAN1|…|WAN10> <send count> <data_size>	It means to specify LAN or WAN interface for such address. <send count>: Set how many packets sent for pinging. <data_size>: 1 to 1452. Set the data size for each packet to be pinged.

Example

```
> ip6 ping 2001:4860:4860::8888 WAN2

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]*

ip6 tracert *<IPV6 address/Host> <LAN1|LAN2|…|LAN100|WAN1|…|WAN10>*

Syntax Description

Parameter	Description
<IPV6 address/Host>	It means to specify the IPv6 address or host for ping.
<LAN1|…|LAN100|WAN1|…	It means to specify an interface for such address.

|*WAN10*>	

Example

```
> ip6 tracert 2001:4860:4860::8888 LAN1
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

```
> ip6 tspc 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 8886666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net
```

```
Status: Connected


>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

Ip6 radvd *<LAN1|LAN2|…|LAN100> [-<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!
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.> ip6 radvd -V
> 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                : 0
%  Reachable time     : 0
%  Retransmit time    : 0
%  Preference         : Medium
>
```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

Syntax

ip6 mngt list

ip6 mngt *list [add <Index> <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) . remove <Index>: It means to remove (delete) the specified IP 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.
% IPv6 Access List :
> ip6 mngt status
% IPv6 Remote Management :
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*|*…*|*WAN10*>

Syntax Description

Parameter	Description
<*WAN1*|*…*|*WAN10*>	It means the connection interface.

Example

```
> ip6 online WAN1
 % WAN1 online status :
 % IPv6 WAN1 Disabled
 % Default Gateway : ::
 % Interface : DOWN
 % UpTime : 0:00:00
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
```

```
 % IPv6 DNS Server: :: Static
 % Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
 % MTU Onlink: 1280 , Config MTU : 0
>
```

Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

Syntax

ip6 aiccu -i <*ifno*> **-r**

ip6 aiccu -i <*ifno*> **-s**

Syntax Description

Parameter	Description
<*Ifno*>	It means the connection interface. 1=WAN1 2=WAN2
-r	It means to remove (delete) the specified index number with IPv6 settings.
-s	It means to display the AICCU status.

Example

```
> ip6 aiccu -i 1 -s
ip6 aiccu -i 1 -s
>
```

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 LAN8. n=17: 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	<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	<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 *[-VcdhrtzZ]*

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-c	It means to show the running call filter rules.
-d	It means to show the running data filter rules.
-h	It means to show the hit-number of the filter rules.
-r	It means to show the running call and data filter rules.
-t	It means to display all the information at one time.
-z	It means to clear a filter rule's statistics.
-Z	It means to clear IP filter's gross statistics.

Example

```
> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available
```

Telnet Command: ipf 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
<Options>	It means to set the firewall general setup and default rule.
<SET_NO><Options>	It means to set the firewall fiter set including comments and next fiter set.
<SET_NO> rule <RULE_NO><Options>	It means to set the firewall rule in 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 300000) <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.
About ipf set <SET_NO> rule <RULE_NO><Options>	
<SET_NO>	Range from 1 to 50.
<RULE_NO>	Range from 1 to 30.
-e <1/0>	Enable the filter set. <1/0>: Enter 1(enable) or 0 (disable).
-v	It means to view the configuration of the rule set.
-D <value>	It means to set the direction of the rule. <value>: 0, 1, 2 0 - LAN/RT/VPN -> WAN 1 - WAN -> LAN/RT/VPN 2 - LAN/RT/VPN -> LAN/RT/VPN 3 - WAN -> Localhost
-I e|d <para1,para2,...>	It means to set incoming interface. e: enable; d:disable <para1,para2,...>: Specify interfaces including all, LAN1 to LAN100, DMZ, RT, VPN, WAN1 to WAN52. RT means IP Routed Subnet.
-O e|d <para1,para2,...>	It means to set outgoing interface.

	e: enable; d:disable <para1,para2,...>: Specify interfaces including all, LAN1 to LAN100, DMZ, RT, VPN, WAN1 to WAN52. RT means IP Routed Subnet.
-s "o|o6|g|g6|c <field> <obj>"	It means to specify source IP object, IP group or country object. o: IP object. Ranges from 0 to 192. 0 means none. o6: IPv6 object. Ranges from 0 to 64. 0 means none. g: IP group. Ranges from 0 to 32. 0 means none. g6: IPv6 group. Ranges from 0 to 32. 0 means none. c: country object. Ranges from 1 to 32. <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 source IP. Example: > ipf rule 3 1 -e 1 -s "o 1 2"
-d "o|o6|g|g6|c <field> <obj>"	It means to set the destination object, group or country. o: IP object. Ranges from 0 to 192. 0 means none. o6: IPv6 object. Ranges from 0 to 64. 0 means none. g: IP group. Ranges from 0 to 32. 0 means none. g6: IPv6 group. Ranges from 0 to 32. 0 means none. c: country object. Ranges from 1 to 32. <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, -d "o 1 2" means IPv4 object profile 1 and 2 are set as destination IP. Example: > 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 set 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_value>	It means to set advanced setting of the protocol and the port range for the service type. <protocol>: Protocol. Ranges from 0 to 255. In which, TCP(6), UDP(17), TCP/UDP(255), Any(0), ICMP(1), ICMPv6(58), Other(other) <source_port_value>: Set port number, port range for the service type. e.g.: 1,3,5 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_vale>: e.g.: 2,4,6 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>	Set the fragment type. <value>: 0 to 3. In which, 0: Don't care 1: ungragmented 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 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 150000) 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.
-A "<Param 0>"	It means to enable or disable the packet capture function. <Param 0>: Enter 0 or 1. 0 : Disable. 1 : Enable.
-I <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 ~ 50. “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. e.g.: ipf set 1 rule 1 -C "600 30"
-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. Example: > 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. e.g.: -t "c 1"
-M <Your Comments>	It means to set comments for the filter rule. <Your Comments>: Enter a brief description.
-U "<Up or 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 set 1 -m sansansan

> ipf set -c 3 -p 0 1

Setting saved.

> ipf set -R "v4 1"

Setting saved.
```

```
> ipf set -R "v6 1"
Setting saved.
> ipf set -v

Call Filter: Enable (Start Filter Set = 3)
Data Filter: Enable (Start Filter Set = 2)
Log Flag   : Disable

Actions for packet not matching any rule:
  Pass or Block    : Pass
  CodePage        : ANSI(1252)-Latin I
  Max Sessions Limit: 150000
  Current Sessions  : 7
  Mac Bind IP      : Non-Strict
  QOS Class        : None
  Packet Capture   : Disable
  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 50).
r	It means Filter Rule r: Enter a value (1~30).
[<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/DMZ/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,…: Available values include all, LAN1, LAN2, …, LAN100, DMZ, RT, VPN, WAN1, …, WAN52. Example: > ipf rule 3 1 -e 1 -I "e LAN1"
-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, …, LAN100, DMZ, RT, VPN, WAN1, …, WAN52. 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 150000) 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.
-A "<Param 0>"	It means to enable or disable the packet capture function. <Param 0>: Enter 0 or 1. 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 3 1 -e 1 -M testtest -s "u 1 192.168.1.20" -F "0 1
Setting saved.
> ipf rule 3 1 -v
Filter Set 3 Rule 1:

Status  : Enable
Comments: testtest
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, LAN5, LAN6, LAN7, LAN8, LAN9, LAN10,
LAN11, LAN12, LAN13, LAN14, LAN15, LAN16, LAN17, LAN18, LAN19, LAN20, LAN21,
LAN22, LAN23, LAN24, LAN25, LAN26, LAN27, LAN28, LAN29, LAN30, LAN31, LAN32,
LAN33, LAN34, LAN35, LAN36, LAN37, LAN38, LAN39, LAN40, LAN41, LAN42, LAN43,
LAN44, LAN45, LAN46, LAN47, LAN48, LAN49, LAN50, LAN51, LAN52, LAN53, LAN54,
LAN55, LAN56, LAN57, LAN58, LAN59, LAN60, LAN61, LAN62, LAN63, LAN64, LAN65,
LAN66, LAN67, LAN68, LAN69, LAN70, LAN71, LAN72, LAN73, LAN74, LAN75, LAN76,
LAN77, LAN78, LAN79,
LAN80, LAN81, LAN82, LAN83, LAN84, LAN85, LAN86, LAN87, LAN88, LAN89, LAN90,
LAN91, LAN92, LAN93, LAN94, LAN95, LAN96, LAN97, LAN98, LAN99, LAN100, Routed,
VPN,

Dst Interface : WAN1, WAN2, WAN3, WAN4, WAN5, WAN6, WAN7, WAN8, WAN9, WAN10,
WAN11, WAN12, WAN13, WAN14, WAN15, WAN16, WAN17, WAN18, WAN19, WAN20, WAN21,
WAN22, WAN23, WAN24, WAN25, WAN26, WAN27, WAN28, WAN29, WAN30, WAN31, WAN32,
WAN33, WAN34, WAN35, WAN36, WAN37, WAN38, WAN39, WAN40, WAN41, WAN42, WAN43,
WAN44, WAN45, WAN46, WAN47, WAN48, WAN49, WAN50, WAN51, WAN52
Source IP         : 192.168.1.20
Destination IP    : Any
Service Type      : Any
Fragments         : Don't Care

Pass or Block             : Pass Immediately
Branch to Other Filter Set : None
Max Sessions Limit        : 150000
Current Sessions          : 0
Mac Bind IP                   : Non-Strict
Qos Class                     : None
```

```
Packet Capture             : Disable
APP Enforcement            : None
URL Content Filter         : None
WEB Content Filter         : None
DNS Filter                     : None
Load-Balance policy        : Auto-select
Log                            : Enable
------------------------------------------------------------------
CodePage                   : ANSI(1252)-Latin I
Window size                : 65535
Session timeout            : 60
DrayTek Banner             : Enable
  ----------------------------------------------------------------
  Strict Security Checking
    [ ]APP Enforcement
>
```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

Syntax

ipf flowtrack set <*-r*/*-e*>

ipf flowtrack view <*-f*/*-b*>

ipf flowtrack set *-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.
- i <IP address>	It means to specify IP address (e.g,, -i 192.168.2.55).
-p <value>	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.

-t <value>	It means to specify a protocol (e.g., -t tcp). Available settings include: *tcp* *udp* *icmp*

Example

```
> ipf flowtrack set -e
Current flowtrack ON
> ipf flowtrack set -i 192.168.1.102 -p 1024 -t tcp
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>>   192.168.1.1:19181 ->   192.168.1.10:  443 ,ifno=0 nat=-1
REPLY >>  192.168.1.10:  443 ->    192.168.1.1:19181 ,ifno=0 nat=-1
       proto=6, age=666084170(4700), flag=20009, timeout=1, num=0, size=0
       origin TCP>> end=0x0, max_end=0x0, max_win=0x0
       reply  TCP>> end=0x0, max_end=0x0, max_win=0x0
End to show the flowtrack sessions state
>
```

Telnet Command: ipf flowtest

This command is used to for RD debug in firewall diagnose.

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: ldap user

This command is used to configure the LDAP profile.

Syntax

ldap user <*INDEX*><*OPTION*>

Syntax Description

Parameter	Description
INDEX	Specify the index number (1 to 8) of the LDAP profile.
OPTION	
-n VALUE	Setup Profile Name.
-b VALUE	Setup Base Distinguished Name.
-a VALUE	If you have added containers to be published, you may need to specify additional LDAP filters for each class of objects included in these containers. Creating LDAP filters is a fairly complex task that should be performed by advanced users only. LDAP filters must be RFC2254-compliant. For example, to exclude from publication all users who either belong to the HR department of your company or are members of the HR Group. For example: >ldap user 1 -a "(!(|(department=HR)(memberOf=CN=HRGroup,OU=Groups, DC=acme,DC=com)))" Additional Filter has been updated.
-g VALUE	Setup Group Distinguished Name.
-c VALUE	Setup Common Name Identifier.
-v	View detail information of the LDAP profile.

Example

```
>ldap user 1 -n LD_user_test1
Profile Name has been updated!
> ldap user 1 -v
Profile Index:1
Profile Name:LD_user_test1
Common Name Identifier:
Base Distinguished Name:
Additional Filter:
Group distinguished Name:
>ldap user 1 -b ou=People,dc=example,dc=com
```

Telnet Command: ldap set

This command is used to set general settings (e.g., IP address, port number) for LDAP server.

Syntax

ldap set <*Options*><*Value*>

Syntax Description

Parameter	Description
enable <0/1>	Enable or disable LDAP function. 0 – Disable the function. 1 – Enable the function.
type <0/1/2>	Set the bind type as Simple(0),Anonymous(1), and Regular(2).
ssl <0/1>	Enable or disable LDAP function via SSL tunnel. 0 – Disable the function. 1 – Enable the function.
IP <VALUE>	Set IP address for LDAP server.
port <VALUE>	Set port number for LDAP server.
dn <VALUE>	Set Regular DN value
PWD <VALUE>	Set Regular password value.

Example

```
>ldap set enable 1
>ldap enabled.
> ldap set ssl 1
LDAP with SSL has been enabled!
> ldap set IP 192.168.100.155
LDAP Server IP has been setting.
> ldap set port 389
LDAP Server Port has been setting.
> ldap set dn dc=example,dc=com
LDAP Regular DN has been setting.
> ldap set PWD 123456
LDAP Regular Password has been setting.
```

Telnet Command: ldap view

This command is used to check current status of LDAP settings configuration.

Syntax

ldap view

Example

```
> ldap view ?
LDAP Enable:Disabled.
```

```
LDAP Bind Type:Simple
LDAP with SSL:Disabled
LDAP Regular DN:
LDAP Regular Password:
LDAP Server IP:
LDAP Server Port:389
```

Telnet Command: tacacsplus set

This command allows users to configure general settings for TACACS+ server

Syntax

tacacspluse set <*Options*><*Value*>

Syntax Description

Parameter	Description
enable <0/1>	Disable (0)/enable(1) the TACACS+ server.
IP <VALUE>	Set the IP address of TACACS+ server.
port <VALUE>	Set the port number of TACACS+ server.
shared_secret <VALUE>	Set the Shared Secret value of TACACS+ Server.

Example

```
> tacacsplus set enable 1
TACACS+ enabled!
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> tacacsplus set IP 192.168.1.59
TACACS+ Server IP has been setting.
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:
```

Telnet Command: tacacsplus view

This command allows users to check the general settings for TACACS+ server

Syntax

tacacspluse view

Example

```
> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:
```

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 type 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 type 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 443
% Set SSL VPN port to 443 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

Syntax

mngt telnetport <*Telnet port*>

Syntax Description

Parameter	Description
Telnet port	It means to type 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 type 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/enforce_https*><*on/off*>

Syntax Description

Parameter	Description
status	It means to display current setting for your reference.
enable	It means to allow the system administrators to login from the Internet.

disable	It means to deny the system administrators to login from the Internet.
http/https/ftp/telnet/ssh/tr069/snmp/enforce_https	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 *–E*
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, ENFORCE_HTTPS, TELNET, SSH, None, All
-i <value>	It means the interface which is allowed to access. Available values include: LAN1~LAN20, 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.
-h	It means to get the usage of such command.

Example

```
> mngt lanaccess -e 1 -s FTP -i LAN1 -I 1
> mngt lanaccess -v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
   - FTP:Yes
   - HTTP:No
   - HTTPS:No
   - TELNET:No
   - SSH:No
   - TR069:No
   - Enforce HTTPS:No
* Subnet:
   - LAN 1: enabled
     - Specific IP(type:IP Object)(index:1) is disabled
   - LAN 2: disabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 3: disabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 4: disabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 5: disabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 6: disabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 7: disabled
```

```
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 8: disabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 9: disabled
     - Specific IP(type:IP Object)(index: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 ten 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	It means adding a new entry.
index	It means to specify the number (1 to 10) of the entry.

IP Object Index	It means to specify an IP object by entering the index number of the object profile. Available value: 1 to 192.
remove	It means to delete the selected item.
flush	It means to remove all the settings in the access list.
flush	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 1
%% Set OK. Please do "sys re" to reboot the router!
> mngt accesslist list
%% Access list :
  [Index]      [IP Object Index]      [IP/CIDR or StartIP ~ EndIP]
================================================================================
  1             1                      192.168.1.9 ~ 192.168.1.9
>
```

Telnet Command: mngt wanlogin

This command allows you to enable or disable WAN login function.

Syntax

mngt wanlogin *enable*

mngt wanlogin *disable*

Example

```
> mngt wanlogin enable
%% wan login enabled.
>
```

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 type in 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 192.168.1.1 -t trapcom -n 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 192.168.1.1
 Trap Community set to trapcom
 Notification Host IP set to 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 type in 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, None 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 300 (seconds).

Example

```
> mngt sshtimeout 200
% SSH timeout : 200s
>
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

Syntax

msubnet switch
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <On/Off>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ….

8/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	100=LAN100
<On/Off>	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msubnet switch 99 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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <IP address>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …. 100=LAN100
<IP address>	Type 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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <IP address>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …. 100=LAN100
<IP address>	Type the subnet mask address for the specified LAN interface.

Example

```
>  msubnet nmask 2 255.255.0.0
% Set 3/44/45/46/47/48/49/50 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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …. 100=LAN100

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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <On/Off>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5

4/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	6=LAN6 …. 100=LAN100
<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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <On/Off>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …. 100=LAN100

<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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <Gateway IP>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …. 100=LAN100
<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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <IP counts>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …. 100=LAN100
<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
<1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>

<1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <On/Off>

Syntax Description

Parameter	Description
<1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …. 100=LAN100
On/Off	On – It means to enable the function. Off **-** It means to disable the function.

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1       and LAN2      !


 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> msubnet talk ?
% msubnet talk <1/2/3/4/5/6> <1/2/3/4/5/6> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:LAN5, 6:LAN6
% Now:
%            LAN1   LAN2   LAN3   LAN4   LAN5   LAN6
% LAN1         V
% LAN2         V     V
% LAN3                     V
% LAN4                            V
% LAN5                                   V
% LAN6                                          V
...
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

msubnet startip
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <Gateway IP>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …… …. 100=LAN100
<Gateway IP>	Type an IP address as the starting IP address for a subnet.

Example

```
> msubnet startip 2 192.168.2.90
% Set
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
Dhcp
 Start IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> msubnet startip ?
% msubnet startip
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/
25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/
49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/
73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/
97/98/99/100> <Gateway IP>
% Now:
```

```
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
192.168.2.90; 82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
192.168.3.10; 86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 192.168.4.10;
90/91/92/93/94/95/96/97/98/99/100 192.168.5.10; 94/95/96/97/98/99/100
192.168.6.10; 98/99/100 192.168.7.10;  192.168.8.10;  192.168.9.10;
192.168.10.10;  192.168.11.10;  192.168.12.10;  192.168.13.10;
192.168.14.10;  192.168.15.10;  192.168.16.10;  192.168.17.10;
192.168.18.10;  192.168.19.10;  192.168.20.10;  192.168.21.10;
192.168.22.10;  192.168.23.10;  192.168.24.10;  192.168.25.10;
192.168.26.10;  192.168.27.10;  192.168.28.10;  192.168.29.10;
192.168.30.10;  192.168.31.10;  192.168.32.10;  192.168.33.10;
192.168.34.10;  192.168.35.10;  192.168.36.10;  192.168.37.10;
192.168.38.10;  192.168.39.10;  192.168.40.10;  192.168.41.10;
192.168.42.10;  192.168.43.10;  192.168.44.10;  192.168.45.10;
192.168.46.10;  192.168.47.10;  192.168.48.10;  192.168.49.10;
192.168.50.10;  192.168.51.10;  192.168.52.10;  192.168.53.10;
192.168.54.10;  192.168.55.10;  192.168.56.10;  192.168.57.10;
192.168.58.10;  192.168.59.10;  192.168.60.10;  192.168.61.10;
192.168.62.10;  192.168.63.10;  192.168.64.10;  192.168.65.10;
192.168.66.10;  192.168.67.10;  192.168.68.10;  192.168.69.10;
192.168.70.10;  192.168.71.10;  192.168.72.10;  192.168.73.10;
192.168.74.10;  192.168.75.10;  192.168.76.10;  192.168.77.10;
192.168.78.10;  192.168.79.10;  192.168.80.10;  192.168.81.10;
192.168.82.10;  192.168.83.10;  192.168.84.10;  192.168.85.10;
192.168.86.10;  192.168.87.10;  192.168.88.10;  192.168.89.10;
192.168.90.10;  192.168.91.10;  192.168.92.10;  192.168.93.10;
192.168.94.10;  192.168.95.10;  192.168.96.10;  192.168.97.10;
192.168.98.10;  192.168.99.10;  192.168.101.10
>
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

msubnet pppip
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <Start IP>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/3	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4

6/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	5=LAN5 6=LAN6 …… …. 100=LAN100
<Start IP>	Type an IP address as the starting IP address for PPP connection.

Example

```
> msubnet pppip 2 192.168.2.250
% Set
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <Start IP>
% Now:
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
192.168.2.250; 82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
192.168.3.200; 86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
192.168.4.200; 90/91/92/93/94/95/96/97/98/99/100 192.168.5.200;
94/95/96/97/98/99/100 192.168.6.200; 98/99/100 192.168.7.200;
192.168.8.200;  192.168.9.200;  192.168.10.200;  192.168.11.200;
192.168.12.200;  192.168.13.200;  192.168.14.200;  192.168.15.200;
192.168.16.200;  192.168.17.200;  192.168.18.200;  192.168.19.200;
192.168.20.200;  192.168.21.200;  192.168.22.200;  192.168.23.200;
192.168.24.200;  192.168.25.200;  192.168.26.200;  192.168.27.200;
192.168.28.200;  192.168.29.200;  192.168.30.200;  192.168.31.200;
192.168.32.200;  192.168.33.200;  192.168.34.200;  192.168.35.200;
192.168.36.200;  192.168.37.200;  192.168.38.200;  192.168.39.200;
192.168.40.200;  192.168.41.200;  192.168.42.200;  192.168.43.200;
192.168.44.200;  192.168.45.200;  192.168.46.200;  192.168.47.200;
```

```
192.168.48.200;  192.168.49.200;  192.168.50.200;  192.168.51.200;
192.168.52.200;  192.168.53.200;  192.168.54.200;  192.168.55.200;
192.168.56.200;  192.168.57.200;  192.168.58.200;  192.168.59.200;
192.168.60.200;  192.168.61.200;  192.168.62.200;  192.168.63.200;
192.168.64.200;  192.168.65.200;  192.168.66.200;  192.168.67.200;
192.168.68.200;  192.168.69.200;  192.168.70.200;  192.168.71.200;
192.168.72.200;  192.168.73.200;  192.168.74.200;  192.168.75.200;
192.168.76.200;  192.168.77.200;  192.168.78.200;  192.168.79.200;
192.168.80.200;  192.168.81.200;  192.168.82.200;  192.168.83.200;
192.168.84.200;  192.168.85.200;  192.168.86.200;  192.168.87.200;
192.168.88.200;  192.168.89.200;  192.168.90.200;  192.168.91.200;
192.168.92.200;  192.168.93.200;  192.168.94.200;  192.168.95.200;
192.168.96.200;  192.168.97.200;  192.168.98.200;  192.168.99.200;
192.168.101.200
>
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

msubnet nodetype
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <count>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …… …. 100=LAN100
<count>	Choose the following number for specifying different node type. 1= B-node 2= P-node 4= M-node

	8= H-node 0= Not specify any type for node.

Example

```
> msubnet nodetype 2 1
% Set 78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
Dhcp
 Node Type done !!!


> msubnet nodetype ?


% msubnet nodetype
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/
29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53
/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/7
8/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>
<count>
% Now:
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
1;82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 0;
86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 0;
90/91/92/93/94/95/96/97/98/99/100 0; 94/95/96/97/98/99/100 0; 98/99/100 0;
0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;
0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;
0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;
0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;
0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  0;  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
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <WINS IP>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/2	It means LAN interface. 2=LAN2

0/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	3=LAN3 4=LAN4 5=LAN5 6=LAN6 …… …. 100=LAN100
<WINS IP>	Type the IP address as the WINS IP.

Example

```
> msubnet primWINS ?
% msubnet primWINS
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/
29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53
/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/7
8/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <WINS
IP>
% Now:
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
0.0.0.0; 82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 0.0.0.0;
86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 0.0.0.0;
90/91/92/93/94/95/96/97/98/99/10
0 0.0.0.0; 94/95/96/97/98/99/100 0.0.0.0; 98/99/100 0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0; 0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0
> msubnet primWINS 2 192.168.3.5
% Set 78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
Dhcp
```

```
 Primary WINS IP done !!!


> msubnet primWINS ?
% msubnet primWINS
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/
29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53
/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/7
8/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <WINS
IP>
% Now:
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
192.168.3.5; 82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
0.0.0.0; 86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 0.0.0.0;
90/91/92/93/94/95/96/97/98/99/100 0.0.0.0; 94/95/96/97/98/99/100 0.0.0.0;
98/99/100 0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

Syntax

msubnet secWINS *% msubnet secWINS*
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <WINS IP>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/2	It means LAN interface. 2=LAN2 3=LAN3

8/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	4=LAN4 5=LAN5 6=LAN6 …… …. 100=LAN100
<WINS IP>	Type the IP address as the WINS IP.

Example

```
> msubnet secWINS 2 192.168.3.89
% Set 78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
Dhcp
 Secondary WINS IP done !!!
> msubnet secWINS ?
% msubnet secWINS
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/
29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53
/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/7
8/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>
<WINS IP>
% Now:
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 192
.168.3.89; 82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
0.0.0.0; 86/87/88/89/90/91/92/93/94/95/96/97/98/99/100 0.0.0.0;
90/91/92/93/94/95/96/97/98/
99/100 0.0.0.0; 94/95/96/97/98/99/100 0.0.0.0; 98/99/100 0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
```

```
0.0.0.0
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

Syntax

msubnet tftp
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <TFTP servername>

Syntax Description

Parameter	Description
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …… …. 100=LAN100
<TFTP servername>	Type a name to indicate the TFTP server.

Example

```
>  msubnet tftp 2 publish
% Set 78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
TFTP Server Name done !!!


> msubnet tftp ?
% msubnet tftp
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/
29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53
/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/7
8/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100> <TFTP
server name>
% Now:
78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
```

```
publish
         82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
         86/87/88/89/90/91/92/93/94/95/96/97/98/99/100
         90/91/92/93/94/95/96/97/98/99/100
         94/95/96/97/98/99/100
         98/99/100
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/DMZ/IP Routed Subnet.

Syntax

msubnet mtu <*interface*> <*value*>

Syntax Description

Parameter	Description
interface	Available settings include LAN1~LAN100, IP_Routed_Subnet.
value	1000 ~ 1508 (Bytes), default: 1500 (Bytes)

Example

```
> msubnet mtu LAN1 1492
> msubnet mtu ?
Usage:

  >msubnet mtu <interface> <value>

  <interface>: LAN1~LAN6,IP_Routed_Subnet,DMZ
  <value>:    1000 ~ 1508 (Bytes), default: 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)
   LAN5 MTU:           1500 (Bytes)
   LAN6 MTU:           1500 (Bytes)
   LAN7 MTU:           1500 (Bytes)
   LAN8 MTU:           1500 (Bytes)
```

```
   LAN9 MTU:           1500 (Bytes)
...
  LAN99 MTU:           1500 (Bytes)
  LAN100 MTU:           1500 (Bytes)
  IP Routed Subnet MTU: 1500 (Bytes)
>
```

Telnet Command: msubnet leasetime

This command allows you to set leasetime for DHCP server. It is helpful to manage the IP address(es) assigned by DHCP server.

Syntax

msubnet leasetime *[1~50][Lease Time (sec.)]*

Syntax Description

Parameter	Description
1~50	1 – 50 represent LAN1 to LAN50.
Lease Time (sec.)	Range from 1 to 259200. If no value specified here, Vigor router system will use the maximum value, 259200, as the leasetime.

Example

```
> DrayTek> msubnet leasetime ?
% msubnet leasetime
<1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23
/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/4
8/49/50> <Lease Time (sec.)>
% Now:9/40/41/42/43/44/45/46/47/48/49/50 86400; 3/44/45/46/47/48/49/50
259200; 7/48/49/50 259200;  259200;  259200;  259200;  259200;  259200;
259200;  259200;  259200;  259200;  259200;  259200;  259200;  259200;
259200;  259200;  259200;  259200;  259200;  259200;  259200;  259200;
259200;  259200;  259200;  259200;  259200;  259200;  259200;  259200;
259200;  259200;  259200;  259200;  259200;  259200;  259200;  259200;
259200;  259200
DrayTek> msubnet leasetime 1
% Set 9/40/41/42/43/44/45/46/47/48/49/50 lease time: 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 I*NDEX -a TYPE <START_IP><END/MASK_IP>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	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]
.
.
.
 [97:][0]
 [98:][0]
 [99:][0]

Set ok!
> object ip grp 2 -i 1
> object ip grp 2 -a "1 2"
 Marketing3910> object ip grp 2 -a "1 2"
 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]
..
 [97:][0]
 [98:][0]
 [99:][0]
Set ok!
```

Telnet Command: object ipv6 obj

This comman is used to create an IP object profile.

Syntax

object ipv6 obj setdefault

object ipv6 obj *INDEX -v*

object ipv6 obj *INDEX -n NAME*

object ipv6 obj *INDEX -i INTERFACE*

object ipv6 obj *INDEX -s INVERT*

object ipv6 obj *INDEX -e MATCH_TYPE*

object ipv6 obj I*NDEX -a TYPE <START_IP><END_IP><Prefix Length>*

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 ipv6 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 ipv6 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 ipv6 obj 8 -i 0`
-e MATCH_TYPE	It means to set the match type of ipv6 object profile. MATCH_TYPE=0, means 128 bits MATCH_TYPE=1, means suffix 64 bits interface ID Example: `object ipv6 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 ipv6 obj 3 -e 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 ipv6 obj 3 -a 2*
<START_IP><END_IP><Prefix Length>	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. *<START_IP><END_IP>:* Type an IPv6 address as the start IPv6 address and another IPv6 address (different with START_IP) as the end IPv6 address. <Prefix Length>: Specify the prefix length.

Example

```
> obj ipv6 obj 3 -a 3 2607:f0d0:1002:51::4 2607:f0d0:1002:51::4
Setting saved.

> obj ipv6 obj 3 -v
 IPv6 Object Profile 3
 Name   :[]
 Address Type:[range]
 Start IPv6 Address:[2607:F0D0:1002:51::4]
 End IPv6 Address:[2607:F0D0:1002:51::4]
 Prefix Length:[0]
 MAC Address:[00:00:00:00:00:00]
 Invert Selection:[0]
 Match Type:[0]
```

Telnet Command: object ipv6 grp

This command is used to integrate several IPv6 objects under an IPv6 group profile.

Syntax

object ipv6 grp setdefault

object ipv6 grp *INDEX -v*

object ipv6 grp *INDEX -n NAME*

object ipv6 grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile.

	Example: *object ipv6 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 ipv6 grp 8 -n bruce*
-a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile. Example: *:object ipv6 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 1 -n marketingtest
 IPv6 Group Profile 1
 Name   :[marketingtest]
 Included ip object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
.
.
.
[97:][0]
[98:][0]
[99:][0]
> object ipv6 grp 1 -a 1 2 3 4 5
 IPv6 Group Profile 1
 Name   :[marketingtest]
 Included ip object index:
 [0:][1]
 [1:][2]
 [2:][3]
 [3:][4]
 [4:][5]
 [5:][0]
```

```
 [6:][0]
 [7:][0]
.
.
[97:][0]
[98:][0]
[99:][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).
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.
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
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 s**ervice 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 to indicate the starting source port. END_P: Enter a port number to indicate the ending source 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 to indicate the starting destination port. END_P: Enter a port number to indicate the ending destination port. Example: *object service obj 3 -d 1 100 200*

Example

```
> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
 Service Object Profile 1
 Name   :[limit]
 Protocol:[TCP/UDP]
 Source port check action:[!=]
 Source port range:[120~240]
 Destination port check action:[!=]
 Destination port range:[200~220]
>
```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

object service grp setdefault

object service grp *INDEX -v*

object service grp *INDEX -n NAME*

object service grp *INDEX -a SER_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	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]
.
.
.
 [97:][0]
 [98:][0]
 [99:][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]
.
.
.
 [97:][0]
 [98:][0]
 [99:][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*

object kw obj *INDEX -c*

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: type 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*
-c	It means to clear the content of keyword object profile.

	Example: *object kw obj 40 -c*

Example

```
> object kw obj 1 -n children
 Profile 1
 Name   :[children]
 Content:[]
> object kw obj 1 -a gambling
 Profile 1
 Name   :[children]
 Content:[gambling]

> object kw obj 1 -v
 Profile 1
 Name   :[children]
 Content:[gambling]
```

Telnet Command: object fe

This command is used to create File Extension Object profile.

Syntax

object fe show

object fe setdefault

object fe obj *INDEX -v*

object fe obj *INDEX -n NAME*

object fe obj *INDEX -e CATEGORY|FILE_EXTENSION*

object fe obj *INDEX -d CATEGORY|FILE_EXTENSION*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX	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 Example: *object fe obj 1 -e Image* FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".aac", ".aiff", ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole", ".tlb", ".viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr", ".torrent" Example: *object fe obj 1 -e .bmp*

Example

```
> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]


-------------------------------------------------------------------------
Image category:
 [ ].bmp   [ ].dib   [ ].gif   [ ].jpeg  [ ].jpg   [ ].jpg2  [ ].jp2   [ ].pct
 [ ].pcx   [ ].pic   [ ].pict  [ ].png   [ ].tif   [ ].tiff
-------------------------------------------------------------------------
Video category:
 [ ].asf   [ ].avi   [ ].mov   [ ].mpe   [ ].mpeg  [ ].mpg   [v].mp4   [ ].qt
 [ ].rm    [v].wmv   [ ].3gp   [ ].3gpp  [ ].3gpp2 [ ].3g2
-------------------------------------------------------------------------
Audio category:
 [v].aac   [v].aiff  [v].au    [v].mp3   [v].m4a   [v].m4p   [v].ogg   [v].ra
 [v].ram   [v].vox   [v].wav   [v].wma
-------------------------------------------------------------------------
Java category:
```

```
 [ ].class [ ].jad   [ ].jar   [ ].jav   [ ].java  [ ].jcm   [ ].js    [ ].jse
 [ ].jsp   [ ].jtk
-------------------------------------------------------------------------
ActiveX category:
 [ ].alx   [ ].apb   [ ].axs   [ ].ocx   [ ].olb   [ ].ole   [ ].tlb   [ ].viv
 [ ].vrm
-------------------------------------------------------------------------
Compression category:
 [ ].ace   [ ].arj   [ ].bzip2 [ ].bz2   [ ].cab   [ ].gz    [ ].gzip  [ ].rar
 [ ].sit   [ ].zip
-------------------------------------------------------------------------
Executation category:
 [ ].bas   [ ].bat   [ ].com   [ ].exe   [ ].inf   [ ].pif   [ ].reg   [ ].scr
```

Telnet Command: object sms

This command is used to create short message object profile.

Syntax

object sms show
object sms setdefault
object sms obj *INDEX -v*
object sms obj *INDEX -n NAME*
object sms obj *INDEX -s Service Provider*
object sms obj *INDEX -u Username*
object sms obj *INDEX -p Password*
object sms obj *INDEX -q Quota*
object sms obj *INDEX -i Interval*
object sms obj *INDEX -l URL*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
[INDEX]	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 CTC
> object sms obj 1 -n CTC
> object sms obj 1 -s 0
> object sms obj 1 -u carrie
> object sms obj 1 -p 19971125cm
> object sms obj 1 -q 2
> object sms obj 1 -i 50
> object sms obj 1 -v
Profile Index: 1
Profile Name:[CTC]
```

```
SMS Provider:[kotsms.com.tw (TW)]
Username:[carrie]
Password:[******]
Quota:[2]
Sending Interval:[50(seconds)]
```

Telnet Command: object mail

This command is used to create mail object profile.

Syntax

object mail show
object mail setdefault
object mail obj *INDEX -v*
object mail obj *INDEX -n <Profile Name>*
object mail obj *INDEX -s <SMTP Server>*
object mail obj *INDEX -l <Connection security>*
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>*
object mail obj *INDEX -w <Interface>*
object mail obj *INDEX -x <Alias IP>*

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 <Connection security>	It means to set the Connection security. 0 - Plaintext 1 - SSL 2 - StartTLS,nice to have 3 - StartTLS, MUST
-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.
-w <Interface>	It means to set the interface of the mail server profile.
-w <Interface>	It means to set the alias IP of the mail server profile.

Example

```
> object mail obj 1 –n buyer
> 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
Interface:[Any]
Alias IP Index:[0]
Profile Name:[DD]
SMTP Server:[ms.draytek.com]
SMTP Port:[25]
Sender Address:[vkao@draytek.com] Connection Security:[Plaintext]

Authentication:[disable]
Username:[]
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 markbei
```

```
> object noti obj 1 –e 1 1
> object noti obj 1 –e 2 1
> object noti obj 1 –e 5 3
> object noti obj 1 –v
> object noti obj 1 -e 1 1
> object noti obj 1 -e 2 1
> object noti obj 1 -e 5 3
> object noti obj 1 -v
Profile Index: 1
Profile Name:[]
    Category                  Status
  WAN                 [v]Disconnected     [ ]Reconnected
  VPN Tunnel          [v]Disconnected     [ ]Reconnected
  Temperature Alert   [ ]Out of Range
  WAN Budget Alert    [ ]Limit Reached
  CVM Alert           [ ]CPE Offline
                      [ ]CPE Config Backup Fail
                      [v]CPE Config Restore Fail
                      [ ]CPE Firmware Fpgrade Fail
                      [ ]CPE VPN Profile Setup Fail
  High Availability   [ ]Failover Occurred
                          Config Sync Fail
                          Router Unstable
```

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: 1 ~ 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>	Set how often the schedule will be applied. [option] – 0: Once, 1: Weekdays [day] – Sun, Mon, Tue, Wed, Thu, Fri, Sat If the [option] set Weekdays, then must select which days of Week. example: To select Sunday, Monday, Thursday, type *> 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 "2016 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)  [ 2016 ]-[ 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
        [ ] Once
        [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, 5, 6, 7, 8, 9, 10, 11, 12, all*> <*AN, 100F, 100H, 10F, 10H, status* >

port <*wan1, wan2, wan3, wan4*> <*AN, 1000F, 100F, 100H, 10F, 10H, status* >

port sniff <*on,off,port,txrx,restart,status*>

port status

port wanfc

Syntax Description

Parameter	Description
<*1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, all*><*AN, 100F, 100H, 10F, 10H, status*>	It means the to set the physical type for a LAN port. <*1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, all*> - It means the number of LAN port. <*AN, 100F, 100H, 10F, 10H*> - It means the physical type for the specific port. AN: auto-negotiate. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex. status: View the Ethernet port status.
<*wan1, wan2, wan3, wan4*> <*AN, 1000F, 100F, 100H, 10F, 10H, status*>	It means the to set the physical type for a LAN port. <*wan1, wan2, wan3, wan4*> - It means the number of WAN port. <*AN, 1000F, 100F, 100H, 10F, 10H, status*> - It means the physical type for the specific port. AN: auto-negotiate. 1000F: 1000M Full Duplex. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex. status: 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
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 !!!
```

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 type in several commands in one line.
-t <sec>	It means “TCP” protocol. <sec>: Type a number to set the TCP session timeout.
-u <sec>	It means “UDP” protocol. <sec>: Type a number to set the UDP session timeout.
-i <sec>	It means “IGMP” protocol. <sec>: Type a number to set the IGMP session timeout.
-w <sec>	It means “TCP WWW” protocol. <sec>: Type a number to set the TCP WWW session timeout.
-s <sec>	It means “TCP SYN” protocol. <sec>: Type a number to set the TCP SYN session timeout.

-f	It means to flush all portmaps (useful for diagnostics).
-l <List>	List all settings.

Example

```
> portmaptime -t 86400 -u 300  -i 10
> portmaptime -l
------ Current setting ------
TCP Timeout   : 86400 sec.
UDP Timeout   : 300 sec.
IGMP Timeout  : 10 sec.
TCP WWW Timeout: 60 sec.
TCP SYN Timeout: 60 sec.
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-W <1~12>	It means to specify WAN interface. The default is WAN1. 1: WAN1; 2:WAN2;....
-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).

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 type in 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>: type the index number for the rule.
-d <no>	It means to delete specified rule. <no>: type 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 type 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 type 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.
[…]	It means that you can type in several commands in one line.

Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80

 Following setting will set in the class2
 class 2 name set to draytek
 Add a rule in class2
 Class2 the 1 rule enabled
 Set local address type to Range, 192.168.1.50:192.168.1.80
```

Telnet Command: qos type

This command allows user to configure protocol type and port number for QoS.

Syntax

qos type *[-a <service name> | -e <no> | -d <no>]***.**

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  192.168.100.1   255.255.255.0   V   192.168.100.10  200  192.168.100.1

[V]LAN2  192.168.5.1    255.255.0.0    V   192.168.2.90   100  192.168.200.1

[X]LAN3  192.168.3.1    255.255.255.0   X   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]LAN100  192.168.101.1   255.255.255.0   V   192.168.101.10  100  192.168.101.1

[X]Route 192.168.0.1    255.255.255.0   V   0.0.0.0       0   192.168.0.1>
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0

%     WAN2 DMZ mapping status:
 Index  Status  WAN2 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0

%     WAN3 DMZ mapping status:
 Index  Status  WAN3 aux IP    Private IP
-------------------------------------------------
   1    Disable 111.251.202.195

%     WAN4 DMZ mapping status:
 Index  Status  WAN4 aux IP    Private IP
-------------------------------------------------
   1    Disable 0.0.0.0

%     WAN5 DMZ mapping status:
 Index  Status  WAN5 aux IP    Private IP
-------------------------------------------------
   1    Disable 172.16.2.191
...
...
%     WAN12 DMZ mapping status:

 Index  Status  WAN12 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]
...
...
%  LAN100  Primary DNS: [Not set]
%  LAN100  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
********************************************************
  1.    Enable  CARR_1        192.168.1.9
Total 1 items listed.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
 Port Redirection Running Table:
Index  Protocol  Public Port   Private IP       Private Port
 1          6       20011   192.168.100.10          8080
 2          6       20022   192.168.100.10          8443
 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
--- 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
-------------------------------------------------------------------------------
  P     Private_IP: Port      Pseudo_IP: Port        Peer_IP:Port ST LastTime DPDK
-------------------------------------------------------------------------------
  6  192.168.100.10:57410 111.251.202.195:57730   52.159.49.199:  443  6    1165    1
  6  192.168.100.10:56901   172.16.2.191:57221     172.16.2.8: 3000  6    3823    1
 17  192.168.100.10:55373 111.251.202.195:55693    224.0.0.252: 5355  0     293    0
 17  192.168.100.10:55374 111.251.202.195:55694  172.217.160.67:  443  0     294    1
 17  192.168.100.10:56529 111.251.202.195:56849 239.255.255.250: 1900  0
...
```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
  Level0 TCP=86400001 UDP=300001 ICMP=10001
  Level1 TCP=600000 UDP=90000 ICMP=7000
  Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 150000
% Maximum Session Usage: 2
% Current Session Usage: 2
% Current Session Used(include waiting for free): 15
% WAN1 Current Session Usage: 0
% WAN2 Current Session Usage: 0
% WAN3 Current Session Usage: 1
```

```
% WAN4 Current Session Usage: 0
% WAN5 Current Session Usage: 1
% WAN6 Current Session Usage: 0
% WAN7 Current Session Usage: 0
% WAN8 Current Session Usage: 0
% WAN9 Current Session Usage: 0
% WAN10 Current Session Usage: 0
% WAN11 Current Session Usage: 0
% WAN12 Current Session Usage: 0
## Session Create this Sec: 0
## Session Create Peak Sec: 17
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:2:8:29
LAN Status
Primary DNS:168.95.192.1     Secondary DNS:168.95.1.1
IP Address:192.168.100.1     Tx Rate:103850   Rx Rate:68112

WAN 1 Status: Disconnected
Enable:Yes      Line:Fiber      Name:
Mode:DHCP Client Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0        TX Rate(bps):0   RX Packets:0        RX Rate(bps):0

WAN 2 Status: Disconnected
Enable:No       Line:Ethernet    Name:
Mode:---        Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0        TX Rate(bps):0   RX Packets:0        RX Rate(bps):0

WAN 3 Status: Connected
Enable:Yes      Line:Ethernet    Name:
Mode:PPPoE      Up Time:2:08:09    IP:111.251.202.195GW IP:168.95.98.254
TX Packets:47380     TX Rate(bps):2600 RX Packets:59135     RX
Rate(bps):5704

WAN 4 Status: Disconnected
Enable:No       Line:Ethernet    Name:

Mode:---        Up Time:0:00:00    IP:---          GW IP:---

TX Packets:0        TX Rate(bps):0   RX Packets:0        RX Rate(bps):0
...
...
```

Telnet Command: show traffic

This comman can display traffic graph for WAN#, transmitted bytes, receivied bytes and sessions.

Syntax

show traffic <*wan1/wan2~wan7*><*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 ,
```

reset <interface>	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: 2 MB ,RX: 25 MB
 WAN4 total TX: 0 Bytes ,RX: 0 Bytes
 WAN5 total TX: 11 MB ,RX: 65 MB
 WAN6 total TX: 0 Bytes ,RX: 0 Bytes
 WAN7 total TX: 0 Bytes ,RX: 0 Bytes
 WAN8 total TX: 0 Bytes ,RX: 0 Bytes
 WAN9 total TX: 0 Bytes ,RX: 0 Bytes
 WAN10 total TX: 0 Bytes ,RX: 0 Bytes
 WAN11 total TX: 0 Bytes ,RX: 0 Bytes
 WAN12 total TX: 0 Bytes ,RX: 0 Bytes
 WAN13 total TX: 0 Bytes ,RX: 0 Bytes
 WAN14 total TX: 0 Bytes ,RX: 0 Bytes
 WAN15 total TX: 0 Bytes ,RX: 0 Bytes
 WAN16 total TX: 0 Bytes ,RX: 0 Bytes
 WAN17 total TX: 0 Bytes ,RX: 0 Bytes
 WAN18 total TX: 0 Bytes ,RX: 0 Bytes
 WAN19 total TX: 0 Bytes ,RX: 0 Bytes
 WAN20 total TX: 0 Bytes ,RX: 0 Bytes
 WAN21 total TX: 0 Bytes ,RX: 0 Bytes
 WAN22 total TX: 0 Bytes ,RX: 0 Bytes
 WAN23 total TX: 0 Bytes ,RX: 0 Bytes

 WAN24 total TX: 0 Bytes ,RX: 0 Bytes
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

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 *[-<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 <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 3 or 4.
-d <id>	Turn off the flag of LAN port 1 or LAN port 2. <id>: Enter 3 or 4.
-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 3 flag: ON
   Port 4 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	It means the starting point of the IP address pool for the DHCP server.
IP address	It means to specify an IP address as the starting point in the IP address pool.
cnt	It means the IP count number.
IP counts	It means to specify the number of IP addresses in the pool. The

	maximum is 10.
status	It means the execution result of this command.
add	It means creating a list of hosts to be assigned.
del	It means removing the selected MAC address.
MAC Addr	It means to specify MAC Address of the host.
all/ALL	It means all of the MAC addresses.

Example

```
> srv dhcp public cnt 3
> srv dhcp public add 14-49-BC-0D-1F-48
> srv dhcp public status
Index   MAC Address
0.     14-49-BC-0D-1F-48 !!!
```

Telnet Command: srv dhcp dns1

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns1 *<DNS IP address>*

Syntax Description

Parameter	Description
<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 168.95.1.1
% srv dhcp dns1 <DNS IP address>
% Now: 168.95.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns2 *<lan1 ~ lan100> <DNS IP address>*

Syntax Description

Parameter	Description
<*lan1 ~ lan100*>	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 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp frcdnsmanl

This command can force the router to invoke DNS Server IP address.

Syntax

srv dhcp frcdnsmanl *on*

srv dhcp frcdnsmanl *off*

Syntax Description

Parameter	Description
on	It means to use manual setting for DNS setting.
Off	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: srv dhcp gateway

This command allows users to specify gateway address for DHCP server.

Syntax

srv dhcp gateway *<Gateway IP>*

Syntax Description

Parameter	Description
<Gateway IP>	It means to specify a gateway address used for DHCP server.

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 (0 to 256) 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 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

srv dhcp status <*LAN1/2/3/.../100/ip_routed_subnet*>

Syntax Description

Parameter	Description
<*LAN1/2/3/.../100/ip_routed_subnet*>	It means to display current status for the selected interface.

Example

```
> srv dhcp status
LAN1      : DHCP Server On   IP Pool: 192.168.188.10 ~ 192.168.188.209
            Default Gateway: 192.168.188.1
LAN2      : DHCP Server On   IP Pool: 159.196.80.239 ~ 159.196.80.248
            Default Gateway: 159.196.80.1
LAN3      : DHCP Server On   IP Pool: 192.168.111.10 ~ 192.168.111.109
            Default Gateway: 192.168.111.1
LAN5      : DHCP Server On   IP Pool: 192.168.5.10 ~ 192.168.5.109
            Default Gateway: 192.168.5.1
------------------------------------------------------------------------
Index   IP Address     MAC Address           Leased Time    HOST ID
------------------------------------------------------------------------
LAN1
```

```
1      192.168.188.14  00-11-D8-E4-58-CE      FIXED IP       TA000628
2      192.168.188.75  00-08-5D-28-9A-5D      FIXED IP
3      192.168.188.103 00-1D-AA-10-36-66      0:00:09
4      192.168.188.120 VPN User: 46          FIXED IP
5      192.168.188.194 VPN User: 30          FIXED IP
LAN2
LAN3
1      192.168.111.62  14-49-BC-10-71-71      FIXED IP
2      192.168.111.63  14-49-BC-0D-18-F9      FIXED IP
LAN5
>
```

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 ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 86400
>
```

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 expired_RecycleIP

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 type 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 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.

Example

```
> srv dhcp option -e 1 -c 18 -v /path
> 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
n	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
m	It means the index number 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.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-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 118.166.171.215
...
```

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
n	It means the index number for the profiles. The range is from 1 to 20.
m	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile.

	0: disable 1:enable
-c <comment>	It means to type 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 -I 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 -I 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: WAN2, ...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 <idx>	It means to delete the specified open port setting. idx: Enter the index number of the profile.
-f <idx>	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.55 -w 1 1 -p TCP -s 56

 Set WAN Port ok!!
```

```
> srv nat openport 1 1 -v

%% Status: Enable

%% Comment: games

%% WAN Interface: WAN1

%% Private IP address: 192.168.1.55

Index   Protocal        Start Port      End Port

**************************************************************

  1.    TCP             56              0


>
```

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 10.
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.

Example

```
> srv nat portmap add 1 name tcp 100 0 0 192.168.1.10 200 wan1 1
> srv nat portmap table

NAT Port Redirection Configuration Table:

Index  Service Name    Protocol  Public Port  Private IP      Private Port ifno
1       name           TCP       100    192.168.1.10          20
0      -1
2      ACS https       TCP       20022  192.168.100.10        844
3      -2
...
...

Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

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	Specify the incoming protocol for such trigger rule.
-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
> srv nat trigger 1 -e 1
> srv nat trigger 1 -p 1
> srv nat trigger 1 -t 2000
> srv nat trigger 1 -P 2
> srv nat trigger 1 -i 3000
> srv nat trigger 1 -v

Port Trigger Rule Index:1

Status:Enable
Comment:after_dinner2000
Triggering Protocol:TCP
Triggering Port:2000
Incoming Protocol:UDP
Incoming Port:3000
```

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          80   192.168.1.11             100
 2          0           0   0.0.0.0                   0
 3          0           0   0.0.0.0                   0
 4          0           0   0.0.0.0                   0
 5          0           0   0.0.0.0                   0
 6          0           0   0.0.0.0                   0
 7          0           0   0.0.0.0                   0
 8          0           0   0.0.0.0                   0
 9          0           0   0.0.0.0                   0
10          0           0   0.0.0.0                   0
11          0           0   0.0.0.0                   0
12          0           0   0.0.0.0                   0
13          0           0   0.0.0.0                   0
14          0           0   0.0.0.0                   0
15          0           0   0.0.0.0                   0
16          0           0   0.0.0.0                   0
17          0           0   0.0.0.0                   0
18          0           0   0.0.0.0                   0
19          0           0   0.0.0.0                   0

20          0           0   0.0.0.0                   0

--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: srv nat showall

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
>  srv nat showall ?
Index   Proto   WAN IP:Port              Private IP:Port          Act
******************************************************************************
R01     TCP     -- ALL --:21009          192.168.177.50:47873      N
R02     ---     -- ALL --:22303          192.168.177.31:5888       N
R03     ---     -- ALL --:47138          192.168.177.31:47873      N
R04     ---     -- ALL --:55641          192.168.177.12:5888       N
R05     ---     -- ALL --:47361          192.168.177.16:47361      N
R06     ---     -- ALL --:41216          192.168.177.15:41216      N
R07     ---     0.0.0.0:33055            192.168.188.118:33055     Y

O01     TCP     0.0.0.0:56~514           192.168.1.55:56~514       Y
O01     ---     0.0.0.0:0~0              192.168.1.55:0~0          Y
```

```
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O01     ---     0.0.0.0:0~0             192.168.1.55:0~0          Y
O02     ---     0.0.0.0:80~80           192.168.177.12:80~80       N
O02     ---     0.0.0.0:0~0             192.168.177.12:0~0         N

O02     ---     0.0.0.0:0~0             192.168.177.12:0~0         N

--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

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).
>
```

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 nat RSTTimeout ?
%% 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 display current switch status.

Example

```
> switch status ?
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  Model_Name   firmware_version

-------------------------------------------------------------------------
---------------------

[1]
00-1d-aa-0c-cd-08  192.168.1.11    On-Line   01:07:45    -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 save the switch log onto Syslog.

Example

```
> switch syslog on
External Device syslog is Enable
```

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*>

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: Enter a new name for local user. Password: Enter 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 bonjour

This command is used to disable/enable and configure the Bonjour service.

Syntax

sys bonjour *[-<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 <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: 3.0.0   Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
   [1] sys cmdlog
   [2] sys cmdlog ?
   [3] sys ?
   [4] sys cfg status
   [5] sys cfg ?
```

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/wan2*> <*Domain Name Suffix*>

sys domainname <*wan1/wan2*> *clear*

Syntax Description

Parameter	Description
wan1/wan2	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 40.
clear	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1     Netmask: 0xFFFFFF00 (Private)
IP Address: 0.0.0.0         Netmask: 0xFFFFFFFF
```

```
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
>
```

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

Syntax

sys name <*wan1/wan2*> <*ASCII string*>

sys name <*wan1/wan2*> **clear**

Syntax Description

Parameter	Description
wan1/wan2	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 20.

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.

Syntax

sys passwd <*old password*> <*new password*>

Syntax Description

Parameter	Description
<*old password*> <*new password*>	It means the password for administrator. The maximum character that you can set is 83.

Example

```
> sys passwd admin123
>
```

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: Vigor3910   Version: 4.3.2 r259_3658_9548064 zh_TW zh_CN
Profile version: 4.0.6   Status: 1 (0xfd805f2c)
Router IP: 192.168.188.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Oct 21 2022 17:23:20
Router Name: FAE3910
Revision: 259_3658_9548064 V400_RD3_432
>
```

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*

sys pollbuf *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 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 clear

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.
clear	It means to clear all tr069 parameters in 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 -h <on/off>	It means to / not to record the high availability 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

```
> Marketing3910> sys tr069 get InternetGatewayDevice.ManagementServer.
Total number of parameter is 98
Total content length of parameter is 6473

InternetGatewayDevice.ManagementServer.URL= http://192.168.100.10:8080/ACSServer
/services/ACSServlet
InternetGatewayDevice.ManagementServer.Username= fae
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= http://192.168.100.
1:8069/cwm/CRN.html
InternetGatewayDevice.ManagementServer.ConnectionRequestUsername= vigor
InternetGatewayDevice.ManagementServer.ConnectionRequestPassword=
InternetGatewayDevice.ManagementServer.UpgradesManaged= 0
InternetGatewayDevice.ManagementServer.UDPConnectionRequestAddress= 111.251.214.
196:38518
InternetGatewayDevice.ManagementServer.UDPConnectionRequestAddressNotification-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= 1
InternetGatewayDevice.ManagementServer.ApplyApEnable= 0
InternetGatewayDevice.ManagementServer.ApplyApPassword=
InternetGatewayDevice.ManagementServer.BWUNEnable= 1
InternetGatewayDevice.ManagementServer.BWUNPeriodic= 3
InternetGatewayDevice.ManagementServer.BWUNWANNumberOfEntries= 12
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.BWUNWAN.3.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.3.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.3.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.3.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.3.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.4.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.4.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.4.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.4.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.4.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.5.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.5.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.5.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.5.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.5.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.6.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.6.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.6.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.6.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.6.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.7.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.7.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.7.High= 0
```

```
InternetGatewayDevice.ManagementServer.BWUNWAN.7.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.7.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.8.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.8.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.8.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.8.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.8.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.9.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.9.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.9.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.9.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.9.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.10.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.10.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.10.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.10.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.10.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.11.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.11.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.11.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.11.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.11.RX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.12.Enable= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.12.Medium= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.12.High= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.12.TX= 0
InternetGatewayDevice.ManagementServer.BWUNWAN.12.RX= 0
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=
```

Telnet Command: sys health

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

Syntax

sys health cpu_usage

sys health mem_usage

sys health arp_status

sys health dos_status

sys health sess_usage

sys health view

sys health vpn_status

sys health voip_status

Syntax Description

Parameter	Description
<command><parameter>	The available commands with parameters are listed below.
cpu_usage <command><parameter>	-E <1/0> : Enable/disable this health parameter settings-CPU usage. -w <threshold> : Sets the warning threshold, 0-100 percent. -e <threshold> : Sets the emergency threshold, 0-100 percent. -r <interval> : Sets the warning report interval, 1-1440 min. -m <interval> : Sets the emergency report interval, 1-1440 min.
mem_usage <command><parameter>	- E <1/0> : Enable/disable this health parameter settings-memory usage. -w <threshold> : Sets the warning threshold, 0-100 percent. -e <threshold> : Sets the emergency threshold, 0-100 percent. -r <interval> : Sets the warning report interval, 1-1440 min. -m <interval> : Sets the emergency report interval, 1-1440 min.
arp_status <command><parameter>	-E <1/0> : Enable/disable this health parameter settings-ARP status. -w <threshold> : Warning threshold, 0-100 percent. -e <threshold> : Emergency threshold, 0-100 percent. -r <interval>: Warning report interval, 1-1440 min. -m <interval>: Emergency report interval, 1-1440 min.
dos_status <command><parameter>	-E <1/0>: Enable / disable this health parameter settings-DoS status. -r <interval>: Warning report interval, 1-1440 min. -m <interval>: Emergency report interval, 1-1440 min.
sess_usage <command><parameter>	-E <1/0>: Enable/disable this health parameter setting-session usage. -w <threshold> : Warning threshold, 0-100 percent. -e <threshold> : Emergency threshold, 0-100 percent. -r <interval>: Warning report interval, 1-1440 min. -m <interval>: Emergency report interval, 1-1440 min.
View	Displays current settings for health parameters.
vpn_status <command><parameter>	-E <1/0>: Enable/disable this health parameter setting-VPN status. -w <threshold> : Warning threshold, 0-100 percent. -e <threshold> : Emergency threshold, 0-100 percent. -r <interval>: Warning report interval, 1-1440 min. -m <interval>: Emergency report interval, 1-1440 min
voip_status <command><parameter>	-E <1/0> : Enable/disable this health parameter setting-VoIP status. -w <threshold> : Warning threshold, 0-100 percent. -e <threshold> : Emergency threshold, 0-100 percent. -r <interval> : Warning report interval, 1-1440 min. -m <interval> : Emergency report interval, 1-1440 min.

Example

```
> sys health vpn_status -m 30
% Set emergency interval to 30 min.
> sys health view
%                                                  Warning  Emergency
% ------------------------------------------------------------------
% [ ] CPU Status                    Threshold:    90       95
%                            Report Interval:    5        2
% ------------------------------------------------------------------
% [ ] Memory Status                  Threshold:    88       95
%                            Report Interval:    5        2
% ------------------------------------------------------------------
% [ ] ARP Status                    Threshold:    60       80
%                            Report Interval:    15       5
% ------------------------------------------------------------------
% [ ] Session Usage                  Threshold:    60       80
%                            Report Interval:    15       5
% ------------------------------------------------------------------
% [ ] DDoS Status              Report Interval:   5        1
% ------------------------------------------------------------------
% [ ] VPN Status               Report Interval:   0        30
% ------------------------------------------------------------------
% [ ] VoIP R-Factor                  Threshold:    60       40
%                             Report Interval:    1        1
```

Telnet Command: sys alg

This command can enable /disable the ALG (Application Layer Gateway) function.

Syntax

sys alg *-e <0/1>*

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
>
```

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*>	-e <1/0>: Enable or disable (0:disable, 1:enable) the

	function of SIP ALG. -p <1 to 65535>: set your listening port for SIP ALG. -u <1/0>: Enable or disable (0:disable, 1:enable) the listen along UDP path. -t <1/0>: Enable or disable (0:disable, 1:enable) the listen along TCP path .

Example

```
> sys sip_alg -e 1
 Enable 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: 5060
 -Max sipalg session num: 512
 -Remain sipalg session num: 512
```

Telnet Command: sys rtsp_alg

This command can turn on/off RTSP (Real Time Streaming Protocol) ALG (Application Layer Gateway) for traversal.

Syntax

sys rtsp_alg <*command*> <*parameter*>

Syntax Description

Parameter	Description
<*command*> <*parameter*>	-e <1/0>: Enable or disable (0:disable, 1:enable) the function of RTSP ALG. -p <1 to 65535>: set your listening port for RTSP ALG. -u <1/0>: Enable or disable (0:disable, 1:enable) the listen along UDP path. -t <1/0>: Enable or disable (0:disable, 1:enable) the listen along TCP path . -v: show RTP and RTCP portmap information of RTSP ALG.

Example

```
> sys rtsp_alg -p 333
 Current listening RTSP Port: 333
> sys rtsp_alg -v
 Current Open PortMap Number of RTSP ALG: 0
```

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 *liclog*

Syntax Description

Parameter	Description
reset_regser	It means the license register server setting.
licera	It means to erase license setting.
licifno <AUTO/WAN#>	It means to license and signature download (authenticatet with MyVigor) interface setting.
licalias <index>	It means to license and signature download WAN Alias IP setting(also affect WCF).
lic_trigger	It means to automatically trigger the license to update on boot time.
liclog	Displays authentication log.

Example

```
> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Download interface is "auto-selected" now.
```

Telnet Command: sys fr_log

This command is used for displaying log information related to web syslog.

Syntax

sys fr_log

Example

```
> sys fr_log ?

------------------------------------------------------------------

Note: This command shows the same log information with Diagnostics>>Syslog
Explo
rer. If you don't see any log information, go to the Web Interface and make
sure Diagnostics>>Syslog Explorer is enabled.
```

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 0
  Arp auto-request enable.
```

Telnet Command: sys daylightsave

This command is used to configure daylight save setting.

Syntax

sys daylightsave *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
[<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can 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	Display DNS IPv4 entry in the DNS cache table.
-s	Display DNS IPv6 entry in the DNS cache table.
-v	Display the TTL limit value in the DNS cache table.
-t < 0/n >	Set the TTL limit value in the DNS cache table. 0 - No limit N – Greater than or equal to 5.
-c	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -l
%DNS Cache Table List
 swm.draytek.com  192.168.18.18     601454  Black List
 relay-20c8ac21.net.anydesk.com 84.17.34.77    11530   Black List
 auth.draytek.com 35.189.201.134    602322  Black List
 www.draytek.com  104.25.10.249     601712  Black List
 ms.draytek.com   172.16.2.8        601448  Black List
>
```

Telnet Command: sys syslog

This command is used to configure

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.
-P	Update the server IP address.
-W <1/0>	Set the write syslog mode. 1 - Stop logging. 0 - Overwrite the oldest logs.
-U <1/0>	Set the unit for saving the Syslog to the USB disk. 1 - MB. 0 - GB.
-S <capacity>	Set the folder capacity for the Syslog in the USB disk. 1-16GB or 1-1024MB

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.
-e <0/1>	Enable/disable Mail Alert. 0 – Disable. 1 – Enable.
-w <0/1/2/...>	Set an interface (physically). <0/1/2/...> - 0 means Any; 1 means WAN1; 2 means WAN2; and so no.
-x <WAN IP Alias index>	Set the WAN IP Alias. In which, index #1 is reserved and must be set

	with an interface first.
-i <MTP 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 <0/1/2/3>	Set the connection security for SSL. 0 : Plaintext. 1: SSL. 2: StartTLS. 3: Force StartTLS.
-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. "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: 255.255.255.255
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 Reboot Debug Log: Disable, Mode: Limited.
-----------------------------------------------
```

Telnet Command: sys time

This command is used to configure system time and date.

Syntax

sys time server <*domain***>**

sys time inquire

sys time show

sys time wan *<option>*

sys time zone *<index>*

sys time pseudo

Syntax Description

Parameter	Description
server <domain>	Enter the domain name of the time server. <domain> - The maximum length is 39 characters.
inquire	Get the time based on the timer server settting.
show	Displays current server setting.
sys time wan <option>	0 - Auto 1 - WAN1 2 - WAN2 3 - WAN3 4 - WAN4 5 - WAN5 6 - WAN6 … 12 - WAN12 If you want to select WAN Alias IP, the value of Send NTP Request Through shouldn't be Auto.
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
pseudo -E <1/0>	Enable (1) or disable (0) the pseudo system time.
pseudo -T <year> <month> <day> <hour> <minute>	Set the pseudo time value. <year> - Enter four digits. <month> - Enter 1 t0 12. <day> - Enter the day in a month. <hour> - Enter the number of the hour (1 to 23). <minute> - Enter the number of the minute (1 to 59).
pseudo -S	Displays pseudo system time.

Example

```
> sys time zone 8
  Set Time Zone OK


> sys time show
  ***************  System Time  ***************
  Current System Time: [2000 Jan 01 Sat 02:09:29]
  Time Server: [pool.ntp.org]
  Time Zone Index: [8]. GMT-07:00
  ******************************************
```

Telnet Command: sys eap_tls

This command is used to disable or enable EAP-TLS.

You might have to enable EAP-TLS compatibility to avoid compatibility issues with some operating systems. But, please note that enabling EAP-TLS compatibility will lower down the connection security level.

Syntax

sys eap_tls set <*0/1***>**

Syntax Description

Parameter	Description

0	Disable EAP-TLS compatibility!
1	Enable EAP-TLS compatibility!

Example

```
> sys eap_tls set 1
Enable EAP_TLS compatibility!
```

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: sys max_session

This command is used to set the maximum sessions.

Syntax

sys max_session *<150K/300K/500K/1000K>*

Syntax Description

Parameter	Description
<150K/300K/500K/1000K>	At present, there are four values avaiable for selection.

Example

```
> sys max_session 150K
 Please reboot to apply settings of MAX sessions : 150K
```

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:[255.255.255.255]
 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 >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<


--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.

> upnp service
>>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL     /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN         uuid:774e9bbe-7386-4128-b627-001daa843464

>>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL     /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN         uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```
> upnp on
UPNP start.
> upnp subscribe
> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1
```

```
  ----- Subscribtion1 -------

    sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

    eventKey =1, ToSendEventKey = 1

    expireTime =6926

    active =1

    DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

  ----- Subscribtion1 -------

    sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

    eventKey =1, ToSendEventKey = 1
.
.
.
```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
> 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 12) 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 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*>	Add a new user profile. <Index> - It means the index number of the user profile.

<Home path>	There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16. <Username> - Type a text (maximum 131 characters) as the username for the user profile. <Password> - Type 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. There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16.
enable <Index>	Enable a 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.
disable <Index>	Disable a 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.
list	Display all of the user profile.

Example

```
> usb user add 1 root 1234 R-DLCR /usr
>
```

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 <0/1>	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: 1 (0:Disable, 1: Enable.)
upper temperature limit: 30.0 C
lower temperature limit: 18.0 C
unit: 0 (0:Celsius, 1: Fahrenheit.)
sensor: 1 (0:Auto select, 1: built-in.)
```

Telnet Command: usb hum

This command is to configure USB humidity.

Syntax Description

usb hum set <*-m*|*-u*|*-l*|*-r*>

usb hum show

usb hum all_data

Syntax Description

Parameter	Description
set -m	Enable or disable the Alarm Setting. 1: Enable

	0: Disable
set -u <value>	Set the upper humidity limit. <value>: Enter a value, e.g., 80.85.
set -l <value>	Set the lower humidity limit. <value>: Enter a value, e.g., 30.12.
set -r	Shows the setting of the humidity.
show	Displays current humidity.
all_data	Displays all humidity data.

Example

```
> usb hum set -m 1
Enable Alarm Settings.
```

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 … 10 - WAN10
-l <LAN_idx>	LAN_idx – Indicate the LAN interface. 1 – LAN1 2 – LAN2 3 – LAN3 4 – LAN4 5 - LAN5 6 - LAN6 …. 100 - LAN100
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 10 -l 100 -e 1
[WAN10] IPv4 bridge is enable. Set subnet[LAN100]
```

Telnet Command: vigbrg closeall

This command can disable vigor bridge function.

Example

```
> vigbrg closeall
Close all bridge and bridge firewall
```

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status
%Vigor Bridge Function is enable!


%Wan1 management is disable!
```

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: Running
WAN mac table:
Index   MAC Address           Stamp Time     PVC     VLan Port


>
```

Telnet Command: vlan group

This command allows you to set VLAN group. You can set four VLAN groups. Please run *`vlan restart`* command after you change any settings.

Syntax

vlan group *id* <*set*/*set_ex*> < *p2*/*p4*/*p9*/*p10*/*p11*/*p12*>

Syntax Description

Parameter	Description
id	It means the group 0 to 99 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.
p2/p4/p9/p10/p11/p12	It indicates LAN port 2 to LAN port 12. To group LAN2, LAN4, LAN9, LAN10, LAN11 and/or LAN12 under one VLAN group, please type the port number(s) you want.

Example

```
> vlan group 3 set p1 p4
 OK.
Use cmd 'vlan status' if you want to check result.
> vlan status
VLAN  is Disable :
-----------------------------------------------------------------------
VLAN Enable VID  Pri   p1 p2 p3 p4 p5 p6 p7 p8 p9 p10 p11 p12  subnet
-----------------------------------------------------------------------
 0    OFF    0   0                                        1:LAN1
 1    OFF    0   0                                        1:LAN1
 2    OFF    0   0                                        1:LAN1
 3    OFF    0   0      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
 8    OFF    0   0                                        1:LAN1
 9    OFF    0   0                                        1:LAN1
10    OFF    0   0                                        1:LAN1
11    OFF    0   0                                        1:LAN1
```

```
12    OFF   0   0                                        1:LAN1
13    OFF   0   0                                        1:LAN1
14    OFF   0   0                                        1:LAN1
15    OFF   0   0                                        1:LAN1
16    OFF   0   0                                        1:LAN1
17    OFF   0   0                                        1:LAN1
18    OFF   0   0                                        1:LAN1

19    OFF   0   0                                        1:LAN1
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
```

Telnet Command: vlan off

This command allows you to disable VLAN function.

Syntax

vlan off

Example

```
> vlan off
 VLAN is Disable!
>
```

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 p5 p6 p7 p8 p9 p10 p11 p12  subnet
-----------------------------------------------------------------------
 0    OFF    0   0                                                 1:LAN1
 1    OFF    0   0                                                 1:LAN1
 2    OFF    0   0                                                 1:LAN1
 3    OFF    0   0      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
 8    OFF    0   0                                                 1:LAN1
 9    OFF    0   0                                                 1:LAN1
10    OFF    0   0                                                 1:LAN1
11    OFF    0   0                                                 1:LAN1
12    OFF    0   0                                                 1:LAN1
13    OFF    0   0                                                 1:LAN1
14    OFF    0   0                                                 1:LAN1
15    OFF    0   0                                                 1:LAN1
16    OFF    0   0                                                 1:LAN1
17    OFF    0   0                                                 1:LAN1
18    OFF    0   0                                                 1:LAN1

19    OFF    0   0                                       1:LAN1
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
>
```

Telnet Command: vlan subnet

This command is used to configure the LAN interface used by the VLAN group.

Syntax

vlan subnet group_id
<1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/99/100>

Syntax Description

Parameter	Description
<1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/48/49/50/51/52/53/54/55/56/57/58/59/60/61/62/63/64/65/66/67/68/69/70/71/72/73/74/75/76/77/78/79/80/81/82/83/84/85/86/87/88/89/90/91/92/93/94/95/96/97/98/	It means interfaces, LAN1 ~ LAN100.

99/100>	

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
>
```

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 channel. The ranage is from 0 to 99.
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 range is from 0 to 7.
vid_no	It means the value of VLAN ID. Enter 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
n	It means VLAN channel. The ranage is from 0 to 7.
vid_no	It means the value of VLAN ID. Enter the value as the VLAN ID number. The range is form 0 to 3828.

Example

```
> vlan sysvid 100
 You have set system VLAN ID to range: 100 ~367,
 We recommend that you reboot the system now.
> vlan sysvid 200
 You have set system VLAN ID to range: 200 ~ 467,
 We recommend that you reboot the system now.
```

```
> vlan sysvid show
 The system VLAN ID is in range: 200 ~ 467
```

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*>

Syntax Description

Parameter	Description
<*list index*> **peerid** <*peerid*>	It means to set the L2L (LAN to LAN) profile with peer identity for aggressive mode. <list index> - Enter the index number of L2L (LAN to LAN) profile. <peerid> - Enter the peer identity string for aggressive mode.
<*list index*> **localid** <*localid*>	It means to set L2L (LAN to LAN) profile with local identity for aggressive mode. <list index> - Enter the index number of L2L (LAN to LAN) profile. <localid> - Enter *the* ocal identity for aggressive mode.
<*list index*> *main* <*auto/proposal index*>	It means to choose proposal for main mode. <list index> - Enter the index number of L2L (LAN to LAN) profile. <auto/proposal index> - Select auto (choose default proposal), proposal (choose specified proposal.), or index number.
<*list index***> aggressive** <*desg1/desg2/aesg1/aesg2/ aesg5/aesg14*>	It means the chosen DH group for aggressive mode. <list index> - Enter the index number of L2L (LAN to LAN) profile. <desg1/desg2/aesg1/aesg2/aesg5/aesg14> - Select one of them.
<*list index***>** *pfs* <*on/off*>	It means “perfect forward secrete”. <list index> - Enter the index number of L2L (LAN to LAN) profile. <on/off>: Turn on or off the PFS function.
<*list index***>** *phase1* <*lifetime*> /	It means phase 1 or 2 of IKE. <list index> - Enter the index number of L2L (LAN to LAN) profile.

phase2 <lifetime>	<lifetime>: Set the lifetime value (in second) for phase 1 and phase 2.
<list index> *x509localid <0/1>*	It means to enable (1) or disable (0) the X509 local ID. <list index> - Enter the index number of L2L (LAN to LAN) profile.

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 h2lidx <*idx*>

vpn l2lDrop <*ifno*>

vpn l2lDrop

Syntax Description

Parameter	Description
l2lname <name>	Terminate LAN to LAN VPN profile by specifying the profile name.
l2lidx <idx>	Terminate LAN to LAN profile name by specifying the index number (1 to 192) of the profile.
h2lname <name>	Terminate remote dial-in user profile (1 to 200) by specifying the profile name.
h2lidx <idx>	Terminate remote dial-in user profile by specifying the index number (1 to 200) of the profile.
<ifno>	Drop VPN with interface number. This is for debug only.
l2lDrop	It means to drop all VPN connections.

Example

```
> vpn l2lDrop
% Drop all VPN
```

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 500).
list	It means to display LAN to LAN profiles (enabled).

Example

```
> vpn l2lDialout list
 List LAN to LAN profiles of the status as Enable
Index  Profile    Status
```

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* <*value*>

vpn dinset <*list index*> *dintype* <*Type*> <*on/off*>

Syntax Description

Parameter	Description
<*list index*>	It means the index number of the profile.
<*on/off*>	It means to enable or disable the profile. on – Enable. off – Disable.
username <*USERNAME*>	It means to set the username for the remote dial-in VPN profile.
password <*PASSWORD*>	It means to set the passowrd for the remote dial-in VPN profile.
motp <*on/off*>	It means to enable or disable the authentication with mOTP function. on – Enable. off – Disable.
pin_secret<*pin*> <*secret*>	It means to set PIN code with secret. <pin> : Enter the code for authentication (e.g, 1234). <secret> : Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)
timeout <*value*>	It means to set idle timeout (0 to 9999). Default is 300 seconds.
<*list index*> *dintype* <*Type*> <*on/off*>	<list index>: Specify the index number of the VPN profile. <Type>: Allowed Dial-In Type includes 0, 1, 2 and 3. <on/off>: on, allowed using the dial-in type to create VPN connection; off, not allowed using the dail-in type to create VPN connection.

	0: PPTP, 1: IPsec Tunnel, 2: L2TP with IPsec Policy, 3: SSL Tunnel

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/.../100*>

Syntax Description

Parameter	Description
<*index*>	It means the index number of the VPN profile.
<*1/2/3/.../100*>	1 – it means LAN1 2 – it means LAN2. 3 – it means LAN3 4 – it means LAN4. ... 100 – it means LAN100

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 ~ 500
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, w2o, w1oB and w2oB. w1f – WAN1 First. w1o – WAN1 Only. w2f – WAN2 First. w2o – WAN2 Only. w1oB - WAN1 Only (Only establish VPN if WAN2 down) w2oB - WAN2 Only (Only establish VPN if WAN1 down)
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). “ctype= c” means SSL Tunnel.
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 [a/m/s/S]” means ESP DES without/with Authentication (Auto, MD5, SHA1 or SHA2). “ometh=esp3/esp3a [a/m/s/S]” means ESP 3DES without/with Authentication (Auto, MD5, SHA1 or SHA2). “ometh=espa [1/9/2']/espaa [a/m/s/S] [1/9/2']” means ESP AES (128, 192, or 256) without/with Authentication (Auto, MD5, SHA1 or SHA2) (128, 192, or 256).
sch	It means Index(1-15) in Schedule Setup. sch=1,3,5,7 Set schedule 1->3->5->7
ikemode	It means to set IKE phase 1 mode. "ikemode=m/a" means the IKE phase 1 mode whill be set as Main Mode / Aggressive Mode.
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).

	“ctype= c” means SSL Tunnel.
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”.
lnip	It means the local network IP. "lnip=1.2.3.0" means to set the local network IP as "1.2.3.0".
lnmask	It means the local Network Mask. “rnmask=255.255.255.0” means to set the local 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
> vpn option 33 pname=carrietest
% Change Log..

% Prifile Name = carrietest
```

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 ~ 500
<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 ~ 500

Example

```
> vpn list 32 all
% Common Settings

% Profile Name            : ???
% Profile Status          : Disable
% Netbios Naming Packet   : Pass
% Call Direction          : Both
% Idle Timeout            : 300
% PING to keep alive      : 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   : AH
% Schedule                : 0,0,0,0
% Remote Callback         : off
% Provide ISDN Number     : off
% IKE phase 1 mode        : Main mode
% IKE Local ID            :


% Dial-In Settings

--- 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 several 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 trunk

This command allows users to configure VPN Backup, VPN load balance, GRE over IPsec, and Binding tunnel policy.

Syntax

vpn trunk show_usable

vpn trunk backup *<add/del> <name> <Member#1> <Member#2>*

vpn trunk backup more_syslog *<ON/OFF>*

vpn trunk backup ERD *<name> <Normal/Recover/Resume><second>*

vpn trunk lb *<add/del> <name> <Member#1> <Member#2>*

vpn trunk lb more_syslog *<ON/OFF>*

vpn trunk lb algorithm *<name><RR/W-RR/ Fastest>*

vpn trunk bind usage *<BindIndex>*

vpn trunk bind show *<LoadBalanceName>*

vpn trunk bind reset_default

vpn trunk bind more_syslog *<ON/OFF>*

vpn trunk bind set *<BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstI p:A~B> <DstPort:A~B> <Proto> <Frag>*

vpn trunk bind insert *<After_BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstIp:A~B> <DstPort:A~B> <Proto> <Frag>*

vpn trunk SetGre show *<Dialout_Index>*

vpn trunk SetGre *<Active/In-active><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic>*

vpn trunk An_Gre GreIPsecAnalyze *<ON/OFF>*

Syntax Description

Parameter	Description
show_usable	Display a list of LAN to LAN dial out profiles.
backup <add/del> <name> <Member#1> <Member#2>	Set multiple VPN tunnels (LAN to LAN profiles) as backup tunnel. add/del - Add or delete a profile for used in VPN Trunk. name – Specify the name of the VPN trunk. Member#1 – Indicate the first LAN to LAN profile. Member#2 – Indicate the second LAN to LAN profile.
backup more_syslog	These commands are used for RD debug.

<ON/OFF> *lb more_syslog <ON/OFF>* *bind more_syslog <ON/OFF>*	
backup ERD <name> <Normal/Recover/Resume>< second>	ERD means Environment Recovers Detection. name – Specify the name of the VPN trunk. Normal – Indicate the Normal mode. All dial-out VPN TRUNK backup profiles will be activated alternatively. Recover – Indicate the duration of VPN backup operation. Resume – When VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection. Second – "0" means to dial each six seconds automatically. "60 ~ 2147483647" means to early handle for less than 30 seconds within designated time.
lb <add/del> <name> <Member#1> <Member#2>	It means to create VPN trunk with load balance. add/del - Add or delete a profile for used in VPN Trunk. name – Specify the name of the VPN trunk. Member#1 – Indicate the first LAN to LAN profile. Member#2 – Indicate the second LAN to LAN profile.
lb more_syslog <ON/OFF>	It means to enable (ON) or disable (OFF) the syslog records.
lb algorithm <name> <RR/W-RR/Fastest>	Set multiple VPN tunnels for using as traffic load balance tunnel. Such command is to configure the algorithm (with round robin mode) of Load Balance. name – Specify the name of the VPN trunk. RR – It means round robin mode. All of the dial-out profiles will be taken turns equally. Fastest - Configure the algorithm (with fastest mode) of Load Balance.
lb algorithm <name><W-RR><Auto> <AccordingRatio> <Member1:Member2>	Such command is to configure the algorithm (with round robin mode) of Load Balance. name – Specify the name of the VPN trunk. W-RR – It means weighted round robin mod based on speed ratio. ● *Auto - the speed must be based on Lay2.* ● *AccordingRatio – the speed must be based on given ratio.* Member#1 – Inidcate the first LAN to LAN profile. Member#2 – Indicate the second LAN to LAN proifle.
lb algorithm <name><Fastest>	Such command is to configure the algorithm (with fastest mode) of Load Balance. Most of traffics will be led to the channel with the

	fastest connection. name – Specify the name of the VPN trunk.
bind usage <BindIndex>	Display detailed information for VPN Load Balance Tunnel Bind. BindIndex – Indicate the index number of the tunnle bind.
bind show <LoadBalanceName>	Display the bind information for VPN Load Balance profile. LoadBalanceName – type the name of VPN Load Balance profile
bind reset_default	Reset the bind tunnel for VPN load balance to factory reset settings.
bind more_syslog <ON/OFF>	It means to enable (ON) or disable (OFF) the syslog records.
bind set <BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstI p:A~B> <DstPort:A~B> <Proto> <Frag>	Set the binding tunnel policy. BindIndex – Indicate the index number (1 ~ 64) for the tunnel to be bound. `vpn trunk bind set 1 y vpnlb 1 192.168.10.1~192.168.10.2 192.168.99.1~192.168.99.254 1~65535 0 OFF` ACT – Specify the action. “y” means active; “n” means inactive or delete. TrunkName - TrunkName - Specify the name of the VPN trunk created by using “vpn trunk lb” command. Member – Specify the index number of the LAN to LAN (dial-out) profile to be bound. SrcIp:A~B – Specify the source IP range (e.g., 192.168.10.0~192.168.10.255. DstI p:A~B - Specify the destination IP range (e.g., 192.168.1.0~192.168.1.255. DstPort:A~B – Specify the destination port range (1~65535). Proto – Specify the protocol. 0 – any 1 – ICMP 2 – IGMP 6 – TCP 17 – UDP 255 – TCP/UDP Frag – “ON” means to bind the fragmented packet; “OFF” means not to care. It is the default setting.
bind insert <After_BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstIp:A~B> <DstPort:A~B> <Proto>	It is used to insert additional load balance policy into an existing policy. After_BindIndex – Specify an index number that new additional policy should be inserted before. See the following example:

<Frag>	*vpn trunk bind insert 1 y vpnlb 2 192.168.10.3~192.168.10.200 192.168.99.200~192.168.99.200 80~80 TCP OFF* ACT – Specify the action. “y” means active; “n” means inactive or delete. TrunkName - Specify the name of the VPN trunk. Member – Specify the index number of the LAN to LAN (dial-out) profile to be bound. SrcIp:A~B – Specify the source IP range (e.g., 192.168.10.0~192.168.10.255. DstI p:A~B - Specify the destination IP range (e.g., 192.168.1.0~192.168.1.255. DstPort:A~B – Specify the destination port range (1~65535). Proto – Specify the protocol. 0 – any 1 – ICMP 2 – IGMP 6 – TCP 17 – UDP 255 – TCP/UDP Frag – “ON” means to bind the fragmented packet; “OFF” means not to care. It is the default setting.
SetGre show <Dialout_Index>	Display the GRE over IPSec settings in specified LAN to LAN profile. Dialout_Index – Index number of the LAN to LAN (dial-out) profile.
SetGre <Active/In-active><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic>	Active/In-active - Specify the action. “y” means active; “n” means inactive. Dialout_Index – Index number of the LAN to LAN (dial-out) profile. GRE_MyIP –Enter the virtual IP for router itself for verified by peer. GRE_PeerIP –Enter the virtual IP of peer host for verified by router. Logical_Traffic - Specify the action for RFC2890. “y” means active; “n” means inactive.
An_Gre GreIPsecAnalyze *<ON/OFF>*	These commands are used for RD debug.

Example

```
> vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1j
```

```
% Username : vigor
% Password : 1234
% Call Direction : Dial-Out
% Type of Server : PPTP
% Dial to : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
> vpn setup 2 market pptp_out 5.6.7.8 vigor 5678 192.168.1.31 255.255.255.0
% Profile Change Log ...

% Profile Index : 2
% Profile Name : market
% Username : vigor
% Password : 5678
% Call Direction : Dial-Out
% Type of Server : PPTP
% Dial to : 5.6.7.8
% Remote NEtwork IP : 192.168.1.31
% Remote NEtwork Mask : 255.255.255.0
> vpn trunk lb add comp 1 2
%% Combination VPN Load Balance profile list :
  <Index>   <    Name    >    <    Member1(Active)Type    >    <
Member2(Act
ive)Type    >
    1        comp                   1(YES)PPTP                    2(YES)P
PTP

%% Note: <Active: NO> The LAN-to-LAN Profile is disable or under Dial-In(Call
Di
rection) at present.
=====================================================================

%  Setting OK.
> vpn trunk bind set 1 y comp 2 192.168.10.1~192.168.10.2
192.168.99.1~192.168.99.254 1~65535 0 OFF
% VPN Load Balance Tunnel Bind Table Index[1] detail:
============================================================
 Action              = ACTIVE
 Trunk Profile(000) Name= comp
 Binding Dial Out Index = 2
 Binding Src IP        = 192.168.10.1 ~ 192.168.10.2
 Binding Dest IP       = 192.168.99.1 ~ 192.168.99.254
 Binding Dest Port     = 1 ~ 65535
 Binding Fragmented    = NO
 Binding Protocol      = ANY Protocol
>
```

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. L2I means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<index>	The index number (1 to 500) 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 - GRE over IPsec 6 - 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 GRE over IPsec - 1 ~ 1365 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
>vpn mss show
 VPN TCP maximum segment size (MSS) :
 PPTP  = 1400
 L2TP  = 1360
 IPSec = 1360
 L2TP over IPSec  = 1360
```

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 (1 to 500) 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*

vpn pass2nd *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*

vpn pass2nat *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 sameSubnet

This command allows users to build VPN between clients via virtual subnet.

Syntax

vpn sameSubnet *-i <index> -e <subnet> -I <Virtual Subnet> -o <add/del>*

vpn sameSubnet *-i <value>*

vpn sameSubnet *-i <value> –E <0/1>*

vpn sameSubnet *-i <value> –e <value>*

vpn sameSubnet *-I <Virtual Subnet>*

vpn sameSubnet *-o <add/del>*

vpn sameSubnet *-v*

vpn sameSubnet *-m <value>*

Syntax Description

Parameter	Description
-i <value>	Specify the index number of VPN profile.
-i <value> –E <0/1>	Enable or disable the IPsec with the same subnet. 1 – enable.

	0 – disable.
-i <value> –e <value>	Translate specified LAN to virtual subnet. 1 – LAN1 2 – LAN2 3 – LAN3 ...
-i <value> -I <Virtual Subnet>	Set the virtual subnet (e.g., 172.16.3.250).
-i <value> -o <add/del>	Set the operation (add or delete) for the VPN profile.
-v	Display current status of virtual subnet.
-m <value>	Set the translated type. <value> - 1 means Whole Subnet; 2 means Specific IP.

Example

```
> vpn sameSubnet -i 1 -e 1 -I 10.10.10.0 -o add
Add entry Succcess!!
> vpn sameSubnet -v
IPsec with the same subnet:
VPN profile 1 enable,
  Whole Subnet:
    translated LAN1 to Virtual subnet: 10.10.10.0
IPsec with the same subnet:
VPN profile 201 enable,
  Whole Subnet:
IPsec with the same subnet:
VPN profile 203 enable,
  Whole Subnet:
>
```

Telnet Command: vpn ovpn

This command allows users to configure general settings for OpenVPN.

Syntax

vpn ovpn *mode <0/1>*

vpn ovpn *show*

vpn ovpn *udp_mode <0/1>*

vpn ovpn *tcp_mode <0/1>*

vpn ovpn *udp_port <1-65535>*

vpn ovpn *tcp_port <1-65535>*

vpn ovpn *cert <0/1>*

vpn ovpn *replay <0/1>*

vpn ovpn *certmode <0/1/2>*

vpn openvpn *hmacmode <0/1/2>*

Syntax Description

Parameter	Description
mode <0/1>	Enable (1) or disable (0) the OpenVPN function.
show	Display the OpenVPN setting status.
udp_mode <0/1>	Enable (1) or disable (0) the UDP mode.
tcp_mode <0/1>	Enable (1) or disable (0) the TCP mode.
udp_port <1-65535>	Set the UDP port number.
tcp_port <1-65535>	Set the TCP port number.
cert <0/1>	Enable (1) or disable (0) the certificate authentication.
replay <0/1>	Enable (1) or disable (0) the replay option.
certmode <0/1/2>	Set the Cipher Algorithm Mode. 0 - AES128 1 - AES256 2 - None
hmacmode <0/1/2>	Set the Cipher HMAC mode. 0 - SHA1 1 - SHA256 2 - None

Example

```
> vpn ovpn show

 Openvpn: Enable
 support UDP: Enable
 UDP port: 1194
 support TCP: Enable
 TCP port: 1194
 Use certificate authentication: Enable
 replay option: Enable
 Cipher Algorithm: AES128
 HMAC Algorithm: SHA1
>
```

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 / mtu2

This command allows users to adjust the size of MTU for WAN.

Syntax

wan mtu *[value]*

wan mtu2 *[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 to 10). 1:WAN1 2:WAN2 3:WAN3 4:WAN4 5:WAN5 6:WAN6 7:WAN7 8:WAN8 9:WAN9 10:WAN10
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!
```

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
BWAN1: Offline, stall=N
 Mode: DHCP Client, 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

BWAN2: 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

BWAN3: Offline, stall=Y
 Mode: PPPoE, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=72581, TX Rate(bps)=0, RX Packets=112651, RX Rate(bps)=0
 Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0

BWAN4: 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

BWAN5: Online, stall=N
...
```

Telnet Command: wan detect

This command allows you to Ping a specified IP to detect the WAN connection (static IP or PPPoE mode).

Syntax

wan detect <*wan1/wan2/…*> <*on/off/strict/always_on*>

wan detect <*wan1*> <*off*> *-t* <*time*>

wan detect <*wan1*> <*off*> *-i* <*Interval*>

wan detect <*wan1/wan2/…*> **target** <*ip addr*>

wan detect <*wan1/wan2/…*> **target2** <*ip addr*>

wan detect <*wan1/wan2/…*> **target_gw** <*1/0*>

wan detect <*wan1/wan2/…*> **ttl** <*value*>

wan detect <*wan1/wan2/...*> **interval** <*interval*>

wan detect <*wan1/wan2/...*> **retry** <*retry*>

wan detect status

Syntax Description

Parameter	Description
<*wan1/wan2/...*> <*on/off/strict/always_on*>	On - It means to enable ping detection. The IP address of the target shall be set. Off - It means to enable ARP detection (default). strict - Enable Strict ARP detection. always_on - disable link detect, always connected(only support static IP)
<*wan1*> <*off*> *-t* <*time*>	Set the time (0 to 256).
<*wan1*> <*off*> *-i* <*Interval*>	Set the time interval (0 to time value).
<*wan1/wan2/...*> *target* <*ip addr*>	Set the ping target. <ip addr> : It means the IP address used for detection. Type an IP address in this field.
<*wan1/wan2/...*> *target2* <*ip addr*>	Set the secondary ping target. <ip addr>: It means the IP address used for detection. Type an IP address in this field.
<*wan1/wan2/...*> *target_gw* <*1/0*>	Set whether to use gateway as ping target. (1: yes 0: no)
<*wan1/wan2/...*> *ttl* <*value*>	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
<*wan1/wan2/...*> *interval* <*interval*>	Set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second. <interval>*:* Type a value.
<*wan1/wan2/...*>*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
 WAN7: arp detect, send time=30, Interval = 5
 WAN8: arp detect, send time=30, Interval = 5
 WAN9: always on
 WAN10: arp detect, send time=30, Interval = 5
 WAN11: arp detect, send time=30, Interval = 5
 WAN12: arp detect, send time=30, Interval = 5
 WAN13: arp detect, send time=30, Interval = 5
 WAN14: arp detect, send time=30, Interval = 5
 WAN15: arp detect, send time=30, Interval = 5
 WAN16: arp detect, send time=30, Interval = 5
 WAN17: arp detect, send time=30, Interval = 5
 WAN18: arp detect, send time=30, Interval = 5
 WAN19: arp detect, send time=30, Interval = 5
 WAN20: arp detect, send time=30, Interval = 5
 WAN21: arp detect, send time=30, Interval = 5
 WAN22: arp detect, send time=30, Interval = 5
 WAN23: arp detect, send time=30, Interval = 5

 WAN24: arp detect, send time=30, Interval = 5
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> wan detect wan1 target 192.168.1.78
 Set OK

> wan detect wan1 on
 Set OK

> wan detect status
 WAN1: on, Target=192.168.1.78, TTL=255
 WAN2: off
 WAN3: off
 WAN4: off
 WAN5: off
...
```

Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

Syntax

wan lb <*wan1/wan2/…*> *on*

wan lb <*wan1/wan2/…*> *off*

wan lb <*ip/session*>

wan lb status

Syntax Description

Parameter	Description
wan1/wan2/….	Specify which WAN will be applied with load balance.
on	Make WAN interface as the member of load balance.
off	Cancel WAN interface as the member of load balance.
<*ip/session*>	Set the load balance mode to IP(default) or session based.
status	Show the current status.

Example

```
> wan lb ip 192.168.2.25
 Set OK
> wan lb status
 WAN1: on
 WAN2: on
 WAN3: on
 WAN4: on
 WAN5: on
 WAN6: on
 WAN7: on
...
```

Telnet Command: wan lbel

This command allows you to define protocol, port and name for the traffic not to be applied with load balance.

Syntax

wan lbel <*enable*> <*idx*> <*protocol*> <*port*> <*portend*> <*comment*>

wan lbel status <*idx*>

Syntax Description

Parameter	Description
Idx	Enter the index number (1 to 32) for the exception list.
enable	Enter 1 (enable) or 0 (disable) the selected profile.
protocol	<protocol>: Enter TCP, UDP, all. "All" means "TCP+UDP".

port	Enter a number (0 to 65535) as starting port. It it is set with "0", then the port range (1 to 65535) will not be applied with load balance.
portend	Enter a number (0 to 65535) as ending port (must be greater than starting port).
comment	Enter a string (less than 11 characters) as a comment.
Status <idx>	Show the current status.

Example

```
> wan lbel 1 1 tcp 0 1 0 300 testforload
 error => 0 < port <= port_end < 65536
> wan lbel status 1
 whitelist[1] status:enable, protocol:udp, port:3478~3478,
comment:STUN
>
```

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 ... >*

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, only 2 to 9 are available for configuration.
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.

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   p7   p8   p9   p10   p11   p12   Se
rvice Type    Tag      Priority
-------------------------------------------------------------------------
   7    ON    0    0    1    1    0    0    0    0    0    0    0    0       N
ormal      0(OFF)       0
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

wan multifno <*channel #*><*WAN interface #*>

wan multifno *status*

Syntax Description

Parameter	Description
<*channel #*><*WAN interface #*>	<*channel #*> - There are several channels including VLAN and PVC. Available settings are: 13=Channel 13 14=Channel 14 … 52=Channel 52 *WAN interface #* - Enter 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 13 uplink ifno: 3
% Channel 14 uplink ifno: 3
% Channel 15 uplink ifno: 3
```

```
% Channel 16 uplink ifno: 3
% Channel 17 uplink ifno: 3
...
>
```

Telnet Command: wan vlan

This command allows you to tag packets on WAN VLAN with specified number.

Syntax

wan vlan wan <#> **tag** <*value*>

wan vlan wan <#> <*enable*/*disable*>

wan vlan wan <#> **pri** <*value*>

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.
pri <*value*>	Set the priority of the WAN interface. <value>: 0 to 7
stat	Display current VLAN status.

Example

```
> wan vlan wan 1 pri 6
> Set priority to 6 for WAN1
> wan vlan stat
% Interface    Pri     Tag    Enabled
% ====================================
% WAN1         6      0
% WAN2         0      0
% WAN3         0      0
% WAN4         0      0
% WAN5         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 (1 to 12). *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
```

Telnet Command: wan detect_mtu

This command allows you to run a WAN MTU Discovery. The user can specify an IPv4 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu *-i <Host/IP address> -s <mtu_size> -d <decrease size> -w <1: WAN1 ,2: WAN2, …> -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.
-w <number>	Specify the WAN interface. number: Enter the number of WAN interface. 1: WAN1 2: WAN2….and etc.
-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 1 -i 8.8.8.8 -s 1500 -d 30 -c 10
 detecting  mtu size:1500!!!

 mtu size:1470!!!
```

Telnet Command: wan detect_mtu6

This command allows you to run a WAN MTU Discovery. The user can specify an IPv6 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu6 *-i <Host/IP address> -s <mtu_size> -w <number>*

Syntax Description

Parameter	Description
-i <Host/IP address>	Specify the IPv6 target to detect. If can be an IPv6 address or domain name. Host/IP address: Enter the IP address/domain name of the target.
-s <mtu_size>	Specify the size of MTU. mtu_size: Available setting is 1280 ~ 1500.
-w <number>	Specify the WAN interface number: Enter the number of WAN interface. 1: WAN1 2: WAN2….and etc.

Example

```
> wan detect_mtu6 -w 2 -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 12.

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 7. 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 7. 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 4 is the selected WAN. Download threshold : 50 Kbpsl; Upload threshold : 20 Kbps. You can type as follows: *wan failover on 2 1 0 4 50 20*
show <index>	Display parameters settings for WAN interface. index – Ranges from 1 to 12.

Example

```
> wan failover on 2 1 0 4 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 setup

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	Indicate available profile to be configured. Number of profile: 1 /2 /3 / 4.
-l	Apply to LAN interfaces. E.g., apply LAN1 and LAN2: -l 1, 2.
-m	Select login mode. 0:skip

	1:click 2:social 3:pin 4:social or pin
-f	Configure facebook login. 0: disable. 1: enable.
-g	Configure google login. 0: disable. 1: enable.
-h	Enable HTTPS redirection. 0: disable. 1: enable.
-v	Enable portal detection. 0: disable. 1: enable.
-i	Configure APP ID. For example, to configure facebook APP id, you can type: >hsportal -p 1 -f -i this_is_app_id Profile 1 set facebook login disabled … [OK]
-k	Configure app key. For example, to configure google APP key, you can type: > hsportal -p 1 -g -i this_is_app_key Profile 1 set google login disabled … [OK]
-r	Configure landing page mode. 0: fixed URL. 1: user request. 2: bulletin. E.g. > hsportal -p 1 -r 0 Profile 1 set landing page mode 0 … [OK]
-e	Enable the specified profile.
-d	Disable the specified profile.
-c	Reset the specified profile. Number of profile: 1 /2 /3 / 4.
-o	Clear profiles for all clients.

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 info

This command is used to enable /disable database, notification, specify object profile for information related to hotspot web portal users.

Syntax

hsportal info -e *<0/1>*

hsportal info –c

hsportal info –n *<0/1>*

hsportal info –a *<0/1>*

hsportal info –m *<1~10>*

hsportal info –s *<1~10>*

Syntax Description

Parameter	Description
-e <0/1>	Enable database to record information. 0 - disable 1 – enable
-c	Clear user information database.
-n <0/1>	Enable notification for user information. 0 - disable 1 – enable
-a <0/1>	Enable auto backup and start a new record for user information. 0 - disable 1 – enable
-m <1~10>	Set email notigication object. 1~10- Index number of object profile.
-s <1~10>	Set SMS notigication object. 1~10- Index number of object profile.

Example

```
> hsportal info -e 1
Enabled database to record information ... [OK]
> hsportal info -a 1
Enabled auto backup and start a new record for user information ...
[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: hsportal pin_gen

This command is for future use.

Telnet Command: radius internal

This command allows you to configure detailed settings for internal RADIUS server and client.

Syntax

radius enable <*0/1*>

radius authport <*port number*>

radius set_auth_method <*method idx*>

radius client *add <idx> -i <address> -m <mask> -p <prefix> -l <length> -s <secret>*

radius client *del <idx>*

radius show

radius enable_dot1x <*0/1*>

radius set_dot1x_method -e <*method_idx*>

radius set_dot1x_method -d <*method_idx***>**

Syntax Description

Parameter	Description
enable <0/1>	Enable (1) or disable (0) the RADIUS server.
authport <port number>	Configure the port number for authentication. Port number: Available range is from 0 to 65535. Default value is "1812".
set_auth_method <method idx>	Specify which method will be used for authentication. Method idx: 0 and 1 0: Only PAP 1: PAP/CHAP/MS-CHAP/MS-CHAPv2
client add <idx> -i <address> -m <mask> -p <prefix> -l <length> -s <secret>	Specify a client to be authenticated by RADIUS server by typing required information as follows: -i <address>: client IPv4 address(domain) -m <mask>: client IPv4 mask -p <prefix>: client IPv6 prefix -l <length>: client IPv6 prefix length -s <secret>: shared secret ex: radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
client del <idx>	*del* - Delete related settings for selected client. *Idx* - Specify the index number of client profiles.
show	Display the status of RADIUS server.
enable_dot1x <0/1>	Enable (1) or disable (0) the 802.1X Authentication function of RADIUS Server. Default is disabled.
set_dot1x_method -e <method_idx>	Set a method for 802.1X authentication of RADIUS server. Method idx: 1 to 4. 1: EAP_PEAP/MSCHAPv2 2: EAP_TTLS/PAP 3: EAP_TTLS/MSCHAP 4: EAP_TTLS/MSCHAPv2
set_dot1x_method -d <method_idx>	Delete the method for 802.1X authentication of RADIUS server. Method idx: 1 to 4. 1: EAP_PEAP/MSCHAPv2 2: EAP_TTLS/PAP 3: EAP_TTLS/MSCHAP 4: EAP_TTLS/MSCHAPv2

Example

```
> radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
 Set radius server client OK
>
```

Telnet Command: radius external

This command allows you to configure detailed settings for external RADIUS server.

Syntax

radius external <*options*>...

Syntax Description

Parameter	Description
<options>...	The available commands with parameters are listed below. *[...]* means that you can type in several parameters in one line.
-V	Show current setting.
-v <index>	Show current setting for certain RADIUS profile. <index>: Enter the index number of the profile.
-l <index>	Show the server status log. <index>: Enter the index number of the profile.
-c "<index> <comment>"	Set the comment for certain RADIUS profile. <index>: Enter the index number of the profile. <comment>: Enter a string.
-f <index>	Set the selected profile as the default external RADIUS profile. <index>: Enter the index number of the profile.
-e "<index> <param>"	Enable or disable the external RADIUS profile. <index>: Enter the index number of the profile. <param>: 0 or 1. 0 is disable; 1 is enable. ex: -e "2 1" to enable the profile 2
-i "<index> <index2> <hostname/IP>"	Set the hostname or IP address for the selected RADIUS server profile. <index>: Enter the index number of the profile. <index2>: 0 or 1. 0 means the primary server; 1 means the secondary server. ex: -i "1 0 192.168.1.1" or -i "2 1 www.google.com"
-p "<index> <index2> <port_number>"	Set the destination port for the selected RADIUS server. <index>: Enter the index number of the profile. <index2>: 0 or 1. 0 means the primary server; 1 means the secondary server. <port_number>: 1 ~ 65535. ex : -p "1 1 1812"
-s "<index> <index2> <secret>"	Set the shared secret for the selected RADIUS server. <index>: Enter the index number of the profile. <index2>: 0 or 1. 0 means the primary server; 1 means the secondary server. <secret>: 1 ~ 65535. ex : -s "3 0 123"
-r "<index> <index2> <retry>"	Set the retry number for the selected RADIUS server. <index>: Enter the index number of the profile. <index2>: 0 or 1. 0 means the primary server; 1 means the secondary server. <retry>: 1 to 3. ex : -s "3 0 2"
-a "<index> <param>"	Enable or disable the accounting port for the selected RADIUS server. <index>: Enter the index number of the profile. <param>: 0 or 1. 0 is disable; 1 is enable.
-b "<index> <index2> <port_number>"	Set the accounting port for the selected RADIUS server. <index>: Enter the index number of the profile. <index2>: 0 or 1. 0 means the primary server; 1 means the secondary server. <port_number>: 1 ~ 65535. ex : -b "1 0 1813"

-d "<index> <index2> <port_number>"	Disconnect the message port for the selected RADIUS server. <index>: Enter the index number of the profile. <index2>: 0 or 1. 0 means the primary server; 1 means the secondary server. <port_number>: 1 ~ 65535. ex : -d "1 1 3799"
-u "<index> <index2> <update interval>"	Set the accounting interim interval for the selected RADIUS server. <index>: Enter the index number of the profile. <index2>: 0 or 1. 0 means the primary server; 1 means the secondary server. <port_number>: 10 ~ 1440 (minutes) ex : -u "1 0 10"

Example

```
> radius external -i "1 0 192.168.1.1"
radius external -i "1 0 192.168.1.1"
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> radius external -V
Profile default enable comment
% 1      v
% 2
% 3
% 4
```

Telnet Command: local_8021x

The command is used to configure general settings for Local 802.1X server built in Vigor router.

Syntax

local_8021x enable *<0/1>*

local_8021x set_localdot1x_method *-e <method_idx>*

local_8021x set_localdot1x_method *-d <method_idx>*

local_8021x show

Syntax Description

Parameter	Description
enable	Enable or disable the configuration. 0: disable. 1: enable.
set_localdot1x_method -e <method number>	Set the authentication method. <method_idx>: 1 to 4, 1: EAP_PEAP/MSCHAPv2 2: EAP_TTLS/PAP 3: EAP_TTLS/MSCHAP 4: EAP_TTLS/MSCHAPv2
set_localdot1x_method -d <method number>	Delete the authentication method. <method_idx>: 1 to 4, 1: EAP_PEAP/MSCHAPv2

	2: EAP_TTLS/PAP 3: EAP_TTLS/MSCHAP 4: EAP_TTLS/MSCHAPv2
show	Display current settings of local 802.1x server.

Example

```
> local_8021x set_localdot1x_method -e 1
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> local_8021x show
> local_8021x show
% Local 802.1X enable: disable
>
```

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.
IP address	It means the LAN IP address of the host. If you want to wake up LAN host by using IP address, be sure that that IP address has been bound with the MAC address (IP BindMAC).
<*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.
setdefault	It means to reset to factory default settings.
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	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*
-I <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 <MB/GB>	It means to set data quota unit (MB/GB).
user setdefault	It means to setup all user profiles to the factory default settings.

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

SSH: 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      Use%
cfg          4194304       7920          4186384         0%
bin_web      33554432      11869493      21684939        35%
cfg-bak      4194304       7920          4186384         0%
bin_web-bak 33554432       11869493      21684939        35%
> 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 Vigor3910.

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.
show	It displays current information of APM profile.
clear	It is used to remove all of the APM profile.

discover	It is used to search VigorAP on LAN.
query	It is used to query any VigorAP which has been registered to APM (Central AP Management) in Vigor router. Information related to the registered AP will be send back to Vigor router 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        - /     -

3 -              -               -           -                 -
4 -              -               -           -                 -
5 -              -               -           -                 -
6 -              -               -           -                 -
7 -              -               -           -                 -
8 -              -               -           -                 -
9 -              -               -           -                 -
10 -             -               -           -                 -
...
...
19
>
```

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 Vigor3910.
clear	It means to remove the information related to VigorAP registered Vigor3910.

Example

```
> apm cache show
MAC          Name                    Auth
------------ --------------------    --------------------
00507FF17EE5 VigorAP903              admin:admin
001DAA04F060 VigorAP1000C            admin:admin
00507FF17EE8 VigorAP903              admin:admin
>
```

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] - This number means to set RSSI threshold (-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
11.RSSI threshold : 0
flag : 0
> apm lbcfg set 1 1 1 3 1 1 1 1 1 1 -100
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 1
2. Enable station limit : 1
3. Enable traffic limit : 1
4. Limit Number : 3
5. Upload limit : 1
6. Download limit : 1
7. Enable disassociation by idle time : 1
8. Enable disassociation by Signal strength : 1
9. Traffic limit unit (upload)   : 1
10.Traffic limit unit (download) : 1
11.RSSI threshold : -100
flag : 63
>
```

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
"2021-01-04 04:12:59", "[APM] [VigorAP903_F17EE5] GET temper/traffic
data failed  "
"2021-01-04 04:13:21", "[APM] [VigorAP903_F17EE5] has no response  "
"2021-01-04 04:13:21", "[APM] [VigorAP903_F17EE5] GET temper/traffic
data failed  "
"2021-01-04 04:13:43", "[APM] [VigorAP903_F17EE5] has no response  "
"2021-01-04 04:13:43", "[APM] [VigorAP903_F17EE5] GET temper/traffic
data failed  "
>
```

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: ha set

This command can be used to configure HA settings for Vigor routers.

Syntax

ha set *[-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several parameters in one line.
-e <1/0>	1: Enable the function of High Availability (HA). 0: Disable the function of High Availability (HA).
-I <1/0>	1: Enable the function of recording the operation record of HA in Syslog. 0: Disable the function of recording the operation record of HA in Syslog.
-M <1/0>	Specify the Redundancy Method for HA. 1: Active-Standby 0: Hot-Standby
-v <1-255>	Specify the group ID (VHID) 1- 255: Setting range.
-R	Set HA settings to Factory Default.
-p <1-30>	Specify the Priority ID. 1-30: Setting range.
-k <key>	Specify the Authentication Key. Key: Max. 31 Characters.
-u <1/0>	Enable or disable the function of Update DDNS. 1: Enable. When a router changes HA status to primary, it will update DDNS automatically. 0: Disable.
-m <interface>	Specify the management interface. Interface: LAN1 ~ LAN8, DMZ.
-s	It means to get the newest status of other router (except the local router).
-y	It means sync local config to other router. Primary can executes this command. Secondary can not execute this commad.
-c <1/0>	Enable or disable the function of Config Sync. 1: Enable. 0: Disable.
-C <config type> <1/0>	Exclude the following settings from config sync. Config type: 1 (WAN setttings)
-I -[M|H|D] <interval>	Set the Config Sync Interval for HA. Minimum interval is 15 minutes. -M: Minute. Setting range is 0/15/30/45. (e.g., ha set -I -M 30) -H: Hour. Setting range is from 0 to 23. (e.g., ha set -I -H 12) -D: Day. Setting range is from 0 to 30. (e.g., ha set -I -D 15)
-h <Subnet> [<Virtual IP>]	Enable and set virtual IP to the subnet. Subnet: LAN1 to LAN8, DMZ.

	Virtual IP*:* The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.0) For example, to enable a virtual IP to the sunet, simply type: ha set –h LAN1 192.168.1.5
-d -<4/6><Subnet>	Disable a virtual IP to the subnet. 4: IPv4; 6: IPv6. Subnet: LAN1 to LAN100*.* For example, to disable a virtual IP to the subnet, just type: *ha set –h LAN1*
-o <1/0>	Run DARP protocol on IPv4 or IPv6. 0: IPv4 1: IPv6

Example

```
> ha set -h LAN1 192.168.1.5
% Enable Virtual IP on LAN1

% Set Virtual IP 192.168.1.5 OK!!

>
```

Telnet Command: ha show

This command can be used to show the *settings information* about config sync and general setup.

Syntax

ha show –c

ha show –g

Syntax Description

Parameter	Description
-c	Show the settings of config sync.
-g	Show the settings of general setup.

Example

```
> ha show -g
%  High Availability      : Disable
%  Redundancy Method      : Active-Standby
%  Group ID               : 1
%  Priority ID            : 10
```

```
%  Update DDNS            : Disable
%  Protocol               : IPv4
%  Management Interface   : LAN1
%  Authentication Key     : draytek
%  Syslog                 : OFF
%
%  [ Index | Enable | Virtual IP ]
%    LAN1    -       192.168.100.2
%    LAN2    -       192.168.200.2
%    LAN3    -       192.168.3.2
%    LAN4    -       192.168.4.2
%    LAN5    -       192.168.5.2
%    LAN6    -       192.168.6.2
%    LAN7    -       192.168.7.2
%    LAN8    -       192.168.8.2
%    LAN9    -       192.168.9.2
%    LAN10    -      192.168.10.2
%    LAN11    -      192.168.11.2
...
...
>
```

Telnet Command: ha status

This command is used to display *HA status information*.

Syntax

ha status -a <*Detail Level*>

ha status -m <*Detail Level*>

Syntax Description

Parameter	Description
-a	Show the status for all of the routers in HA group.
-m	Show the status of local router only.
Detail Level	0: Basic information. 1: Basic information with more data (e.g., firmware version, model, HTTPs port. MAC address and etc). 2: Basic information with some HA settings.

Example

```
> ha status -m 2
%   [Local Router] Marketing3910
%   IP                    : 192.168.100.1 (FE80::21D:AAFF:FE4B:3E80)
%   Status                : !
```

```
%   High Availability     : ! Disable
%   Redundancy Method     : Active-Standby
%   Group ID              : 1
%   Priority ID           : 10
%   Update DDNS           : Disable
%   Protocol              : IPv4
%   Management Interface  : LAN1
%   Authentication Key    : draytek
%   Virtual IP: (Max. 51 Virtual IPs)
%     ! OFF
%   Virtual IPv6: (Max. 51 Virtual IPv6s)
%     ON       LAN1  FE80::200:5EFF:FE00:101
%     ON       LAN2  FE80::200:5EFF:FE00:101
%     ON       LAN3  FE80::200:5EFF:FE00:101
%     ON       LAN4  FE80::200:5EFF:FE00:101
%     ON       LAN5  FE80::200:5EFF:FE00:101
%     ON       LAN6  FE80::200:5EFF:FE00:101
%     ON       LAN7  FE80::200:5EFF:FE00:101
%     ON       LAN8  FE80::200:5EFF:FE00:101
%     ON       LAN9  FE80::200:5EFF:FE00:101
%     ON       LAN10 FE80::200:5EFF:FE00:101
%     ON       LAN11 FE80::200:5EFF:FE00:101
%     ON       LAN12 FE80::200:5EFF:FE00:101
%     ON       LAN13 FE80::200:5EFF:FE00:101
%     ON       LAN14 FE80::200:5EFF:FE00:101
%     ON       LAN15 FE80::200:5EFF:FE00:101
%     ON       LAN16 FE80::200:5EFF:FE00:101
%     ON       LAN17 FE80::200:5EFF:FE00:101
%     ON       LAN18 FE80::200:5EFF:FE00:101
%     ON       LAN19 FE80::200:5EFF:FE00:101
%     ON       LAN20 FE80::200:5EFF:FE00:101
%     ON       LAN21 FE80::200:5EFF:FE00:101
%%
>
```

Telnet Command: swm show

This command is used to display general setting of of VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm show <*LAN_port*>

Syntax Description

Parameter	Description
LAN_port	Specify the LAN port number (1 to 12).

Example

```
>swm show 3

** If you want to display SWM debug log : "swm show debug log"
** Enable/Disable SWM console debug log : "swm show console log en/dis"
** Enable/Disable SWM syslog debug log  : "swm show syslog log en/dis"


** If you connected a VigorSwitch but does not display here.
** Please check the LLDP is enabled and VLAN ID is matched on VigorSwitch.

*******************************************************************************
LAN Port  Level    UP - Link Model   UP - MAC    UP - Port Model Name      MA
C         IP Address     Down - Port
--------- --------- ----------------  ------------ --------- ---------------- --
3        1        Router                     8        G2280           0
01DAA0CCD08 192.168.1.10
-------------------------------------------------------------------------------


*******************************************************************************

Internal VLAN is [Disable]


G2280           Level 1         MAC 00:1D:AA:0C:CD:08
-------------------------------------------------------------------------------

VLAN Port Table:
PVID    Port Num           Egress   Frame Type  Port Type    Ingress Flt
----- -------------------- -------- ----------- ------------ -----------
1    1-28              hybric   all        unaware      enabled
-------------------------------------------------------------------------------

VLAN Table:
VID    VLAN Name       Port Num           Forbidden Port Num
----- ------------ -------------------- --------------------
1    vlan1       1-28              none
*******************************************************************************


(Total 1 Switch)
```

Telnet Command: swm get

This command is used to **get** configuration information of VigorSwitch which connecting to Vigor router in LAN. Before using such command, make sure VigorSwitch has been managed under Vigor router (refer to Telnet Command: swm profile for adding a VigorSwitch device onto Vigor router).

Syntax

swm get <*MAC*>

Syntax Description

Parameter	Description
MAC	Enter the MAC address (e.g., 001DAA0CCD08) of the VigorSwitch.

Example

```
> swm get 001DAA0CCD08
Start get cfg from 001daa0ccd08 external switch

Please wait a few seconds...

Result: [OK].
>
```

Telnet Command: swm post

This command is used to transfer switch configuration to VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm post <*MAC*>

Syntax Description

Parameter	Description
MAC	Enter the MAC address (e.g., 001DAA0CCD08) of the VigorSwitch.

Example

```
> swm post 001DAA0CCD08
Start post cfg to 001daa0ccd08 external switch with currect settings.
Please wait a few seconds...
Result: [OK].
>
```

Telnet Command: swm auth

This command is used to display or remove the authentication record for external switch.

Syntax

swm auth *show*

swm auth *clear <index>*

Syntax Description

Parameter	Description
show	Display recorded external switch MAC address list.
clear <index>	Clear specific index of authentication record table. Index range: (1 - 30)

Example

```
> swm auth show
===== SWM Auth Records List=====
Index Model   Mac
----- ------- ------------
================================
> swm auth clear 1

 Clear index (1) swm auth record OK
```

Telnet Command: swm extvlan

This command is used to configure port VLAN of VigorSwitch. Before using such command, make sure you have configured VLAN settings well.

Syntax

swm extvlan <*LAN_Port*><*VLAN_idx*><*Port_Description*>

Syntax Description

Parameter	Description
LAN_Port	Setting range is from 1 to 12. Specify the LAN port connecting to VigorSwitch.
VLAN_idx	Type the enabled internal VLAN number. Index number range for VLAN is from 0 to 99.
Port_Description	Setting range is from 1 to 24.

Example

```
> swm extvlan 2 1 10
Set OK
```

System will cover the original VLAN settings on your VigorSwitch. Please backup the configuration file before you run this function.

System also will select the physical connect port as trunk port and let it join each VLAN group.

Before using such command, please use [swm show] to check valid VLAN index firstly.

Telnet Command: swm enable / disable

This command is used to enable / disable the external device.

Example

```
> swm enable ?
Enable Switch Mangement:   swm enable

> swm enable
External Device Discovery is not enable.
We will enable both.
```

Telnet Command: swm group

This command is used to add, edit or display the switch management group.

Syntax

swm group *set <IDX> <NAME> <1> <PASSWD>*
swm group *set <IDX> <NAME> <0>*
swm group *show*
swm group *add <IDX> <MAC>*
swm group *delete <IDX> <MAC>*

Syntax Description

Parameter	Description
set <IDX> <NAME> <1> <PASSWD>	It means to set group name and group password. <IDX>: Enter the index number (1 to 10) of the group. <NAME>: Enter the name of the group. <1>: It means the password flag. <PASSWD>: Enter a string as the password.
show	It means to display switch group status.
add <IDX> <MAC>	It means to add a switch into the group as a member switch. <IDX>: Enter the index number (1 to 10) of the group. <MAC>: Enter the MAC address of VigorSwitch.
delete <IDX> <MAC>	It means to delete a switch from the group. <IDX>: Enter the index number (1 to 10) of the group. <MAC>: Enter the MAC address of VigorSwitch.

Example

```
> swm group set 10 pease 1 jpsword
> swm group show
Index   Group Name     Passwd Flag    Member Switch
------ --------------- -----------
-------------------------------------
1       peace             1      G2280(192.168.1.10),
2                        0
3                        0
4                        0
5                        0
6                        0
7                        0
8                        0
9                        0
10      pease             1

Name              IP Address       MAC
----------------- ---------------- ------------
G2280             192.168.1.10     001daa0ccd08
```

Telnet Command: swm profile

This command is used to add, edit or display the switch management profile.

Syntax

swm profile *add/delete <MAC>*

swm profile *show*

swm profile *enable_all/disable_all <MAC>*

Syntax Description

Parameter	Description
add/delete <MAC>	It means to add or delete a member switch from the profile. <MAC>: Enter the MAC address of the switch.
show	It means to display switch profile.
enable_all/disable_all <MAC>	It means to enable or disable all LAN ports of the specified switch managed by Vigor router. <MAC>: Enter the MAC address of the member switch.

Example

```
> swm profile show
Name           IP Address      MAC           Model   Group
-------------  -------------- -----------    ------ ------------------------
G2280          192.168.1.10   001daa0ccd08   G2280   peace,pease,

IP Address     MAC          Model
---------------- ------------  ------

>
```

Telnet Command: swm detail

This command is used to configure general settings (e.g., switch name, password) and port settings for VigorSwitch.

Syntax

swm detail *comment <MAC> <COMMENT>*

swm detail *name <MAC> <NAME>*

swm detail *passwd <MAC> <PASSWD>*

swm detail *config <MAC> <config>*

swm detail *show*

swm detail *port show <MAC>*

swm detail *port <MAC> <PORT> <FLAG> <SCHED1> <SCHED2> <DESCRIPTION>*

swm detail *rate <MAC> <PORT> <i/e> <e/d>*

swm detail *rate <MAC> <PORT> <i/e> <ratelimit>*

Syntax Description

Parameter	Description
comment <MAC> <COMMENT>	It means to set a comment for VigorSwitch. <MAC>: Enter the MAC address of the VigorSwitch to be modified. <COMMENT>: Add an additional explanation for the switch.
name <MAC> <NAME>	It means to set a name for VigorSwitch. <MAC>: Enter the MAC address of the VigorSwitch to be modified. <NAME>: Enter the name of VigorSwitch.

passwd <MAC> <PASSWD>	It means to set a login password for VigorSwitch. <MAC>: Enter the MAC address of the VigorSwitch to be modified. <NAME>: Enter the login password of VigorSwitch.
config <MAC> <config>	It means to apply the configuration of VigorSwitch B to other Vigorswitch A. <MAC>: Enter the MAC address of the VigorSwitch A to be modified. <config>: Enter the index number of the profile set in VigorSwitch B.
show	It means to display comment, MAC and connection status of the switch.
port show <MAC>	It means to display a list of LAN ports of the VigorSwitch. <MAC>: Enter the MAC address of the VigorSwitch to be modified.
port <MAC> <PORT> <FLAG> <SCHED1> <SCHED2> <DESCRIPTION>	It means to set a description and schedule profile for each port of VigorSwitch. <MAC>: Enter the MAC address of the VigorSwitch to be modified. <PORT>: Enter the index number (e.g., 1 to 28) of the VigorSwitch LAN port. The number of LAN ports will vary according to the Switch to be modified. <SCHED1> <SCHED2>*:* Determine and type two index numbers of the schedule profiles you want. <DESCRIPTION>: Enter a desription for each port of VigorSwitch.
rate <MAC> <PORT> <i/e> <e/d>	It means to enable / disable the rate limit for each port of VigorSwitch. <MAC>: Enter the MAC address of the VigorSwitch to be modified. <PORT>: Enter the index number (e.g., 1 to 28) of the VigorSwitch LAN port. The number of LAN ports will vary according to the Switch to be modified. <i/e>: "i" means Ingress Rate; "e" means Egress Rate. <e/d>" "e" means enable; "d" means disable the setting.
rate <MAC> <PORT> <i/e> <ratelimit>	It means to modify the rate limit for each port of VigorSwitch. <MAC>: Enter the MAC address of the VigorSwitch to be modified. <PORT>: Enter the index number (e.g., 1 to 28) of the VigorSwitch LAN port. The number of LAN ports will vary according to the Switch to be modified. <i/e>: "i" means Ingress Rate; "e" means Egress Rate. <ratelimit>: Enter a value.

Example

```
> swm detail rate 001DAA0CCD08 1 i 5000
> swm detail comment 001DAA0CCD08 availablefor2floor
> swm detail rate 001DAA0CCD08 1 i 5000
> swm detail show
Idx  Name            MAC         Comment          Config
Status
---- ---------------- ------------  ---------------- ------------
--------
1    G2280           001daa0ccd08               1  None
Connect

> swm detail comment 001DAA0CCD08 availablefor2floor
> swm detail show
Idx  Name            MAC         Comment          Config
Status
---- ------------- ------------  -------------- ------------ --------
```

```
1   G2280          001daa0ccd08 availablefor2floor 1  None
Connect

>
```

Telnet Command: swm maintain

This command is used to reboot or reset the switch to factory default setting.

Syntax

swm maintain *reboot <MAC>*
swm maintain *reset <MAC>*
swm maintain *show*

Syntax Description

Parameter	Description
reboot <MAC>	It means to reboot VigorSwitch with current settings. <MAC>: Enter the MAC address of the VigorSwitch to be modified.
reset <MAC>	It means to reset VigorSwitch with factory default settings. <MAC>: Enter the MAC address of the VigorSwitch to be modified.
show	It means to display comment, MAC and connection status of the switch.

Example

```
> swm maintain show
Name           IP Address      MAC         Model
---------------- ---------------- ------------  ------
G2280          192.168.1.10    001daa0ccd08 G2280
> swm maintain reset 001daa0ccd08
Preparing to reset.
Please wait for few minutes and do not turn off power.
```

Telnet Command: swm search

This command is used to search Vigor Switch by MAC / IP address / specific description and display information.

Syntax

swm search *mac <MAC>*
swm search *ip <IP>*
swm search *description <Input>*

Syntax Description

Parameter	Description
Mac <MAC>	<MAC>: Enter the MAC address of the VigorSwitch to be searched.
ip <IP>	<IP>: Enter the IP address of the VigorSwitch to be searched.
description <input>	<input>: Enter the model name of the VigorSwitch to be searched.

Example

```
> swm search mac 001daa0ccd08
Type    IP Address      MAC             Description / Name        Lan Port
 UpLink Port     Level   Port
------- ----------- ----------------- --------------------------- --------
 --------------- ----- -------
Switch  192.168.1.10    00:1D:AA:0C:CD:08 G2280                      P3
   Vigor Router    0    3
>
```

Telnet Command: swm db

This command is used to enable/disable database to record switch management information.

Syntax

swm db *ctl en/dis*
swm db *ctl show*
swm db *alert notify <N/S>*
swm db *alert action <S/B>*
swm db *alert sms <IDX>*
swm db *alert mail <IDX>*

Syntax Description

Parameter	Description
ctl en/dis	It means to enable or disable the function of displaying database control status. en: Enable the function. dis: Disable the function.
ctl show	It means to show the the database control status.
alert notify <N/S>	It means to set alert notification (N or S) condition when storage exceeded. N:Don't send notification. S: Send notification.
alert action <S/B>	It means to set the alert action (S or B) condition when storage exceeded. S: Stop recording urser information. B: Backup and clean up all user info, and start a new record.
alert sms <IDX>	It means to set SMS object which will get the information from Vigor router if something wrong with VigorSwitch. <IDX>: Enter the index number of the mail object.
alert mail <IDX>	It means to set mail object which will get the information from Vigor router if something wrong with VigorSwitch. <IDX>: Enter the index number of the mail object.

Example

```
> swm db ctl en
Enable database to recoard SWM information.
>
```

Telnet Command: swm alert

This command is used to define the name of alert, level of alert (in color), and determine to record the data in the database, or send a notification message to the user based on the level.

Syntax

swm alert *enable/disable*
swm alert *show*
swm alert *en/dis <Idx>*
swm alert *set <Idx> log <e/d>*
swm alert *set <Idx> name <name>*
swm alert *set <Idx> color <O/R/N>*
swm alert *set <Idx> notif <e/d>*
swm alert *set <Idx> obj <object idx> <object value>*
swm alert *display*
swm alert *en/dis <sw/port> <mac>*
swm alert *sw show <mac>*
swm alert *set sw <mac> <incident idx> <level idx>*
swm alert *port show <mac>*
swm alert *set port <mac> <port num><incident idx> <level idx>*

Syntax Description

Parameter	Description
enable/disable	It means to enable/disable Alert mechanism. enable: Enable the mechanism. disable: Disable the mechanism.
show	It means to display a list of all alert setup.
en/dis <Idx>	It means to enable / disable the Alert Action settings. en: Enable the settings. dis: Disabel the settings. <Idx>: Enter the index number (1 to 8) of the alert action item.
set <Idx> log <e/d>	It means to enable / disable the function of creating log of alert. e: Enable the settings. d: Disabel the settings. <Idx>: Enter the index number (1 to 8) of the alert action item. Note that No Log for index 1; and log for index 2 is enabled in default.
set <Idx> name <name>	It means to set level name of each alert. <Idx>: Enter the index number (1 to 8) of the alert action item. <name>: Enter a short description of the alert.
set <Idx> color <O/R/N>	It means to define the color for each level of alert. The color of index 1 is No color and unable to be changed. <Idx>: Enter the index number (2 to 8) of the alert action item. <O/R/N>: "O" means orange; "R" means red; "N" means no color.
set <Idx> notif <e/d>	It means to enable or disable the function of sending notifiction to specified phone number via SMS. <Idx>: Enter the index number (3 to 8) of the alert action item. e: Enable the settings. d: Disabel the settings.
set <idx> obj <object idx> <object value>	It means to specify SMS/Email service object(s) for the alert item. Each alert can be set with up to four objects. <Idx>: Enter the index number (3 to 8) of the alert action item. <object idx>: Enter the queue number (1 to 4) for specifying an object profile. <object value>*:* Enter the index number (1 to 10) of the SMS/Email service object profile.

display	It means to display all switches with port alert state.
en/dis <sw/port> <mac>	It means to enable or disable the Switch Alert /Port Alert action. en: Enable the function. dis: Disable the function. <sw/port>: "sw" means Switch Alert; "port" means Port Alert. <mac>: Enter the MAC address of the VigorSwitch.
sw show <mac>	It means to display incident and alert type of the VigorSwitch. <mac>: Enter the MAC address of the VigorSwitch.
set sw <mac> <incident idx> <level idx>	It means to set incident and alert type of the VigorSwitch. <mac>: Enter the MAC address of the VigorSwitch. <incident idx>: Range 1 - ???? <level idx>: 1 - 8
port show <mac>	Display Port Incident Alert <mac>: Enter the MAC address of the VigorSwitch.
set port <mac> <port num> <incident idx> <level idx>	Set Port Incident Alert <mac>: Enter the MAC address of the VigorSwitch. <port num>: Range 1 - ???? <incident idx>: Range 1 - ???? <level idx>: 1 - 8

Example

```
> swm alert set 2 color N
> swm alert show
Idx En/Dis   Level            Color     Create    Log       Send Notification(1-4)
--- -----   ----------------- --------- --------- ----------------------------
1    En    No Alert           No Color  Disable   Disable   0  , 0  , 0  , 0
2    En    Minor Alert        No Color  Enable    Disable   0  , 0  , 0  , 0
3    En    Moderate Alert     Orange    Enable    Disable   0  , 0  , 0  , 0

4    En    Major Alert        Red       Enable    Disable   0  , 0  , 0  , 0
5    Dis                      No Color  Disable   Disable   0  , 0  , 0  , 0
6    Dis                      No Color  Disable   Disable   0  , 0  , 0  , 0
7    Dis                      No Color  Disable   Disable   0  , 0  , 0  , 0
8    Dis                      No Color  Disable   Disable   0  , 0  , 0  , 0
>
>
```

Telnet Command: swm log

This command is used to display switch managent log.

Syntax

swm log *show filter*

swm log *show day*

swm log *show week*

swm log *set level <idx> on/off*

swm log *set type <idx> on/off*

swm log *set switch <mac> on/off*

Syntax Description

Parameter	Description

show filter	It means to display the log filter setup.
show day	It means to display the quantity of day log.
show week	It means to display the quantity of week log.
set level <idx> on/off	It means to turn on or turn off the alert level. <idx>: 1 to 8. on/off: Set the status (on or off) of the alert.
set type <idx> on/off	It means to turn on or turn off the port alert/switch alert. <idx>: 1 to 2. "1" means Port Alert; "2" means Switch Alert. on/off: Set the status (on or off) of the alert.
set switch <mac> on/off	It means to set Switch Filter: <mac>: Enter the MAC address of the VigorSwitch. on/off: Set the status (on or off) of the alert.

Example

```
> swm log show filter
Index Status Level         En/Dis
----- ------ --------------- --------
1     off    No Alert         En
2     off    Minor Alert      En
3     off    Moderate Alert   En
4     off    Major Alert      En
5     off                     Dis
6     off                     Dis
7     off                     Dis
8     off                     Dis

Index Status Type
----- ------ -------------
1     on     Port Alert
2     off    Switch Alert

Index Status Switch Name    Model  Mac Address
----- ------ --------------- ------ --------------
1     on     G2280         G2280  001daa0ccd08
> swm log set level 8 on
>
```

Telnet Command: swm snmp

This command is used to display switch information via SNMP query.

Syntax

swm snmp *sys <MAC>*

swm snmp *iftbl <MAC> <port_num>*

swm snmp *poe <MAC>*

swm snmp *trpcom show <MAC>*

swm snmp *trpcom set <MAC> <name>*

Syntax Description

Parameter	Description
sys <MAC>	It means to show the system information. <MAC>: Enter the MAC address of the VigorSwitch.
iftbl <MAC> <port_num>	It means to show port interface information. <MAC>: Enter the MAC address of the VigorSwitch. <port_num>: Enter the index number (e.g., 1 to 28) of the VigorSwitch LAN port. The number of LAN ports will vary according to the Switch to be modified.
poe <MAC>	It means to show snmp POE interface information. <MAC>: Enter the MAC address of the VigorSwitch.
trpcom show <MAC>	It means to show Trap Community. <MAC>: Enter the MAC address of the VigorSwitch.
trpcom set <MAC> <name>	It means to set Trap Community. <MAC>: Enter the MAC address of the VigorSwitch. <name>: Enter a string as tramp community.

Example

```
> swm snmp sys 001daa0ccd08
sysDescr:
sysObjectID:
sysUpTime:0 hr 0 m 0 s
sysContact:
sysName:
sysLocation:
sysServices:0
ifNumber:0
> swm snmp trpcom show 001daa0ccd08
Trap Community:public
>
```

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   : Vigor3910 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 []
>
```